ABSTRACT ALGEBRA I



Pamini Thangarajah
Mount Royal University



Elementary Abstract Algebra

Pamini Thangarajah

Mount Royal University

This text is disseminated via the Open Education Resource (OER) LibreTexts Project (https://LibreTexts.org) and like the thousands of other texts available within this powerful platform, it is freely available for reading, printing, and "consuming."

The LibreTexts mission is to bring together students, faculty, and scholars in a collaborative effort to provide an accessible, and comprehensive platform that empowers our community to develop, curate, adapt, and adopt openly licensed resources and technologies; through these efforts we can reduce the financial burden born from traditional educational resource costs, ensuring education is more accessible for students and communities worldwide.

Most, but not all, pages in the library have licenses that may allow individuals to make changes, save, and print this book. Carefully consult the applicable license(s) before pursuing such effects. Instructors can adopt existing LibreTexts texts or Remix them to quickly build course-specific resources to meet the needs of their students. Unlike traditional textbooks, LibreTexts' web based origins allow powerful integration of advanced features and new technologies to support learning.



LibreTexts is the adaptable, user-friendly non-profit open education resource platform that educators trust for creating, customizing, and sharing accessible, interactive textbooks, adaptive homework, and ancillary materials. We collaborate with individuals and organizations to champion open education initiatives, support institutional publishing programs, drive curriculum development projects, and more.

The LibreTexts libraries are Powered by NICE CXone Expert and was supported by the Department of Education Open Textbook Pilot Project, the California Education Learning Lab, the UC Davis Office of the Provost, the UC Davis Library, the California State University Affordable Learning Solutions Program, and Merlot. This material is based upon work supported by the National Science Foundation under Grant No. 1246120, 1525057, and 1413739.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation nor the US Department of Education.

Have questions or comments? For information about adoptions or adaptions contact info@LibreTexts.org or visit our main website at https://LibreTexts.org.

This text was compiled on 06/08/2026

TABLE OF CONTENTS

Licensing

Preface

Chapter 0: Preliminaries

- 0.0: Introduction to proofs
- 0.1: Sets
- 0.2: Relations
- 0.3: Functions
- 0.5: Proof Templates
- 0E: Exercises

Chapter 1: Integers

- 1.1: Division Algorithm
- 1.2: Greatest common divisor and least common multiple
- 1.3: Primes
- 1.4: Integers modulo n
- 1.5 Linear Congruence
- 1E: Exercises

Chapter 2: Groups

- 2.1: Introduction to Group
- 2.2: Properties of Group Elements
- 2.3: Subgroups
- 2.4: Cyclic groups
- 2E: Exercises

Chapter 3: Permutation Groups

- 3.1: Symmetric Groups
- 3.2: Alternating Groups
- 3.3: Dihedral Groups (Group of Symmetries)
- 3E: Exercises

Chapter 4: Cosets, special groups, and homorphism

- 4.1: Cosets and Lagranges Theorem
- 4.2: Normal Supgroups and Factor Groups
- 4.3: Homomorphisms
- 4.4: On Special Groups
- 4.5: Isormormophism theorems
- 4.6: Classification of Groups
- 4E: Exercises

Chapter 5: Rings and fileds

- 5.1: Introduction to Rings
- 5.2: Ideals and Factor Rings
- 5.3: Ring Homomorphisms
- 5E: Excercises

Mock Exams (Celebration of Learning)

- Sample final
- Test 1
- Test 2

Sample Assignments with solution

- Assignment 1
- Assignment 2
- Assignment 3
- Assignment 4
- Assignment 5
- Assignment 6

Index

Glossary

Detailed Licensing

Licensing

*A detailed breakdown of this resource's licensing can be found in **Back Matter/Detailed Licensing**.*

Preface

This text introduces abstract algebra with applications in cryptography. Topics studied include groups and rings, polynomial arithmetic and the division algorithm, and congruencies.

The content was created by Pamini Thangarajah and her winter 2019 MATH 2101 class under the supervision of Pamini Thangarajah and used in MATH 2101 at Mount Royal University. Updated in winter 2021, Fall 2023 and Fall 2024.

A Note on Formatting:

Throughout this resource, practice exercises are provided at the end of each chapter. Some questions do not have an answer key to encourage students to engage with mathematics as a creative and synthetic field and to attend class for further discussion. The "Thinking Out Loud" sections are designed to prompt discussion—students are encouraged to collaborate with classmates and justify their positions using their knowledge.

Acknowledgments:

The creation of this resource was not made possible without significant help from various sources, including:

- Professor Delmar Larsen, LibreTexts, for his unconditional support
- The Department of Mathematics and Computing at Mount Royal University
- The Faculty of Science & Technology at Mount Royal University
- Former students who donated their class notes as reference material, particularly undergraduate student James Bergeron at Mount Royal University.

Thank you all so very much for your invaluable help, insights, and resources.

If you find any errors or mistakes, please email me stating the section number.

Pamini Thangarajah, PhD

Calgary, Alberta

September 2024, last edited in December 2024.

email: pthangarajah@mtroyal.ca

- **Preface** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.

Chapter 0: Preliminaries

This page titled Chapter 0: Preliminaries is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

0.0: Introduction to proofs

This page is a draft and is under active development.

0.0.1 Introduction to Proofs/Contradiction

In this section, we will explore different techniques of proving a mathematical statement "If p then q". ($p \to q$). This is a **conditional statement**.

0.0.2 From DR. THI DINH'S PROOF WRITING HANDBOOK THIS BIBLE:

0.0.2.0.1 In the beginning...

Let P and Q be statement variables. When needed, suppose that P = P(x) depends on a variable x. The symbol "$\forall$" means "for all" or "for any". The symbol $\exists$ means "there exists".

Type of statement	**What must we do to prove that it is true**
(1) If P, then Q (2) $\forall P$, Q	Suppose that P is true. Prove that Q is true.
(3) $\exists x P(x)$ such that Q	Choose x so that $P(x)$ is true. Prove that Q is true. Note: You **need not** explain how you find x.

0.0.2.0.1 The first (and only) commandment

To prove that a statement is **false**, thou shalt **write out the negation of the statement and prove that**.

0.0.2.0.1 The five cardinal sins

- When proving any of the types of statements (1), (2), or (3):

1. **Thou shalt not**: suppose that Q is true.

2. **Thou shalt not**: overuse symbols and violate the rules of English grammar. You must write in full sentences and use symbols correctly.

- When proving a statement of the form (2) P, Q:

3. **Thou shalt not**: choose or exhibit an example in place of a proof.

- When proving a statement of the form (3) "$\forall x P(x)$ such that Q:

4. **Thou shalt not**: attempt to construct all possible x so that $P(x)$ and Q are true.

- When proving a statement by contradiction:

5. **Thou shalt not**: claim a contradiction has been reached without explanation. You must clearly identify the contradiction being made by making a statement of the form "P and NOT P, which is a contradiction".

0.0.2.1 Direct Proof

In this technique, we shall assume p and show that q is true.

Theorem 0.0.1

Let n be an integer. If n is even then n^2 is even.

Proof

Assume that n is even. Then $n = 2m$ for some integer m.

Consider $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$. Since m is an integer, $(2m^2)$ is an integer.

Thus n^2 is even.□

Example 0.0.1

Show that for all integers n, if n is odd then n^2 is odd.

Proof

Assume that n is odd. Then $n = 2m + 1$ for some integer m.

Consider $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$.

Since m is an integer, $(2m^2 + 2m)$ is an integer.

Thus n^2 is odd.□

0.0.2.2 Proof by Contrapositive

In this technique, we shall assume $\neg p$ and show that $\neg q$ is true.

Theorem 0.0.2

Let n be an integer. If n^2 is even then n is even.

Proof

We shall prove this statement by assuming n is odd. Then $n = 2m + 1$ for some integer m.

Consider $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$.

Since m is an integer, $(2m^2) + 2m$ is an integer.

Thus n^2 is odd.□

Example 0.0.2

Show that for all integers n, if n^2 is odd then n is odd.

Proof

We shall prove this statement by assuming n is even. Then $n = 2m$ for some integer m.

Consider $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$.

Since m is an integer, $(2m^2)$ is an integer. Thus n^2 is even.□

0.0.2.3 Proof by Contradiction

In this technique, we shall assume the negation of the given statement is true, and come to a contradiction.

Theorem 0.0.3

$\sqrt{2}$ is irrational.

Proof

Assume that $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{b}{a}$, where $b \in \mathbb{Z}, a \in \mathbb{Z} \setminus \{0\}$, with no common factors between a and b. Now, $\sqrt{2}a = b$. Then $2a^2 = b^2$. Since 2 divides $2a^2$, 2 divides b^2. Thus b^2 is even. Therefore, b is even, (by theorem 2). Since b is even, 2 divides b. Therefore, 2^2 divides b^2.

Since $2a^2 = b^2$, 2^2 divides $2a^2$. Therefore, 2 divides a^2. Which implies a is even. This contradicts the fact that a and b have no common factors. Thus $\sqrt{2}$ is irrational.□

0.0.2.4 Proof by Counterexample

Example 0.0.3:

Decide whether the statement is true or false and justify your answer:

For all integers a, b, u, v, and $u \neq 0, v \neq 0$, if $au + bv = 0$ then $a = b = 0$.

Solution: The statement is false.

Counterexample: Choose $a = 1, b = -1, u = 2, v = 2$, then $au + bv = 0$, but $a \neq 0 . b \neq 0, a \neq b$.

0.0.2.5 Mathematical Induction

Process of Proof by Induction

Let $p(n)$ be a mathematical statement, $n \in \mathbb{N}$ i.e., $n \geq 1$.

1. Prove the statement is true for the lowest value of n.
2. Assume that $p(n)$ is true for all $n = k$.
3. Prove $p(k + 1)$ is true.

✔ Example 0.0.4

Prove $2^n > n + 4$ for $n \geq 3, n \in \mathbb{N}$.

Proof

Let $n = 3$. Then $2^3 > 3 + 4$ is true since clearly $8 > 7$. Thus the statement is true for $n = 3$.

Assume that $2^n > n + 4$ is true for some $n = k$.

We will show that $2^{k+1} > (k + 1) + 4$.

Consider $2^{k+1} = 2 \cdot 2^k > 2 \cdot (k + 4) = 2k + 8$.

Since $2k > k + 1$ and $8 > 4$, we have $2k + 8 > (k + 1) + 4$.

Thus the statement is true for all $n = k$.

By induction, $2^n > n + 4$ for all $n \geq 3, n \in \mathbb{Z}$.□

✔ Example 0.0.5

Show that $9|(10^{n+1} + 3(10^n) + 5), \forall n \geq 1$.

Proof

Let $n = 1$. Then $9|(10^2) + 3(10) + 5$, which is $9|135$, which is true since $135 = 9(15)$ and $15 \in \mathbb{Z}$.

Assume that $9|(10^{n+1} + 3(10^n) + 5$ is true for some $n = k$.

We will show that $10^{k+1+1} + 3(10^{k+1}) + 5 = 9m$ for some $m \in \mathbb{Z}$.

Consider $10^{k+1+1} + 3(10^{k+1}) + 5 = 10(10^{k+1} + 3(10^k) + 5) - 9(5)$

$= 10(9m) - 9(5)$

$= 9(10m - 5)$, where $10m - 5 \in \mathbb{Z}$.

By induction, $9|(10^{n+1} + 3(10^n) + 5), \forall n \geq 1$.□

Example 0.0.6

Show that $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2},\ \forall\ n \geq 1$.

Proof

Let $n = 1$. Then $1 = \frac{1(1+1)}{2}$ which is true.

Assume $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$ is true for some $n = k$.

We will show that $1 + 2 + 3 + \cdots + n + (n + 1) = \frac{(n+1)(n+1+1)}{2}$

Consider $1 + 2 + 3 + \cdots + n + (n + 1) = [1 + 2 + 3 + \cdots + n] + (n + 1)$.

$= \frac{n(n+1)}{2} + (n + 1)$

$= \frac{n(n+1)+2(n+1)}{2}$

$= \frac{(n+1)(n+1+1)}{2}$.

By induction, $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2},\ \forall\ n \geq 1$.□

Example 0.0.7

Prove that $3|(10^{n+1} + 10^n + 1),\ \forall\ n \geq 1$.

Proof

Let $n = 1$. Then $3|(10^2 + 10 + 1)$ is true since $111 = 3(37)$ and $37 \in \mathbb{Z}$.

Assume that $3|(10^{n+1} + 10^n + 1)$ for some $n = k$.

We will show that $10^{k+1+1} + 10^{k+1} + 1 = 3m, m \in \mathbb{Z}$.

Consider $10^{k+1+1} + 10^{k+1} + 1 = 10(10^{k+1} + 10^k + 1) - 9(1)$

$= 10(3m) - 3(3)$

$= 3(10m - 3)$ where $10m - 3 \in \mathbb{Z}$.

By induction, $3|(10^{n+1} + 10^n + 1),\ \forall\ n \geq 1$.□

0.0.3 Bi-conditional statements

Bi-conditional statements are conditional statements which depend on both component propositions. They read "p if and only if q" and are denoted $p \leftrightarrow q$ or "p iff q", which is logically equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$.

Example 0.0.8

Consider the statement: "Two lines are perpendicular **if and only if** they intersect to form a right angle."

The component propositions are:

1. p: Two lines are perpendicular
2. q: [The lines] intersect to form a right angle

Logically, we can see that if two lines are perpendicular, then they must intersect to form a right angle. Also, we can see that if two lines form a right angle, then they are perpendicular.

If two lines are not perpendicular, then they cannot form a right angle. Conversely, if two lines do not form a right angle, they cannot be perpendicular. This is why, if both propositions in a biconditional statement are false, the statement itself is true!

0.0.4 Proof Do's and Dont's

0.0.4.1 Do's:

1. Write the statement to be proved. It should be clear what you are proving.
2. Clearly mark the beginning of your proof with the word "*Proof*".
3. Make your proof self-contained. In particular, identify all variables used in your proof in the body of your proof.
4. Write proof in complete English sentences.

Example 0.0.9: Acceptable

Proof: Let $n \in \mathbb{Z}$. Assume n is an even integer. Then $n = 2k$, for some $k \in \mathbb{Z}$.

Example 0.0.10: Unacceptable

Proof: n is even $\implies$ 2k.

5. Indicate what method of proof you are using. (The default assumption is that it is a direct proof).

6. Learn the definitions and how they come into play when proving various types of statements.

0.0.4.2 Don'ts:

1. Argue from examples. A general statement can't be proved true by showing it is true for special cases.
2. Use the same letter to mean two different things within a proof.

Example 0.0.11:

Proof: Let $n \in \mathbb{Z}$. Assume n is an even integer. Then $n = 2k$, for some $k \in \mathbb{Z}$. So $n^2 = 4K^2 = 2(2k^2)$. Thus $n^2 = 2k, k \in \mathbb{Z}$ is even. (The reader asks, does $n = n^2$?)

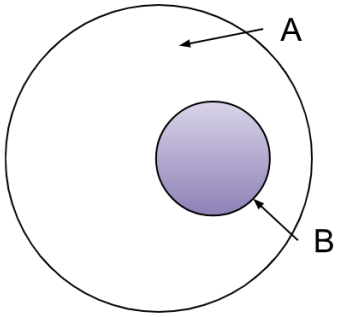
3. Assume what you are trying to prove. This is also known as begging the question. You can do it inadvertently in the middle of proof if you are not careful.

This page titled 0.0: Introduction to proofs is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

- **0.2: Introduction to Proofs/Contradiction** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.
- **1.1: Compound Statements** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.
- **0.3: Proof Do's and Dont's** by Pamini Thangarajah is licensed CC BY-NC-ND 4.0.

0.1: Sets

0.1.0.1 Sets



- Sets are collections of objects,
- Sets are normally denoted by capital letters.
- Elements are denoted by lower-case letters.
- Subsets:
  - Every element of B is an element of A, written as $B \subset A$.
  - $B = \{a \in A : \ldots..$condition on okay!.
  - Trivial subsets of A are A and $\emptyset$ (empty set).
- How do we test if an element belongs to a set?

Example 0.1.1

$M_{22}(\mathbb{R}) :=$ set of all 2 x 2 matrices with real numbers, where $\mathbb{R} :=$ set of all real numbers.

Let $A = \left\{ [x] \in M_{22}(\mathbb{R}) | \, [x] \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} [x] \right\}$.

Determine whether the following entries belong to A.

1. $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ does not belong to A.

Answer

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ and
$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

Since $\begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \notin A$.□

2. $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ does belong to A.

Answer

$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = [0 \quad 10 \quad 0]$
$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$

Since $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in A$.□

3. $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ does not belong to A.

Answer

$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}$

$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}\cdot\begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}=\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix}$

Since $\begin{bmatrix}0 & 0\\1 & 1\end{bmatrix}\neq\begin{bmatrix}1 & 0\\1 & 0\end{bmatrix},\begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}\notin A$.□

4. $\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$ does not belong to A.

Answer

$\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\cdot\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}=\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$

$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}\cdot\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}=\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}$

Since $\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\neq\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix},\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\notin A$.□

5. $\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$. does belong to A.

Solution

This one is obviously true, thus $\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}\in A$.

Notations:

- $\cup$ or / union
- $\cap$ and / intersection
- $\{\}^c$ complement of a set (aka $\{\}'$).
- $A\backslash B$ is equivalent to $A\cap B'$.
- $\mathbb{Z}:=$ set of all integers $=\{\ldots,-2,-1,0,1,2,\ldots\}$. A countable set.
- $\mathbb{Q}:=$ set of all rational numbers $=\{\frac{a}{b}:a,b\in\mathbb{Z},b\neq 0\}$. A countable set.
- $\mathbb{Q}^c:=$ set of all irrational numbers $=\{\pm e,\pm\pi,\pm\sqrt{2},\ldots\}$. Not a countable set.
- $\mathbb{R}:=$ set of all real numbers $=\mathbb{Q}\cup\mathbb{Q}^c$. Note $\mathbb{Q}\cap\mathbb{Q}^c=\emptyset$. Not a countable set.
- $\mathbb{C}:=$ set of all complex numbers.
- $M_{mn}(\mathbb{R}):=$ set of all $m\times n$ matrices over real numbers.
- $M_{mn}(\mathbb{C}):=$ set of all $m\times n$ matrices over complex numbers.
- The cardinality of a set A is written as $|A|$.
-

Example 0.1.2

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

Example 0.1.3

Let $A=\{1,2,3,5\}$. Therefore $|A|=4$. In this case, A is called a finite set.

This page titled 0.1: Sets is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

0.2: Relations

Definition: Binary Relation

Let S be a nonempty set. Then any subset R of $S \times S$ is said to be a relation over S. In other words, a relation is a rule that is defined between two elements in S. Intuitively, if R is a relation over S, then the statement aRb is either **true** or **false** for all $a, b \in S$.

If the statement aRb is false, we denote this by $a \not R b$.

Example 0.2.1:

Let $S = \{1, 2, 3\}$. Define R by aRb if and only if $a < b$, for $a, b \in S$.

Then $1R2, 1R3, 2R3$ and $2 \not R 1$.

We can visualize the above binary relation as a graph, where the vertices are the elements of *S*, *and* there is an edge from a to b if and only if aRb, *for* $ab \in S$.

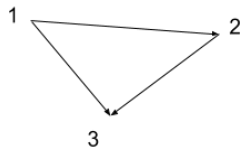


Figure **0.2.1**: Relation as a graph. (Copyright: Pamini Thangarajah)

The following are some examples of relations defined on $\mathbb{Z}$.

Example 0.2.2:

1. Define R by aRb if and only if $a < b$, for $a, b \in \mathbb{Z}$.
2. Define R by aRb if and only if $a > b$, for $a, b \in \mathbb{Z}$.
3. Define R by aRb if and only if $a \leq b$, for $a, b \in \mathbb{Z}$.
4. Define R by aRb if and only if $a \geq b$, for $a, b \in \mathbb{Z}$.
5. Define R by aRb if and only if $a = b$, for $a, b \in \mathbb{Z}$.

Definition: Divisor/Divides

Let a and b be integers. We say that a divides b is denoted $a \mid b$, provided we have an integer m such that $b = am$. In this case we can also say the following:

- b is divisible by a
- a is a factor of b
- a is a divisor of b
- b is a multiple of a

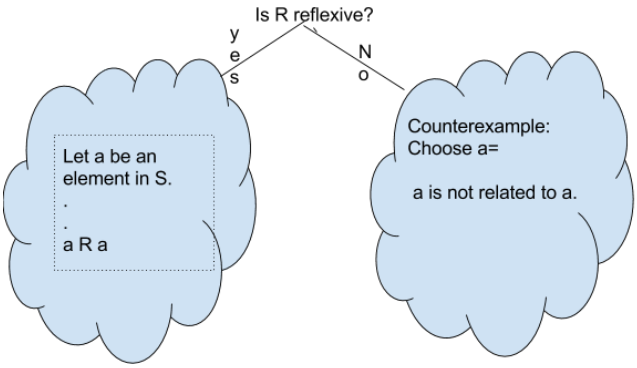
If a does not divide b, then it is is denoted by $a \nmid b$.

0.2.1 Properties of binary relation:

Definition: Reflexive

Let S be a set and R be a binary relation on S. Then R is said to be reflexive if $aRa, \forall a \in S$.

We will follow the template below to answer the question about reflexive.



Example 0.2.7:

Define R by aRb if and only if $a < b$, for $a, b \in \mathbb{Z}$. Is R reflexive?

Counter Example:

Choose $a = 2$.

Since $2 \not< 2$, R is not reflexive.

Example 0.2.8:

Define R by aRb if and only if $a \mid b$, for $a, b \in \mathbb{Z}$. Is R reflexive?

Proof:

Let $a \in \mathbb{Z}$. Since $a = (1)(a)$, $a \mid a$.

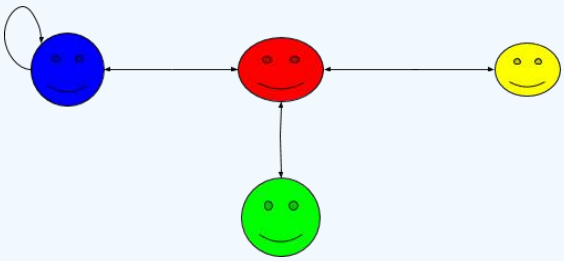
Thus R is reflexive. □

Definition: Symmetric

Let S be a set and R be a binary relation on S. Then R is said to be symmetric if the following statement is true:

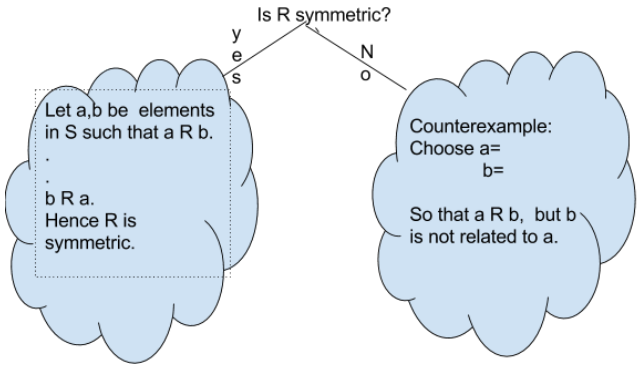
$\forall a, b \in S$, if aRb then bRa, in other words, $\forall a, b \in S, aRb \implies bRa$.

Example 0.2.8: Visually



$\forall a, b \in S, aRb \implies bRa$. holds!

We will follow the template below to answer the question about symmetric.



Example 0.2.9:

Define R by aRb if and only if $a < b$, for $a, b \in \mathbb{Z}$. Is R symmetric?

Counter Example:

$1 < 2$ but $2 \not< 1$.

Example 0.2.10:

Define R by aRb if and only if $a \mid b$, for $a, b \in \mathbb{Z}$. Is R symmetric?

Counter Example:

$2 \mid 4$ but $4 \nmid 2$.

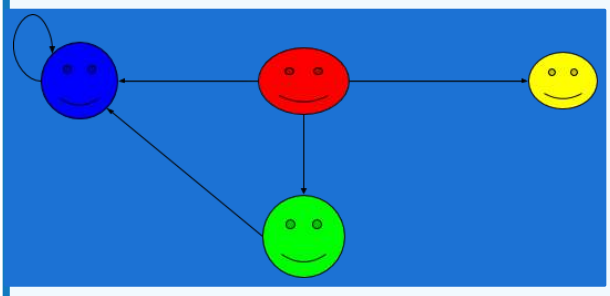
Definition: Transitive

Let S be a set and R be a binary relation on S. Then R is said to be transitive if the following statement is true

$\forall a, b, c \in S$, if aRb and bRc, then aRc.

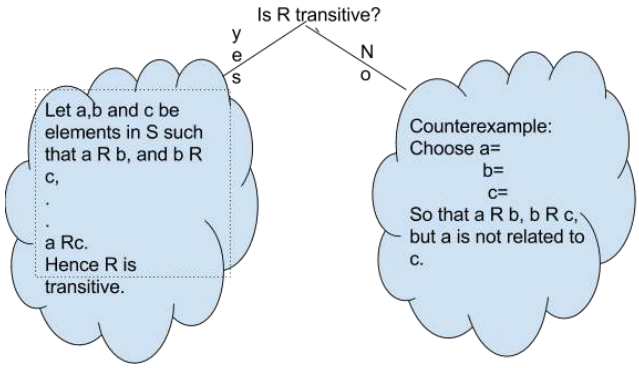
In other words, $\forall a, b, c \in S$, $aRb \wedge bRc \implies aRc$.

Example 0.2.14: VISUALLY



$\forall a, b, c \in S$, $aRb \wedge bRc \implies aRc$ holds!

We will follow the template below to answer the question about transitive.



Example 0.2.15:

Define R by aRb if and only if $a < b$, for $a, b \in \mathbb{Z}$. Is R transitive?

Example 0.2.16:

Define R by aRb if and only if $a \mid b$, for $a, b \in \mathbb{Z}_+$. Is R transitive?

Definition: Equivalence Relation

A binary relation is an equivalence relation on a nonempty set S if and only if the relation is reflexive(R), symmetric(S) and transitive(T).

Example 0.2.1: =

Let $S = \mathbb{R}$ and R be =. Is the relation a) reflexive, b) symmetric, c) antisymmetric, d) transitive, e) an equivalence relation, f) a partial order.

Solution:

1. Yes R is reflexive.

   Proof:

   Let $a \in \mathbb{R}$.

   Then $a = a$.

   Hence R is reflexive. ■

   Yes R is symmetric.

   Proof:

   Let $(a, b) \in \mathbb{R}$ such that $a = b$.

   Clearly $b = a$.

   Hence R is symmetric. ■

Yes R is antisymmetric.

Proof:

Let $a, b \in \mathbb{R}$ s.t. $a = b$ and $b = a$. Then clearly $a = b \; \forall a, b \in \mathbb{R}$. ■

Yes R is transitive.

Proof:

Let $a, b, c \in \mathbb{R}$ s.t. $a = b$ and $b = c$.

We shall show that aRc.

Since $a = b$ and $b = c$ it follows that $a = c$

Thus aRc. ■

Yes R is an equivalence relation.

Proof:

Since R is reflexive, symmetric and transitive, it is an equivalence relation.

Yes R is a partial order.

Proof:

Since R is a partial order since R is reflexive, antisymmetric and transitive.

Example 0.2.2: Less than or equal to

Let $S = \mathbb{R}$ and R be $\leq$. Is the relation a) reflexive, b) symmetric, c) antisymmetric, d) transitive, e) an equivalence relation, f) a partial order.

Solution

1. Yes, R is reflexive.

Proof:

We will show that aRa is true.

Let $a \in S$ that is $a \in \mathbb{R}$.

Since $a \leq a$, R is reflexive.□

2. No, R is not symmetric.

Counterexample:

Let $a = 2$ and $b = 3$ which are both $\in \mathbb{R}$.

It is true that $2 \leq 3$, but it is not true that $3 \leq 2$.

Thus R is not symmetric.□

3. Yes, R is antisymmetric.

Proof:

We will show that given $a \leq b$ and $b \leq a$ that $a = b$.

Since $a \leq b$, $\exists \{x \in \mathbb{R} : x > 0\}$ s.t. $a + x = b$.

Further, since $b \leq a$, $\exists \{y \in \mathbb{R} : y > 0\}$, $b + y = a$.

Then $a + x - a - b$.

Thus, $x + y = 0$.

Since, $x, y > 0$, $x, y = 0$ thus $a = b$.□

4. Yes, R is transitive.

Proof:

We will show that given $a \leq b$ and $b \leq c$ that $a \leq c$.

Since $a \leq b$, $\exists \{x \in \mathbb{R} : x > 0\}$ s.t. $a + x = b$.

Further, since $b \leq c$, $\exists \{y \in \mathbb{R} : y > 0\}$, $b \mid y = c$.

Then $a \quad x \mid y \leq c$.

Since, $x.y > 0$, thus $a \leq c$.□

5. No, R is not an equivalence relation on S since it is not symmetric.

6. Yes, R is a partial order on S since it is reflexive, antisymmetric and transitive.

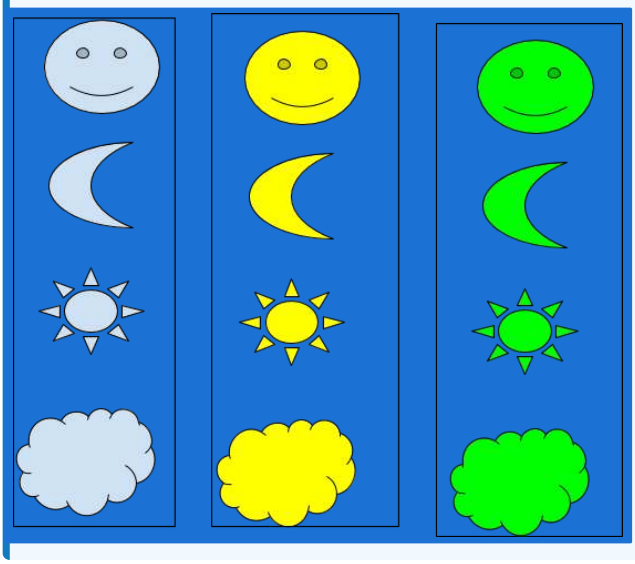
Definition: Equivalence Class

Given an equivalence relation R over a set S, for any $a \in S$ the equivalence class of a is the set $[a]_R = \{b \in S \mid aRb\}$, that is $[a]_R$ is the set of all elements of S that are related to a.

Example 0.2.3: Equivalence relation

Define a relation that two shapes are related iff they are the same color. Is this relation an equivalence relation?

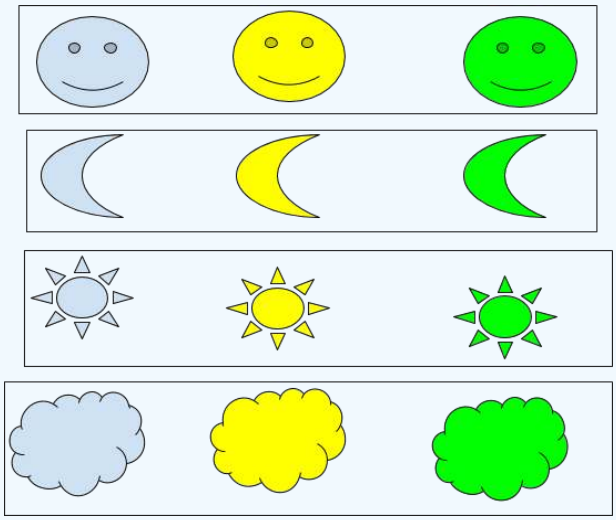
Equivalence classes are:



Example 0.2.4:

Define a relation that two shapes are related iff they are similar. Is this relation an equivalence relation?

Equivalence classes are:



Definition: Partition

Let A be a nonempty set. A partition of A is a set of nonempty pairwise disjoint sets whose union is A.

Note

For every equivalence relation over a nonempty set S, S has a partition.

Theorem 0.2.1

If $\sim$ is an equivalence relation over a nonempty set S. Then the set of all equivalence classes is denoted by $\{[a]_\sim | a \in S\}$ forms a partition of S.

This means

1. Either $[a] \cap [b] = \emptyset$ or $[a] = [b]$, for all $a, b \in S$.

2. $S = \cup_{a \in S} [a]$.

Proof

Assume $\sim$ is an equivalence relation on a nonempty set S.

Let $x, y \in S$. If $[x]_\sim \cap [y]_\sim = \emptyset$, then we are done. Otherwise,

assume $[x]_\sim \cap [y]_\sim \neq \emptyset$.

Let a be the common element between them.

Let $a \in [x]_\sim \cap [y]_\sim$

Then $a \in [x]_\sim$ and $a \in [y]_\sim$, which means that $a \sim x$ and $a \sim y$.

Since $\sim$ is an equivalence relation and $a \sim x, x \sim a$.

Since $x \sim a$ and $a \sim y$ (due to transitive property), $x \sim y$.

Thus $y \in [x]_\sim$ and $x \in [y]_\sim$.

Hence $[x]_\sim = [y]_\sim$.

Next, we will show that $S = \cup_{x \in S} [x]_\sim$.

First we shall show that $S \subseteq \cup_{x \in S} [x]_\sim$.

Let $m \in S$.

Then $[m]_\sim$ exists and $m \in [m]_\sim$.

Hence $m \in \cup_{x \in S} [S]_\sim$.

Thus $S \subseteq \cup_{x \in S} [x]_\sim$.

Conversely, we shall show that $\cup_{x \in S} [x]_\sim \subseteq S$.

Let $d \in \cup_{x \in S} [x]_\sim$.

Then $d \in [x]_\sim$ for some $x \in S$.

Thus $d \sim x \therefore d \in S$.

Thus $\cup_{x \in S} [x]_\sim \subseteq S$.

Since $S \subseteq \cup_{x \in S} [x]_\sim$ and $\cup_{x \in S} [x]_\sim \subseteq S$, then $S = \cup_{x \in S} [x]_\sim$. $\square$

For the following examples, determine whether or not each of the following binary relations R on the given set A is reflexive, symmetric, antisymmetric, or transitive. If a relation has a certain property, prove this is so; otherwise, provide a counterexample to show that it does not. If R is an equivalence relation, describe the equivalence classes of A.

Example 0.2.5:

Let $S = \{0,1,2,3,4,5,6,7,8,9\}$. Define a relation R on $A = S \times S$ by $(a,b)R(c,d)$ if and only if $10a+b \leq 10c+d$.

Solution

1. R is reflexive on S.

Proof:

Let $(a,b) \in A$.

We will show that $10a \quad b < 10a \mid b$.

Since $10a+b = 10a-b$, then $10a+b < 10a+b$.

Since $(a,b)R(a,b)$, R is reflexive on S.□

2. is not symmetric on S.

Counter Example:

Let $a \quad 0, b \quad 1, c \quad 2, d \quad 3$.

Note $10(0)+1 < 10(2)+3$, specifically $(a,b)R(c,d)$, $1 < 23$ is true.

However, $(c,d)R(a,b)$, $23 < 1$ is false.

Since $b \not R\, a$, R is not symmetric on S.□

3. is antisymmetric on S.

Proof:

Let $a,b,c,d \in S$ s.t. $10a+b < 10c+d$ and $10c+d < 10a+b$.

Since $10a \mid b < 10c \mid a$ and $10c \quad d < 10a \mid b$, $10a+b = 10c+d$.

We will show that $a - c$ and $b - a$.

$0 \leq a,b,c,d \leq 9$ by definition.

Since $0 \leq b,d \leq 9$ and $0 \leq a,c \leq 9$, $10a = 10c$ thus $a \quad c$.

Since $a \quad c, b = d$.

Thus $(a,b)R(c,d)$ is antisymmetric on S.□

5. is transitive on S.

Proof:

Let $a,b,c,d,e,f \subset S$ s.t. $10a \mid b < 10c \mid a$ and $10c+d < 10e+f$.

We will show that $10a \quad b < 10e \mid f$.

Since $10a+b < 10c+d$, $10a \quad b < 10e \quad f$.

Thus R is transitive on S.□

6. is not an equivalence relation since it is not reflexive, symmetric, and transitive.

Example 0.2.6:

Let $A = \mathbb{Z}\backslash\{0\}$. Define a relation R on A, by aRb if and only if $ab > 0$.

Solution

1. R is reflexive on A.

Proof:

Let $a \in \mathbb{Z} \setminus \{0\}$ we will show that $a \cdot a > 0$.

Clearly $a^2 > 0$ since $a \neq 0$ and a negative integer multiplied by a negative integer is a positive integer in $\mathbb{Z}$.

Since aRa, R is reflexive on A.□

2. is symmetric on A.

Proof:

We will show that if aRb, then bRa.

Let $a, b \in A$ s.t. aRb, that is $ab > 0$.

Since $ab = ba \in \mathbb{Z}$, $ba > 0$.

Since bRa, R is symmetric on A.□

3. is not antisymmetric on A.

Counter Example:

Let $a = 3$ and $b = 4$ then $3 \cdot 4 > 0$ and $4 \cdot 3 > 0$.

Since $3 \neq 4$, R is not antisymmetric on A.□

4. is transitive on A.

Proof:

Let $a, b \in A$ s.t $ab > 0$ and $b, c \in A$ s.t. $bc > 0$.

There are two cases to be examined:

Case 1: $a > 0$ and $b > 0$.

Since $b > 0$, $c > 0$ thus $ac > 0$.

Case 2: $a < 0$ and $b < 0$.

Since $b < 0$, $c < 0$ thus $ac > 0$.

Since $(a\ R\ c)$ in both possible cases R is transitive on A.□

5. Since R is reflexive, symmetric and transitive, it is an equivalence relation. Equivalence classes are $[1]$ and $[-1]$.

Let $a \in A$, then $[a] = \{x \in A : x \sim a\}$

$= \{x \in A : xa > 0\}$.

Case 1: $a > 0$, then $x > 0$.

$[a] = \{x \in A : x > 0\}$.

$[1] = \{1, 2, 3, \ldots\}$.

Case 2: $a < 0$, then $x < 0$.

$[a] = \{x \in A : x < 0\}$.

$[-1] = \{\ldots, -3, -2, -1\}$.

Note this is a partition since $[x] \cap [y] = \emptyset$ or $[x] = [y], \forall x, y \in S$. So we have all the intersections are empty.

$[1] \cap [-1] = \emptyset$.

Further, we have $S = \bigcup_{x \in S} [x]$. Note that 0 is excluded from S.

Recall:

Let $m, n \in \mathbb{Z}$.

We say that m divides n (written as $m|n$) if $n = mk$ for some $k \in \mathbb{Z}$.

Example 0.2.7

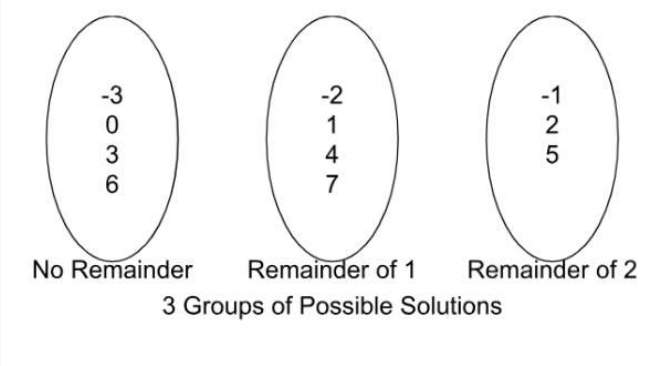
Let $S = \mathbb{Z}, m \in \mathbb{Z}_+$. Define aRb if and only if $m|(a-b), \forall a, b \in \mathbb{Z}$.

Note that m is a positive integer.

Let $m = 3$. Choose $a = 1$ and $b = 2$.

Are 1 and 2 related? i.e. does $3|1-2$? Does $1-2 = 3k, k \in \mathbb{Z}$? Since there is no integer k s.t. $-1 = 3k$, $\therefore$ 1 is not related to 2.

However, we can see that we have three groups, as shown in the image below:



Definition: Modulo

Let $m \in \mathbb{Z}_+$.

a is congruent to b modulo m denoted as $a \equiv b (mod\, n)$, if a and b have the remainder when they are divided by n, for $a, b \in \mathbb{Z}$.

0.2.2 Properties

Let $n \in \mathbb{Z}_+$. Then

0.2.2.0.1 Theorem 1 :

Two integers a and b are said to be congruent modulo n, $a \equiv b (mod\, n)$, if all of the following are true:

a) $m \mid (a-b)$.

b) both a and b have the same remainder when divided by n.

c) $a - b = kn$, for some $k \in \mathbb{Z}$.

NOTE: Possible remainders of n are $0, ..., n-1$.

0.2.2.1 Reflexive Property

0.2.2.1.1 Theorem 2:

The relation " $\equiv$ " over $\mathbb{Z}$ is reflexive.

Proof: Let $a \in \mathbb{Z}$.

Then $a - a = 0(n)$, and $0 \in \mathbb{Z}$.

Hence $a \equiv a (mod\, n)$.

Thus congruence modulo n is Reflexive.

0.2.2.2 Symmetric Property

0.2.2.2.1 Theorem 3:

The relation " $\equiv$ " over $\mathbb{Z}$ is symmetric.

Proof: Let $a, b \in \mathbb{Z}$ such that $a \equiv b$ (mod n).

Then $a - b = kn$, for some $k \in \mathbb{Z}$.

Now $b - a = (-k)n$ and $-k \in \mathbb{Z}$.

Hence $b \equiv a(mod\, n)$.

Thus the relation is symmetric.

0.2.2.3 Antisymmetric Property

Is the relation " $\equiv$ " over $\mathbb{Z}$ antisymmetric?

Counter Example: n is fixed

choose: $a = n + 1, b = 2n + 1$, then

$a \equiv b(mod\, n)$ and $b \equiv a(mod\, n)$

but $a \neq b$.

Thus the relation " $\equiv$ "on $\mathbb{Z}$ is not antisymmetric.

0.2.2.1 Transitive Property

0.2.2.1.1 Theorem 4 :

The relation " $\equiv$ " over $\mathbb{Z}$ is transitive.

Proof: Let $a, b, c \in \mathbb{Z}$, such that $a \equiv b(mod n)$ and $b \equiv c(mod n)$.

Then $a = b + kn, k \in \mathbb{Z}$ and $b = c + hn, h \in \mathbb{Z}$.

We shall show that $a \equiv c(mod\, n)$.

Consider $a = b + kn = (c + hn) + kn = c + (hn + kn) = c + (h + k)n, h + k \in \mathbb{Z}$.

Hence $a \equiv c(mod\, n)$.

Thus congruence modulo n is transitive.

0.2.2.1.2 Theorem 5:

The relation " $\equiv$ " over $\mathbb{Z}$ is an equivalence relation.

0.2.3 Modulo classes

Let $m \in \mathbb{Z}_+$. The relation $\equiv$ on $\mathbb{Z}$ by $a \equiv b$ if and only if $m|(a - b)$, is an equivalence relation. The Classes of $(\mathrm{mod}\ m)$ have the following equivalence classes:

$[0], [1], [2], \ldots, [m - 1]$.

Example of writing equivalence classes:

Example 0.2.3:

The equivalence classes for $(mod\, 3)$ are (need to show steps):

$|0| - \{x \in \mathbb{Z} : x \sim 0\} = \{x \in \mathbb{Z} : x \equiv 0 \pmod 3\}$
$- \{x \in \mathbb{Z} : 3|(x - 0)\} - \{x \in \mathbb{Z} : 3|x\}$
$- \{x \in \mathbb{Z} : x - 3m, m \in \mathbb{Z}\} - \{\ldots, -6, -3, 0, 3, 6, \ldots\}.$

$|1| - \{x \in \mathbb{Z} : x \sim 1\} = \{x \in \mathbb{Z} : x \equiv 1 \pmod 3\}$
$- \{x \in \mathbb{Z} : 3|(x - 1)\} = \{x \in \mathbb{Z} : 3|(x - 1)\}$
$- \{x \in \mathbb{Z} : x - 3m - 1, m \in \mathbb{Z}\} - \{\ldots, -5, -2, 1, 4, 7, \ldots\}.$

$|2| - \{x \in \mathbb{Z} : x \sim 2\} - \{x \in \mathbb{Z} : x = 2 \pmod 3\}$
$- \{x \subset \mathbb{Z} : 3|(x \quad 2)|$ $- \{x \subset \mathbb{Z} : 3|(x \quad 2)|$
$- \{x \in \mathbb{Z} : x - 3m - 2, m \in \mathbb{Z}\} - \{\ldots \quad 1. \quad 1, 2, 5, 8, \ldots\}.$

0.2.4 Modulo Arithmetic

In this section, we will explore arithmetic operations in a modulo world.

Let $n \in \mathbb{Z}_+$.

0.2.4.1 Theorem 5 :

Let $a, b, c, d, \in \mathbb{Z}$ such that $a \equiv b (mod\, n)$ and $c \equiv d (mod\, n)$. Then $(a + c) \equiv (b + d) (mod\, n)$.

Proof:

Let $a, b, c, d \in \mathbb{Z}$, such that $a \equiv b (mod\, n)$ and $c \equiv d (mod\, n)$.

We shall show that $(a + c) \equiv (b + d) (mod\, n)$.

Since $a \equiv b (mod\, n)$ and $c \equiv d (mod\, n), n \mid (a - b)$ and $n \mid (c - d)$

Thus $a = b + nk$, and $c = d + nl$, for k and $l \in \mathbb{Z}$.

Consider $(a + c) - (b + d) = a - b + c - d = n(k + l), k + l \in \mathbb{Z}$.

Hence $(a + c) \equiv (b + d) (mod\, n)$.□

0.2.4.2 Theorem 6:

Let $a, b, c, d, \in \mathbb{Z}$ such that $a \equiv b (mod\, n)$ and $c \equiv d (mod\, n)$. Then $(ac) \equiv (bd) (mod\, n)$.

Proof:

Let $a, b, c, d \in \mathbb{Z}$, such that $a \equiv b (mod\, n)$ and $c \equiv d (mod\, n)$.

We shall show that $(ac) \equiv (bd) (mod\, n)$.

Since $a \equiv b (mod\, n)$ and $c \equiv d (mod\, n), n \mid (a - b)$ and $n \mid (c - d)$

Thus $a = b + nk$, and $c = d + nl$, for k and $l \in \mathbb{Z}$.

Consider $(ac) - (bd) = (b + nk)(d + nl) - bd = bnl + dnk + n^2lk = n(bl + dk + nlk)$, where $(bl + dk + nlk) \in \mathbb{Z}$.

Hence $(ac) \equiv (bd) (mod\, n)$.□

0.2.4.3 Theorem 7:

Let $a, b \in \mathbb{Z}$ such that $a \equiv b (mod\, n)$. Then $a^2 \equiv b^2 (mod\, n)$.

Proof:

Let $a, b \in \mathbb{Z}$, and n $\in \mathbb{Z}_+$, such that $a \equiv b (mod\, n)$.

We shall show that $a^2 \equiv b^2 (mod\, n)$.

Since $a \equiv b (mod\, n), n \mid (a - b)$.

Thus $(a - b) = nx$, where $x \in \mathbb{Z}$.

Consider $(a^2 - b^2) = (a + b)(a - b) = (a + b)(nx), = n(ax + bx), ax + bx \in \mathbb{Z}$.

Hence $n \mid a^2 - b^2$, therefore $a^2 \equiv b^2 (mod\, n)$. □

0.2.4.4 Theorem 8:

Let $a, b \in \mathbb{Z}$ such that $a \equiv b (mod\, n)$. Then $a^m \equiv b^m (mod\, n)$, $\forall \in \mathbb{Z}$.

Proof:

Exercise.

By using the above result, we can solve many problems. Some of them are discussed below:

Example 0.2.1: $mod\,3$ Arithmetic

Let $n = 3$.

Addition

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Multiplication

x	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Example 0.2.2: $mod\,4$ Arithmetic

Let $n = 4$.

x	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Example 0.2.3:

Find the remainder when $(101)(103)(107)(109)$ is divided by 11.

Answer

$101 \equiv 2 (mod\, 11)$

$103 \equiv 4 (mod\, 11)$

$107 \equiv 8 (mod\, 11)$

$109 \equiv 10 (mod\, 11)$.

Therefore,

$(101)(103)(107)(109) \equiv (2)(4)(8)(10) (mod\ 11) \equiv 2 (mod\ 11)$.

Example 0.2.4:

Find the remainder when 7^{1453} is divided by 8.

Answer

$7^0 \equiv 1 (mod\, 8)$

$7^1 \equiv 7 (mod\, 8)$

$7^2 \equiv 1 (mod\, 8)$

$7^3 \equiv 7(mod\, 8)$,

As there is a consistent pattern emerging and we know that 1453 is odd, then $7^{1453} \equiv 7(mod\, 8)$. Thus the remainder is 7.

Example 0.2.5:

Find the remainder when 7^{2020} is divided by 18.

Answer

$7^0 \equiv 1(mod\, 18)$

$7^1 \equiv 7(mod\, 18)$

$7^2 \equiv 13(mod\, 18)$

$7^3 \equiv 1(mod\, 18)$,

As there is a consistent pattern emerging and we know that $2020 = (673)3 + 1$, $7^{2020} = 7^{(673)3+1} = (7^3)^{673}\, 7^1 \equiv 7(mod\ 18)$. Thus the remainder is 7.

Example 0.2.6:

Find the remainder when 26^{1453} is divided by 3.

This page titled 0.2: Relations is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

- **2.1: Binary Relations** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.
- **2.2: Equivalence Relations, and Partial order** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.
- **3.1: Modulo Operation** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.
- **3.2: Modulo Arithmetic** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.

0.3: Functions

0.3.0.1

Definition: Cartesian Product

Let A be a set. Then $A \times A = \{(a_1, a_2) | a_1, a_2 \in A\}$ is the Cartesian product of A.

Example 0.3.1

If $A = \mathbb{R}$ then this is the Cartesian plane - Like $\{x, y : x, y \in A\}$.

Definition: Function

A function f is a subset (symbol is $\subseteq$) of $A \times B$ such that for every $a \in A$ there exists a unique $b \in B$ such that $f(a) = b$.

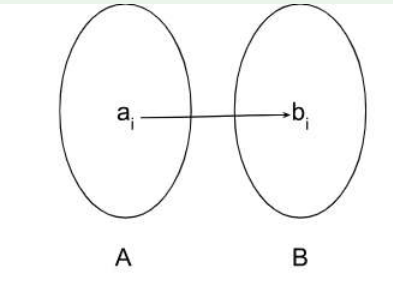
Denoted by $f : A \to B$ or $A \xrightarrow{f} B$.

A is the domain of the function f.

B is the co-domain of the function f.

The range of f is $f(A) = \{f(x) : x \in A\} \subseteq B = Im(f)$, the image of f.

A well-defined function is one that for every value of A, there is one and only one value of B.



Definition:

Let f be a function from $A \to B$.

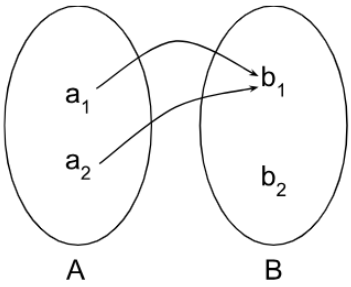
1. f is called onto (surjective) if $f(A) = B$.
2. f is called one to one (injective) if $f(x_1) = f(x_2), x_1, x_2 \in A$ then $x_1 = x_2$.
3. f is bijective if it is surjective and injective.
4. A function can be injective, surjective, bijective (both injective & surjective), or neither.

Note:

Let $f : A \to B$. If f is 1-1 and onto then f is a bijection from $A \to B$.

If there is a bijection between two finite sets, the number of elements in each set is the same. Notationally: |A| = |B|.

Example 0.3.2

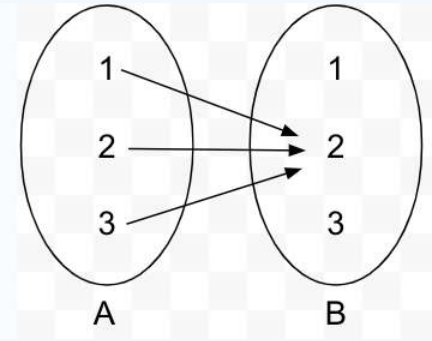


This is not injective since both a_1 and a_2 point to the b_1 element in B.

This is not surjective since there is no mapping from A to b_2.

Example 0.3.3

Consider the mapping:



Is this mapping

a) Well defined?

b) Is it surjective?

c) Is it injective?

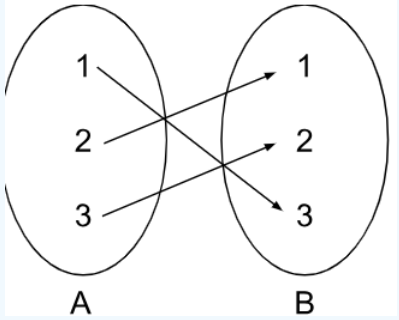
d) Is it bijective?

Solution

The function is well-defined. Not injective. Not subjective, not bijective.

Example 0.3.4

Consider the mapping:



Is this mapping

a) Well defined?

b) Is it surjective?

c) Is it injective?

d) Is it bijective?

Solution

This is well defined bijective function.

Example 0.3.5

Given $f : \mathbb{Q} \to \mathbb{Z}$ where $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ and $f(\frac{a}{b}) = a$. Is this a well-defined function?

Solution

Let A and B be sets such that $A = \{\frac{a}{b} : a, b \in \mathbb{Z}, a \neq 0\}$ and $B = \mathbb{Z}$.

Using a counterexample, $f(\frac{a}{b})$ is not a well-defined function since $f(\frac{1}{2}) = 1$ and $f(\frac{2}{4}) = 2$, but $\frac{1}{2} = \frac{2}{4}$. This is an example of an element in A that maps to more than one element in B.

Example 0.3.6

Let

$\mathbb{Q} = \{\frac{a}{b} : b > 0, \text{and } gcd(a, b) = 1\}$

and $f : \mathbb{Q} \to \mathbb{Z}$ that is defined by

$f(\frac{a}{b}) = a$.

a) Is f a well-defined function? b) Is it surjective? c) Is it injective? d) Is it bijective?

Solution

1. The function is well-defined.

Let A and B be set.

Let $a \in A$.

We need to show that if $f(a) = b$ then $b \in B$ and if $f(a) = b_1$ that $b = b_1$.

We are given $f : \mathbb{Q} \to \mathbb{Z}$, which means that this is a function thus $f(a)$ will map to one and only one element of B. Thus if $f(a) = b$ and if $f(a) = b_1$ then $b = b_1$.

In b) below, we have shown that the function is surjective, thus $f(a) = b$,

2. The function is surjective

Proof:

We shall show that $f(\mathbb{Q}) = \mathbb{Z}$ by showing that $f(\mathbb{Q}) \subseteq \mathbb{Z}$ and $\mathbb{Z} \subseteq f(\mathbb{Q})$.

Since we are given $f : \mathbb{Q} \to \mathbb{Z}$, $f(\mathbb{Q}) \subseteq \mathbb{Z}$.

Next, we shall show that $\mathbb{Z} \subseteq f(\mathbb{Q})$.

Let $n \in \mathbb{Z}$, then $\frac{n}{1} \in \mathbb{Q}$ and $f\left(\frac{n}{1}\right) = n$.

Hence $n \in f(\mathbb{Q})$.

Hence $\mathbb{Z} \subseteq f(\mathbb{Q})$.

Since $\mathbb{Z} \subseteq f(\mathbb{Q})$ and $f(\mathbb{Q}) \subseteq \mathbb{Z}, f(\mathbb{Q}) = \mathbb{Z}$.□

3. The function is not injective.

Counterexample:

Let $A = \left\{\frac{a}{b} : b > 0, \text{and } gcd(a, b) = 1\right\}$ and $B = \mathbb{Z}$.

