Introduction to Abstract Algebra

Dr. Abdullah Al-Azemi

Mathematics Department
Kuwait University

June 1, 2023

Contents

0 Review **1**

0.0 Basic Notation 1

1 Mapping and Operations **3**

1.1 Mappings 3

1.2 Composition. Invertible Mappings 6

1.3 Operations 10

1.4 Composition as an Operation 16

2 Introduction To Groups **19**

2.5 Definition and Examples 19

2.6 Permutations and Symmetric Group 27

2.7 Subgroups 32

3 Equivalence. Congruence. Divisiblity **43**

3.9 Equivalence Relations 43

3.10 Congruence. The Division Algorithm 47

3.11 Integers Modulo n 53

3.12 Greatest Common Divisor. The Euclidean Algorithm 56

3.13 Factorization. Euler's Phi-Function 60

4 Groups **65**

4.14 Elementary Properties 65

4.14.1 Solving Book Problems from Section 14 71

4.15 Direct Products 75

4.16 Cosets 79

4.16.1 Solving Book Problems from Section 16 84

4.17 Lagrange's Theorem. Cyclic Groups 88

4.17.1 Solving Book Problems from Section 17 92

4.18 Isomorphism 95

4.19 More On Isomorphism 101

5 Group Homomorphisms **105**

5.21 Homomorphism of Groups. Kernels 105

5.22 Quotient Groups 111

Chapter

0 Review

Section 0.0: Basic Notation

Definition 0.0.1

- A set is a collection of objects (called elements or members).
- We write $x \in A$ to indicate that an element x belongs to set A, while we write $x \notin A$ to indicate that x does not belong to A.
- For any two sets A and B, we write $A \subseteq B$ if $\forall x \in A, x \in B$.
- **Equality**: $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.
- **Intersection**: $A \cap B = \{x : x \in A \text{ and } x \in B\}$.
- **Union**: $A \cup B = \{x : x \in A \text{ or } x \in B\}$.
- **Difference**: $A - B = \{x : x \in A \text{ and } x \notin B\}$.
- **Cartesian (Cross) Product**: $A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$.
- Note that in general, $A \times B \neq B \times A$.

$\star$ **Notations**: We define the following sets of numbers:

- $\mathbb{N}$: the set of all natural numbers $\{1, 2, 3, \cdots\}$.
- $\mathbb{Z}$: the set of all integers $\{\cdots, -2, -1, 0, 1, 2, \cdots\}$.
- $\mathbb{Q}$: the set of all rational numbers $\{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\}$.
- $\mathbb{R}$: the set of all real numbers.
- $\mathbb{C}$: the set of all complex numbers.
- S^*: the whole set S without the '0' element.
- S^+: the set of all positive numbers in S.

- S^-: the set of all negative numbers in S.
- $M_{n\times n}$: the set of all $n \times n$ matrices with entries of real numbers.
- $N_{n\times n}$: the set of all $n \times n$ non-singular matrices with entries of real numbers.

Chapter 1

Mapping and Operations

Section 1.1: Mappings

Definition 1.1.1

A **mapping** from a set S to a set T is a relationship that maps every element of S to a uniquely determined element of T. Moreover, If $\alpha : S \to T$ is a mapping from S to T, then we say that S is the **domain** and T is the **codomain** of α. Such a mapping is written as $S \xrightarrow{\alpha} T$ sometimes. Moreover, if $S = T$, we simply say that α is a mapping on S.

Example 1.1.1

Let $S = \{a, b, c\}$ and $T = \{1, 2, 3\}$. Let $\alpha : S \to T$ so that:

$$
\begin{array}{rlll}
i.\ \alpha(a) = 1, & \alpha(b) = 2, & \alpha(c) = 3, & \alpha \text{ is a mapping,} \\
ii.\ \alpha(a) = 1, & \alpha(b) = 1, & \alpha(c) = 2, & \alpha \text{ is a mapping,} \\
iii.\ \alpha(a) = 1, & \alpha(a) = 3, & \alpha(b) = 2, & \alpha \text{ is not a mapping.}
\end{array}
$$

Clearly $iii.$ is not a mapping since first α does not map c and second because $\alpha(a) = 1 \neq 3 = \alpha(a)$.

Definition 1.1.2

If $\alpha : S \to T$ is a mapping and $\alpha(a) = b$ for some $a \in S$ and $b \in T$, then we say that b is the **image** of a and that a is the **preimage** of b.
Moreover, if $A \subseteq S$, then $\alpha(A) = \{\alpha(x) : x \in A\} \subseteq T$.

Definition 1.1.3

A mapping (**function**) α from a set S into a set T is **one-to-one** if each element of T has at most one element of S mapped into it. Moreover, α is **onto** T if each element of T has at least one element of S mapped into it.

Definition 1.1.4

A mapping α is called a bijection if it is one-to-one and onto.

Remark 1.1.1

Let $\alpha : S \to T$ be a function. Then,

1. α is a one-to-one function if for all $a, b \in S$, $\alpha(a) = \alpha(b)$ implies $a = b$.
2. α is onto T if for each $b \in T$, there is $a \in S$ such that $\alpha(a) = b$.

Example 1.1.2

Consider the two mappings $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ and $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = x^3$. Decide whether f and g are one-to-one and onto?

Solution:

- Clearly, f is not one-to-one since $f(1) = f(-1) = 1$ but $-1 \neq 1$. Also, f is not onto since there is no $x \in \mathbb{R}$ with $f(x) = -1$ for instance. Therefore f is not a bijection.
- g is one-to-one since if $g(x) = g(y)$, then $x^3 = y^3$ and hence $x = y$. Also it is onto since for any $y \in R$, there is $x = y^{\frac{1}{3}} \in \mathbb{R}$ with $g(x) = (y^{\frac{1}{3}})^3 = y$. Hence g is a bijection.

Example 1.1.3

Let f be a mapping on $\mathbb{N}$ defined by $f(x) = 2x$. Is f a bijection? Explain.

Solution:

Clearly, f is one-to-one since $f(a) = f(b)$ implies that $2a = 2b$ and hence $a = b$. But f is not onto, since $1 \in \mathbb{N}$ and no $a \in \mathbb{N}$ with $f(a) = 1$. That is f is not a bijection.

Exercise 1.1.1

Solve the following exercises from the book at page 14:

- 1.1 – 1.6,
- 1.12 – 1.13.

Section 1.2: Composition. Invertible Mappings

Definition 1.2.1

Let A, B, and C be three nonempty sets. If $f : A \to B$ and $g : B \to C$ are two mappings, then the composition of f and g, denoted by $g \circ f$, is the mapping from A to C defined by $(g \circ f)(x) = g(f(x))$ for each $x \in A$.

Example 1.2.1

Let $A = \{x, y, z\}$, $B = \{1, 2, 3\}$ and $C = \{a, b, c\}$. Define $f : A \to B$ and $g : B \to C$ by

$$f(x) = 2,\ f(y) = 1,\ \text{and}\ \ f(z) = 3,\ \text{and}\ g(1) = b,\ g(2) = c,\ \text{and}\ \ g(3) = a.$$

List all the elements of $g \circ f$.

Solution:

- $(g \circ f)(x) = g(f(x)) = g(2) = c$,
- $(g \circ f)(y) = g(f(y)) = g(1) = b$,
- $(g \circ f)(z) = g(f(z)) = g(3) = a$.

Example 1.2.2

Let f and g be two mapping on $\mathbb{R}$ where $f(x) = 2x + 1$ and $g(x) = x - 1$. Is $g \circ f = f \circ g$? Explain.

Solution:

Clearly,

- $(g \circ f)(x) = g(f(x)) = g(2x + 1) = (2x + 1) - 1 = 2x$, while
- $(f \circ g)(z) = f(g(x)) = f(x - 1) = 2(x - 1) + 1 = 2x - 1$.

Therefore, $g \circ f \neq f \circ g$.

Theorem 1.2.1: This is from Math-250

Assume that $f : A \to B$ and $g : B \to C$ are two mappings. Then,

1. If f and g are onto, then $g \circ f$ is onto.
2. If $g \circ f$ is onto, then g is onto.
3. If f and g are one-to-one, then $g \circ f$ is one-to-one.
4. If $g \circ f$ is one-to-one, then f is one-to-one.
5. If f and g are bijections, then $g \circ f$ is a bijection.

Proof:

Recall this Theorem from Math-250.

1. Assume that both f and g are onto. Let $z \in C$, then there is $y \in B$ such that $g(y) = z$ since g is onto. Also, there is $x \in A$ such that $f(x) = y$ since f is onto. Therefore, $(g \circ f)(x) = g(f(x)) = g(y) = z$ and hence $g \circ f$ is onto.
2. Assume that $g \circ f$ is onto. If $z \in C$, then there is $x \in A$ such that $(g \circ f)(x) = z$ (since $g \circ f$ is onto). That is $g(f(x)) = z$ with $f(x) = y \in B$. Thus g is onto.
3. Assume that both f and g are one-to-one. Then $(g \circ f)(x) = (g \circ f)(y)$ implies $g(f(x)) = g(f(y))$ which implies that $f(x) = f(y)$ since g is one-to-one. Hence $x = y$ because f is one-to-one. Therefore, $g \circ f$ is one-to-one.
4. Assume that $g \circ f$ is one-to-one. Let $f(x) = f(y)$. Then $(g \circ f)(x) = g(f(x)) = g(f(y)) = (g \circ f)(y)$ and since $g \circ f$ is one-to-one, we get that $x = y$. Hence f is one-to-one.
5. Assume that f and g are both bijections. Combining part 1 and part 3 concludes the result. Hence $g \circ f$ is a bijection.

Definition 1.2.2

Let I_A denote the identity mapping on A. That is,

$$I_A(x) = x \quad \text{for every} \quad x \in A.$$

Note that this mapping is an example of a bijection mapping.

Definition 1.2.3

A mapping $g : B \to A$ is an inverse of a mapping $f : A \to B$ if both $g \circ f = I_A$ and $f \circ g = I_B$. In that case, f is called **invertible** and we write $f^{-1} = g$.

Theorem 1.2.2

A mapping $f : A \to B$ is invertible if and only if f is a bijection.

Proof:

„ $\Rightarrow$": Assume that f is invertible. Then $f^{-1} \circ f = I_A$ is one-to-one, and hence f is one-to-one. Moreover, $f \circ f^{-1} = I_B$ is onto and hence f is onto. Therefore, f is a bijection.
„ $\Leftarrow$": Assume that f is a bijection. We construct $f^{-1} : B \to A$ as follows: If $y \in B$, then there is $x \in A$ such that $f(x) = y$ (since f is onto). But since f is one-to-one, this element x is unique. Let $f^{-1}(y) = x$. This is can be done to all elements $y \in B$ and hence $f^{-1} : B \to A$ satisfying $f \circ f^{-1} = I_B$ and $f^{-1} \circ f = I_A$. Thus f is invertible.

Theorem 1.2.3

If $f : A \to B$ is a bijection, then $f^{-1} : B \to A$ is a bijection.

Proof:

This is can be done using your knowledge from Math-250.

Exercise 1.2.1

Solve the following exercises from the book at page 18:

- 2.1 – 2.6,
- 2.11 – 2.13.

Section 1.3: Operations

Definition 1.3.1

A **binary operation** " $*$ " on a set S is a relationship that maps each ordered pair of elements of S to a unique element of S. That is $* : S \times S \to S$, where $S \times S$ is the **Cartesian product** of S with S which contains all ordered pairs (a, b) with $a, b \in S$.

Definition 1.3.2

Let $*$ be a binary operation on a set S. For all $a, b \in S$, $a * b \in S$. This property of $*$ is called **closure** and we say that S is **closed with respect to** $*$.

Note that we write $(S, *)$ for a defined binary operation $*$ on a set S.

Example 1.3.1

Decide if the following is binary operation:

$(\mathbb{N}, -)$	NO, $1, 2 \in \mathbb{N}$ but $1 - 2 = -1 \notin \mathbb{N}$
$(\mathbb{Z}, +)$	YES
$(\mathbb{Z}, -)$	YES
$(\mathbb{Z}, \cdot)$	YES
$(\mathbb{Z}, \div)$	NO, $1, 2 \in \mathbb{Z}$ but $\frac{1}{2} \notin \mathbb{Z}$
$(\mathbb{Q}, \div)$	NO, $0, 1 \in \mathbb{Q}$ but $\frac{1}{0} \notin \mathbb{Q}$
$(\mathbb{Q}^*, \div)$	YES
$(\mathbb{R}, +)$	YES
$(\mathbb{R}, -)$	YES
$(\mathbb{R}, \cdot)$	YES
$(\mathbb{R}^*, \div)$	YES

Example 1.3.2

Let $*$ be defined on $\mathbb{Z}^+$ by $m * n = m^n$ for all $m, n \in \mathbb{Z}^+$. Is $*$ a binary operation? Does the order of elements make any difference?

Solution:

Clearly, for any $m, n \in \mathbb{Z}^+$, $m * n = m^n \in \mathbb{Z}^+$. Thus, $*$ is a binary operation on $\mathbb{Z}^+$. However, the order makes difference since $3 * 2 = 3^2 = 9$ while $2 * 3 = 2^3 = 8$.

Definition 1.3.3

If S is a finite set, then we can specify a binary operation on S by means of a **table**. We put $a * b$ at the intersection of the row containing a and the column containing b, for all $a, b \in S$. Changing one more of the entries in the table will give a different binary operation. Such defined tables are called **Cayley tables**.

Example 1.3.3

Let $S = \{a, b, c\}$. Give two different Cayley tables.

Solution:

$*_1$	a	b	c
a	a	c	c
b	b	b	a
c	b	c	b

$*_2$	a	b	c
a	b	b	b
b	a	b	c
c	b	b	b

Remark 1.3.1

In general there are n^{n^2} Cayley tables for $S = \{a_1, a_2, \cdots, a_n\}$. This is because each row has n positions with n possible elements in each position. That is, each row has n^n possible ways. Overall we have n rows and thus we have $n^n \cdot n^n \cdot \cdots \cdot n^n$ (n-times) which is n^{n^2}.

Example 1.3.4

Decide whether $+$ and $\cdot$ are binary operations on $M_{2\times 2}$

Solution:

Yes, because for any 2×2 matrices, we have

- $\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} a+x & b+y \\ c+z & d+w \end{bmatrix} \in M_{2\times 2}$,
- $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} ax+bz & ay+bw \\ cx+dz & cy+dw \end{bmatrix} \in M_{2\times 2}$,

Definition 1.3.4

A binary operation $*$ on a set S is said to be **associative** if the **associative law**

$$a*(b*c) = (a*b)*c$$

is satisfied for all $a, b, c \in S$.

Definition 1.3.5

A binary operation $*$ on a set S is said to be **commutative** if the **commutative law**

$$a*b = b*a$$

is satisfied for all $a, b \in S$.

Example 1.3.5

Discuss the associative and commutative properties on

1. $(\mathbb{Z}, +)$,
2. $(\mathbb{Z}, -)$,
3. $(\mathbb{Q}^*, \div)$

Solution:

1) Clearly, $m+(n+k) = (m+n)+k$ for all $m, n, k \in \mathbb{Z}$, then $+$ is associative on $\mathbb{Z}$. Also, $m+n = n+m$ for all $m, n \in \mathbb{Z}$ and hence $+$ is commutative on $\mathbb{Z}$.
2) $2-(1-3) = 4$ while $(2-1)-3 = -2$ and hence $-$ is not associative on $\mathbb{Z}$. Moreover, $1-2 \neq 2-1$. Thus $-$ is not commutative on $\mathbb{Z}$.
3) "$\div$" is not associative on $\mathbb{Q}^*$ since $1 \div (3 \div 2) = \frac{2}{3}$ while $(1 \div 3) \div 2 = \frac{1}{6}$. Moreover,

$1 \div 2 \neq 2 \div 1$, hence $\div$ is not commutative on $\mathbb{Q}^*$.

Definition 1.3.6

Let S be a set with a binary operation $*$. An element $e \in S$ is called an **identity** (or identity element) for $*$ on S if

$$e * a = a * e = a$$

for all $a \in S$.

Definition 1.3.7

Let e be an identity for a binary operation $*$ on a set S. An element $b \in S$ is called an **inverse of** a relative to $*$ if

$$a * b = b * a = e.$$

Example 1.3.6

Discuss the identity and inverse elements in what follows:

1. $(\mathbb{Z}, +)$: 0 is the identity element for $+$ on $\mathbb{Z}$, while "$-a$" is the inverse of a relative to $+$ for every $a \in \mathbb{Z}$. Note that $a + (-a) = 0$.

2. $(\mathbb{Q}^*, \cdot)$: 1 is the identity for $\cdot$ on $\mathbb{Q}^*$, while $\frac{1}{a}$ is the inverse of $a \in \mathbb{Q}^*$. That is $a \cdot \frac{1}{a} = 1$ for all $a \in \mathbb{Q}^*$.

3. $(\mathbb{Z}^+, +)$: has no identity and no inverse.

4. $(2\mathbb{Z}, \cdot)$: $2\mathbb{Z} = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$ has no identity and no inverses.

5. $(M_{2\times 2}, +)$: the identity matrix is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and for any $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}$ the inverse element is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

6. $(M_{2\times 2}, \cdot)$: the identity matrix is $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Some matrices have no inverse and some

do. For instance the matrix $\begin{bmatrix} 1 & 2 \\ 0 & 0 \end{bmatrix}$ has no inverse since its determinant equals zero.