Note $\frac{1}{4}, \frac{1}{3} \in A$ and that $f(\frac{1}{4}), f(\frac{1}{3}) \in B$ and that $f(\frac{1}{4}) = f(\frac{1}{3}) = 1$.

Since $\frac{1}{4} \neq \frac{1}{3}$, the function is not injective.

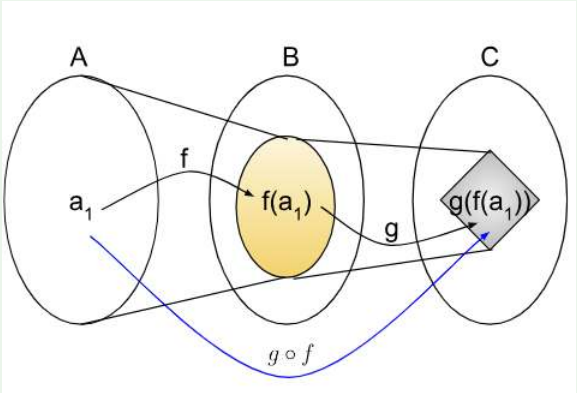
4. The function is not bijective since it has been shown not to be both injective and surjective.

0.3.1 Operation on functions: Composition

Definition:Composition of functions

Let $f : A \to B$ and $g : B \to C$. Then the composition functions of g and f, $g \circ f : A \to C$, defined by

$(g \circ f)(a) = g(f(a)),\ \forall a \in A$.



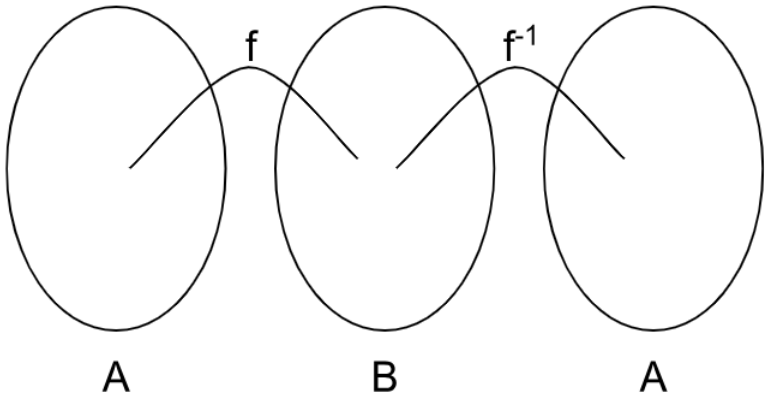
Definition: Identity function

Identity function $id_A : A \to A$ defined by $id_A(x) = x, \forall x \in A$.

Definition: Inverse of a function

Let $f : A \to B$ then f has an inverse $g : B \to A$ if $(f \circ g) = id_B$ and $(g \circ f) = id_A$. Note the domain of $f \circ g$ is the domain of g.

Let $f : A \to B$ be a bijection. Then the inverse of f, denoted by $f^{-1} : B \to A$ defined by $f^{-1}(b) = a$ if $f(a) = b$ if $a \in A$ and $b \in B$. In this case, $f \circ f^{-1} = id_A$, and $f^{-1} \circ f = id_B$.



Example 0.3.7

Let $f : A \to B$ and $g : B \to C$. Then $g \circ f : A \to C$.

1. If f and g are surjective, then $g \circ f$ is surjective.

Proof:

We will show that $g \circ f$ is surjective.

Let $c \in C$. Since g is surjective, there exists $b \in B$ such that $g(b) = c$.

Since f is surjective, there exists $a \in A$ such that $f(b) = a$.

Hence there exists $a \in A$ such that $gf(f(a)) = c$.

Therefore, if f and g are surjective, then $g \circ f$ is surjective.□

(better proof) If f is onto and g is onto then $g \circ f$ is onto.

Proof:

We shall show that $(g \circ f)(A) = C$.

Since f and g are onto, by definition of a function, $(g \circ f)(A) \subseteq C$.

Now we need to show that $C \subseteq (g \circ f)(A)$.

Let $c \in C$.

Since g is onto $\exists b \in B$ s.t. $c = g(b)$.

Since f is onto, $\exists a \in A$ s.t. $b = f(a)$.

Consider $(g \circ f)(a) = g(f(a))$ (by definition)

$= g(b)$

$= c.$

Therefore $c \in (g \circ f)(A)$.

Hence $C \subseteq (g \circ f)(A)$.

Since $(g \circ f)(A) \subseteq C$ and $C \subseteq (g \circ f)(A)$, then $g \circ f$ is onto.□

Example 0.3.8

1. If f and g are injective, then $g \circ f$ is injective. That is,

If f is 1-1 and g is 1-1 then $g \circ f$ is 1-1.

Proof:

Let $a_1, a_2 \in A$ such that $g \circ f(a_1) = g \circ f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$.

Since g is 1-1, $f(a_1) = f(a_2)$.

Since, f is 1-1, $a_1 = a_2$.

Hence $g \circ f$ is injective.

Example 0.3.9

Given A is a matrix and $T_A : \mathbb{R}^2 \to \mathbb{R}^2$ defined by $T_A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$. Note this is a matrix transformation which is linear.

1. Is T_A 1-1?

Yes, T_A is 1-1.

Proof:

Let $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix}$ and $\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} \in \mathbb{R}^2$ s.t. $T_A \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = T_A \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$.

We will show that $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$.

$T_A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + y \\ y \end{bmatrix}$.

Thus $\begin{bmatrix} x_1 + y_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_2 + y_2 \\ y_2 \end{bmatrix}$.

Thus $x_1 + y_1 = x_2 + y_2$ and $y_1 = y_2$.

Thus $x_1 = x_2$ and $y_1 = y_2$.

Hence $\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_2 \\ y_2 \end{bmatrix}$.

Thus T_A is 1-1.□

2. Is $T_A \begin{bmatrix} x \\ y \end{bmatrix}$ onto?

Yes, $T_A \begin{bmatrix} x \\ y \end{bmatrix}$ is onto.

Proof:

We know by definition that $T_A \begin{bmatrix} x \\ y \end{bmatrix} \subseteq \mathbb{R}^2$.

We need to show that $\mathbb{R}^2 \subseteq T_A \begin{bmatrix} x \\ y \end{bmatrix}$.

Let $\begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{R}^2$.

Find $\begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2$ s.t. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$.

$\begin{bmatrix} x+y \\ y \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$.

Thus $y = b$ and $x = a - b$.

Thus $T_A \begin{bmatrix} a-b \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$.

Thus T_A is onto.□

3. Does T_A have an inverse? If so, what is it?

a) Yes T_A has an inverse since it is a bijection (1-1 and onto) $\therefore T_A^{-1}$ exists.

Proof: By definition? Obvious?

b) $T_A^{-1} : \mathbb{R}^2 \to \mathbb{R}^2$.

$T_A^{-1} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$

$= \begin{bmatrix} x-y \\ y \end{bmatrix}$.

Check: $T_A^{-1} \cdot T_A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Example 0.3.10

Let $f : A \to B$ and $g : B \to C$. Then $g \circ f : A \to C$. Given $g \circ f$ is injective and f is onto, prove that g is injective.

Proof:

Assume $g \circ f$ is injective. (by definition)

Let $x_1, x_2 \in B$ s.t. $g(x_1) = g(x_2)$.

We shall show that $x_1 = x_2$.

Let $a_1, a_2 \in A$.

Since f is surjective (by definition), we know that $f(a_1) = x_1$ and $f(a_2) = x_2$.

Since $x_1 \in B$ and f is surjective, $\exists a_1 \in A$ s.t. $f(a_1) = x_1$.

Since $x_2 \in B$ and f is surjective, $\exists a_2 \in A$ s.t. $f(a_2) = x_2$.

Since $g(x_1) = g(x_2)$, then $g(f(a_1)) = g(f(a_2))$ and $g \circ f)(a_1) = (g \circ f)(a_2)$.

Since $g \circ f)$ is injective, $a_1 = a_2$.

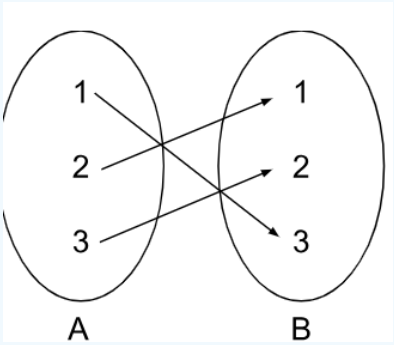
Thus $f(a_1) = f(a_2)$ since f is a function.

Therefore, $x_1 = x_2$.

Hence g is injective.

Example 0.3.11

Consider the mapping α:



Find α^2 , α^3 and α^{-1}.

This page titled 0.3: Functions is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

0.5: Proof Templates

From DR. THI DINH'S PROOF WRITING HANDBOOK THIS BIBLE:

0.5.0.0.1 In the beginning...

Let P and Q be statement variables. When needed, suppose that P = P(x) depends on a variable x. The symbol "$\forall$" means "for all" or "for any". The symbol $\exists$ means "there exists".

Type of statement	**What must we do to prove that it is true**
(1) If P, then Q (2) $\forall P$, Q	Suppose that P is true. Prove that Q is true.
(3) $\exists x P(x)$ such that Q	Choose x so that $P(x)$ is true. Prove that Q is true. Note: You **need not** explain how you find x.

0.5.0.0.1 The first (and only) commandment

To prove that a statement is **false**, thou shalt **write out the negation of the statement and prove that**.

To prove injective relationship (ie prove one-to-one)

YES If $f(x_1) = f(x_2)$ then you need to prove $x_1 = x_2$.

Let A be a set. Let $x_1, x_2 \in A$ such that $f(x_1) = f(x_2)$.

$\vdots$

Show $x_1 = x_2$.

NO then you need to provide one counterexample where $x_1 \neq x_2$ when $f(x_1) = f(x_2)$.

Is there a surjective relationship (i.e. prove onto)?

YES Note we are starting from $f : A \to B$. Thus $f(A) \subseteq B$ by definition.

Let A and B be sets where A is onto B if and only if $f(A) \subseteq B$ and $B \subseteq f(A)$.

By definition, $f(A) \subseteq B$. Next show $B \subseteq f(A)$.

Let $x \in B$.

$\vdots$

Show $x \in f(A)$.

Conclude with: Since $f(A) \subseteq B$ and $B \subseteq f(A)$ therefore f is onto.$\square$

NO then need to find a counterexample where $b \in B$, but there is no $a \in A$ whereby $f(a) = b$.

- **Reflexive, Symmetric, Anti Symmetric Transitive Property Proofs**

Need a non-empty set A and a relation R.

- Reflexive

Let $a \in A$. ← Starting point

⋮

Show aRa ← Ending point

- Symmetric

Let $a, b \in A$ s.t. aRb.

⋮

Show bRa

- Antisymmetric

Let $a, b \in A$ s.t. aRb and bRa

⋮

Show $a = b$.

- Transitive

Let $a, b, c \in A$ s.t. aRb and bRa.

⋮

Show aRc.

This page titled 0.5: Proof Templates is shared under a not declared license and was authored, remixed, and/or curated by Pamini Thangarajah.

0E: Exercises

Exercise $0E.1$

Define $h : \mathbb{Z} \to \mathbb{Z}$ by $h(x) = x^2 + 4$. Determine (with reasons) whether or not h is one−to−one and whether or not h is onto.

Exercise $0E.2$

Suppose $f : A \to B$ and $g : B \to C$ are functions. Prove or disprove the following statements:

1. If $g \circ f$ is one-to-one then g is one-to-one.
2. If $g \circ f$ is one-to-one and f is onto, then g is one-to-one.
3. If $g \circ f$ is onto and g is one-to-one, then f is onto.

Exercise $0E.3$

Determine whether or not each of the following binary relations R on the given set A is reflexive, symmetric, antisymmetric, or transitive. If a relation has a certain property, prove this is so; otherwise, provide a counterexample to show that it does not. If R is an equivalence relation, describe the equivalence classes of A.

1. Let $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Define a relation R on $A = S \times S$ by $(a, b)R(c, d)$ if and only if $10a + b \leq 10c + d$.
2. Let $A = \mathbb{Z}\backslash\{0\}$. Define a relation R on A, by aRb if and only if $ab > 0$.
3. Define a relation R on $A = \mathbb{Z}$ by aRb if and only if $4|(3a + b)$.
4. Define a relation R on $A = \mathbb{Z}$ by aRb if and only if $3|(a^2 - b^2)$.
5. Let $A = \mathbb{R}$, If $a, b \in \mathbb{R}$, define aRb if and only if $a - b \in \mathbb{Z}$.
6. Define a relation R on the set $\mathbb{Z} \times \mathbb{Z}$ by $(a, b)R(c, d)$ if and only if $ac = bd$.
7. Define a relation R on $\mathbb{Z}$ by aRb if and only if $2 \mid a^2 + b$.
8. Let $A = \mathbb{R}$, If $a, b \in \mathbb{R}$, define aRb if and only if $a - b \in \mathbb{Q}$.
9. Let $A = \mathbb{R} \times \mathbb{R}$, If $(x, y), (x_1, y_1) \in \mathbb{R} \times \mathbb{R}$, define $(x, y)\ R\ (x_1, y_1)$ if and only if $x^2 + y^2 = x_1^2 + y_1^2$.
10. Define a relation R on $\mathbb{Z}$ by aRb if and only if $5|(2a + 3b)$.

Answer

1. R is reflexive on $\mathbb{Z}$.

Proof:

Let $a \in \mathbb{Z}$.

We shall show that aRa, specifically $5|(2a + 3a)$.

Consider that $2a + 3a = 5a$ and $a \in \mathbb{Z}$.

Thus $5|(2a + 3a)$, and aRa.

Therefore R is reflexive on $\mathbb{Z}$.□

2. R is symmetric on $\mathbb{Z}$.

Proof:

Let $a, b \in \mathbb{Z}$ s.t. $5|(2a+3b$.

Thus $2a+3b=5m$ for some $m \in \mathbb{Z}$.

We will show that $3a+2b=5k$ for some $k \in \mathbb{Z}$.

Consider that $-2a-3b=-5m$ for some $m \in \mathbb{Z}$.

Then $5(a+b)-2a-3b=5(a+b)-5m$.

Thus $3a+2b=5(a+b-m)$ where $a+b-m=k \in \mathbb{Z}$.

Hence $5|(3a+2b)$ and bRa.

Since bRa, R is symmetric on $\mathbb{Z}$.

3. R is not antisymmetric on $\mathbb{Z}$.

Counter Example:

Let $a=0$ and $b=5$.

Then $5|(2(0)+3(5))$ and $5|(2(5)+3(0)$.

However, since $0 \neq 5$ R is not antisymmetric on $\mathbb{Z}$.□

4. R is transitive on $\mathbb{Z}$.

Let $a, b, c \in \mathbb{Z}$ s.t. aRb, $5|(2a+3b)$ and bRa, $5|(2b+3c)$.

We will show that aRc, $5|(2a+3c)$.

Since $5|(2a+3b)$, $2a+3b=5(k)$ for some $k \in \mathbb{Z}$.

Since $5|(2b+3c)$, $2b+3c=5(m)$ for some $m \in \mathbb{Z}$.

Consider $2a+3c=(2a+3b)+(2b+3c)-5b$

$=5(k)+5(m)-5(b)$

$=5(k+m-b)$, where $k+m-b \in \mathbb{Z}$.

Hence $5|2a+3c$ and aRc.

Hence R is transitive on $\mathbb{Z}$.□

Since R is reflexive, symmetric and transitive on $\mathbb{Z}$, R is an equivalence relation.

Te equivalence classes of aRb iff $5|(2a+3b)$ are $[0], [1], [2], [3]$ and $[4]$.

Let $a \in \mathbb{Z}$, then $[a]=\{a \in \mathbb{Z} : x \sim a\}$.

$[0]=\{x \in \mathbb{Z} : x \sim 0\}$

$=\{x \in \mathbb{Z} : 5|(2x+3(0))\}$

$=\{x \in \mathbb{Z} : 5|2x\}$

$=\{x \in \mathbb{Z} : 2x=5m, m \in \mathbb{Z}\}$

$=\{\ldots, -10, -5, 0, 5, 10, \ldots\}$.

$[1]=\{x \in \mathbb{Z} : x \sim 1\}$

$$= \{x \in \mathbb{Z} : 5|(2x + 3(1))\}$$
$$= \{x \in \mathbb{Z} : 5|(2x + 3)\}$$
$$= \{x \in \mathbb{Z} : 2x + 3 = 5m, m \in \mathbb{Z}\}$$
$$= \{x \in \mathbb{Z} : 2x = 5m - 3, m \in \mathbb{Z}\}$$
$$= \{..., -9, -4, 1, 6, 11, ...\}.$$

$$[2] = \{x \in \mathbb{Z} : x \sim 2\}$$
$$= \{x \in \mathbb{Z} : 5|(2x + 3(2))\}$$
$$= \{x \in \mathbb{Z} : 5|(2x + 6)\}$$
$$= \{x \in \mathbb{Z} : 2x + 6 = 5m, m \in \mathbb{Z}\}$$
$$= \{x \in \mathbb{Z} : 2x = 5m - 6, m \in \mathbb{Z}\}$$
$$= \{..., -8, -3, 2, 7, 12, ...\}.$$

$$[3] = \{x \in \mathbb{Z} : x \sim 3\}$$
$$= \{x \in \mathbb{Z} : 5|(2x + 3(3))\}$$
$$= \{x \in \mathbb{Z} : 5|(2x + 9)\}$$
$$= \{x \in \mathbb{Z} : 2x + 9 = 5m, m \in \mathbb{Z}\}$$
$$= \{x \in \mathbb{Z} : 2x = 5m - 9, m \in \mathbb{Z}\}$$
$$= \{..., -7, -2, 3, 8, 13, ...\}.$$

$$[4] = \{x \in \mathbb{Z} : x \sim 4\}$$
$$= \{x \in \mathbb{Z} : 5|(2x + 3(4))\}$$
$$= \{x \in \mathbb{Z} : 5|(2x + 12)\}$$
$$= \{x \in \mathbb{Z} : 2x + 12 = 5m, m \in \mathbb{Z}\}$$
$$= \{x \in \mathbb{Z} : 2x = 5m - 12, m \in \mathbb{Z}\}$$
$$= \{..., -6, -1, 4, 9, 14, ...\}$$

This page titled 0E: Exercises is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

Chapter 1: Integers

This page titled Chapter 1: Integers is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

1.1: Division Algorithm

This page is a draft and is under active development.

In the proof of numerous theorems, we will utilize the well-ordering principle.

Theorem 1.1.1: Well ordering principle

Every non-empty subset of $\mathbb{N}$ has the smallest number.

1.1.1 Division Algorithm

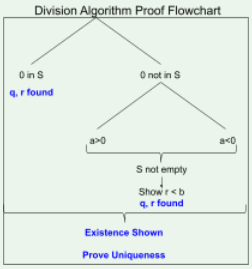
Theorem 1.1.2: Division Algorithm

Let a and $b \neq 0$ be integers. Then there exist unique integers q and r such that $a = bq + r, 0 \leq r < |b|$, where q is the quotient and r is the remainder, and the absolute value of d is defined as:

$$|b| = \begin{cases} b, \text{if } b \geq 0 \\ -b, \text{if } b < 0. \end{cases} \tag{1.1.1}$$

Proof

We will show that $q, r \in \mathbb{Z}$ exist and are unique.



Let $a, b \in \mathbb{Z}$ s.t. $b > 0$.

Let S be a set defined by $S = \{a - bm : a - bm \geq 0, m \in \mathbb{Z}\}$.

We will show existence by examining the possible cases.

Case 1: $0 \in S$

If $0 \in S$, then $a - bm = 0$ for some $m \in \mathbb{Z}$.

Thus, $a = bm$

Since $b|a$, $q = m$ and $r = 0$.

Therefore existence has been proved.

Case 2: $0 \notin S$.

Since $0 \notin S$, we will show that $S \neq \emptyset$ by examining the possible cases. Note: $S \subseteq \mathbb{N}$.

Case a: $a > 0$.

Since $a > 0$, $a = a - b(0) > 0$.

Therefore $a \in S$.

Case b: $a < 0$.

Consider $a - bm$, where $m = 2a$.

Thus $a - b(2a) = a(1 - 2b)$.

Consider $1 - 2b$ is always negative since $b > 0, b \in \mathbb{N}$, thus greatest $1 - 2b$ can be in -1.

Therefore $a(1 - 2b) \geq 0$ since $b \geq 1$.

Note: The $\geq$ could be $>$ without loss of generality.

Since both case a & b are non-empty sets, $S \neq \emptyset \subseteq \mathbb{N}$.

Thus S has the smallest element by the well-ordering principle, and lets call it r.

That means $r = a - bm$, for some $m \in \mathbb{Z}$ where $r \geq 0$.

Thus the non-empty set is $r = a - bm \geq 0$.

We shall show that $r < b$ by proceeding with a proof by contradiction.

Assume that $r \geq b$.

Then $a - b(m + 1) = a - bm - b = r - b \geq 0$ for some $m \in \mathbb{Z}$.

Then $r - b \in S$ and $r - b < r$. Note $(b > 0)$

This contradicts that r is the smallest element of S.

Therefore $r < b$.

Having examined all possible cases, $a = bq + r, 0 \leq r < b$ exists.

Next, we will show uniqueness.

Let r_1, r_2, q_1, q_2 s.t. $a = bq_1 + r_1$ and $a = bq_2 + r_2$ with $0 \leq r_1, r_2 < b$.

Consider $bq_1 + r_1 = bq_2 + r_2$, $0 \leq r_1 < b$.

Further since $b(q_1 - q_2) = r_2 - r_1$, $b|(r_2 - r_1)$, but b has to be $\leq r_1$.

Since, $r_2 - r_1 < b$, $r_2 - r_1 = 0$ and $r_1 = r_2$.

Hence $q_1 = q_2$.

Therefore uniqueness has been shown.

Example 1.1.1

Find the q is the quotient and r is the remainder for the following values of n and d.

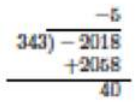
1. $n = 2018$ and $d = 343$.

$$\begin{array}{r} 5 \\ 343\overline{)2018} \\ -1715 \\ \hline 303 \end{array}$$

Thus $2018 = (5)(343) + 303$.

2. $n = -2018$ and $d = 343$.

https://math.libretexts.org/@go/page/131030



Thus $-2018 = (-6)(343) + 40$.

3, . $n = 2018$ and $d = -343$.

Thus $2018 = (6)(-343) + 40$.

4.

$n = -2018$ and $d = -343$.

Thus $-2018 = (6)(-343) + 40$.

This page titled 1.1: Division Algorithm is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

- **2.6: Division Algorithm** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.

1.2: Greatest common divisor and least common multiple

Think out loud

We want to tile a 253 ft by 123 ft ($a = 253$ and $b = 123$, with $a, b \in \mathbb{Z}$) floor with identical square tiles. What is the largest square tile we can use?

Definition: Greatest Common Divisor

Let $a, b \in \mathbb{Z}$, where not both a, b is zero.

Then, we say that an integer $d = \gcd(a, b) \in \mathbb{Z}_+$., greatest common divisor if it satisfies the following conditions:

1. $d|a$ and $d|b$, Note: d must divide both numbers

2. If $c \in \mathbb{Z}$, $c|a$ and $c|b$ then $c \leq d$. Note: d is the greatest number divides both.

Thus, the greatest common divisor of two integers a and b, also known as GCD of a and b, is the greatest positive integer that divides both the integers a and b. This class will use the following notation: $\gcd(a, b)$.

Example 1.2.1:

What is the $\gcd$ of 15 and 20?

A process to find the solution:

List all positive divisors of 15 and 20.
The positive divisors of 15 are $1, 3, 5,$ and 15.
The positive divisors of 20 are $1, 2, 4, 5, 10,$ and 20.
The common positive divisors are $1, 5$.
As you can see from the list the gcd of 15 and 20 is 5. That is, the $\gcd(15, 20) = 5$.

Example 1.2.2:

An elementary gym teacher has 3 grade 4 gym classes with $21, 35$ and 28 students in them. The teacher wants to order equipment that equal-sized groups can use in each class. What is the largest group size that will work for all 3 classes?

Solution:

You will need to find the GCD of all 3 classes.
Firstly, you will find the GCD of 21 and 35.
The positive divisors of 21 are $1, 3, 7,$ and 21.
The positive divisors of 35 are $1, 5, 7,$ and 35.
The GCD of 21 and 35 is 7.

Since $7 \mid 28$ you will now find the GCD of 7 and 28, which turns out to be 7.
Therefore the GCD of $21, 35$ and 28 is 7.
Thus, the largest number of students in a group for each class will be 7.

Properties:

Let $a, b, c \in \mathbb{Z}$.

Then:

1. $\gcd(a, a) = |a|, a \neq 0$.
2. $\gcd(a, b) = \gcd(b, a)$.
3. $\gcd(a, b, c) = \gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.
4. $\gcd(a, 0) = a$.
5. $\gcd(0, 0)$ is undefined.

Now, let's explore an algorithm for determining the GCD. The Euclidean Algorithm, developed by the renowned Greek mathematician Euclid, is a highly effective method for computing the GCD of two integers.

Definition: Euclidean Algorithm

If $a, b \in \mathbb{Z} \setminus \{0\}$, then by using division algorithm iteratively, we obtain

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0q_1 + r_1 \\ r_0 &= r_1q_2 + r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_n &= r_nq_{n+1} + 0 \end{aligned}$$

Notice that, the last non-zero remainder is r_n, such an r_n exists, since $|b| > |r_0| > |r_1| \cdots > |r_n|$. The $r_n = \gcd(a, b)$.

Example 1.2.3

Find $\gcd(2420, 230)$.

Note: Work from right to left to follow the steps shown in the image below.

$$\begin{array}{r|l} 10 & 110 \\ \hline 11 & \\ 100 & \\ \hline 10 & \\ 10 & \\ \hline 0 & \end{array} \qquad \begin{array}{r|l} 110 & 120 \\ \hline 1 & \\ 110 & \\ \hline 10 & \end{array} \qquad \begin{array}{r|l} 120 & 230 \\ \hline 1 & \\ 120 & \\ \hline 110 & \end{array} \qquad \begin{array}{r|l} 230 & 2420 \\ \hline 10 & \\ 2300 & \\ \hline 120 & \end{array}$$

Hence, $\gcd(2420, 230) = 10$.

BEZOUT'S IDENTITY

For integers a and b, let d be the greatest common divisor, d = GCD (a, b). Then there exists integers x and y such that ax+by=d. Any integer that is of the form ax+by, is a multiple of d.

Note

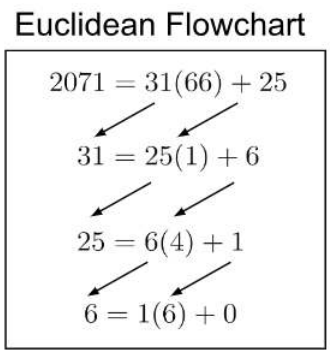
This condition will be a necessary and sufficient case of $d = 1$. We will prove this result in the section Relatively Prime numbers.

Example 1.2.4

Write gcd as a linear combination. $\gcd(2071, 31) = 2071x + 31y$, with $x, y \in \mathbb{Z}$.

Solution

Steps are listed (a,b,c,d) for ease of reference to Bezout's algorithm



a) $2071 = 31(66) + 25$

b) $31 = 25(1) + 6$

c) $25 = 6(4) + 1$

d) $6 = 1(6) + 0$. The process stops when the remainder is zero. Thus, $\gcd = 1$.

Bezout's Algorithm

1. $25 = 2071 + 31(-66)$ from a) above.
2. $6 = 31 + 25(-1)$ from b) above.
3. $1 = 25 + 6(-4)$ from c) above.

$1 = 25 + 6(-4)$ from 3) above.

$= 25 + (31 + 25(-1))(-4) = 25(5) + 31(-4)$ using 2) above.

$= (2071 + 31(-66))(5) + 31(-4)$ using 1) above

Example 1.2.5

Write gcd as a linear combination. $\gcd(3915, 825) = 3915x + 825y$, with $x, y \in \mathbb{Z}$.

Solution

From the calculation below, $\gcd(3915, 825) = 15$.

```
        2
210 | 615
      420
      ---
      195

        1
615 | 825
      615
      ----
      210

        4
825 | 3915
      3300
      ----
       615

        1
195 | 210
      195
      ---
       15

         13
15 | 195
      15
      --
      45
      45
      --
       0
```

We will use the following tabular method:

Bezout's algorithm Using Tabular Method

3915 x+825 y	x	y	operations
3915	1	0	
825	0	1	
615	1	-4	$R_2+(-4)R_1$
210	-1	5	$R_2+(-1)R_1$
195	3	-14	$R_2+(-2)R_1$
15	-4	20	$R_2+(-13)R_1$
Where R_1, R_2 are one row above and two rows above.			

Thus, $\gcd(3915, 825) = 3915(-4) + 825(20)$.

Example 1.2.6

Let $a, b \in \mathbb{Z}\backslash\{0\}$. Prove or disprove: $d = ax + by$ for some $x, y \in \mathbb{Z}$ then $\gcd(a, b) = d$.

Counterexample:

Let $d = 6,\ a = 2071$, and $b = 31$.

Consider $6 = 2071(-1) + 31(67)$.

Further consider that $1 = 2017(5) + 31(-334)$.

Since $1 < 6$ and 1 is the lowest possible $\gcd(a, b)$.

Example 1.2.7

Prove or disprove: If $1 = ax + by$ then $\gcd(a, b) = 1$.

Proof:

Let $a, b \in \mathbb{Z}\backslash\{0\}$ s.t. $1 = ax + by$ with $x, y \in \mathbb{Z}$.

Suppose $d = \gcd(a, b)$. We will show that $d = 1$.

Since $d = \gcd(a, b),\ \ d|a$ and $d|b$.

Since $d|a, a = md,\ m \in \mathbb{Z}$.

Since $d|b, b = nd,\ n \in \mathbb{Z}$.

Now, $ax + by = (md)x + (nd)y$

$= d(mx + ny)$.

Since $mx, ny \in \mathbb{Z}, mx + ny \in \mathbb{Z}$.

Now $1 = ax + by = d(mx + ny)$.

Therefore $d|1$.

Thus, $d = \pm 1$, but since $d \geq 0, d = 1$.

1.2.1 Relatively prime

Definition: Relatively prime

Two integers a and b are said to be relatively prime if $\gcd(a, b) = 1$.

Example 1.2.8

Show that $\gcd(n, n + 1) = 1,\ \forall n \in \mathbb{Z}$. That is, show that any two consecutive integers are relatively prime.

Since $n(-1) + (n + 1)(1) = 1$, $\gcd(n, n + 1) = 1$.

Example 1.2.9

Find two integers x and y such that $\gcd(-4357, 3754) = -4357(x) + 3754(y)$.

First use Euclidean Algorithm

$-4357 = 3754(-2) + 3151$ Note: Remainder must be greater than or equal to zero.

$$\begin{aligned} 3754 &= 3151(1) + 603 \\ 3151 &= 603(5) + 136 \\ 603 &= 136(4) + 59 \\ 136 &= 59(2) + 18 \\ 59 &= 18(3) + 5 \\ 18 &= 5(3) + 3 \\ 5 &= 3(1) + 2 \\ 3 &= 2(1) + 1 \\ 2 &= 1(2) + 0 \end{aligned}$$

Therefore $\gcd(-4357, 3754) = 1$.

Then use Bezout's Algorithm.

Bezout's Algorithm

Using Tabular Method

Note Columns 1 and 2 come from the Euclidean algorithm above.

		x	y
-4357		1	0
3754	-2	0	1
3151	1	1	2
603	5	-1	-1
136	4	6	7
59	2	-25	-29
18	3	56	65
5	3	-193	-224
3	1	635	737
2	1	-828	-961
1	2	1463	1698

Thus $\gcd(-4357, 3754) = -4357(1463) + 3754(1698) = 1$.

Definition:

For $n \in \mathbb{N}$, the Euler's totient function $\phi(n)$ is defined to be the number of positive integers less than n that are relatively prime to n.

Euler's totient function has numerous applications in number theory, cryptography, and other branches of mathematics. It plays a vital role in RSA encryption, where it is used to compute the encryption and decryption keys.

Example 1.2.10

Determine the value $\phi(n)$ for each integer $n \leq 30$. For $n \in \mathbb{N}$, $\phi(n)$ is defined to be the number of positive integers less than or

equal to n that are relatively prime to n.

Number of $n \in \mathbb{N}$, Relatively Prime to n		
n	$\phi(n)$	Set of $n \in \mathbb{N}$ that are relatively Prime to n.
1	1	{1}
2	1	{1}
3	2	{1,2}
4	2	{1,3}
5	4	{1,2,3,4}
6	2	{1,5}
7	6	{1,2,3,4,5,6}
8	4	{1,3,5,7}
9	6	{1,2,4,5,7,8}
10	4	{1,3,7,9}
11	10	{1,2,3, … ,8,9,10}
12	4	{1,5,7,11}
13	12	{1,2,3, … ,10,11,12}
14	6	{1,3,5,9,11,13}
15	8	{1,2,4,7,8,11,13,14}
16	8	{1,3,5,7,9,11,13,15}
17	16	{1,2,3, … ,14,15,16}
18	6	{1,5,7,11,13,17}
19	18	{1,2,3, … ,16,17,18}
20	8	{1,3,7,9,11,13,17,19}
21	12	{1,2,4,5,8,10,11,13,16,17,19,20}
22	10	{1,3,5,7,9,13,15,17,19,21}
23	22	{1,2,3, … ,20,21,22}
24	8	{1,5,7,11,13,17,19,23}
25	20	{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24}
26	12	{1,3,5,7,9,11,15,17,19,21,23,25}

27	18	{1,2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26}
28	12	{1,3,5,9,11,13,15,17,19,23,25,27}
29	28	{1,2,3, … ,26,27,28}
30	8	{1,7,11,13,17,19,23,29}

1.2.2 Least Common Multiples

Definition: Least Common Multiples

Let a and b be integers. Then any integer that is a multiple of both a and b is called a common multiple of a and b. The least common multiple of integers a and b, denoted by $lcm(a,b)$, is the smallest positive common multiple of a and b.

Example 1.2.13:

Find

1. $lcm(5,10)$
2. $lcm(-6,18)$
3. $lcm(0,5)$

Solution

1. 10, 2. 18 3. undefined.

Finding LCM using GCD

The least common multiple of integers a and b, also known as the LCM, is the smallest number divisible by both integers a and b. You can determine the LCM by dividing the absolute value of the product of a and b by the GCD of a and b.

That is

$$lcm(a,b) = \frac{|ab|}{\gcd(a,b)} \tag{1.2.1}$$

Example 1.2.14:

What is the LCM of 24 and 35?

Solution:

We must first determine the GCD of 24 and 35.

Find the divisors of 24 and 35.

$24 : 1, 2, 3, 4, 8, 12, 24$

$35 : 1, 5, 7, 35$

Therefore the GCD of 24 and 35 is 1.

Now that we have determined the GCD, we can continue to determine the least common multiple.

$\frac{(24)(35)}{1} = 840$.

Hence $lcm(24,35) = 840$.

Properties:

Let $a, b, c \in \mathbb{Z}$.

Then:

1. $lcm(a, a) = a$.
2. $lcm(a, b) = lcm(b, a)$.
3. $lcm(a, b, c) = lcm(lcm(a, b), c) = lcm(a, lcm(b, c))$.
4. $lcm(a, 0) =$ undefined.

This page titled 1.2: Greatest common divisor and least common multiple is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

- **4.1: Greatest Common Divisor** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.
- **4.2: Euclidean algorithm and Bezout's algorithm** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.
- **4.3: Least Common Multiple** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.

1.3: Primes

Definition:

Prime Numbers - integers greater than 1 with exactly 2 positive divisors: 1 and itself.
Let n be a positive integer greater than 1. Then n is called a prime number if n has exactly two positive divisors, 1 and n.

Composite Numbers - integers greater than 1 which are not prime.

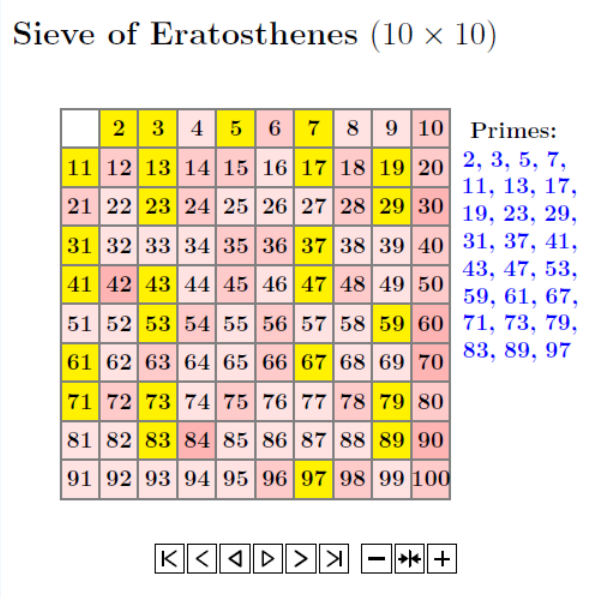
Note that: 1 is neither prime nor composite.

There are infinitely many primes, which was proved by Euclid in 100BC.

Example 1.3.1: Method of Sieve of Eratosthenes

Examples of prime numbers are 2 (this is the only even prime number), $3, 5, 7, 9, 11, 13, 17, ...$

Method of Sieve of Eratosthenes:



The following will provide us a way to decide given number is prime.

Theorem 1.3.1

Let n be a composite number with exactly 3 positive divisors. Then there exists a prime p such that $n = p^2$.

Proof

Let n be a positive integer with exactly 3 positive divisors. Then two of the positive divisors are 1 and n.
Let d be the third positive divisor. Then $1 < d < n$ and the only positive divisors of d are 1 and d.
Therefore d is prime.
Since $d \mid n$, $n = md, m \in \mathbb{Z}_+$.
Since $m \mid n$ and $1 < m < n, m = d, n = d^2$.
Thus, d is prime. □

Theorem 1.3.2

Every composite number n has a prime divisor less than or equal to $\sqrt{n}$. If p is a prime number and $p \mid n$, then $1 < p \leq \sqrt{n}$.

Proof

Suppose p be the smallest prime divisor of n. Then there exists an integer m such that $n = pm$. Assume that $p > \sqrt{n}$. Then $m < \sqrt{n}$.

Let q be any prime divisor of m. Then q is also a prime divisor of n and $q < m < \sqrt{n} < p$. This is a contradiction.

Example 1.3.2:

Is 223 a prime number?

Solution:

The prime numbers $< \sqrt{223}$ are as follows: $2, 3, 5, 7, 11,$ and 13. Note that $17^2 > 223$.

Since 223 is not divisible by any of the prime numbers identified above, 223 is a prime number.

Exercise 1.3.3

Is 2011 a prime number?.

Answer

yes.

Theorem 1.3.3: Prime divisibility theorem

Let p be a prime number. If $p \mid ab, a, b \in \mathbb{Z}$, then $p \mid a$ or $p \mid b$.

Proof

Let p be a prime number and let $a, b \in \mathbb{Z}$. Assume that $p \mid ab$. If $p \mid a$, we are done. So we suppose that p does not divide a. Thus $gcd(a, p) = 1$. Thus there exists $x, y \in \mathbb{Z}$ such that $1 = ax + py$. Hence $b = abx + pby$. Since $p \mid ab$, $ab = pm, m \in \mathbb{Z}$. Thus $b = pmx + pby = p(mx + by)$. Hence, $p \mid b$.

Theorem 1.3.5

There are infinitely many primes.

Proof

Proof by contradiction.

Suppose there are finitely many primes $p_1, p_2, ..., p_n$, where n is a positive integer. Consider the integer Q such that

$$Q = p_1 p_2 ... p_n + 1. \tag{1.3.1}$$

Notice that Q is not prime. Hence Q has at least a prime divisor, say q. If we prove that q is not one of the primes listed then we obtain a contradiction. Suppose now that $q = p_i$ for $1 \leq i \leq n$. Thus q divides $p_1 p_2 ... p_n$ and as a result q divides $Q - p_1 p_2 ... p_n$. Therefore q divides 1. But this is impossible since there is no prime that divides 1 and as a result q is not one of the primes listed.

The following theorem explains the gaps between prime numbers:

Theorem 1.3.5

Let n be an integer. Then there exists n consecutive composite integers.

Proof

Let n be an integer. Consider the sequence of integers

$$(n+1)!+2, (n+1)!+3, ..., (n+1)!+n, (n+1)!+(n+1) \tag{1.3.2}$$

Notice that every integer in the above sequence is composite because k divides $(n+1)!+k$ if $2 \leq k \leq (n+1)$.

Example 1.3.4:

Does there exist a block of 1000000 consecutive integers without a prime number among them?

Solution

Use $1000001!$ and consider $1000001!+2, \ldots, 1000001!+1000001$

Example 1.3.5:

Consider the formula $y = x^2 + x + 13$. Then

1. Find the values y for $x = 1, \cdots, 12$. How many of these values are prime?

2. Can we conclude that this formula always generates a prime number?

Definition: Twin primes

Two prime numbers are called twin primes if they differ by 2.

Theorem 1.3.6 Fundamental Theorem of Arithmetic (FTA)

Let $n \in \mathbb{Z}_+$, then n can be expressed as a product of primes in a unique way. This means

$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, where $p_1 < p_2 < ... < p_k$ are primes.

Neither the fundamental theorem nor the proof shows us how to find the prime factors. We can use tests for divisibility to find prime factors whenever possible.

Example 1.3.6:

Find the prime factorization of

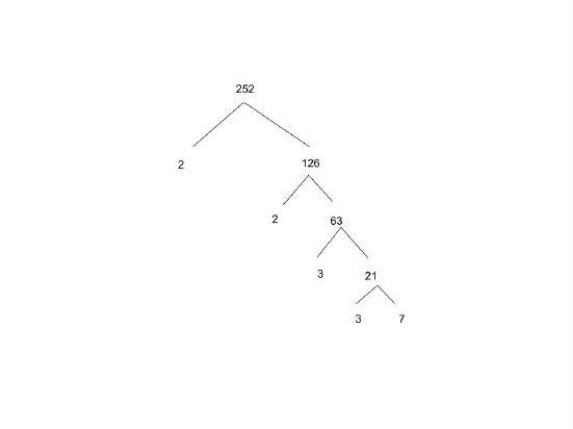
1. 252

2. 2018.

3. 1000

Solution

1. Using divisibility tests, we can find that $252 = 2^2 3^2 7$



2. We can see that 2018 is divisible by 2, and $2018 = 2 \times 1009$. 1009 is prime (why?).

3. $1000 = 10^3 = ((2)(5))^3 = 2^3 5^3$

Example 1.3.7:

Find the prime factorization of 1000001.

Solution

Consider $1000001 = 1000000 + 1 = 10^6 + 1 = (10^2)^3 + 1^3 = (10^2 + 1^2)(10^4 - 10^2 + 1^2) = 101 \times 9901$. 101 and 9901 are prime (why?)

Example 1.3.8

Determine $gcd(2^6 \times 3^9, 2^4 \times 3^8 \times 5^2)$ and $lcm(2^6 \times 3^9, 2^4 \times 3^8 \times 5^2)$.

Solution

$gcd(2^6 \times 3^9, 2^4 \times 3^8 \times 5^2) = 2^4 \times 3^8$ (the lowest powers of all prime factors that appear in both factorizations) and $lcm(2^6 \times 3^9, 2^4 \times 3^8 \times 5^2) = 2^6 \times 3^9 \times 5^2$ (the largest powers of each prime factors that appear in factorizations).

Note: Conjectures

Goldbach's Conjecture(1742)

Every even integer $n > 2$ is the sum of two primes.

Goldbach's Ternary Conjecture:

Every odd integer $n \geq 5$ is the sum of at most three primes.

1.3.0.1 Wilson's Theorem

Theorem 1.3.7

Let p be a prime number. Then $(p-1)! + 1$ is divisible by p.

Proof:

Consider the product $P = 1 \cdot 2 \cdot 3 \cdots (p-1)$. Now, let's pair each number k from 1 to $p-1$ with its modular inverse k^{-1} modulo p.

We know that for every k such that $1 \leq k \leq p-1$, there exists a unique k^{-1} such that $kk^{-1} \equiv 1 \pmod{p}$. Moreover, these pairs will be distinct because if $kk^{-1} \equiv 1 \pmod{p}$ and $jj^{-1} \equiv 1 \pmod{p}$ for $k \neq j$, then $k = kj^{-1}$ and $j = jk^{-1}$, implying $k = j$, which contradicts the distinctness of the pairs.

Thus, we can pair each k with k^{-1} such that the product of these pairs is congruent to $1 \pmod{p}$. Therefore, $P \equiv (p-1)! \equiv -1 \pmod{p}$. Adding 1 to both sides gives $(p-1)! + 1 \equiv 0 \pmod{p}$, which means $(p-1)! + 1$ is divisible by p.

1.3.0.1 Fermat's Little Theorem

Theorem 1.3.8

For any prime number p and any positive integer a such that p does not divide a, we have $a^{p-1} \equiv 1 \pmod{p}$.

1.3.0.1 Euler's Theorem

Theorem 1.3.9

If a and n are relatively prime (i.e., $\gcd(a, n) = 1$), then

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{1.3.3}$$

The following results will help us find Euler's totient function$\phi(n)$ for $n \in \mathbb{N}$.

Theorem 1.3.10

1. If p is prime then $\phi(p) = p - 1$.
2. If p is prime and k is a positive integer then $\phi(p^k) = p^k - p^{k-1}$.
3. If m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$.
4. $$\phi(n) = n \times \prod_{p|n} \left(1 - \frac{1}{p}\right) \tag{1.3.4}$$

where the product is taken over distinct prime factors p of n.

Example 1.3.9

Find $\phi(252)$.

Solution

Since $252 = 2^2 3^2 7$, $\phi(252) = (2^2 - 2)(3^2 - 3)(7 - 1) = 72$.

This page titled 1.3: Primes is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

- **6.1: Prime numbers** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.
- **6.2: GCD, LCM and Prime factorization** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.

1.4: Integers modulo n

Definition: modulo

Let $n \in \mathbb{Z}_+$.

a is congruent to b modulo n denoted as $a \equiv b \pmod{n}$, if a and b have the remainder when they are divided by n, for $a, b \in \mathbb{Z}$.

Example 1.4.1:

Suppose $n = 5$, then the possible remainders are $0, 1, 2, 3$, and 4, when we divide any integer by 5.

Is $6 \equiv 11 \pmod{5}$? Yes, because 6 and 11 both belong to the same congruent/residue class 1. That is to say when 6 and 11 are divided by 5 the remainder is 1.

Is $7 \equiv 15 \pmod{5}$? No, because 7 and 15 do not belong to the same congruent/residue class. Seven has a remainder of 2, while 15 has a remainder of 0, therefore 7 is not congruent to $15 \pmod{5}$. That is $7 \not\equiv 15 \pmod{5}$.

Example 1.4.2: Clock arithmetic

Find $18:00$, that is find $18 \pmod{12}$.

Solution

$18 \pmod{1}2 \equiv 6$. 6 pm.

Properties

Let $n \in \mathbb{Z}_+$. Then

Theorem 1 :

Two integers a and b are said to be congruent modulo n, $a \equiv b \pmod{n}$, if all of the following are true:

a) $m \mid (a - b)$.

b) both a and b have the same remainder when divided by n.

c) $a - b = kn$, for some $k \in \mathbb{Z}$.

NOTE: Possible remainders of n are $0, ..., n - 1$.

Reflexive Property

Theorem 2:

The relation " $\equiv$ " over $\mathbb{Z}$ is reflexive.

Proof: Let $a \in \mathbb{Z}$.

Then $a - a = 0(n$, and $0 \in \mathbb{Z}$.

Hence $a \equiv a \pmod{n}$.

Thus congruence modulo n is Reflexive.

Symmetric Property

Theorem 3:

The relation " $\equiv$ " over $\mathbb{Z}$ is symmetric.

Proof: Let $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$.

Then $a - b = kn$, for some $k \in \mathbb{Z}$.

Now $b - a = (-k)n$ and $-k \in \mathbb{Z}$.

Hence $b \equiv a \pmod{n}$.

Thus, the relation is symmetric.

Antisymmetric Property

Is the relation " $\equiv$ " over $\mathbb{Z}$ antisymmetric?

Counter Example: n is fixed

choose: $a = n+1, b = 2n+1$, then

$a \equiv b \pmod{n}$ and $b \equiv a \pmod{n}$

but $a \neq b$.

Thus the relation " $\equiv$ "on $\mathbb{Z}$ is not antisymmetric.

Transitive Property

Theorem 4 :

The relation " $\equiv$ " over $\mathbb{Z}$ is transitive.

Proof: Let $a, b, c \in \mathbb{Z}$, such that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$.

Then $a = b + kn, k \in \mathbb{Z}$ and $b = c + hn, h \in \mathbb{Z}$.

We shall show that $a \equiv c \pmod{n}$.

Consider $a = b + kn = (c + hn) + kn = c + (hn + kn) = c + (h + k)n, h + k \in \mathbb{Z}$.

Hence $a \equiv c \pmod{n}$.

Thus congruence modulo n is transitive.

Theorem 5:

The relation " $\equiv$ " over $\mathbb{Z}$ is an equivalence relation.

\pmodulo classes

Let $m \in \mathbb{Z}_+$. The relation $\equiv$ on $\mathbb{Z}$ by $a \equiv b$ if and only if $m|(a-b)$, is an equivalence relation. The Classes of $(\mathrm{mod}\ m)$ have the following equivalence classes:

$[0], [1], [2], \ldots, [m-1]$.

Example of writing equivalence classes:

Example 1.4.3:

The equivalence classes for $\pmod 3$ are (need to show steps):

$[0] = \{x \in \mathbb{Z} : x \sim 0\} = \{x \in \mathbb{Z} : x = 0 \pmod 3\}$
$= \{x \in \mathbb{Z} : 3 \mid (x - 0)\} = \{x \in \mathbb{Z} : 3 \mid x\}$
$= \{x \in \mathbb{Z} : x = 3m, m \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$.

$[1] = \{x \in \mathbb{Z} : x \sim 1\} = \{x \in \mathbb{Z} : x = 1 \pmod 3\}$
$= \{x \in \mathbb{Z} : 3 \mid (x - 1)\} = \{x \in \mathbb{Z} : 3 \mid (x - 1)\}$
$= \{x \in \mathbb{Z} : x = 3m + 1, m \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$.

$[2] = \{x \in \mathbb{Z} : x \sim 2\} = \{x \in \mathbb{Z} : x = 2 \pmod 3\}$
$= \{x \in \mathbb{Z} : 3 \mid (x - 2)\} = \{x \in \mathbb{Z} : 3 \mid (x - 2)\}$
$= \{x \in \mathbb{Z} : x = 3m + 2, m \in \mathbb{Z}\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Below, we will explore arithmetic operations in a modulo world.

Let $n \in \mathbb{Z}_+$.

Theorem 5 :

Let $a, b, c, d, \in \mathbb{Z}$ such that $a \equiv b \pmod{}n$ and $c \equiv d \pmod{}n$. Then $(a + c) \equiv (b + d) \pmod{}n$.

Proof:

Let $a, b, c, d \in \mathbb{Z}$, such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

We shall show that $(a + c) \equiv (b + d) \pmod{n}$).

Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}, n \mid (a - b$ and $n \mid (c - d$

Thus $a = b + nk$, and $c = d + nl$, for k and $l \in \mathbb{Z}$.

Consider $(a + c) - (b + d) = a - b + c - d = n(k + l), k + l \in \mathbb{Z}$.

Hence $(a+c) \equiv (b+d) \pmod{n}$.□

Theorem 6:

Edit section

Let $a, b, c, d, \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then $(ac) \equiv (bd) \pmod{n}$.

Proof:

Let $a, b, c, d \in \mathbb{Z}$, such that $a \equiv b \pmod{n})$ and $c \equiv d \pmod{n}$.

We shall show that $(ac) \equiv (bd) \pmod{n}$.

Since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}, n \mid (a-b$ and $n \mid (c-d$

Thus $a = b + nk$, and $c = d + nl$, for k and $l \in \mathbb{Z}$.

Consider $(ac) - (bd) = (b+nk)(d+nl) - bd = bnl + dnk + n^2lk = n(bl + dk + nlk)$, where $(bl + dk + nlk) \in \mathbb{Z}$.

Hence $(ac) \equiv (bd) \pmod{n}$.□

Theorem 7:

Let $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$. Then $a^2 \equiv b^2 \pmod{n}$.

Proof:

Let $a, b \in \mathbb{Z}$, and n $\in \mathbb{Z}_+$, such that $a \equiv b \pmod{n}$.

We shall show that $a^2 \equiv b^2 \pmod{n}$.

Since $a \equiv b \pmod{n}, n \mid (a-b)$.

Thus $(a-b) = nx$, where $x \in \mathbb{Z}$.

Consider $(a^2 - b^2) = (a+b)(a-b) = (a+b)(nx), = n(ax+bx), ax+bx \in \mathbb{Z}$.

Hence $n \mid a^2 - b^2$, therefore $a^2 \equiv b^2 \pmod{n}$. □

Theorem 8:

Let $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$. Then $a^m \equiv b^m \pmod{n}$, $\forall \in \mathbb{Z}$.

Proof:

Exercise.

By using the above results, we can solve many problems. Some of them are discussed below:

Example 1.4.4: $\pmod{3}$ Arithmetic

Let $n = 3$.

Addition

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Multiplication

x	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]

[2]	[0]	[2]	[1]

Example 1.4.5: $(\text{mod } 4)$ Arithmetic

Let $n = 4$.

x	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Example 1.4.6:

Find the remainder when $(101)(103)(107)(109$ is divided by 11.

Answer

$101 \equiv 2 \pmod{1)1}$

$103 \equiv 4 \pmod{1)1}$

$107 \equiv 8 \pmod{1)1}$

$109 \equiv 10 \pmod{1)1}$.

Therefore,

$(101)(103)(107)(109) \equiv (2)(4)(8)(10) \pmod{1)1} \equiv 2 \pmod{1)1}$.

Example 1.4.7:

Find the remainder when7^{1453} is divided by 8.

Answer

$7^0 \equiv 1 \pmod{8}$

$7^1 \equiv 7 \pmod{8}$

$7^2 \equiv 1 \pmod{8}$

$7^3 \equiv 7 \pmod{8}$,

As there is a consistent pattern emerging and we know that 1453 is odd, then $7^{1453} \equiv 7 \pmod{8}$. Thus the remainder is 7.

Example 1.4.8:

Find the remainder when 7^{2020} is divided by 18.

Answer

$7^0 \equiv 1 \pmod{1)8}$

$7^1 \equiv 7 \pmod{1)8}$

$7^2 \equiv 13 \pmod{1)8}$

$7^3 \equiv 1 \pmod{1)8}$,

As there is a consistent pattern emerging and we know that $2020 = (673)3 + 1$, $7^{2020} = 7^{(673)3+1} = (7^3)^{673} 7^1 \equiv 7 \pmod{1)8}$. Thus the remainder is 7.

Example 1.4.9:

Find the remainder when 26^{1453} is divided by 3.

Example 1.4.12:

Show that n^2+1 is not divisible by 3 for any integer n.

Answer

Proof: Let $n \in \mathbb{Z}$. We shall show that (n^2+1) is not divisible by 3 using the language of congruency.

We shall show that $(n^2+1) \pmod 3) \not\equiv 0$ by examining the possible cases.

Case 1: $n \equiv 0 \pmod 3$.

$\implies n^2 \equiv 0^2 \pmod 3$.

$\implies (n^2+1) \equiv 1 \pmod 3$.

Hence n^2+1 is not divisible by 3.

Case 2: $n \equiv 1 \pmod 3$.

$n^2 \equiv 1^2 \pmod 3$.

$(n^2+1) \equiv 1 \pmod 3$.

Hence n^2+1 is not divisible by 3.

Case 3: $n \equiv 2 \pmod 3$.

$n^2 \equiv 2^2 \pmod 3) \equiv 1 \pmod 3)$.

$(n^2+1) \equiv 2 \pmod 3)$.

Hence n^2+1 is not divisible by 3.

Since none of the possible cases is congruent to $0 \pmod 3), n^2+1$ is not divisible by 3. □

Example 1.4.13:

Show that $5 \mid a^5+4a$ for any integer a.

Answer

Notice that $4 \equiv -1 \pmod 5)$. Therefore, $5 \mid a^5+4a$ iff $5 \mid a^5-a$ for all integer a.

Let $a \in \mathbb{Z}$.

We shall show that $a^5 = a \pmod 5), \forall a \in \mathbb{Z}$.

Then $5 \mid (a^5 \quad a)$ and $a^5 \quad a \equiv 0 \pmod 5)$.

We will proceed by examining the 5 possible cases of \(a \) Specifically, $a \in \{0,1,2,3,4\}$.

Case $a = 0$: If $a = 0$ then $a^5 = 0^5$

$\equiv 0 \pmod 5)$.

Thus $a^5 \quad a \equiv 0 \pmod 5)$.

Case $a = 1$: If $a = 1$ then $a^5 = 1^5$

$\equiv 1 \pmod 5)$.

Thus $a^5 \quad a \equiv 0 \pmod 5)$.

Case $a = 2$: If $a = 2$ then $a^5 = 2^5$

$= 5(6) + 2$

$= 2 \pmod 5)$.

Thus $a^5 \quad a \equiv 0 \pmod 5)$.

Case $a = 3$: If $a = 3$ then $a^5 = 3^5$

$= 5(48) + 3$

$\equiv 3 \pmod 5$.

Thus $a^5 \equiv a \pmod 5$.

Case $a = 4$: If $a = 4$ then $a^5 = 4^5$

$= 5(204) + 4$

$\equiv 4 \pmod 5$.

Thus $a^5 \equiv a \pmod 5$.

Having examined all possible cases, $a^5 \equiv a \pmod 5$. □

Answer

Let $a \equiv b \pmod 5$ where $a \in \mathbb{Z}$ and $b \in \{0, 1, 2, 3, 4\}$.

Then $5 \mid (a - b)$.

Thus $a - b = 5m, m \in \mathbb{Z}$. Rearranging, we obtain $a = 5m + b$.

Consider $a^5 = (5m + b)^5$

$= \sum_{k=0}^{5} (5m)^{(5-k)} \cdot b^k$

$= \left(\sum_{k=0}^{4} (5m)^{(5-k)} \cdot b^k \right) + b^5$

$= 5m \cdot \left(\sum_{k=0}^{4} (5m)^{(5-k-1)} \cdot b^k \right) + b^5$.

Let $q = m \cdot \left(\sum_{k=0}^{4} (5m)^{(5-k-1)} \cdot b^k \right)$.

Since $k, m, b \in \mathbb{Z}$, then $q \subset \mathbb{Z}$.

Thus $a^5 = 5q + b^5$.

Clearly, $5 \mid 5q$. We shall examine the possible cases of b^5.

Case b=0: If $b = 0$ then $a^5 = 5q + 0^5$. Thus $a^5 \equiv a \pmod 5$.

Case b=1: If $b = 1$ then $a \equiv 1 \pmod 5$ and $a^5 = 5q + 1$ where q $\in \mathbb{Z}$.

Thus $a^5 = 5q + 1 \pmod 5 \equiv a \pmod 5$.

Case b=2: If $b = 2$ then $a \equiv 2 \pmod 5$ and $2^5 = 5(6) + 2$.

Thus $a^5 = 5q + 5(6) + 2 \pmod 5 = 5(q + 6) + 2 \equiv a \pmod 5$.

Case b=3: If $b = 3$ then $a \equiv 3 \pmod 5$ and $3^5 = 5(48) + 3$.

Thus $a^5 = 5q + 5(48) + 3 \pmod 5 = 5(q + 48) + 3 \equiv a \pmod 5$.

Case b=4: If $b = 4$ then $a \equiv 4 \pmod 5$ and $4^5 = 5(204) + 4$.

Thus $a^5 = 5q + 5(204) + 4 \pmod 5 = 5(q + 204) + 4 \equiv a \pmod 5$.

Having examined all possible cases, $a^5 \equiv a \pmod 5$. □

Example 1.4.14

For every positive integer n, prove that $n^3 - n$ is divisible by 3.

Answer

Proof:

Let $S(n)$ be the statement $3 \mid (n^3 - n)$.

$S(n)$ says that $n^3 - n = 3m, m \subset \mathbb{Z}$.

$S(1)$ says that $1^3 - 1 = 3m, m \in \mathbb{Z}$. Since $0 = 3(0)$ and $0 \in \mathbb{Z}$, $S(1)$ is true.

Assume $S(n)$ is true for some $k = n$.

We will show that $S(k+1)$ is true.

Specifically, we will show that $(k+1)^3-(k+1)=3t, t\in\mathbb{Z}$.

Consider that $(k+1)^3-(k+1)=(k+1)^3-(k+1)$

$=k^3+3k^2+3k+1-k-1$

$=(k^3-k)+3k^2+3k$

$=3m+3k^2-3k$

$=3(m+k^2-k)$.

Since $m,k\in\mathbb{Z}$, $m+k^2-k\in\mathbb{Z}$.

Let $t=m+k^2-k$.

Thus $(k+1)^3-(k+1)=3t, t\in\mathbb{Z}$.

Having shown the inductive step, for every positive integer n, n^3-n is divisible by 3.

Multiplicative inverse modulo m

Let $m\in\mathbb{Z}_+$. Let $a\in\mathbb{Z}$ such that a and m are relatively prime. Then there exist integers x and y such that $ax+my=1$. Then $ax\equiv 1 \pmod m$, also denoted by $ax\cong 1 \pmod m$. Note that 1 is the multiplicative identity on \pmod m \). In this case, $x \pmod m$ is the inverse of $a \pmod m$.

Example 1.4.10

If possible, find multiplicative inverse of $2 \pmod{10}$.

Solution

Since $\gcd(2,10)=2\neq 1$, 2 has no multiplicative inverse modulo 10.

Example 1.4.11

If possible, find multiplicative inverse of $16 \pmod{35}$.

Solution

Using the Euclidean Algorithm, we will find $gcd(16,35)$.

$$\begin{aligned} 35 &= (16)(2)+3 \\ 16 &= (3)(5)+1 \\ 3 &= (1)(3)+0 \end{aligned}$$

Thus $gcd(16,35)=1$. Hence multiplicative inverse of $16 \pmod{35}$ exists.

By using the Bezout's algorithm,

$$\begin{aligned} 1 &= 16+(3)(-5) \\ &= 16+(35+(16)(-2))(-5) \\ &= (35)(-5)+(16)(11) \end{aligned}$$

Thus $gcd(16,35)=1=(35)(-5)+(16)(11)$. Hence the multiplicative inverse of $16 \pmod{35}$ is 11.

If m is prime, then by Fermat's little theorem, $a^m\cong a \pmod m$, for all integers a.

Hence $a^{(m-1)}\cong 1 \pmod m$, for all integers a that are relatively prime to m. Thus, if $gcd(a,m)=1$ and m is prime then $a^{-1}\cong a^{(m-2)} \pmod m$),

Odd and Even integers:

An integer n is even iff $n\equiv 0 \pmod 2$).

An integer n is odd iff $n\equiv 1 \pmod 2$).

Two integers a and b are said to have some parity if they are both even or both odd otherwise a and b are said to have different parity.

Example 1.4.15:

Show the sum of an odd integer, and an even integer is odd.

Answer

Proof: Let a be an odd integer and let b be an even integer. We shall show that $a+b$ is odd by using the language of congruency.

Since a is odd, $a \equiv 1 \pmod 2$.

Since b is even, $b \equiv 0 \pmod 2$.

Then $(a+b) \equiv (1+0) \pmod 2$,

$$(a+b) \equiv 1 \pmod 2.$$

Hence $a+b$ is odd.□

Example 1.4.16:

Show that the product of an odd integer and an even integer is even.

Answer

Proof: Let a be an odd integer and let b be an even integer. We shall show that ab is even by using the language of congruency.

Since a is odd, $a \equiv 1 \pmod 2$.

Since b is even, $b \equiv 0 \pmod 2$.

Then $(ab) \equiv (1)(0) \pmod 2$,

$$(ab) \equiv 0 \pmod 2.$$

Hence ab is even.□

1.4: Integers modulo n is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

- **3.1: Modulo Operation** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.
- **3.2: Modulo Arithmetic** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.

1.5 Linear Congruence

Linear Congruences

Definition: Linear Congruences

A linear congruences in one variable has the form $ax \equiv b(mod\, m)$, where $m \in \mathbb{Z}_+$, $a, b \in \mathbb{Z}$ and $x \in \mathbb{Z}$ is a variable.

A linear congruence is similar to a linear equation, solving linear congruence means finding all integer x that makes, $ax \equiv b(mod\, m)$ true. In this case, we will have only a finite solution in the form of $x \equiv (mod\, m)$. Thus there will be at most m solutions, namely $0, 1, \ldots, m-1$.

Thus, a linear congruence in one variable x is of the form $ax \equiv b(mod\ m)$, where $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}_+$. This form of linear congruence has at most m solutions.) In this section, we shall assume $a(\neq 0) \in \mathbb{Z}$.

Method I: We can find the solutions to a linear congruence, by checking all possible $0, 1, \ldots, m-1$.

Example 1:

Find all solutions to $x \equiv 6(mod\, 11)$, between 0 and 10 inclusive.

Solution

Possible solutions are $0, 1, 2, \ldots, 10$. The only solution is 6.

Example 2:

Find all solutions to $2x \equiv 3(mod\, 7)$, between 0 and 6 inclusive.

Solution

Possible solutions are $0, 1, 2, \ldots, 6$. The only solution is 5.

Example 3:

Solve $3x \equiv 1(mod\, 8)$.

Solution

Possible solutions are $0, 1, 2, \ldots, 7$. The only solution is 3.

Example 4

Find all solutions to $3x \equiv 1(mod\, 6)$, between 0 and 5 inclusive.

Solution

Possible solutions are $0, 1, 2, 3, 4, 5$. In this case $3x(mod\ 6)$ is $0, 3, 0, 3, 0, 3$. Thus, $3x \equiv 1(mod\, 6)$ has no solutions.

Example 5:

Solve $2x \equiv 2(mod\, 4)$.

Solution

Possible solutions are $0, 1, 2, 3$. The solutions are 1 and 3.

The following theorems give a criterion for the solvability of $ax \equiv b(mod\, m)$.

Method II:

Theorem 1

Let $m \in \mathbb{Z}_+$ and $a, b, c \in \mathbb{Z}$. If $\gcd(c, m) = 1$ and $ac \equiv bc (mod\, m)$ then $a \equiv b (mod\, m)$

Proof

Let $m \in \mathbb{Z}_+$ and $a, b, c \in \mathbb{Z}$. Assume that $\gcd(c, m) = 1$ and $ac \equiv bc (mod\, m)$. Since $ac \equiv bc (mod\, m)$, $ac - bc = mn$, for $n \in \mathbb{Z}$. Thus $(a - b)c = mn$. Thus $m \mid (a - b)c$. Since $\gcd(c, m) = 1$, $m \mid (a - b)$. Hence, $a \equiv b (mod\, m)$.

Example 6

Solve $3x \equiv 1 (mod\, 8)$.

Solution

We will solve using the above theorem. $3x \equiv 1 \equiv 9 (mod\, 8)$. Hence, $x \equiv 3 (mod\, 8)$.

Theorem 2

Let $m \in \mathbb{Z}_+$ and $a, b, c \in \mathbb{Z}$. Then $ac \equiv bc (mod\, m)$ if and only if $a \equiv b \left(mod \frac{m}{\gcd(c, m)} \right)$

Proof

TBA

Example 7

Solve $9x \equiv 6 (mod\, 24)$.

Solution

Since $\gcd(3, 24) = 3$,, $3x \equiv 2 (mod\, 8)$. Thus $3x \equiv 2 \equiv 10 \equiv 18 (mod\, 8)$. Hence $x \equiv 6 (mod\, 8)$.

The above two methods are tedious when the numbers are large.

Theorem 3

Let $m \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$, with a be non-zero. Then

$ax \equiv b (mod\, m)$ has a solution if and only if $\gcd(a, m) | b$. Moreover, if $x = x_0$ is a particular solution to this congruence, then the set of all solutions is $\{x \in \mathbb{Z} | x \equiv x_0 (mod\, m)\} = \left\{ x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d} \right\}$, where $d = \gcd(a, m)$.

Proof

TBA

We will see below how to find the solution for a particular case: Using Multiplicative inverse modulo m

Let $m \in \mathbb{Z}_+$. Let $a \in \mathbb{Z}$ such that a and m are relatively prime. Then there exist integers x and y such that $ax + my = 1$. Then $ax \equiv 1 (mod\, m)$. Note that 1 is the multiplicative identity on $mod\, m$. In this case, $x (mod\, m)$ is the inverse of $a (mod\, m)$.

Theorem 3

If $\gcd(a, m) = 1$ then $ax \equiv b (mod\ m)$ has a unique solution $x \equiv a^{-1} b (mod\ m)$. Thus, the set of all solutions is $\{x \in \mathbb{Z} | x \equiv a^{-1} b (mod\, m)\}$.

Proof

Since $\gcd(a, m) = 1$, therefore a has an inverse $a^{-1} \mod m$. Hence $x \equiv a^{-1} b (mod\, m)$.

Example 8

Solve $16x \equiv 11 (mod\, 35)$.

Solution

Since $16x \equiv 11 (mod\, 35)$, $x \equiv (16)^{-1}11 (mod\, 35) \equiv (11)(11) (mod\, 35) \equiv 16 (mod\, 35)$.

The following theorem guides on solving linear congruence. However, we will discuss it after learning the linear Diophantine equations.

Theorem 4

Let $m \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$, with a be non-zero. Then, the linear congruence

$ax \equiv b (mod\, m)$ has a solution if and only if $\gcd(a, m)|b$. Moreover, if $x = x_0$ is a particular solution to this congruence, then the set of all solutions is $\{x \in \mathbb{Z} | x \equiv x_0 (mod\, m)\} = \left\{x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}\right\}$, where $d = \gcd(a, m)$.

The Chinese Remainder Theorem

In this section, we will explore solving simultaneous linear congruences.

Theorem 5

Let $a, b \in \mathbb{Z}$ and $n, m \in \mathbb{N}$ such that $\gcd(n, m) = 1$. Then there exists $x \in \mathbb{Z}$ such that $x \equiv a (mod\, n)$ and $x \equiv b (mod\, m)$. Moreover x is unique modulo mn.

Example 5:

Solve $x \equiv 2 (mod\, 3)$ and $x \equiv 3 (mod\, 5)$.

Solution

Since $x \equiv 2 (mod\, 3)$, the possible solutions are $2, 5, 8, 11, 15, \ldots$.

Since $x \equiv 3 (mod\, 5)$, the possible solutions are $3, 8, 13, \ldots$.

Then $x = 8$. Since any y such that $y \equiv 8 (mod\, 15)$ are also solutions, we have $23, 38, \cdots$

Theorem 6: Chinese Remainder Theorem

Let $a_1, \cdots, a_k \in \mathbb{Z}$ and $m_1, \cdots, m_k \in \mathbb{N}$ such that $\gcd(m_i, m_j) = 1$, for all $i \neq j$. Then there exists $x \in \mathbb{Z}$ such that

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{1}$$

.

Moreover x is unique modulo $m_1 \ldots m_k$.

Note

Solving Congruences, using Chinese Remainder Theorem

Let

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{2}$$

.

Then

Step 1: Calculate the product $M = m_1 \times m_2 \times ... \times m_k$.

Step 2: Calculate the Modulus Factors. For each m_i, calculate $M_i = \frac{M}{m_i}$.

Step 3: Compute the Inverses. For each M_i, compute the modular inverse M_i^{-1} modulo m_i.

Step 4: Combine Solutions. Finally, the solution x to the system of congruences is given by:

$$x = \left(\sum_{i=1}^{k} a_i M_i M_i^{-1} \right) \pmod{M} \tag{3}$$

We can use the following table to compute all the listed variables.

a_i	m_i	M_i	M_i^{-1}	M

Example 6

Solve

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{7} \\ x \equiv 6 \pmod{8} \end{cases} \tag{4}$$

.

Answer

a_i	m_i	M_i	M_i^{-1}	M
3	5	$\frac{280}{5} = 56$	1	280
1	7	$\frac{280}{7} = 40$	3	280
6	8	$\frac{280}{8} = 35$	3	280

First we calculate $M = (5)(7)(8)280$. Now we can calculate M_1, M_2 and M_3.

Next we calculate M_1^{-1}, M_2^{-1} and M_3^{-1}.

To calculate M_1^{-1}: we need to solve $56x_1 \equiv 1 \pmod{5}$. Place these values into the table.

Now, $x \equiv ((3)(56)(1) + (7)(40(3) + (8)(35)(3)) \pmod{280} \equiv 918 \pmod{280} \equiv 78 \pmod{280}$.

1.5 Linear Congruence is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

- **4.5: Linear Congruences** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.

1E: Exercises

Exercise $1E.1$

For every positive integer n, prove that $\frac{1}{(1)(2)} + \frac{1}{(2)(3)} + \cdots + \frac{1}{(n)(n+1)} = \frac{n}{n+1}$.

Answer

We can rewrite each term as $\frac{1}{k(k+1)} = \frac{k+1-k}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$. Therefore, the sum telescopes as follows:

$$\begin{aligned} &\frac{1}{1} - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \cdots + \frac{1}{n} - \frac{1}{n+1} \\ &= 1 - \frac{1}{n+1} = \frac{n}{n+1}. \end{aligned}$$

Exercise $1E.2$

For any positive integer n, prove that $2^n 3^{2n} - 1$ is always divisible by 17.

Answer

By Fermat's Little Theorem, $2^{16} \equiv 1 \pmod{17}\$and\$3^{16} \equiv 1 \pmod{17}$. Therefore, $2^{16n} \equiv 1 \pmod{17}$ and $3^{32n} \equiv 1 \pmod{17}$. Hence, $2^n 3^{2n} - 1 \equiv 1 \cdot 1 - 1 \equiv 0 \pmod{17}$.

Exercise $1E.3$

a. Let $a, b, c \in \mathbb{Z}_+$. Show that $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

b. Let $a, b, c, d \in \mathbb{Z}$. If $a|b$ and $c|d$, show that $gcd(a, c)|gcd(b, d)$.

Exercise $1E.4$

Show that $a^5 \equiv a \pmod{5}$ for all integers a.

Exercise $1E.5$

Using Euclidean algorithm to find $\gcd(2520, 154)$ and express $\gcd(2520, 154)$ as an integer combination of 2520 and 154. Also,

Using the Euclidean algorithm to find $\gcd(-2520, 154)$ and express $\gcd(-2520, 154)$ as an integer combination of -2520 and 154.

Exercise $1E.6$

For every positive integer n, prove that $n^3 - n$ is divisible by 3.

Exercise $1E.7$

For any $k \in \mathbb{N}$ prove that $\gcd(4k + 3, 7k + 5) = 1$.

Exercise $1E.8$

a) Use the Euclidean algorithm to find the $\gcd(-29, 571)$?

b) Find integers x and y s.t. $\gcd(-29, 571) = -29(x) + 571(y)$?

Exercise $1E.9$

Show that any two consecutive odd integers are relatively prime.

Exercise $1E.10$

If m, n are any odd integers, show that $m^2 - n^2$ is divisible by 8.

Exercise $1E.11$

a) Prove that for all integers $n \geq 1$,

$\frac{1}{2!} + \frac{2}{3!} + \cdots + \frac{n}{(n+1)!} = 1 - \frac{1}{(n+1)!}$.

b) Prove that for all integers $n \geq 1$,

$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} \geq \sqrt{n}$.

Exercise $1E.12$

For integer $n \geq 1$, define

$S_n = -\binom{2}{2} + \binom{3}{2} - \binom{4}{2} + \binom{5}{2} \cdots + \binom{2n+1}{2}$.

1. Evaluate S_n for $n = 1, 2, 3, 4$ and 5.
2. Use part (a) to guess a formula for S_n.
3. Use mathematical induction to prove your guess.

Exercise $1E.13$

Find the remainder when 8^{391} is divided by 5.

Exercise $1E.14$

For each of the following pairs of integers a and n. show that a and n are relatively prime, determine multuplicative inverse of $[a]$ in $\mathbb{Z}_n$, and Find all integers x for $ax \cong 11 (mod\, n)$.

1. $a = 16, n = 35$.
2. $a = 69, n = 89$.

Exercise $1E.15$

Find the remainder when $(201)(203)(205)(207)$ is divided by 13.

This page titled 1E: Exercises is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

Chapter 2: Groups

Groups are a fundamental concept in abstract algebra. Understanding their definitions and properties and studying examples is important in order to gain a comprehensive understanding of algebraic structures.

Learning Objectives

- Define and understand the basic concepts of groups and properties.
- Define and distinguish between various types of groups, such as finite and infinite groups, abelian and non-abelian groups, and cyclic and non-cyclic groups..
- Determine whether a given subset of a group is a subgroup.
- Prove basic results involving various types of groups.
- Solve basic problems involving various groups and its subgroups.

This page titled Chapter 2: Groups is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

2.1: Introduction to Group

Definition: Group

Let G be a non-empty set.

A **binary operation**, $\star$, on G is defined as : $a \star b$ for all $a, b \in G$.

A **closed binary operation**, $\star$, on G is defined as a function: $\star : G \times G \to G, \star(a, b) = a \star b \in G$.

Then G with the closed binary operation $\star$, $(G, \star)$, is a group if all of the following conditions are satisfied:

1. **Associative**: $a \star (b \star c) = (a \star b) \star c$; $\forall a, b, c \in G$.
2. **Identity**: There exists an identity, $e \in G$, s.t. $e \star a = a \star e = a$.
3. **Inverse**: For each element $a \in G$, there exists an element $b \in G$ s.t. $a \star b = b \star a = e$.

In other words, A group is a non-empty set associated with a binary operation that satisfies certain axioms. The operation must be closed, associative, and have an identity element. Additionally, every element must have an inverse.

Definition: Abelian Group

Let $(G, *)$ be a group. Then $(G, *)$ is called an **abelian** group if $a \star b = b \star a, \forall a, b \in G$. That is that the group satisfies the **commutative** property

A summary of the terms is shown below.

Term	Notation	Meaning
SET	G	A set.
↓		
SET w OPERATION	(G, ✷)	A set with an operation
↓		
SEMIGROUP	(G, ✷)	A set with an operation that is associative
↓		
MONOID	(G, ✷)	A set with an operation that is associative & has an identity.
↓		
GROUP	(G, ✷)	A set with an operation that is associative, has an identity & inverse
↓		
ABELIAN GROUP	(G, ✷)	A set with an operation that is associative, has an identity, has an inverse and is commutative.

Example 2.1.1

The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ with addition $+$ are groups with the identity of 0 and each element a an inverse $-a$.

Example 2.1.2

$(\mathbb{Z}, \cdot)$ is a monoid, has no inverse, and is thus not a group. Why?

It's a set with an operation, is closed, is associative, and has an identity but does not have an inverse.

Counterexample:

$2 \in \mathbb{Z}$, but there is no element $b \in \mathbb{Z}$ s.t. $2 \cdot b = 1$.

Example 2.1.3

Let V be a vector space, then $(V,+)$ is an abelian group.

Example 2.1.4

Let $n \in \mathbb{Z}_+$.

Let $M_{nn}(\mathbb{R})$ be the set of all $n \times n$ matrices over $\mathbb{R}$ then $(M_{nn}(\mathbb{R}),+)$ is an abelian group.

Let $M_{nn}(\mathbb{C})$ be the set of all $n \times n$ matrices over $\mathbb{C}$ then $(M_{nn}(\mathbb{C}),+)$ is an abelian group.

Example 2.1.5

$GL_2(\mathbb{R}) = \left\{A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} | a,b,c,d \in \mathbb{R}, \det(A) = ad - bc \neq 0\right\}$ where $GL_2(\mathbb{R})$ stands for General Linear Group that is a 2×2 matrix.

Is $(GL_2(\mathbb{R}),\cdot)$ a group? Yes, but not an Abelian group.

$[A] \cdot ([B] \cdot [C]) = ([A] \cdot [B]) \cdot [C]$ is true, so we have associativity.

Every element $[A]$ in $GL_2(\mathbb{R})$ has an inverse since $det(A) \neq 0$.

Since $I \in GL_2(\mathbb{R}), GL_2(\mathbb{R})$ has an identity.

Matrix multiplication is not commutative since $[A] \cdot [B] \neq [B] \cdot [A]$.

Counterexample:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix}$$

Notice that $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in GL_2(\mathbb{R})$.

Since $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix}$, $(GL_2(\mathbb{R}),\cdot)$ is not commutative.

Thus $(GL_2(\mathbb{R}),\cdot)$ is a group, but not an abelian group since it is not commutative.

Note

Let $n \in \mathbb{Z}_+$.

$GL_n(\mathbb{R}) = \left\{A \in M_{nn}(\mathbb{R}) | \det(A) \neq 0\right\}$, **General Linear Group** over $\mathbb{R}$.

$GL_n(\mathbb{C}) = \left\{A \in M_{nn}(\mathbb{C}) | \det(A) \neq 0\right\}$, **General Linear Group** over $\mathbb{C}$.

Example 2.1.6

Let $SL_2(\mathbb{R}) = \left\{A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} | a,b,c,d \in \mathbb{R}, \det(A) = ad - bc = 1\right\}$, where $SL_2(\mathbb{R})$ stands for **Special Linear Group** that is a 2×2 matrix. Is $(SL_2(\mathbb{R}),\cdot)$ a group?

Proof:

Let $A, B \in SL_2(\mathbb{R})$.

Then $\det(A) = \det(B) = 1$.

Consider $\det(AB) = \det(A) \cdot \det(B) = (1)(1) = 1$.

Hence $AB \in SL_2(\mathbb{R})$.

Since matrix multiplication is associative, $(SL_2(\mathbb{R}), \cdot)$ is associative.

Since the 2×2 matrix identity, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{R})$, and $AI = IA = A$ for all $A \in SL_2(\mathbb{R})$, $(SL_2(\mathbb{R}), \cdot)$ has the identity.

Inverse:

Proof:

Let $A \in SL_2(\mathbb{R})$.

Then $\det(A) = 1$, therefore A^{-1} exists.

Consider $\det(A^{-1}) = \frac{1}{\det(A)} = 1$.

Therefore $A^{-1} \in SL_2(\mathbb{R})$.

Hence $SL_2(\mathbb{R})$ is a group, but not an abelian group.

Note that $SL_2(\mathbb{R}) \subseteq GL_2(\mathbb{R})$.

Definition:

If $(G, *)$ is a group, then

1. If $|G|$ is finite, then $(G, *)$ is called a finite group.
2. If $|G|$ is infinite, then $(G, *)$ is called an infinite group.

Cayley Table

A Cayley table, named after the British mathematician Arthur Cayley, is a square table used in group theory to represent the binary operation of a finite group. It provides a concise way to display all possible combinations of group elements and the result of their operation.

Here are some examples of Cayley tables.

Example 2.1.7

Define a relation on $\mathbb{Z}$ by aRb iff $a \equiv b \pmod 4$, $a, b \in \mathbb{Z}$, then R is an equivalence relation and the equivalence classes are $[0], [1], [2]$ and $[3]$. Another way to show the equivalence classes is to use the following notation: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

Cayley Tables for $+$ and $\cdot (mod 4)$ are shown below.

Note: The above tables are commutative; we can see them by noticing a mirror image along the diagonal.

$(\mathbb{Z}_4, +)$ is an abelian group. In fact, $(\mathbb{Z}_n, +)$ is an abelian group for every positive integer n.

Addition Table Mod 4				
+(mod 4)	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Multiplication Table Mod 4				
✶(mod 4)	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Note: In the case of multiplication, we must remove zero to make a group in many cases. We will denote $\mathbb{Z}_n^* = \{1, 2, \cdots, n-1\}$. However, in the case of $(\mathbb{Z}_4^*, +)$ and $(\mathbb{Z}_4^*, *)$ this would not make a group, since $2 + 2 = 0 \pmod 4$, $2 \cdot 2 = 0 \pmod 4$, but $0 \notin \mathbb{Z}_4^*$. $(\mathbb{Z}_n^*, *)$ forms a group if n is prime.

Note

Thinking Out Loud - Discussion of Modular Operations

Let $m \in \mathbb{Z}_+$.

If $a \equiv b \pmod m$ and $c \equiv d \pmod m$,then

$ac \equiv bd \pmod m$, $a + c \equiv b + d \pmod m$, and $a^n \equiv b^n \pmod m$.

In terms of $\pmod m$, we use $\mathbb{Z}_m = \{0, 1, 2, 3, \ldots m-1\}$.

Note $(\mathbb{Z}_m, + \pmod m)$ is always an abelian group.

Note $(\mathbb{Z}_m, \bullet \pmod m)$ is not always a group (need to remove zero and for $m =$ a prime). If $(\mathbb{Z}_m^*, \bullet \pmod m)$ is a group, then the group is abelian, since $ab \equiv ba \pmod m$.

Example 2.1.8

Let $(G, *)$ be the set $\{A, R, L, B\}$ where A stands for "attention," R stands for "turn right," L stands for "Turn Left," and B stands for "About Face." The Cayley table is shown below:

*	A	R	L	B
A	A	R	L	B
R	R	B	A	L
L	L	A	B	R
B	B	L	R	A

Note that the multiplication table is same as $(\mathbb{Z}_4, + \pmod 4)$. In this case, we say that this group isomorphic to $(\mathbb{Z}_4, + \pmod 4)$.

Example 2.1.9

Is $(\mathbb{Z}_2 \times \mathbb{Z}_2, \bigoplus)$ a group?

Cayley Table for $(\mathbb{Z}_2 \times \mathbb{Z}_2, \bigoplus)$				
$\bigoplus$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

1. The product (in this case, component modulo 2) of any two elements is contained in the set.
2. The set and operation are associative since $a \bigoplus (b \bigoplus c) = (a \bigoplus b) \bigoplus c) \forall a, b, c \in \mathbb{Z}_2 \times \mathbb{Z}_2$.
3. The SEMIGROUP has an identity since $a \bigoplus e = e \bigoplus a = a, \forall a \in \mathbb{Z}_2 \times \mathbb{Z}_2$. The identity is $(0,0)$.
4. The semigroup has an inverse since $\exists a, b \in \mathbb{Z}_2 \times \mathbb{Z}_2 | a \bigoplus b = b \bigoplus a = e$. Look at $(0,1) \bigoplus (0,1) = (0,0)$, which is the identity. For proof, we would need to examine all cases.
5. The GROUP is also abelian since it is commutative (determined by seeing that the top diagonal matrix is the same as the bottom diagonal matrix).
6. The group is also finite since we could list all the elements.

Note: $(\mathbb{Z}_2 \times \mathbb{Z}_2, \bigoplus)$ is called a **Klein 4 (K_4) Group**. This can be defined as $K_4 = \{e, a, b, c\}$ such that $a^2 = b^2 = c^2 = e$ with the product of any two distinct non-identity elements is the third: $ab = c$, $ac = b$, and $bc = a$.

Example 2.1.10

Quaternion Group:

$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, where i is the complex number such that $i^2 = -1$.

Define $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$. Then Q_8 with multiplication forms a group. This is a finite non-abelian group. Why?

Note

Notation Notes:

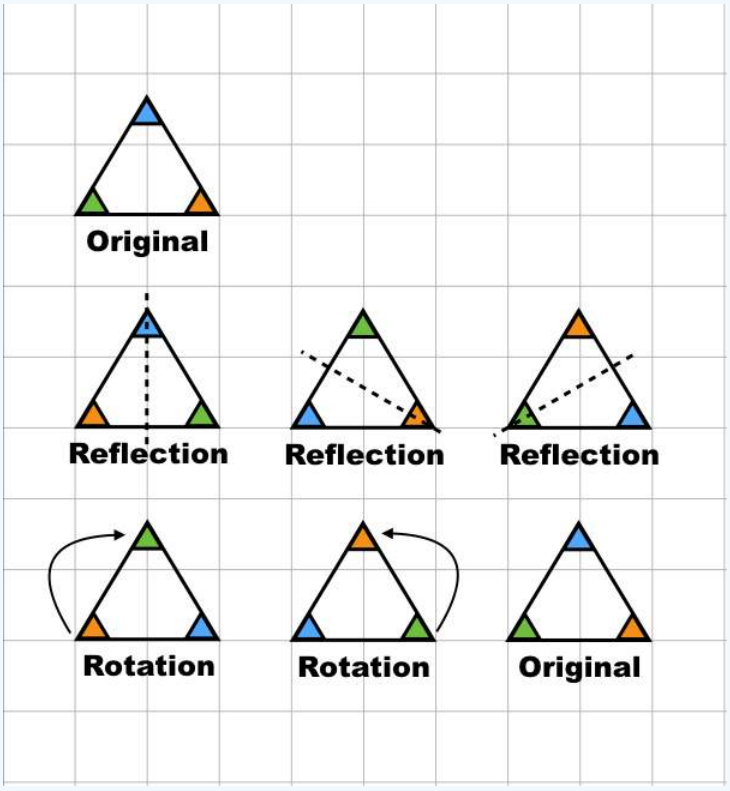
$(\mathbb{Q}^*, \bullet)$: the * indicates that zero is eliminated. This is usually done to obtain an inverses.

$(\mathbb{Z}_n, +)$: The subscript indicates the operation is $(\mathbf{mod}\ n)$.

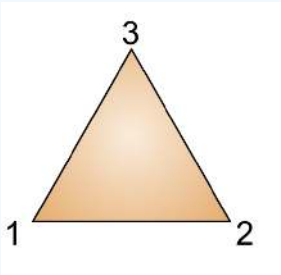
We will discuss these examples in detail later.

Example 2.1.11: Dihedral Group

Consider the equilateral triangle below. What rigid motions can we make to it that will result in the triangle occupying the same space? What happens if we combine rigid motions? Keep in mind that "doing nothing" is also a rigid motion.



Symmetries of equilateral triangles:



Let r be a rotation then there are three rotations I, r, r^2. Let s be a reflection, then there are s, rs, r^2s elements. In this case, $r^3 = s^2 = I$ and $sr = r^2s$. Thus $D_3 = \{I, r, r^2, s, rs, r^2s\}$.

Example 2.1.12:Symmetric Group

Notation:

$1 \equiv \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ the identity matrix.

$(1,2) \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Note that 3 points to itself.

$(1,2,3) \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

$(1,3,2) \equiv \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix}$.

$S_3 = \{1, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$. This is the list of possible permutations of the above triangle in Example 2.1.11. Note that $(1,2,3)$ and $(3,2,1)$ are rotations, while $(1,2), (1,3)$, and $(2,3)$ are reflections around the missing angles bisection. $|S_3| = 3! = 2 \cdot 3 = 6$.

Cayley Table for S_3						
	1	(1,2,3)	(1,3)	(1,2)	(2,3)	(1,3,2)
1	1	(1,2,3)	(1,3)	(1,2)	(2,3)	(1,3,2)
(1,2,3)	(1,2,3)	(1,3,2)	(2,3)	(1,3)	(1,2)	1
(1,3)	(1,3)	(1,2)	1	(1,2,3)	(1,3,2)	(2,3)
(1,2)	(1,2)	(2,3)	(1,3,2)	1	(1,2,3)	(1,3)
(2,3)	(2,3)	(1,3)	(1,2,3)	(1,3,2)	1	(1,2)
(1,3,2)	(1,3,2)	1	(1,2)	(2,3)	(1,3)	(1,2,3)

Notes: The operation goes from right to left. For example, the operation is $(1,2,3)(1,3) = (2,3)$. In this case $(1,3)$ done first and then $(1,2,3)$.

S_3 is a non-abelian group of order 6.

Example 2.1.13

Let n be a positive integer.

Then define $U(n) = \{a \in \mathbb{Z}_+ | \gcd(a,n) = 1\}$. Then $(U(n), \cdot \mod n)$ is an abelian group. $U(n)$ is a unitary group of order $|\phi(n)|$.

2.1.1 Summary:

Examples of Sets with Binary Operation $(G, *)$ have associative property, identity, and an inverse.			
Examples	↙	↘	**Examples**
S_3, Q_8	Finite Group	Infinite Group	
	↓	↓	
$(\{e\}, *)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_p, \cdot)$, $(\mathbb{Z}_2 \times \mathbb{Z}_2, \bigoplus)$, $U(n)$	Abelian (commutative)	Abelian (commutative)	$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $SL_n(\mathbb{R}) = \{M_n(\mathbb{R}) \mid \det(M_n(\mathbb{R}) = 1\}$, $GL_n(\mathbb{R}) = \{M_n(\mathbb{R}) \mid \det(M_n(\mathbb{R}) \neq 0\}$, $(\mathbb{Q}^*, \bullet)$, ….

Note

When referring to a group, we will denote $(G, *)$ as G and represent the operation as ab instead of $a * b$ for simplicity and clarity.

This page titled 2.1: Introduction to Group is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

- **4.4: Transformations** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.

2.2: Properties of Group Elements

Theorem 2.2.1

Let $(G,*)$ be a group. Then

1. The identity is unique,
2. For each $a \in G$, one and only one inverse exists.
3. For each $a \in G,\ (a^{-1})^{-1} = a$.
4. $(a*b)^{-1} = b^{-1} * a^{-1}, \forall a, b \in G.$

Note if G is abelian,$(a*b)^{-1} = b^{-1} * a^{-1} = a^{-1} * b^{-1}, \forall a, b \in G.$

5. If $xy = xz, \forall x, y, z \in G$, then $y = z$. (Left cancellation)
6. If $yx = zx, \forall x, y, z \in G$, then $y = z$. (Right cancellation)

Answer

Proof:

Let $(G,*)$ be a group.

1. We shall show that identity is unique.

Assume that G has two identity elements, e_1 and e_2.

Thus $a * e_1 = e_1 * a = a$ and $a * e_2 = e_2 * a = a$, $\forall a \in G$.

We will show that $e_1 = e_2$.

Consider $e_1 * e_2 = e_2 * e_1 = e_1$ and $e_2 * e_1 = e_1 * e_2 = e_2$.

Thus since $e_1 = e_2$, the identity is unique.□

2. We shall show that for each $a \in G$, one and only one inverse exists.

Let $a \in G$.

Assume that a has two inverses, b and c.

Then $a * b = b * a = e$ and $a * c = c * a = e$.

We shall show that $b = c$.

Consider $b = b * e$

$= b * (a * c)$

$= (b * a) * c$

$= e * c$

$= c.$

Thus $b = c$ and for each $a \in G$, there exists one and only one inverse.

3. We shall show that for each $a \in G,\ (a^{-1})^{-1} = a$.

Let $a \in G$. Then $a * a^{-1} = a^{-1} * a = e$.

Thus $(a^{-1})^{-1} = b^{-1} = a$.

Assume that G has two identity elements, e_1 and e_2.

Thus $a * e_1 = e_1 * a = a$ and $a * e_2 = e_2 * a = a$, $\forall a \in G$.

We will show that $e_1 = e_2$.

Consider $e_1 * e_2 = e_2 * e_1 = e_1$ and $e_2 * e_1 = e_1 * e_2 = e_2$.

Thus since $e_1 = e_2$, the identity is unique.□

4.

Let $a, b \in G$.

Then $a * b \in G$, $a^{-1} \in G$, $b^{-1} \in G$ and $a * b \in G$.

Consider $(b^{-1} * a^{-1})(a * b) = b^{-1} * (a^{-1}a) * b)$

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

$= b^{-1} * b$

$= e$.

And consider $(a * b)(b^{-1} * a^{-1}) = a * (b^{-1} * b) * a^{-1}$

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

$= a^{-1} * a$

$= e$.

Since $(b^{-1} * a^{-1})(a * b) = e = (a * b)(b^{-1} * a^{-1})$, then $(a * b)^{-1} = b^{-1} * a^{-1}, \forall a, b \in G$.□

5.

Let $x, y, z \in G$ s.t. $xy = xz$.

Note: $x^{-1} \in G$ since G is a group.

Thus $x^{-1}(xy) = x^{-1}(xz)$

Thus $(x^{-1}x)y = (x^{-1}x)z$ since associative.

Thus $ey = ez$ and $y = z$.□

6.

Let $x, y, z \in G$ s.t. $y * x = z * x$.

Note: $x^{-1} \in G$ since G is a group.

Thus $(y * x) * x^{-1} = (z * x) * x^{-1}$

Thus $y * (x^{-1} * x) = z * (x^{-1} * x)$ since associative.

Thus $y * e = z * e$ and $y = z$.□

Definition:

Let G be a group. If $g \in G$, then define $g^0 = e$ and $g^{n+1} = gg^n$ for $n \in \mathbb{N}$.) $Also, define \backslash (g^{-n} = (g^n)^{-1}$, for $n \geq 2$.

Theorem 2.2.2

Let G be a group.

Let $g, h \in G$ and $m, n \in \mathbb{N}$.

Then

1. $g^m * g^n = g^{m+n}$ where $g^m = g * \cdots * g$. Note there would be m g's.

2. $(g^m)^n = g^{mn}$.

3. $(gh)^{-m} = (h^{-1}g^{-1})^m$.

Note

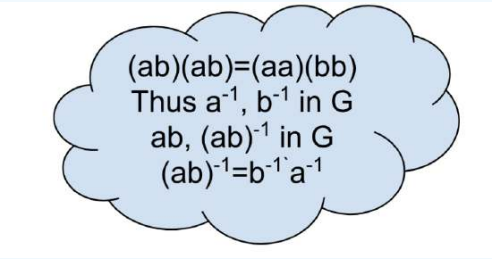
With the addition operation $g^m = mg$.

Example 2.2.1

Let G be a group and suppose that $(ab)^2 = a^2b^2$ for all a and b in G. Prove that G is an abelian group.

Solution

Let G be a group.



Let $(ab)^2 = a^2b^2,\ \forall a, b \in G$.

We shall show that G is abelian.

Let $a, b \in G$.

We shall show that $ab = ba$.

Note that $(a \star b) \star (a \star b) = (a \star a) \star (b \star b)$.

Consider that $a^{-1} \star (a \star b) \star (a \star b) \star b^{-1} = a^{-1} \star (a \star a) \star (b \star b) \star b^{-1}$.

Then $(a^{-1} \star a) \star b \star a \star (b \star b^{-1}) = (a^{-1} \star a) \star a \star b \star (b \star b^{-1})$.

Thus $e \star b \star a \star e = e \star a \star b \star e$.

Thus $b \star a = a \star b$.□

Note: Operator * included for students.

This page titled 2.2: Properties of Group Elements is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

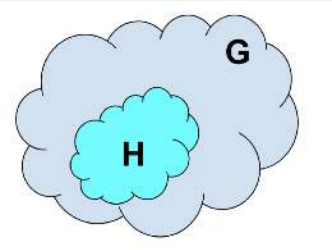
2.3: Subgroups

Subgroups are non-empty subsets of a group that are themselves groups. In this section, we will explore how to define and characterize subgroups.

Definition: Subgroup

Let G be a group. Let H is a non empty subset of G and $(H, *)$ is a group, then H is a subgroup of G. We write this as $H \leq G$.

Trivial subgroups of G are $\{e\}$ and G (the group itself).



Note

To ensure a set is a group, we need to check for the following five conditions:

1. Non-empty set,
2. Closure,
3. Associativity,
4. Identity, and
5. inverse.

The following theorem allows us to check three conditions (rather than 5) to ensure a subset is a subgroup.

Example 2.3.1

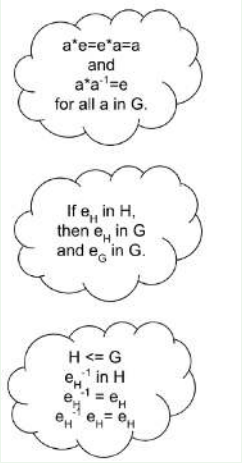
1. The trivial subgroups of a group G are $\{e\}$ and G.
2. $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$. In fact $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ are subgroups of $\mathbb{R}$ under addition.
3. But $(\mathbb{Q}^*, \cdot)$ is not a subgroup of $(\mathbb{R}, +)$. (why?)

Theorem 2.3.1

Let $(G, *)$ be a group then $H \subseteq G$ is a subgroup if and only if

The following conditions are satisfied:

1. The identity $e \in G$ is in H.
2. If $h_1, h_2 \in H$, then $h_1 * h_2 \in H$.
3. If $h \in H$ then $h^{-1} \in H$.



Proof

Assume that $H \subseteq G$.

We shall show that $e_H = e_G$, where e_H is the identity of H and e_H is the identity of G.

Thus, it is clear that $H \leq G$.□

- 1. From (2), we have shown $h_1 * h_2 \in H, \forall h_1, h_2 \in H$.
  2. From (1), we have shown the identity.
  3. From (3), we have shown the inverses exist.
  4. Every element of $h_1, h_2, h_3 \in G$ therefore associativity applies because H inherits it from G by definition.

- Conversely, assume that $H \subseteq G$ satisfies 1, 2, and 3 shown in Theorem 1.

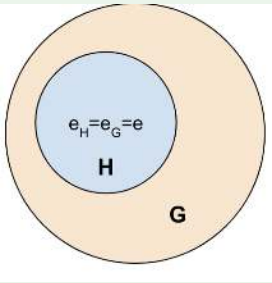
  From (1), we have shown that H is a non-empty set - it has at least an identity.

  Since e_G is the identity of G and $e_H \in G$, $e_G e_H = e_H e_G = e_H$.

  Further, $e_H \in H, e_H^{-1} = e_H \in H$.

  Since $e_H, e_H^{-1} \in G$, $e_H e_H^{-1} = e_G$, but $e_H e_H^{-1} = e_H$.

  Hence $e_G = e_H$.□



  Note: all subgroups of a group have a common element - the identity e. They could have more common elements. Since H is a subset of G, e_H is in H by default.

  2. We shall show that, if $h_1, h_2 \in H$, then $h_1 * h_2 \in H$.

  Let $h_1, h_2 \in H$.

  Since $(H, *)$ is a group, $h_1 * h_2 \in H$.□

  Note a group is closed by definition.

  3. We shall show that,if $h \in H$ then $h^{-1} \in H$.

  Since $(H, *)$ is a group, $h^{-1} \in H$.□

  Note each element in a group has an inverse by definition.

  $H \leq G$ iff:

  $H \neq \{\}$.

  $(H, *)$ is a group. Need to check:

  1. ,$h_1 * h_2 \in H, \forall h_1, h_2 \in H$
  2. $e \in H$, where $e \in G$,
  3. $h^{-1} \in H, \forall\ h \in H$,
  4. $h_1(h_2 h_3) = (h_1 h_2)h_3, \forall\ a, b, c \in H$.

The following theorem allows us to check two conditions (rather than 5) to ensure a subset is a subgroup.

Theorem 2.3.2

Let $(G, *)$ be a group.

Then $H(\subseteq G)$ is a subgroup of G iff the following conditions are satisfied:

1. $e_G \in H$, and
2. $g * h^{-1} \in H, \forall\ g, h \in H$.

Proof:

Assume that $H \leq G$.

Assume that $H \subseteq G$.

Since $e * h_2 \in H, e * h_2^{-1} \in H$.

Further, $eh_2^{-1} = h_2^{-1} \in H$.

Since $h_1 * h_2 \in H,\ h_1 * (h_2^{-1})^{-1} \in H$.

Therefore $h_1 * h_2 \in H$. □

It has an identity since $H \neq \{\}$.

See proof of (a) above

Associativity comes because $h_1, h_2, h_3 \in H$.

1. Let $h_1, h_2 \in H$.

Conversely, assume that $H \subseteq G$ satisfies (1) and (2) of Theorem 2.

We shall show $H \leq G$.

$H \neq \{\}$. Since we have a group, we have at least an identity.

$h_1 * h_2 \in H, \forall h_1, h_2 \in H$,

$e \in H$, where $e \in G$,

$h^{-1} \in H, \forall\ h \in H$,

$h_1(h_2h_3) = (h_1h_2)h_3, \forall\ a, b, c \in H$.

We shall show that $g * h^{-1} \in H, \forall\ g, h \in H$.

Then $h^{-1} \in H$ because $H \subseteq G$.

Since $g, h^{-1} \in H$, $gh^{-1} \in H$,

Hence the result.□

$H \leq G$ iff:

$H \neq \{\}$.

$(H, *)$ is a group. Need to check:

We shall show that $e_H = e_G$, where e_H is the identity of H and e_H is the identity of G.

Since e_G is the identity of G and $e_H \in G$, $e_Ge_H = e_He_G = e_H$.

Further, $e_H \in H, e_H^{-1} = e_H \in H$.

Since $e_H, e_H^{-1} \in G$, $e_He_H^{-1} = e_G$, but $e_He_H^{-1} = e_H$.

Hence $e_G = e_H$.□

Let $g, h \in H$.

Example 2.3.2

Consider $(\mathbb{R}^*, \bullet)$. Decide if the following sets form subgroups of $\mathbb{R}^*$.

1. $H = \{x \in \mathbb{R}^* | x = 1$ or x is irrational $\}$.

No.

Counter example:

Consider $\sqrt{2} \in H$.

Further $\sqrt{2} \bullet \sqrt{2} = 2$ but $2 \notin H$

Therefore since there is no closure, $H \not\leq \mathbb{R}^*$.□

2. $K = \{x \in \mathbb{R}^* | x \geq 1\}$.

No.

Counter example:

Consider $2 \in K$.

Note that $2^{-1} = \frac{1}{2}$, but $\frac{1}{2} \notin K$.

Thus the inverse of 2 does not exist.

Since $a^{-1} \nexists \forall a \in K$, $K \not\leq \mathbb{R}^*$.□

Example 2.3.3

Let $G = \left(M_{22}(\mathbb{R}), +\right)$.

Suppose you take this matrix s.t. the trace of the matrix is zero.

Thus $H = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a + d = 0 \right\}$.

Show that $H \leq G$.

Solution:

Note that $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is the identity of G and it is clearly an element of H. Thus condition (1) of Theorem 2 is satisfied.

We will show that $g * h^{-1} \in H, \forall\ g, h^{-1} \in H$.

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, \begin{bmatrix} e & f \\ g & h \end{bmatrix} \in H$.

Then $a + d = 0$ and $e + h = 0$ since the two matrices belong to H.

Consider $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} -e & -f \\ -g & -h \end{bmatrix} = \begin{bmatrix} a-e & b-f \\ c-g & d-h \end{bmatrix}$.

Then $(a - e) + (d - h) = (a + d) - (e + h) = 0 - 0 = 0$.

Hence $\begin{bmatrix} a-e & b-f \\ c-g & d-h \end{bmatrix} \in H$.

Thus $H \leq G$.

Example 2.3.4

Let $GL_2(\mathbb{R}) = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} | a, b, c, d \in \mathbb{R}, \det(A) = ad - bc \neq 0 \right\}$ where $GL_2(\mathbb{R})$ stands for General Linear Group that is a 2×2 matrix and $SL_2(\mathbb{R}) = \left\{ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} | a, b, c, d \in \mathbb{R}, \det(A) = ad - bc = 1 \right\}$, where $SL_2(\mathbb{R})$. Show that $SL_2(\mathbb{R}) \leq GL_2\mathbb{R})$.

Example 2.3.5

Let n be a nonnegative integer, Then show that $n\mathbb{Z} = \{nm | m \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$.

Answer

Add texts here. Do not delete this text first.

Definition: finite group

Let G be a group. If G is finite and $|G| = n$ then we say that the order of $G = n$.

Theorem 2.3.3

Subgroup test for finite groups:

Let $H \subseteq G$.

Then $H \leq G$ iff:

1. $H \neq \{\}$. (non-empty).
2. $a, b \in H$ then $ab \in H$ (closed).

Example 2.3.6

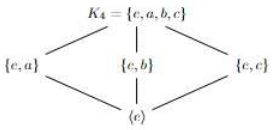
Find all subgroups of **Klein 4** (K_4) **Group** $K_4 = \{e, a, b, c\}$ such that $a^2 = b^2 = c^2 = e$ with the product of any two distinct non-identity elements is the third: $ab = c$, $ac = b$, and $bc = a$.

Solution

Since K_4 is a finite Group, $H_1 = \{e, a\}, H_2 = \{e, b\}$ and $H_3 = \{e, c\}$ are subgroups of K_4. Any subgroup of K_4 with more than 3 elements must contain two distinct non-identity elements. Therefore it must contain the third. Hence $\{e\}, H_1 = \{e, a\}, H_2 = \{e, b\}$ and $H_3 = \{e, c\}, K_4$ are subgroups of K_4.

2.3.1 Lattice Diagram of all subgroups

Example 2.3.7: Lattice diagram of subgroups of K_4



2.3.2 Special subgroups

2.3.2.1 **Centralizer of** an element

Definition: Centralizer of an element

Let G be a group. For any $a \in G$, the **Centralizer of** a **in the group** G, $C(a) = \{g \in G | ag = ga\}$.

Theorem 2.3.4

Let G be a group. For any $a \in G$, the **Centralizer of** a **in the group** G, $C(a) = \{g \in G | ag = ga\}$. Then $C(a) \leq G$.

Proof

If $C(a) = \{g \in G | ag = ga\} = G$, then we are done. Otherwise, let $x_1, x_2 \in C(a)$.

We will show that $x_1 x_2^{-1} \in C(a)$ and $e_G \in C(a)$.

Consider

$$\begin{aligned} ax_1 &= x_1 a \\ ax_1 x_2^{-1} &= x_1 a x_2^{-1} \\ ax_1 x_2^{-1} &= x_1 (a x_2^{-1}) \\ ax_1 x_2^{-1} &= x_1 (x_2^{-1} a) \\ ax_1 x_2^{-1} &= x_1 x_2^{-1} a \end{aligned}$$

, $x_1, x_2^{-1} \in C(a)$.

Since $x_2, x_2^{-1} \in C(a)$, $x_2 x_2^{-1} = e$, where e is the identity element, e in $C(a)$.

Since $x_1 x_2^{-1}, e \in C(a)$, $C(a) \leq G$.□

Example 2.3.8

Let $G = GL(2, \mathbb{R})$. Then find

1. $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right)$.
2. $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right)$.

Solution:

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$, Then $a, b, c, d \in \mathbb{R}$, and $ad - bc \neq 0$.

Consider $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right)$ means that $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$.

Thus $\begin{bmatrix} a+c & b+d \\ a & b \end{bmatrix} = \begin{bmatrix} a+b & a \\ c+d & c \end{bmatrix}$.

Thus $a+b=a+c$, $a=b+d$, $c+d=a$ and $c=b$.

Thus $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{ A = \begin{bmatrix} a & b \\ b & a-b \end{bmatrix} \middle| a, b \in \mathbb{R}, \det(A) \neq 0 \right\}$.

2. $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$, Then $a, b, c, d \in \mathbb{R}$, and $ad - bc \neq 0$.

Consider $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$ means that $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Thus $\begin{bmatrix} c & d \\ a & b \end{bmatrix} = \begin{bmatrix} b & a \\ d & c \end{bmatrix}$.

Thus $b = c$ and $d = a$.

Thus $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{ B = \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| a, b \in \mathbb{R}, \det(B) \neq 0 \right\}$.

2.3.2.2 Center of a group

Definition: Center

Let G be a group. Then the center of G is defined as, $Z(G) = \{x \in G | gx = xg \forall\ g \in G\}$.