7. $(N_{2\times 2}, \cdot)$: the identity matrix is I_2 and the inverse of a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is given by $\frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. That is, $A^{-1} = \frac{1}{|A|}\mathrm{adj}(A)$.

Exercise 1.3.1

Solve the following exercises from the book at page 23:

- 3.1 – 3.8,
- 3.13.

Exercise 1.3.2

Let $*$ be defined by $m * n = m^n$ for all positive integers m and n. Is $*$ a commutative binary operation on $\mathbb{Z}^+$? Explain.

Section 1.4: Composition as an Operation

Example 1.4.1

Let S be any nonempty set, and let $M(S)$ denote the set of all mappings from S to S. Is "$\circ$", the composition, an operation on $M(S)$? Explain.

Solution:

Let $\alpha, \beta \in M(S)$. Then $\alpha : S \to S$ and $\beta : S \to S$ and hence $\beta \circ \alpha : S \to S$. Thus, $\beta \circ \alpha \in M(S)$ and the composition "$\circ$" is an operation on $M(S)$.

Theorem 1.4.1

Let S denote any nonempty set. Then

1. Composition is an associative operation on $M(S)$, with the identity element I_S.
2. Composition is an associative operation on the set of all invertible mappings in $M(S)$, with identity I_S.

Proof:

1. Let $f, g, h \in M(S)$. Then for any $x \in S$, we have

$$[h \circ (g \circ f)](x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = [(h \circ g) \circ f](x).$$

That is $\circ$ is associative on $M(S)$. Moreover, it is clear that $f \circ I_S = I_S \circ f = f$ for any $f \in M(S)$.

2. Assume that $f, g \in M(S)$ and that both are invertible. Thus both f and g are bijections and hence $g \circ f$ is a bijection which implies that $g \circ f$ is invertible. Since the composition is associative on $M(S)$, it is associative on any of its subsets and hence it is associative on the subset of invertible mappings. Moreover, I_S is invertible and thus it is the identity element on the subset of invertible elements in $M(S)$.

Remark 1.4.1

Note that the composition operation "$\circ$" is not commutative in general since $f \circ g \neq g \circ f$ for some mappings f and g.

Chapter

2 Introduction To Groups

Section 2.5: Definition and Examples

Definition 2.5.1

A **group** $(G, *)$ is a set G, **closed under a binary operation** $*$, such that the following conditions are satisfied

$\mathcal{G}_1$: associativity: $*$ is associative on G,

$\mathcal{G}_2$: identity element: there is $e \in G$ such that $e * g = g * e = g$ for every $g \in G$,

$\mathcal{G}_3$: inverse element: for every $g \in G$, there exists $h \in G$ (usually written as $h = g^{-1}$) such that $g * h = h * g = e$. That is every element in G has an inverse in G.

Example 2.5.1

Show that the set of even integers, denoted by $2\mathbb{Z}$, with addition is a group.

Solution:

We show that $(2\mathbb{Z}, +)$ is a group by showing the conditions of Definition 2.5.1 as follows:

$\mathcal{G}_1$: Let $a, b, c \in 2\mathbb{Z}$. Then $(a + b) + c = a + b + c = a + (b + c)$ and hence $+$ is associative.

$\mathcal{G}_2$: The identity element is $0 \in 2\mathbb{Z}$ since $a + 0 = 0 + a = a$ for all $a \in 2\mathbb{Z}$.

$\mathcal{G}_3$: For any $a \in 2\mathbb{Z}$, $-a \in 2\mathbb{Z}$ and $a + (-a) = 0 = (-a) + a$.

Therefore $(2\mathbb{Z}, +)$ is a group.

Example 2.5.2

Is $(\mathbb{Z}^+, +)$ a group? Explain.

Solution:

No. There is no identity element in $\mathbb{Z}^+$ and there is no inverse in $\mathbb{Z}^+$ for any element in $\mathbb{Z}^+$.

Example 2.5.3

Decide whther $(M_{2\times 2}, \cdot)$ "the set of all 2×2 matrices" is a group.

Solution:

Clearly, $\cdot$ is associative on $M_{2\times 2}$ and there is identity element $I_2 \in M_{2\times 2}$. But for some elements $A \in M_{2\times 2}$ there is no inverse. For instance the inverse of $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ does not exist. Thus $(M_{2\times 2}, \cdot)$ is not a group.

Definition 2.5.2

A group G is called **abelian** if its binary operation is commutative. It is called **non-abelian** otherwise.

Definition 2.5.3

For $a, n \in \mathbb{Z}$ with $n > 0$, define the congruence class of a modulo n in $\mathbb{Z}$ by

$$[a] = \overline{a} = \{x \in \mathbb{Z} : a \equiv_n x \Leftrightarrow n \mid a - x\}.$$

Moreover, for $[a], [b] \in \mathbb{Z}_n$, define

$$[a] \oplus [b] = [a + b].$$

Theorem 2.5.1

Let n be a positive integer, then $\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$ is an abelian group with respect to the operation $\oplus$.

Proof:

$\mathcal{G}_1$:

$$\begin{aligned} [a] \oplus ([b] \oplus [c]) &= [a] \oplus [b + c] = [a + b + c] = [(a + b) + c] \\ &= [a + b] \oplus [c] = ([a] \oplus [b]) \oplus [c]. \end{aligned}$$

$\mathcal{G}_2$: The identity is $[0]$ since $[0] \oplus [a] = [0 + a] = [a] = [a + 0] = [a] \oplus [0]$.

$\mathcal{G}_3$: The inverse of $[a]$ is $[-a]$:

$$[a] \oplus [-a] = [a + (-a)] = [0] = [(-a) + a] = [-a] \oplus [a].$$

Note that $[-a]$ is congruent modulo n to exactly one integer in $\{[0], [1], \cdots, [n-1]\}$.

To show that $\mathbb{Z}_n$ is abelian, let $[a], [b] \in \mathbb{Z}_n$, then

$$[a] \oplus [b] = [a+b] = [b+a] = [b] \oplus [a].$$

Thus, $\mathbb{Z}_n$ is abelian group with respect to $\oplus$.

Remark 2.5.1

Notation:

For simplicity, we write $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$ instead of $\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$.

Example 2.5.4

The following are examples of some groups:

$$(\mathbb{Z}, +), (\mathbb{Q}, +), (M_{2\times 2}, +), \text{ and } (M_{m\times n}, +).$$

$$(N_{n\times n}, \cdot), (\mathbb{Q}^*, \cdot), (\mathbb{Q}^+, \cdot), \text{ and } (2\mathbb{Z}, +).$$

Theorem 2.5.2

Let $(G, *)$ be a group. Then:

1. The identity element of G is unique.
2. The inverse of each element in G is unique.

Proof:

1. Let e_1 and e_2 be two identity elements in G. Then $e_1 * a = a$ for all $a \in G$. In particular, $e_1 * e_2 = e_2$ and $e_1 * e_2 = e_1$. Thus, $e_1 = e_1 * e_2 = e_2$, and hence $e_1 = e_2$.

2. Let a_1 and a_2 be two inverses of $a \in G$. Then,

$$a_1 = a_1 * e = a_1 * (a * a_2) = (a_1 * a) * a_2 = e * a_2 = a_2.$$

Definition 2.5.4

The **order** of a group is the number of elements in G denoted by $|G|$. If G is finite, we write $|G| < \infty$. Otherwise, we say that G is infinite group.

Groups of small order:

⋆ Groups of order 1: $\mathbb{Z}_1 = \{0\}, +$:

If $G = \{e\}$, then G is a group of order 1, with $e^{-1} = e$.

$*$	e
e	e

⋆ Groups of order 2: $\mathbb{Z}_2 = \{0, 1\}, +$:

Let $G = \{e, a\}$. The identity element is e and the inverse of a is a.

$*$	e	a
e	e	a
a	a	e

Remark 2.5.2

Each element needs an inverse in any group. Thus, there must be identity input in each row and column in the Caylay table of the group.

Remark 2.5.3

The equations $a * x = b$ and $y * a = b$ have unique solutions. Therefore, each element appears exactly once in each row and column of the Caylay table of the group.

⋆ Groups of order 3: $\mathbb{Z}_3 = \{0, 1, 2\}, +$:

Table 1.

$*$	e	a	b
e	e	a	b
a	a		
b	b		

Let $G = \{e, a, b\}$. We start with Table 1.
Now if $a * a = e$, then $a * b = b$ since each element appears once in each row and column. But this suggests that $a = e$ which is not the case. Thus, we must have $a * a = b$ and $a * b = e$. Therefore, we get Table 2.

Table 2.

$*$	e	a	b
e	e	a	b
a	a	**b**	**e**
b	b	**e**	**a**

Remark 2.5.4

For any element a in a group G and n is a natural number, we have:

1. $a^n = a * a * \cdots * a$, n-times.
2. $a^{-n} = (a^{-1})^n = (a^n)^{-1} = a^{-1} * a^{-1} * \cdots * a^{-1}$, n-times.
3. $a^0 = e$.

Definition 2.5.5

If two groups G_1 and G_2 have the same structure, one group can be made to look exactly like the other by a renaming of elements. Then they are said to be **isomorphic**, denoted by $G_1 \cong G_2$. In particular, $|\, G_1 \,| = |\, G_2 \,|$.

Example 2.5.5

Consider $\mathbb{Z}_3 = \{0, 1, 2\}$ with "+ modulo 3". Find its order.

Solution:

This is a group of order 3 as above by renaming $e = 0$, $a = 1$, and $b = 2$. Thus, $|\, \mathbb{Z}_3 \,| = 3$.

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\star$ Groups of order 4: $\mathbb{Z}_4$ and $\mathbb{Z}_2^2 = D_2$:

Let $G = \{e, a, b, c\}$. Thus, the Caylay table is

$*$	e	a	b	c
e	e	a	b	c
a	a	?		
b	b			
c	c			

The question mark can NOT be filled with a, but it can be filled either with e or with $\{b \text{ or } c\}$.

Case-1: The ? spot filled with "e": Note that $a * b \neq b$ since $a \neq e$. Thus, we get two possible tables

T_1 and T_2 as follows:

$$T_1(\text{The Klein 4-group}): \begin{array}{c|cccc} * & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & \mathbf{e} & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array} \quad \text{or} \quad T_2: \begin{array}{c|cccc} * & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & \mathbf{e} & c & b \\ b & b & c & a & e \\ c & c & b & e & a \end{array}$$

Case-2: The ? spot filled with "b" without loss of generality, and $a * c \neq c$ since $a \neq e$. We get T_3:

$$T_3: \begin{array}{c|cccc} * & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & \mathbf{b} & c & e \\ b & b & c & e & a \\ c & c & e & a & b \end{array}$$

We end up with three tables T_1, T_2, and T_3. Note that T_2 has the same structure as T_3 when we interchanging letters a and b in table T_2 everywhere and then rewrite the table to get exactly table T_3. Note that T_1 is the smallest example of a non-cyclic group which is called the Klein 4-group.

Example 2.5.6

Consider the group $(\mathbb{Z}_4, +)$. Find its order.

Solution:

This is a group of order 4 and it is isomorphic to the table T_3, namely $(\mathbb{Z}_4, +)$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Exercise 2.5.1

Show that $G = \{2^m 3^n : m, n \in \mathbb{Z}\}$ is a group with respect to multiplication.

Exercise 2.5.2

Let G denote $M(\mathbb{R})$, the set of all mappings on $\mathbb{R}$. For $f, g \in G$ define $f + g$ by $(f + g)(x) = f(x) + g(x)$ for all $x \in \mathbb{R}$. Verify that G with this operation is a group.

Exercise 2.5.3

Let $G = \{A \in M_{2\times 2} : \det A \in \mathbb{Q}^*\}$. Show that $(G, \cdot)$ is a group.

Exercise 2.5.4

Let $G = \{A \in M_{2\times 2} : \det A = 1\}$. Show that $(G, \cdot)$ is a group.

Exercise 2.5.5

Prove that if G is a group, $a \in G$, and $a * b = b$ for some $b \in G$, then a is the identity element of G.

Exercise 2.5.6

Solve the following exercises from the book at pages 33 - 34:

- $5.1 - 5.14$,
- $5.16 - 5.18$,
- 5.22.

Exercise 2.5.7

Consider the group $(U_4, \cdot)$ where $U_4 = \{1, i, -1, -i\}$. Find its order and its isomorphic group.

Section 2.6: Permutations and Symmetric Group

Definition 2.6.1

A permutation of a set A is a mapping $\phi : A \to A$ that is both one-to-one and onto A. That is $\phi : A \xrightarrow[onto]{1-1} A$.

The composition mapping is a binary operation on the collection of all permutations of a set A. We will call this operation **permutation multiplication**.

Theorem 2.6.1

The set of all permutations of a nonempty set A is a group with respect to permutation multiplication. This group is called the symmetric group on A and is denoted by $\mathrm{Sym}(A)$.

If $A = \{1, 2, \cdots, n\}$ is a set, then the group $\mathrm{Sym}(A)$ is commonly denoted by S_n, and is called **the symmetric group on n letters**.

Example 2.6.1

Let $A = \{1, 2, 3\}$. Find the elements of $\mathrm{Sym}(A)$ or simply S_3.

Solution:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Which is (in cycle notation):

$$e,\ (2\ \ 3),\ (1\ \ 2),\ (1\ \ 2\ \ 3),\ (1\ \ 3\ \ 2),\ \text{and}\ (1\ \ 3)$$

Theorem 2.6.2

The order of $S_n = n!$.

Proof:

Counting the number of possibilities of permutations $\begin{pmatrix} 1 & 2 & \cdots & n \\ .. & .. & \cdots & .. \end{pmatrix}$.

Remark 2.6.1

- the identity element in S_n is $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$.
- the inverse element is obtained by reading from bottom to top. That is, for instance,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

  That is $(1\ \ 3\ \ 4\ \ 2)^{-1} = (1\ \ 2\ \ 4\ \ 3)$.

- Compute in S_4:

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

  That is $(1\ \ 2\ \ 4\ \ 3) \circ (1\ \ 3\ \ 2) = (3\ \ 4)$ ”in cycle notation”.

Theorem 2.6.3

S_1 and S_2 are abelian groups. If $n \geq 3$, then S_n is non-abelian group.

Proof:

Let α and β in S_n $(n \geq 3)$ be defined by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 2 & 1 & 4 & \cdots & n \end{pmatrix}.$$

Then,

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 3 & 1 & 4 & \cdots & n \end{pmatrix} \quad \text{and} \quad \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 3 & 1 & 2 & 4 & \cdots & n \end{pmatrix}.$$

That is $\alpha \circ \beta \neq \beta \circ \alpha$, and the group is non-abelian.

Definition 2.6.2

If A is a set and $a_1, a_2, \cdots, a_k \in A$, then $(a_1 \ a_2 \ \cdots \ a_k)$ denotes the permutation of A for which $a_1 \mapsto a_2, a_2 \mapsto a_3, \cdots, a_{k-1} \mapsto a_k, a_k \mapsto a_1$, and $x \mapsto x$ for all other $x \in A$. Such a permutation is called a **cycle** or **k-cycle**.

Example 2.6.2

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

Solution:

We multiply from right to left to get, $(1 \ \ 3 \ \ 2 \ \ 5)(1 \ \ 4 \ \ 3 \ \ 2) = (1 \ \ 4 \ \ 2 \ \ 3 \ \ 5)$.

Example 2.6.3

Compute $(1 \ \ 2 \ \ 3 \ \ 4)^{-1}$ in S_4.

Solution:

$(1 \ \ 2 \ \ 3 \ \ 4)^{-1} = (1 \ \ 4 \ \ 3 \ \ 2)$

Definition 2.6.3

We say that cycles $(a_1 \ \ a_2 \ \ \cdots \ \ a_m)$ and $(b_1 \ \ b_2 \ \ \cdots \ \ b_n)$ are **disjoint cycles** if $a_i \neq b_j$ for all i and j.

Theorem 2.6.4

Disjoint cycles commute; That is if α and β represent disjoint cycles, then $\alpha\beta = \beta\alpha$.

Theorem 2.6.5

Any permutation of a finite set is either a cycle or can be written as a product of pairwise disjoint cycles. The resulting form is called the **cyclic decomposition** of the permutation.

Example 2.6.4

Find the cyclic decomposition of the following permutations: 1. $(1\ \ 3)(2\ \ 5\ \ 4)$, 2. $(1\ \ 4\ \ 5)(2\ \ 3\ \ 5)$, 3. $(1\ \ 2)(1\ \ 3)(4\ \ 5)$, and 4. $(1\ \ 5\ \ 4\ \ 6\ \ 3\ \ 2)(4\ \ 3\ \ 6)(2\ \ 5)$.

Solution:

1. $(1\ \ 3)(2\ \ 5\ \ 4) = (1\ \ 3)(2\ \ 5\ \ 4)$.
2. $(1\ \ 4\ \ 5)(2\ \ 3\ \ 5) = (1\ \ 4\ \ 5\ \ 2\ \ 3)$.
3. $(1\ \ 2)(1\ \ 3)(4\ \ 5) = (1\ \ 3\ \ 2)(4\ \ 5)$.
4. $(1\ \ 5\ \ 4\ \ 6\ \ 3\ \ 2)(4\ \ 3\ \ 6)(2\ \ 5) = (1\ \ 5)(2\ \ 4)$.
5. $(1\ \ 3\ \ 2)(2\ \ 4\ \ 5)(1\ \ 4) = (1\ \ 5)(2\ \ 4\ \ 3)$.