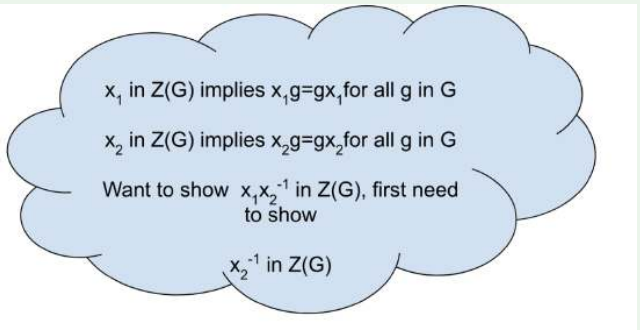
Theorem 2.3.4

Let $(G, *)$ be a group then $Z(G)$ is a subgroup of G.

Proof:

Let G be a group and $g \in G$.

We will show that $Z(G) = \{x \in G | gx = xg\ \forall g \in G\}$.



Let e be the identity of G.

We will show that $e \in Z(G)$.

Since $eg = ge\ \forall g \in G$, $e \in Z(G)$.

Let $x_1, x_2 \in Z(G)$.

We shall show that $x_1 x_2^{-1} \in Z(G)$.

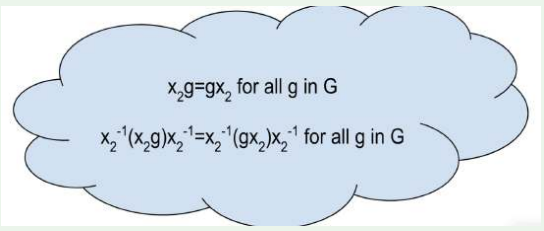
Consider that $x_2^{-1} g = g x_2^{-1}$.

Further $(x_1 x_2^{-1})g = x_1 g x_2^{-1}$.

$= (x_1 g) x_2^{-1}$

$= (g x_1) x_2^{-1}$

$= g(x_1 x_2^{-1})$.□



https://math.libretexts.org/@go/page/131257

Note

Note that if G is abelian, $Z(G) = G$.

Example 2.3.9

Let $G = GL(2, \mathbb{R})$. Then find $\mathbb{Z}(G)$.

Solution:

$\mathbb{Z}(G) = \{g \in G | gx = xg, \forall x \in G\}$.

Let $[a \quad bc \quad d] \in G$, Then $a, b, c, d \in \mathbb{R}$, and $ad - bc \neq 0$.

We have shown $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{ \begin{bmatrix} a & b \\ b & a-b \end{bmatrix} \middle| a, b \in \mathbb{R}, \det \neq 0 \right\}$ and $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = \left\{ [a \quad bb \quad a] \middle| a, b \in \mathbb{R}, \det \neq 0 \right\}$, $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in G$.

Thus for $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ to be in $\mathbb{Z}(G)$, $\begin{bmatrix} a & b \\ b & a-b \end{bmatrix} = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$.

Thus since $a - b = a$, $b = 0$.

Thus, $\mathbb{Z}(G) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \middle| a \in \mathbb{R}, a \neq 0 \right\}$.

Example 2.3.10

Prove that for each element $a \in G$, where G is a group, that $C(a) = C(a^{-1})$.

Proof:

Let $x_1 \in C(a)$ s.t. $ax_1 = x_1a$.

We will show that $x_1a^{-1} = a^{-1}x_1$.

Consider that $a^{-1}ax_1 = a^{-1}x_1a$

$ex_1 = a^{-1}x_1a$

$x_1 = a^{-1}x_1a$

$x_1a^{-1} = a^{-1}x_1aa^{-1}$

$x_1a^{-1} = a^{-1}x_1e$

$x_1a^{-1} = a^{-1}x_1$.

Thus, $x_1 \in C(a^{-1})$.

Hence $C(a^{-1}) \subseteq C(a)$.

Let $x_2 \in C(a^{-1})$ s.t. $a^{-1}x_2 = x_2a^{1}$.

Consider that $aa^{-1}x_2 = ax_2a^{-1}$

$ex_2 = ax_2a^{-1}$

$x_2 = ax_2a^{-1}$

$x_2a = ax_2a^{-1}a$

$x_2a = ax_2e$

$x_2a = ax_2$.

Thus, $x_2 \in C(a)$.

Hence $C(a) \subseteq C(a^{-1})$.
Since $C(a^{-1}) \subseteq C(a)$ and $C(a) \subseteq C(a^{-1})$, $C(a) = C(a^{-1})$.□

2.3.2.3 Centralizer

Definition: Centralizer

Let G be a group and H be a subgroup of G then the **Centralizer of H in G is** $C(H) = \{g \in G | gh = hg \ \forall \ h \in H\}$.

Note that if $H = \{e\}$ then $C(H) = G$.

Theorem 2.3.5

Let G be a group and H be a subgroup of G then the **Centralizer of H in G is** $C(H) = \{g \in G | gh = hg \ \forall \ h \in H\}$ is a subgroup of G.

Proof:

Let G be a group and H be a subgroup of G. We will show that $C(H)$ is a subgroup of G.

Let e be the identity element of G, then $e \in C(H)$.

Let $g_1, g_2 \in C(H)$.

We will show that $g_1 g_2^{-1} h = h g_1 g_2^{-1}$.

Consider that $g_1 h = h g_1$, $g_2 h = h g_2$, $\forall h \in H$.

Since $g_1 h = h g_1$,

$g_1 h g_2^{-1} = h g_1 g_2^{-1}$

$g_1 g_2^{-1} h = h g_1 g_2^{-1}$.

Thus $g_1 g_2^{-1} \in C(H)$

Hence $C(H) \leq G$.

2.3.2.3.1 Conjugacy classes of a group G

Two elements x, y in a group G are conjugate if $y = gxg^{-1}$ for some $g \in G$. This is an equivalence relation of G.

Conjugacy classes of G are subsets of G in which elements are conjugate to each other. That is, $[x] = \{gxg^{-1} | g \in G\}$, $x \in G$.

2.3.2.4 Normalizer

Let G be a group and H be a subgroup of G. For any $x \in G$, $N(H) = xHx^{-1} = \{xhx^{-1} | h \in H\}$.

This subgroup is called the **Normalizer of H in the group G**.

Definition: Normalizer

Let G be a group and H be a subgroup of G. Then

for any $x \in G, N_x(H) = xHx^{-1} = \{xhx^{-1} | h \in H\}$ Gonjugates of G, and

the **Normalizer of H in the group G,** $N(H) = \{xHx^{-1} | x \in G\}$.

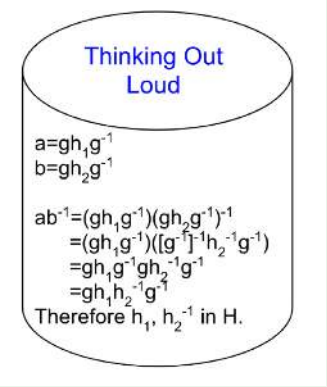
Theorem 2.3.6

Let G be a group and H be a subgroup of G. Then for each $g \in G$, $N_g(H) = gHg^{-1}$ is a subgroup of G. These subgroups are called conjugates of H in G.

Proof:

Let $g \in G$. Let e be the identity of H then $geg^{-1} \in gHg^{-1}$.

Consider $geg^{-1} = (ge)g^{-1} = gg^{-1} = e$. Thus $e \in gHg^{-1}$.



Let $a, b \in gHg^{-1}$.

We will show that $ab^{-1} \in H$.

Consider $a = gh_1g^{-1}$ and $b = gh_2g^{-1}$, $h_1, h_2 \in H$.

Then $ab^{-1} = (gh_1g^{-1})(gh_2g^{-1})^{-1}$

$= (gh_1g^{-1})((g^{-1})^{-1}h_2^{-1}g^{-1})$

$= gh_1g^{-1}gh_2^{-1}g^{-1}$

$= gh_1h_2^{-1}g^{-1} \in gHg^{-1}$.

Thus since $h_1, h_2^{-1} \in N_g(H)$ and $e \in N_g(H)$, $N_g(H)$ is a subgroup of G.□

2.3.2.5

This page titled 2.3: Subgroups is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

2.4: Cyclic groups

2.4.1 Order of group element

Definition: order of an element

Let $(G, \star)$ be a group.

Let $a \in G$, then the order of an element $a \in G$, denoted by $|a|$, be the smallest positive integer n s.t. $a^n = e$. If no such n exists, we say that the order is infinite.

Example 2.4.1

Consider the group $\mathbb{Z}_{10}$ with addition modulo 10. What is the order of its elements?

Consider $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Note that $\{0\}$ is the identity and its order is 1.

element	Order	Calculations
0	$\|\langle 0\rangle\| = 1$	
1	$\|\langle 1\rangle\| = 10$	$1^{10} \equiv 0 \pmod{10}$
2	$\|\langle 2\rangle\| = 5$	$2^1 \equiv 2 \pmod{10}$, $2^2 \equiv 4 \pmod{10}$, $2^3 \equiv 6 \pmod{10}$, $2^4 \equiv 8 \pmod{10}$, and $2^5 \equiv 0 \pmod{10}$.
3	$\|\langle 3\rangle\| = 10$	$3^1 \equiv 3 \pmod{10}$, $3^2 \equiv 6 \pmod{10}$, $3^3 \equiv 9 \pmod{10}$, $3^4 \equiv 2 \pmod{10}$, $3^5 \equiv 5 \pmod{10}$, $3^6 \equiv 8 \pmod{10}$, $3^7 \equiv 1 \pmod{10}$, $3^8 \equiv 4 \pmod{10}$, $3^9 \equiv 7 \pmod{10}$, and $3^{10} \equiv 0 \pmod{10}$.
4	$\|\langle 4\rangle\| = 5$	$4^1 \equiv 4 \pmod{10}$, $4^2 \equiv 8 \pmod{10}$, $4^3 \equiv 2 \pmod{10}$, $4^4 \equiv 6 \pmod{10}$, and $4^5 \equiv 0 \pmod{10}$.
5	$\|\langle 5\rangle\| = 2$	$5^1 \equiv 5 \pmod{10}$, and $5^2 \equiv 0 \pmod{10}$.
6	$\|\langle 6\rangle\| = 5$	$6^1 \equiv 6 \pmod{10}$, $6^2 \equiv 2 \pmod{10}$, $6^3 \equiv 8 \pmod{10}$, $6^4 \equiv 4 \pmod{10}$ and $6^5 \equiv 0 \pmod{10}$.
7	$\|\langle 7\rangle\| = 10$	$7^1 \equiv 7 \pmod{10}$, $7^2 \equiv 4 \pmod{10}$, $7^3 \equiv 1 \pmod{10}$, $7^4 \equiv 8 \pmod{10}$, $7^5 \equiv 5 \pmod{10}$, $7^6 \equiv 2 \pmod{10}$, $7^7 \equiv 9 \pmod{10}$, $7^8 \equiv 6 \pmod{10}$, $7^9 \equiv 3 \pmod{10}$, and $7^{10} \equiv 0 \pmod{10}$.
8	$\|\langle 8\rangle\| = 5$	$8^1 \equiv 8 \pmod{10}$, $8^2 \equiv 6 \pmod{10}$, $8^3 \equiv 4 \pmod{10}$, $8^4 \equiv 2 \pmod{10}$, and $8^5 \equiv 0 \pmod{10}$.
9	$\|\langle 9\rangle\| = 10$	$9^1 \equiv 9 \pmod{10}$, $9^2 \equiv 8 \pmod{10}$, $9^3 \equiv 7 \pmod{10}$, $9^4 \equiv 6 \pmod{10}$, $9^5 \equiv 5 \pmod{10}$, $9^6 \equiv 4 \pmod{10}$, $9^7 \equiv 3 \pmod{10}$, $9^8 \equiv 2 \pmod{10}$, $9^9 \equiv 1 \pmod{10}$, and $9^{10} \equiv 0 \pmod{10}$.

Caution:Order

The order of a group is the number of elements in the group.

The order of an element $a \in G$, denoted by $|a|$, be the smallest positive integer n s.t. $a^n = e$.

Definition:

Let $(G,\star)$ be a group.

Let $X=\{x_1,x_2\ldots,x_n\}$ where $x_1,x_2\ldots,x_n\in G$, then the subset of G generated by X denoted by $\langle X\rangle$ is $\{x_1^{m_1}x_2^{m_2}\cdots x_n^{m_n}\mid m_1,m_2\cdots,m_n\in\mathbb{Z}\}$.

Definition:

Let $(G,\star)$ be a group.

Let $a\in G$, then define the set generated by a denoted by $\langle a\rangle$ is $\{a^m|m\in\mathbb{Z}\}=\{\cdots,a^{-2},a^{-1},e,a,a^2,\cdots\}$.

Note: $a^0=e$.

Theorem 2.4.1

Let $(G,\star)$ be a group.

Let $a\in G$, then $\langle a\rangle$ is the smallest subgroup of G that contains a.

Proof

Let $(G,\star)$ be a group. Let $a\in G$. If $a=e$ then $\langle a\rangle=\{e\}$ is the smallest subgroup of G that contains e.

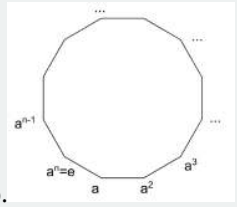
Suppose $a\neq e$. Clearly $e\in\langle a\rangle$. Let $g,h\in\langle a\rangle$. Then $g=a^m$ for some $m\in\mathbb{Z}$ and $h=a^n$ for some $n\in\mathbb{Z}$.

Consider $gh^{-1}=a^m\left(a^n\right)^{-1}=a^ma^{-n}=a^{m-n}$. Since $m-n\in\mathbb{Z}$, $gh^{-1}\in\langle a\rangle$.

Thus, $\langle a\rangle\leq G$. Suppose H is a subgroup of G that contains a. Clearly, $\langle a\rangle\leq H$. □

Note

Let $(G,\star)$ be a group.



Let $a\in G$, then $\langle a\rangle$ is called cyclic subgroup of G.

2.4.2 Cyclic group

Definition: Cyclic group

If $G=\langle a\rangle$ for some $a\in G$, then G is called a cyclic group.

Remember the definition of a unitary group:

Let n be a positive integer. Then define $U(n)=\{a\in\mathbb{Z}_+|\gcd(a,n)=1\}$. Then $(U(n),\cdot\pmod n)$ is an abelian group. $U(n)$ is a unitary group of order $|\phi(n)|$.

Example 2.4.2

$U(15)=\{1,2,4,7,8,11,13,14\}$ and $\star=\cdot\pmod{15}$.

Let $a\in U(15)$ and $b\in U(15)$.

Then $a(x)+15(y)=1$ and $ab(x)+15by=b$ therefore $U(15)$ is closed.

Since $U(15)$ is a finite group, the order of the group is $|U(15)|=8$.

However, $U(15)$ is not a cyclic group.

Proof: (by exhaustion)

Let $a \in U(15)$.

We will show that $\nexists a \in U(15)$, s.t. $|\langle a \rangle| = 8$.

$|\langle 1 \rangle| = 1$ since $1^1 \equiv 1 \pmod{15}$

$|\langle 2 \rangle| = 4$ since $2^4 \equiv 1 \pmod{15}$

$|\langle 4 \rangle| = 2$ since $4^2 \equiv 1 \pmod{15}$

$|\langle 7 \rangle| = 4$ since $7^4 \equiv 1 \pmod{15}$.

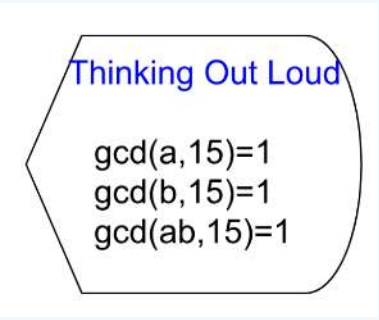
$|\langle 8 \rangle| = 4$ since $8^4 \equiv 1 \pmod{15}$.

$|\langle 11 \rangle| = 2$ since $11^2 \equiv 1 \pmod{15}$.

$|\langle 13 \rangle| = 4$ since $13^4 \equiv 1 \pmod{15}$.

$|\langle 14 \rangle| = 2$ since $14^2 \equiv 1 \pmod{15}$.

Since $\nexists a \in U(15)$, s.t. $|\langle a \rangle| = 8$, $U(15)$ is not a cyclic group.□



Example 2.4.3

Prove that $(U(14), (\cdot \pmod{14}))$ is cyclic.

Proof:

We will show that $\exists a \in U(14)$ s.t. $|\langle a \rangle| = |U(14)|$.

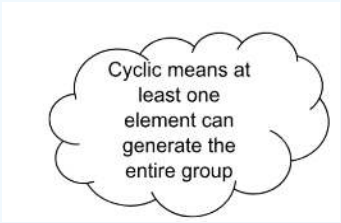
Consider $U(14) = \{1, 3, 5, 9, 11, 13\}$ where $|U(14)| = 6$.

Consider $3^1 \equiv 3 \pmod{14}$, $3^2 \equiv 9 \pmod{14}$, $3^3 \equiv 13 \pmod{14}$, $3^4 \equiv 11 \pmod{14}$, $3^5 \equiv 5 \pmod{14}$ and $3^6 \equiv 1 \pmod{14}$.

$|\langle 3 \rangle| = 6$ since $3^6 \equiv 1 \pmod{14}$.

Thus $|\langle 3 \rangle| = 6$.

Therefore, $U(14)$ is cyclic and 3 is a generator.□



The following is an infinite cyclic group. Any infinite cyclic group is isomorphic to this group.

Example 2.4.4

Is $(\mathbb{Z}, +)$ cyclic group? If so, what are the possible generators?

Yes, $(\mathbb{Z}, +)$ is a cyclic group that is generated by ± 1.

Proof of being a cyclic group:

Since the group generated by 1 contains 1, the identity 0, and the inverse of $1, (-1)$, as well as all multiples of 1 and (-1), $(\mathbb{Z}, +)$ is cyclic.

Possible Generators:

Note 1^n is $1+1+\cdots+1$ with n terms when $n\rangle 0$ and $(-1)+(-1)+\cdots+(-1)$ with n terms when n is $\langle 0$.

We shall show $\mathbb{Z}=\langle 1\rangle=\langle -1\rangle$.

Consider that 1^n means $1+1+\cdots+1$ with n terms and that 1^{-n} means $+(-1)+(-1)+\cdots+(-1)$ with n terms.

It should be clear that 1^n will generate $\mathbb{Z}_+$ and that 1^{-n} will generate $\mathbb{Z}_-$. Note that 1^0 is interpreted as $0\cdot 1=0$.

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

Thus $\langle 1\rangle$ is a generator of $(\mathbb{Z},+)$.

Similarly, we will show that $\langle -1\rangle$ is a generator of $(\mathbb{Z},+)$.

Consider that $(-1)^n$ means $+(-1)+(-1)+\cdots+(-1)$ with n terms and that 1^{-n} means $1+1+\cdots+1$ with n terms.

It should be clear that 1^n will generate $\mathbb{Z}_-$ and that 1^{-n} will generate $\mathbb{Z}_+$. $\langle -1\rangle=\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$.

Thus the generators of $(\mathbb{Z},+)$ are $\langle 1\rangle$ and $\langle -1\rangle$.

2.4.3 Properties:

Theorem 2.4.2

Cyclic groups are abelian.

Proof:

Let $(G,\star)$ be a group.

If G is cyclic, then G is abelian.

Assume that G is cyclic.

Then $G=\langle g\rangle$ for some $g\in G$.

Let $a,b\in G$.

We will show $ab=ba$.

Then $a=g^m$ and $b=g^n$, $m,n\in\mathbb{Z}$.

Consider

$$\begin{aligned} ab &= g^m g^n \\ &= g^{m+n} \\ &= g^{n+m} \\ &= g^n g^m \\ &= ba. \end{aligned}$$

Hence, G is abelian.□

Note

The converse is not true. Specifically, if a group is abelian, it is not necessarily cyclic. A counterexample is $(U(15),\bullet)$ since it is abelian but not cyclic.

Theorem 2.4.3

Every subgroup of a cyclic group will be cyclic.

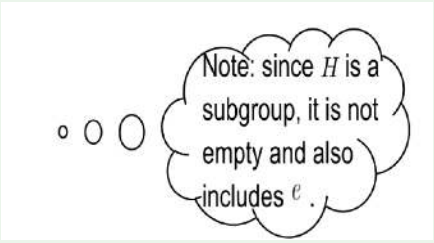
Let $(G,\star)$ be a cyclic group. If $H\leq G$, then H is a cyclic group.

Proof

Let $G = \langle g \rangle,\ g \in G$.

We will show $H = \langle g^k \rangle$ for some $k \in \mathbb{Z}$.

There are two cases to consider.



Case 1: $H = \{e\}$

Let $H = \{e\}$, then we are done since $e \star e = e$ thus $|H| = |\langle e \rangle| = 1$.

Case 2: $H \neq \{e\}$

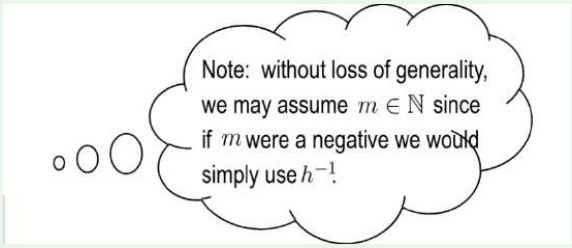
Let $H \neq \{e\}$.

Thus $\exists h \in H$ s.t. $h \neq e$.

Since $h \in H$, $h \in G$.

Hence $h = g^m$ for some $m \in \mathbb{Z}$.

Without loss of generality, we may assume $m \in \mathbb{N}$.



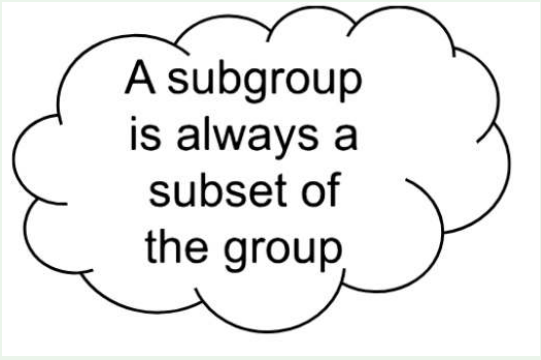
Define $S = \{n \in \mathbb{N} | g^n \in H\} \subseteq \mathbb{N}$.

Since $S(\neq \{\})$ by the well ordering principle S has a smallest element k.

We shall show that $H = \langle g^k \rangle$.

Since $g^k \in H$, $\langle g^k \rangle \leq H$.

Let $h \in H$.



We shall show that $h \in \langle g^k \rangle$.

Since $h \in H$, $h = g^m, m \in \mathbb{Z}$.

Since $k, m \in \mathbb{Z}$, by the division algorithm, there exists q, r s.t. $m = qk + r,\ 0 \leq r < k$.

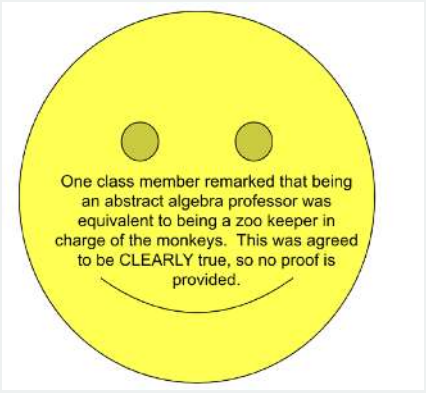
Then $g^m = g^{qk} g^r$ and $g^{m-qk} = g^r$.

Since $g^m, g^{qk} \in H$, then $g^r \in H$.

Since k is the smallest, $r = 0$. (I think this is because $g^0 = e$)

Therefore $g^m = (g^k)^q \in \langle g^k \rangle$.

Thus $H \leq \langle g^k \rangle$.□



Note

The Converse is not true. Every sub-group of the Klein 4-group is cyclic, but not the group.

Corollary 2.4.4

Subgroups of $(\mathbb{Z}, +)$ are of the form $(n\mathbb{Z}, +)$, $n \in \mathbb{N}$.

Theorem 2.4.5

Let G be a cyclic group s.t. $G = \langle a \rangle$ and $|G| = n$.

Then $a^k = e$ iff $n|k$.

Proof

Let $G = \langle a \rangle$ with $a^n = e$.

$\langle a \rangle = \{e, a, a^2 \ldots, a^{n-1}\}$.

Let $a^k = e,\ k \in \mathbb{Z}$.



Since by the division algorithm, unique integers q and r exist such that $k = nq + r,\ 0 \leq r < n,\ q, r \in \mathbb{Z}$.

Consider $a^r = a^{k-nq}$

$= a^k(a^n)^{-q}$ Note: $a^k = e$ is our assumption & n is the order of group.

$= ee^{-q}$

$= e$.

Hence $r = 0$.



Thus $k = nq$.

Therefore $n|k$.

Conversely, assume that $n|k$.

Then $k = nm, m \in \mathbb{Z}$.

$a^k = a^{nm}$.

$= (a^n)^m$

$= e^m$

$= e$.

Hence the result.□

Example 2.4.6

Consider the group $\mathbb{Z}_{12}$ with addition modulo 12.

1. Is $(\mathbb{Z}_{12}, +mod(12))$ cyclic group? If so, what are the possible generators? How many distinct generators are there? What can you say about the number of generators (hint: Euler totient number) and the possible generators (Hint: Divisors)?

3. Find all subgroups of $\mathbb{Z}_{12}$ generated by each element. What are the orders of them? What can you say about these orders?

Answer

1. Consider $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ with addition modulo 12. Note that $\{0\}$ is the identity and its order is 1.

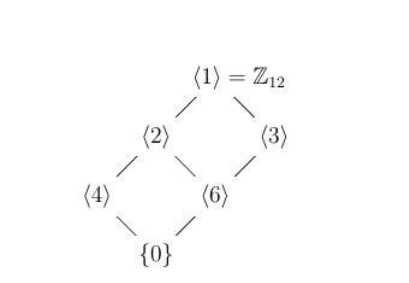
Element	Order	Calculations

0	$\|\langle 0\rangle\| = 1$	
1	$\|\langle 1\rangle\| = 12$	$1^{12} \equiv 0 \pmod{12}$
2	$\|\langle 2\rangle\| = 6$	$2^1 \equiv 2 \pmod{12}$, $2^2 \equiv 4 \pmod{12}$, $2^3 \equiv 6 \pmod{12}$, $2^4 \equiv 8 \pmod{12}$, $2^5 \equiv 10 \pmod{12}$ and $2^6 \equiv 0 \pmod{12}$.
3	$\|\langle 3\rangle\| = 4$	$3^1 \equiv 3 \pmod{12}$, $3^2 \equiv 6 \pmod{12}$, $3^3 \equiv 9 \pmod{12}$, and $3^4 \equiv 0 \pmod{12}$.
4	$\|\langle 4\rangle\| = 3$	$4^1 \equiv 4 \pmod{12}$, $4^2 \equiv 8 \pmod{12}$, and $4^3 \equiv 0 \pmod{12}$.
5	$\|\langle 5\rangle\| = 12$	$5^1 \equiv 5 \pmod{12}$, $5^2 \equiv 10 \pmod{12}$, $5^3 \equiv 3 \pmod{12}$, $5^4 \equiv 8 \pmod{12}$, $5^5 \equiv 1 \pmod{12}$, $5^6 \equiv 6 \pmod{12}$, $5^7 \equiv 11 \pmod{12}$, $5^8 \equiv 4 \pmod{12}$,$5^9 \equiv 9 \pmod{12}$, $5^{10} \equiv 2 \pmod{12}$, $5^{11} \equiv 7 \pmod{12}$, and $5^{12} \equiv 0 \pmod{12}$.
6	$\|\langle 6\rangle\| = 2$	$6^1 \equiv 6 \pmod{12}$, and $6^2 \equiv 2 \pmod{12}$.
7	$\|\langle 7\rangle\| = 12$	$7^1 \equiv 7 \pmod{12}$, $7^2 \equiv 2 \pmod{12}$, $7^3 \equiv 9 \pmod{12}$, $7^4 \equiv 4 \pmod{12}$, $7^5 \equiv 11 \pmod{12}$, $7^6 \equiv 6 \pmod{12}$, $7^7 \equiv 1 \pmod{12}$, $7^8 \equiv 8 \pmod{12}$, $7^9 \equiv 3 \pmod{12}$, $7^{10} \equiv 10 \pmod{12}$, $7^{11} \equiv 5 \pmod{12}$, and $7^{12} \equiv 0 \pmod{12}$.
8	$\|\langle 8\rangle\| = 3$	$8^1 \equiv 8 \pmod{12}$, $8^2 \equiv 4 \pmod{12}$ and $8^3 \equiv 0 \pmod{12}$.
9	$\|\langle 9\rangle\| = 4$	$9^1 \equiv 9 \pmod{12}$, $9^2 \equiv 6 \pmod{12}$, $9^3 \equiv 3 \pmod{12}$ and $9^4 \equiv 0 \pmod{12}$. $9^5 \equiv 5 \pmod{10}$, $9^6 \equiv 4 \pmod{10}$, $9^7 \equiv 3 \pmod{10}$, $9^8 \equiv 2 \pmod{10}$, $9^9 \equiv 1 \pmod{10}$, and $9^{10} \equiv 0 \pmod{10}$.
10	$\|\langle 10\rangle\| = 6$	$10^1 \equiv 10 \pmod{12}$, $10^2 \equiv 8 \pmod{12}$, $10^3 \equiv 6 \pmod{12}$, $10^4 \equiv 4 \pmod{12}$, $10^5 \equiv 2 \pmod{12}$ and $10^6 \equiv 0 \pmod{12}$.
11	$\|\langle 11\rangle\| = 12$	$11^1 \equiv 11 \pmod{12}$, $11^2 \equiv 10 \pmod{12}$, $11^3 \equiv 9 \pmod{12}$, $11^4 \equiv 8 \pmod{12}$, $11^5 \equiv 7 \pmod{12}$, $11^6 \equiv 6 \pmod{12}$, $11^7 \equiv 5 \pmod{12}$, $11^8 \equiv 4 \pmod{12}$, $11^9 \equiv 3 \pmod{12}$, $11^{10} \equiv 2 \pmod{12}$, $11^{11} \equiv 1 \pmod{12}$, and $11^{12} \equiv 0 \pmod{12}$.

From the table, $(\mathbb{Z}_{12}, +mod(12))$ is a cyclic group, the set of all possible generators are $\{1,5,7,11\} = \{a \in \mathbb{Z} | gcd(a,12) = 1, 1 \leq a < 12\}$. Hence, the number of generators is the same as the number of integers relatively prime to $12 = 2^2 3$. That is, the number of generators is the Euler totient number $\phi(12) = (2^2 - 2)(3^1 - 1) = 4$.

2. From the above table, we see that the orders of the subgroups are $1, 2, 3, 4, 6$ and 12, which are all divisors of the order of $\mathbb{Z}_{12}$. Specifically, the order of the subgroup generated by $g \in \mathbb{Z}_{12}$ is $\frac{n}{gcd(g,n)}$.

Note that $12 = 2^2 3$. Then the cyclic subgroups are $\langle 1\rangle, \langle 6\rangle, \langle 4\rangle, \langle 3\rangle, \langle 2\rangle, \langle 0\rangle$ with orders $12, 2, 3, 4, 6$ and 1.



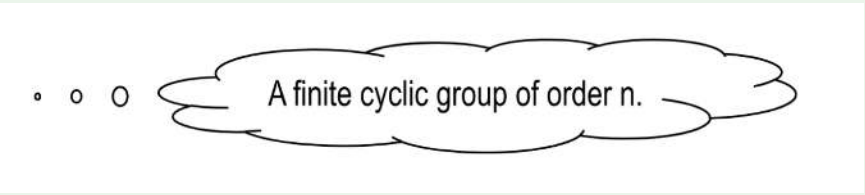
Theorem 2.4.6

$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

Let $G = \langle a \rangle$ be a cyclic group with $|G| = n$.

Let $b \in G$.

If $b = a^k$ then $|b| = \frac{n}{d},\ d = \gcd(k, n)$.



Answer

Let $G = \langle a \rangle$ with $|G| = n$ and $a \in G$.

Let $a^n = e$.

We will show that $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

Let $x \in \langle a^k \rangle$.

Since $\gcd(n, k) = d$ for some $d \in \mathbb{Z}_+$, $d|n$ and $d|k$.

Thus, $k = md, m \in \mathbb{Z}$.

Consider an arbitrary power of a^k, $(a^k)^j \in \langle a^k \rangle$.

$(a^k)^j = (a^{md})^j = (a^d)^{jm} \in \langle a^d \rangle \in \langle a^{\gcd(n,k)} \rangle$.

Let $d = xn + yk,\ n, k \in \mathbb{Z}$.

Using the division algorithm, $(a^{xn+yk})^h = (a^n)^{xh}(a^k)^{yh},\ n, k, h \in \mathbb{Z}$

$= (a^k)^{yh} \in \langle a^k \rangle$.

Thus $a^k = a^d$.

Now we want to show $|a^k| = \frac{n}{d}$.

Consider $(a^k)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e$.

Thus $|a^k| \leq \frac{n}{d}$.

Now consider $(a^d)^{\frac{n}{d}} = (a^n) = e \ \Rightarrow\ |a^d| \leq \frac{n}{d}$.

Now consider $0 \leq i < \frac{n}{d}$.

Thus $di < n$, where d is positive since it is the greatest common denominator.

Thus $(a^d)^i = a^{di} \neq e$ for $di < n$.

Then we can show $|a^d| = \frac{n}{d}$.

Consider $|a^k| = |\langle a^k \rangle| = |\langle a^d \rangle| = |a^d| = \frac{n}{d}$.

Hence $|a^k| = \frac{n}{d}$.

Thinking Out Loud

We are given G=<a> is a cyclic group with |G|=n.
Let b=a^k then |b|=n/d, where d=gcd(n,k).

Usama followed these main steps:

1) Show <a^k>=<a^d>. He took an element in <a^k> and showed it was in <a^d> and then took an element of <a^d> and showed that it was is <a^k>. Lret x in <a^k> then x=a^{kj}, j in **Z**. Now consider $a^{kj}=(a^{dm})^j = (a^d)^{mj}$ in <a^d> since mj in **Z**. Thus <a^k> is a subset of <a^d>. Now we will show that <a^d> is a subset of <a^k>. ….
2) Show $|a^k|$ = n/d. To do that look at $|a^d|$. Since $|a^d|=|a^k|$ from step 1. Let p= $|a^d|$ s.t. p is the smallest satisfying that condition.

Theorem 2.4.7

Let $G = \langle g \rangle$ be a cyclic group with $|g| = n$. Then $G = \langle g^k \rangle$ if and only if $gcd(k, n) = 1$.

Proof

Let $G = \langle g \rangle$ be a cyclic group with $|g| = n$. Then
$g \in G$ and $g^n = e$.

Assume that $G = \langle g^k \rangle$. Then $g = (g^k)^x$ for some $x \in \mathbb{Z}$.

Thus,
$g^{1-kx} = e$.
By Theorem 2.4.5, $n \mid (1 - kx)$. Therefore,
$1 - kx = ny$, for some $y \in \mathbb{Z}$.
Which implies,
$1 = kx + ny$,
hence,
$\gcd(k, n) = 1$.

Conversly, we shall show that if $\gcd(k, n) = 1$, then $G = \langle g^k \rangle$.
Suppose that $\gcd(k, n) = 1$. Then
$kx + ny = 1$, for some $x, y \in \mathbb{Z}$.
By using the properties of powers in a group and $g^n = e$, we get,

$$g^1 = g^{kx+ny} = (g^k)^x (g^n)^y = (g^k)^x. \tag{2.4.1}$$

Hence $g \in \langle g^k \rangle$.

Therefore, we have $G \subseteq \langle g^k \rangle$. Since $\langle g^k \rangle \subseteq G$,
$G = \langle g^k \rangle$.

Theorem 2.4.8:

Let $G = \langle a \rangle$ be a cyclic group with $|G| = n$. Prove the following statements:

a) If $H \leq G$ then $H = \langle a^k \rangle$ for some integer k that divides n.

b) If $k|n$ then $\langle a^{\frac{n}{k}} \rangle$ is the unique subgroup of G of order k.

Proof

a) Let $G = \langle a \rangle$ with $|G| = n$. Assume that $H \leq G$. By Theorem 2.4.3, H is cyclic. Hence $H = \langle a^k \rangle$ for some integer $k \in \mathbf{Z}$. Let $d = gcd(k, n)$. We shall show that $H = \langle a^d \rangle$. Since $d = gcd(k, n)$, $kx + ny = d$, for some $x, y \in \mathbb{Z}$. Consider,

$$a^d = a^{kx+ny} = (a^k)^x (a^n)^y = (a^k)^x. \tag{2.4.2}$$

Thus $a^d \in H$. Therefore $\langle a^d \rangle \subseteq H$.
Since $d|k, k = md$, for some $m \in \mathbb{Z}$. Thus, $a^k = a^{md} = (a^d)^m$. Hence $H \subseteq \langle a^d \rangle$. Thus $H = \langle a^d \rangle$ and $d|n$.

b) Let $G = \langle a \rangle$ with $|G| = n$. Assume that $k|n$. Suppose K be subgroup of G of order k. We shall show that $K = \langle a^{\frac{n}{k}} \rangle$. Since K is a subgroup of G, $K = \langle a^m \rangle$, for some, $m \in \mathbb{Z}$. By part a, $m|n$. Then $(a^m)^{n/m} = e$. We shall show that $\frac{n}{m}$ is the smallest positive integer with this property.

Now, $|K| = \frac{n}{m} = k$. Thus, $m = \frac{n}{k}$. Thus $K = \langle a^{\frac{n}{k}} \rangle$ which is unique.

Theorem 2.4.9

A group of prime order is cyclic.

Proof

Let G be a group s.t. $|G| = p$, where p is a prime number.
Let $g \in G$ s.t. $H = \langle g \rangle$ is a subgroup of G.

Since $p > 1$, $g \neq \{e\}$.

Since H is cyclic, $\exists\ g^k = e$, for some $k \in \mathbb{Z}$.

By the division algorithm, $k = nq + r$ where $0 \leq r < n$.

Hence, $e = g^k = g^{nq+r} = g^{nq}g^r = eg^r = g^r$.

Since the smallest positive integer k such that $g^k = e$ is n, $r = 0$. Thus $n|k$.

Conversely, if $n|k$, then $k = nm$, $m \in \mathbb{Z}$.

Consequently, $g^k = g^{nm} = (g^n)^m = e^m = e$.

Thus, $|\langle g \rangle|$ divides $|G|$.

Consider that the only two divisors of a prime number are the prime number itself and 1.

Since $p < 1$, $|G| = p$.

Since $|G| = p$, G is cyclic.□

Example 2.4.7

List all the cyclic subgroups of $U(30)$.

$U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$ and $|U(30)| = 8$.

k	Calculations	$\lvert k \rvert$
7	$7^1 \equiv 7 \pmod{30}$, $7^2 \equiv 19 \pmod{30}$, $7^3 \equiv 13 \pmod{30}$, $7^4 \equiv 1 \pmod{30}$	4
11	$11^1 \equiv 11 \pmod{30}$, $11^2 \equiv 1 \pmod{30}$	2
13	$13^1 \equiv 13 \pmod{30}$, $13^2 \equiv 19 \pmod{30}$, $13^3 \equiv 7 \pmod{30}$, $13^4 \equiv 1 \pmod{30}$	4
17	$17^1 \equiv 17 \pmod{30}$, $17^2 \equiv 19 \pmod{30}$, $17^3 \equiv 23 \pmod{30}$, $17^4 \equiv 1 \pmod{30}$	4
19	$19^1 \equiv 19 \pmod{30}$, $19^2 \equiv 1 \pmod{30}$	2
23	$23^1 \equiv 23 \pmod{30}$, $23^2 \equiv 19 \pmod{30}$, $23^3 \equiv 17 \pmod{30}$, $23^4 \equiv 1 \pmod{30}$	4
29	$29^1 \equiv 29 \pmod{30}$, $29^2 \equiv 1 \pmod{30}$	2

Since $\nexists a \in U(30)$ s.t. $|\langle a \rangle| = |U(30)| = 8$, $U(30)$ is not a cyclic group.

However the following subgroups of $U(30)$ are cyclic: $\{1, 7, 13, 19\}$, $\{1, 17, 19, 23\}$, $\{1, 11\}$, $\{1, 19\}$, $\{1, 29\}$ and $\{1\}$.

Theorem 2.4.10: Primitive Root Theorem

Let $n \geq 1$. Then $U(n)$ is cyclic iff $n = 1, 2, 4, p^k$ or $2p^k$ where p is an odd prime and $k \geq 1$.

Note

$U(n)$ is not cyclic if n is divisible by two distinct odd primes or by 4 and an odd prime.

Example 2.4.8

$U(1), U(2), U(3), U(4), U(5), U(6), U(7), U(9), U(10), U(11), U(18), U(27)$ are cyclic.

$U(8), U(16), U(20), U(30)$ are not cyclic.

This page titled 2.4: Cyclic groups is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

2E: Exercises

Exercise $2E.1$

Check the following structures for the group properties:

1. $\mathbb{Z}_4$ under addition.
2. $\mathbb{Z}_5^*$ under multiplication.
3. $\mathbb{Z}_8^*$ under multiplication.
4. $\{\pm 1, \pm i\}$ under multiplication.
5. Rotations that map a brick to itself.
6. The four functions $f(x) = x, g(x) = -x, h(x) = \frac{1}{x}, j(x) = \frac{-1}{x}$ under composition.
7. The four matrices $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ under multiplication.

Answer

5. If a, b, c denote rotations about three mutually perpendicular axes, then $a^2 = b^2 = c^2 = e$ the identity rotation. Also $ab = c, ac = b, bc = a$ Thus this group is isomorphic to K_4.

Exercise $2E.2$

Let $H(C) = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \, a, b, c, \in \mathbb{C} \right\}$.

Show that $H(\mathbb{C})$ is a group under matrix multiplication. Demonstrate explicitly that $H(\mathbb{C})$ is always non-abelian.

Exercise $2E.3$

Let $S = \mathbb{R} \backslash \{-1\}$ and define a binary operation $\oplus$ on S by $a \oplus b = a + b + ab$. Prove that $(S, \oplus)$ is an abelian group.

Exercise $2E.4$

Given the groups $\mathbb{R}^*$ and $\mathbb{Z}$, let $G = \mathbb{R}^* \times \mathbb{Z}$. Define a binary operation $\star$ by $(a, m) \star (b, n) = (ab, m + n)$. Show that $(G, \star)$ is a group under this operation.

Exercise $2E.5$

Let G be a group. Show that if $a^2 = e$, for all elements of $a \in G$, then G must be abelian.

Exercise $2E.6$

Let H consists of 2×2 matrices of the form $\begin{bmatrix} \cos(x) & -\sin(x) \\ \sin(x) & \cos(x) \end{bmatrix}$, where $x \in \mathbb{R}$. Prove that H is a subgroup of $SL_2(\mathbb{R})$.

Exercise $2E.7$

Prove or disprove the following statements: Let H and K be subgroups of a group G.

1. $H \cup K$ is a subgroup of G.
2. $H \cap K$ is a subgroup of G.

Exercise $2E.8$

Prove that for each element $a \in G$, where G is a group, the centralizer of a, $C(a)$ is a subgroup of G. Prove that for each element $a \in G$, where G is a group, that $C(a) = C(a^{-1})$.

Exercise $2E.9$

Let $G = GL(2, \mathbb{R})$. Then find

1. $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$.
2. $C\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right)$.
3. $\mathbb{Z}(G)$.

Exercise $2E.10$

Let G be a group. $H = \{g^2 : g \in G\}$.

1. Prove or disprove: If G is abelian then H is a subgroup.
2. Prove or disprove: If H is a subgroup then G is abelian.

Exercise $2E.11$

List the cyclic subgroups of $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

Exercise $2E.12$

Show that $U(20) \neq < k >$ for any k in $U(20)$. [Hence, $U(20)$ is not cyclic.]

Exercise $2E.13$

Decide whether $U(10)$ is cyclic or not. Justify your answer.

Exercise $2E.14$

Is $(\mathbb{Z}, +)$ cyclic group? If so, what are the possible generators?

Exercise $2E.15$

Decide whether the following H is a subgroup of G. Justify your answer.

1. $H = \mathbb{N}, G = \mathbb{Z}$
2. $H = \{1, 3\}, G = \mathbb{Z}_{10}^*$
3. $H = \{1, 3\}, G = \mathbb{Z}_{15}^*$
4. $H = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} |\ 2 \mid (n + m)\}, G = \mathbb{Z} \times \mathbb{Z}$

Exercise $2E.16$

Prove or disprove: If K is a subgroup of H and H is a subgroup of G then K is a subgroup of G.

This page titled 2E: Exercises is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

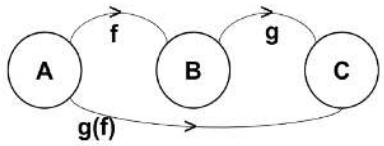
Chapter 3: Permutation Groups

Learning Objectives

- Define and understand the properties of Permutation groups, symmetric groups, alternating groups and dihedral groups
- Solve problems involving the Permutation groups, symmetric groups, alternating groups and dihedral groups

Definition: Permuatation Group

Let X be a non-empty set. Then, the set of all the bijections from X to X with compositions forms a group; this group is called a Permutation group.



This page titled Chapter 3: Permutation Groups is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

3.1: Symmetric Groups

Definition: Symmetric Group

Let $n \in \mathbb{N}$. Let $X = \{1, \dots, n\}$, be a set. Then S_n is the set of all the bijections from X to X (permutations). Note that there are $n!$ permutations. The operation $\star :=$ composition of bijections. Note that it is a **right-to-left** composition.

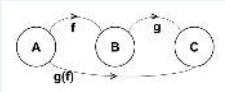


Figure 3.1.1: composition of bijections. (Copyright: Pamini Thangarajah)

S_n with compositions forms a group; this group is called a Symmetric group. S_n is a finite group of order $n!$ and are permutation groups consisting of all possible permutations of n objects.

Identity permutation is denoted as e.

We will denote a permutation by $\sigma = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{bmatrix} \in S_n$

Example 3.1.1

Let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} \in S_5$ and

$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \in S_5$.

Lets find $\gamma \circ \sigma$.

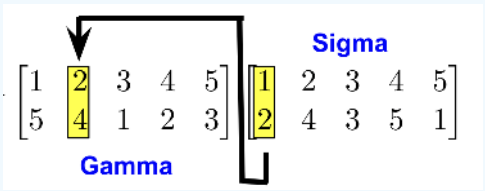


Figure 3.1.2: $\gamma \circ \sigma$. (Copyright; Pamini Thangarajah via Google draw)

Figure 3.1.2 illustrates the process of moving from one function to another. Note the system is closed since it is a bijection. Completing the process, we obtain the following:

Consider $\gamma \circ \sigma = \gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$

Note, if we switch the order of the functions are switched, we obtain: $\sigma\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{bmatrix}$.

Note that $\sigma\gamma \neq \gamma\sigma$. To prove not abelian, we need only show that for at least one element, k, $\sigma\gamma(k) \neq \gamma\sigma(k)$.

Note

The inverse of a permutation σ is the inverse of the function σ, and it is denoted by σ^{-1}.

Thus, $\sigma^{-1}\sigma = \sigma\sigma^{-1} = e$.

Example 3.1.2

Let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} \in S_5$. Then Let $\sigma^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{bmatrix} \in S_5$.

3.1.0.0.1 Cycle Notation

Cycle notation, a simple and straightforward method, is a convenient way to represent permutations in the symmetric group. For example:

Example 3.1.3

Let $\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} = (1, 5, 3)(2, 4)$.

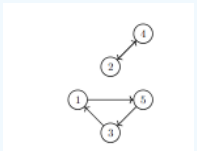


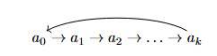
Figure 3.1.3: γ. (Copyright: Pamini Thangarajah)

$(1, 5, 3)$ can be read as 1 goes to 5, 5 goes to 3, and 3 goes back to 1, and is called a cycle of γ of length 3. Then 2 goes to 4, and then 4 goes back to 2, and $(2, 4)$ is called a cycle of γ of length 2.

Note

- $(1, 2, 4, 5)$ means that 1 goes to 2, 2 goes to 4, 4 goes to 5 and 5 goes to 1. Note that 3 is not included, so 3 goes to 3.
- There is no cycle notation in the case of the identity, e, and we use e.
- The cycles are always listed in a logical and clear order-descending order of their smallest element.
- If the permutation fixes an element (i.e., it remains unchanged), it is often omitted from the cycle notation.

Definition: Cycle

A cycle $\gamma = (a_1, \dots, a_k)$ means 

Definition: disjoint cycles

Disjoint cycles mean that the elements involved in one cycle are distinct from those in another.

Two cycles in S_n, $\gamma = (a_1, \dots, a_k)$ and $\sigma = (b_1, \dots, b_l)$ are disjoint if $a_i \neq b_j,\ \forall i, j$.

Note that the length of the cycles does not need to be the same.

Example: $(1,2)$ and $(3,4)$ are disjoint, but $(1,2,3)$ and $(3,4)$ are not disjoint.

Example 3.1.4

Let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 2 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 \end{bmatrix}$

Then, a cycle decomposition of

$\sigma = (1, 12, 8, 10, 4)(2)(3)(5, 11, 7)(6, 9) = (1, 12, 8, 10, 4)(5, 11, 7)(6, 9).$

Note that these are disjoint cycles; therefore, they commute.

Theorem 3.1.1

1. Disjoint cycles are commutative.

Let γ and σ be disjoint cycles, then $\gamma\sigma = \sigma\gamma$.

2. Every permutation of a finite set can be written as a cycle or a product of disjoint cycles.

3.1.0.1 The inverse of a cycle:

Theorem 3.1.2

$(a_1, a_2, \cdots, a_k)^{-1} = (a_k, a_{k-1}, \cdots, a_1)$

Example 3.1.5

$(1,2,3)^{-1} = (3,2,1)$, and $(1,2)^{-1} = (2,1) = (1,2)$.

Let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 2 & 3 & 1 & 11 & 9 & 5 & 10 & 6 & 4 & 7 & 8 \end{bmatrix} = (1, 12, 8, 10, 4)(5, 11, 7)(6, 9).$

In a cycle decomposition, to find the inverse, just reverse the order of the cycles and find the inverse of each cycle. Hence,

$\sigma^{-1} = (6,9)^{-1}(5,11,7)^{-1}(1,12,8,10,4)^{-1} = (9,6)(7,11,5)(4,10,8,12,1)$

Note that disjoint cycles are commutative!

Caution

$(2,3)(1,2) = (1,3,2) = (3,2,1) = (2,1,3)$ Note: 1 goes to 2 first, then to 2 and then gets to 3.

$(1,2)(2,3) = (1,2,3) = (2,3,1) = (3,1,2)$ Note: Since there is no 1 in the inner function, it goes to itself and then goes to 2.

3.1.1 Type of a permutation (cycle structure of a permutation)

The type of a permutation (or cycle structure of a permutation) is the integer partition formed from the cycle lengths in decreasing order. We will denote it by type(σ), where σ is a permutation in S_n.

Example 3.1.6

Let $\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} = (1,5,3)(2,4) \in S_5$.

The type of γ is, type $(\gamma) = \underline{3\,2}$.

Example 3.1.7

Let $\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = (1,4,3,2) \in S_4$.

The type σ is, type $(\sigma) = \underline{4}$.

Note

A partition of a positive integer n is a sum of nonnegative integers $n = k_1 + \cdots + k_s, k_i \in \mathbb{N}$, where the order of the summand is not important. For example:

The partitions of 6 are $6, 5+1, 4+2, 4+1+1, 3+3, 3+2+1, 3+1+1+1, 2+2+2, 2+2+1+1, 2+1+1+1+1, 1+1+1+1+1+1$.

Example 3.1.8

How many permutations in S_6 have type $\underline{321}$?

Type (321) permutation is of the form Double subscripts: use braces to clarify. There are $6!$ ways of filling the blanks. Note that each cycle can be restarted anywhere.

Hence, the number of permutations in S_6 have type (321) is $\frac{6!}{(3)(2)(1)}$.

Example 3.1.9

How many permutations in S_6 have 3 cycles of length 2?

The permutation is of the form Double subscripts: use braces to clarify. There are $6!$ ways of filling the blanks. Since each cycle has two representations matching this format (by restarting at any two places), so divided by 2^3.

The order of the whole cycle can be changed while keeping the pattern. Divide by $3!$ ways to reorder the cycles.

Hence, the number of permutations in S_6 have 3 cycles of length 2 is $\frac{6!}{(2^3)(3!)}$.

Theorem 3.1.3

Suppose the number of cycles of length i is m_i, for $i = 1, \cdots, k$. and $n = m_1 + 2m_2 + \cdots + (k-1)m_{(k-1)} + km_k$.

The number of permutations in S_n of the type $(m_k m_{(k-1)} \cdots m_1)$ is

$$\frac{n!}{1^{m_1}2^{m_2}\cdots k^{m_k} m_1! m_2! \cdots m_k!}.$$

Example 3.1.10

$|S_3| = 3! = 2 \cdot 3 = 6$.

Table 3.1.1: Cycle type for S_3

Cycle type	111	21	3
Number of permutations	$\frac{3!}{1^3 3!} = 1$	$\frac{3!}{1^1 2^1 1!1!} = 3$	$\frac{3!}{3^1 1!1!} = 2$

Notation:

$1 \equiv \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ the identity matrix.

$(1,2) \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Note that 3 points to itself.

$(1,2,3) \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

$(1,3,2) \equiv \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix}$.

Hence, $S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

Table 3.1.2: Cayley table for S_3

	e	(1,2,3)	(1,3)	(1,2)	(2,3)	(1,3,2)
e	e	(1,2,3)	(1,3)	(1,2)	(2,3)	(1,3,2)
(1,2,3)	(1,2,3)	(1,3,2)	(2,3)	(1,3)	(1,2)	e
(1,3)	(1,3)	(1,2)	e	(1,2,3)	(1,3,2)	(2,3)
(1,2)	(1,2)	(2,3)	(1,3,2)	e	(1,2,3)	(1,3)
(2,3)	(2,3)	(1,3)	(1,2,3)	(1,3,2)	e	(1,2)
(1,3,2)	(1,3,2)	e	(1,2)	(2,3)	(1,3)	(1,2,3)

Example 3.1.11

Let's explore S_4. Note S_4 has $4! = 24$ elements.

Table 3.1.3: Cycle type for S_4

Cycle type	1111	211	22	31	4
Number of permutations	$\frac{4!}{1^4 4!} = 1$	$\frac{4!}{1^2 2^1 2!1!} = 6$	$\frac{4!}{2^2 2!} = 3$	$\frac{4!}{1^3 3^1 1!1!} = 8$	$\frac{4!}{4^1 1!} = 6$

Hence,

$$S_4 = \{e, (1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,3), (1,3,2), (2,3,4), (2,4,3), (3,4,1), (3,1,4), (4,1,2), (4,2,1), (1,2,3,4), (1,2,4,3), (1,3,4,2), (1,3,2,4), (1,4,2,3), (1,4,3,2)\}. \tag{3.1.1}$$

Note

Notice that all the elements in S_3 in S_4.

The following theorem proves that S_n are non-Abelian for integer n ≥ 3, which means that the order in which we compose permutations matters.

Theorem 3.1.4

S_n is non-Abelian for all integers n ≥ 3.

Proof

Let $a, b \in S_3$.

We will show that there exists $a, b \in S_n, s.t. ab \neq ba, n \geq 3$.

Note $S_3 = \{e, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$.

Let $a = (1,2)$ and $b = (2,3)$ both elements of S_3.

Consider $ab = (1,2)(1,3) = (1,3,2)$ and $ba = (1,3)(1,2) = (1,2,3)$.

Since $(1,3,2) \neq (1,2,3)$, $ab \neq ba$ $\forall a, b \in S_3$, thus S_3 is non-abelian.

Since $a, b \leq S_n$, $\forall n \geq 3$, S_n in non-abelian for $n \geq 3$.□

Example 3.1.12

Given $\alpha, \beta \in S_4$ with $\alpha\beta = (1,4,3,2)$, $\beta\alpha = (1,2,4,3)$, and $\alpha(1) = 4$, determine α and β.

Solution:

Let $\alpha = (1,4,c,d)$ and $\beta = (w,x,y,z)$.

Since $\alpha(1) = 4$ and $\beta\alpha(1) = 2$, implies $\beta(4) = 2$.

Since $\beta(4) = 2$ and $\alpha\beta(4) = 3$, implies $\alpha(2) = 3$.

Since $\alpha(2) = 3$ and $\beta\alpha(2) = 4$, implies $\beta(3) = 4$.

Since $\beta(3) = 4$ and $\alpha\beta(3) = 2$, implies $\alpha(4) = 2$.

Since $\alpha(4) = 2$ and $\beta\alpha(4) = 3$, implies $\beta(2) = 3$.

Since $\beta(2) = 3$ and $\alpha\beta(2) = 1$, implies $\alpha(3) = 1$.

Since $\alpha(3) = 1$ and $\beta\alpha(3) = 1$, implies $\beta(1) = 1$.

$\alpha = (1,4,2,3)$ and $\beta = (2,3,4)$.

Then $\beta\alpha = (2,3,4)(1,4,2,3) = (2,4,3,1) = (1,2,4,3)$.

And $\alpha\beta = (1,4,2,3)(2,3,4) = (4,3,2,1) = (1,4,3,2)$.

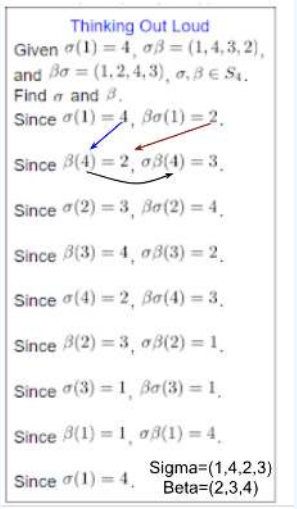


Figure 3.1.4: Thinking out Loud (Copyright: Pamini Thangarajah)

Note that every permutation of a finite set can be written as a cycle or a product of disjoint cycles.

3.1.1.0.1 2 Cycle (Transposition)

Definition: Transposition

(i,j), $i \leq j$, $j \leq n$, $i \neq j$.

$(i,j)^{-1} = (j,i) = (i,j)$.

Example 3.1.1

(1, 3, 2) = (1, 2) (1, 3) 1 goes to 3, 3 goes to itself, then to 1 then to 2.

(1, 2, 3) = (1, 3) (1, 2).

(2, 4, 1, 3, 5) = (2, 5) (2, 3) (2, 1) (2, 4)

Note: Any cycle can be written as a composition of two cycles.

Theorem 3.1.5

A k–cycle $(i_1, i_2 \cdots, i_k)$ can be decomposed into a product of $k-1$ transpositions. That is,

$(i_1, i_2 \cdots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_2)$.

Theorem 3.1.6

Every permutation in S_n can be expressed as a product of 2-cycles (Transpositions). The number of transpositions will either always be even or odd.

If a permutation α can be expressed as a product of an even number of 2-cycles, then every decomposition of α into a product of 2-cycles has an even number of 2-cycles. A similar statement holds for odd.

Permutation parity

Definition: Parity

Let $\sigma \in S_n$. (i.e. a permutation)

Then

(1) σ is an even permutation if σ can be expressed as a product of an even number of two cycles (transpositions).

(2) σ is an odd permutation if σ can be expressed as a product of an odd number of two cycles (transpositions).

Theorem 3.1.7

1. A cycle of even length is odd.

2. A cycle of odd length is even.

Example 3.1.13

1. let's explore S_4. Note S_4 has $4! = 24$ elements.

Consider S_4
$= \{e, (1,2), (1,3), (1,4), (2,3), (2,4), (3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,2,3), (1,3,2), (2,3,4), (2,4,3), (3,4,1), (3,1,4), (4,1,2), (4,2,1), (1,2,3,4), (1,2,4,3), (1,3,4,2), (1,3,2,4), (1,4,2,3), (1,4,3,2)\}$

2. Find the center of S_4.

Since all symmetrical groups, S_n, $n \geq 3$, are non-abelian, the centre of S_4 is trivial, being the identity e, or (1)(2)(3)(4). (what do you think of this proof? Is this a valid argument?)

Alternatively, proof by exhaustion: Having tried all $x \in S_4$, the only $x \in S_4$ that satisfies $xg = gx, \ \forall g \in S_4$ is the identity.

3. Find the cyclic subgroup of S_4 that has an order of 4.

The subgroup of $S_4, C4 = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$, has an order 4 and is generated by $(1,2,3,4)$.

$(1,2,3,4)^2 = (1,3)(2,4)$, $(1,2,3,4)^3 = (1,4,3,2)$, and $(1,2,3,4)^4 = e$.

4. Find a non-cyclic subgroup of S_4 that has order 4.

The 2-2 cycles together will form an order 4 group.

$\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ is a subgroup of S_4 and has order 4. Note the inverse of $(1,2)(3,4)$ is $(4,3)(2,1)$, which is $(1,2)(3,4)$. Since a similar argument can be made for the other 2-2 cycles, the inverses of each element exist. In addition, the set is closed under composition.

Theorem 3.1.8

The center of $S_4, Z(S_4) = \{e\}$.

Proof

Proof by contradiction

Let $\gamma(\neq e) \in Z(S_n)$. We shall find an $\alpha \in S_n$ such that $\gamma\alpha \neq \alpha\gamma$. Since $\gamma(\neq e)$, there exist $l, m \in \{1, 2, 3, \cdots, n\}$ such that $\gamma(l) = m \neq l$. Now we can choose an element $k \in \{1, 2, 3, \cdots, n\}$ such that $k \neq l$ and $k \neq m$. Choose $\alpha = (l, k)$. Then $\gamma\alpha(l) = \gamma(k)$ and $\alpha\gamma(l) = \alpha(m) = m$. Since γ is a bijection and $\gamma(l) = m \neq l$, $\gamma(k) \neq m$. This is a contradiction. Hence, $Z(S_n) = \{e\}$.

3.1.1.0.1

3.1.1.0.1 Order of a permutation

Let $\sigma = (1,2,3)$.

Then $\sigma^2 = (1,2,3)(1,2,3) = (1,3,2) = \sigma^{-1}$.

Further $\sigma^3 = (1,2,3)(1,3,2) = (1)(2)(3) = e$. We shall refer to e as 1.

Thus the order of σ, $|\sigma| = 3$.

Theorem 3.1.9

If $\sigma = (a_1, \ldots, a_k)$, then the $|\sigma| = k$.

Proof

Since $\sigma^k(a_i) = a_i, \forall i = 1, cdots, n, \sigma^=(a_1, \ldots, a_k)^k = e$. We shall show that k the smallest positive integer such that $\sigma^k = e$. Suppose m is a positive integer such that $0 < m < k.)Then\backslash(\sigma^m(a_i)$ $= a_{i+m} \neq a_i \ \forall i = 1, cdots, n).Hence\backslash(k$ the smallest positive integer such that $\sigma^k = e$.

Example 3.1.14

Let $\gamma = (1,2,4)$. Then

$\gamma^2 = (1,2,4)(1,2,4) = (1,4,2)$.

$\gamma^3 = (1,2,4)(1,4,2) = (1)(2)(4) = e$.

Theorem 3.1.10

The order of a permutation of a finite set, written in disjoint cycle form, is the least common multiple of the lengths of the cycles.

Thinking out loud

a,b in **Z**\{0}.

lcm(a,b)=|ab|/gcd(a,b).

Example:

lcm(187,286) =|187*286|/gcd(187,286)
=(187*286)/11
=4862

286 X 17		
	10	7
200	2000	1400
80	800	560
6	60	42
		4862

Example 3.1.15

Find the orders of the 5040 elements of S_7.

Solution

The longest cycle in S_7 is the one that includes all the elements -- 7. We will show cycle lengths as $\underline{7}$. Note the underlining. The possible cycles are shown in the table below. Note that the leading term is the longest cycle in the permutation.

Cycle type	Order	Cycle type	Order	Cycle type	Order
$\underline{7}$	7	$\underline{4}\,\underline{2}\,\underline{1}$	4	$\underline{3}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}$	3
$\underline{6}\,\underline{1}$	6	$\underline{4}\,\underline{1}\,\underline{1}\,\underline{1}$	4	$\underline{2}\,\underline{2}\,\underline{2}\,\underline{1}$	2
$\underline{5}\,\underline{2}$	10	$\underline{3}\,\underline{3}\,\underline{1}$	3	$\underline{2}\,\underline{2}\,\underline{1}\,\underline{1}\,\underline{1}$	2
$\underline{5}\,\underline{1}\,\underline{1}$	5	$\underline{3}\,\underline{2}\,\underline{2}$	6	$\underline{2}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}$	2
$\underline{4}\,\underline{3}$	12	$\underline{3}\,\underline{2}\,\underline{1}\,\underline{1}$	6	$\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}$	1

3.1.2 Conjugacy classes of S_n

Recall:

Two elements x, y in a group G are conjugate if $y = gxg^{-1}$ for some $g \in G$.

Theorem 3.1.11

For $\alpha, \beta \in S_n$, define $\alpha \sim \beta$ if there exists a $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Then $\sim$ is an equivalence relation on S_n.

Proof

Reflexive: Let $\alpha \in S_n$. Then $e \in S_n$ and $e\alpha e^{-1} = \alpha$. Hence $\alpha \sim \alpha$. Thus $\sim$ is reflexive on S_n.

Symmetric: Let $\alpha, \beta \in S_n$ such that $\alpha \sim \beta$. Then there exists a $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Therefore, $\sigma^{-1}\beta\sigma = \alpha$, and $\sigma^{-1} \in S_n$. Hence, $\beta \sim \alpha$. Thus $\sim$ is symmetric on S_n.

Transitive: Let $\alpha, \beta, \gamma \in S_n$ such that $\alpha \sim \beta$ and $\beta \sim \gamma$. Then there exist $\sigma_1, \sigma_2 \in S_n$ such that $\sigma_1\alpha\sigma_1^{-1} = \beta$, and $\sigma_2\beta\sigma_2^{-1} = \gamma$. Consider,

$$\begin{aligned}\gamma &= \sigma_2\beta\sigma_2^{-1} \\ &= \sigma_2\left(\sigma_1\alpha\sigma_1^{-1}\right)\sigma_2^{-1} \\ &= \left(\sigma_2\sigma_1\right)\alpha\left(\sigma_1^{-1}\sigma_2^{-1}\right) \\ &= \left(\sigma_2\sigma_1\right)\alpha\left(\sigma_2\sigma_1\right)^{-1}.\end{aligned}$$

Hence, $\alpha \sim \gamma$. Thus $\sim$ is transitive on S_n.

Since $\sim$ is reflexive, symmetric and transitive, $\sim$ is an equivalence relation on S_n.

The equivalence classes are called conjugacy classes of G, subsets of G in which elements are conjugate to each other.

Theorem 3.1.12

Two permutations in S_n are conjugate if and only if they have the same cycle structure, i.e. they have the same cycle type.

Example 3.1.16

Conjugacy classes of S_3.

Solution

There are three conjugacy classes. Those are $\{(1,2),(2,3),(1,3)\}, \{e\}, \{(1,2,3),(3,2,1)\}$.

This page titled 3.1: Symmetric Groups is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

3.2: Alternating Groups

Definition: Alternating groups

Alternating groups A_n is the set of all even permutations associated with composition. $|A_n| = \frac{n!}{2}$. A_n is a subgroup of the symmetric group S_n.

Example 3.2.1

$A_3 = \{1, (1,2,3), (3,2,1)\}$. A_3 is a cyclic group of order 3.

Theorem 3.2.1

A_n is non abelian for $n \geq 4$.

Proof:

Let $a, b \in A_4$.

We will show that $ab \neq ba,\ \forall a, b \in A_n,\ n \geq 4$.

Note $A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (124), (134), (234), (432), (431), (421), (321)\}$.

Let $a = (1,2)(3,4)$ and $b = (4,1)(4,2)$.

Consider $ab = (1,2)(3,4)(4,1)(4,2) = (1,3,4,2)$.

Further consider, $ba = (4,1)(4,2)(1,2)(3,4) = (1,4,3,2)$.

Since $(1,3,4,2) \neq (1,4,3,2),\ \forall a, b \in A_4$, thus A_4 is non-abelian.

Since a copy of A_4 is a subgroup of $A_n,\ \forall n \geq 4$, A_n is non-abelian for $N \geq 4$.□

Example 3.2.1

Find a cyclic subgroup of A_8 that has order 4.

Consider the subgroup $\{e, (1,2,3,4), (1,3)(2,4), (4,3,2,1)\}$ which is a subgroup of A_8 of order 4.

Then consider $(1,2,3,4)(1,2,3,4) = (1,3)(2,4) \in A_8$.

Further $(1,2,3,4)(1,3)(2,4) = (1,4,3,2) \in A_8$.

Further $(1,2,3,4)(1,4,3,2) = e$.

Thus $\{e, (1,2,3,4), (1,3)(2,4), (4,3,2,1)\}$, a subgroup of A_8 that is order 4 and cyclic.

Example 3.2.2

Find a non-cyclic subgroup of A_8 that has order 4.

Consider $\{e, (1,2), (2,3), (3,4)\}$ which is a subgroup of A_8 of order 4.

Then consider $(1,2)^n$.

There is no n for which $(1,2)^n = (3,4)$ or $(2,3)$.

Similarly, there is no n for which $(2,3)^n = (1,2)$ or $(3,4)$.

Similarly, there is no n for which $(3,4)^n = (1,2)$ or $(2,3)$.

Thus $\{e, (1,2), (2,3), (3,4)\}$ is not cyclic.

Version 2:

Let $G = \{e, i, j, k\}$.

Let $i = (1,2)(3,4)$, $j = (5,6)(7,8)$ and $k = (1,2)(3,4)(5,6)(7,8)$.

Consider $ij = k$, $ik = j$, and $jk = i$.

Thus there is closure in G.

Further, consider $i^{-1} = i$, $j^{-1} = j$, and $k^{-1} = k$.

Thus, inverses exist for all elements of G.

Note there is no n for which $i^n = j$ or k.

Similarly, there is no n for which $j^n = i$ or k.

Similarly, there is no n for which $k^n = j$ or k.

Since there is no $< g >\in G$, G is not cyclic.

Example 3.2.3

Find the conjugacy classes of A_3.

Solution

$\{e\}, \{(1,2,3)\}, \{(3,2,1)\}$.

$[e] = \{\sigma^{-1} e \sigma \mid \sigma \in A_4\} = \{e\}$.

$[(1,2,3)] = \{\sigma^{-1}(1,2,3)\sigma \mid \sigma \in A_4\} = \{e^{-1}(1,2,3)e, (1,2,3)^{-1}(1,2,3)(1,2,3), (3,2,1)^{-1}(1,2,3)(3,2,1)\} = \{(1,2,3)\}$.

$[(3,2,1)] = \{\sigma^{-1}(3,2,1)\sigma \mid \sigma \in A_4\} = \{e^{-1}(3,2,1)e, (1,2,3)^{-1}(3,2,1)(1,2,3), (3,2,1)^{-1}(3,2,1)(3,2,1)\} = \{(3,2,1)\}$.

This page titled 3.2: Alternating Groups is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

3.3: Dihedral Groups (Group of Symmetries)

Dihedral groups are an essential class of abstract algebra groups that arise naturally in geometry and other areas of mathematics.

Definition: Dihedral Groups

Let $n(\geq 2) \in \mathbb{Z}$ Then the **Dihedral group** D_n is defined by

$$D_n =< r, s | s^2 = e, r^n = e, srs = r^{-1} >= \{e, r, r^2, r^3, \cdots, r^{n-1}, s, rs, \cdots, r^{n-1}s\} \tag{3.3.1}$$

and, $|D_n| = 2n$.

Alternatively, for $n(\geq 3) \in \mathbb{Z}$, a dihedral group is a group of symmetries of a regular polygon with n sides. The dihedral group of order $2n$, denoted by D_n, is the group of all possible rotations and reflections of the regular n sided polygon. in this case $r = (1, 2, 3, \cdots, n)$ represents a rotation of $(360/n)$ degrees clockwise about the center of the polygon, and $s = (1, n-1)(2, n-2)(3, n-3)\cdots$ represents the rotation of 180 degrees about a line through a vertex n and the center of the figure. If n is odd, s fixes only one vertex n and if If $n = 2m$ is even, s fixes vertices n and m.

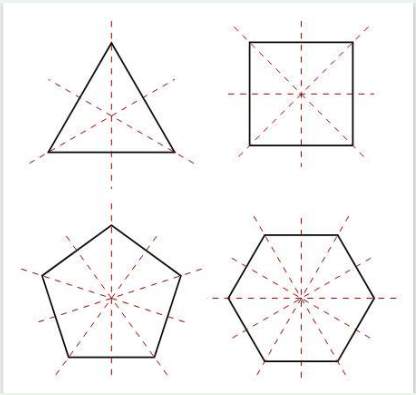


Figure 3.3.1: Reflections of polygons. (Copyright; Tikz Library)

Thus the group D_n consists of $2n$ elements, which can be depicted as follows:

- n rotations, denoted by $R_0, R_{360/n}, R_{(360)(2)/n}\cdots, R_{(n-1)360/n}$, where $R_{i(360)/n}$ represents a rotation of $(360i/n)$ degrees clockwise about the center of the polygon, for $i = 1, \cdots, n$..
- n reflections, denoted by $F_0, F_1, F_2, ..., F_{(n-1)}$, where F_i represents a reflection across a line passing through the center of the polygon and one of its vertices.

All rigid motions on n-gon:

a. To replace the first vertex, we have n choices.

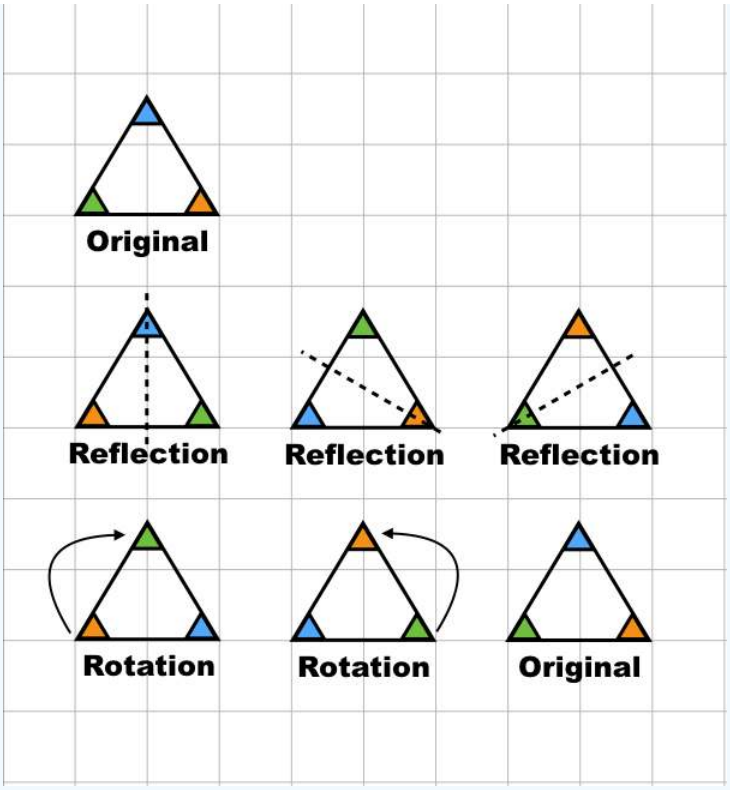
b. the second vertex can be replaced by k^{th} vertex by $k+1$ or $k-1$.

The group operation in D_n, is the composition of symmetries.

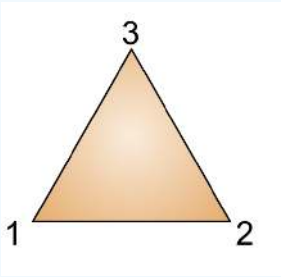
Recall from chapter 2, section 2.1 Example 11

Example 3.3.1

Consider the equilateral triangle below. What rigid motions can we make to it that will result in the triangle occupying the same space? What happens if we combine rigid motions? Keep in mind that "doing nothing" is also a rigid motion.



Symmetries of equilateral triangles:



Let r be a rotation then there are three rotations I, r, r^2. Let s be a reflection, then there are s, rs, r^2s elements. In this case, $r^3 = s^2 = I$ and $sr = r^2s$. Thus $D_3 = \{I, r, r^2, s, rs, r^2s\}$.

Theorem 3.3.1

Dihedral groups D_n are non-abelian, for integers $n \geq 3$.

Proof

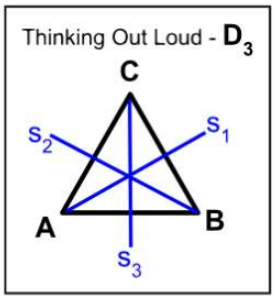
Let $a, b \in D_3$.

We will show that $ab \neq ba, \ \forall a, b \in D_n, n \geq 3$.

$D_3 = \{e, (AB), (AC), (BC), (ABC), (ACB)\}$.

Since D_3 is isomorphic to S_3, $D_3$is non-abelian.

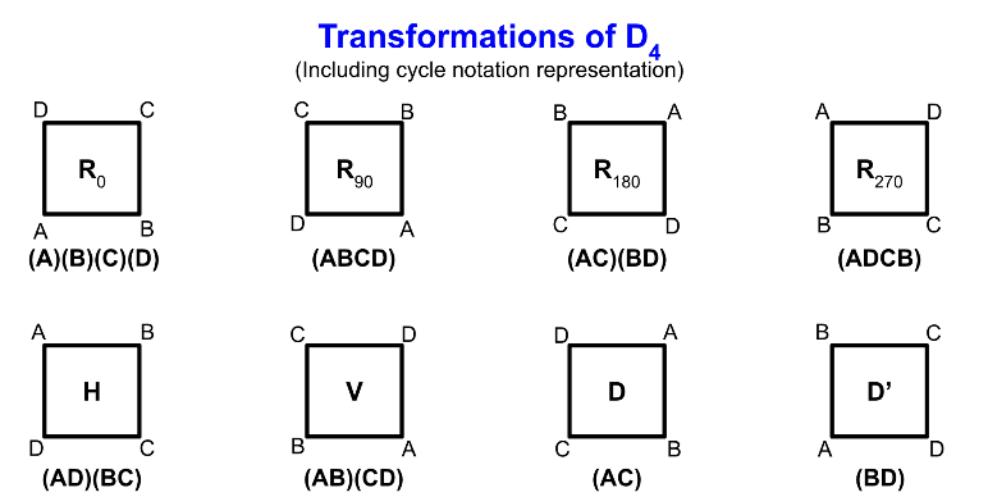
Since $D_3 \leq D_n, \forall\ n \geq 3, D_n$ is non-abelian for $n \geq 3$.



The Dihedral group D_3 is isomorphic to S_3.

Example 3.3.2

Consider the possible rotations and reflections of a 4-sided regular polygon -Square, D_4.



	Cayley Table for D_4							
	R_0	R_{90}	R_{180}	R_{270}	**H**	**V**	**D**	**D'**
R_0	R_0	R_{90}	R_{180}	R_{270}	**H**	**V**	**D**	**D'**
R_{90}	R_{90}	R_{180}	R_{270}	R_0	**D'**	**D**	**H**	**V**
R_{180}	R_{180}	R_{270}	R_0	R_{90}	**V**	**H**	**D'**	**D**
R_{270}	R_{270}	R_0	R_{90}	R_{180}	**D**	**D'**	**V**	**H**
H	**H**	**D**	**V**	**D'**	R_0	R_{180}	R_{90}	R_{270}
V	**V**	**D'**	**H**	**D**	R_{180}	R_0	R_{270}	R_{90}
D	**D**	**V**	**D'**	**H**	R_{270}	R_{90}	R_0	R_{180}
D'	**D'**	**H**	**D**	**V**	R_{90}	R_{270}	R_{180}	R_0

Example 3.3.5

D_5 dihedral group of order 10, is the group of symmetries of a regular pentagon. It is composed of 10 elements, which can be represented as rotations and reflections of the pentagon.

The Cayley table for D_5:

$\circ$	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
e	e	r	r^2	r^3	r^4	s	rs	r^2s	r^3s	r^4s
r	r	r^2	r^3	r^4	e	rs	r^2s	r^3s	r^4s	s
r^2	r^2	r^3	r^4	e	r	r^2s	r^3s	r^4s	s	rs
r^3	r^3	r^4	e	r	r^2	r^3s	r^4s	s	rs	r^2s
r^4	r^4	e	r	r^2	r^3	r^4s	s	rs	r^2s	r^3s
s	s	rs	r^2s	r^3s	r^4s	e	r	r^2	r^3	r^4
rs	rs	r^2s	r^3s	r^4s	s	r	r^2	r^3	r^4	e
r^2s	r^2s	r^3s	r^4s	s	rs	r^2	r^3	r^4	e	r
r^3s	r^3s	r^4s	s	rs	r^2s	r^3	r^4	e	r	r^2
r^4s	r^4s	s	rs	r^2s	r^3s	r^4	e	r	r^2	r^3

Examples abound of corporations using Dihedral groups, D_n, as their logos. Below are examples of D_1, D_3, and D_5.





Example 3.3.6

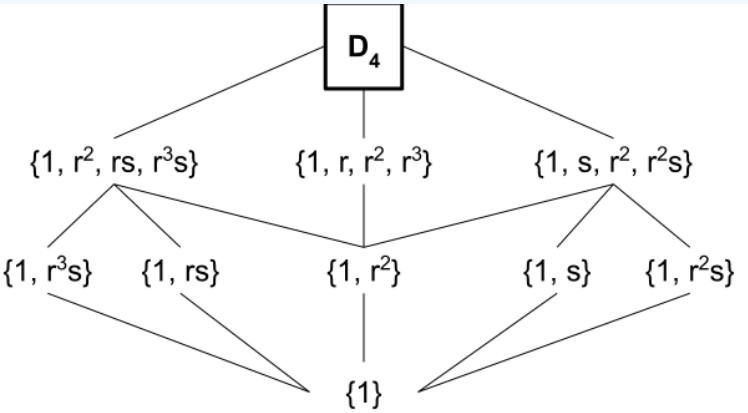
Consider the Dihedral group D_4. $D_4 =< r, s | r^4 = e, s^2 = e, srs = r^{-1} >$.

https://math.libretexts.org/@go/page/132269

$\circ$	e	r	r^2	r^3	s	rs	r^2s	r^3s
e	e	r	r^2	r^3	s	rs	r^2s	r^3s
r	r	r^2	r^3	e	rs	r^2s	r^3s	s
r^2	r^2	r^3	e	r	r^2s	r^3s	s	rs
r^3	r^3	e	r	r^2	r^3s	s	rs	r^2s
s	s	r^3s	r^2s	rs	e	r	r^2	r^3
rs	rs	s	r^3s	r^2s	r	r^2	r^3	e
r^2s	r^2s	rs	s	r^3s	r^2	r^3	e	r
r^3s	r^3s	r^2s	rs	s	r^3	e	r	r^2

1. Find all the subgroups lattice of D_4, the Dihedral group of order 8.

$D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$. Thus, the subgroup lattice would look like this:



2. Prove that every subgroup of D_4 of odd order is cyclic.

Proof:

We shall show that all odd subgroups of D_4 are cyclic.

The only possible odd subgroup, which is cyclic, is $\{e\}$.

Thus, every subgroup of D_4 of odd order is cyclic.□

Theorem 3.3.2

Let the group $D_n =< r, s | r^n = e, s^2 = e, srs = r^{-1} >$.

1. Then $r^k s = sr^{-k}$.

Proof

Consider $r^k s = er^k s = s^2 r^k s = ssr^k s = sr^{-k}$.

2. The order of r^k is $\frac{n}{\gcd(k,n)}$.

Proof

We will first show that $r^k = e$ if and only if $n|k$.

Consider $e = r^k$.

Then by the division algorithm, $k = na + b$ where $0 \leq b < n$.

Thus $e = r^k = r^{na+b} = r^{na}r^b = er^b = r^b$.

Since the smallest possible integer, m, such that $r^m = e$ is n, $b = 0$.

Conversely, if $n|k$, then $k = ns, s \in \mathbb{Z}$.

Thus $r^k = r^{ns} = (r^n)^s = e^s = e$.

Thus $r^k = e$ iff $n|k$.

Let $b = r^k, \in D_4$ since r is a generator of D_n.

We shall show that the smallest integer, m s.t. $r^k = e$ is $\frac{n}{k}$.

Let $d = \gcd(n, k)$.

Consider $e = b^m = r^{km}$.

Since this is the smallest integer m such that $n|km$. Thus $\frac{n}{d}|m(\frac{k}{d})$.

Since d is the greatest common divisor of n and k, $\frac{n}{d}$ and $\frac{k}{d}$ are relatively prime.

Hence $\frac{n}{d}|m(\frac{k}{d})$ means that $\frac{n}{d}|m$. The smallest such m is $\frac{n}{d}$.

Thus $|r^k| = \frac{n}{\gcd(n,k)}$.□

Example 3.3.7

Find the centre of D_n.

Solution:

Let $D_n =< r, s|r^n = e, s^2 = e, srs = r^{-1} >$

We shall show that,

$$Z(D_n) = \{x \in D_n \mid dx = xd, \forall d \in D_n\} = \begin{cases} \{e\}, & \text{if } n \text{ is not divisible by } 2 \\ \{e, r^2\}, & \text{if } n \text{ is divisible by } 2 \end{cases}$$

Let's consider an element x in D_n that commutes with every other element in the group. Therefore, any element in D_n that commutes with every other element is either the identity element e or a rotation r^k where k is a multiple of $n/2$ (for even n).

- If x is the identity element e, it commutes with every element and is in the center.
- If x is a rotation r^k, where k is a multiple of $n/2$) (for even n), or x is the identity element e (for odd n), then it commutes with every element, and it is in the center.
- If x is a rotation r^k, where k is not a multiple of $n/2$(for even n), then it commutes with all rotations but not with reflections. Therefore, it cannot commute with every element and is not in the center.

By combining these two statements, we can conclude that the center of D_n consists of the identity element e and the rotation $r^{n/2}$ (if n is divisible by 2), or just the identity element e (if n is not divisible by 2) for even n. For odd n, the center consists only of the identity element e.

This page titled 3.3: Dihedral Groups (Group of Symmetries) is shared under a CC BY-NC-SA license and was authored, remixed, and/or curated by Pamini Thangarajah.

- **4.4: Transformations** by Pamini Thangarajah is licensed CC BY-NC-SA 4.0.

3E: Exercises

Exercise $3E.1$

Compute the following permutations:

1. $(1435)(231)$
2. $143)(231)^2$
3. $(1345)^{-1}(234)(123)$
4. $(1234)^4$

Exercise $3E.2$

1. Consider the symmetric group S_4.
    1. Find all the subgroup lattice of S_4, the symmetric group of order 24.
    2. Find the centre of S_4.
    3. Find the normalizer of each subgroup of S_4.
    4. Find the cyclic subgroup of S_4 with an order of 4.
    5. Find a non-cyclic subgroup of S_4 with order 4.

Exercise $3E.3$

1. Consider the Dihedral group D_4.
    1. Find all the subgroup lattice of D_4, the Dihedral group of order 8.
    2. Find the centre of D_4.
    3. Find the normalizer of each subgroup D_4.
    4. Prove that every subgroup of D_4 of odd order is cyclic.

Exercise $3E.4$

1. Prove that the following groups are non-abelian.
    1. S_n, for $n \geq 3$.
    2. A_n for $n \geq 4$.
    3. D_n, for $n \geq 3$.

Exercise $3E.5$

Show that for $n \geq 3$, $Z(S_n) = \{1\}$.

Exercise $3E.6$

a. Find a cyclic subgroup of A_8 that has order 4.

b. Find a non-cyclic subgroup of A_8 that has order 4.

Exercise $3E.7$

Suppose that σ and τ in S_5 satisfying $\tau\sigma = (1, 5, 2, 3)$ and $\sigma\tau = (1, 2, 4, 5)$. If $\sigma(1) = 2$, find σ and τ.

Exercise $3E.8$

1) Factor the permutation $(1,2,3,4,5)(6,7)(1,3,5,7)(1,6,3)$ into disjoint cycles.

2) Express the permutation $(1,2,3,4,5)(6,7)(1,3,5,7)(1,6,3)$ as products of transpositions, and decide if it is even or odd.

Exercise $3E.9$

Let $\sigma = (k_1, k_2, \cdots, k_r)$ be an r–cycle. If $\gamma \in S_n$, show that $\gamma\sigma\gamma^{-1}$ is also a cycle; infact $\gamma\sigma\gamma^{-1} = (\gamma(k_1), \gamma(k_2), \cdots, \gamma(k_r))$

Exercise $3E.10$

Show that every product of 3– cycles is an even permutation.

Exercise $3E.11$

Show that every even permutation is a product of 3– cycles.

Exercise $3E.12$

Let G be a group. $H = \{g^2 : g \in G\}$. Prove or disprove: H is a subgroup.

(Hint: $G = A_4$.)

Exercise $3E.13$

a. Find an element of maximum order in S_5.

b. Find an element of maximum order in S_7.

Exercise $3E.14$

a. Let H be a subgroup of A_4 containing $K = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$. Show that if H contains a $3-$ cycle then $H = A_4$.

b. Show that A_4 has no subgroup of order 6.

This page titled 3E: Exercises is shared under a CC BY-NC-SA license and was authored, remixed, and/or curated by Pamini Thangarajah.

Chapter 4: Cosets, special groups, and homorphism

Chapter 4: Cosets, special groups, and homorphism is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

4.1: Cosets and Lagranges Theorem

xDefinition: Cosets

Let G be a group. Let $H \leq G$ and $g \in G$. Then

a) **left coset** of H with representative $g \in G$ is denoted by $gH = \{gh | h \in H\}$.

b) **right coset** of H with representative $g \in G$ is denoted by $Hg = \{hg | h \in H\}$.

Note: if G is abelian then H will be abelian, therefore $gH = Hg, \ \forall g \in G$. The right cosets and left cosets are the same. Also, since H is a group, $hH = H = Hh, \forall h \in H$.

Example 4.1.1

Let $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with the operation addition $(mod\, 6)$.

Let $H = \{0, 3\}$ which is a subgroup of $\mathbb{Z}_6$. We must ensure that H is a subgroup by ensuring closure and that the identity of G is an element of H because H is finite. Notice that $0 \in H$.

$+(mod 6)$	0	3
0	0	3
3	3	0

Hence, by the Cayley table, H is a subgroup of G.

Left cosets of H will be:

$0 + H = \{0, 3\}$. Note: this is equal to H and also equal to $3 + H$.

Note: the count of cosets is based on unique sets; thus, $0 + H = 3 + H$ counts as one left coset.

$1 + H = \{1, 4\}$. Note: this is equal to $4 + H$.

$2 + H = \{2, 5\}$. Note that this is also equal to $5 + H$.

Therefore, there are 3 left cosets in H.

Note, in this case, the right cosets will be the same sets as the left cosets, since $\mathbb{Z}_6$ is commutative.

Theorem 4.1.1

Let G be a group, and let $H \leq G$. Then,

$gH = H = Hg$ if and only if $g \in H$.

Proof

Left to the reader.

Example 4.1.2

Let $G = S_3 = \{e, (1, 2), (1, 3), (2, 3), (1, 2, 3), (3, 2, 1)\}$ with the operation composition.

a) Let $H = A_3 = \{e, (1, 2, 3), (3, 2, 1)\}$.

Without showing the work, $eA_3 = A_3$ and $eA_3 = (1, 2, 3)A_3 = (3, 2, 1)A_3 = A_3$.

Consider $(1, 2)A_3 = \{(1, 2)e, (1, 2)(1, 2, 3), (1, 2)(3, 2, 1)\}$

$= \{(1,2),(2,3),(1,3)\}$.

$(1,3)A_3 = \{(1,3)e,(1,3)(1,2,3),(1,3)(3,2,1)\}$

$= \{(1,3),(1,2),(2,3)\}$.

$(2,3)A_3 = \{(2,3)e,(2,3)(1,2,3),(2,3)(3,2,1)\}$

$= \{(2,3),(1,3),(1,2)\}$.

Therefore $(1,2)A_3 = (1,3)A_3 = (2,3)A_3$.

Thus we have 2 left cosets of H, A_3 and $\{(2,3),(1,3),(1,2)\}$.

To calculate the right cosets, we have A_3G. Applying a process similar to that to determine the left cosets, we obtain the number of right cosets, which happen to be equal to the number of left cosets.

b) Let $K = \{e,(1,2)\}$. Then $eK = (1,2)K = K$.

Consider

$(2,3)K = \{(2,3)e,(2,3)(1,2)\} = \{(2,3),(1,3,2)\} = (1,3,2)K$.

$(1,3)K = \{(1,3)e,(1,3)(1,2)\} = \{(1,3),(1,2,3)\} = (1,2,3)K$.

Hence, three left cosets of K in G exist.

Now, $Ke = K(1,2) = K$.

Consider,

$K(2,3) = \{e(2,3),(1,2)(2,3)\} = \{(2,3),(1,2,3)\} = (1,2,3)K$.

$K(1,3) = \{e(1,3),(1,2)(1,3)\} = \{(1,3),(1,3,2)\} = (1,3,2)K$.

Hence, three right cosets of K in G exist.

Notice that the number of elements in the left coset is the same as in the right coset. But $K(2,3) \neq (2,3)K$.

Theorem 4.1.2

Let G be a group. Let H be a finite subgroup of G. Then $|gH| = |H| = |Hg|$ for all $g \in G$.

Proof

Let G be a group and let H be a finite subgroup of G. Let $g \in G$. Define $\phi : H \to gH$ by $\phi(h) = gh$, for $h \in H$.

We shall show that ϕ is well-defined bijection. Clearly, ϕ is well defined.

ϕ is injective: Let $h_1, h_2 \in H$ such that $\phi(h_1) = \phi(h_2)$. Then $gh_1 = gh_2$. Since $g \in G$, Extra \left or missing \right\right) \implies \left(g^{-1}g\right)h_1=\left(g^{-1}g\right)h_2 \implies h_1=h_2.\) Hence ϕ is injective.

ϕ is surjective: Let $gh \in gH$. then $h \in H$ such that $\phi(h) = gh$. Thus ϕ is surjective.

Since ϕ is a well-defined bijection, $|H| = |gH|$, for all $g \in G$. Similarly we can show that $|H| = |Hg|$ for all $g \in G$.

Theorem 4.1.3

Let G be a group and let $H \leq G$. For $g_1, g_2 \in G$, the following statements are equivalent:

1. $g_1H = g_2H$. Does this mean $g_1 = g_2$ or just that there is a g_1 and g_2 that will generate H?
2. $g_2^{-1}g_1H = H$.
3. $Hg_1^{-1} = Hg_2^{-1}$.
4. $g_2 \in g_1H$.
5. $g_1H \subseteq g_2H$.

Theorem 4.1.4

Let G be a group and let $H \leq G$. Let $\mathcal{L}_H = \{gH \mid |g \in G\}$ set of all left cosets of H in G, and $\mathcal{R}_H = \{Hg \mid |g \in G\}$ set of all right cosets of H in G. Then $|\mathcal{L}_H| = |\mathcal{R}_H|$.

Proof

Let G be a group and let $H \leq G$. Define $\phi : \mathcal{L}_H \to \mathcal{R}_H$ by $\phi(gH) = Hg^{-1}$, for $g \in G$.

We shall show that ϕ is well-defined bijection. Clearly, ϕ is well defined.

ϕ is injective: Let $g_1, g_2 \in G$ such that $\phi(g_1H) = \phi(g_2H)$. Thus, $Hg_1^{-1} = Hg_2^{-1}$. By Theorem 4.1.3, $g_1H = g_2H$. Hence the result.

ϕ is surjective: Let $Hg \in \mathcal{R}_H$. Then $g^{-1} \in G$,$g^{-1}H\mathcal{L}_H$ and $\phi(g^{-1}H) = Hg$. Thus ϕ is surjective.

Since ϕ is a well-defined bijection, $|\mathcal{L}_H| = |\mathcal{R}_H|$.

Example 4.1.3

Let G be a group and let $H \leq G$. Define a relation on G by $g_1 \sim g_2$ is the same as $g_1H = g_2H$, for $g_1, g_2 \in G$. Then we can show that $\sim$ is an equivalence relation (i.e., it is reflexive, symmetric, and transitive). Then $G = \underset{g \in G}{\cup} gH$, either $g_1H = g_2H$ or $g_1H \cap g_2H = \{\}$.

Theorem 4.1.5

Let G be a group and let $H \leq G$. Then, the set of all left cosets of H in G is a partition of G. That is $G = \underset{g \in G}{\cup} gH$ and

either $g_1H = g_2H$ or $g_1H \cap g_2H = \{\}$, for $g_1, g_2 \in G$.

Proof

Let G be a group and let $H \leq G$. Every $g \in G) is a element of \(gH$, so clearly $G \subset \underset{g \in G}{\cup} gH$ and the other inclusion is obvious. Thus, $G = \underset{g \in G}{\cup} gH$.

Let $g_1, g_2 \in G$. such that $g_1H \cap g_2H \neq \{\}$. Thus there exist $y \in g_1H \cap g_2H$. Hence $y \in g_1H$ and $y \in g_2H$. Thus $y = g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$. Which implies $g_1 = (g_2h_2)\, h_1^{-1} = g_2\left(h_2h_1^{-1}\right) \in g_2H$. By Theorem 4.1.3, $g_1H = g_2H$. Hence the result.

Definition: Index

Let G be a group and $H \leq G$.

The index of H in $G = [G : H]$ Note: $[G : H]$ is an integer.

$=$ the number of left cosets of H in G.

$=$ the number of right cosets of H in H in G.

Theorem 4.1.4: Lagranges Theorem

Let G be a finite group and $H \leq G$. Then the order of H divides the order of G and $|G| = [G : H]|H|$.

Note:$[G : H] = \frac{|G|}{|H|}$.

Proof

Let $|G| = n$ and $H \leq G$ of order k. There are finitely many left cosets of H in G, suppose m of them. Then by Theorem 4.1.5, $G = g_1H \cup \cdots \cup g_mH$, where $g_i \in G, \forall i = 1, \cdots m$. Then by Theorem 4.1.2, $n = mk$. Hence the order of H divides the order of G and $|G| = [G : H]|H|$.

Example 4.1.4

Since $|S_3| = 6$ and let $|K| = 2$ then $[S_3 : K] = \frac{6}{2} = 3$, which is what we obtained in the previous example.

Example 4.1.5

Using Lagrange's Theorem, we can prove that A_4 has no subgroup of order 8.

Since$|A_4| = 12$, by Lagrange's theorem, the possible subgroups of A_4 will have orders of 1, 2, 3, 4, 6, or 12. Thus, there will not be a subgroup of order 8.

Lemma 4.1.1

Let G be a group and $H \leq G$.

If the index of H in $G = [G : H] = 2$, then $gH = Hg, \ \forall\, g \in G$.

Proof

Add texts here. Do not delete this text first.

Caution

The converse of Lagrange's Theorem is not necessarily true.

Counterexample: Consider A_4. 6 divides $|A_4|$, but A_4 has no subgroup of order 6.

$A_4 = \{e, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

Answer

Assume that H is a subgroup of A_4 such that $|H| = 6$. Since $|H| = 6$, at least one of the 3– cycle in A_4 must be in H.Without loss of generality, we may assume $(1\,2\,3) \in H$. Since H is a subgroup of A_4, h must contain $(1\,2\,3)^{-1} = (3\,2\,1)$.

Since $[A_4, H] = \frac{12}{6} = 2$, $gH = Hg, \ \forall g \in A_4$. Thus $gHg^{-1} \in H, \ \forall g \in A_4$.

Choose $g = (1\,2\,4) \in A_4$. Then $(1\,2\,4)(1\,2\,3)(1\,2\,4)^{-1} = (1\,2\,4)(1\,2\,3)(4\,2\,1) = (2\,4\,3) \in H$. Since H is a subgroup of A_4 , $(2\,4\,3)^{-1} = (3\,4\,2) \in H$. Now, $(2\,4\,3)(1\,2\,3)(2\,4\,3)^{-1} = (2\,4\,3)(1\,2\,3)(3\,4\,2) = (1\,4\,2) \in H$.

Thus $H = \{e, (1\,2\,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3), \cdots\}$. Thus H has more than 6 elements. This is a contradiction. Hence A_4 has no subgroup of order 6.

Note

The converse of Lagrange's Theorem is true for finite cyclic groups (see Theorem 2.4.8). (2.4: Cyclic groups)

The following are some consequences of Lagrange's Theorem:

Corollary 4.1.1

Let G be a finite group of order n, and let $g \in G$. Then the order of g divides n.

Proof

Let G be a finite group of order n, and let $g \in G$. Suppose $H = \langle g \rangle$. Then $|H| = |\langle g \rangle|$. Hence by Lagrange's Theorem $|H| \mid n$. Thus, the order of g divides n.

Corollary 4.1.2

Let G be a finite group of order n, then $g^n = e$ for all $g \in G$.

Proof

Let G be a finite group of order n, and let $g \in G$. Then by Corollary 4.1.1, the order of g divides n. Suppose the order of $g = k$. Then $n = mk$ for some $m \in \mathbb{Z}$. Now, Consider, $g^n = g^{mk} = (g^k)^m = e^m = e$. Hence, $g^n = e$ for all $g \in G$.

Corollary 4.1.3

Every group of prime order is cyclic.

Proof

Another proof can be found in Theorem 2.4.9 (2.4: Cyclic groups).

Let G be a finite group of order p, where p is prime. Then there exists $g \in G$, not the identity e. Suppose $H = \langle g \rangle$. Hence by Lagrange's Theorem $|H| \mid p$. Since p is prime, $|H| = 1$ or $|H| = p$. Since $g \neq e$, $|H| \neq 1$. Hence $|H| = p$. Thus $G = H$. Therefore, G is cyclic.

Note

The proof of the Corollary 4.1.2 shows that if G is a finite group of prime order, then every non-identity element of G is a generator of G.

Caution

$\mathbb{Z}_6$ is cyclic but the order is not prime.

Corollary 4.1.3

If $K \leq H \leq G$ then $[G : K] = [G : H][H : K]$.

Example 4.1.6

Let H and K be subgroups of a finite group G, and $\gcd(|H|, |K|) = 1$. Then show that $H \cap K = \{e\}$.

Answer

Since H and K be subgroups of a finite group G, $H \cap K \leq H$, and $H \cap K \leq H$,. By Lagrange's Theorem $|H \cap K| \mid |H|$ and $|H \cap K| \mid |K|$. Since $\gcd(|H|, |K|) = 1, |H \cap K| = 1$. Hence, $H \cap K = \{e\}$.

This page titled 4.1: Cosets and Lagranges Theorem is shared under a not declared license and was authored, remixed, and/or curated by Pamini Thangarajah.

4.2: Normal Supgroups and Factor Groups

Normal subgroups

Definition: Normal subgroup

Let G be a group, and let $H \leq G$. Then H is called a **normal subgroup** of G if $gH = Hg, \forall g \in G$, denoted as $H \trianglelefteq G$.

That is, normal subgroups are those that are invariant under conjugation by any element of the group.

Thinking out loud

We are going to concentrate on a limited number of groups. $(\mathbf{Z},+)$, $(\mathbf{Z}_n,+(\text{mod } n))$, $(\mathbf{R}^*,X)$ and $(\mathbf{R},+)$ are abelian.

S_3, S_4, A_3, A_4, D_3, and D_4 are the groups we will concentrate on.

Suppose $H \leq G$.

H is a normal subgroup of G, if $gH = Hg,\ \forall g \in G$. Means left cosets=right cosets.

For any group G, the trivial subgroups $\{e\}$ and G are normal subgroups.

Example 4.2.1

Consider $S_3 = \{e, (123), (321), (12), (13), (23)\}$.

1. Is $H = \{e, (12)\} \trianglelefteq S_3$?

Since $(123)H = \{(123), (13)\} \neq H(123) = \{(123), (23\}$, thus $H \ntrianglelefteq S_3$.

2. Is $A_3 = \{\langle(123)\rangle\} \trianglelefteq S_3$?

$A_3 = \{e, (123), (321)\}$.

There will be 2 cosets of A_3 in S_3 since $\frac{|S_3|}{|A_3|} = \frac{6}{3} = 2$.

The first will be the set itself since $eH = He = H$. To find the second, take any element

in S_3, not in S_4 and determine its coset. Having done so, the cosets are: $A_3, \{(12), (13), (23)\}$.

Theorem 4.2.1

Let G be a group, and H be a subgroup of G. If $[G : H] = 2$, then show that H is a normal subgroup of G.

Proof:

Let G be a group and $H \leq G$ s.t. $[G : H] = 2$.

H partitions G into 2 cosets. The left cosets being $\{H, xH\}$. Similarly, the right cosets are $\{H, Hx\}$ where $x \in G$ and $x \notin H$.

Case 1:

If $x \in H$ then $xH = H = Hx$.

Since $xH = Hx$, $H \trianglelefteq G$.

Case 2:

If $x \in G$, but not in H. We will show this as $x \in G - H$.

Then $xH = G - H = Hx$.

Since $xH = Hx$, $H \trianglelefteq G$.

Thus $xH = Hx,\ \forall x \in G$, thus $H \trianglelefteq G$.□

Example 4.2.2

Show that A_n is a normal subgroup of $S_n,\ \forall n \in \mathbb{N}$.

Solution

Consider $\frac{|S_n|}{|A_n|} = \frac{n!}{\frac{n!}{2}} = 2$.

From previous theorem, given $H \leq G$ then if $[G : H] = 2$ then $H \trianglelefteq G$.

Since $A_n \trianglelefteq S_n$ and $[S_n : A_n] = 2$, $H \trianglelefteq G$.□

Example 4.2.3

List all normal subgroups in D_4.

Solution

$D_4 = \langle r, s \mid r^4 = e, s^2 = e, srs = r^{-1} \rangle = \{e, r, r^2, r^3, s, sr^2, sr^3\}$. Note that $\{1\}$ and D_4 are normal subgroups of D_4.

Since $|D_4| = 8$, by Lagranges thereom, nontrivial subgroups of D_4 has order 2 or 4.

The subgroups of order 4 are:

$H_1 = \langle r \rangle = \{e, r, r^2, r^3\}, H_2 = \langle s, r^2 \rangle = \{e, s, r^2, sr^2\}, H_3 = \langle sr, r^2 \rangle = \{e, sr, r^2, sr^3\}$.

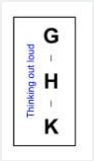
Since $[D_4 : H_i] = \frac{8}{4} = 2, \forall i = 1, 2, 3$, $H_i \trianglelefteq D_4$, $\forall i = 1, 2, 3$.

We know that $Z(D_4) = \{e, r^2\}$, $\{e, r^2\} \trianglelefteq D_4$. (see below Theorem 3)

Verify that the subgroup of order $2, \langle s \rangle \ntrianglelefteq D_4$.

Note: Let G be a group.

If $H \leq G$ and $K \leq H$ then $K \leq G$. However, this does not work for normal subgroups. Thus, given $H \trianglelefteq G$ and $K \trianglelefteq H$, it does not follow that $K \trianglelefteq G$; see the following example.



Example 4.2.4

Let $G = A_4$, $H = \{e, (1,2)(3,4), (1,3)(2,4), (2,3)(1,4)\}$*and*\($K = \{\{e, (1,2)(3,4)\}$.

Then $H \trianglelefteq G$ and $K \trianglelefteq H$, but K is not a normal subgroup of A_4. That is $K \ntrianglelefteq G$.

Answer

Let $G = A_4, H = K_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ and $K = \{e, (12)(34)\}$. Consider the Cayley table for H and K,

	e	(1,2)(3,4)	(1,3)(2,4)	(1,4)(2,3)
e	e	(1,2)(3,4)	(1,3)(2,4)	(1,4)(2,3)
(1,2)(3,4)	(1,2)(3,4)	e	(1,4)(2,3)	(1,3)(2,4)
(1,3)(2,4)	(1,3)(2,4)	(1,4)(2,3)	e	(1,2)(3,4)
(1,4)(2,3)	(1,4)(2,3)	(1,3)(2,4)	(1,2)(3,4)	e

	e	(1,2)(3,4)
e	e	(1,2)(3,4)
(1,2)(3,4)	(1,2)(3,4)	e

Then clearly, $H \leq G$, $K \leq G$. We shall show that $H \trianglelefteq G$ and $K \trianglelefteq H$.

By Lagranges Theorem. $[H : K] = \frac{|H|}{|K|} = 2, gK = Kg, \forall\ g \in H$. Thus, $K \trianglelefteq H$. Now, by Lagranges Theorem. $[G : H] = \frac{|G|}{|H|} = \frac{12}{4} = 3$, Hence H has 3 cosets in G.

Now, consider the left cosets of H in G:

$$eH = \{ee, e(12)(34), e(13)(24), e(14)(23)\} = \{e, (12)(34), (13)(24), (14)(23)\} \tag{4.2.1}$$

$$= ((1,2)(3,4))H = ((1,3)(2,4))H = ((1,4)(2,3))H \tag{4.2.2}$$

$$(1,2,3)H = \{(1,2,3)e, (1,2,3)(12)(34), (1,2,3)(13)(24), (1,2,3)(14)(23)\} \tag{4.2.3}$$

$$= \{(1,2,3), (1,3,4), (2,4,3), (4,2,1)\} = (1,3,4)H = (2,4,3)H = (4,2,1)H \tag{4.2.4}$$

$$(3,2,1)H = \{(3,2,1)e, (3,2,1)(12)(34), (3,2,1)(13)(24), (3,2,1)(14)(23)\} \tag{4.2.5}$$

$$= \{(3,2,1), (2,3,4), (1,2,4), (1,4,3)\} = (2,3,4)H = (1,2,4)H = (1,4,3)H. \tag{4.2.6}$$

And the right cosets of H are:

$$He = \{ee, (12)(34)e, (13)(24)e, (14)(23)e\} = \{e, (12)(34), (13)(24), (14)(23)\} = H((1,2)(3,4)) = H((1,3)(2,4)) = H((1,4)(2,3)) \tag{4.2.7}$$

$$H(1,2,3) = \{e(1,2,3), (12)(34)(1,2,3), (13)(24)(1,2,3), (14)(23)(1,2,3)\} = \{(1,2,3), (2,4,3), (1,4,2), (1,3,4)\} = H(1,3,4) = H(2,4,3) = H(1,4,2) \tag{4.2.8}$$

$$H(3,2,1) = \{e(3,2,1), (12)(34)(3,2,1), (13)(24)(3,2,1), (14)(23)(3,2,1)\} = \{(3,2,1), (1,4,3), (2,3,4), (1,2,4)\} = H(2,3,4) = H(1,2,4) = H(1,4,3) \tag{4.2.9}$$

Since the right cosets are the same as the left cosets, we know that K is normal in H.

Since the right cosets are the same as the left cosets, we know that H is normal in G.

We shall show that K is not a normal subgroup of A_4. Since $(1,2,3)(12)(34)(3,2,1) = (1,3)(2,4) \notin K$, K is not a normal subgroup of A_4.