Example 2.6.5

Write down the Caylay table for S_3 defined by ”row $\circ$ column”.

Solution:

$\circ$	e	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$
e	e	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	e	$(1\ 3)$	$(2\ 3)$	$(1\ 2)$
$(1\ 3\ 2)$	$(1\ 3\ 2)$	e	$(1\ 2\ 3)$	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$
$(1\ 2)$	$(1\ 2)$	$(2\ 3)$	$(1\ 3)$	e	$(1\ 3\ 2)$	$(1\ 2\ 3)$
$(1\ 3)$	$(1\ 3)$	$(1\ 2)$	$(2\ 3)$	$(1\ 2\ 3)$	e	$(1\ 3\ 2)$
$(2\ 3)$	$(2\ 3)$	$(1\ 3)$	$(1\ 2)$	$(1\ 3\ 2)$	$(1\ 2\ 3)$	e

Exercise 2.6.1

Solve the following exercises from the book at page 40:

- 6.1 – 6.4.

Exercise 2.6.2

Compute $(1\ \ 4\ \ 6)^{-1}(1\ \ 2\ \ 4\ \ 3\ \ 5)$ in S_6.

Section 2.7: Subgroups

Definition 2.7.1

A subset H of a group G is a **subgroup** of G if H is itself a group under the binary operation of G. In that case, we write $H \leq G$. In addition, if $H \neq G$, we simply write $H < G$.

Example 2.7.1

The following are some examples of subgroups:

- $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$,
- $(\{1, -1\}, \cdot) \leq (\mathbb{R}^*, \cdot)$,
- (improper subgroup) $(G, *) \leq (G, *)$ for any group G with operation $*$, and
- (improper subgroup) $(\{e\}, *) \leq (G, *)$ for any group G with operation $*$.

Remark 2.7.1

Let H be a subgroup of a group $(G, *)$, i.e. $H \leq G$. Then:

- $a * b \in H$ for all $a, b \in H$. In particular, H must be closed under the operation $*$.
- $e_H = e_G$ and for $a \in H$, a^{-1} in H is the same as a^{-1} in G.

Theorem 2.7.1

A subset H is a subgroup of a group G if and only if the following properties hold:

$\mathcal{S}_1$: H is not empty.

$\mathcal{S}_2$: If $a, b \in H$, then $a * b \in H$, and

$\mathcal{S}_3$: If $a \in H$, then $a^{-1} \in H$.

Proof:

„ $\Rightarrow$" Assume that H is a subgroup of G. Then H is a group itself and the properties 1, 2, and 3 hold.

„ $\Leftarrow$" Assume now that properties 1, 2, and 3 hold. Then we show that H is a group contained in G:

$\mathcal{G}_1$: Clearly $*$ is associative on G and hence it is associative on its subset H.

$\mathcal{G}_2$: H is not empty by Property 1, and hence there is $a \in H$ and thus $a^{-1} \in H$ (by Property 3). Therefore, $a * a^{-1} = e \in H$ (by Property 2).

$\mathcal{G}_3$: For any $a \in H$, there is an inverse of a in H by Property 3.

Therefor H is a subgroup of G.

Definition 2.7.2

A subgroup H of a group G is called a **proper subgroup** if $H \neq \{e\}$ "the trivial subgroup of G", and $H \neq G$ "the improper subgroup of G".

Example 2.7.2: Exercise 7.22 at page 46

Prove that if G is a group with operation $*$, and H is a subset of G, then H is a subgroup of G if and only if:

1. H is not empty.
2. If $a, b \in H$, then $a * b^{-1} \in H$, and

Solution:

„ $\Rightarrow$" Assume that $H \leq G$. Then H is a group and the properties 1, and 2 hold.

„ $\Leftarrow$" Assume now that properties 1, and 2 hold. Then we show that H is a group in G:

$\mathcal{G}_1$: Clearly $*$ is associative on G and hence it is associative on its subset H.

$\mathcal{G}_2$: Let $a \in H$, then $e = a * a^{-1} \in H$ (by Property 2).

$\mathcal{G}_3$: For any $a \in H$, we have $e * a^{-1} \in H$ (by Property 2) and hence there is an inverse of a in H.

Therefor H is a subgroup of G.

Remark 2.7.2

1. $(\mathbb{R},+) \geq (\mathbb{Q},+) \geq (\mathbb{Z},+) \geq (n\mathbb{Z},+), n \in \mathbb{Z}, \geq \{0\}$.
2. $(\mathbb{R}^*,\cdot) \geq (\mathbb{Q}^*,\cdot) \geq (\mathbb{Q}^+,\cdot) \geq \{1\}$.
3. Note that $(3\mathbb{Z},+) \not\leq (2\mathbb{Z},+)$ since $3\mathbb{Z} \not\subseteq 2\mathbb{Z}$.

Example 2.7.3

Show that $H = \{0, 2\}$ is a subgroup of $\mathbb{Z}_4$ under the addition modular 4.

Solution:

$+$	0	2
0	0	2
2	2	$4 \equiv_4 0$

Clearly, H is not empty and the identity element is 0 and the inverse of each element in H is itself. Thus $H \leq \mathbb{Z}_4$.

Example 2.7.4

Show that $H = \{e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$ is a subgroup of S_3 under the permutation multiplication.

Solution:

We show that by proving that H satisfying the three properties of Theorem 2.7.1. We first start with the following table:

$\circ$	e	$(1\ \ 2\ \ 3)$	$(1\ \ 3\ \ 2)$
e	e	$(1\ \ 2\ \ 3)$	$(1\ \ 3\ \ 2)$
$(1\ \ 2\ \ 3)$	$(1\ \ 2\ \ 3)$	$(1\ \ 3\ \ 2)$	e
$(1\ \ 3\ \ 2)$	$(1\ \ 3\ \ 2)$	e	$(1\ \ 2\ \ 3)$

$\mathcal{S}_1$: Clearly H is not empty.

$\mathcal{S}_2$: The previous table shows that H is closed under the operation $\circ$.

$\mathcal{S}_3$: Finally, $e^{-1} = e \in H$, $(1\ \ 2\ \ 3)^{-1} = (1\ \ 3\ \ 2) \in H$, and $(1\ \ 3\ \ 2)^{-1} = (1\ \ 2\ \ 3) \in H$.

Therefore, H is a subgroup of S_3.

Remark 2.7.3

Subgroups of S_3 are:

1. S_3.
2. $\{e\}$.
3. $\{e, (1\ \ 2)\}$.
4. $\{e, (1\ \ 3)\}$.
5. $\{e, (2\ \ 3)\}$.
6. $\{e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$.

Remark 2.7.4

A **transposition** is a 2-cycle element in S_n.

- Every element in S_n is a transposition or a product of transpositions (not in a unique way). For instance in S_3, $(1\ \ 2\ \ 3) = (1\ 3)(1\ 2) = (2\ 3)(1\ 2)(1\ 3)(2\ 3)$ and in general in S_n we have
$$(a_1\ a_2\ \ \cdots\ \ a_k) = (a_1\ a_k)(a_1\ a_{k-1})\cdots(a_1\ a_2).$$
- A permutation is even (or odd) if it can be written as a product of an even (or an odd, respectively) number of transpositions.

Example 2.7.5

Decide whether $\alpha = (1\ \ 2\ \ 3\ \ 4\ \ 5)$ and $\beta = (1\ \ 2\ \ 5)(3\ \ 4)$ are even or odd permutations in S_5.

Solution:

- α is even (4 transpositions): $\alpha = (1\ \ 2\ \ 3\ \ 4\ \ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$, and
- β is odd (3 transpositions): $\beta = (1\ \ 2\ \ 5)(3\ \ 4) = (1\ 5)(1\ 2)(3\ 4)$.

Definition 2.7.3

The set of all even permutations in S_n is called the alternating group and is denoted by A_n. Moreover, it is of order $\frac{1}{2}\,n!$.

Theorem 2.7.2

For each $n \geq 2$, A_n is a subgroup of S_n.

Proof:

Let $n \geq 2$, then

$\mathcal{S}_1$: The identity permutation $e = (1\ \ 2)(1\ \ 2) \in A_n$ and hence $A_n \neq \phi$.

$\mathcal{S}_2$: If $a, b \in A_n$, then both are even permutations and the product of two even number of transpositions is an even number. Thus $ab \in A_n$.

$\mathcal{S}_3$: If $a = (a_1\ a_2)(a_3\ a_4)\cdots(a_{k-1}\ a_k) \in A_n$, then $a^{-1} = (a_{k-1}\ a_k)\cdots(a_3\ a_4)(a_1\ a_2) \in A_n$

Therefore, $A_n \leq S_n$.

Remark 2.7.5

Note that the subgroup H of Example 2.7.4 is in fact A_3 which is a subgroup of S_3 and its order is $3 = \frac{1}{2}\,3!$.

Definition 2.7.4

Let G be a permutation group on a set S, and let $T \subseteq S$. We define:

- $G_T = \{\alpha \in G : \alpha(t) = t \text{ for all } t \in T\}$, which leaves T elementwise invariant.
- $G_{(T)} = \{\alpha \in G : \alpha(T) = T\}$, which leaves T setwise invariant.

Example 2.7.6

Let $S = \{1, 2, 3, 4\}$, $G = sym(S) = S_4$, and $T = \{1, 2\}$. Find G_T and $G_{(T)}$.

Solution:

$$G_T = \{(1)(2)(3)(4), (1)(2)(3\ \ 4)\} = \{e, (3\ \ 4)\}.$$

$$G_{(T)} = \{(1)(2)(3)(4), (1\ \ 2)(3)(4), (1)(2)(3\ \ 4), (1\ \ 2)(3\ \ 4)\} = \{e, (1\ \ 2), (3\ \ 4), (1\ \ 2)(3\ \ 4)\}.$$

Theorem 2.7.3

If G is a permutation group on S, and $T \subseteq S$, then G_T and $G_{(T)}$ are subgroups of G. Moreover, G_T is a subgroup of $G_{(T)}$.

Proof:

We first show that $G_T \leq G$.

$\mathcal{S}_1$: Clearly, the identity mapping I of G is in G_T, and hence $G_T \neq \phi$.

$\mathcal{S}_2$: Let $\alpha, \beta \in G_T$, then for each $t \in T$, we have

$$(\alpha \circ \beta)(t) = \alpha(\beta(t)) = \alpha(t) = t.$$

So, $\alpha \circ \beta \in G_T$.

$\mathcal{S}_3$: If $\alpha \in G_T$, and $t \in T$, then $\alpha^{-1} \in G_T$ because

$$\begin{aligned} \alpha(t) &= t \\ \alpha^{-1}(\alpha(t)) &= \alpha^{-1}(t) \\ (\alpha^{-1} \circ \alpha)(t) &= \alpha^{-1}(t) \\ t &= \alpha^{-1}(t). \end{aligned}$$

Therefore G_T is a subgroup of G. Next we show that $G_{(T)} \leq G$.

$\mathcal{S}_1$: Clearly $I(T) = T$ and hence $G_{(T)} \neq \phi$.

$\mathcal{S}_2$: If $\alpha, \beta \in G_{(T)}$, then $(\alpha \circ \beta)(T) = \alpha(\beta(T)) = \alpha(T) = T$ and hence $\alpha \circ \beta \in G_{(T)}$.

$\mathcal{S}_3$: If $\alpha \in G_{(T)}$, then $\alpha(T) = T \;\Rightarrow\; \alpha^{-1}(\alpha(T)) = \alpha^{-1}(T) \;\Rightarrow\; T = \alpha^{-1}(T)$ and hence $\alpha^{-1} \in G_{(T)}$.

Therefore, $G_{(T)} \leq G$.

To show that $G_T \leq G_{(T)}$, we only show that $G_T \subseteq G_{(T)}$ as follows: If $\alpha \in G_T$, then $\alpha(t) = t$ for each $t \in T$ and hence $\alpha(T) = T$. That is $\alpha \in G_{(T)}$. Therefore, $G_T \subseteq G_{(T)}$ and hence $G_T \leq G_{(T)}$.

Example 2.7.7: Exercise 7.13 at page 46

Let H and K be two subgroups of $(G, *)$. Show that $H \cap K$ is also a subgroup of $(G, *)$.

Solution:

We show that $H \cap K$ is a subgroup of G as follows:

$\mathcal{S}_1$**: $H \cap K \neq \phi$:** Since H and K are both subgroups of G, then $e \in H$ and $e \in K$, and hence $e \in H \cap K$.

$\mathcal{S}_2$**: $H \cap K$ is closed under $*$:** Let $a, b \in H \cap K$. Then

1. $a, b \in H$, and since H is a subgroup of G, $a * b \in H$, and
2. $a, b \in K$, and since K is a subgroup of G, $a * b \in K$.

Thus, $a * b \in H \cap K$.

$\mathcal{S}_3$**: For each $a \in H \cap K$, there exists $a^{-1} \in H \cap K$:** Let $a \in H \cap K$. Thus, $a \in H$ and hence $a^{-1} \in H$. Also, $a \in K$ and hence $a^{-1} \in K$. Therefore, $a^{-1} \in H \cap K$.

Therefore, $H \cap K$ is a subgroup of G.

Definition 2.7.5

Let G be a group with operation $*$ and that $a \in G$. The **centralizer of a in G** is defined by

$$C(a) = \{g \in G : a * g = g * a\}.$$

Definition 2.7.6

Let G be a group with operation $*$. The **center of G** is defined by

$$Z(G) = \{g \in G : g * a = a * g \text{ for all } a \in G\}.$$

Remark 2.7.6

For the sake of simplicity, we write ab instead of $a * b$ for any elements a and b in $(G, *)$.

Example 2.7.8: Exercises 7.23 & 7.24 at page 46

Let G be a group with operation $*$. Then,

(a) Show that $C(a)$ is a subgroup of G for $a \in G$.

(b) Show that $Z(G)$ is a subgroup of G.

Solution:

We first show that $C(a) \leq G$ for $a \in G$ as follows:

$\mathcal{S}_1$: Clearly, $ae = a = ea$. Hence, $e \in C(a) \neq \phi$.

$\mathcal{S}_2$: Let $g, h \in C(a)$. Then, $ag = ga$ and $ah = ha$. Thus,

$$a(gh) = (ag)h = (ga)h = g(ah) = g(ha) = (gh)a.$$

Since $a(gh) = (gh)a$, $(gh) \in C(a)$, and $C(a)$ is closed.

$\mathcal{S}_3$: Let $g \in C(a)$. Then,

$$ag = ga \;\Leftrightarrow\; g^{-1}(ag) = a \;\Leftrightarrow\; g^{-1}a = ag^{-1}.$$

Hence, $g^{-1} \in C(a)$.

Therefore, $C(a) \leq G$. Next we show that $Z(G) \leq G$ as follows:

$\mathcal{S}_1$: For all $a \in G$, $ae = a = ea$. Hence, $e \in Z(G) \neq \phi$.

$\mathcal{S}_2$: Let $g, h \in Z(G)$, then $ga = ag$ and $ha = ah$ for all $a \in G$. Thus, for all $a \in G$, we have

$$a(gh) = (ag)h = (ga)h = g(ah) = g(ha) = (gh)a.$$

Therefore, $gh \in Z(G)$.

$\mathcal{S}_3$: Let $g \in C(a)$. Then, $ag = ga$ for all $a \in G$. Then

$$g^{-1}ag = a \;\Leftrightarrow\; g^{-1}a = ag^{-1}.$$

Therefore, $Z(G) \leq G$.

Example 2.7.9

Suppose that G is an abelian group with operation $*$. Let H and K be two subgroups of G. Show that $HK = \{hk : h \in H \text{ and } k \in K\}$ is also a subgroup of G.

Solution:

$\mathcal{S}_1$: Clearly, $e \in H$ and $e \in K$. Thus, $e = ee \in HK \neq \phi$.

$\mathcal{S}_2$: Let $a = h_1k_1, b = h_2k_2 \in HK$ so that $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then, $h_1h_2 \in H$ and $k_1k_2 \in K$ since both H and K are subgroups of G. Since G is abelian, we have

$$ab = (h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2) = hk \in HK,$$

where $h = h_1h_2 \in H$ and $k = k_1k_2 \in K$. Thus HK is closed.

$\mathcal{S}_3$: Let $a = hk \in HK$ where $h \in H$ and $k \in K$. Then, $h^{-1} \in H$ and $k^{-1} \in K$. Thus,

$$a^{-1} = (hk)^{-1} = k^{-1}h^{-1},$$

and since G is abelian, we have

$$a^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$$

Therefore, HK is a subgroup of G.

Remark 2.7.7

Note that if G is a group (not abelian), then HK is not necessary a subgroup of G for any subgroups H and K. For instance consider $G = S_3$ and $H = \{e, (1\ \ 2)\}$ and $K = \{e, (2\ \ 3)\}$.

Example 2.7.10

Let G be a group. If $a, b \in G$ with $ab \in Z(G)$, then $ab = ba$.

Solution:

We show that $aba^{-1}b^{-1} = e$ which is equivalent to showing that $ab = ba$. Note that $(ab)g = g(ab)$ for all $g \in G$. Then

$$(ab)a^{-1}b^{-1} = a^{-1}(ab)b^{-1} = e.$$

Exercise 2.7.1

Solve the following exercises from the book at pages 45 - 46:

- 7.1 – 7.4,
- 7.8, 7.10, 7.13, 7.15,
- 7.22 – 7.24.

Exercise 2.7.2

Prove or disprove: For any given group G,

$$Z(G) = \bigcap_{a \in G} C(a).$$

Exercise 2.7.3

For any given group G, Compute $C(e)$.

Exercise 2.7.4

Let $GL_n(\mathbb{R}) = \{\text{all } n \times n \text{ nonsingular matrices with real entries}\}$ be a group with the operation of matrix multiplication and let $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \;:\; \det(A) = 1\}$. Show that $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

Exercise 2.7.5

Let $GL_2(\mathbb{R}) = \{\text{all } 2 \times 2 \text{ nonsingular matrices with real entries}\}$ be a group with the operation of matrix multiplication. Find $C\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}\right)$.

Chapter

3 Equivalence. Congruence. Divisiblity

Section 3.9: Equivalence Relations

Definition 3.9.1

Let A and B be sets. A **relation** $\sim$ from A to B is a subset of $A \times B$. If $a \in A$ is related to $b \in B$, then we write $a \sim b$. Otherwise, $a \not\sim b$. Moreover, if $A = B$, we simply say that $\sim$ is a relation on A.

Definition 3.9.2

Let $\sim$ be a relation on a set A. Then $\sim$ is called an **equivalence relation** if and only if:

1. $\sim$ is **reflexive** on A: $(\forall x \in A)\ x \sim x$.
2. $\sim$ is **symmetric** on A: $(\forall x, y \in A)$ if $x \sim y$, then $y \sim x$.
3. $\sim$ is **transitive** on A: $(\forall x, y, z \in A)$ if $x \sim y$ and $y \sim z$, then $x \sim z$.

Example 3.9.1

Let $\sim$ be the relation on $\mathbb{Z}$ given by $x \sim y$ iff $x - y$ is even. Show that $\sim$ is an equivalence relation on $\mathbb{Z}$.

Solution:

- for all $x \in \mathbb{Z}$, $x - x = 0$ which is even, hence $x \sim x$ and $\sim$ is reflexive.
- for any $x, y \in \mathbb{Z}$, let $x \sim y$. Then $x - y$ is even. That is $x - y = 2k$ for some $k \in \mathbb{Z}$. Hence $y - x = 2(-k)$ which is even as well. Thus, $y \sim x$ and $\sim$ is symmetric.
- for any $x, y, z \in \mathbb{Z}$, let $x \sim y$ and $y \sim z$. Then, $x-y$ and $y-z$ is even. So, $(x-y)+(y-z) = x - z$ is also even. Thus, $x \sim z$ and $\sim$ is transitive.

Therefore, $\sim$ is an equivalence relation on $\mathbb{Z}$.

Example 3.9.2

Let $\alpha : A \to B$ be a mapping and define a relation $\sim$ on A so that for any $x, y \in A$, $x \sim y$ iff $\alpha(x) = \alpha(y)$. Clearly, $\sim$ is an equivalence relation. (Can you show it!?).

Definition 3.9.3

Let A be a non-empty set. A **partition** of the set A is a family of nonempty subsets $A_1, A_2, \cdots, A_n$ such that:

1. $\bigcup_{i=1}^{n} A_i = A$, and
2. $A_i \cap A_j = \phi$ if $i \neq j$.

Example 3.9.3

Let E denote the set of even integers and O the set of odd integers. Then, $\{E, O\}$ forms a partition of the set of all integers. Note that $\{0, 1\}$ is a complete set of equivalence class representatives.

Definition 3.9.4

Let $\sim$ be an equivalence relation on a set A. For $x \in A$, define the **equivalence class** of x determined by $\sim$ as

$$[x] = \{y \in A : x \sim y\}.$$

Remark 3.9.1

It is always true that $x \in [x]$ because $\sim$ is reflexive. And if $y \in [x]$, then $x \in [y]$ because $\sim$ is symmetric.

Theorem 3.9.1

If $\sim$ is an equivalence relation on a nonempty set A, then the set of equivalence classes of $\sim$ forms a partition of A.

Theorem 3.9.2

Let G be a permutation group on nonepmty set S and define a relation $\sim$ on S by $a \sim b$ iff $\alpha(a) = b$ for some $\alpha \in G$. Then $\sim$ is an equivalence relation on S.

Proof:

We show that $\sim$ is reflexive, symmetric, and transitive relations as follows:

Ref.: If $a \in S$, then $I(a) = a$ and hence $a \sim a$.

Symm.: If $a, b \in S$ and $a \sim b$, then $\alpha(a) = b$ for some $\alpha \in G$ and hence $\alpha^{-1}(b) = a$ with $\alpha^{-1} \in G$. Thus $b \sim a$.

Trans.: If $a, b, c \in S$ with $a \sim b$ and $b \sim c$, then there are $\alpha, \beta \in G$ such that $\alpha(a) = b$ and $\beta(b) = c$. Thus $\beta \circ \alpha \in G$ with

$$(\beta \circ \alpha)(a) = \beta(\alpha(a)) = \beta(b) = c.$$

That is $a \sim c$.

Example 3.9.4

Let $G = \{e, (1 \;\; 2 \;\; 5), (1 \;\; 5 \;\; 2)\}$ and $S = \{1, 2, 3, 4, 5\}$ and define a relation $\sim$ on S by $a \sim b$ iff $\alpha(a) = b$ for some $\alpha \in G$. Find all the equivalence classes of $\sim$ on S.

Solution:

Clearly, $\{1, 2, 5\}, \{3\}, \{4\}$ are the equivalence classes of $\sim$ on S. Moreover, $\{1, 3, 4\}$ are called equivalence classes representatives.

Exercise 3.9.1

Solve the following exercises from the book at pages 55 - 56:

- 9.1 – 9.4,
- 9.8, 9.9, 9.13
- 9.19.

Exercise 3.9.2

Let $\sim$ be a relation on $\mathbb{N}$ so that $x \sim y$ iff $3 \big| x + y$. Is $\sim$ an equivalence relation on $\mathbb{N}$? Explain your answer.

Exercise 3.9.3

Let $\sim$ be a relation on $\mathbb{N}$ so that $x \sim y$ iff $3 \big| x + 2y$. Show that $\sim$ is an equivalence relation on $\mathbb{N}$.

Section 3.10: Congruence. The Division Algorithm

Definition 3.10.1

Let $a, b \in \mathbb{Z}$. Then b is divisible by a if there is $k \in \mathbb{Z}$ such that $b = ak$. In that case we say:

- a divides b, written as $a \mid b$,
- b is a multiple of a, and
- a is a factor of b.

Theorem 3.10.1

If $a, b \in \mathbb{Z}$, not both zero, then there is a unique positive integer d such that

1. $d \mid a$ and $d \mid b$, and
2. if $c \in \mathbb{Z}$ with $c \mid a$ and $c \mid b$, then $c \mid d$.

In that case, d is called the greatest common divisor and it is denoted by $d = \text{GCD}(a, b)$.

Remark 3.10.1

The following are some general facts about integer numbers:

1. An integer p is a prime if $p > 1$ and has no positive factors other than 1 and p,
2. If $a \mid b$, then $a \mid -b$, and
3. If $a \mid b$ and $a \mid c$, then $a \mid (b \pm c)$.
4. If $a, b \in \mathbb{Z}$ (not both zeros), then $\text{GCD}(a, b) = 1$ if and only if there are integers m and n such that $am + bn = 1$.

Definition 3.10.2

Let n be a positive integer. Integers a and b are said to be **congruent modulo** n if $a - b$ is divisible by n. This is written as $a \equiv b \pmod{n}$ or $a \equiv_n b$. That is

$$a \equiv_n b \iff n \mid a - b \iff a = kn + b \text{ or } a - b = kn \text{ for some } k \in \mathbb{Z}.$$

Example 3.10.1

Here is some examples of some integers modulo n for some positive integer n:

- $17 \equiv 3 \pmod 7$ since $7 \mid (17-3) = 14$,
- $4 \equiv 22 \pmod 9$ since $9 \mid (4-22) = -18$,
- $19 \equiv 19 \pmod{11}$ since $11 \mid (19-19) = 0$,
- but $17 \not\equiv 3 \pmod 8$ since $8 \nmid (17-3) = 14$.

Theorem 3.10.2

Congruence modulo n is an equivalence relation on $\mathbb{Z}$, for each $n \in \mathbb{Z}^+$.

Proof:

We show that "$\equiv_n$" is reflexive, symmetric, and transitive:

Ref.: for all $a \in \mathbb{Z}$, $a \equiv_n a$ since $n \mid (a-a) = 0$.

Symm.: for all $a, b \in \mathbb{Z}$, if $a \equiv_n b$, then $n \mid a-b$ and so $n \mid b-a$. That is $b \equiv_n a$.

Trans.: for all $a, b, c \in \mathbb{Z}$, if $a \equiv_n b$ and $b \equiv_n c$, then $n \mid a-b$ and $n \mid b-c$. Thus, $n \mid [(a-b)+(b-c)]$ which implies $n \mid a-c$. Hence, $a \equiv_n c$.

Remark 3.10.2

The equivalence classes for the equivalence relation "$\equiv_n$" are called congruence classes modulo n.

Theorem 3.10.3

Let n be a positive integer and $x, y \in \mathbb{Z}$. Then, $x \equiv_n y$ if and only if $[x] = [y]$.

Proof:

„ $\Rightarrow$ ": Assume that $x \equiv_n y$. Then, $n \mid x-y$.

$$z \in [x] \Longleftrightarrow z \equiv_n x \Longleftrightarrow z \equiv_n y \Longleftrightarrow z \in [y].$$

„ $\Leftarrow$ ": Assume that $[x] = [y]$. Then $x \in [x] = [y]$ implies that $x \equiv_n y$.

Example 3.10.2

Find a complete set of equivalence class representatives of $\equiv_4$ on $\mathbb{Z}$.

Solution:

There are four congruence classes modulo 4:

$$\begin{aligned}
[0] &= \{\cdots, -8, -4, 0, 4, 8, \cdots\} && : 4 \mid 0 - a \text{ where } a \in \mathbb{Z}, \\
[1] &= \{\cdots, -7, -3, 1, 5, 9, \cdots\} && : 4 \mid 1 - a \text{ where } a \in \mathbb{Z}, \\
[2] &= \{\cdots, -6, -2, 2, 6, 10, \cdots\} && : 4 \mid 2 - a \text{ where } a \in \mathbb{Z}, \\
[3] &= \{\cdots, -5, -1, 3, 7, 11, \cdots\} && : 4 \mid 3 - a \text{ where } a \in \mathbb{Z}.
\end{aligned}$$

Thus $\{0, 1, 2, 3\}$ is a complete set of congruence class representatives.

Theorem 3.10.4

Let n be a positive integer. Then each integer is congruent modulo n to exactly one of the integers $0, 1, 2, \cdots, n-1$.

Definition 3.10.3

Let n be a positive integer. Then $\mathbb{Z}_n$ denotes a complete set of congruence classes modulo n. That is $\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$.

Least Integer Principle

Every nonempty set of positive integers contains a least element.

Example 3.10.3

Note that

$$\frac{11}{4} = 2 + \frac{3}{4} \text{ is the same as } 11 = 4 \cdot 2 + 3.$$

Theorem 3.10.5: The Division Algorithm

If $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique integers q and r such that

$$a = bq + r; \quad 0 \le r < b. \quad \text{That is, } a \equiv r \pmod{b}.$$

Example 3.10.4

Note that (1) $11 = 4 \cdot 2 + 3$ and (2) $-6 = 4 \cdot (-2) + 2$ as in $a = b \cdot q + r$. That is

1. $r = 3$ is the smallest positive integer in the congruence class mod 4 containing $a = 11$, and $q = 2$ is the number of positions (right) that moves us from $r = 3$ to $a = 11$.
2. $r = 2$ is the smallest positive integer in the congruence class mod 4 containing $a = -6$, and $q = -2$ is the number of positions (left) that moves us from $r = 2$ to $a = -6$.

Example 3.10.5: Exercise 10.3 at page 60

Find the smallest nonnegative integer congruent modulo 7 for

$$a.\ 12 \qquad\qquad b.\ 100 \qquad\qquad c.\ -25$$

Solution:

a $\frac{12}{7} = 1 + \frac{5}{7} \;\Rightarrow\; 12 = 1 \cdot 7 + 5 \;\Rightarrow\; 12 \equiv 5 \pmod{7}$,

b $\frac{100}{7} = 14 + \frac{2}{7} \;\Rightarrow\; 100 = 14 \cdot 7 + 2 \;\Rightarrow\; 100 \equiv 2 \pmod{7}$,

c $\frac{-25}{7} = -3 - \frac{4}{7} + (1 - 1) = -4 + \frac{3}{7} \;\Rightarrow\; -25 = -4 \cdot 7 + 3 \;\Rightarrow\; -25 \equiv 3 \pmod{7}$.

Example 3.10.6: Exercise 10.5 at page 60

Find all x such that $2x \equiv x \pmod{5}$.

Solution:

Clearly, $2x \equiv x \pmod{5} \quad \Leftrightarrow \quad 5 \mid (2x - x) \quad \Leftrightarrow \quad 5 \mid x \quad \Leftrightarrow \quad x = \{5k : k \in \mathbb{Z}\}$.

Example 3.10.7: Exercise 10.11 at page 60

For each pair a and b, find the unique integers q and r such that $a = bq + r$ with $0 \le r < b$.

(a) $a = 19, b = 5$, (b) $a = -7, b = 5$, (c) $a = 11, b = 17$,

(d) $a = 50, b = 6$, (e) $a = 13, b = 20$, (f) $a = 30, b = 1$.

Solution:

Recall that $a = q \cdot b + \boxed{r} \quad \Leftrightarrow \quad \frac{a}{b} = q + \frac{r}{b} \quad \Leftrightarrow a - r = br \quad \Leftrightarrow \quad a \equiv r \pmod{b}$. Then,

(a) $\frac{19}{5} = 3 + \frac{4}{5} \quad \Rightarrow \quad 19 = 3 \cdot 5 + \boxed{4}$.

(b) $\frac{-7}{5} = -2 + \frac{3}{5} \quad \Rightarrow \quad -7 = -2 \cdot 5 + \boxed{3}$.

(c) $\frac{11}{17} = 0 + \frac{11}{17} \quad \Rightarrow \quad 11 = 0 \cdot 17 + \boxed{11}$.

(d) $\frac{50}{6} = 8 + \frac{2}{6} \quad \Rightarrow \quad 50 = 8 \cdot 6 + \boxed{2}$.

(e) $\frac{13}{20} = 0 + \frac{13}{20} \quad \Rightarrow \quad 13 = 0 \cdot 20 + \boxed{13}$.

(f) $\frac{30}{1} = 30 + \frac{0}{1} \quad \Rightarrow \quad 30 = 30 \cdot 1 + \boxed{0}$.

Exercise 3.10.1

Solve the following exercises from the book at pages 60 - 61:

- 10.1,
- $10.3 - 10.8$,
- $10.11 - 10.18$,
- 10.24.

Section 3.11: Integers Modulo n

Remark 3.11.1

With n is a fixed positive integer and k is any integer, let $[k]$ denote the congruence class to which k belongs (mod n). That is

$$[k] = \{h \in \mathbb{Z} : h \equiv k \pmod{n}\}.$$

Definition 3.11.1

Let $[a], [b] \in \mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$, define $[a] \oplus [b]$ by

$$[a] \oplus [b] = [a+b].$$

Example 3.11.1

For $n = 5$, compute $[3] \oplus [4]$ and $[18] \oplus [-1]$.

Solution:

1. $[3] \oplus [4] = [3+4] = [7] = [2] \in \mathbb{Z}_5$, and
2. $[18] \oplus [-1] = [18 + (-1)] = [17] = [2] \in \mathbb{Z}_5$.

Theorem 3.11.1

$\mathbb{Z}_n$, the group of integers modulo n, is an abelian group with respect to the operation $\oplus$.

Proof:

Clearly, $\mathbb{Z}_n$ is abelian since $[a] \oplus [b] = [a+b] = [b+a] = [b] \oplus [a]$. To show that $\mathbb{Z}_n$ is a group:

$\mathcal{G}_1$: $\oplus$ is associative:

$$\begin{aligned} [a] \oplus ([b] \oplus [c]) &= [a] \oplus [b+c] = [a + (b+c)] \\ &= [(a+b)+c] = [a+b] \oplus [c] = ([a] \oplus [b]) \oplus [c]. \end{aligned}$$

$\mathcal{G}_2$: The identity is $[0]$ since $[a] \oplus [0] = [a] = [0] \oplus [a]$.

$\mathcal{G}_3$: For $[a] \in \mathbb{Z}_n$, the inverse is $[-a] \in \mathbb{Z}_n$ with $[a] \oplus [-a] = [a + (-a)] = [0]$.

Theorem 3.11.2

There is a group of order n for each positive integer n.

Proof:

$(\mathbb{Z}_n, \oplus)$ has n elements $\{[0], [1], \cdots, [n-1]\}$.

Definition 3.11.2

For $[a], [b] \in \mathbb{Z}_n$, define $[a] \odot [b] = [ab]$.

Remark 3.11.2

$(\mathbb{Z}_n, \odot)$ is not a group in general, but $\odot$ is associative and commutative on $\mathbb{Z}_n$ and $\mathbb{Z}_n$ has $[1]$ as an identity element. Note that $[0]$ has no inverse in $\mathbb{Z}_n$.

Theorem 3.11.3

$(\mathbb{Z}_n^*, \odot)$ is a group if and only if n is a prime number.