Theorem 4.2.2

Let G be a group and $H \leq G$. Then the following statements are equivalent:

1. $H \trianglelefteq G$.
2. $\forall\, g \in G,\ gHg^{-1} \subseteq H$.
3. $\forall\, g \in G,\ gHg^{-1} = H$.

Theorem 4.2.3

Let G be a group and $H \leq G$. Then

1. if G is abelian, then $H \trianglelefteq G$.
2. $Z(G) \trianglelefteq G$.

Example 4.2.5

Prove or disprove the statements:

1. If all the subgroups of a group G are normal subgroups of G then G is abelian.
2. If $H \trianglelefteq G$ then $H = Z(G)$.
3. If $H \trianglelefteq G$ then $[G : H] = 2$.
4. If $H \leq G$ and H is abelian then $H \trianglelefteq G$.

Solution

1. Counterexample: $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k \mid i^2 = j^2 = k^2, ij = k, jk = i, ki = j\}$
2. Counterexample: $G = S_3$. Then $Z(S_3) = \{e\}$ and $A_3 \trianglelefteq G$. Normal subgroups are not necessarily the center of the group.
3. Counterexample: $G = A_4$ and $H = \{e, (1,2)(3,4), (1,3)(2,4), (2,3)(1,4)\}$.
4. Counterexample: $G = A_4$ and $K = \{e, (12)(34)\}$.

4.2.0.0.1 Simple Subgroups

Definition: Simple

A group G is called simple if G has no nontrivial normal subgroups.

Example 4.2.5

$\mathbb{Z}_2$ is simple since the normal subgroups are $\{0\}, \mathbb{Z}_2$. $\mathbb{Z}_p$, for prime p and A_n for $n \geq 5$ are simple.

4.2.0.0.1 Factor Groups

Definition: Factor Groups

Let G be a group and $N \trianglelefteq G$.

Thus $\{gN | g \in G\}$ are all the cosets (i.e., the set of sets), and the factor group is defined as $G/N = \{gN | g \in G\}$, which is a group with the operation of $(g_1N)(g_2N) = g_1g_2N$ for $g_1g_2 \in G$. If G is finite, the order $|G/N| = [G : N]$.

We shall show that G/N is a group $gN\, hN = (g \star h)N$ with $\star$ being the operation in G .

Note: This is the process used to combine groups.

First, we shall show that $N =$ is the identity of G/N.

Consider $gN\, N = (g \star e)N = N\, gN$. Thus, the identity N exists.

Suppose $g \in G$. Then $gN \star g^{-1}N = (gg^{-1})N = eN = N$. Thus, the inverse exists $g^{-1}N$ for each element gN.

G/N is associative since G was associative.

Since G/N has an identity, has an inverse for each element, and is associative, G/N is a group, which is called a **factor group (or quotient group)**.

Example 4.2.6

$S_3/A_3 = \{A_3, (12)A_3\}$.

The Cayley Table for S_3/A_3:

	A_3	$(12)A_3$
A_3	A_3	$(12)A_3$
$(12)A_3$	$(12)A_3$	A_3

Example 4.2.7

Let $(\mathbb{Z}, +)$. Consider $n\mathbb{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$. Is this a group?

Yes, since it is a non-empty set that contains the identity and $gh^{-1} \in n\mathbb{Z}, \forall g, h \in n\mathbb{Z}$.

Therefore, the set is a subgroup of $\mathbb{Z}$. Since $\mathbb{Z}$ is abelian, it is a normal subgroup of $\mathbb{Z}$. Hence,

$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots (n-1) + n\mathbb{Z}\}$.

Example 4.2.8

Let $G =< a >$ where $|a| = 12$, and let $H =< a^3 >$. Find all cosets in G/H and write down the Cayley table. Is G/H cyclic? Why or why not?

Solution

By Theorem 2.4.8, $H \leq G$. Since G is abelian, $H \trianglelefteq G$. The factor group $G/H = \{H, aH, a^2H\}$.

Cayley table for G/H			
	H	aH	a^2H
H	H	aH	a^2H
aH	aH	a^2H	H
a^2H	a^2H	H	aH

Notice that $G/H = \{H, aH, a^2H\} = \{\langle aH \rangle \mid a^3H = H\}$. Thus G/H is cyclic.

Theorem 4.2.4

1. A factor group of a cyclic group is cyclic.
2. A factor group of an abelian group is abelian.
3. A factor group of a finite group is finite.

Note

A factor group of a non-abelian group can be abelian or cyclic. (see example 4.2.6)

A factor group of an infinite group can be finite.

Theorem 4.2.5

Let G be a group and let K be a subgroup of $Z(G)$ be the centre of G. If G/K is cyclic, then G is abelian.

Corollary 4.2.1

Let G be a non-abelian group of order pq, where p and q are different prime numbers. Then the center of G, $Z(G) = \{e\}$.

Proof

Let G be a non-abelian group of order pq, where p and q are prime.

By Lagranges thereom, the subgroups of G has order 1 , p, q or pq.

Since G is non-abelian, $Z(G) \neq G$.

Assume that $|Z(G)|$ is p or q, then $G/Z(G)$ is of prime order. Therefore, it is cyclic. Hence by Theorem 4.2.3, G is abelian.

This contradicts the fact that G is non-abelian. Hence $|Z(G)| = 1$. Thus $Z(G) = \{e\}$.

Example 4.2.9

Let G be a group and let $G' = \langle aba^{-1}b^{-1} \rangle$, that is, G' is the subgroup of all infinite products of elements in G of the form $aba^{-1}b^{-1}$. The subgroup G' is called the commutator subgroup of G.

1. Show that G' is a normal subgroup of G.

Proof:

Let $g \in G$ and $h \in G'$.

We will show that $G' \trianglelefteq G$.

Consider $h = aba^{-1}b^{-1}, a, b \in G$.

Then $ghg^{-1} = gaba^{-1}b^{-1}g^{-1}$

$= geaebea^{-1}eb^{-1}g^{-1}$

$= (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1})$ Note: $g^{-1}g = e$

$= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \in G'$.

Thus $G' \trianglelefteq G$.□

2. Let N be a normal subgroup of G. Prove that G/N is abelian iff N contains the commutator subgroup of G.

Proof:

Let $N \trianglelefteq G$.

We shall show that G/N is abelian if and only if N contains the commutator subgroup of G.

Let G/N be abelian.

Let $a, b \in G$.

We shall show that the commutator subgroup of $G \subseteq N$

Consider $(aN)(bN) = (bN)(aN)$ since G/N is abelian.

Thus, $abN = baN$.

Thus $ab(ba)^{-1} \in N$ Note: due to cosets.

Thus $ab(ba)^{-1} = aba^{-1}b^{-1} \in N$.

Therefore the commutator subgroup of $G \subseteq N$.

Conversely, let the commutator subgroup of $G \subseteq N$ and $a, b \in G$.

We shall show that G/N is abelian.

Since the commutator subgroup of $G \subseteq N$, $aba^{-1}b^{-1} \in N$.

Thus, $ab(ba)^{-1}N = N$.

Thus $(aN)(bN) = (bN)(aN)$.

Therefore G/N is abelian.

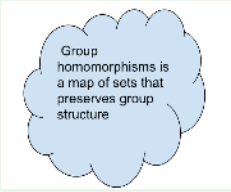
Therefore G/N is abelian iff N contains the commutator subgroup of G.□

This page titled 4.2: Normal Supgroups and Factor Groups is shared under a CC BY-NC-SA license and was authored, remixed, and/or curated by Pamini Thangarajah.

4.3: Homomorphisms

Definition: Homomorphism

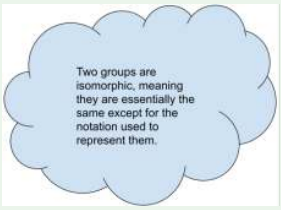
Let $(G_1, \star_1)$, $(G_2, \star_2)$ be groups. Then a function $h : G_1 \to G_2$ such that $h(g_1) = g_2, g_1 \in G$ and $g_2 \in G_2$ is called a homomorphism from the group G_1 to the group G_2 if



$$h(g_1 \star_1 g_1') = h(g_1) \star_2 h(g_1'), \text{ for } g_1, g_1' \in G_1.$$

Further, if h is a bijection and homomorphism, then h is called an isomorphism. In this case, we say $G_1 \cong G_2$, which means that G_1 is isomorphic to G_2.

Moreover, if h is an isomorphism from a group G to itself, then h is called an automorphism. $Aut(G)$ = Set of all automorphisms=$\{h : G \to G \mid h \text{ is an isomorphism}\}$.



Example 4.3.1

Let $C_n = \{\langle a \rangle \mid a^n = e\}$. be a cyclic group.

Define: $h : C_n \to \mathbb{Z}_n$ by $h(a^k) = k \pmod n$. Then

1. Is h a homomorphism?
2. Is h injective (1-1)?
3. Is h surjective (onto)?

If all three are true, then h is an isomorphism.

Answer

We will show a finite cyclic group is always isomorphic to $(\mathbb{Z}_n, + \pmod n)$.

Proof of Homomorphism:

Let $g_1, g_2 \in C_n$.

We shall show that $h(g_1 \star_1 g_2) = h(g_1) \star_2 h(g_2)$.

Consider $g_1 = a^{k_1}$ and $g_2 = a^{k_2}$.

Then $h(g_1) = k_1 \pmod n$ and $h(g_2) = k_2 \pmod n$.

$g_1 \star_1 g_2 = a^{k_1} \star_1 a^{k_2} = a^{k_1 + k_2}$.

Thus $h(g_1 \star_1 g_2) = k_1 + k_2 \pmod n$.

Now consider $h(g_1) \star_2 h(g_2) = k_1 \pmod n + k_2 \pmod n$

$= k_1 + k_2 \pmod n$.

Hence $h(g_1 \star_1 g_2) = h(g_1) \star_2 h(g_2)$.

Hence h is a homomorphism.□

Proof of Injection (1-1):

Let $g_1, g_2 \in G$ s.t. $h(g_1) = h(g_2)$.

Since $g_1, g_2 \in C_n$, $g_1 = a^{k_1}$ and $g_2 = a^{k_2}$, $k_1, k_2 \in \mathbb{Z}$.

Now, $h(g_1) = k_1 \pmod n = k_2 \pmod n = h(g_2)$.
Therefore, $k_1 = k_2 \in \mathbb{Z}_n$.

Hence h is injective (1-1).□

Thinking out loud
Recall if h is injective, then given h(a)=h(b), a=b.

Proof of Surjective (onto):

Let $k \in \mathbb{Z}_n$.

Since $a^k \in C_n$ by definition $h(a^k) = k \pmod n$.

Hence h is surjective.□

Thinking out loud
Recall if h is surjective, then every element in Z_n can be generated by an element in C_n.

Since a finite cyclic group is homomorphic, injective and surjective to $(\mathbb{Z}_n, + \pmod n)$, it is isomorphic to $(\mathbb{Z}_n, + \pmod n)$). □

Example 4.3.2

Define $h : (\mathbb{Z}, +) \to (\mathbb{Z}_n, \cdot \pmod n)$ defined by

$h(k) = a^k$, where $\mathbb{Z}_n =< a >, k \in \mathbb{Z}$. Then

For $k, m \in \mathbb{Z}, h(k + m) = a^{k+m} = a^k a^m = h(k)h(m)$. Thus h is a homomorphism.

Notice that

Table 4.3.2: Homomorphism

0 $\pm n$ $\pm 2n$ $\pm 3n$	1 $1 \pm n$ $1 \pm 2n$ $1 \pm 3n$	...	...	$(n-1)$ $(n-1) \pm n$ $(n-1) \pm 2n$ $(n-1) \pm 3n$	$\mathbb{Z}$
↓	↓	↓	↓	↓	
a^0	a^1			$a^{(n-1)}$	$\mathbb{Z}_n$

Hence h is onto but not one to one.

Note

Let $(G_1, \star_1)$, $(G_2, \star_2)$ be groups.

Then a function $h : G_1 \to G_2$ s.t. $h(g_1) = e_2, \forall g_1 \in G_1$ **and the identity** $e_2 \in G_2$ is called a **trivial homomorphism** from the group G_1 to the group G_2.

Example 4.3.3

Let G be a group. The mapping $1_G : G \to G$ defined by $1_G(g) = g, \forall g \in G$ is a homomorphism.

Example 4.3.4

Define a mapping from $h : D_4 \to D_4$ by $h(a) = a^3, a \in D_4$. Is h a homomorphism?

Solution

No. $D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ such that $r^4 = e, s^2 = e, srs = r^{-1}$. Consider $h(s) = s^3 = s, h(r) = r^3$ and $h(sr) = (sr)^3 = (sr)(sr)(sr) = (srs)r(sr) = r^2r(sr) = r^3(r^2s) = rs = sr^2$. But $h(s)h(r) = sr^3$.

Example 4.3.5

Define a mapping from $h : S_4 \to S_4$ by $h(\sigma) = \sigma^2$, for $\sigma \in S_4$. Is h a homomorphism?

Solution

No. $h((1,2)) = h((2,3)) = e$ but $h((1,2)(2,3)) = h((1,2,3)) = (3,2,1)$.

Example 4.3.6

Let $\phi : \mathbb{Z}_5 \to \mathbb{Z}_2$ mapping defined by $\phi(a) = \begin{cases} 1 & if\ a \text{ is odd} \\ 0 & if\ a \text{ is even} \end{cases}$.

Show that ϕ is not a homomorphism.

Solution

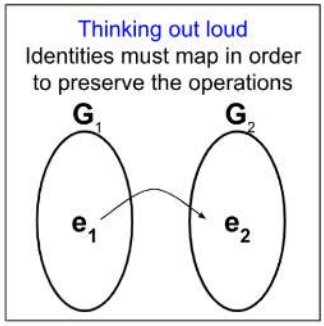
$\phi(2+4) = \phi(1) = 1$ but $\phi(2) + \phi(4) = 0$.

Properties of homomorphisms:

Theorem 4.3.1

Let $(G_1, \star_1)$, $(G_2, \star_2)$ be groups and let $h : G_1 \to G_2$ be a homomorphism. Then:

1. $h(e_1) = e_2$, where e_1, e_2 are identities of G_1, G_2 respectively.
2. $h(g_1^{-1}) = h(g_1)^{-1}, g_1 \in G_1$.
3. $h(g_1^n) = h(g_1)^n$, $n \in \mathbb{Z}$ and $g_1 \in G_1$.



Proof:

1.Since e_1 is the identity of G_1, $e_1e_1 = e_1$.

Since h is a homomorphism, $h(e_1e_1) = h(e_1)h(e_1) = h(e_1) = e_2h(e_1)$.

By cancellation law, $e_2 = h(e_1)$.

2. Let $g_1 \in G_1$. Then $g_1g_1^{-1} = e_1$.

Since h is a homomorphism, $h(g_1g_1^{-1}) = h(g_1)h(g_1^{-1}) = h(e_1) = e_2$.

Hence $(h(g_1))^{-1} = h(g_1^{-1})$.

3. Use induction on $\mathbb{Z}_+$.

Corollary 4.3.1

Let $(G_1, \star_1)$, $(G_2, \star_2)$ be groups and let $h : G_1 \to G_2$ be a homomorphism. If $g_1 \in G_1$ has a finite order then $h(g_1)$ has a finite order, and $|h(g_1)|$ divides $|g_1|$.

Proof:

Let $(G_1, \star_1)$, $(G_2, \star_2)$ be groups and let $h : G_1 \to G_2$ be a homomorphism. Assume that $g_1 \in G_1$ has a finite order n. Then $g_1^n = e_1$. Hence $h(g_1)^n = h(g_1^n) = h(e_1) = e_2$. By Theorem 2.4.5(2.4: Cyclic groups), $|h(g_1)|$ divides n. Hence $|h(g_1)|$ divides $|g_1|$.

The following theorem allows us to determine if two homomorphisms are equal by checking only the generators instead of every element in the domain.

Note

Recall: Let $(G, \star)$ be a group.

Let $X = \{x_1, x_2, \cdots, x_n\}$ where $x_1, x_2 \cdots, x_n \in G$, then the subset of G generated by X denoted by $\langle X \rangle$ is

$\{x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} \mid m_1, m_2 \cdots, m_n \in \mathbb{Z}\}$.

Theorem 4.3.2

Let $h : G \to G_1$ and $h_1 : G \to G_1$ be group homomorphisms and $G = \langle X \rangle$ is generated by a subset X, then show that $h = h_1$ if and only if $h(x) = h_1(x), \forall x \in X$.

Proof:

Let $X = \{g_1, \cdots, g_n\}$. Assume $h(g_i) = h_1(g_i), \forall g_i \in X, i \in \mathbb{Z}$. Let $g \in G$. Since $G = \langle X \rangle, g = g_1^{m_1} \cdots g_n^{m_n}$, where $m_1, \ldots, m_n \in \mathbb{Z}$. Consider $h(g) = h(g_1^{m_1} \ldots g_n^{m_n}) = h(g_1^{m_1}) \cdots h(g_n^{m_n})$, as h is a homomorphism. Then;

$$\begin{aligned} h(g) &= (h(g_1))^{m_1} \ldots (h(g_n))^{m_n} \\ &= ((h_1(g_1))^{m_1} \cdots (h_1(g_n))^{m_n} \qquad \textbf{(by assumption)} \\ &= h_1(g_1^{m_1}) \cdots h_1(g_n^{m_n}), \\ &= h_1(g_1^{m_1} \ldots g_n^{m_n}) \\ &= h_1(g). \end{aligned}$$

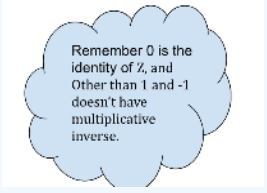
Hence, $h(g) = h_1(g), \forall g \in G$. The converse is clearly true. Hence the result.

Example 4.3.7

Describe all group homomorphisms from $\mathbb{Z}$ to itself. From which, how many of them are surjective?

Solution

Since $\mathbb{Z} = \langle 1 \rangle$, any such group homomorphism h determined by $h(1)$. If $h(1) = k, k \in \mathbb{Z}$, then $h(n) = kn, \forall n \in \mathbb{Z}$. Hence there is such a group homomorphism for every $k \in \mathbb{Z}$. The only surjective group homomorphisms are $k = \pm 1$.



Example 4.3.8

Find all group homomorphisms from C_3 to A_4, where $C_3 = \{\langle a \rangle \mid a^3 = e\}$.

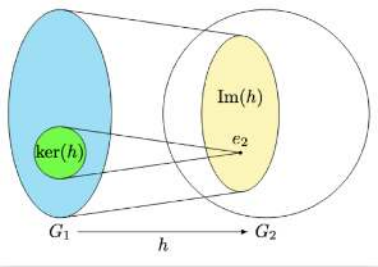
Solution

Let $C_3 = \langle c \rangle$. Any group homomorphism $h : C_3 \to G$, any group G, determined by $h(c)$, and $h(c)$ must be an element of order 1 or 3 in G. If $h(c) = e, e \in A_4$, then h is a trivial homomorphism. Otherwise, $h(c)$ must be a $3-$ cycle in A_4. There are $\frac{4!}{3^1 1^1 1!1!} = 8$, $3-$cycle permutations in A_4. Hence, eight such group homomorphisms.

Definition:

Let $h : G_1 \to G_2$ be a homomorphism. Then

1. The kernel of h is defined as $ker(h) = \{g_1 \in G_1 | h(g_1) = e_2\}$.
2. The image of h is defined as $im(h) = \{g_2 \in G_2 | h(g_1) = g_2, g_1 \in G_1\}$.



Theorem 4.3.2

Let $h : G_1 \to G_2$ be a homomorphism. Then $ker(h) \leq G_1$ and $im(h) \leq G_2$. Also, $\ker(h)$ is a normal subgroup of G_1.

Proof:

Let $h : G_1 \to G_2$ be a homomorphism.

Since $h(e_1) = e_2, e_1 \in ker(h)$. Let $g_1, g_1' \in ker(h)$. Then $h(g_1) = e_2$ and $h(g_1') = e_2$.

Similarly, we can show that $im(h) \leq G_2$.

We shall show that $g_1^{-1} g_1' \in ker(h)$.

Consider $h(g_1^{-1} g_1') = h(g_1^{-1}) h(g_1') = h(g_1)^{-1} h(g_1') = e_2^{-1} e_2 = e_2$. Hence $g_1^{-1} g_1' \in ker(h)$. Thus $ker(h) \leq G_1$.

We shall show that $\ker(h)$ is a normal subgroup of G_1.

Let $x \in \ker(h)$ s.t. $h(x) = e_2$.

We will show $gxg^{-1} \in \ker(h), \forall\ g \in G_1$. Let $g \in G_1$.

Consider $h(gxg^{-1}) = h(g)h(x)h(g^{-1})$

$$= h(g)h(x)(h(g))^{-1}$$

$$= h(g)e_2(h(g))^{-1}$$

$$= h(g)(h(g))^{-1}$$

$$= e_2.$$

So $\ker(h)$ is a normal subgroup of G_1.

Example 4.3.9

Let $h : G_1 \to G_2$ be a group homomorphism with $K = ker(h)$. Show that for any $g_1 \in G_1$, $g_1 K = \{g \in G_1 \mid h(g) = h(g_1)\}$.

Solution

Let $g_1 \in G_1$. Let $g \in g_1 K$. Then $g = g_1 k$ where $k \in ker(h)$. Thus, $h(k) = e_2$. Consider $h(g) = h(g_1 k) = h(g_1)h(k) = h(g_1)e_2 = h(g_1)$. Hence, $g_1 K \subset \{g \in G_1 \mid h(g) = h(g_1)\}$. Conversely, suppose $x \in \{g \in G_1 \mid h(g) = h(g_1)\}$. Then $h(x) = h(g_1) \implies h(g_1^{-1} x) = h(g_1^{-1})h(x) = (h(g_1))^{-1} h(x) = e_2$. Hence, $g_1^{-1} x \in K$. Thus $x \in g_1 K$. Hence the reuslt.

Theorem 4.3.3

Let $h : G_1 \to G_2$ be a homomorphism. Then $ker(h) = \{e_1\}$ if and only if h is injective.

Proof

Let $h : G_1 \to G_2$ be a homomorphism. Assume that $ker(h) = \{e_1\}$. We shall show that h is injective. Let $x, y \in G_1$ such that $h(x) = h(y)$. Then \(h(xy^{-1}= e_2.\) Thus, \(xy^{-1) \in ker(h)\). Hence \(xy^{-1}=e_1 \implies x=y.\) Thus h is injective. Conversely, assume that h is injective. Since $h(e_1 = e_2,\ ker(h) = \{e_1\}$. Hence the result.

Note

If both G_1 and G_2 are finite and h is an injective homomorphism (is called monomorphism) then h is an isomorphism.

Example 4.3.10

Find all group homomorphisms from A_4 to C_3, where $C_3 = \{\langle a\rangle \mid a^3 = e\}$.

Solution

The kernel of a group homomorphism $h : A_4 \to G$, any group G, is a normal subgroup of A_4. Hence $ker(h)$ is either $\{e\}, K = \{e, (12)(34), (13)(24), (14)(23)\}$ or A_4. Since $|A_4| \neq |C_3|,\ ker(h) \neq \{e\}$. Suppose $ker(h) = K$. Let $\phi : A_4 \to A_4/K$ be the coset map defined by $\phi(\sigma) = \sigma K$, for $\sigma \in A_4$. Note that $|A_4/K| = 3$, and $A_4/K = \{K, (1\ 2\ 3)K, (1\ 2\ 3)^2K\} = \langle(1\ 2\ 3)K\rangle$. There are exactly two isomorphisms from A_4/K to C_3 in the following way:

Let $\bar{\phi} : A_4/K \to C_3$ be the isomorphism such that $h = \bar{\phi} \circ \phi$, then $\bar{\phi}((1\,2\,3)K)$ is either a or a^2 giving two group homomorphisms

$$h_1(x) = \begin{cases} e & \text{if } x \in K \\ a & \text{if } x \in (1\,2\,3)K \\ a^2 & \text{if } x \in (3\,2\,1)K \end{cases} \tag{4.3.1}$$

, and

$$h_1(x) = \begin{cases} e & \text{if } x \in K \\ a^2 & \text{if } x \in (1\,2\,3)K \\ a & \text{if } x \in (3\,2\,1)K \end{cases} \tag{4.3.2}$$

.

If $ker(h) = A_4$, then h is a trivial homomorphism.

4.3.1 Isomorphic Groups

As we said earlier in Chapter 2, we can use the Cayley tables to identify isomorphic groups. For example:

Cayley table for Klein 4-group: $H = \{\langle a, b, c\rangle \mid a^2 = e, b^2 = e, c^2 = e$ and $ab = ba = c, bc = cb = a, ac = ca = b\} = \{e, a, b, c\}$.

Table 1: Cayley table for Klein 4-group

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Compare it with the Cayley tables for $(\mathbb{Z}_4, +(mod\,4))$ and $(U(5), \cdot(mod 5)$.

Table 2: Cayley table for $(\mathbb{Z}_4, +(mod\,4))$

$+(mod\,4)$	0	1	2	3
0	0	1	2	0
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$U(5) = \{1, 2, 3, 4\}$.

Table 3: Cayley table for $(U(5), \cdot(mod\,4))$

$\cdot(mod\,5)$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

We can see that Tables 2 and 3 are identical (mapping: $0 \mapsto 1, 1 \mapsto 2, 2 \mapsto 4, 3 \mapsto 3$), while Table 1 is different. Hence, we say that the groups $\mathbb{Z}_4$ and $U(5)$ are isomorphic and denoted by $\mathbb{Z}_4 \cong U(5)$, and the groups $\mathbb{Z}_4$ and K_4 are not isomorphic and denoted by $\mathbb{Z}_4 \ncong K_4$.

Definition: Isomorphic Groups

Two groups G and H are isomorphic, denoted by $G \cong H$,if there exists an isomorphism from G to H.

Example 4.3.11

$\mathbb{Z}_4 \cong U(5)$

Example 4.3.12

$\mathbb{Z} \cong 4\mathbb{Z}$

Answer

The function $\phi : \mathbb{Z} \to 4\mathbb{Z}$, $\phi(x) = 4x, x \in \mathbb{Z}$ is clearly a bijection.

Theorem 4.3.4

Let G be a group, and let $g \in G$. Then

1. If $|g|$ is infinite then $\langle g \rangle \cong \mathbb{Z}$.

Proof

Use \(\phi: \langle g\rangle \to \mathbb{Z}\) such that $\phi(g^k) = k$.

2. If $|g| = n$ then $\langle g \rangle \cong \mathbb{Z}_n$.

Proof

Use \(\phi: \langle g\rangle \to \mathbb{Z}_n\) such that $\phi(g^k) = k (mod\, n)$.

Theorem 4.3.5

1. Let G be group of order 4 then either G is cyclic or $G \cong K_4$.
2. Let G be group of order 6 then either G is cyclic or $G \cong D_3$.

Examples of structural properties of a group G:

1. G is abelian.
2. G is cyclic.
3. G is finite.
4. $|G| = n$.
5. G has no element of order k.

and many more.....

Theorem 4.3.6

If two groups G and H are isomorphic and G has a structural property, then H has the structural property.

Theorem 4.3.7: Cayley's Theorem

Every group of order n is isomorphic to a subgroup of S_n.

Example 4.3.13

Find all isomorphisms from $\mathbb{Z}$ to $U(7)$.

Solution

Add example text here.

Example 4.3.14

Prove or disprove: S_4 and D_{12} are isomorphic.

Solution

Even though $|S_4| = |D_{12}| = 24$ and both are non abelian, $S_4 \ncong D_{12}$. Since $D_{12} = \{\langle r, s\rangle \mid r^{12} = e, s^2 = e, srs = r^{-1}\}, r \in D_{12}$ and $|r| = 12$.

Now, we shall show that the order of all the elements of S_4 is less than or equal to 4. This can be achieved by examining all possible types of permutations and their corresponding orders. The partitions of 4 are $4, 3+1, 2+2, 2+1+1$ and $1+1+1+1$. Hence the possible orders of permutations are $4, lcm(3,1), lcm(2,2), lcm(2,1,1)$ and $lcm(1,1,1,1)$. Thus the possible orders of permutations are $4, 3, 2, 1$. Hence the order of all the elements of S_4 is less than or equal to 4. Therefore, S_4 doesn't have an element of order 12. Hence, S_4 and D_{12} are not isomorphic.

Example 4.3.15

Prove or disprove: $(\mathbb{Q}, +)$ and $(\mathbb{Q} \setminus \{0\}, \cdot)$ are isomorphic.

Solution

Let $\phi : (\mathbb{Q}, +) \to (\mathbb{Q} \setminus \{0\}, \cdot)$ be an isomorphism. Since $2 \in \mathbb{Q} \setminus \{0\}$ and ϕ is subjective, there exists $a \in \mathbb{Q}$ such that $\phi(a) = 2$. Now, $\phi(a) = \phi\left(\frac{a}{2} + \frac{a}{2}\right) = \phi\left(\frac{a}{2}\right)\phi\left(\frac{a}{2}\right)$. Thus, $\phi\left(\frac{a}{2}\right)^2 = 2$. Hence $\phi\left(\frac{a}{2}\right) = \sqrt{2} \notin \mathbb{Q}$. This is a contradiction. Hence $(\mathbb{Q}, +)$ and $(\mathbb{Q} \setminus \{0\}, \cdot)$ are not isomorphic.

4.3.2 Automorphisms

Example 4.3.16

Let G be a finite abelian group of order n. Let $\phi_m : G \to G$ be the m-power map $\phi_m(g) = g^m$. Then

1. Show that ϕ_m is a homomorphism.
2. Show that $ker(\phi_m) = \{g \in G \mid g^d = e, d = gcd(m.n)\}$.
3. If m and n are relatively prime, then show that ϕ_m is an automorphism.

Definition:

$Aut(G)$ is defined as the set of all automorphisms of a group G.

Note

The identity homomorphism $1_G \in Aut(G)$.

Theorem 4.3.8

Let G be a group. Then $Aut(G)$ forms a group under the composition of functions.

Example 4.3.17

Let G be a group and let $a \in G$ then show that $\sigma_a : G \to G$ defined by $\sigma_a(g) = aga^{-1}$is an isormorphism.

Solution

Let $g, g' \in G$, consider

$$\begin{aligned}\sigma_a(g)\sigma_a(g') &= aga^{-1}ag'a^{-1} \\ &= ageg'a^{-1} \\ &= a(gg')a^{-1} \\ &= \sigma_a(gg')\end{aligned}$$

Thus, σ_a is a homomorphism. Now we will show that σ_a is bijective. Let $g, g' \in G$ such that $\sigma_a(g) = \sigma_a(g')$. We will show that $\sigma_a(g) = \sigma_a(g') \implies g = g'$.

$$\begin{aligned}\sigma_a(g) &= \sigma_a(g') \\ aga^{-1} &= ag'a^{-1} \\ a^{-1}aga^{-1}a &= a^{-1}ag'a^{-1}a \\ ege &= eg'e \\ g &= g'\end{aligned}$$

Hence, σ_a is injective. Now, let $h \in G$, we will show that $\exists\ g \in G$ such that $\sigma_a(g) = h$. Let $g = a^{-1}ha$, then

$$\begin{aligned}\sigma_a(g) &= aga^{-1} \\ &= a(a^{-1}ha)a^{-1} \\ &= ehe \\ &= h\end{aligned}$$

Thus, σ_a is a surjective homomorphism. Hence $\sigma_a : G \mapsto G$ is an isomorphism.

Definition:

An inner automorphism of a group G is defined as, $h_a : G \to G, a \in G,\ h_a(x) = axa^{-1}, \forall x \in G$.

$Inn(G) = \{h_a : G \to G \mid h_a(x) = axa^{-1}, a, x \in G\}$, is the set of all inner automorphisms of a group G

Theorem 4.3.9

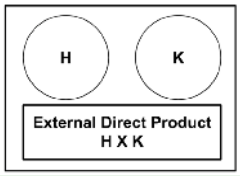
Let G be a group. Then $Inn(G) \leq Aut(G)$.

4.3: Homomorphisms is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

4.4: On Special Groups

4.4.0.0.1 External Direct Product

Definition:



Let $(G,\star)$ and $(G,\diamond)$ be groups.

Then the external direct product is defined by $G_1 \times G_2 = \{(g_1,g_2)|g_1 \in G_1, g_2 \in G_2\}$. $(g_1,g_2)(h_1,h_2) = (g_1 \star h_1, g_2 \diamond h_2)$.

Example 4.4.1

Consider the following

$(\mathbb{Z}_2 \times \mathbb{Z}_2, + \pmod 2)$.

Cayley Table $(\mathbb{Z}_2 \times \mathbb{Z}_2, + \pmod 2)$

$+ \pmod 2$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Notice that $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$, and every element which is not the identity has order 2. Therefore, the abelian group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not isomorphic to the cyclic group $\mathbb{Z}_4$.

Note

If you have many groups $G_i, i = 1, \cdots n$, then the external direct product can be written as $\prod_{i=1}^{n} G_i$.

Example 4.4.1

Consider the following:

$(\mathbb{Z}_2 \times \mathbb{Z}_3, +(mod 6))$.

$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$.

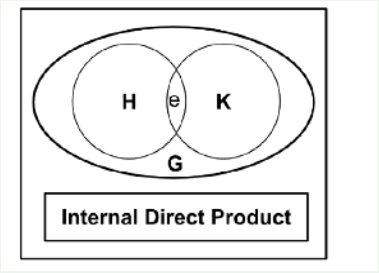
Notice that $(1,1)^6 (mod\ 2) = (0,0)$. Therefore $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle(1,1)\rangle$. Hence $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group of order 6. Therefore, $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

Theorem 4.4.1

The group $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ iff $gcd(m,n) = 1$.

4.4.0.0.1 Internal Direct Product

Definition:



Let G be a group with subgroups H and K, with the following conditions satisfied:

1. $H \leq G$ and $K \leq G$.
2. $G = HK = \{hk | h \in H, k \in K\}$
3. $H \cap K = \{e\}$.
4. $hk = kh,\ \forall h \in H,\ k \in K$.

Then we say that G is the internal direct product of H and K.

Example 4.4.1

$H = \{1, 3\}$, $K = \{1, 5\}, G = U(8) = \{1, 3, 5, 7\}$. Is $G = HK$?

Yes.

Proof:

Let $H = \{1, 3\}, K = \{1, 5\}, G = U(8) = \{1, 3, 5, 7\}$.

We will show $H \leq G$ and $K \leq G$.

$H \subseteq G, e_H = e, ab^{-1} \in H$ thus $H \leq G$.

Similarly, $K \leq G$.

$H \cap K = \{e\}$ by inspection.

We will show $hk = kh,\ \forall h \in H, k \in K$.

Consider $1 \cdot 1 = 1 \cdot 1 = 1 \in G$

$1 \cdot 5 = 5 \cdot 1 = 5 \in G$

$3 \cdot 1 = 1 \cdot 3 = 3 \in G$

$3 \cdot 5 = 5 \cdot 3 = 7 \in G$

Thus $G = HK$.□

Example 4.4.2

Let $G = D_6 = \langle r, s | r^6 = e, s^2 = e, r^{-1}sr = s^{-1} \rangle$.

Let $H = \{e, r^3\}$, $K = \{e, r^2, r^4, s, r^2s, r^4s\}$.

Is $G = HK$?

$H \leq G$ and $K \leq G$.

$H \cap K = \{e\}$.

By inspection, $hk = kh, \forall k \in K, h \in H$.

Thus $G = HK$.

4.4: On Special Groups is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

4.5: Isormormophism theorems

An isomorphism between two groups is a bijective mapping between two groups that preserves the group structure.

Definition: Isormorphism

Let G and H be groups. Let $\phi : G \to H$.

An isomorphism from G to H is a function $\phi : G \to H$ that satisfies the following two properties:

1. **Homomorphism property**: For any $g_1, g_2 \in G$, the operation in H corresponding to $\phi(g_1)$ and $\phi(g_2)$ is the same as the operation in G corresponding to g_1 and g_2. In other words, $\phi(g_1 g_2) = \phi(g_1) \cdot \phi(g_2)$, where $\cdot$ represents the group operation.
2. **Bijective property**: The function ϕ is one-to-one (injective) and onto (surjective), meaning that every element in H is the image of exactly one element in G under ϕ.

If an isomorphism exists between two groups G and H, we say that G and H are isomorphic, denoted by $G \cong H$. This means the two groups have the same group structure, even though their elements and operation symbols may differ.

Isomorphisms are significant in mathematics because they establish a correspondence between different groups, allowing us to understand the structure and properties of one group by studying the properties of another group.

Recall: The kernel of ϕ, denoted by $\mathbf{Ker}(\phi)$, is defined as the set of elements in G that map to the identity element of H. the image of ϕ is the set of all values that ϕ takes on as it maps elements from G to H, denoted by $\mathbf{Im}(\phi) == \{\phi(g) \mid g \in G\}$.

Theorem 4.5.1: First isomorphism Theorem

Let G and H be groups. Let $\phi : G \to H$ be a group homomorphism. Then, the factor group $G/\mathbf{Ker}(\phi)$ is isomorphic to the image of G, under ϕ, $\mathbf{Im}(\phi)$. That is, $G/\mathbf{Ker}(\phi) \cong \mathbf{Im}(\phi)$

Example 4.5.1

Consider the groups $G = (\mathbb{Z}, +)$ (the group of integers under addition) and $H = (\mathbb{Z}/4\mathbb{Z}, +4)$ (the group of integers modulo 4 under addition modulo 4). Define the homomorphism$\varphi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ as$\varphi(x) = x \mod 4$.

The kernel ofφ is$\mathbf{Ker}(\varphi) = x \in \mathbb{Z}, \mid, \varphi(x) = 0 = x \in \mathbb{Z}, \mid, x \mod 4 = 0 = 4\mathbb{Z}$ (the subgroup of multiples of 4).

By applying the First Isomorphism Theorem, we have$G/\mathbf{Ker}(\varphi) \cong \mathbf{Im}(\varphi)$. In this case,$G/\mathbf{Ker}(\varphi)$ is isomorphic to the image of$G$ underφ.

Using the theorem, we find that$G/\mathbf{Ker}(\varphi) \cong H$, which means$(\mathbb{Z}/4\mathbb{Z}, + \pmod 4)$ is isomorphic to itself.

Theorem 4.5.2: Second isomorphism Theorem

Let G be a group,H and$K$ be subgroups of G such that $H \leq G$. Then, the set $HK = \{hk, \mid, h \in H, k \in K\}$ is a subgroup of$G$, and $H \cap K$ is a normal subgroup of$H$. Moreover, the factor group$(HK)/(H \cap K)$ is isomorphic to$K/(H \cap K)$.

That is, $(HK)/(H \cap K) \cong K/(H \cap K)$

Example 4.5.2

Consider the group $G = (\mathbb{Z}, +)$ (the group of integers under addition). Let $H = (2\mathbb{Z}, +)$ be the subgroup of even integers, and $K = (3\mathbb{Z}, +)$ be the subgroup of multiples of 3.

In this case, H and K are both normal subgroups of G.

By applying the Second Isomorphism Theorem, we have $(HK)/(H \cap K) \cong K/(H \cap K)$. Here, $(HK)/(H \cap K)$ is isomorphic to $K/(H \cap K)$.

Using the theorem, we find that $(2\mathbb{Z} + 3\mathbb{Z})/(2\mathbb{Z} \cap 3\mathbb{Z}) \cong (3\mathbb{Z})/(2\mathbb{Z} \cap 3\mathbb{Z})$.

In this example, $(2\mathbb{Z} + 3\mathbb{Z})/(2\mathbb{Z} \cap 3\mathbb{Z})$ represents the set of all integers that are divisible by both 2 and 3, which is equivalent to $(6\mathbb{Z})/(6\mathbb{Z}) = 0$ (the trivial group). Similarly, $(3\mathbb{Z})/(2\mathbb{Z} \cap 3\mathbb{Z})$ represents the set of all integers that are divisible by 3 but not divisible by 2, which is isomorphic to $(\mathbb{Z}/3\mathbb{Z}, +3)$ (the group of integers modulo 3 under addition modulo 3).

Therefore, we conclude that $0 \cong \mathbb{Z}/3\mathbb{Z}$.

Theorem 4.5.3: Third isomorphism Theorem

Let G be a group, and let N and M be normal subgroups of G, with $N \leq M$. Then, the factor group M/N is isomorphic to a subgroup of G/N.

That is, $M/N \cong (M/N)/(N/N)$

Example 4.5.3

Consider the group $G = (\mathbb{Z}, +)$ (the group of integers under addition). Let $N = (6\mathbb{Z}, +)$ be the normal subgroup of multiples of 6, and $M = (9\mathbb{Z}, +)$ be the normal subgroup of multiples of 9.

In this case, $N \leq M$.

By applying the Third Isomorphism Theorem, we have $M/N \cong (M/N)/(N/N)$.

Using the theorem, we find that $(9\mathbb{Z})/(6\mathbb{Z}) \cong (9\mathbb{Z}/6\mathbb{Z})/(6\mathbb{Z}/6\mathbb{Z})$.

The factor group $(9\mathbb{Z})/(6\mathbb{Z})$ represents the set of all integers that are multiples of 9, modulo 6. This is isomorphic to $(\mathbb{Z}/6\mathbb{Z}, +6)$ (the group of integers modulo 6 under addition modulo 6).

Similarly, $(9\mathbb{Z}/6\mathbb{Z})/(6\mathbb{Z}/6\mathbb{Z})$ represents the set of cosets of $(6\mathbb{Z}/6\mathbb{Z})$ within $(9\mathbb{Z}/6\mathbb{Z})$. Since $(6\mathbb{Z}/6\mathbb{Z})$ is the trivial group, there is only one coset, which is $6\mathbb{Z}$.

Therefore, we conclude that $\mathbb{Z}/6\mathbb{Z} \cong 6\mathbb{Z}$ (the trivial group).

4.5: Isormormophism theorems is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

4.6: Classification of Groups

4.6.0.1 Classification of finite groups

The following table gives the number of distinct groups of finite order. Here C_n stands for a cyclic group of order n.

Group order	**Abelian**	**Non-abelian**	Comments
1	{e}		
2	$C_2 = D_1$		Prime p
3	C_3		Prime p
4	C_4 or $C_2 \times C_2 \cong D_2 \cong K_4$		Order of the form p^2
5	C_5		
6	C_6	$S_3 \cong D_3$	Order of the form pq, p, q are prime with $q \equiv 1 mod p$
7	C_7		
8	C_8 or $C_2 \times C_4$ or $C_2 \times C_2 \times C_2$	D_4 or Q_8	p^3
9	C_9 or $C_3 \times C_3$		p^2
10	C_{10}	D_5	
11	C_{11}		
12	C_{12}	D_6 or A_4	
13	C_{13}		
14	C_{14}	D_7	
15	C_{15}		
16	C_{16} or		
17	C_{17}		

This page titled 4.6: Classification of Groups is shared under a CC BY-NC-SA license and was authored, remixed, and/or curated by Pamini Thangarajah.

4E: Exercises

Exercise $4E.1$

Find the number of inner automorphisms of D_4.

$D_4 = \{1, r, r^2, r^3, s, rs, r^2s, r^3s\}$.

Exercise $4E.2$

Find two groups G_1 and G_2 such that $G_1 \ncong G_2$, but $\text{Aut}(G_1) \equiv \text{Aut}(G_2)$.

Exercise $4E.3$

Prove or disprove $U(5) \equiv \mathbb{Z}_4$.

Exercise $4E.4$

Find the five non-isomorphic groups of order 8.

Exercise $4E.5$

Prove or disprove: S_4 is isomorphic to D_{12}.

Exercise $4E.6$

Check the following structures for isomorphism.

1. $\mathbb{Z}_4$ under addition.
2. $\mathbb{Z}_5^*$ under multiplication.
3. $\mathbb{Z}_8^*$ under multiplication.
4. $\{\pm 1, \pm i\}$ under multiplication.
5. Rotations that map a brick to itself.
6. The four functions $f(x) = x, g(x) = -x, h(x) = \dfrac{1}{x}, j(x) = \dfrac{-1}{x}$ under composition.
7. The four matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \tag{4E.1}$$

Under multiplication.

Exercise $4E.7$

Let $G = \langle a \rangle$ and $|a| = 6$. Define a mapping $\phi : G \to G$ by $\phi(g) = g^2$ for all $g \in G$..

1. Show that ϕ is a homomorphism.
2. Find $Ker(\phi)$.
3. Find $Im(\phi)$.

4E: Exercises is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

Chapter 5: Rings and fileds

This page titled Chapter 5: Rings and fileds is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

5.1: Introduction to Rings

Recall a group is a set with a binary operation; rings are algebraic structures similar to groups but with two operations instead of one.

Definition: Ring

A non-empty set R with two binary operations, addition and multiplication - denoted by $+$ and $\cdot$, is called a **ring** if:

1. $(R,+)$ is an abelian group .
2. $(R,\cdot)$ is a semigroup: $a\cdot b\in R,\ \forall a,b\in R$ and $a\cdot(b\cdot c)=(a\cdot b)\cdot c,\ \forall a,b,c\in R.$ R in this context is a ring.
3. Multiplication distributes over addition: $a\cdot(b+c)=a\cdot b+a\cdot c$ and $(b+c)\cdot a=b\cdot a+c\cdot a,\ \forall a,b,c\in R.$ (Distributive property).

Note

We call the additive identity 0 is zero. The additive inverse is called the negative element.

$\{0\}$ is a ring called zero ring.

In this chapter, we will denote $a\cdot b$ as ab (skipping the $\cdot$ notation).

Definition: Commutative Ring

A ring $(R,+,\cdot)$ is called a **commutative ring** if $ab=ba,\ \forall a,b\in R.$

Definition: Unity

A ring $(R,+,\cdot)$ has a **unity(identity)** $e\in R$ if $ae=ea=a,\ \forall a\in R.$ Note unity is always a unique, single element.

Definition: Unit

An element $a\in R$ is called a **unit** if there exists an $a^{-1}\in R$ s.t. $aa^{-1}=e$.

Example 5.1.1

1. $(\mathbb{Z},+,\cdot)$ is a commutative ring with unity 1.
2. $(\mathbb{Z}_n,\oplus,\odot)$ (modulo n addition and multiplication) is a commutative ring with unity 1 and units of $U(n)$ since they must be all the elements relatively prime to n.
3. $(\mathbb{Z}_{[x]},+,\cdot)$ where $\mathbb{Z}_{[x]}$ is the set of all integer polynomials in variable x, is a commutative ring with unity of 1 and units of ± 1.
4. $(M_{22}(\mathbb{Z}),+,\cdot)$ is a ring, from the set of all 2×2 matrices with integer entries, that has unity I. It is a non-commutative ring. The units are the set of all 2×2 matrices with a non zero determinant $(GL_2(\mathbb{Z}))$.
5. $(\mathbb{Q},+,\cdot)$ is a field.It is a commutative ring with unity 1 and each $a\in\mathbb{Q}\setminus\{0\}$ is a unit.
6. $(\mathbb{R},+,\cdot)$ is a field. It is a commutative ring, and inverses exist for all elements except 0.
7. $(\mathbb{C},+,\cdot)$ is also a field, and inverses exist for all elements except 0.
8. A polynomial ring $R[x]$ over a ring R is defined as $\{(p(x)=a_0+a_1x+\cdots+a_nx^n\mid n\in\mathbb{Z},n\geq 0,a_i\in R,\forall i=1,\cdots,n\}$. Where a_i is the coefficient of x^i, also called the coefficients of the polynomial, and the non-negative integer n is called the degree of the polynomial.

The coefficients a_i can be elements from any ring, such as integers, rational numbers, real numbers, complex numbers, or even other polynomials. The addition and multiplication of $R[x]$ are the addition and multiplication R.

5.1.1 Integral Domain (ID)

Recall: $(R, +, \cdot)$ is a non-empty set with closed binary operations.

$(R, +)$ is abelian.

$(R, \cdot)$ is a semigroup. Recall that this is a set with an associative operation and no identity.

$(R, +, \cdot)$ is distributive, has unity (aka identity) of 1 and unit of $aa^{-1} = e$

If $ab = ba$, the ring is commutative on $\cdot$.

Definition: Integral Domain

A commutative ring with unity (aka identity), R, is called an **integral domain** if for every $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.

Example 5.1.2

Examples of non-integral domains:

1. In the ring $\mathbb{Z}_6$ (integers modulo 6), $2 \cdot 3 = 6 \equiv 0 \pmod 6$, but neither 2 nor 3 is zero in $\mathbb{Z}_6$.

2. In the ring $(M_{22}(\mathbb{Z}), +, \cdot)$;

$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, but neither $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ nor $\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ equal zero.

Definition: Division Ring

A **division ring** is a ring, (R), with an identity in which for every non-zero $a \in R$, there exists $b \in R$ s.t. $ab = 1 = ba$.

Example 5.1.3

Examples of division rings:

$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$, $\mathbb{Z}_p$, where p is prime.

Definition: Field

A **field** is a commutative division ring.

Example 5.1.4

Examples of fields are: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $\mathbb{Z}_p$, where p is prime,

and $(\mathbb{C}, +, \cdot)$, with the later being algebraically closed.

Definition: Zero divisor

A non-zero element of $a \in R$ is called a zero divisor if there exists $ab \in R$ s.t. $ab = 0$.

Example 5.1.5

$(\mathbb{Z}, +, \cdot)$.

Since there are no zero divisors, it is an integral domain. It is a commutative ring. Not every non-zero element is a unit. Thus, it is not a field.

Example 5.1.6

$(\mathbb{Z}_n, \oplus, \odot)$.

There are two cases.

This is a finite field if n is prime.

If n is not prime, it is not an integral domain since it will have a zero divisor.

Example 5.1.7

The set of all real-valued differentiable functions on $[a, b]$ is a commutative ring with a unit. This area of study is called differential algebra.

Example 5.1.8

$M_{22}(\mathbb{R}, +, \cdot))$.

The addition is abelian. It is not commutative. It has an identity. It's not an integral domain.

This area of study is called matrix algebra.

Example 5.1.9

Let

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}.$$

In other words, $I^2 = J^2 = K^2 = IJK = -1$.

Define

$\mathbb{H} = \{a + bI + cJ + dK \mid a, b, c, d \in \mathbb{R}\}$. Then $\mathbb{H}$ is Ring of Quaternions which is a division ring but not a field.

* discovered by Hamilton in 1843.

Example 5.1.10

Let

$$\mathbb{H} = \left\{ \begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix} \mid a, b \in \mathbb{C} \right\}.$$

Then $\mathbb{H}$ is a division ring with matrix addition and multiplication, but not an integral domain.

5.1.2 Properties of Rings

Theorem 5.1.1: Cancellation Law

Let D be a commutative ring with identity. Then D is an integral domain if and only if $ab = bc$ implies $b = c \; \forall a, b, c \in D$.

Theorem 5.1.2

Let $(R, +, \cdot)$ be a ring and $a, b \in R$.

1. $a0 = 0 = 0a$.
2. $a(-b) = (-a)b = -ab$.
3. $(-a)(-b) = (ab)$.

Answer

1. Let $a \in R$. Then $0a = (0 + 0)a = 0a + 0a. \implies 0a + 0 = 0a + 0a$. By cancellation law of $+$, we get $0a = 0$. Similarly, we can show that $a0 = 0$.
2. Let $a, b \in R$. Then $ab + (-a)b = (a + (-a))b = 0b = 0. \implies (-a)b = -(ab)$. Similarly, $ab + a(-b) = a(b + (-b)) = a0 = 0. \implies a(-b) = -(ab)$.

5.1.3 **Subring**:

Let $(R, +, \cdot)$ be a ring.

Let $S(\neq 0) \subseteq R$.

Then S is a subring of R if $(S, +, \cdot)$ is a ring with the same operations.

Theorem 5.1.3

Subring Test

Let $(R, +, \cdot)$ be a ring.

$S \subseteq R$ is a subring if and only if the following conditions are satisfied:

1. $S \neq \{\}$. At least $0 \in S$.
2. $a - b \in S$.
3. $ab \in S, \; \forall a, b \in S$.

Example 5.1.11

Let $(R, +, \cdot)$ be a ring then $\{0\}$ and R are subrings of R and are called the trivial subrings of R.

Example 5.1.12

Let $(\mathbb{Q},+,\cdot)$ is a subring of $(\mathbb{R},+,\cdot)$ and $(\mathbb{R},+,\cdot)$ is a subring of $(\mathbb{C},+,\cdot)$.

Example 5.1.13

$(\mathbb{Z}_6,\oplus,\odot)$ is a ring.

1. Let $S=\{0,3\}$.

Clearly, S is non-empty.

Since $0\oplus 3$, $0\oplus 0$, and $3\oplus 3$, $a-b\in S$.

Since $0\odot 3$, $0\odot 0$, and $3\odot 3$, then $ab\in S$.

Thus S is a subring of $(\mathbb{Z}_6,\oplus,\odot)$.

2.

Let $T=\{0,2,4\}$.

Clearly, T is non-empty.

Since $0\oplus 0$, $0\oplus 2$, $0\oplus 4$, $2\oplus 2$,$2\oplus 4$ and $4\oplus 4\in T$ then $a-b\in T$

Since $0\odot 0$, $0\odot 2$, $0\odot 4$, $2\odot 2$, $2\odot 4$, and $4\odot 4\in T$, then $ab\in T$.

Thus T is a subring of $(\mathbb{Z}_6,\oplus,\odot)$.

Example 5.1.14

Define $\mathbb{Z}[i]=\{m+ni|m.n\in\mathbb{Z}\}$, where $i^2=-1$.

This is a ring called **Gaussian integers**. The units of this ring are ± 1 and $\pm i$. Hence The ring of Gaussian integers is not a field.This is a subring of $(\mathbb{C},+,\cdot)$.

Theorem 5.1.4: Wedderburn's Theorem

Every finite integral domain is a field.

Answer

Let D be a finite integral domain.

Let $D^*=D\backslash\{0\}$.

We shall show that every element in D^* is a unit (i.e., $aa^{-1}=e,\ \forall a\in D^*$).

Let $a\in D^*$.

Define $\lambda_a: D^*\to D^*$ by $\lambda_a(x)=ax,\ x\in D^*$.

We shall show that λ_a is injective.

Let $x_1,x_2\in D^*$ s.t. $\lambda_a(x_1)=\lambda_a(x_2)$.

Consider $ax_1=ax_2$.

Thus $ax_1-ax_2=0$.

So $a(x_1-x_2)=0$.

Since D is an integral domain, either $a = 0$ or $(x_1 - x_2)$=0\).\)

Since D^* excludes zero, $a \neq 0$.

Thus $x_1 - x_2 = 0$.

Hence $x_1 = x_2$ and λ_a is injective.

Since D and D^* are finite, λ_a is surjective.

Since $1 \in D^*$, $\exists x \in D^*$ s.t. $\lambda_a(x) = 1$.

Thus, a is a unit, and therefore, it is a field

5.1.4 Characteristic of a ring R

Definition: Characteristic

Let $r \in R$, then $r + r = 2r, r + r + r = 3r, \cdots, r + \cdots + r = nr$.

The characteristic of a ring R is the least positive integer n such that $nr = 0, \forall r \in R$. If no such n exists, we say that the characteristic of ring R is 0.

Example 5.1.15

1. $(\mathbb{Z}, +\cdot), (\mathbb{Q}, +\cdot), (\mathbb{R}, +\cdot), (\mathbb{C}, +\cdot)$ are rings of characteristic 0.
2. $(\mathbb{Z}_6, \oplus, \odot)$ is a ring of characteristic 6.

Theorem 5.1.5

1. Let R be ring with identity 1. If n is the least positive integer such that $n1 = 0$, then the characteristic of ring R is 0.
2. The characteristic of an integral domain is either prime or 0.