Proof:

„ $\Rightarrow$" By contradiction assume that n is not prime. Then $n = ab$ for some $1 < a, b < n$. Considering the equivalence classes, we have $[a], [b] \in \mathbb{Z}_n^*$. Then

$$[a][b] = [ab] = [n] = [0] \notin \mathbb{Z}_n^*.$$

Then, Z_n^* is not a group, which is contradiction.

„ $\Leftarrow$" Assume that n is a prime. Then,

1. Let $a, b \in \mathbb{Z}_n^*$, then $ab \in \mathbb{Z}_n^*$ since $ab \neq n$.
2. Clearly, $1 \in \mathbb{Z}_n^*$ (the identity is in $\mathbb{Z}_n^*$).
3. Let $a \in \mathbb{Z}_n^*$, then (the greatest common divisor of a and n) $GCD(a, n) = 1$ which implies

$$\exists\, b, c \in \mathbb{Z} \text{ such that } ab + nc = 1 \Rightarrow ab = 1 - nc \Rightarrow ab = 1 \pmod{n} \Rightarrow b = a^{-1} \in \mathbb{Z}_n^*.$$

Exercise 3.11.1

Solve the following exercises from the book at pages 64 - 65:

- 11.1 – 11.8.

Exercise 3.11.2

Prove or disprove the following statements:

- $(\mathbb{Z}_4^*, \odot)$ is a group.
- $(\mathbb{Z}_5^*, \odot)$ is a group.

Section 3.12: Greatest Common Divisor. The Euclidean Algorithm

The Euclidean Algorithm

Let $a, b \in \mathbb{Z}$ with $a > b > 0$. Then to find the GCD(a, b), we do:

$$a = b\, q_1 + r_1, \qquad 0 \le r_1 < b.$$

If $r_1 = 0$, then GCD$(a, b) = b$. Otherwise,

$$b = r_1\, q_2 + r_2, \qquad 0 \le r_2 < r_1.$$

If $r_2 = 0$, then GCD$(a, b) = r_1$. Otherwise, we go on as follows

$$\begin{aligned} a &= b\, q_1 + r_1, & 0 &\le r_1 < b \\ b &= r_1\, q_2 + r_2, & 0 &\le r_2 < r_1 \\ r_1 &= r_2\, q_3 + r_3, & 0 &\le r_3 < r_2 \\ r_2 &= r_3\, q_4 + r_4, & 0 &\le r_4 < r_3 \end{aligned}$$

and so on. At some point for some k, $r_{k+1} = 0$ so that

$$\begin{aligned} r_{k-2} &= r_{k-1}\, q_k + r_k, & 0 &\le r_k < r_{k-1} \\ r_{k-1} &= r_k\, q_{k+1}. \end{aligned}$$

Therefore, GCD$(a, b) = r_k$.

Example 3.12.1

Compute the GCD$(12, 5)$ by The Euclidean Algorithm, and write it as a linear combination of 12 and 5.

Solution:

Following the Euclidean Algorithm, we get:

$$\begin{aligned} 12 &= 5 \cdot 2 + 2, \\ 5 &= 2 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 \end{aligned}$$

Therefore, $\text{GCD}(12, 5) = 1$. To write 1 as a linear combination of 12 and 5, we go back as follows:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (12 - 5 \cdot 2) \\ &= 5 \cdot 5 - 12 \cdot 2. \end{aligned}$$

Thus, $1 = 5 \cdot 5 - 12 \cdot 2$.

Example 3.12.2

Compute the $\text{GCD}(1001, 357)$ by The Euclidean Algorithm, and write it as a linear combination of 1001 and 357. Do the same thing for $\text{GCD}(252, 105)$? =?21.

Solution:

Following the Euclidean Algorithm, we get:

$$\begin{aligned} 1001 &= 357 \cdot 2 + 287, \\ 357 &= 287 \cdot 1 + 70, \\ 287 &= 70 \cdot 4 + 7, \\ 70 &= 7 \cdot 10. \end{aligned}$$

Therefore, $\text{GCD}(1001, 357) = 7$. To write 7 as a linear combination of 1001 and 357, we go back as follows:

$$\begin{aligned} 7 &= 287 - 70 \cdot 4 \\ &= (1001 - 357 \cdot 2) - (357 - 287 \cdot 1) \cdot 4 \\ &= (1001 - 357 \cdot 2) - (357 - (1001 - 357 \cdot 2)) \cdot 4 \\ &= (1001 - 357 \cdot 2) - 357 \cdot 4 + (1001 - 357 \cdot 2) \cdot 4 \\ &= 1001 \cdot 5 - 357 \cdot 14. \end{aligned}$$

Thus, $7 = 1001 \cdot 5 - 357 \cdot 14$.

Remark 3.12.1

Two integers a and b are said to be relatively prime if $\mathrm{GCD}(a, b) = 1$. For instance, 4 and 9 are relatively prime integers.

Example 3.12.3: Exercise 12.7 at page 69

Find the $\mathrm{GCD}(-90, 1386)$ and write it as a linear combination of -90 and 1386.

Solution:

Following the Euclidean Algorithm for 1386 and 90, we get:

$$\begin{aligned} 1386 &= 90 \cdot 15 + 36, \\ 90 &= 36 \cdot 2 + 18, \\ 36 &= 18 \cdot 2 \end{aligned}$$

Therefore, $\mathrm{GCD}(-90, 1386) = 18$. To write 18 as a linear combination of -90 and 1386, we go back as follows:

$$\begin{aligned} 18 &= 90 - 36 \cdot 2 \\ &= 90 - (1386 - 90 \cdot 15) \cdot 2 \\ &= 90 \cdot 31 - 1386 \cdot 2 \\ &= (-90) \cdot (-31) - 1386 \cdot 2 \end{aligned}$$

Thus, $18 = (-90) \cdot (-31) - 1386 \cdot 2$.

Example 3.12.4: Exercise 12.21 at page 69

Prove that if $\mathrm{GCD}(a, m) = 1$, then there is a solution (for x) to the congruence $ax \equiv b \pmod{m}$.

Solution:

Since $\mathrm{GCD}(a, m) = 1$, we have $au + mv = 1$ for some $u, v \in \mathbb{Z}$. Then

$$a(ub) + m(vb) = b \qquad \Rightarrow \qquad a(ub) \equiv b \pmod{m}.$$

That is $x = ub$ is a solution.

Exercise 3.12.1

Solve the following exercises from the book at page 69:

- 12.1 – 12.7,
- 12.21.

Section 3.13: Factorization. Euler's Phi-Function

Theorem 3.13.1

If $a, b, c \in \mathbb{Z}$, with $a \mid bc$ and $\text{GCD}(a, b) = 1$, then $a \mid c$.

Proof:

Since $\text{GCD}(a, b) = 1$, then there is $m, n \in \mathbb{Z}$ such that $am + bn = 1$. Thus, $amc + bnc = c$. Clearly $a \mid amc$ and $a \mid bnc$ because $a \mid bc$. Thus, $a \mid (amc + bnc) = c$.

Theorem 3.13.2: Fundamental Theorem of Arithmetic

Each integer $n > 1$ can be written as a product of primes in one way. That is $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where $p_1 < p_2 < \cdots < p_k$ are primes and $e_1, e_2, \cdots, e_k$ are positive integers.

Definition 3.13.1

For each integer $n > 1$, let $\phi(n)$ denote the number of positive integers that are less than n and relatively prime to n. Also, let $\phi(1) = 1$. The function ϕ is called the Euler phi-function.

Example 3.13.1

Find $\phi(n)$ for $n = 5, 6,$ and 7.

Solution:

- $n = 5$, $\phi(5) = 4$, since 5 is relatively prime (and less than) to the set $\{1, 2, 3, 4\}$.
- $n = 6$, $\phi(6) = 2$, since 6 is relatively prime (and less than) to the set $\{1, 5\}$.
- $n = 7$, $\phi(7) = 6$, since 7 is relatively prime (and less than) to the set $\{1, 2, 3, 4, 5, 6\}$.

Theorem 3.13.3

Assume that p is a prime and r is a positive integer. Then

$$\phi(p^r) = p^r - p^{r-1} = p^r(1 - \frac{1}{p}).$$

In particular, $\phi(p) = p - 1$.

Theorem 3.13.4

If p and q are distinct primes, then

$$\phi(pq) = (p-1)(q-1).$$

Theorem 3.13.5

If $m, n \in \mathbb{Z}^+$ with $\text{GCD}(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Theorem 3.13.6

If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ with $p_1 < p_2 < \cdots < p_k$ are primes and $e_1, e_2, \cdots, e_k$ are positive integers, then

$$\begin{aligned}\phi(n) &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).\end{aligned}$$

Example 3.13.2

Find $\phi(12)$.

Solution:

Clearly, $12 = 2^2 \cdot 3$. That is

$$\phi(12) = 12 \;\cdot\; (1 - \frac{1}{2})\;(1 - \frac{1}{3}) = 12 \;\cdot\; \frac{1}{2} \;\cdot\; \frac{2}{3} = 4.$$

That is because 12 is relatively prime (and less than) to the set $\{1, 5, 7, 11\}$.

Definition 3.13.2

For each positive integer n, let $\mathbb{U}_n$ denote the set of congruence classes mod n defined as follows:

$$\mathbb{U}_n = \{[k] \;:\; 1 \leq k < n \text{ and } \text{GCD}(k, n) = 1\}.$$

Example 3.13.3

Find $\mathbb{U}_6$.

Solution:

Clearly 6 is relatively prime (and less than) to $\{1, 5\}$ and hence $\mathbb{U}_6 = \{[1], [5]\}$.

Example 3.13.4

Find $\mathbb{U}_9$.

Solution:

Clearly 9 is relatively prime to $\{1, 2, 4, 5, 7, 8\}$ and hence $\mathbb{U}_9 = \{[1], [2], [4], [5], [7], [8]\}$.

Theorem 3.13.7

$(\mathbb{U}_n, \odot)$ is an abelian group. The order of the group $\mathbb{U}_n$ is $\phi(n)$.

Proof:

We first show that $\mathbb{U}_n$ is closed under the operation $\odot$. Let $[a], [b] \in \mathbb{U}_n$, then $\mathrm{GCD}(a, n) = \mathrm{GCD}(b, n) = 1$. Hence there are r, s, t, u such that $ar + ns = 1$ and $bt + nu = 1$. Thus

$$(ar + ns)(bt + nu) = abrt + arnu + nsbt + n^2su = 1$$
$$\Rightarrow ab(rt) + n(aru + sbt + nsu) = 1 \quad \Rightarrow \quad \mathrm{GCD}(ab, n) = 1.$$

That is $[ab] \in \mathbb{U}_n$. We now show that $(\mathbb{U}_n, \odot)$ is abelian group.

$\mathcal{G}_1$: $\odot$ is associative and commutative on $\mathbb{Z}_n$ and hence it is associative and commutative on $\mathbb{U}_n$.

$\mathcal{G}_2$: Clearly, $[1] \in \mathbb{U}_n$ is the identity element.

$\mathcal{G}_3$: Let $[a] \in \mathbb{U}_n$. Then $\mathrm{GCD}(a, n) = 1$ and $ar + ns = 1$ for some $r, s \in \mathbb{Z}$. That is $ar = 1 + (-s)n$ and $ar \equiv 1 \pmod{n}$. Therefore, $[a] \odot [r] = [ar] = [1]$ which implies that $[r]$ is the inverse of $[a]$.

The order of $\mathbb{U}_n$ is $\phi(n)$ by the definition of $\mathbb{U}_n$ and $\phi(n)$.

Example 3.13.5

Find the inverse of $[37]$ in $\mathbb{U}_{50}$.

Solution:

Clearly, $\mathrm{GCD}(37, 50) = 1$, then $37r + 50s = 1$ for some $r, s \in \mathbb{Z}$. That is $37r = 1 + (-s)50$ which implies that $37r \equiv 1 \pmod{50}$. Therefore,

$$\begin{aligned}
50 &= 37 \cdot 1 + 13 \\
37 &= 13 \cdot 2 + 11 \\
13 &= 11 \cdot 1 + 2 \\
11 &= 2 \cdot 5 + 1 \\
2 &= 1 \cdot 2
\end{aligned}$$

Therefore,

$$\begin{aligned}
1 &= 11 - 2 \cdot 5 \\
&= 11 - (13 - 11 \cdot 1) \cdot 5 \\
&= -13 \cdot 5 + 11 \cdot 6 \\
&= -13 \cdot 5 + (37 - 13 \cdot 2) \cdot 6 \\
&= -13 \cdot 5 + 37 \cdot 6 - 13 \cdot 12 \\
&= 37 \cdot 6 - 13 \cdot 17 \\
&= 37 \cdot 6 - (50 - 37 \cdot 1) \cdot 17 \\
&= (-17) \cdot 50 + 37 \cdot 6 + 37 \cdot 17 \\
&= (-17) \cdot 50 + 37 \cdot (23).
\end{aligned}$$

Thus, the inverse of $[37]$ is $[23]$ in $\mathbb{U}_{50}$.

Exercise 3.13.1

Solve the following exercises from the book at pages 72 - 73:

- 13.1 – 13.4,
- 13.7 – 13.10,
- 13.13 – 13.14.

Exercise 3.13.2

Find the least non-negative integer x so that:

1. $17x \equiv 3 \pmod{29}$. **<u>Solution</u>**: Note that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$. Therefore, to find x, we do:

$$17x \equiv 3 \pmod{29} \Rightarrow x \equiv 17^{-1}3 \pmod{29}.$$

We use Euclid's Algorithm to find 17^{-1}:

$$\begin{aligned} 29 &= 17 \cdot 1 + 12 \\ 17 &= 12 \cdot 1 + 5 \\ 12 &= 5 \cdot 2 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 \end{aligned}$$

Therefore,

$$1 = \cdots = (12)17 + 29(-7).$$

Therefore, $17^{-1} = 12$ and hence $x \equiv 12 \cdot 3 \pmod{29}$. That is $x \equiv 36 \pmod{29}$. Therefore, $x \equiv 7 \pmod{29}$. ☐

2. $17x \equiv 1 \pmod{43}$. **<u>Solution</u>**: $x \equiv (-5) \equiv 38\, (mod\ 43)$. ☐

Chapter

4 Groups

Section 4.14: Elementary Properties

Theorem 4.14.1

Let $(G, *)$ be a group. Then:

a. If $a, b, c \in G$ and $a * b = a * c$, then $b = c$. "left cancelation law"

b. If $a, b, c \in G$ and $b * a = c * a$, then $b = c$. "right cancelation law"

c. If $a, b \in G$, then each of the equation $a * x = b$ and $x * a = b$ has a unique solution. In the first, $x = a^{-1} * b$; in the second, $x = b * a^{-1}$.

d. If $a \in G$, then $(a^{-1})^{-1} = a$.

e. If $a, b \in G$, then $(a * b)^{-1} = b^{-1} * a^{-1}$.

Proof:

a. Assume that $a * b = a * c$ for $a, b, c \in G$. We multiply both sides from left by a^{-1}:

$$a^{-1} * a * b = a^{-1} * a * c$$
$$e * b = e * c$$
$$b = c.$$

b. Similar to part "a.".

c. Consider the equation $a * x = b$ and multiply both sides from left by $a^{-1} \in G$:

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

Uniqueness: If x_1 and x_2 are two solutions to the equation $a * x = b$, then

$$a^{-1} * a * x_1 = a^{-1} * b = a^{-1} * a * x_2$$
$$e * x_1 = a^{-1} * b = e * x_2$$
$$x_1 = a^{-1} * b = x_2.$$

The second equation "$x * a = b$" can be proved in a similar way by multiplying both sides from right by a^{-1}.

d. The inverse of a^{-1} is the unique element $b \in G$ such that $a^{-1} * b = e$. But clearly, $a^{-1} * a = e$; thus, $b = a$ is the inverse of a^{-1}.

e. Clearly,

$$(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * a^{-1} = e, \quad \textit{and}$$
$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * (a^{-1} * a) * b = b^{-1} * b = e.$$

Thus, $(a * b)^{-1} = b^{-1} * a^{-1}$.

Definition 4.14.1

Let G be a group and $a \in G$. Then we define the integral power as follows:

$$a^0 = e, \; a^1 = a, \; a^2 = a * a, \; \cdots, \; a^{n+1} = a^n * a.$$

Moreover, $a^{-n} = (a^{-1})^n$ for each positive integer n.

Remark 4.14.1

$\star$ Multiplicative notation:	$\star$ Additive notation
$a^m a^n = a^{m+n}$	$ma + na = (m+n)a$
$(a^m)^n = a^{mn}$	$n(ma) = (mn)a$
$(a^{-1})^n = a^{-n}$	$n(-a) = (-n)a.$

Example 4.14.1

Consider some powers for the elements of $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the operation "+".

Solution:

Consider 1 for instance to get

$$\left.\begin{aligned} &1^1 && = 1 \\ &1^2 = 1+1 && = 2 \\ &1^3 = 1+1+1 && = 3 \\ &1^4 = 1+1+1+1 && = 4 \end{aligned}\right\} \quad \text{all } \mathbb{Z}_4 \text{ elements.}$$

While

$$\left.\begin{aligned} &2^1 && = 2 \\ &2^2 = 2+2 && = 4 = 0 \\ &2^3 = 2+2+2 && = 6 = 2 \end{aligned}\right\} \quad \text{elements of } \{0,2\} \text{ in } \mathbb{Z}_4.$$

For 3, we have

$$\left.\begin{aligned} &3^1 && = 3 \\ &3^2 = 3+3 && = 6 = 2 \\ &3^3 = 3+3+3 && = 9 = 1 \\ &3^4 = 3+3+3+3 && = 12 = 0 \end{aligned}\right\} \quad \text{all } \mathbb{Z}_4 \text{ elements.}$$

Note that,

$$\left.\begin{aligned} &1^{-1} && = 3 \\ &1^{-2} = 1^{-1}+1^{-1} && = 3+3 = 6 = 2 \\ &1^{-3} = 1^{-1}+1^{-1}+1^{-1} && = 3+3+3 = 9 = 1 \\ &1^{-4} = 1^{-1}+1^{-1}+1^{-1}+1^{-1} && = 3+3+3+3 = 12 = 0 \end{aligned}\right\} \quad \text{all } \mathbb{Z}_4 \text{ elements.}$$

Definition 4.14.2

Let G be a group and $a \in G$. Then $\langle\, a \,\rangle = \{a^n : n \in \mathbb{Z}\}$. That is

$$\langle\, a \,\rangle = \{\cdots, a^{-2}, a^{-1}, a^0 = e, a^1, a^2, \cdots\}.$$

Definition 4.14.3

A group G is called **cyclic** if there is some element $a \in G$ such that $\langle\, a \,\rangle = G$.

Definition 4.14.4

An element a of a group G **generates** G and is a **generator of** G if $\langle a \rangle = G$.

Definition 4.14.5

The group $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is the **cyclic subgroup of** G **generated by** a.

Theorem 4.14.2

Let G be a group with $a \in G$. Then $\langle a \rangle$ is a subgroup of G. In fact, it is the smallest subgroup of G containing a.

Proof:

$\mathcal{S}_1$: Clearly, $a \in \langle a \rangle$ and hence $\langle a \rangle$ is nonempty.

$\mathcal{S}_2$: Let $b, c \in \langle a \rangle$, then $b = a^m$ and $c = a^n$ for some $m, n \in \mathbb{Z}$. Clearly, $m + n \in \mathbb{Z}$ and thus $bc = a^m a^n = a^{m+n} \in \langle a \rangle$. Therefore, $\langle a \rangle$ is closed.

$\mathcal{S}_3$: Let $a^t \in \langle a \rangle$ for some $t \in \mathbb{Z}$. Then $-t \in \mathbb{Z}$ and $a^{-t} \in \langle a \rangle$ where $a^t a^{-t} = e$. Thus each element in $\langle a \rangle$ has inverse.

Note that $a \in \langle a \rangle$ and since it is a subgroup of G,

$$aa = a^2 \in \langle a \rangle, \; a^2 a = a^3 \in \langle a \rangle, \quad \text{and so on.}$$

That is a subgroup containing a must contain $\{a^n : n \in \mathbb{Z}\} = \langle a \rangle$. Thus, it is the smallest subgroup of G containing a.

Example 4.14.2

Example of some cyclic groups:

1. $\langle 2 \rangle = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\} = 2\mathbb{Z} \leq \mathbb{Z}$ is cyclic.
2. $\langle 1 \rangle = \mathbb{Z}$ is cyclic.
3. $\langle -1 \rangle = \mathbb{Z}$ is cyclic.
4. $\mathbb{Z}$ has only two generators which are 1 and -1.

5. $\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle$ is cyclic.

6. $\langle 2 \rangle = \{0, 2\} \leq \mathbb{Z}_4$ is cyclic.

Theorem 4.14.3

Every cyclic group is abelian.

Proof:

Let G be a cyclic group and say $G = \langle a \rangle$ for some $a \in G$. Thus, for $g, h \in G$, there are $r, s \in \mathbb{Z}$ such that $g = a^r$ and $h = a^s$. Then,

$$gh = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg.$$

Thus G is abelian.

Definition 4.14.6

Let a be an element of a group G. If the cyclic subgroup $\langle a \rangle$ of G is finite, then the **order of** a, denoted by $o(a)$, is the order $|\langle a \rangle|$ of this cyclic subgroup. Otherwise, we say that a is of infinite order.

Remark 4.14.2

If $a \in G$ is of finite order m, then m is the smallest positive integer such that $a^m = e$. In that case, $\langle a \rangle = \{a^0 = e, a, a^2, \cdots, a^{m-1}\}$.

Example 4.14.3

Let $G = \langle a \rangle$, $a \in G$ and $|G| = 5$. So, $a^5 = e$. Therefore, $G = \{e, a, a^2, a^3, a^4\}$.

Remark 4.14.3

If G is a cyclic group with $G = \langle a \rangle$, then $G = \langle a^{-1} \rangle$.

Example 4.14.4

S_3 is not cyclic since there is no $a \in S_3$ with $\langle a \rangle = S_3$. Moreover, if S_3 is cyclic, then it is abelian which is not the case.

Example 4.14.5

Compute $A_3 = \langle (1\ \ 3\ \ 2) \rangle$ in S_3.

Solution:

$$(1\ \ 3\ \ 2)^0 = id$$
$$(1\ \ 3\ \ 2)^1 = (1\ \ 3\ \ 2)$$
$$(1\ \ 3\ \ 2)^2 = (1\ \ 3\ \ 2)(1\ \ 3\ \ 2) = (1\ \ 2\ \ 3)$$
$$(1\ \ 3\ \ 2)^3 = (1\ \ 3\ \ 2)(1\ \ 3\ \ 2)(1\ \ 3\ \ 2) = id.$$

Thus, $A_3 = \langle (1\ \ 3\ \ 2) \rangle = \{id, (1\ \ 3\ \ 2), (1\ \ 2\ \ 3)\}$, and the order of $(1\ \ 3\ \ 2)$ in S_3 is 3.

4.14.1 Solving Book Problems from Section 14

Exercise 4.14.1

Q.14.1: Solve the equation $(1\ \ 2)\ x = (1\ \ 2\ \ 3)$ in S_3.

Solution:

$$\begin{aligned} x &= (1\ \ 2)^{-1}(1\ \ 2\ \ 3) \\ &= (1\ \ 2)(1\ \ 2\ \ 3) = (2\ \ 3). \end{aligned}$$

Exercise 4.14.2

Q.14.14(a): Prove that if a and b are elements of an abelian group G with $o(a) = m$ and $o(b) = n$, then $(ab)^{mn} = e$.

Solution:

We have $o(a) = m$ and $o(b) = n$ which implies that $a^m = e$ and $b^n = e$. Thus,

$$\begin{aligned} (ab)^{mn} &= ab \cdot ab \cdot \cdots \cdot ab, && mn\text{-times} \\ &= (a^{mn})\ (b^{mn}) = (a^m)^n\ (b^n)^m, && G \text{ is abelian} \\ &= e^n\ e^m = e. \end{aligned}$$

Exercise 4.14.3

Q.14.18: Assume that a and b are elements of a group G.

1. Prove that $ab = ba$ if and only if $a^{-1}b^{-1} = b^{-1}a^{-1}$.
2. Prove that $ab = ba$ if and only if $(ab)^2 = a^2b^2$.

Solution:

(1.) Clearly, $ab = ba \ \Leftrightarrow\ (ab)^{-1} = (ba)^{-1} \ \Leftrightarrow\ b^{-1}a^{-1} = a^{-1}b^{-1}$.

(2.) „ $\Rightarrow$ ": Assume that $ab = ba$, then

$$(ab)^2 = (ab)(ab) = a\,\underline{b\,a}\,b = a\,a\,b\,b = a^2\,b^2.$$

„ $\Leftarrow$ ": Assume that $(ab)^2 = a^2b^2$. Thus, $(\cancel{a}b)\,(a\,\cancel{b}) = \cancel{a}\,a\,b\,\cancel{b}$, implies that $ba = ab$.

Exercise 4.14.4

Q.14.23: Prove that a non-identity element of a group has order 2 if and only if it is its own inverse.

Solution:

„ $\Rightarrow$ ": Assume that $a \neq e$ such that $o(a) = 2$. Then,

$$a^2 = e \Leftrightarrow a^{-1}a^2 = a^{-1}e \Leftrightarrow a = a^{-1}.$$

„ $\Leftarrow$ ": If $a = a^{-1}$, then $a \cdot a = a \cdot a^{-1}$ and hence $a^2 = e$. That is $o(a) = 2$.

Exercise 4.14.5

Q.14.24: Prove that every group of even order has an element of order 2.

Solution:

Assume that G is a group of even order. Let $A = \{a \in G : a \neq a^{-1}\} \subseteq G$. Clearly, $e \notin A$ since $e = e^{-1}$. Also, if $a \in A$, then $a^{-1} \in A$. Thus, $\{e\} \cup A$ has an odd number of elements, but $\{e\} \cup A \subsetneqq G$ "because $|G|$ is even". Therefore there exists $x \in G$ such that $x \neq e$ and $x \notin A$ with $x = x^{-1}$. Thus, $x^2 = e$ which means $o(x) = 2$.

Exercise 4.14.6

Q.14.29: Prove that a group G is abelian if each of its non-identity elements has order 2.

Solution:

Suppose that G is a group so that if $a \in G$ and $a \neq e$, then $o(a) = 2$. Thus, $a^2 = e$ and $a = a^{-1}$. If $a, b \in G$, then $ab \in G$ and hence $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

Exercise 4.14.7

Q.14.33: Prove or give a counterexample: If a group G has a subgroup of order n, then G has an element of order n.

Solution:

False. Consider $S_3 \leq S_3$ where both are of order $3! = 6$ but no element in S_3 has order 6.

Exercise 4.14.8

Q.14.34: Prove that if a group G has no subgroup other than G and $\{e\}$, then G is cyclic.

Solution:

Let $a \in G$ so that $a \neq e$. Then $\langle a \rangle$ is a subgroup of G. Then $\langle a \rangle = e$ or $\langle a \rangle = G$. But since $a \neq e$, we have $\langle a \rangle \neq e$. Therefore, $\langle a \rangle = G$ and hence G is a cyclic group.

Exercise 4.14.9

Q.14.38: Prove that if A and B are subgroups of a group G, and $A \cup B$ is also a subgroup of G, then $A \subseteq B$ or $B \subseteq A$.

Solution:

A proof by contradiction: Assume that $A \nsubseteq B$ and $B \nsubseteq A$. Then, there is $x \in (A - B)$ and there is $y \in (B - A)$. But $x, y \in A \cup B$ (which is a subgroup). Thus, $xy \in A \cup B$. Hence, $xy \in A$ or $xy \in B$.

Case 1: $xy \in A$ where $x \in A$. Then $x^{-1} \in A$ and hence $x^{-1}xy = y \in A$ (contradiction).

Case 1: $xy \in B$ where $y \in B$. Then $y^{-1} \in B$ and hence $xyy^{-1} = x \in B$ (contradiction).

Therefore, $A \subseteq B$ or $B \subseteq A$.

Exercise 4.14.10

Solve the following exercises from the book at pages 79 - 81:

- $14.1 - 14.6$,
- 14.13,
- $14.14(a)$,
- 14.18,
- $14.23 - 14.26$,
- $14.28 - 14.30$,
- $14.33 - 14.34$,
- 14.38.

Section 4.15: Direct Products

Definition 4.15.1

Let G and H be two groups. Then $G \times H$ is the (Cartesian) product of G and H and is defined by

$$G \times H = \{(g, h) : g \in G \text{ and } h \in H\}.$$

Theorem 4.15.1

If G and H are groups, then $G \times H$ is a group with the operation defined by

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$$

for all $g_1, g_2 \in G$ and $h_1, h_2 \in H$. The group $G \times H$ is called **the direct product of G and H**.

Remark 4.15.1

To prove the previous theorem, we need to note that:

1. The identity element of $G \times H$ is (e_G, e_H) where e_G is the identity element of G and e_H is the identity element of H.
2. The inverse of the element $(g, h) \in G \times H$ is the element $(g^{-1}, h^{-1}) \in G \times H$.

Remark 4.15.2

Note that in $\mathbb{Z} \times \mathbb{Z}$ we have $(a, b)(c, d) = (a + c, b + d)$ for all $a, b, c, d \in \mathbb{Z}$.

Remark 4.15.3

Note that if A and B are finite, then so is $A \times B$ with $|A \times B| = |A| \cdot |B|$.

Example 4.15.1

Compute $\mathbb{Z}_3 \times S_2$ and compute $([1], (1\ \ 2))([2], e)$ in $\mathbb{Z}_3 \times S_2$.

Solution:

Note that $\mathbb{Z}_3 = \{[0],[1],[2]\}$ and $S_2 = \{e,(1\ \ 2)\}$. Thus,

$$\mathbb{Z}_3 \times S_2 = \{([0],e),([0],(1\ \ 2)),([1],e),([1],(1\ \ 2)),([2],e),([2],(1\ \ 2))\}.$$

Moreover,

$$([1],(1\ \ 2))([2],e) = ([1]\oplus[2],(1\ \ 2)e) = ([0],(1\ \ 2)).$$

Example 4.15.2

Simplify $([2],(1\ \ 2\ \ 3))^{-1}([1],(2\ \ 4))([2],(1\ \ 2\ \ 3))$ in $\mathbb{Z}_4 \times S_4$.

Solution:

$$\begin{aligned}([2],(1\ \ 2\ \ 3))^{-1}([1],(2\ \ 4))([2],(1\ \ 2\ \ 3)) &= ([2],(1\ \ 3\ \ 2))([3],(1\ \ 4\ \ 2\ \ 3)) \\ &= ([1],(1\ \ 4)).\end{aligned}$$

Example 4.15.3: Exercise 15.17 at page 84

Let G and H be two groups. Show that $G\times\{e_H\}$ and $\{e_G\}\times H$ are both subgroups of $G\times H$.

Solution:

Note that $G\times\{e_H\} = \{(g,e_H) : g\in G\}$. Thus

$\mathcal{S}_1$: Clearly, $(e_G,e_H)\in G\times\{e_H\}$ and hence $G\times\{e_H\}$ is nonempty.

$\mathcal{S}_2$: Let $(g_1,e_H),(g_2,e_H)\in G\times\{e_H\}$. Then

$$(g_1,e_H)(g_2,e_H) = (g_1g_2,e_H)\in G\times\{e_H\} \text{ since } g_1g_2\in G.$$

$\mathcal{S}_3$: Let $(g,e_H)\in G\times\{e_H\}$. Then $g^{-1}\in G$ since $g\in G$ and hence

$$(g,e_H)(g^{-1},e_H) = (gg^{-1},e_H) = (e_G,e_H).$$

That is (g^{-1},e_H) is the inverse of (g,e_H) and it is in $G\times\{e_H\}$.

Therefore, $G\times\{e_H\}$ is a subgroup of $G\times H$. The other part can be preved in a similar way.

Example 4.15.4: Exercise 15.18 at page 84

Let G and H be two groups. Show that $G \times H$ is abelian group if and only if both G and H are abelian.

Solution:

" $\Rightarrow$ ": Assume that $G \times H$ is abelian group and let $g_1, g_2 \in G$ and $h_1, h_2 \in H$. Then

$$\begin{aligned}(g_1g_2, h_1h_2) &= (g_1, h_1)(g_2, h_2) \\ &= (g_2, h_2)(g_1, h_1) = (g_2g_1, h_2h_1).\end{aligned}$$

Thus, $g_1g_2 = g_2g_1$ and G is abelian; and $h_1h_2 = h_2h_1$ and H is abelian.

" $\Leftarrow$ ": Assume that G and H are abelian groups and that $(g_1, h_1), (g_2, h_2) \in G \times H$. Then,

$$\begin{aligned}(g_1, h_1)(g_2, h_2) &= (g_1g_2, h_1h_2) \\ &= (g_2g_1, h_2h_1) = (g_2, h_2)(g_1, h_1).\end{aligned}$$

Thus, $G \times H$ is abelian.

Exercise 4.15.1

Solve the following exercises from the book at pages 84 - 85:

- 15.9,
- 15.16 – 15.18,
- 15.20 – 15.21.

Exercise 4.15.2

Simplify $([2],(1\ \ 2\ \ 3))^{-1}([1],(2\ \ 4))([2],(1\ \ 2\ \ 3))$ in $\mathbb{Z}_4 \times S_4$.

Section 4.16: Cosets

Recall that if $n \in \mathbb{Z}$, then $\langle\, n\,\rangle$ is the subgroup consisting of all multiples of n. Because

$$a \equiv b\ (mod\ n) \ \Leftrightarrow\ n \mid a-b \ \Leftrightarrow a-b = kn,\ \text{for some } k \in \mathbb{Z}.$$

Thus, $a \equiv b\ (mod\ n) \ \Leftrightarrow\ a-b \in \langle\, n\,\rangle$.

Theorem 4.16.1

Let H be a subgroup of a group G and define a relation $\sim$ on G by $a \sim b$ if and only if $ab^{-1} \in H$. Then $\sim$ is an equivalence relation on G.

Proof:

Reflexive: If $a \in G$, then $a \sim a$ because $a\,a^{-1} = e \in H$.

Symmetric: If $a \sim b$, then $ab^{-1} \in H$ and so is $(ab^{-1})^{-1} = ba^{-1} \in H$ because H contains the inverse of any of its elements. Thus $b \sim a$.

Transitive: If $a \sim b$ and $b \sim c$, then $ab^{-1}, bc^{-1} \in H$. Since H is a subgroup of G, it contains the product of ab^{-1} and bc^{-1}. Thus, $ab^{-1} \cdot bc^{-1} = ac^{-1} \in H$. Hence $a \sim c$. Therefore, $\sim$ is an equivalence relation on G.