This page titled 5.1: Introduction to Rings is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

5.2: Ideals and Factor Rings

Ideals:

Definition: Ideal

Let R be a ring. Then a subring I of R is called an **ideal** of R, denoted $I \lhd R$, if $ar \in I$, and $ra \in I, \forall a \in I$ and $r \in R$.

That is $rI \subseteq I$ and $Ir \subseteq I$ for all $r \in R$.

Example 5.2.1

1. Triivial ideals of a ring R are $\{0\}$ and R.

Theorem 5.2.1

Let R be a commutative ring with unity, and let $a \in R$ then the set $\langle a \rangle = \{ar \mid r \in R\}$ is an ideal of R.

Proof

Since $0 \in \langle a \rangle$, $\langle a \rangle \backslash \text{empty}$. Let $r_1, r_2 \in R$. Then $ar_1, ar_2 \in \langle a \rangle$. Since $(r_1 - r_2), ar_1 r_2 \in \langle a \rangle, ar_1 - ar_2 = a(r_1 - r_2) \in langlea\rangle$ and $(ar_1)(ar_2) = a(ar_1 r_2) \in langlea\rangle$. Thus $\langle a \rangle$ is a subring of R. Clearly $r\langle a \rangle = \langle a \rangle r \subseteq \langle a \rangle$, for all $r \in R$. Hence, $\langle a \rangle = \{ar \mid r \in R\}$ is an ideal of R.

Definition:

Let R be a commutative ring with unity, and let $a \in R$ then $\langle a \rangle = \{ar \mid r \in R\}$ is called a **principal ideal generated by** a of R.

Example 5.2.2

Add example text here.

Solution

Add example text here.

Factor Rings

This page titled 5.2: Ideals and Factor Rings is shared under a not declared license and was authored, remixed, and/or curated by Pamini Thangarajah.

5.3: Ring Homomorphisms

5.3.0.1 Ring Homomorphisms

Definition: Ring homomorphisms

Let R, S be rings. A function $\phi : R \to S$ is called a ring homomorphism if

1. $\phi(a+b) = \phi(a) + \phi(b), \forall a, b \in R$, and
2. $\phi(ab) = \phi(a)\phi(b), \forall a, b \in R$.

If ϕ is bijective, then ϕ is called isomorphism.

Example 5.3.1

Show that the function $\phi : \mathbb{Z}_2 \to \mathbb{Z}_2$ defined by $\phi(x) = x^2, x \in \mathbb{Z}_2$ is a ring homomorphism.

Solution

Let $a, b \in i\mathbb{Z}_2$.

Consider $\phi(a+b) = (a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2 = \phi(a) + \phi(b)$.

Consider $\phi(ab) = (ab)^2 = a^2b^2 = \phi(a)\phi(b)$.

Hence, ϕ is a ring homomorphism.

Example 5.3.2

Whether or not the function $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(x) = 2x, x \in \mathbb{Z}$ is a ring homomorphism? Justify your answer.

Solution

Choose $a = 2$ and $b = 3$. Then $\phi(2) = 4$ and $\phi(3) = 6$, $\phi(a)\phi(b) = (4)(6) = 24$ but $\phi(ab) = \phi((2)(3)) = \phi(6) = 12 \neq \phi(a)\phi(b)$.

Hence, ϕ is not a ring homomorphism.

Definition: Kernel of a homomorphism

The kernel of ϕ is denoted and defined as $Ker(\phi) = \{r \in R | \phi(r) = 0\}$.

Example 5.3.3

Define $\phi : \mathbb{Z} \to \mathbb{Z}_n$ by $\phi(a) = a(modn), \forall a \in R$.

Then ϕ is a ring homomorphism but not an isomorphism. In this case, $Ker(\phi) = n\mathbb{Z}$.

5.3.1 Properties of ring homomorphisms:

Theorem 5.3.1

Let R, S be rings. Let $\phi : R \to S$ be a ring homomorphism. Then,

Then

1. $\phi(0) = 0$.
2. if R is a commutative ring, then $\phi(R)$ is also a commutative ring.
3. if R is a field and $\phi(R) \neq \{0\}$ then $\phi(R)$ is also a field.

4. if R and S have an identity. If ϕ is onto then $\phi(1_R) = 1_S$.

5.3.2 Theorem 5.3.2

Let R, S be rings. Let $\phi : R \to S$ be a ring homomorphism. Then $Ker(\phi)$ is an ideal of R.

5.3.3

This page titled 5.3: Ring Homomorphisms is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

5E: Excercises

Exercise $5E.1$

1. Prove or disprove: Every finite integral domain is a field.
2. Prove or disprove: Every division ring is an integral domain.

Exercise $5E.2$

List or characterize all of the units in each of the following rings.

1.

Exercise $5E.3$

Prove or disprove: $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$ is an integral domain.

Exercise $5E.4$

p be a prime. Prove that $\mathbb{Z}_{(p)} = \{a/b | a, b \in \mathbb{Z} \, and \, \gcd(b, p) = 1\}$ is a ring.

Exercise $5E.5$

Let R be a ring. If $ab + ba = 1$ and $a^3 = a$, $\forall a, b \in R$, then show that $a^2 = 1$.

Exercise $5E.6$

Show that $\mathbb{Q}(\sqrt{5}i) = \{r + s\sqrt{5}i : r, s \in \mathbb{Q}\}$ is a subfield of $\mathbb{C}$.

Exercise $5E.7$

An element e of a ring R is said to be **idempotent** if $e^2 = e$.

1. Find all idempotents in $\mathbb{Z}_{12}$.
2. Find all the idempotents in an integral domain R.
3. If $a^m = a^{m+n}, m, n \in \mathbb{N}$, show that some power of a is an idempotent.
4. If R is a finite ring, show that some power of each element of R is an idempotent.

Exercise $5E.8$

Show that the multiplication defined for the field of quotients of an integral domain:

1. Is well defined
2. Is associative
3. Satisfies the distributive laws.

Exercise $5E.9$

An element a of a ring R is said to be **nilpotent** if $a^n = 0$, for some $n \in \mathbb{N}$.

1. Find all nilpotents in $\mathbb{Z}_{12}$.
2. Find all the nilpotents in an integral domain R.

Exercise $5E.10$

Let $a, u \in R$. If u is a unit and a is nilpotent such that $ua = au$, show that $u + a$ is a unit.

This page titled 5E: Excercises is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

Mock Exams (Celebration of Learning)

Mock Exams (Celebration of Learning) is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

Sample final

These mock exams are provided to help you prepare for Term/Final tests. The best way to use these practice tests is to try the problems as if you were taking the test. Please don't look at the solution until you have attempted the question(s). Only reading through the answers or studying them, will typically not be helpful in preparing since it is too easy to convince yourself that you understand them.

Exercise 1

Consider the symmetric group S_7.

1. Factor the permutation $(12345)(67)(1357)(613)$ into disjoint cycles.
2. Identify all possible types of permutations and specify the quantity of each type.
3. Find the possible order of all the elements of S_7.
4. Show that S_7 is not abelian.

Exercise 2

1. Show that A_4 is normal to S_4.
2. What are the conjugacy classes of A_4?

Exercise 3

Consider $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ with $a^4 = e, b^2 = e, ba = a^3b$.

1. Show that $Z(D_4) = \{e, a^2\}$. (Hint: $Z(G) = \{x \in G | ax = xa, \forall a \in G\}$.)
2. List the left and right cosets of $Z(D_4)$, in D_4.

Exercise 4

1. Prove or disprove: $U(5)$ is isormorphic to $\mathbb{Z}_4$.
2. Prove or disporove: $\mathbb{Z}$ under addition is isormorphic to $\mathbb{Q}$ under addition.

Exercise 5

1. Show that 17 and 60 are relatively prime, determine the multiplicative inverse of $[17]$ in $\mathbb{Z}_{60}$.
2. Find all $x \in \mathbb{Z}$ satisfying the equation $17x \equiv 12 (mod\, 60)$.

Exercise 6

Let G be a group. Prove or disprove the following statements:

Let H and K be subgroups of the group G. Then

1. $H \cup K$ is a subgroup of G.
2. $H \cap K$ is a subgroup of G.

Exercise 7

Consider the group $\mathbb{Z}_{12}$ with addition modulo 12.

1. Is $(\mathbb{Z}_{12}, +mod(12))$ cyclic group? If so, what are the possible generators? How many distinct generators exist? What can you say about the number of generators, considering the Euler totient function and the possible generators in relation to divisors?
2. Let $G = \langle g \rangle$ be a cyclic group with $|g| = n$. Then $G = \langle g^k \rangle$ if and only if $gcd(k, n) = 1$.

3. Find all subgroups of $\mathbb{Z}_{12}$ generated by each element. What are their respective orders? What can you say about these orders?

Exercise 8

1. Let $G =< a >$ where $|a| = 12$, and let $H =< a^4 >$. Find all cosets in G/H and write down the Cayley table. Is G/H cyclic? Why or why not?
   Find the cosets in $D_6/Z(D_6)$, write down the Cayley table of $D_6/Z(D_6)$. Is $D_6/Z(D_6)$ cyclic, why or why not?
2. Prove or disprove the following statements: If H is a normal subgroup of G such that H and G/H are abelian, then G is abelian.

Exercise 9

An element e of a ring R is said to be idempotent if $e^2 = e$.

1. If e is an idempotent of a ring R, then show that $1 - 2e$ is a unit.
2. Find all idempotents in $\mathbb{Z}_{12}$.
3. Find all the idempotents in an integral domain R.

Exercise 10

List or characterize all of the following rings' units. Justify your answer.

1. $\mathbb{Z}_{12}$
2. $M_{22}(\mathbb{Z}_2)$
3. $\mathbb{Z}(i)$

Sample final is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

Test 1

These mock exams are provided to help you prepare for Term/Final tests. The best way to use these practice tests is to try the problems as if you were taking the test. Please don't look at the solution until you have attempted the question(s). Only reading through the answers or studying them will typically not be helpful in preparing since it is too easy to convince yourself that you understand them.

Exercise 1

Define a relation $\sim$ on $\mathbb{N}$ by:

$a \sim b$ if and only if $a^2 + b$ is even.

1. [4 marks] Prove that $\sim$ defines an equivalence relation.
2. [2 marks] What is the equivalence class of 3?

Answer

Add texts here. Do not delete this text first.

Exercise 2

1. [6 marks] Show that 17 and 60 are relatively prime, determine multuplicative inverse of $[17]$ in $\mathbb{Z}_{60}$.
2. [4 marks] Find all $x \in \mathbb{Z}$ satisfying the equation $17x \equiv 12 (mod\, 60)$.

Answer

Add texts here. Do not delete this text first.

Exercise 3

[5 marks] If $f \circ g$ is one-to-one then g is one-to-one.

[5 marks] If $f \circ g$ is one-to-one and g is onto, then f is one-to-one.

Answer

Add texts here. Do not delete this text first.

Exercise 4

1. [5 marks] Prove or disprove: $U(10)$ is cyclic group.
2. [5 marks] Show that $H = \{0, 2, 4, 6\}$ is a subgroup of $\mathbb{Z}_8$, using the operation $+ \mod (8)$.

Answer

Add texts here. Do not delete this text first.

Exercise 5

[10 marks] Let G be a group. Prove or disprove the following statements.

1. If G is abelian, then G is cyclic.
2. If G is cyclic, then G is abelian.

Test 1 is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

Test 2

These mock exams are provided to help you prepare for Term/Final tests. The best way to use these practice tests is to try the problems as if you were taking the test. Please don't look at the solution until you have attempted the question(s). Only reading through the answers or studying them will typically not be helpful in preparing since it is too easy to convince yourself that you understand them.

Exercise 1

Consider the symmetric group S_7.

1. Factor the permutation $(12345)(67)(1357)(613)$ into disjoint cycles.
2. Identify all possible types of permutations and specify the quantity of each type.
3. Find the possible order of all the elements of S_7.
4. Show that S_7 is not abelian.

Exercise 2

Consider the group $\mathbb{Z}_{12}$ with addition modulo 12.

1. Is $(\mathbb{Z}_{12}, +mod(12))$ cyclic group? If so, what are the possible generators? How many distinct generators exist? What can you say about the number of generators, considering the Euler totient function, and the possible generators in relation to divisors?
2. Let $G = \langle g \rangle$ be a cyclic group with $|g| = n$. Then $G = \langle g^k \rangle$ if and only if $gcd(k, n) = 1$.
3. Find all subgroups of $\mathbb{Z}_{12}$ generated by each element. What are their respective orders? What can you say about these orders?

Exercise 3

Consider the symmetric group S_4.

1. Find the centre of S_4.
2. If possible, find a cyclic subgroup of S_4 with an order of 4.
3. Find a non-cyclic subgroup of S_4 with order 4 if possible.

Exercise 4

Consider $\mathbf{Z}_8$ and the operation $+mod 8$.

1. Show that $H = \{0, 2, 4, 6\}$ is a subgroup of $\mathbf{Z}_8$.
2. List the left and right cosets of $H = \{0, 2, 4, 6\}$ in $\mathbf{Z}_8$.

Exercise 5

Consider $D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$ with $a^4 = e, b^2 = e, ba = a^3b$.

1. Show that $Z(D_4) = \{e, a^2\}$. (Hint: $Z(G) = \{x \in G | ax = xa, \forall a \in G\}$.)
2. List the left and right cosets of $Z(D_4)$, in D_4.

Test 2 is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

Sample Assignments with solution

Sample Assignments with solution is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

Assignment 1

Exercise 1

Determine whether or not each of the following binary relations R on the given set A is reflexive, symmetric, antisymmetric, or transitive. If a relation has a certain property, prove this is so; otherwise, provide a counterexample to show that it does not. If R is an equivalence relation, describe the equivalence classes of A.

Exercise 1

Define a relation R on $A = \mathbb{Z}$ by

$a\,R\,b$ if and only if $4 \mid (3a + b)$, for $a, b \in \mathbb{Z}$.

Answer

R is reflexive on $\mathbb{Z}$.

Proof:

Let $a \in \mathbb{Z}$.

We shall show that aRa, specifically $4|(3a + a)$.

Consider $3a + a = 4a$ and $a \in \mathbb{Z}$.

Thus $4|(3a + a)$, and aRa.

Therefore R is reflexive on $\mathbb{Z}$.□

R is symmetric on $\mathbb{Z}$.

Proof:

Let $a, b \in \mathbb{Z}$ s.t. $4|(3a + b)$.

Thus $3a + b = 4m$ for some $m \in \mathbb{Z}$.

We will show that $4 \mid 3b + a$.

Since $3a + b = 4m$, $-3a - b = -4m$.

Then $4(a + b) - 3a - b = 4(a + b) - 4m$.

Thus $3b + a = 4(a + b - m)$ where $a + b - m \in \mathbb{Z}$.

Hence $4|(3b + a)$. Hence bRa.

Thus R is symmetric on $\mathbb{Z}$.

R is not antisymmetric on $\mathbb{Z}$.

Counterexample:

Let $a = 0$ and $b = 4$.

Then $4|(3(0) + 4)$ and $4|(3(4) + 0)$. Thus $4R0$ and $0R4$

However, since $0 \neq 4$ R is not antisymmetric on $\mathbb{Z}$.□

R is transitive on $\mathbb{Z}$.

Proof:

Let $a, b, c \in \mathbb{Z}$ s.t. aRb and bRc.

Since aRb, $4|(3a+b)$ and bRc, $5|(3b+c)$.

We will show that aRc, that is $4|(3a+c)$.

Since $4|(3a+b)$, $3a+b=4(k)$ for some $k \in \mathbb{Z}$.

Since $4|(3b+c)$, $3b+c=4(m)$ for some $m \in \mathbb{Z}$.

Consider

$$\begin{aligned} 3a+c &= (3a+b)+(3b+c)-4b \\ &= 4(k)+4(m)-(b) \\ &= 5(k+m-b), \end{aligned}$$

where $k+m-b \in \mathbb{Z}$.

Hence $4|3a+c$. Thus aRc.

Hence R is transitive on $\mathbb{Z}$.□

Since R is reflexive, symmetric and transitive on $\mathbb{Z}$, R is an equivalence relation.

Te equivalence classes of aRb iff $4|(3a+b)$ are $[0], [1], [2]$ and $[3]$.

Let $a \in \mathbb{Z}$, then $[a] = \{a \in \mathbb{Z} : x \sim a\}$.

$$\begin{aligned} [0] &= \{x \in \mathbb{Z} : x \sim 0\} \\ &= \{x \in \mathbb{Z} : 4|(3x+(0))\} \\ &= \{x \in \mathbb{Z} : 4|3x\} \\ &= \{x \in \mathbb{Z} : 3x = 4m, m \in \mathbb{Z}\} \\ &= \{\ldots, -8, -4, 0, 4, 8, \ldots\}. \end{aligned}$$

$$\begin{aligned} [1] &= \{x \in \mathbb{Z} : x \sim 1\} \\ &= \{x \in \mathbb{Z} : 4|(3x+(1))\} \\ &= \{x \in \mathbb{Z} : 4|(3x+1)\} \\ &= \{x \in \mathbb{Z} : 3x+1 = 4m, m \in \mathbb{Z}\} \\ &= \{x \in \mathbb{Z} : 3x = 4m-1, m \in \mathbb{Z}\} \\ &= \{\ldots, -7, -3, 1, 5, 9, \ldots\}. \end{aligned}$$

$$\begin{aligned} [2] &= \{x \in \mathbb{Z} : x \sim 2\} \\ &= \{x \in \mathbb{Z} : 4|(3x+2)\} \\ &= \{x \in \mathbb{Z} : 3x+2 = 4m, m \in \mathbb{Z}\} \\ &= \{x \in \mathbb{Z} : 3x = 4m-2, m \in \mathbb{Z}\} \\ &= \{\ldots, -6, -2, 2, 6, 10, \ldots\}. \end{aligned}$$

$$\begin{aligned} [3] &= \{x \in \mathbb{Z} : x \sim 3\} \\ &= \{x \in \mathbb{Z} : 4|(3x+3)\} \\ &= \{x \in \mathbb{Z} : 3x+3 = 4m, m \in \mathbb{Z}\} \\ &= \{x \in \mathbb{Z} : 3x = 4m-3, m \in \mathbb{Z}\} \\ &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}. \end{aligned}$$

Exercise 2

Define a relation R on $A = \mathbb{N}$ by $a\,R\,b$ if and only if $2 \mid a^2 + b$, for $a, b \in \mathbb{N}$.

Answer

Proof of Reflexivity:

Let $a \in \mathbb{N}$.

We shall show that $a^2 + a = 2m, m \in \mathbb{Z}$.

We can show this directly or using cases:

Directly:

Since $a^2 + a = a(a + 1)$, and $a, a + 1$ are consecutive integers,

$a^2 + a$ is even. Thus R is reflexive on $\mathbb{N}$.

Proof of Symmetry:

Let $a, b \in \mathbb{N}$ such that aRb.

That means $a^2 + b = 2m, m \in \mathbb{Z}$.

We will show that $b^2 + a = 2k, k \in \mathbb{Z}$.

Since

$a^2 = 2m - b$, $b^2 + a = (2m - a^2)^2 + a = 4m^2 - 4ma^2 + a^4 + a$.

Thus

$b^2 + a = 2(2m^2 - 2ma^2) + a(a^3 + 1) = 2(2m^2 - 2ma^2) + a(a + 1)(a^2 - a + 1)$.

Since a(a+1) is even, $b^2 + a$ is even.

Thus R is symmetric on $\mathbb{N}$.

Antisymmetry:

Caution: $0 \notin \mathbb{N}$.

Let $a = 1, b = 3$.

$1^2 + 3 = 2(2)$, and $3^2 + 1 = 2(5)$

But $1 \neq 3$, hence, R is \textbf{not} antisymmetric on $\mathbb{N}$.

Proof of Transitivity:

Let$a, b, c \in \mathbb{N}$ such that $2|a^2 + b$ and$2|b^2 + c$.

We will show that $2|a^2 + c$.

Consider $a^2 + b = 2m, m \in \mathbb{Z}$ and $b^2 + c = 2n, n \in \mathbb{Z}$.

Further, consider that $a^2 + c = 2m - b + 2n - b^2 = 2(m + n) - (b^2 + b)$.

Since R is reflexive on $\mathbb{N}$, $b^2 + b = 2q, q \in \mathbb{Z}$

Thus $a^2 + c = 2(m + n - q), m, n, q \in \mathbb{Z}$.

Thus R is transitive on $\mathbb{N}$.

Having shown that R is reflexive, symmetric and transitive on $\mathbb{Z}$,R is an equivalence relation on $\mathbb{Z}$.□

Let $a \in \mathbb{Z}$, then $[a] = \{x \in \mathbb{Z} : x \sim a\}$. **Caution:** $0 \notin \mathbb{N}$.

$a = 1$:

$$[1] = \{x \in \mathbb{Z} : x \sim 1\}$$
$$= \{x \in \mathbb{Z} : 2|(x^2 + 1)\}$$
$$= \{x \in \mathbb{Z} : x^2 + 1 = 2m, m \in \mathbb{Z}\}$$
$$= \{\pm 1, \pm 3, \cdots\}.$$

$a = 2$:

$$[2] = \{x \in \mathbb{Z} : x \sim 2\}$$
$$= \{x \in \mathbb{Z} : 2|(x^2 + 2)\}$$
$$= \{x \in \mathbb{Z} : x^2 + 2 = 2m, m \in \mathbb{Z}\}$$
$$= \{0, \pm 2, \pm 4, \cdots\}.$$

Exercise 3

Let $A = \mathbb{R} \times \mathbb{R}$. Define $(x, y)\, R\, (x_1, y_1)$ if and only if $x^2 + y^2 = x_1^2 + y_1^2$, for $(x, y), (x_1, y_1) \in \mathbb{R} \times \mathbb{R}$.

Answer

Reflexive

Proof:

Let $(a, b) \in \mathbb{R} \times \mathbb{R}$.

Since $a^2 + b^2 = a^2 + b^2$, $(a, b)\, R\, (a, b)$

Thus R is reflexive.

Symmetric:

Proof:

Let $(a, b), (a_1, b_1) \in \mathbb{R} \times \mathbb{R}$, s.t $(a, b) R (a_1, b_1)$

Thus $a^2 + b^2 = a_1^2 + b_1^2$

We shall show $b\, R\, a$.

Since $a^2 + b^2 = a_1^2 + b_1^2$, $a_1^2 + b_1^2 = a^2 + b^2$

Thus $(a_1, b_1)\, R\, (a, b)$, and R is symmetric.

antisymmetric:

Counterexample

let $a = 1, b = 2, a_1 = 2, b_1 = 1$

then $(1)^+(2)^2 = 5 = 2^2 + 1^2$

Thus $(a, b) R (a_1, b_1)$ and $(a_1, b_1)\, R\, (a, b)$

But $(1, 2) \neq (2, 1)$

Thus R is not anti-symmetric

Transitive:

Proof:

Let $(a, c), (a_1, c_1), (a_2, c_2) \in \mathbb{R} \times \mathbb{R}$ such that $(a, c) R (a_1, c_1)$ and $(a_1, c_1) R (a_2, c_2)$.

Since $(a,c)R(a_1,c_1)$, $a^2+b^2=a_1^2+b_1^2$.

Since $(a_1,c_1)R(a_2,c_2)$, $b^2+c^2=b_1^2+c_1^2$

Thus, $a^2+c^2=a_1^2+c_1^2$

Hence $(a,c)R(a_2,c_2)$ and R is transitive.

Since R is reflexive, symmetric and transitive, R is an equivalence relation on A.

The equivalence classes are

$[(0,0)]=\{(x_1,y_1)\in\mathbb{R}\times\mathbb{R}\mid x_1^2+y_1^2=0\}\{0\}$

$[(x,y)]=\{(x_1,y_1)\in\mathbb{R}\times\mathbb{R}\mid r^2=x_1^2+y_1^2=x^2+y^2\}$

Exercise 2

Consider the function $f:\mathbb{Z}\to\mathbb{Z}$ define by $f(n)=n^2+1$.

Determine whether f is one-to-one and whether f is onto. If f is not onto, find the range of f.

Answer

No, f is not injective.

Counterexample:

Let $x_1=-2$ and $x_2=2$.

Then $f(-2)=(-2)^2+4=8$ and $f(2)=(2)^2+4=8$.

Thus $f(-2)=f(2)$ but $-2\neq 2$.

Therefore h is not injective.□

No,h is not surjective.

Counterexample:

Let $A=\mathbb{Z}$ and $B=\mathbb{Z}$ s.t. $h:A\to B$ is defined by $f(x)=x^2+1$.

Note that $3\in B$.

Thus $3=x^2+1\implies x=\pm\sqrt{2}\notin A$.

Thus, f is not surjective. Range of $f=\{x^2+1\mid x\in\mathbb{Z}\}=\{1,2,5,10,17,26\cdots\}$.

Exercise 3

Suppose $f:B\to C$ and $g:A\to B$ are functions.

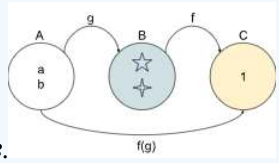
Prove or disprove the following statements:

1. If $f\circ g$ is onto then g is onto.
2. If $f\circ g$ is onto and f is one-to-one, then g is onto.

Answer

1. Let $A = \{a, b\}$, $B = \{\star, \times\}$, $C = \{1\}$.

Let $g(a) = \star$ and $g(b) = \star$.



Let $f(x) = 1$, for all $x \in B$.

We will show that $\forall a \in A$, s.t. $g(a) = b$, $\forall b \in B$.

Note that $f \circ g$ is surjective since $\forall c \in C$, $\exists a \in A$ s.t. $(f \circ g)(a) = c$.

However $\exists a \in A$ s.t. $g(a) = \star \in B$.

Thus g is not surjective.□

2. Proof:

Let $b \in B$.

We shall show that $g(A) = B$.

Since g is a function, $g(A) \subset B$ by definition of a function.

Since $f \circ g$ is surjective, $\exists a \in A$ s.t. $(f \circ g)(a) = c$, $c \in C$.

Thus $(f(g(a)) = c$.

Since f is injective, $f(b_1) = f(b_2), b_1, b_2 \in B$ means that $b_1 = b_2$.

Thus $\exists a \in A$ s.t $g(a) = b$, $\forall b \in B$.

Thus $B \subseteq g(A)$.

Since $g(A) \subset B$ and $B \subset g(A)$, $g(A) = B$.□

This page titled Assignment 1 is shared under a CC BY-NC-SA 4.0 license and was authored, remixed, and/or curated by Pamini Thangarajah.

Assignment 2

Exercise 1

1. Compute $gcd(-231, 150)$ and express it as a linear combination of -231 and 150.
2. Find $gcd(-231, 150)$ and $lcm(231, 150)$ using prime factorization.
3. Find Euler Totient function $\phi(150)$ and $\phi(231)$.

Answer

1.

$$\begin{aligned} -231 &= -2(150) + 69 \\ 150 &= 2(69) + 12 \\ 69 &= 5(12) + 9 \\ 12 &= 1(9) + 3 \\ 9 &= 3(3) + 0. \end{aligned}$$

Hence, $gcd(-231, 150) = 3$. By using Bezout's algorithm,

$$\begin{aligned} 3 &= 12(1) + (-9)(1) \\ &= 12(1) + (-69(1) + 12(5))(1) \\ &= 12(6) + (-69)(1) \\ &= (150(1) - 69(2))(6) + (-69)(1) \\ &= 150(6) + (-69)(13) \\ &= 150(6) - (-231(1) + 150(2))(13) \\ &= 150(-20) + (-231)(-13). \end{aligned}$$

2. Since $gcd(-231, 150) = gcd(231, 150)$, $231 = (3)(7)(11)$, and $150 = (2)(3)(5^2)$,$gcd(-231, 150) = gcd(231, 150) = 3$.

$lcm((3)(7)(11), (2)(3)(5^2)) = (2)(3)(5^2)(7)(11)$.

3. $\phi(150) = (2-1)(3-1)(5^2-5) = 40$ and $\phi(231) = (3-1)(7-1)(11-1) = 120$.

Exercise 2

1. Let $a, b, c \in \mathbb{Z}_+$. Show that $gcd(a, bc) = 1$ if and only if $gcd(a, b) = 1$ and $gcd(a, c) = 1$.
2. For every integer n, prove that $n^3 + 2n$ is divisible by 3.

Answer

1. Let $a, b, c \in \mathbb{Z}_+$ Assume that $gcd(a, bc) = 1$. Then there exist integers$x$ and y such that $a(x) + bc(y) = 1$. Thus $a(x) + b(cy) = 1$ and $a(x) + c(by) = 1$. Since $x, cy, by \in \mathbb{Z}$, $gcd(a, b) = 1$ and $gcd(a, c) = 1$.

Conversely, assume that $gcd(a, b) = 1$ and $gcd(a, c) = 1$. Then there exist integersx, y, v and w such that $a(x) + b(y) = 1$ and $a(v) + c(w) = 1$. Consider $1 = (ax + by)(av + cw) = a^2xv + axcw + byav + bycw = a(axv + xcw + yav) + (bc)yw$. Since $(axv + xcw + yav), yw \in \mathbb{Z}$, $gcd(a, bc) = 1$.

2. Let $n \in \mathbb{Z}$.

Proof by Cases:

Case 1: $n \equiv 0 (\mod 3) \implies n^3 \equiv 0^3 (\mod 3)$

Consider $n^3 + 2n = (0^3 + 0)(mod\, 3) \equiv 0 (\mod 3)$.

Thus $3 \mid (n^3 + 2n)$.

Case 2: $n \equiv 1(\mod 3) \implies n^3 \equiv 1^3(\mod 3)$

Consider $n^3 + 2n = (1+2)(\mod 3) \equiv 3(\mod 3)$

Thus, $3 \mid (n^3 + 2n)$

Case 3: $n \equiv 2(\mod 3) \implies n^3 \equiv 2^3(\mod 3)$

Consider $n^3 + 2n = (8+4)(\mod 3) \equiv 12(\mod 3)$

Thus $3 \mid (n^3 + 2n)$.

Hence the result.

Exercise 3

Let $a, b, c \in \mathbb{Z}$, and $m \in \mathbb{Z}_+$, such that $a \equiv b(\mod m)$. Show that

1. $a + c \equiv b + c(\mod m)$.
2. $ac \equiv bc(\mod m)$.
3. $a^2 \equiv b^2(\mod m)$.

Answer

Let $a, b, c \in \mathbb{Z}$, and $m \in \mathbb{Z}_+$, such that $a \equiv b(\mod m)$. Since $a \equiv b(mod\ m), m \mid (a-b)$. That is, $\exists k \in \mathbb{Z}$ such that $a = b + km$.

1. Now, consider $a + c = (b + km) + c = (b + c) + km$. Thus, $(a + c) - (b + c) = km$. Since $k \in \mathbb{Z}$, $m \mid ((a + c) - (b + c))$. Hence, $a + c \equiv b + c(\mod m)$.

2. Now, consider $ac = c(b + km) = bc + ckm$. Thus, $ac - bc = (ck)m$. Since $ck \in \mathbb{Z}$, $m \mid (ac - bc)$. Hence, $ac \equiv bc(\mod m)$.

3. Now, consider $a^2 = (b + km)^2 = b^2 + 2bkm + k^2m^2$. Thus $a^2 - b^2 = m(2bk + k^2m)$. Since $(2bk + k^2m) \in \mathbb{Z}$, $m \mid (a^2 - b^2)$. Therefore $a^2 \equiv b^2(\mod m)$.

Exercise 4

For each of the following pairs of integers a and n. show that a and n are relatively prime, determine multiplicative inverse of $[a]$ in $\mathbb{Z}_n$, and find all integers x for $ax \cong 11(\mod n)$.

1. $a = 16, n = 37$.
2. $a = 19, n = 35$.
3. $a = 69, n = 89$.

Answer

1.

$$37 = 2(16) + 5$$
$$16 = 3(5) + 1.$$

Thus, $gcd(37, 16) = 1$.

$$5 = 37 - 2(16)$$
$$1 = 16 - 3(5).$$

Now,

$$1 = 16 - 3(5)$$
$$= 16 - 3(37 - 2(16)) = 16(7) + 37(-3).$$

Hence, the multiplicative inverse of 16 is 7.

Now $x \equiv (7)(11)(\mod 37) \equiv (77)(\mod 37) \equiv 3(\mod 37)$. Thus, the solution set is $\{3 + 37m | m \in \mathbb{Z}\}$.

2.

$$35 = (1)19 + 16$$
$$19 = (1)16 + 3$$
$$16 = (5)3 + 1.$$

Thus, $gcd(35, 19) = 1$.

Now,

$$\begin{aligned} 1 &= 16 + 3(-5) \\ &= 16 + (-5)(19 - 16) \\ &= (6)16 + (-5)19 \\ &= (6)(35 + 19(-1)) + (-5)19 \\ &= 35(6) + 19(-11). \end{aligned}$$

So the multiplicative inverse of 19 is $-11(\mod 35) \equiv 24(\mod 35)$. Thus $19x \cong 11(\mod 35) \implies x \cong (24)(11)(\mod 35) \cong 19(\mod 35)$.

Thus, the solution set is $\{19 + 35m | m \in \mathbb{Z}\}$.

3.

$$89 = 1(69) + 20$$
$$69 = 3(20) + 9$$
$$20 = 2(9) + 2$$
$$9 = 4(2) + 1.$$

Thus, $gcd(69, 89) = 1$.

$$\begin{aligned} 1 &= 9(1) - 4(2) \\ &= 9(1) - (20(1) - 9(2))(4) \\ &= 9(9) - 20(4) \\ &= (69(1) - 3(20))(9) - 20(4) \\ &= 69(9) - 20(31) \\ &= 69(9) - (89(1) - 69(1))(31) \\ &= 69(40) - 89(31). \end{aligned}$$

So, the multiplicative inverse 69 is $40(\mod 89)$.

Now solve $69x \cong 11(\mod 89) \implies x \cong (11)(40)(\mod 89) \cong 440 \cong 84(\mod 89)$.

Thus, the solution set is $\{84 + 89m | m \in \mathbb{Z}\}$.

This page titled Assignment 2 is shared under a CC BY-NC-SA license and was authored, remixed, and/or curated by Pamini Thangarajah.

Assignment 3

Exercise 1

For the following, either show that G is a group with a given operation or list the condition(s) that fail.

1. $G = \mathbb{R}$ with the binary operation $a \star b = a + b - ab$ for $a, b \in \mathbb{R}$.
2. $G = 3\mathbb{Z} = \{3m | m \in \mathbb{Z}\}$ with addition.
3. $G = \{4, 8, 12, 16\}$ with multiplication $\mod(20)$.

Answer

1. Let$G := \mathbb{R}$, and let $a, b, c \in G$. Let an operation $\star$) on$G$ be defined as$a \star b := a + b - a \cdot b$. \

Is $(G, \star)$ closed? $(\star)$ is comprised of $(+)$, $(-)$, and $(\cdot)$ over real numbers. These operations are closed over $\mathbb{R}$. Therefore, since$G = \mathbb{R}$, $(G, \star)$ is closed.

Is$(G, \star)$ associative? Consider the following:

$$\begin{aligned} a \star (b \star c) &= a \star (b + c - bc), && (1)\\ &= a + (b + c - bc) - a(b + c - bc), && (2)\\ &= a + b + c - bc - ab - ac + abc, && (3)\\ &= (a + b - ab) + c - c(a + b - ab), && (4)\\ &= (a + b - ab) \star c, && (5)\\ &= (a \star b) \star c. \end{aligned}$$

Therefore, $(G, \star)$ is associative.

Does$G$ contain the identity e? Consider $0 \in G$.

$$\begin{aligned} a \star 0 &= a + 0 - a \cdot 0, && (6)\\ &= a + 0 - 0, && (7)\\ &= a. && (8)\\ & && (9)\\ 0 \star a &= 0 + a - 0 \cdot a, && (10)\\ &= 0 + a - 0, && (11)\\ &= a. \end{aligned}$$

Since$a \star 0 = 0 \star a = a$ for any $a \in G$, and $0 \in G$;$e = 0$ is the identity of $(G, \star)$.

Does each element of G have an inverse in G? Let's assume for contradiction that $a^{-1} \in G$ exists for all $a \in G$. Then we can say that:

$$\begin{aligned} a \star a^{-1} &= 0, && (12)\\ a + a^{-1} - a \cdot a^{-1} &= 0, && (13)\\ a^{-1}(1 - a) &= -a, && (14)\\ a^{-1} &= \frac{-a}{1 - a}. \end{aligned}$$

Now consider where $a = 1$. In this case, $1^{-1} = \frac{1}{1-1} = \frac{1}{0}$. Clearly $\frac{1}{0} \notin G$, so$1^{-1} \notin G$. This is a contradiction. Therefore, there exists $a \in G$ such that $a^{-1} \notin G$.

Since$(G, \star)$ is closed, has an identity, is associative, but does not contain an inverse for each element; $(G, \star)$ is not a group.\ ((G, \star)\) is a monoid.

2. Let $G := 3\mathbb{Z} = \{3m : m \in \mathbb{Z}\}$. Let $m, n, p \in \mathbb{Z}$. Clearly $3m, 3n, 3p \in 3\mathbb{Z}$ by definition of $3\mathbb{Z}$. Consider $(G, +)$.

Is $(G, +)$ closed? Consider the following:

$$3m + 3n = 3(m + n).$$

Since $\mathbb{Z}$ is closed under addition, $(m + n) \in \mathbb{Z}$, and $3(m + n) \in G$. Therefore, $(G, +)$ is closed.

Is $(G, +)$ associative? Consider the following:

$$3m + (3n + 3p) = 3(m + (n + p)). \quad (15)$$

$$= 3((m+n)+p), \tag{16}$$
$$= (3m+3n)+3p.$$

Therefore, $(G,+)$ is associative.

Does$G$ contain the identity e? Consider $0 \in G$.

$$3m+0 = 3m. \tag{17}$$
$$0+3m = 3m.$$

Clearly $3m+0 = 0+3m = 3m$. Therefore, $e = 0$ is the identity of $(G,+)$.

Does$(G,+)$ contain the inverse for each element in$G$? Consider $3(-n)$ as the inverse for $3n$. Since $-n \in \mathbb{Z}$, $3(-n) \in G$.

$3n+3(-n) = 3(n-n) = 3(0) = 0 = e$. and $3(-n)+3n = 3((-n)+n) = 3(0) = 0 = e$.

Therefore $3n+3(-n) = 3(-n)+3n = e$. So for any $a \in G$, there exists $a^{-1} \in G$.

Since $(G,+)$ is closed, associative, and contains the identity and an inverse for every element, $(G,+)$ is a group.

3. The Cayley table of G with multiplication $\mod(20)$:

$\cdot(mod 20)$	4	8	12	16
4	16	12	8	4
8	12	4	16	8
12	8	16	4	12
16	4	8	12	16

Is $(G,\cdot(mod(20))$ closed? Yes, we can see from the Cayley table that all results of $\cdot(mod(20)$ are in G.

Does G contain the identity for $\cdot(mod(20)$? Again, by the Cayley table, we can see that the identity $e = 16$.

Is $(G,\cdot(mod(20))$ associative? Yes. We know by the properties of $\mathbb{Z}$ that multiplication of integers is associative. Also, by the properties of modular arithmetic that the modulo operation has no impact on associativity. Therefore, $(G,\cdot(mod(20))$ is associative. \

Does G contain an inverse for each element under $\cdot(mod(20)$? Yes, consider the following:

$$\begin{aligned} 4 \cdot 4 &\equiv 16 mod(20) \implies 4^{-1} = 4. \\ 8 \cdot 12 &\equiv 16 mod(20) \implies 8^{-1} = 12. \\ 12 \cdot 8 &\equiv 16 mod(20) \implies 12^{-1} = 8. \\ 16 \cdot 16 &\equiv 16 mod(20) \implies 16^{-1} = 16. \end{aligned}$$

So clearly for each $a \in G$, there exists $a^{-1} \in G$. Since $(G,\cdot(mod(20))$ is closed, associative, and contains the identity and an inverse for every element, $(G,\cdot(mod(20))$ is a group.

? Exercise 2

Decide whether the following structures form a group or not by looking at the Cayley table.

1. $\{\pm 1, \pm i\}$ with multiplication, Where i is the complex number such that $i^2 = -1$.
2. $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, where i is the complex number such that $i^2 = -1$.

Define $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$. Q_8 with matrix multiplication.

Answer

1. Let $G = \{1, -1, i, -i\}$ with complex multiplication.

We are to determine whether the set G forms a group $(G, \cdot)$ under multiplication, where i is the imaginary unit with $i^2 = -1$. We will construct and examine the Cayley table to verify the group properties.

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Since it is closed, has an identity, and every element has an inverse according to the table, multiplication is associative on 2×2 matrices over the complex numbers; it is a group.

2. $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$, where $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $J = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$, $K = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$, where i is the complex number such that $i^2 = -1$.

$\times$	1	-1	I	$-I$	J	$-J$	K	$-K$
1	1	-1	I	$-I$	J	$-J$	K	$-K$
-1	-1	1	$-I$	I	$-J$	J	$-K$	K
I	I	$-I$	-1	1	K	$-K$	$-J$	J
$-I$	$-I$	I	1	-1	$-K$	K	J	$-J$
J	J	$-J$	$-K$	K	-1	1	I	$-I$
$-J$	$-J$	J	K	$-K$	1	-1	$-I$	I
K	K	$-K$	J	$-J$	$-I$	I	-1	1
$-K$	$-K$	K	$-J$	J	I	$-I$	1	-1

Since it is closed, has an identity, and every element has an inverse according to the table, multiplication is associative on 2×2 matrices over the complex numbers; it is a group.

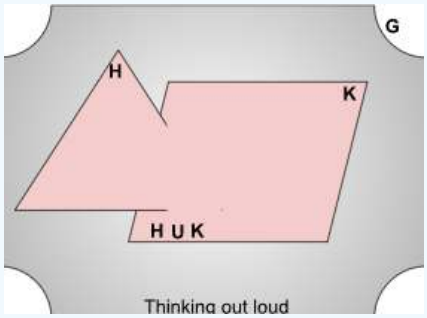
Exercise 3

Prove or disprove: Let H and K be subgroups of the group G. Then

1. $H \cup K$ is a subgroup of G.
2. $H \cap K$ is a subgroup of G.

Answer

1. No, $H \cup K$ is a subgroup of G.



Answers may vary.

Counterexample:

Let $G = (Z_6, +\pmod 6)$.

Thus $e_G = 0$.

We shall show that $H \cup K$ is not a subgroup of G.

Consider $Z_6 = \{0, 1, 2, 3, 4, 5\}$.

Let $H = (\{0, 2, 4\}, +\pmod 6)$.

Note $H \leq G$ since$e_G = 0 \in H$ and $\exists_1 h^{-1}, \forall h \in H$.

Let $K = (\{0, 3\}, +\pmod 6)$.

Note $K \leq G$ since $e_K = 0 \in H$ and $\exists_1 k^{-1}, \forall k \in K$.

Thus $H \cup K = (\{0, 2, 3, 4\}, +\pmod 6)$.

Let $a = 2$ and$b = 3$, where $2, 3 \in H \cup K$.

https://math.libretexts.org/@go/page/166411

However, since $2+3 \equiv 5 \pmod{6} \notin H \cup K$, $H \cup K$ is not a group.

Thus, $H \cup K$ is not a subgroup of$G$.

2. Yes, $H \cap K$ is a subgroup of G .

Proof:

Let e be the identity of G .

Then e is the identity of both H and K .

Therefore $e \in H \cap K$.

Let $g_1, g_2 \in H \cap K$.

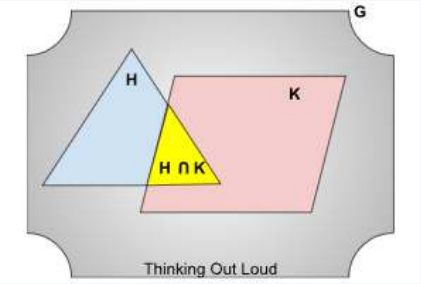
Then we shall show that $g_1 g_2^{-1} \in H \cap K$.

Since $g_1, g_2 \in H \cap K$, $g_1, g_2 \in H$ and $g_1, g_2 \in K$.

Since $H \leq G$ and $K \leq G$, $g_1, g_2, g_1^{-1}, g_2^{-1}$ are in both H and K .

Hence $g_1 g_2^{-1} \in H \cap K$.

Therefore $H \cap K \leq G$.□



Exercise 4

1. Show that $U(20) \neq < k >$ for any k in $U(20)$. [Hence $U(20)$ is not cyclic.]

2. Prove that if G is an abelian group, then for each element $a \in G$, $C(a) = \{x \in G | xa = ax\}$ is a subgroup of G.

Answer

1.

$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$ and $|U(20)| = 8$.

We shall show that$U(20) \neq k,\ k \in U(20)$.

k	Calculations	Order of$k$
1	$1 \equiv 1 \pmod{20}$	1
3	$3^1 \equiv 3 \pmod{20}$;$3^2 \equiv 9 \pmod{20}$;$3^3 \equiv 7 \pmod{20}$;$3^4 \equiv 1 \pmod{20}$	4
7	$7^1 \equiv 7 \pmod{20}$;$7^2 \equiv 9 \pmod{20}$;$7^3 \equiv 3 \pmod{20}$;$7^4 \equiv 1 \pmod{20}$	4
9	$9^1 \equiv 9 \pmod{20}$;$9^2 \equiv 1 \pmod{20}$	2
11	$11^1 \equiv 11 \pmod{20}$;$11^2 \equiv 1 \pmod{20}$	2
13	$13^1 \equiv 13 \pmod{20}$;$13^2 \equiv 9 \pmod{20}$;$13^3 \equiv 17 \pmod{20}$;$13^4 \equiv 1 \pmod{20}$	4
17	$17^1 \equiv 17 \pmod{20}$;$17^2 \equiv 9 \pmod{20}$;$17^3 \equiv 13 \pmod{20}$;$17^4 \equiv 1 \pmod{20}$	4
19	$19^1 \equiv 19 \pmod{20}$;$19^2 \equiv 1 \pmod{20}$	2

Since $|k| \neq |U(20)|,\ \forall\ k \in U(20)$, there is no $k \in U(20)$ that generates $U(20)$.

2. Since G is abelian, for each $a \in G$, $C(a) = \{x \in G | xa = ax\} = G$ is a subgroup of G.

This page titled Assignment 3 is shared under a CC BY-NC-SA license and was authored, remixed, and/or curated by Pamini Thangarajah.

Assignment 4

Some of these solutions are written by Fall 2024 MATH 2101 students.

Exercise 1

Consider the group $\mathbb{Z}_{12}$ with addition modulo 12.

1. Is $(\mathbb{Z}_{12}, +mod(12))$ cyclic group? If so, what are the possible generators? How many distinct generators are there? What can you say about the number of generators (hint: Euler totient number) and the possible generators (Hint: Divisors)?

2. Let $G = \langle g \rangle$ be a cyclic group with $|g| = n$. Then $G = \langle g^k \rangle$ if and only if $gcd(k, n) = 1$.

3. Find all subgroups of $\mathbb{Z}_{12}$ generated by each element. What are the orders of them? What can you say about these orders?

4. Let $G = \langle a \rangle$ be a cyclic group with $|G| = n$. Prove the following statements:

a) If $H \leq G$ then $H = \langle a^k \rangle$ for some integer k that divides n.

b) If $k|n$ then $\langle a^{\frac{n}{k}} \rangle$ is the unique subgroup of G of order k.

Answer

Consider $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ with addition modulo 12. Note that $\{0\}$ is the identity and its order is 1.

Element	Order	Calculations
0	$\lvert\langle 0\rangle\rvert = 1$	
1	$\lvert\langle 1\rangle\rvert = 12$	$1^{12} \equiv 0 \pmod{12}$
2	$\lvert\langle 2\rangle\rvert = 6$	$2^1 \equiv 2 \pmod{12}$, $2^2 \equiv 4 \pmod{12}$, $2^3 \equiv 6 \pmod{12}$, $2^4 \equiv 8 \pmod{12}$, $2^5 \equiv 10 \pmod{12}$ and $2^6 \equiv 0 \pmod{12}$.
3	$\lvert\langle 3\rangle\rvert = 4$	$3^1 \equiv 3 \pmod{12}$, $3^2 \equiv 6 \pmod{12}$, $3^3 \equiv 9 \pmod{12}$, and $3^4 \equiv 0 \pmod{12}$.
4	$\lvert\langle 4\rangle\rvert = 3$	$4^1 \equiv 4 \pmod{12}$, $4^2 \equiv 8 \pmod{12}$, and $4^3 \equiv 0 \pmod{12}$.
5	$\lvert\langle 5\rangle\rvert = 12$	$5^1 \equiv 5 \pmod{12}$, $5^2 \equiv 10 \pmod{12}$, $5^3 \equiv 3 \pmod{12}$, $5^4 \equiv 8 \pmod{12}$, $5^5 \equiv 1 \pmod{12}$, $5^6 \equiv 6 \pmod{12}$, $5^7 \equiv 11 \pmod{12}$, $5^8 \equiv 4 \pmod{12}$,$5^9 \equiv 9 \pmod{12}$, $5^{10} \equiv 2 \pmod{12}$, $5^{11} \equiv 7 \pmod{12}$, and $5^{12} \equiv 0 \pmod{12}$.
6	$\lvert\langle 6\rangle\rvert = 2$	$6^1 \equiv 6 \pmod{12}$, and $6^2 \equiv 2 \pmod{12}$.
7	$\lvert\langle 7\rangle\rvert = 12$	$7^1 \equiv 7 \pmod{12}$, $7^2 \equiv 2 \pmod{12}$, $7^3 \equiv 9 \pmod{12}$, $7^4 \equiv 4 \pmod{12}$, $7^5 \equiv 11 \pmod{12}$, $7^6 \equiv 6 \pmod{12}$, $7^7 \equiv 1 \pmod{12}$, $7^8 \equiv 8 \pmod{12}$, $7^9 \equiv 3 \pmod{12}$, $7^{10} \equiv 10 \pmod{12}$, $7^{11} \equiv 5 \pmod{12}$, and $7^{12} \equiv 0 \pmod{12}$.
8	$\lvert\langle 8\rangle\rvert = 3$	$8^1 \equiv 8 \pmod{12}$, $8^2 \equiv 4 \pmod{12}$ and $8^3 \equiv 0 \pmod{12}$.
9	$\lvert\langle 9\rangle\rvert = 4$	$9^1 \equiv 9 \pmod{12}$, $9^2 \equiv 6 \pmod{12}$, $9^3 \equiv 3 \pmod{12}$ and $9^4 \equiv 0 \pmod{12}$. $9^5 \equiv 5 \pmod{10}$, $9^6 \equiv 4 \pmod{10}$, $9^7 \equiv 3 \pmod{10}$, $9^8 \equiv 2 \pmod{10}$, $9^9 \equiv 1 \pmod{10}$, and $9^{10} \equiv 0 \pmod{10}$.
10	$\lvert\langle 10\rangle\rvert = 6$	$10^1 \equiv 10 \pmod{12}$, $10^2 \equiv 8 \pmod{12}$, $10^3 \equiv 6 \pmod{12}$, $10^4 \equiv 4 \pmod{12}$, $10^5 \equiv 2 \pmod{12}$ and $10^6 \equiv 0 \pmod{12}$.
11	$\lvert\langle 11\rangle\rvert = 12$	$11^1 \equiv 11 \pmod{12}$, $11^2 \equiv 10 \pmod{12}$, $11^3 \equiv 9 \pmod{12}$, $11^4 \equiv 8 \pmod{12}$, $11^5 \equiv 7 \pmod{12}$, $11^6 \equiv 6 \pmod{12}$, $11^7 \equiv 5 \pmod{12}$, $11^8 \equiv 4 \pmod{12}$, $11^9 \equiv 3 \pmod{12}$, $11^{10} \equiv 2 \pmod{12}$, $11^{11} \equiv 1 \pmod{12}$, and $11^{12} \equiv 0 \pmod{12}$.

From the table, $(\mathbb{Z}_{12}, +mod(12))$ is a cyclic group, the set of all possible generators are $\{1, 5, 7, 11\} = \{a \in \mathbb{Z} | gcd(a, 12) = 1,\ 1 \leq a < 12\}$. Hence, the number of generators is the same as the number of integers relatively prime to $12 = 2^2\,3$. That is, the number of generators is the Euler totient number $\phi(12) = (2^2 - 2)(3^1 - 1) = 4$.

Answer

Let $G = \langle g \rangle$ be a cyclic group with $|g| = n$. Then
$g \in G$ and $g^n = e$.

Assume that $G = \langle g^k \rangle$. Then $g = (g^k)^x$ for some $x \in \mathbb{Z}$.

Thus,
$g^{1-kx} = e$.
By Theorem 2.4.5 from the text, $n \mid (1-kx)$. Therefore,
$1 - kx = ny$, for some $y \in \mathbb{Z}$.
Which implies,
$1 = kx + ny$,
hence,
$\gcd(k, n) = 1$.

Conversly, we shall show that if $\gcd(k, n) = 1$, then $G = \langle g^k \rangle$.
Suppose that $\gcd(k, n) = 1$. Then
$kx + ny = 1$, for some $x, y \in \mathbb{Z}$.
By using the properties of powers in a group and $g^n = e$, we get,

$$g^1 = g^{kx+ny} = (g^k)^x (g^n)^y = (g^k)^x. \tag{1}$$

Hence $g \in \langle g^k \rangle$.

Therefore, we have $G \subseteq \langle g^k \rangle$. Since $\langle g^k \rangle \subseteq G$,
$G = \langle g^k \rangle$.

Answer

From the above table, we see that the orders of the subgroups are $1, 2, 3, 4, 6$ and 12, which are all divisors of the order of $\mathbb{Z}_{12}$. Specifically, the order of the subgroup generated by $g \in \mathbb{Z}_{12}$ is $\frac{n}{gcd(g,n)}$.

Answer

a) Let $G = \langle a \rangle$ with $|G| = n$. Assume that $H \leq G$. By Theorem 2.4.3, H is cyclic. Hence $H = \langle a^k \rangle$ for some integer $k \in \mathbf{Z}$. Let $d = gcd(k, n)$. We shall show that $H = \langle a^d \rangle$. Since $d = gcd(k, n)$, $kx + ny = d$, for some $x, y \in \mathbb{Z}$. Consider,

$$a^d = a^{kx+ny} = (a^k)^x (a^n)^y = (a^k)^x. \tag{2}$$

Thus $a^d \in H$. Therefore $\langle a^d \rangle \subseteq H$.
Since $d|k, k = md$, for some $m \in \mathbb{Z}$. Thus, $a^k = a^{md} = (a^d)^m$. Hence $H \subseteq \langle a^d \rangle$. Thus $H = \langle a^d \rangle$ and $d|n$.

b) Let $G = \langle a \rangle$ with $|G| = n$. Assume that $k|n$. Suppose K be subgroup of G of order k. We shall show that $K = \langle a^{\frac{n}{k}} \rangle$. Since K is a subgroup of G, $K = \langle a^m \rangle$, for some, $m \in \mathbb{Z}$. By part a, $m|n$. Then $(a^m)^{n/m} = e$. We shall show that $\frac{n}{m}$ is the smallest positive integer with this property.

Now, $|K| = \frac{n}{m} = k$. Thus, $m = \frac{n}{k}$. Thus $K = \langle a^{\frac{n}{k}} \rangle$ which is unique.

? Exercise 2

Let G be a group.

1. Show that $|g| = |g^{-1}|$, for all $g \in G$.

2. Show that $|h| = |ghg^{-1}|$, for all $g, h \in G$.

3. Show that $|hg| = |gh|$, for all $g, h \in G$.

Answer

Let G be a group.