Definition 4.16.1

Let G be a group with a subgroup H. For any $a \in G$, define:

1) **the left coset of** H **in** G by $aH = \{ah : h \in H\}$,

2) **the right coset of** H **in** G by $Ha = \{ha : h \in H\}$.

Note that, if the group operation is $+$, then $H + a$ and $a + H$ is used instead of Ha and aH, respectively.

Example 4.16.1

Let $G = \mathbb{Z}$ and $H = \langle\, 7\,\rangle$. Compute $H + 3$

Solution:

$$H + 3 = \langle\, 7\,\rangle + 3 = \{\cdots, -14, -7, 0, 7, 14, \cdots\} + 3 = \{\cdots, -11, -4, 3, 10, 17, \cdots\}.$$

Note that $H+3$ is the congruence class $[3]$ in $\mathbb{Z}_7$. In $\mathbb{Z}_7$, $[3] = \{k : k \equiv 3(\mathrm{mod} 7) \text{ iff } 7 \mid 3-k\}$.

Example 4.16.2

Let $G = S_3$ and $H = \{e, (1\ \ 2)\}$. Compute He, $H(1\ \ 2\ \ 3)$, and $H(1\ \ 3\ \ 2)$.

Solution:

$$\begin{aligned} He &= \{ee, (1\ \ 2)e\} = \{e, (1\ \ 2)\} \\ H(1\ \ 2\ \ 3) &= \{e(1\ \ 2\ \ 3), (1\ \ 2)(1\ \ 2\ \ 3)\} = \{(1\ \ 2\ \ 3), (2\ \ 3)\} \\ H(1\ \ 3\ \ 2) &= \{e(1\ \ 3\ \ 2), (1\ \ 2)(1\ \ 3\ \ 2)\} = \{(1\ \ 3\ \ 2), (1\ \ 3)\} \end{aligned}$$

Note that these three sets form a partition of G.

Example 4.16.3

Let $G = S_3$ and $H = \{e, (1\ \ 3)\}$. Find $(1\ \ 2)H$, $H(1\ \ 2)$, and $(1\ \ 3\ \ 2)H$.

Solution:

$S_3 = \{e, (1\ \ 2), (1\ \ 3), (2\ \ 3), (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$. So,

$$(1\ \ 2)H = \{(1\ \ 2), (1\ \ 3\ \ 2)\} \qquad H(1\ \ 2) = \{(1\ \ 2), (1\ \ 2\ \ 3)\}, \text{ and}$$
$$(1\ \ 3\ \ 2)H = \{(1\ \ 3\ \ 2), (1\ \ 2)\}.$$

Remark 4.16.1

Considering the previous example, we conclude:

1. Cosets are not subgroups in general.
2. aH might be the same as bH even though $a \neq b$. For instance, $(1\ \ 2)H = (1\ \ 3\ \ 2)H$ in the previous example.
3. aH need not be equal to Ha, in general. From the previous example we conclude that $(1\ \ 2)H = \{(1\ \ 2), (1\ \ 3\ \ 2)\}$ is not the same as $H(1\ \ 2) = \{(1\ \ 2), (1\ \ 2\ \ 3)\}$.
4. Cosets have the same number of elements as H, i.e. $|\,aH\,| = |\,H\,| = |\,Ha\,|$ for any $a \in G$.

Theorem 4.16.2

If H is a subgroup of a group G, and $a, b \in G$, then the following conditions are equivalent:

1. $a^{-1}b \in H$.
2. $b = ah$ for some $h \in H$.
3. $b \in aH$.
4. $bH = aH$.

Proof:

We show that the conditions are equivalent by showing that $1 \to 2$, $2 \to 3$, $3 \to 4$, and $4 \to 1$.

a. $1 \to 2$: Let $a^{-1}b = h \in H$, then $aa^{-1}b = ah$ and hence $b = ah$ with $h \in H$.

b. $2 \to 3$: If $b = ah$ for some $h \in H$, then $b \in aH$ by the definition of aH.

c. $3 \to 4$: If $b \in aH$, then $b = ah$ for some $h \in H$. We show that $bH \subseteq aH$ and $aH \subseteq bH$. First, Let $s \in bH$ with $s = br$ for some $r \in H$. Then

$$s = br = (ah)r = a(hr) \text{ with } hr \in H.$$

Therefore,

$$s \in aH, \text{ and hence } bH \subseteq aH.$$

Now, let $t \in aH$ with $t = as$ for some $s \in H$. Note that $b = ah$ implies that $a = bh^{-1}$. Thus

$$t = as = (bh^{-1})s = b(h^{-1}s) \text{ with } h^{-1}s \in H.$$

Therefore,

$$t \in bH, \text{ and hence } aH \subseteq bH.$$

Therefore, $aH = bH$.

d. $4 \to 1$: If $bH = aH$, then $b = ah$ for some $h \in H$. Hence $a^{-1}b = a^{-1}ah$ and hence $a^{-1}b = h \in H$.

Remark 4.16.2

To compute all of the right cosets of a subgroup H in a finite group G, we do the following:

1. First write H as $H = He$.
2. Next choose $a_1 \in G - H$ and compute Ha_1.
3. Next choose $a_2 \in G - (H \cup Ha_1)$ and compute Ha_2.
4. Continue in this way until the elements of G have been considered.
5. Finally $G = H \cup Ha_1 \cup Ha_2 \cup \cdots \cup Ha_n$ for some n.

Example 4.16.4

Let $G = \mathbb{Z}_9$ and $H = \langle 3 \rangle$. Find all right cosets of H in G.

Solution:

$$H = H + 0 = \{3, 6, 0\}, \qquad H + 1 = \{4, 7, 1\},$$
$$H + 2 = \{5, 8, 2\}.$$

Note that $G = \mathbb{Z}_9 = H \cup H + 1 \cup H + 2$.

Theorem 4.16.3

Let H be a subgroup of a group G and let $a, b \in G$. Then

1. $a \in aH$.
2. $aH = H$ if and only if $a \in H$.
3. It is either $aH = bH$ or $aH \cap bH = \phi$.
4. $aH = bH$ if and only if $a^{-1}b \in H$.
5. $|\,aH\,| = |\,H\,|$ for finite subgroup H.
6. $aH = Ha$ if and only if $H = aHa^{-1}$.
7. aH is a subgroup of G if and only if $a \in H$.

Proof:

1. Clearly $e \in H$, then $ae = a \in aH$.

2. „ $\Rightarrow$ " By 1, we have $a \in aH = H$, then $a \in H$.

   „ $\Leftarrow$ " Assume that $a \in H$. For any $h \in H$, we have $ah \in aH$ (by definition of aH). But also $ah \in H$ (since H is a subgroup) and hence $aH \subseteq H$.

   Let $h \in H$. If $a \in H$, then $a^{-1} \in H$ (H is a subgroup) and hence $a^{-1}h \in H$. Therefore, $a(a^{-1}h) = h \in aH$ (by definition of aH). That is $H \subseteq aH$ and hence $aH = H$.

3. Assume that there is $x \in aH \cap bH$, then $x \in aH$ and $x \in bH$. That is $ah_1 = x = bh_2$ and hence $bh_2 \in aH$ and $ah_1 \in bH$ which implies that $aH = bH$. Otherwise, there is no $x \in aH \cap bH$ and hence $aH \cap bH = \phi$.

4. $aH = bH$ if and only if $a^{-1}bH = H$ if and only if $a^{-1}b = h \in H$ (by (2)).

5. There is a bijection $\alpha : H \to aH$ which is defined by $\alpha(h) = ah$.

6. Clearly, $aH = Ha$ if and only if $aHa^{-1} = H$.

7. „ $\Rightarrow$ ": Since $a \in aH$ (by (1)), then $a^2 \in aH$ and hence $a^2 = ah$ for some $h \in H$ and hence $a = h \in H$.

   „ $\Leftarrow$ ": If $a \in H$, then $aH = H$ (by (2)). Thus $aH \leq G$.

4.16.1 Solving Book Problems from Section 16

Exercise 4.16.1

Q.16.1: Determine the right cosets of $\langle 4 \rangle$ in $\mathbb{Z}_8$.

Solution:

Note that $\langle 4 \rangle = \{4, 0\}$. Therefore,

$$\langle 4 \rangle = \{4,0\}, \qquad \langle 4 \rangle + 1 = \{5,1\},$$
$$\langle 4 \rangle + 2 = \{6,2\}, \qquad \langle 4 \rangle + 3 = \{7,3\}.$$

Thus, $\mathbb{Z}_8 = \langle 4 \rangle \cup \langle 4 \rangle + 1 \cup \langle 4 \rangle + 2 \cup \langle 4 \rangle + 3$.

Exercise 4.16.2

Q.16.5: Determine the right cosets of $\langle (1\ \ 2\ \ 3) \rangle$ in S_3.

Solution:

Let $H = \langle (1\ \ 2\ \ 3) \rangle = \{e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$. Therefore,

$$H = \{e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\} \qquad \text{and} \qquad H(1\ \ 2) = \{(1\ \ 2), (1\ \ 3), (2\ \ 3)\}.$$

Thus, $S_3 = H \cup H(1\ \ 2)$.

Exercise 4.16.3

Q.16.11: If H is a subgroup of a group G and $a, b \in G$, then the following four conditions are equivalent:

1. $a^{-1}b \in H$.
2. $b = ah$ for some $h \in H$.
3. $b \in aH$.
4. $aH = bH$.

Solution:

We proof that the four conditions are equivalent by showing that 1 implies 2, 2 implies 3, 3 implies 4, and 4 implies 1.

1. Suppose that $a^{-1}b \in H$. Then, there is $h \in H$ with $a^{-1}b = h$ and hence $b = ah$.
2. Assume that $b = ah$ for some $h \in H$. Therefore, $b \in aH$.
3. Suppose that $b \in aH$. Then, there is $h \in H$ with $b = ah$. Thus $a^{-1}b = h \in H$. Hence $a^{-1}b \in H$ and $a^{-1}bH = H$ which implies that $aH = bH$.
4. Assume that $aH = bH$. Thus, $H = a^{-1}bH$, and hence $a^{-1}b \in H$.

Exercise 4.16.4

Q.16.12: Verify that if H is a subgroup of an abelian group G, and $a \in G$, then $aH = Ha$.

Solution:

First, $ah \in aH$ and hence (since G is abelian) $ha \in aH$ but $ha \in Ha$. Thus, $aH \subseteq Ha$. Second, $ha \in Ha$ and hence (since G is abelian) $ah \in Ha$, but $ah \in aH$. Then $Ha \subseteq aH$. Therefore, $aH = Ha$.

Exercise 4.16.5

Q.16.17: Compute the left cosets (or right) of $\langle\, ((1\ \ 2), 1)\,\rangle$ in $S_3 \times \mathbb{Z}_2$.

Solution:

Let $H = \langle\, ((1\ \ 2), 1)\,\rangle = \{(e, 0), ((1\ \ 2), 1)\}$. Then the left cosets are:

$$\begin{aligned}
H &= \{(e, 0), ((1\ \ 2), 1)\} \\
(e, 1)H &= \{(e, 1), ((1\ \ 2), 0)\}, \\
((1\ \ 3), 0)H &= \{((1\ \ 3), 0), ((1\ \ 2\ \ 3), 1)\}, \\
((1\ \ 3), 1)H &= \{((1\ \ 3), 1), ((1\ \ 2\ \ 3), 0)\}, \\
((2\ \ 3), 0)H &= \{((2\ \ 3), 0), ((1\ \ 3\ \ 2), 1)\}, \\
((2\ \ 3), 1)H &= \{((2\ \ 3), 1), ((1\ \ 3\ \ 2), 0)\},
\end{aligned}$$

Hence

$$S_3 \times \mathbb{Z}_2 = H \cup (e,1)H \cup ((1\ \ 3),0)H \cup ((1\ \ 3),1)H \cup ((2\ \ 3),0)H \cup ((2\ \ 3),1)H.$$

Exercise 4.16.6

Q.16.18: Compute the left cosets (or right) of $\langle\, (1\ \ 2)\,\rangle \times \langle\, 1\,\rangle$ in $S_3 \times \mathbb{Z}_2$.

Solution:

Let $H = \langle\, (1\ \ 2)\,\rangle \times \langle\, 1\,\rangle = \{e, (1\ \ 2)\} \times \{0, 1\} = \{(e,0), (e,1), ((1\ \ 2),0), ((1\ \ 2),1)\}$. Then the left cosets are:

$$\begin{aligned}
H &= \{(e,0), (e,1), ((1\ \ 2),0), ((1\ \ 2),1)\},\\
((1\ \ 3),0)H &= \{((1\ \ 3),0), ((1\ \ 3),1), ((1\ \ 2\ \ 3),0), ((1\ \ 2\ \ 3),1)\},\\
((2\ \ 3),0)H &= \{((2\ \ 3),0), ((2\ \ 3),1), ((1\ \ 3\ \ 2),0), ((1\ \ 3\ \ 2),1)\}.
\end{aligned}$$

Hence

$$S_3 \times \mathbb{Z}_2 = H \cup ((1\ \ 3),0)H \cup ((2\ \ 3),0)H.$$

Exercise 4.16.7

Q.16.21: Prove that if H and K are subgroups of a group G, then any left (right, respectively) coset of $H \cap K$ in G is the intersection of a left (right) coset of H in G and a left (right) coset of K in G.

Solution:

First note that since H and K are both subgroups of G, then $H \cap K$ is also a subgroup of G. Assume that $a(H \cap K)$ be any left coset of $H \cap K$ in G. Then

$$\begin{aligned}
& w \in a(H \cap K) \Leftrightarrow a^{-1}w \in H \cap K \text{ (this is by Q.16.11)}\\
\Leftrightarrow\ & \exists h \in H \text{ and } \exists k \in K \text{ such that } a^{-1}w = h = k\\
\Leftrightarrow\ & \exists h \in H \text{ and } \exists k \in K \text{ such that } w = ah = ak\\
\Leftrightarrow\ & w \in aH \text{ and } w \in aK\\
\Leftrightarrow\ & w \in aH \cap aK.
\end{aligned}$$

Therefore, $a(H \cap K) = aH \cap aK$.

Exercise 4.16.8

Solve the following exercises from the book at pages 87 - 88:

- 16.1 – 16.2,
- 16.5 – 16.6,
- 16.12 – 16.12,
- 16.17 – 16.18,
- 16.21.

Section 4.17: Lagrange's Theorem. Cyclic Groups

Definition 4.17.1

If G is a finite group and H is a subgroup of G, then the number of distinct left cosets of H in G, denoted by $\left[G : H\right]$, is called the **index** of H in G.

Theorem 4.17.1: Lagrange's Theorem

If G is a finite group and H is a subgroup of G, then $|\,H\,|$ divides $|\,G\,|$. Moreover $\left[G : H\right] = \dfrac{|\,G\,|}{|\,H\,|}$.

Proof:

Recall that two left cosets of H in G are either equal or disjoint. That is, the left cosets of H, being equivalence classes, form a partition of G. Note that $|\,aH\,| = |\,H\,|$. Thus all cosets have the same number of elements as H. Thus, $G = a_1H \cup a_2H \cup \cdots \cup a_rH$, where $r = \dfrac{|\,G\,|}{|\,H\,|}$ as $\{a_1H, \ldots, a_rH\}$ is a partitioning of G. Therefore,

$$\begin{aligned} |\,G\,| &= |\,a_1H\,| + |\,a_2H\,| + \cdots + |\,a_rH\,| \\ &= |\,H\,| + |\,H\,| + \cdots + |\,H\,| \\ &= r\,|\,H\,|. \end{aligned}$$

Hence$|\,H\,|$ divides $|\,G\,|$.

Theorem 4.17.2

If G is a finite group and $a \in G$, then $o(a)$ divides $|\,G\,|$.

Proof:

Clearly, $o(a) = |\,\langle\, a\,\rangle\,|$ where $\langle\, a\,\rangle \leq G$. Thus, by Lagrange's Theorem, $o(a)$ divides $|\,G\,|$.

Theorem 4.17.3

If G is a finite group and $a \in G$, then $a^{|\,G\,|} = e$.

Proof:

Clearly, $o(a) \mid |G|$, then $|G| = k \cdot o(a)$ for some $k \in \mathbb{Z}$. Therefore, $a^{|G|} = a^{k \cdot o(a)} = (a^{o(a)})^k = e^k = e$.

Theorem 4.17.4: Euler's Theorem

If n is a positive integer and a and n are relatively prime, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof:

Note that the group $\mathbb{U}_n$ has order $\phi(n)$. Thus, $[a]^{\phi(n)} = [1]$ in $\mathbb{U}_n$. But $[a]^{\phi(n)} = [a^{\phi(n)}]$, which implies that $a^{\phi(n)} \equiv 1 \pmod{n}$.

Theorem 4.17.5: Fermat's Little Theorem

Assume that p is a prime. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. For all a, $a^p \equiv a \pmod{p}$.

Proof:

If p-prime and $p \nmid a$, then $\phi(p) = p - 1$ and $\mathrm{GCD}(a, p) = 1$. By Euler's Theorem, we have $a^{p-1} \equiv 1 \pmod{p}$. Multiplying a in both sides we get $a^p \equiv a \pmod{p}$. Note that if $p \mid a$, then $a^p \equiv 0 \pmod{p}$ and $a \equiv 0 \pmod{p}$.

Theorem 4.17.6

A group G of a prime order contains no subgroups other than $\{e\}$ and G.

Proof:

Let $H \leq G$, then by Lagrange's Theorem $|H|$ divides $|G| = p$, and p is a prime. Then, $|H| = 1$ or $|H| = |G|$. That is $H = \{e\}$ or $H = G$.