1. Suppose $g \in G$, then let $n \in \mathbb{Z}$ such that $|g| = n$. Now consider:

$$\begin{aligned} & g^n = e, \\ \iff & (g^n)^{-1} = e^{-1}, \\ \iff & (g^{-1})^n = e. \end{aligned}$$

Now suppose $k \in \mathbb{Z}$ such that $|g^{-1}| = k$. Since $(g^{-1})^n = e$, it must be true that $k \leq n$.
Now consider:

$$\begin{aligned}
&(g^{-1})^k = e, \\
\iff &(g^{-1})^{-k} = e^{-1}, \\
\iff &g^k = e.
\end{aligned}$$

Since $g^k = e$ and $|g| = n$, it must be the case that $n \leq k$.
Therefore $n \leq k \leq n \implies n = k$.
Therefore $|g| = |g^{-1}|$.

2. Suppose $h \in G$, the let $n \in \mathbb{Z}$ such that $|h| = n$. Now consider:

$$\begin{aligned}
(ghg^{-1})^n &= (ghg^{-1})(ghg^{-1}) \dots (ghg^{-1}) \\
&= gh(g^{-1}g)h(g^{-1}g)h \dots (g^{-1}g)hg^{-1} \\
&= gh^n g^{-1} \\
&= geg^{-1} \\
&= gg^{-1} \\
&= e.
\end{aligned}$$

Now let $k \in \mathbb{Z}$ such that $|ghg^{-1}| = k$. Since $(ghg^{-1})^n = e$, it must be the case that $k \leq n$. Now consider:

$$\begin{aligned}
&(ghg^{-1})^k = e, \\
\iff &(ghg^{-1})(ghg^{-1}) \dots (ghg^{-1}) = e, \\
\iff &gh(g^{-1}g)h(g^{-1}g) \dots (g^{-1}g)hg^{-1} = e, \\
\iff &gh^k g^{-1} = e, \\
\iff &g^{-1}gh^k g^{-1}g = g^{-1}eg, \\
\iff &eh^k e = g^{-1}g, \\
\iff &h^k = e.
\end{aligned}$$

Since $h^k = e$ and $|h| = n$, then $n \leq k$.
Therefore $k \leq n \leq k \implies n = k$.
Therefore $|h| = |ghg^{-1}|$.

3. Suppose $g, h \in G$. Let $n \in \mathbb{Z}$ such that $|hg| = n$. Now consider:

$$\begin{aligned}
&(hg)^n = e, \\
\iff &(hg)(hg) \dots (hg)(hg) = e, \\
\iff &h(gh)(gh) \dots (gh)g = e, \\
\iff &h(gh)^{n-1}g = e, \\
\iff &h^{-1}h(gh)^{n-1}gh = h^{-1}eh, \\
\iff &e(gh)^n = h^{-1}h, \\
\iff &(gh)^n = e.
\end{aligned}$$

Now let $k \in \mathbb{Z}$ such that $|gh| = k$. Since $(gh)^n = e$, it must be the case that $k \leq n$. Now consider:

$$\begin{aligned}
&(gh)^k = e, \\
\iff &(gh)(gh) \dots (gh)(gh) = e, \\
\iff &g(hg)(hg) \dots (hg)h = e, \\
\iff &g(hg)^{k-1}h = e, \\
\iff &g^{-1}g(hg)^{k-1}hg = g^{-1}eg, \\
\iff &e(hg)^k = g^{-1}g, \\
\iff &(hg)^k = e.
\end{aligned}$$

Since $(hg)^k = e$ and $|hg| = n$, then it must be the case that $n \leq k$.
Therefore $n \leq k \leq n \implies n = k$.
Therefore $|hg| = |gh|$.

? Exercise 3

Let G be a group.

1. If G is an abelian group then show that $H = \{g^2 | g \in G\}$ is a subgroup of G. Show that H is not necessarily a subgroup if G is not abelian by taking $G = A_4$.

2. If $a^2 = e$, for all $a \in G$, show that G is abelian. Give an example to show that the converse of the above statement is not true.

Answer

1.To show that H is a subgroup of G when G is abelian, we use the subgroup criterion:

Since $e \in G$ and $e^2 = e$, $e \in H$. Let $a, b \in H$. Then $a = g_1^2, b = g_2^2$ for some $g_1, g_2 \in G$.

Consider, $ab^{-1} = g_1^2 (g_2^2)^{-1} = g_1^2 \left(g_2^{-1}\right)^2 = g_1(g_1 g_2^{-1}) g_2^{-1} = g_1(g_2^{-1} g_1) g_2^{-1}$ (since G is abelian). Thus $ab^{-1} = \left(g_1 g_2^{-1}\right)^2$. Since $g_1 g_2 \in G, \left(g_1 g_2^{-1}\right)^2 \in H$.

Therefore, H is a subgroup of G when G is abelian.

Consider $G = A_4$, we will show that H is not a subgroup of G .

$$
\begin{aligned}
(\,1\,2\,3\,)^2 &= (\,1\,3\,2\,) = (\,3\,2\,1\,) \\
(\,1\,2\,4\,)^2 &= (\,1\,4\,2\,) = (\,4\,2\,1\,) \\
(\,1\,3\,4\,)^2 &= (\,1\,4\,3\,) = (\,4\,3\,1\,) \\
(\,2\,3\,4\,)^2 &= (\,2\,4\,3\,) = (\,4\,3\,2\,) \\
(\,4\,3\,2\,)^2 &= (\,4\,2\,3\,) = (\,2\,3\,4\,) \\
(\,4\,3\,1\,)^2 &= (\,4\,1\,3\,) = (\,1\,3\,4\,) \\
(\,4\,2\,1\,)^2 &= (\,4\,1\,2\,) = (\,1\,2\,4\,) \\
(\,3\,2\,1\,)^2 &= (\,3\,1\,2\,) = (\,1\,2\,3\,) \\
(\,1\,2\,)(\,3\,4\,)(\,1\,2\,)(\,3\,4\,) &= e \\
(\,1\,3\,)(\,2\,4\,)(\,1\,3\,)(\,2\,4\,) &= e \\
(\,1\,4\,)(\,2\,3\,)(\,1\,4\,)(\,2\,3\,) &= e
\end{aligned}
$$

$$
H = \left\{ e,\ (\,1\,2\,3\,),\ (\,1\,2\,4\,),\ (\,1\,3\,4\,),\ (\,2\,3\,4\,),\ (\,4\,3\,2\,),\ (\,4\,3\,1\,),\ (\,4\,2\,1\,),\ (\,3\,2\,1\,) \right\}
$$

We can see that $H \subseteq G$, we will show that H is not closed. We know that $(\,1\,2\,3\,) \in H$ and $(\,1\,2\,4\,) \in H$. Consider

$$
\begin{aligned}
(\,1\,2\,3\,)(\,1\,2\,4\,) &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 4 \\ 3 & 4 & 2 \end{pmatrix} \\
&= (\,1\,3\,)(\,2\,4\,) \notin H
\end{aligned}
$$

$\therefore\ H \not\leq G.$

2. The statement is false. Answers may vary.

Consider the quaternion group Q_8 , which is non-abelian and defined by:

$$
Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \tag{3}
$$

with multiplication rules:

$$
i^2 = j^2 = k^2 = -1, \qquad ij = k, \qquad ji = -k \tag{4}
$$

Consider

$$
\begin{aligned}
(\pm 1)^2 &= 1, \\
(\pm i)^2 = (\pm j)^2 &= (\pm k)^2 = -1
\end{aligned}
$$

Then

$$
H = \{1, -1\}
$$

Clearly, H is a subgroup of Q_8. (You can use a Cayley table to show this!)

Now we will show that Q_8 is non-abelian. consider $i, j, k \in Q_8$

$$
\begin{aligned}
& i \cdot j = k, \\
& j \cdot i = -k \\
& k \neq -k \\
\iff & i \cdot j \neq j \cdot i
\end{aligned}
$$

$\therefore$ the existence of $H = \{g^2 \mid g \in G\}$ as a subgroup of G does not imply that G is abelian.

2.

Assume that $a^2 = e$ for all $a \in G$. Let $a, b \in G$. Consider the product ab . By using the properties of an abelian group, we have

$$\begin{aligned}(ab)^2 &= (ab)(ab)\\ &= a(ba)b\\ &= a(ab)b\\ &= (aa)(bb)\\ &= a^2 \cdot b^2\\ &= e \cdot e\\ &= e\end{aligned}$$

Since $(ab)^2 = e$, we have:

$$(ab)^2 = e \implies abab = e. \tag{5}$$

Multiply both sides on the left by a and on the right by b :

$$a(abab)b = aeb \implies (aa)babb = ab. \tag{6}$$

Simplify using $a^2 = e$ and $b^2 = e$:

$$e \cdot ba \cdot e = ab \implies ba = ab. \tag{7}$$

Hence, $ab = ba$, $\therefore$ G is abelian.

Showing the converse is false:

Consider the cyclic group $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under $+(\mathrm{mod} 4)$. $\mathbb{Z}_4$ is abelian, but not all elements satisfy $a^2 = e$.
Consider $1^2 \in \mathbb{Z}_4$.

$$\begin{aligned}1 + 1 &= 2\\ &\neq 0\end{aligned}$$

Thus, $\mathbb{Z}_4$ is abelian, but $a^2 = e$ does not hold for all $a \in \mathbb{Z}_4$. This shows that the converse is not true.

? Exercise 4

Consider the symmetric group S_4

1.Show that S_4 is not abelian.

2. Find the centre of S_4.

3. Given $\alpha, \beta \in S_4$ with $\alpha\beta = (1432), \beta\alpha = (1243)$, and
$\alpha(1) = 4$, determine α and β.

4. Find the cyclic subgroup of S_4 that has an order of 4.

5. Find a non-cyclic subgroup of S_4 that has order 4.

Answer

1.

Let $a = (1, 2)$ and $b = (2, 3)$ both elements of S_4.

Consider $ab = (1, 2)(1, 3) = (1, 3, 2)$ and $ba = (1, 3)(1, 2) = (1, 2, 3)$.

Since $(1, 3, 2) \neq (1, 2, 3)$, $ab \neq ba \; for some a, b \in S_4$, S_4 is non-abelian.

2.

S_4
$= \{e, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (124), (134), (234), (432), (431), (421), (321), (1234), (1243), (1324), (1342), (1423), (1432)\}$.

Method I:

Let $s \in S_4$, and $N = \{1, 2, 3, 4\}$.
case 1: $s = e.e$ is commutative by definition. Therefore $e \in Z(S_4)$
case 2: s is of type $[2, 1, 1]$.
It follows that $s = (i, j)$for some distinct $i, j \in N$. Consider $t = (i, k)$ for some $k \in N$ such that $i \neq k \neq j$. Then $st = (i, k, j)$. But $ts = (i, j, k) \neq st$. So those of type [2,1,1] are not in $Z(S_4)$.

case 3: s is of type [2,2].
It follows that s = (i, j)(k,l) for some distinct i, j, k,l ∈ N. Consider t = (i, j, k). Then st = (j,l, k) ≠ (i, k,l) = ts. So $s \notin Z(S_4)$.

case 4: s is of type [3,1].
It follows that s = (i, j, k) for some distinct i, j, k ∈ N. Consider t = (i,l) such that $l \in$ {i, j, k}. Then st = (i,l, j, k) ≠ (i, j, k,l) = ts.

Case 5: s is of type [4].
It follows that s = (i, j, k,l) for some distinct i, j, k,l ∈ N. Consider t = (i,l). Then st = (j, k,l) ≠ (i, j, k) = ts.

Except for e, all elements have some other element they do not commute with.
So $Z(S_4)$ = \{e\}.\)

Method II:

Proof by exhaustion:

Clearly $e \in Z(S_4)$. \)
$(12)(13) = (132), \quad (13)(12) = (123), \quad (12), (13) \notin Z(S_4)$
$(14)(12) = (124), \quad (12)(14) = (142), \quad (14), (12) \notin Z(S_4)$
$(23)(12) = (132), \quad (12)(23) = (123), \quad (23), (12) \notin Z(S_4)$
$(24)(12) = (142), \quad (12)(24) = (124), \quad (24), (12) \notin Z(S_4)$
$(34)(13) = (143), \quad (13)(34) = (341), \quad (34)(13) \notin Z(S_4)$
$(12)(34)(13) = (1432), \quad (13)(12)(34) = (3412), \quad (12)(34) \notin Z(S_4)$
$(13)(24)(12) = (1423), \quad (12)(13)(24) = (3421), \quad (13)(24) \notin Z(S_4)$
$(14)(23)(12) = (1324), \quad (12)(14)(23) = (2314), \quad (14)(23) \notin Z(S_4)$
$(123)(12) = (13), \quad (12)(123) = (23), \quad (123) \notin Z(S_4)$
$(132)(12) = (23), \quad (12)(132) = (13), \quad (132) \notin Z(S_4)$
$(124)(12) = (14), \quad (12)(124) = (24), \quad (124) \notin Z(S_4)$
$(142)(12) = (24), \quad (12)(142) = (14), \quad (142) \notin Z(S_4)$
$(134)(12) = (4123), \quad (12)(134) = (4213), \quad (134) \notin Z(S_4)$
$(143)(12) = (1243), \quad (12)(143) = (1432), \quad (143) \notin Z(S_4)$
$(234)(12) = (4213), \quad (12)(234) = (4123), \quad (234) \notin Z(S_4)$
$(243)(12) = (1432), \quad (12)(243) = (4312), \quad (243) \notin Z(S_4)$
$(1234)(12) = (134), \quad (12)(1234) = (234), \quad (1234) \notin Z(S_4)$
$(1243)(12) = (143), \quad (12)(1243) = (243), \quad (1243) \notin Z(S_4)$
$(1324)(12) = (14)(23), \quad (12)(1324) = (13)(24), \quad (1324) \notin Z(S_4)$
$(1342)(12) = (342), \quad (12)(1342) = (134), \quad (1342) \notin Z(S_4)$
$(1423)(12) = (13)(24), \quad (12)(1423) = (14)(23), \quad (1423) \notin Z(S_4)$
$(1432)(12) = (243), \quad (12)(1432) = (143), \quad (1432) \notin Z(S_4)$
Having tried all $x \in S_4$, the only $x \in S_4$ that satisfies $xg = gx, \ \forall g \in S_4$ is the identity. Hence, $Z(S_4) = \{e\}$.

Method III: Proof by contradiction

Let $\gamma(\neq e) \in Z(S_4)$. We shall find an $\alpha \in S_4$ such that $\gamma\alpha \neq \alpha\gamma$. Since $\gamma(\neq e)$, there exist $l, m \in \{1, 2, 3, 4\}$ such that $\gamma(l) = m \neq l$. Now we can choose an element $k \in \{1, 2, 3, 4\}$ such that $k \neq l$ and $k \neq m$. Choose $\alpha = (l, k)$. Then $\gamma\alpha(l) = \gamma(k)$ and $\alpha\gamma(l) = \alpha(m) = m$. Since γ is a bijection and $\gamma(l) = m \neq l$, $\gamma(k) \neq m$. This is a contradiction. Hence, $Z(S_4) = \{e\}$.

3. Let $\alpha, \beta \in S_4$ with $\alpha\beta = (1432), \beta\alpha = (1243)$, and $\alpha(1) = 4$,

$$\begin{aligned}
\beta\alpha(1) &= \beta(\alpha(1)) = \beta(4) = 2 \\
\alpha\beta(4) &= \alpha(\beta(4)) = \alpha(2) = 3 \\
\beta\alpha(2) &= \beta(\alpha(2)) = \beta(3) = 4 \\
\alpha\beta(3) &= \alpha(\beta(3)) = \alpha(4) = 2 \\
\beta\alpha(4) &= \beta(\alpha(4)) = \beta(2) = 3 \\
\alpha\beta(2) &= \alpha(\beta(2)) = \alpha(3) = 1 \\
\beta\alpha(3) &= \beta(\alpha(3)) = \beta(1) = 1
\end{aligned}$$

from above, $\alpha = (1423)\beta = (234)$.

4.

The subgroup of $S_4, C_4 = \{e, (1,2,3,4), (1,3)(2,4), (1,4,3,2)\}$, has an order 4 and is generated by $(1,2,3,4)$.

$(1,2,3,4)^2 = (1,3)(2,4)$, $(1,2,3,4)^3 = (1,4,3,2)$, and $(1,2,3,4)^4 = e$.

5.

The 2-2 cycles together will form an order 4 group.

$\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ is a subgroup of S_4 and has order 4. Note the inverse of $(1,2)(3,4)$ is $(4,3)(2,1)$, which is $(1,2)(3,4)$. Since a similar argument can be made for the other 2-2 cycles, the inverses of each element exist. In addition, the set is closed under composition.

Exercise 5

Consider the symmetric group S_7.

1. Find all possible types of permutations and state how many of each type.

2. Find the possible order of all the $7!$ elements of the symmetric group S_7.

3. Factor the permutation $(12345)(67)(1357)(163)$ into disjoint cycles.

4. Find an element of maximum order in S_7.

Answer

Cycle Type	Order	Number of Permutations	
$\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}$	1	1	$\frac{7!}{1^7\,7!} = 1$
$\underline{2}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}$	2	21	$\frac{7!}{2^1\,1^5\,1!\,5!} = \frac{(6)(7)}{(2)} = 21$
$\underline{2}\,\underline{2}\,\underline{1}\,\underline{1}\,\underline{1}$	2	105	$\frac{7!}{2^2\,1^3\,2!\,3!} = \frac{(5)(6)(7)}{(2)} = 105$
$\underline{2}\,\underline{2}\,\underline{2}\,\underline{1}$	2	105	$\frac{7!}{2^3\,1^1\,3!\,1!} = \frac{(5)(6)(7)}{(2)} = 105$
$\underline{3}\,\underline{1}\,\underline{1}\,\underline{1}\,\underline{1}$	3	70	$\frac{7!}{3^1\,1^4\,1!\,4!} = \frac{(5)(6)(7)}{(3)} = 70$
$\underline{3}\,\underline{2}\,\underline{1}\,\underline{1}$	6	420	$\frac{7!}{3^1\,2^1\,1^2\,1!\,1!\,2!} = \frac{(4)(5)(6)(7)}{(2)} = 420$
$\underline{3}\,\underline{2}\,\underline{2}$	6	210	$\frac{7!}{3^1\,2^2\,1!\,2!} = \frac{(5)(6)(7)}{(1)} = 210$
$\underline{3}\,\underline{3}\,\underline{1}$	3	280	$\frac{7!}{3^2\,1^1\,2!\,1!} = \frac{(4)(5)(6)(7)}{(3)} = 280$
$\underline{4}\,\underline{1}\,\underline{1}\,\underline{1}$	4	210	$\frac{7!}{4^1\,1^3\,1!\,3!} = \frac{(5)(6)(7)}{(1)} = 210$
$\underline{4}\,\underline{2}\,\underline{1}$	4	630	$\frac{7!}{4^1\,2^1\,1^1\,1!\,1!\,1!} = \frac{(3)(5)(6)(7)}{(1)} = 630$
$\underline{4}\,\underline{3}$	12	420	$\frac{7!}{4^1\,3^1\,1!\,1!} = \frac{(2)(5)(6)(7)}{(1)} = 420$
$\underline{5}\,\underline{1}\,\underline{1}$	5	504	$\frac{7!}{5^1\,1^2\,1!\,2!} = \frac{(3)(4)(6)(7)}{(1)} = 504$
$\underline{5}\,\underline{2}$	10	504	$\frac{7!}{5^1\,2^1\,1!\,1!} = \frac{(3)(4)(6)(7)}{(1)} = 504$
$\underline{6}\,\underline{1}$	6	840	$\frac{7!}{6^1\,1^1\,1!\,1!} = \frac{(2)(3)(4)(5)(7)}{(1)} = 840$
$\underline{7}$	7	720	$\frac{7!}{7^1\,1!} = \frac{(2)(3)(4)(5)(6)}{(1)} = 720$

3. (1723456)

4.The cycle type in S_7 with the largest order is $\underline{43}$. An example of an element of this class would be: $(1234)(567)$.

Assignment 5

Assignment 4 is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

Assignment 5

Exercise 1

1. If $\sigma \in A_n$ and $\tau \in S_n$, show that $\tau^{-1}\sigma\tau \in A_n$.
2. What are the possible cycle structures of elements of A_5? What about A_6?

Answer

1. Let $\sigma \in A_n$ and $\tau \in S_n$.

If $\tau \in A_n$ then $\tau^{-1}\sigma\tau \in A_n$. Otherwise τ is odd permutation and τ^{-1} is also odd (show). Then sum of odd numbers is even, $\tau^{-1}\sigma\tau \in A_n$.

2, The possible cycle types in A_5 are:
$11111, 221, 311$
The possible cycle types in A_6 are:
$111111, 2211, 3111, 33, 42$

Exercise 2

1. Find all of the subgroups in A_4. What is the order of each subgroup?
2. What are the conjugacy classes of A_4?
3. Let $H = \{e, (12)(34), (13)(24), (14)(23)\}$. Find the left cosets and right cosets of H in A_4.

Answer

1. Since $|A_4| = 12$, by Lagrange's theorem, the possible order of subgroups are $1, 2, 3, 4, 6$ and 12. But A_4 has no subgroup of order 6 (done in class).
Hence, the subgroups of A_4 are:
Order $1 : \{e\}$
Order $2 : \{e, (12)(34)\}, \{e, (13)(24)\}, \{e, (14)(23)\}$
Order $3 : \{e, (123), (321)\}, \{e, (124), (421)\}, \{e, (134), (431)\}, \{e, (234), (431)\}$
Order $4 : \{e, (12)(34), (13)(24), (14)(23)\}$
Order $12 : A_4$

2. Show that the conjugacy classes of A_4 are:
$\{e\}, \{(12)(34), (13)(24), (14)(23)\}, \{(123), (134), (243), (142)\}, \{(321), (431), (234), (124)\}$.

3. Since $[A_4 : H] = \frac{12}{4} = 3$. Hence there are 3 left cosets of H in A_4 and 3 right cosets of H in A_4
Left cosets:
$eH = H = (12)(34)H = (13)(24)H = (14)(23)H$
Since $(123)(12)(34) = (134)$, $(123)(13)(24) = (243)$, $(123)(14)(23) = (142)$,
$(123)H = (134)H = (243)H = (142)H = \{(123), (134), (243), (142)\}$
Since $(132)(12)(34) = (234)$, $(132)(13)(24) = (124)$, $(132)(14)(23) = (143)$.
$(132)H = (234)H = (124)H = (143)H = \{(132), (234), (124), (143)\}$
Right cosets:
$He = H = H(12)(34) = H(13)(24) = (14)(23)H$
Since $(12)(34)(123) = (243)$, $(13)(24)(123) = (142)$, $(14)(23)(123) = (134)$,
$H(123) = H(243) = H(142) = H(134) = \{(123), (243), (142), (134)\}$
Since $(12)(34)(132) = (143)$, $(13)(24)(132) = (234)$, $(14)(23)(132) = (124)$,
$(132)H = (143)H = (234)H = (124)H = \{(132), (143), (234), (124)\}$.

Exercise 3

1. Find the center of D_4 and D_5. Justify your answer.
2. What is the center of D_n?
3. Find the conjugacy classes of D_4. Justify your answer.

Answer

1. Consider $a = s^r k$ and $b = r^j$ in D_n for some $0 \leq k, j < n$. Then

$$ab = s^{r(k+j)}, \tag{1}$$

and,

$$ba = s^{r(k-j)}. \tag{2}$$

The equation $ab = ba$ implies that

$$k - j \equiv k + j \pmod{n}. \tag{3}$$

But this is only true if $j = \frac{n}{2}$ or $j = 0$.
Therefore, all reflections are not in the center of D_n. Furthermore, the only rotation that is in the center is $r^{\frac{n}{2}}$ (and trivially e).
So, if n is odd, then the center of D_n is $\{e\}$, otherwise, the center of D_n is $\{e, r^{\frac{n}{2}}\}$.
For example,

$$Z(D_4) = \{e, r^2\}, \quad Z(D_5) = \{e\}. \tag{4}$$

2. The center of D_n is $\{e\}$ if n is odd and $\{e, r^{n/2}\}$ if n is even.

3.

Let $D_4 =< r, s | r^4 = e, s^2 = e, srs = r^{-1} >$.
The conjugacy classes of D_4 are $\{e\}, \{r^2\}, \{r, r^3\}, \{s, r^2 s\}, \{rs, r^3 s\}$.
Clearly, $[e] = \{e\}$.

Consider the following for the class $[r^m]$ for some m:

$$r^n r^m r^{-n} = r^m, \tag{5}$$

and

$$s r^n r^m r^{-n} s = r^{-m}, \tag{6}$$

for all n. Therefore, $[r^m] = \{r^m, r^{-m}\}$. That is,

$$[r] = \{r, r^3\}, \quad [r^2] = \{r^2\}. \tag{7}$$

Consider the class $[sr^m]$ for some m. We have:

$$r^n s r^m r^{-n} = s r^{m-2n}, \tag{8}$$

and

$$s r^n s r^m s r^{-n} = s s r^{-n+m+n} = s r^{-m}. \tag{9}$$

for all n. Since D_4 has an even number of rotations, we can partition the reflections into two conjugacy classes: even and

odd. If there were only one conjugacy class of reflections, $m-2n$ would not cycle properly. Thus, we have:

$$[sr^2] = \{sr^n \mid n \in 2\mathbb{N}\} = \{s, sr^2\}, \tag{10}$$

and

$$[sr] = \{sr, sr^3\}. \tag{11}$$

To summarize, the conjugacy classes are:

$$[e], [r], [r^2], [s], [sr]. \tag{12}$$

Thus, the members of a conjugacy class of D_4 are different but have the same type of effect on a square:

1. r and r^3 are a 90-degree rotation in some direction,
2. s and r^2s are a reflection across a diagonal,
3. rs and r^3s are a reflection across an edge bisector.

? Exercise 4

List all of the subgroups of S_4. Find each of the following sets:

1. $\{\sigma \in S_4 : \sigma(1) = 3\}$
2. $\{\sigma \in S_4 : \sigma(2) = 2\}$
3. $\{\sigma \in S_4 : \sigma(1) = 3 \text{ and } \sigma(2) = 2\}$.
4. Are any of these sets subgroups of S_4?

? Exercise 5

Let $\sigma \in S_X$. If $\sigma^n(x) = y$ for some $n \in \mathbb{Z}$, we will say that $x \sim y$.

1. Show that $\sim$ is an equivalence relation on X.
2. Define the orbit of $x \in X$ under $\sigma \in S_X$ to be the set

$$\mathcal{O}_{x,\sigma} = \{y : x \sim y\}.$$

Compute the orbits of each element in $\{1, 2, 3, 4, 5\}$ under each of the following elements in S_5:

$$\alpha = (1254)$$
$$\beta = (123)(45)$$
$$\gamma = (13)(25).$$

That is for example:

$$\begin{aligned}\mathcal{O}_{x,\sigma} &= \{y \in \{1, 2, 3, 4, 5\} : x \sim y\} \\ &= \{y : \sigma^n(x) = y, \text{for some } n \in \mathbb{N}\}\end{aligned}$$

3. If $\mathcal{O}_{x,\sigma} \cap \mathcal{O}_{y,\sigma} \neq \emptyset$, prove that $\mathcal{O}_{x,\sigma} = \mathcal{O}_{y,\sigma}$. The orbits under a permutation σ are the equivalence classes corresponding to the equivalence relation $\sim$.
   A subgroup H of S_X is transitive if for every $x, y \in X$, there exists a $\sigma \in H$ such that $\sigma(x) = y$. Prove that $\langle\sigma\rangle$ is transitive if and only if $\mathcal{O}_{x,\sigma} = X$ for some $x \in X$.

Assignment 5 is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

Assignment 6

Exercise 1

1. Find subgroups H and K of D_4 such that K is normal to H and H is normal to D_4 but K is not normal to D_4.
2. Find subgroups H and K of S_4 such that K is normal to H and H is normal to S_4 but K is not normal to S_4.
3. Prove or disprove: If all the subgroups of a group G are normal subgroups of G, then G is abelian.

Answer

1. Let $G = D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$ with $r^4 = 4, s^2 = e$ and $srs = r^{-1}$. Since $|D_4| = 8$, possible order of subgroups are $1, 2, 4$ and 8. Let $H = \{1, r^2, s, sr^2\}$. We shall show that H is normal to D_4. Consider the following Cayley table for H,

Table 1: Cayley Table

	e	r^2	s	sr^2
e	e	r^2	s	sr^2
r^2	r^2	e	sr^2	s
s	s	sr^2	e	r^2
sr^2	sr^2	s	r^2	e

Hence, $H \leq G$. By Lagranges Theorem, $[G : H] = \frac{|G|}{|H|} = 2, gH = Hg, \forall\ g \in G$. Thus, $H \trianglelefteq G$.

Choose $K = \{e, s\}$. We shall show that K is normal to H and K is not normal to D_4. Consider the following Cayley table for H,

Table 2: Cayley Table

	e	s
e	e	s
e	e	s
s	s	e

Clearly $K \leq G$ and $K \leq H$. Since $[H : K] = 2$, then $hK = Kh, \forall\ h \in H$. Therefore $K \trianglelefteq H$. Let $k = s \in K$ and $g = r \in G$. Consider $gkg^{-1} = rsr^{-1} = sr^{-1}r^{-1} = sr^{-2} = sr^2 \notin K$. Thus $K \ntrianglelefteq G$.

2. Let $G = S_4, H = K_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ and $K = \{e, (12)(34)\}$. Consider the Cayley table for H and K,

	e	(1,2)(3,4)	(1,3)(2,4)	(1,4)(2,3)
e	e	(1,2)(3,4)	(1,3)(2,4)	(1,4)(2,3)
(1,2)(3,4)	(1,2)(3,4)	e	(1,4)(2,3)	(1,3)(2,4)
(1,3)(2,4)	(1,3)(2,4)	(1,4)(2,3)	e	(1,2)(3,4)
(1,4)(2,3)	(1,4)(2,3)	(1,3)(2,4)	(1,2)(3,4)	e

	e	(1,2)(3,4)
e	e	(1,2)(3,4)
(1,2)(3,4)	(1,2)(3,4)	e

Then clearly, $H \leq G$, $K \leq G$. We shall show that $H \trianglelefteq G$ and $K \trianglelefteq H$.

By Lagrange's Theorem, $[H : K] = \frac{|H|}{|K|} = 2, gK = Kg, \forall\ g \in H$. Thus, $K \trianglelefteq H$.

Now, by Lagrange's Theorem, $[G : H] = \frac{|G|}{|H|} = \frac{24}{4} = 6$, Hence H has 6 cosets in G.

Now, consider the left cosets of H in G:

$$eH = \{ee, e(12)(34), e(13)(24), e(14)(23)\} = \{e, (12)(34), (13)(24), (14)(23)\} \quad (1)$$

$$= ((1,2)(3,4))H = ((1,3)(2,4))H = ((1,4)(2,3))H. \quad (2)$$

$$(1,2,3)H = \{(1,2,3)e, (1,2,3)(12)(34), (1,2,3)(13)(24), (1,2,3)(14)(23)\} = \{(1,2,3), (1,3,4), (2,4,3), (4,2,1)\} = (1,3,4)H = (2,4,3)H = (4,2,1)H. \quad (3)$$

$$(3,2,1)H = \{(3,2,1)e, (3,2,1)(12)(34), (3,2,1)(13)(24), (3,2,1)(14)(23)\} = \{(3,2,1), (2,3,4), (1,2,4), (1,4,3)\} = (2,3,4)H = (1,2,4)H = (1,4,3)H. \quad (4)$$

$$(12)H = \{(12), (34), (1324), (1243)\}. \quad (5)$$

$$(13)H = \{(13), (24), (1423), (1234)\}. \quad (6)$$

$$(14)H = \{(14), (23), (1342), (1432)\}. \quad (7)$$

And the right cosets of H are:

$$He = \{ee, (12)(34)e, (13)(24)e, (14)(23)e\} = \{e, (12)(34), (13)(24), (14)(23)\} = H((1,2)(3,4)) = H((1,3)(2,4)) = H((1,4)(2,3)) \quad (8)$$

$$H(1,2,3) = \{e(1,2,3), (12)(34)(1,2,3), (13)(24)(1,2,3), (14)(23)(1,2,3)\} = \{(1,2,3), (2,4,3), (1,4,2), (1,3,4)\} = H(1,3,4) = H(2,4,3) = H(1,4,2) \quad (9)$$

$$H(3,2,1) = \{e(3,2,1), (12)(34)(3,2,1), (13)(24)(3,2,1), (14)(23)(3,2,1)\} = \{(3,2,1), (1,4,3), (2,3,4), (1,2,4)\} = H(2,3,4) = H(1,2,4) = H(1,4,3) \quad (10)$$

$$H(12) = \{(12), (34), (1324), (1243)\}. \quad (11)$$

$$H(13) = \{(13), (24), (1423), (1234)\}. \quad (12)$$

$$H(14) = \{(14), (23), (1342), (1432)\}. \quad (13)$$

Since the right cosets are the same as the left cosets, we know that H is normal in G.

We shall show that K is not a normal subgroup of S_4. Since $(1,2,3)(12)(34)(3,2,1) = (1,3)(2,4) \notin K$, K is not a normal subgroup of S_4.

3. Consider $G = Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. Then, by Lagrange's theorem, possible orders of subgroups of Q_8 are $1, 2, 4$ and 8. The trivial subgroups Q_8 and $\{e\}$ of order 8 and 1 are normal subgroups of G. Let H be a subgroup of order 4. Then, by Lagrange's Theorem, $[G : H] = \frac{|G|}{|H|} = \frac{8}{4} = 2$. Hence the subgroups of order 4 (namely $H_1 = \{1, -1, i, -i\}, H_2 = \{1, -1, j, -j\}, H_3 = \{1, -1, k, -k\}$) are normal subgroups of G. Consider the subgroups of order 2, $\langle -1 \rangle = Z(Q_8)$. Hence, the subgroup of order 4 is a normal subgroup of G. Therefore, all subgroups of G are abelian. However, since $ij = k \neq -k = ji$, G is not abelian.

? Exercise 2

1. Let $G =< a >$ where $|a| = 12$, and let $H =< a^4 >$. Find all cosets in G/H and write down the Cayley table. Is G/H cyclic? Why or why not?
   Find the cosets in $D_6/Z(D_6)$, write down the Cayley table of $D_6/Z(D_6)$. Is $D_6/Z(D_6)$ cyclic, why or why not?

Answer

1. Let $G = \langle a \rangle$ and let $H = \langle a^4 \rangle$. Then, $|H| = \frac{12}{gcd(12,4)} = \frac{12}{4} = 3$. Hence, by Lagrange's Theorem. $[G : H] = \frac{|G|}{|H|} = \frac{12}{3} = 4$, Hence H has 4 cosets in G.

First, let's find all elements in G/H.

$$G = \{a, a^2, \ldots\ a^{10}, a^{11}, e\}$$
$$H = \{a^4, a^8, e\}$$
$$eH = \{a^4, a^8, e\} = a^4H = a^8H$$
$$aH = \{a, a^5, a^9\} = a^5H = a^9H$$
$$a^2H = \{a^2, a^6, a^{10}\} = a^6H = a^{10}H$$
$$a^3H = \{a^3, a^7, a^{11}\} = a^7H = a^{11}H$$
$$G/H = \{H, aH, a^2H, a^3H\}$$

The Cayley table for G/H is:

$\cdot$	H	aH	a^2H	a^3H
H	H	aH	a^2H	a^3H
aH	aH	a^2H	a^3H	H
a^2H	a^2H	a^3H	H	aH
a^3H	a^3H	H	aH	a^2H

From the table, $G/H = \langle aH \rangle$. Hence G/H is a cyclic group.

2. Find the cosets in $D_6/Z(D_6)$, write down the Cayley table of $D_6/Z(D_6)$. Is $D_6/Z(D_6)$ cyclic, why or why not?

Answer

Find all the cosets in $D_6/Z(D_6)$:

Let $G = D_6 = \{e, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}$ and let $H = Z(D_6) = \{e, r^3\}$. Then $D_6/Z(D_6) = \{gZ(D_6) | g \in G\}$.

Index of $Z(D_6)$ in D_6} The index of $Z(D_6)$ in D_6 is calculated as follows:

$$[D_6 : Z(D_6)] = \frac{|D_6|}{|Z(D_6)|} = \frac{12}{2} = 6. \tag{14}$$

Therefore, the factor group $D_6/Z(D_6)$ has 6 elements.

$$\begin{array}{lll} er^3 = r^3, & r^3r^3 = r^6 = e, & \{e, r^3\} = eH = r^3H \\ rr^3 = r^4, & r^4r^3 = r^7 = r, & \{r, r^4\} = rH = r^4H \\ r^2r^3 = r^5, & r^5r^3 = r^8 = r^2, & \{r^2, r^5\} = r^2H = r^5H \\ sr^3 = sr^3, & sr^3r^3 = sr^6 = s, & \{s, sr^3\} = sH = sr^3H \\ srr^3 = sr^4, & sr^4r^3 = sr^7 = sr, & \{sr, sr^4\} = srH = sr^4H \\ sr^2r^3 = sr^5, & sr^5r^3 = sr^8 = sr^2, & \{sr^2, sr^5\} = sr^2H = sr^5H \end{array}$$

The Cayley table for $D_6/Z(D_6)$ is:

$\cdot$	$Z(D_6)$	$rZ(D_6)$	$r^2Z(D_6)$	$sZ(D_6)$	$rsZ(D_6)$	$r^2sZ(D_6)$
$Z(D_6)$	$Z(D_6)$	$rZ(D_6)$	$r^2Z(D_6)$	$sZ(D_6)$	$rsZ(D_6)$	$r^2sZ(D_6)$
$rZ(D_6)$	$rZ(D_6)$	$r^2Z(D_6)$	$Z(D_6)$	$rsZ(D_6)$	$r^2sZ(D_6)$	$sZ(D_6)$
$r^2Z(D_6)$	$r^2Z(D_6)$	$Z(D_6)$	$rZ(D_6)$	$r^2sZ(D_6)$	$sZ(D_6)$	$rsZ(D_6)$
$sZ(D_6)$	$sZ(D_6)$	$rsZ(D_6)$	$r^2sZ(D_6)$	$Z(D_6)$	$rZ(D_6)$	$r^2Z(D_6)$
$rsZ(D_6)$	$rsZ(D_6)$	$r^2sZ(D_6)$	$sZ(D_6)$	$rZ(D_6)$	$r^2Z(D_6)$	$Z(D_6)$
$r^2sZ(D_6)$	$r^2sZ(D_6)$	$sZ(D_6)$	$rsZ(D_6)$	$r^2Z(D_6)$	$Z(D_6)$	$rZ(D_6)$

Is $D_6/Z(D_6)$ Cyclic?

We analyze the orders of the elements of $D_6/Z(D_6)$:

$$|\langle eZ(D_6)\rangle| = 1, \quad |\langle rZ(D_6)\rangle| = 3, \quad |\langle r^2Z(D_6)\rangle| = 3, \tag{15}$$

$$|\langle sZ(D_6)\rangle| = 2, \quad |\langle rsZ(D_6)\rangle| = 2, \quad |\langle r^2sZ(D_6)\rangle| = 2. \tag{16}$$

Thus, $D_6/Z(D_6)$ has no elements of order 6, and therefore, it has no possible generators. Hence, $D_6/Z(D_6)$ is not a cyclic group.

3. Prove or disprove the following statements: If H is a normal subgroup of G such that H and G/H are abelian, then G is abelian.

Answer

Counterexample: Let $G = S_3$ and $H = A_3$. Then

$$|G/H| = [G : H] = 2. \tag{17}$$

Thus, H is a normal subgroup of G, and G/H is cyclic. Clearly, A_3 is also cyclic. Therefore, both G/H and H are abelian. However, S_3 is not abelian.

? Exercise 3

1. Let G be a group. Show that the center of the group $Z(G)$ is a normal subgroup of G.
2. If $G/Z(G)$ is cyclic , then G is abelian.
3. Let G be a non-ablian group of order pq, where p and q are prime. Then the center of G, $Z(G) = \{e\}$.

Answer

1. First we shall show that $Z(G)$ is a subgroup of G. Since $e \in G$ and $eg = ge$, $\forall g \in G$. Thus $e \in Z(G)$. Let $g_1, g_2 \in Z(G)$. Then $g_1g = gg_1, g_2g = gg_2$ for all $g \in G$.

Let $g \in G$. Consider $g(g_1g_2) = (gg_1)g_2 = (g_1g)g_2 = g_1(gg_2) = g_1(g_2g) = (g_1g_2)g$. Thus $(g_1g_2 \in Z(G)$.

Since $g_1g = gg_1$, $g_1^{-1}(g_1g) = g_1^{-1}(gg_1) \implies gg_1^{-1} = g_1^{-1}g$. Thus $g_1^{-1} \in Z(G)$. Thus $Z(G)$ is a subgroup of G.

Since $g_1 \in Z(G)$, $g^{-1}g_1g = g_1 \in Z(G)$. Thus $g^{-1}Z(G)g \subset Z(G)$. Hence $Z(G)$ is a normal subgroup of G.

2. Suppose $G/Z(G)$ is cyclic. Then $G/Z(G) = \langle (gZ(G))\rangle$, for some $g \in G$. Let $g_1, g_2 \in G$ Then $g_1Z(G) = g^mZ(G)$, $g_2Z(G) = (gZ(G))^n = g^nZ(G)$, for some $m, n \in \mathbb{Z}$. Thus $g_1 = g^mf_1$, $g_2 = g^nf_2$, for some $f_1, f_2 \in Z(G)$. Now consider:

$$g_1g_2 = g^mf_1g^nf_2, \tag{18}$$

$$= g^mg^nf_1f_2, \tag{19}$$

$$= g^{m+n}f_1f_2, \tag{20}$$

$$= g^{n+m} f_1 f_2, \tag{21}$$

$$= g^n f_2 g^m f_1, \tag{22}$$

$$= g_2 g_1. \tag{23}$$

Thus, $g_1 g_2 = g_2 g_1$, which shows that G is abelian.

3. Let $H := Z(G)$. Since $H \leq G$, by Lagrange's Theorem (Theorem 4.1.4), we know that $|H| \mid |G|$. Hence the potential values of $|H|$ are $1, p, q, pq$. Let's consider each.

Case 1:$|H| = pq$, If $|H| = pq$ then $|H| = |G|$, and $H = G$. This would mean that $G = Z(G)$, but since G is non-abelian, this is a contradiction. Therefore, $|H| \neq pq$.

Case 2:$|H| = p$ or $|H| = q$. This means that H is of prime order, and by the previous problem, this implies that G is abelian. Again, this is a contradiction. Therefore $|H| \neq p$ and $|H| \neq q$.

Therefore, if G is a non-abelian group of order pq, then $Z(G) = \{e\}$.

? Exercise 4

1. Let $h : G \to G_1$ be a group homomorphism. If K is normal to subgroup of G, then show that $h(K)$ is a normal subgroup of $h(G)$.
2. If $h_1 : G \to G_1$ is a group homomorphism and $G = \langle X \rangle$ is generated by a subset X, then show that $h = h_1$ if and only if $h(x) = h_1(x), \forall x \in X$.
3. Show that there are almost six homomorphisms from S_3 to a cyclic group of order 6, $\mathbb{Z}_6$.

Answer

1. Let $k_1, k_2 \in K$, then since K is a subgroup of G, then $h(k_1 k_2) = h(k_1)h(k_2) \in h(K)$. The identity element $e \in K$ maps to $h(e) = e_{G_1}$ (the identity in G_1), so $e_{G_1} \in h(K)$. If $k \in K$, then $k^{-1} \in K$ and hence $h(k^{-1}) = h(k)^{-1} \in h(K)$. Thus, $h(K)$ is a subgroup of $h(G)$. To show $h(K) \trianglelefteq h(G)$, we need to show that for every $h(g) \in h(G)$ and $h(k) \in h(K)$,

$$h(g)h(k)h(g)^{-1} \in h(K). \tag{24}$$

Given $h(g) \in h(G)$, there exists some $g \in G$ such that $h(g) = h(g)$. Similarly, for $h(k) \in h(K)$, there exists some $k \in K$. Consider the element gkg^{-1} in G. Since $K \trianglelefteq G$, we have:

$$gkg^{-1} \in K. \tag{25}$$

Consider,

$$h(gkg^{-1}) = h(g)h(k)h(g^{-1}) = h(g)h(k)h(g)^{-1}. \tag{26}$$

Since $gkg^{-1} \in K$ and K is mapped into $h(K)$, we get:

$$h(gkg^{-1}) \in h(K). \tag{27}$$

But $h(gkg^{-1}) = h(g)h(k)h(g)^{-1}$, hence:

$$h(g)h(k)h(g)^{-1} \in h(K). \tag{28}$$

This shows that $h(K)$ is normal in $h(G)$. Hence,

$$K \trianglelefteq G \implies h(K) \trianglelefteq h(G). \tag{29}$$

2. Discussed in Tutorial.

3. Discussed in Tutorial.

? Exercise 5

1. Let G be a group and let $a \in G$ then show that $\sigma_a : G \to G$ defined by $\sigma_a(g) = aga^{-1}$is an isormorphism.
2. Prove or disprove the following statements:

a. $U(5)$ is isormorphic to $\mathbb{Z}_4$.

b. $\mathbb{Z}$ under addition is isormorphic to $\mathbb{Q}$ under addition.

Answer

a. Let $\phi : \mathbb{Z}_4 \to U(5)$ be defined by: $\phi(n) = 2^n \pmod 5$. That is

$\phi(0) = 1$, $\phi(1) = 2$, $\phi(3) = 8 \equiv 3 \pmod 5$, and $\phi(2) = 4$.

We will show $\phi(a + b) = \phi(a)\phi(b)$, $\forall a, b \in \mathbb{Z}_4$.

We will proceed by proof by exhaustion.

There are 10 cases to consider since addition and multiplication are both commutative.

$\phi(0+0) = \phi(0) = 1 = (1)(1) = \phi(0) \times \phi(0)$.

$\phi(0+1) = \phi(1) = 2 = (1)(2) = \phi(0) \times \phi(1)$.

$\phi(0+2) = \phi(2) = 4 = (1)(4) = \phi(0) \times \phi(2)$.

$\phi(0+3) = \phi(3) = 3 = (1)(4) = \phi(0) \times \phi(3)$.

$\phi(1+1) = \phi(2) = 4 = (2)(2) = \phi(1) \times \phi(1)$.

$\phi(1+2) = \phi(3) = 3 = (1)(3) = \phi(1) \times \phi(3)$.

$\phi(1+3) = \phi(0) = 1 \equiv (2)(3) = \phi(1) \times \phi(3)$.

$\phi(2+2) = \phi(0) = 1 = (1)(1) = \phi(0) \times \phi(0)$.

$\phi(2+3) = \phi(1) = 2 \equiv (4)(3) = \phi(2) \times \phi(3)$.

$\phi(3+3) = \phi(2) = 4 \equiv (3)(3) = \phi(3) \times \phi(3)$.

Having examined all the possible cases, $\phi(ab) = \phi(a)\phi(b),\ \forall a, b \in \mathbb{Z}_4$.

b. **Counterexample**:

We know that $(\mathbb{Z}, +)$ is a cyclic group generated by $\langle -1 \rangle$ and $\langle +1 \rangle$.

Assume that $(\mathbb{Q}, +)$ is cyclic. We will show that $(\mathbb{Q}, +)$ is not cyclic.

Since $\mathbb{Q}$ is cyclic, it can be generated by some $\frac{p}{q}, p, q(\neq 0) \in \mathbb{Z}$.

Thus $\frac{p}{2q} = n\frac{p}{q}$ for some $n \in \mathbb{Z}$. That is $\frac{p}{2q} = \frac{np}{q} \implies n = \frac{1}{2}$.

This is a contradiction, and therefore $(\mathbb{Q}, +)$ is not cyclic.

? Exercise 6

List or characterize all of the following rings' units. Justify your answer.

1. $\mathbb{Z}_{12}$
2. $M_{22}(\mathbb{Z}_2)$
3. $\mathbb{Z}(i)$

Answer

1. Let $a \in \mathbb{Z}_{12}$ be a unit. Then there exists $x \in \mathbb{Z}_{12}$ such that $ax \equiv 1 \pmod{12}$. Thus $12 \mid (ax - 1) \implies (ax - 1) = 12y$, for some $y \in \mathbb{Z}$. Therefore, $ax - 12y = 1$. Hence $gcd(a, 12) = 1$. Therefore the units are $1, 5, 7, 11$.

2. Let $A \in M_{22}(\mathbb{Z}_2)$ be a unit. . Then there exists $X \in M_{22}(\mathbb{Z}_2)$ such that

$$AX = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

, and $det(A) \neq 0$. The determinant of a 2×2 matrix A is:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \text{and} \quad \det(A) = ad - bc \pmod{2}. \tag{30}$$

We now list all matrices in $M_2(\mathbb{Z}_2)$ with $\det(A) \equiv 1 \pmod{2}$. These matrices are:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \tag{31}$$

Thus, the units in $M_2(\mathbb{Z}_2)$ are these six matrices. Each of these has an inverse in $M_2(\mathbb{Z}_2)$, confirming that they are units.

3. Let $z = a + bi \in \mathbb{Z}[i]$ where $a, b \in \mathbb{Z}$ be a unit. Then multiplicative inverse of z is given by z^{-1}. Then $zz^{-1} = 1 \implies |z||z^{-1}| = 1$. Since $|z|$ is a nonnegative integer, $|z| = 1$. Thus $a^2 + b^2 = 1$.)*Hence*\($a = \pm 1$ or $b = \pm 1$.

Therefore the units of $\mathbb{Z}[i]$ are $\{-1, 1, -i, i\}$.

Exercise 7

An element e of a ring R is said to be idempotent if $e^2 = e$.

1. If e is an idempotent of a ring R, then show that $1-2e$ is a unit.
2. Find all idempotents in $\mathbb{Z}_{12}$.
3. Find all the idempotents in an integral domain R.

Answer

1. Let $e \in R$ be an idempotent of a ring R. We shall show that $1-2e$ is a unit of R.

Consider,

$$\begin{aligned}(1-2e)(1-2e) &= 1-2e-2e+4e^2 \\ &= 1-4e+4e \\ &= 1.\end{aligned}$$

Since $(1-2e)(1-2e) = 1$, $(1-2e)$ is a unit of R.

2. Let x be an idempotent in $\mathbb{Z}_{12}$, Then $x^2 = 1 \pmod{12}$. Let's find these by exhaustion.

Idempotents	Non-Idempotents
$0^2 = 0 \equiv 0 \pmod{12}$	$2^2 = 4 \equiv 4 \pmod{12}$
$1^2 = 1 \equiv 1 \pmod{12}$	$3^2 = 9 \equiv 9 \pmod{12}$
$4^2 = 16 \equiv 4 \pmod{12}$	$5^2 = 25 \equiv 1 \pmod{12}$
$9^2 = 81 \equiv 9 \pmod{12}$	$6^2 = 36 \equiv 0 \pmod{12}$
	$7^2 = 49 \equiv 1 \pmod{12}$
	$8^2 = 64 \equiv 4 \pmod{12}$
	$10^2 = 100 \equiv 4 \pmod{12}$
	$11^2 = 121 \equiv 1 \pmod{12}$

Therefore, the idempotents of $\mathbb{Z}_{12}$ are $\{0, 1, 4, 9\}$.

3. Let e be an idempotent in an integral domain R. Then $e^2 = e \implies e^2 - e = 0 \implies e(e-1) = 0$.

Since the integral domain R contains no zero divisors, $e = 0$ or $e-1 = 0$. Therefore, the idempotents of R are 0, and 1.

Assignment 6 is shared under a not declared license and was authored, remixed, and/or curated by LibreTexts.

Index

Glossary

Sample Word 1 | Sample Definition 1

Detailed Licensing

1 Overview

Title: Abstract Algebra I

Webpages: 60

Applicable Restrictions: Noncommercial

All licenses found:

- CC BY-NC-SA 4.0: 55% (33 pages)
- Undeclared: 45% (27 pages)

2 By Page

- Abstract Algebra I - *CC BY-NC-SA 4.0*
  - Front Matter - *Undeclared*
    - TitlePage - *Undeclared*
    - InfoPage - *Undeclared*
    - Table of Contents - *Undeclared*
    - Licensing - *Undeclared*
    - Preface - *CC BY-NC-SA 4.0*
  - Chapter 0: Preliminaries - *CC BY-NC-SA 4.0*
    - 0.0: Introduction to proofs - *CC BY-NC-SA 4.0*
    - 0.1: Sets - *CC BY-NC-SA 4.0*
    - 0.2: Relations - *CC BY-NC-SA 4.0*
    - 0.3: Functions - *CC BY-NC-SA 4.0*
    - 0.5: Proof Templates - *Undeclared*
    - 0E: Exercises - *CC BY-NC-SA 4.0*
  - Chapter 1: Integers - *CC BY-NC-SA 4.0*
    - 1.1: Division Algorithm - *CC BY-NC-SA 4.0*
    - 1.2: Greatest common divisor and least common multiple - *CC BY-NC-SA 4.0*
    - 1.3: Primes - *CC BY-NC-SA 4.0*
    - 1.4: Integers modulo n - *Undeclared*
    - 1.5 Linear Congruence - *Undeclared*
    - 1E: Exercises - *CC BY-NC-SA 4.0*
  - Chapter 2: Groups - *CC BY-NC-SA 4.0*
    - 2.1: Introduction to Group - *CC BY-NC-SA 4.0*
    - 2.2: Properties of Group Elements - *CC BY-NC-SA 4.0*
    - 2.3: Subgroups - *CC BY-NC-SA 4.0*
    - 2.4: Cyclic groups - *CC BY-NC-SA 4.0*
    - 2E: Exercises - *CC BY-NC-SA 4.0*
  - Chapter 3: Permutation Groups - *CC BY-NC-SA 4.0*
    - 3.1: Symmetric Groups - *CC BY-NC-SA 4.0*
    - 3.2: Alternating Groups - *CC BY-NC-SA 4.0*
    - 3.3: Dihedral Groups (Group of Symmetries) - *CC BY-NC-SA 4.0*
    - 3E: Exercises - *CC BY-NC-SA 4.0*
  - Chapter 4: Cosets, special groups, and homorphism - *Undeclared*
    - 4.1: Cosets and Lagranges Theorem - *Undeclared*
    - 4.2: Normal Supgroups and Factor Groups - *CC BY-NC-SA 4.0*
    - 4.3: Homomorphisms - *Undeclared*
    - 4.4: On Special Groups - *Undeclared*
    - 4.5: Isormormophism theorems - *Undeclared*
    - 4.6: Classification of Groups - *CC BY-NC-SA 4.0*
    - 4E: Exercises - *Undeclared*
  - Chapter 5: Rings and fileds - *CC BY-NC-SA 4.0*
    - 5.1: Introduction to Rings - *CC BY-NC-SA 4.0*
    - 5.2: Ideals and Factor Rings - *Undeclared*
    - 5.3: Ring Homomorphisms - *CC BY-NC-SA 4.0*
    - 5E: Excercises - *CC BY-NC-SA 4.0*
  - Mock Exams (Celebration of Learning) - *Undeclared*
    - Sample final - *Undeclared*
    - Test 1 - *Undeclared*
    - Test 2 - *Undeclared*
  - Sample Assignments with solution - *Undeclared*
    - Assignment 1 - *CC BY-NC-SA 4.0*
    - Assignment 2 - *CC BY-NC-SA 4.0*
    - Assignment 3 - *CC BY-NC-SA 4.0*
    - Assignment 4 - *Undeclared*
    - Assignment 5 - *Undeclared*
    - Assignment 6 - *Undeclared*
  - Back Matter - *Undeclared*
    - Index - *Undeclared*
    - Glossary - *Undeclared*
    - Detailed Licensing - *Undeclared*