Theorem 4.17.7

Every group of prime order is cyclic, generated by one of its non-identity elements.

Proof:

If $a \in G \neq \{e\}$ (since it has a prime order) and $a \neq e$ then $\langle a \rangle \neq \{e\}$. Thus $\langle a \rangle = G$ (by the previous Theorem).

Example 4.17.1

Show that any non-abelian group has at least six elements. That is, any group of order less than 6 is an abelian group.

Solution:

We show the statement by showing that all groups of order at most 5 are abelian.

- order 1: Then $G = \{e\}$ which is abelian.
- prime order: If the order is 2, 3, or 5, then the order is a prime and hence G is abelian.
- order 4: Then $|\,G\,| = 4$ and hence (by Lagrange's Theorem) if $a \neq e \in G$ then $o(a) = 1, 2,$ or 4. Case 1: If $o(a) = 4$ then G is cyclic since $G = \langle\, a \,\rangle$. Case 2: Note that $o(a) \neq 1$ since $a \neq e$. Case 3: If $o(a) = 2$, then $a^2 = e$ which means that $a = a^{-1}$ and hence $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Thus G is abelian.

Example 4.17.2

Suppose that G is a non-abelian group of order 14. Show that G has an element of order 7.

Solution:

Let $a \neq e$ in G. Then by Lagrange's Theorem $o(a) = 7$ or 2 (this is because $a \neq e$ so $o(a) \neq 1$ and $o(a) \neq 14$ since G is not cyclic as it is not abelian). If all $a \in G$ is of order 2, then G is abelian which is not the case. Therefore, there is $a \neq e$ in G with $o(a) = 7$.

Theorem 4.17.8: Fundamental Theorem of Finite Cyclic Groups

Let G be a cyclic group of a finite order n with $G = \langle\, a \,\rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. Then

1. Every subgroup of G is cyclic.
2. If $1 \leq k < n$, then a^k generates a subgroup of order $\frac{n}{gcd(k,n)}$.
3. If $1 \leq k < n$, then a^k is a generator of G if and only if $gcd(k, n) = 1$. [How many generators we have].
4. For each positive divisor d of n, G has exactly one subgroup of order d.

Example 4.17.3

Consider $\mathbb{Z}_{24}$. Find the orders of $\langle 3 \rangle, \langle 4 \rangle$, $\langle 5 \rangle$, and $\langle 9 \rangle$.

Solution:

- $|\langle 3 \rangle| = \frac{24}{gcd(3,24)} = \frac{24}{3} = 8$.
- $|\langle 4 \rangle| = \frac{24}{gcd(4,24)} = \frac{24}{4} = 6$.
- $|\langle 5 \rangle| = \frac{24}{gcd(5,24)} = \frac{24}{1} = 24$.
- $|\langle 9 \rangle| = \frac{24}{gcd(9,24)} = \frac{24}{3} = 8$.

Example 4.17.4

If G is a cyclic group of order 10, find the generators of G and find the orders of all subgroups of G.

Solution:

Assume that a is a generator for G. That is, $G = \langle a \rangle$. If $1 \leq k < 10$ is the order of a generator, then it must satisfies $gcd(k, 10) = 1$. That is, a^1, a^3, a^7, and a^9 are the generators of G. The order of any subgroup of G must divides the order of G which is 10. Therefore, the orders of all subgroups are $1, 2, 5$, and 10.

Example 4.17.5

List all subgroups of $\mathbb{Z}_{12}$.

Solution:

$\mathbb{Z}_{12}$ is a cyclic group and hence it has exactly one cyclic subgroup of order $k > 0$ where $k \mid 12$. That is $k = 1, 2, 3, 4, 6,$ or 12.

4.17.1 Solving Book Problems from Section 17

Exercise 4.17.1

Q.17.1: Find $\left[S_3 : \langle (1\ \ 2) \rangle\right]$.

Solution:

Clearly, $\langle (1\ \ 2) \rangle = \{e, (1\ \ 2)\}$. Thus $|\langle (1\ \ 2) \rangle| = 2$. Therefore, $\left[S_3 : \langle (1\ \ 2) \rangle\right] = \frac{|S_3|}{|\langle (1\ \ 2) \rangle|} = \frac{6}{2} = 3$.

Exercise 4.17.2

Q.17.3: Find the index of $\langle [2] \rangle$ in $\mathbb{Z}_{10}$, i.e. $\left[\mathbb{Z}_{10} : \langle 2 \rangle\right]$.

Solution:

Clearly $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$ and hence $|\langle 2 \rangle| = 5$. Thus, $\left[\mathbb{Z}_{10} : \langle 2 \rangle\right] = \frac{|\mathbb{Z}_{10}|}{|\langle 2 \rangle|} = \frac{10}{5} = 2$.

Exercise 4.17.3

Q.17.24: Prove that if G is a group of order p^2 (p-prime) and G is not cyclic, then $a^p = e$ for each $a \in G$.

Solution:

Let $a \in G$, then by Lagrange's Theorem $o(a) = 1$, $o(a) = p$, or $o(a) = p^2$. Clearly $o(a) \neq p^2$ because G is not cyclic. Thus $o(a) = 1$ or $o(a) = p$ and hence $a^p = e$ for any $a \in G$.

Exercise 4.17.4

Q.17.18: Assume that G is a cyclic group of order n, that $G = \langle a \rangle$, that $k \mid n$, and that $H = \langle a^k \rangle$. Find $\left[G : H\right]$.

Solution:

Note that $(a^k)^{\frac{n}{gcd(k,n)}} = a^n = e$. Then, since $|G| = n$, we have

$$|H| = \left|\langle a^k \rangle\right| = \frac{n}{gcd(k, n)}.$$

Thus $\left[G : H\right] = \frac{|\,G\,|}{|\,H\,|} = \frac{n}{\frac{n}{gcd(k,n)}} = gcd(k,n) = k.$

Exercise 4.17.5

Q.17.30: If H is a subgroup of a group G and $\left[G : H\right] = 2$, then the right cosets of H in G are the same as the left cosets of H in G. Why?

Solution:

Since $\left[G : H\right] = 2$, the left cosets of H in G are: H and aH for $a \in G$. Also, the right cosets of H in G are: H and Ha for $a \in G$.
Hence $G = H \cup aH = H \cup Ha$ which implies that $aH = G - H$ and that $Ha = G - H$. Therefore, $aH = Ha$.

Exercise 4.17.6

Q.17.32: Prove that if H is a subgroup of a finite group G, then the number of right cosets of H in G equals the number of left cosets of H in G.

Solution:

The number of right cosets of H in G is $\left[G : H\right]$ which is equal to the number of left cosets of H in G and both are equal to $\frac{|\,G\,|}{|\,H\,|}$.

Exercise 4.17.7

Use Fermat's Little Theorem to find the least non-negative integer x so that:

1. $3^{50} \equiv x \pmod 7$. **Solution**: $3^{50} = (3^6)^8 \cdot 3^2 \equiv 1^8 \cdot 9 \equiv 9(mod\ 7) \equiv 2(mod\ 7)$. Therefore, $x = 2$. $\square$
2. $3^{52} \equiv x \pmod{11}$. **Solution**: $3^{52} = (3^{10})^5 \cdot 3^2 \equiv 1^5 \cdot 9 \equiv 9(mod\ 11)$. Therefore, $x = 9$. $\square$
3. $3^{123} \equiv x \pmod{11}$. **Solution**: $3^{123} = (3^{10})^{12} \cdot 3^3 \equiv 1^{12} \cdot 27 \equiv 27(mod\ 11) \equiv 5(mod\ 11)$. Therefore, $x = 5$. $\square$

Exercise 4.17.8

Solve the following exercises from the book at pages 92 - 93:

- 17.1 – 17.4,
- 17.7 – 17.8,
- 17.13,
- 17.17 – 17.18,
- 17.24,
- 17.30,
- 17.32.

Section 4.18: Isomorphism

Example 4.18.1

Discuss the similarities between the groups $\langle\,(1\ \ 2\ \ 3)\,\rangle$ and $\mathbb{Z}_3$.

Solution:

Note that $\langle\,(1\ \ 2\ \ 3)\,\rangle = \{e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$ under the composition operation, and $\mathbb{Z}_3 = \{[0], [1], [2]\}$ under the addition operation. These two groups are alike given the corresponding

$$e \Leftrightarrow [0], \quad (1\ \ 2\ \ 3) \Leftrightarrow [1], \quad \text{and } (1\ \ 3\ \ 2) \Leftrightarrow [2].$$

$\circ$	e	$(1\ 2\ 3)$	$(1\ 3\ 2)$
e	e	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	e
$(1\ 3\ 2)$	$(1\ 3\ 2)$	e	$(1\ 2\ 3)$

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Definition 4.18.1

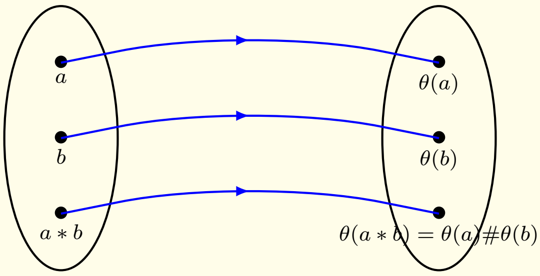
Let G be a group with operation $*$ and let H be a group with operation $\#$. An isomorphism of G onto H is a mapping $\theta : G \to H$ that is one-to-one and onto and satisfies

$$\theta(a * b) = \theta(a) \,\#\, \theta(b) \qquad \text{for all } a, b \in G.$$

If there is such a mapping then we say that G and H are isomorphic and we write $G \approx H$. Moreover, θ is called an isomorhism.

Remark 4.18.1

The condition $\theta(a * b) = \theta(a)\#\theta(b)$ is sometimes described by saying that θ preserves the operation. That is, it makes no difference whether we operate in G first and then apply θ, or apply θ first and then operate in H. In either way, we get the same result.



Example 4.18.2

Show that $\langle (1\ \ 2\ \ 3) \rangle \approx \mathbb{Z}_3$.

Solution:

Consider the mapping $\theta : \langle (1\ \ 2\ \ 3) \rangle \to \mathbb{Z}_3$ defined by $\theta(e) = [0]$; $\theta((1\ \ 2\ \ 3)) = [1]$; and $\theta((1\ \ 3\ \ 2)) = [2]$. Then clearly, θ is a bijection. Moreover, for any $a, b \in \langle (1\ \ 2\ \ 3) \rangle$, we have $\theta(a \circ b) = \theta(a) \oplus \theta(b)$, for instance

$$\theta((1\ \ 2\ \ 3)(1\ \ 3\ \ 2)) = \theta(e) = [0] = [1] \oplus [2] = \theta((1\ \ 2\ \ 3)) \oplus \theta((1\ \ 3\ \ 2)).$$

There are 9 $(3 \cdot 3)$ equations to be checked. Can you do it?

Example 4.18.3

Show that $\mathbb{Z} \approx 3\mathbb{Z}$.

Solution:

Let $\theta : \mathbb{Z} \to 3\mathbb{Z}$ given by $\theta(a) = 3a$ for all $a \in \mathbb{Z}$. This mapping is clearly one-to-one and onto $3\mathbb{Z}$. Moreover, it preserves addition:

$$\theta(a + b) = 3(a + b) = 3a + ab = \theta(a) + \theta(b).$$

Therefore, θ is an isomorphism and $\mathbb{Z} \approx 3\mathbb{Z}$.

Example 4.18.4

Show that $\mathbb{Z}$ is isomorphic to the multiplicative group of all rational numbers of the form 2^m for $m \in \mathbb{Z}$.

Solution:

Let $\alpha : \mathbb{Z} \to H$, where $H = \{2^m : m \in \mathbb{Z}\}$. **Onto:** Let $x \in H$, then $x = 2^n$ for some $n \in \mathbb{Z}$. That is $\alpha(n) = 2^n = x$ Thus α is onto H. **One-to-one:** Let $\alpha(a) = \alpha(b)$ for some $a, b \in \mathbb{Z}$. Then $2^a = 2^b$ and hence $a = b$. Thus α is 1-1. Finally, note that for any $a, b \in \mathbb{Z}$ we have

$$\alpha(a + b) = 2^{a+b} = 2^a \cdot 2^b = \alpha(a) \cdot \alpha(b).$$

Therefore, α is an isomorphism and $\mathbb{Z} \approx H$.

Theorem 4.18.1

If G and H are isomorphic groups and G is abelian, then H is abelian.

Proof:

Let $*$ and $\#$ be the operations of G and H, respectively, and let $\theta : G \to H$ be an isomorphism. If $x, y \in H$, there are elements $a, b \in G$ such that $\theta(a) = x$ and $\theta(b) = y$. Since θ preserves the operation (meaning that $\theta(a * b) = \theta(a) \# \theta(b)$) and G is abelian,

$$x \# y = \theta(a) \# \theta(b) = \theta(a * b) = \theta(b * a) = \theta(b) \# \theta(a) = y \# x.$$

That is H is abelian.

Theorem 4.18.2

If G and H are isomorphic groups and G is cyclic, then H is cyclic.

Proof:

Exercise: Try to show that if $G = \langle a \rangle$, then $H = \langle \theta(a) \rangle$ for an isomorphism θ.

Theorem 4.18.3

Let G and H be groups with operations $*$ and $\#$, respectively, and let $\theta : G \to H$ be a mapping such that $\theta(a * b) = \theta(a) \# \theta(b)$ for all $a, b \in G$. Then,

1. $\theta(e_G) = e_H$,
2. $\theta(a^{-1}) = \theta(a)^{-1}$ for each $a \in G$,
3. $\theta(a^k) = \theta(a)^k$ for each $a \in G$ and each $k \in \mathbb{Z}$,

4. $\theta(G) = \{\theta(g) : g \in G\}$, the image of θ, is a subgroup of H, and

5. if θ is one-to-one, then $G \approx \theta(G)$.

Proof:

1. Clearly, $\theta(e_G)\theta(e_G) = \theta(e_G e_G) = \theta(e_G) \in H$. Thus $\theta(e_G) = \theta(e_G)e_H$ and then $\theta(e_G)\theta(e_G) = \theta(e_G)e_H$. By left cancelation law, $\theta(e_G) = e_H$.

2. $e_H = \theta(e_G) = \theta(aa^{-1}) = \theta(a)\theta(a^{-1})$ for each $a \in G$. Thus, $\theta(a^{-1}) = (\theta(a))^{-1}$.

3. Consider three cases of $k \in \mathbb{Z}$: **Case 1:** $k = 0$, then $\theta(e_G) = e_H$. **Case 2:** $k > 0$: Using induction if $k = 1$, then $\theta(a^1) = \theta(a)^1$ which is true. Assume that $\theta(a^k) = \theta(a)^k$ for some k. Then $\theta(a^{k+1}) = \theta(a^k \cdot a) = \theta(a^k) \cdot \theta(a) = \theta(a)^k \cdot \theta(a) = \theta(a)^{k+1}$. **Case 3:** $k < 0$: Use same idea as in case 2, but for the negative integers.

4. We show that $\theta(G) \leq H$ by showing the following three conditions:

   $\mathcal{S}_1$: (Closure of $\theta(G)$) Let $\theta(g_1), \theta(g_2) \in \theta(G)$ for any $g_1, g_2 \in G$. Then

   $$\theta(g_1)\theta(g_2) = \theta(g_1 g_2) \in \theta(G) \text{ since } g_1 g_2 \in G.$$

   $\mathcal{S}_2$: (identity) $\theta(e_G) = e_H$ by part 1.

   $\mathcal{S}_3$: (inverse of $\theta(g)$) Let $\theta(g) \in \theta(G)$ for $g \in G$, then $g^{-1} \in G$ and hence $\theta(g^{-1}) = \theta(g)^{-1} \in \theta(G)$.

5. $\theta(G)$ is 1-1 is given. Note that $\theta(ab) = \theta(a)\theta(b)$ by the assumption. Also, considering θ as a mapping from G to $\theta(G)$ shows that θ is onto. Therefore, $\theta : G \to \theta(G)$ is an isomorphism.

Definition 4.18.2

Let G and H be groups with operations $*$ and $\#$, respectively. Then $\theta : G \to H$ is a homomorphism if

$$\theta(a * b) = \theta(a) \,\#\, \theta(b) \qquad \text{for all } a, b \in G.$$

Example 4.18.5

Let $\theta : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ defined by $\theta(x) = e^x$. Show that θ is an isomorphism.

Solution:

$1-1$: Let $x, y \in \mathbb{R}$ with $\theta(x) = \theta(y)$, then $e^x = e^y$ and hence $e^{x-y} = 1$ which implies $x - y = 0$ and hence $x = y$.

onto: Let $y \in \mathbb{R}^+$, then $y = e^x$ for some $x \in \mathbb{R}$. Then $\ln(y) = x$ and hence $\theta(\ln(y)) = e^{\ln(y)} = y$.

hom.: Let $x, y \in \mathbb{R}$, then $\theta(x + y) = e^{x+y} = e^x e^y = \theta(x)\theta(y)$. Therefore θ is homomorphism.

Therefore θ is an isomorphism, and $(\mathbb{R}, +) \approx (\mathbb{R}^+, \cdot)$.

Exercise 4.18.1

Solve the following exercises from the book at pages 96 - 97:

- 18.1 – 18.6,
- 18.9 – 18.12.

Section 4.19: More On Isomorphism

Theorem 4.19.1

Isomorphism, denoted by $\approx$, is an equivalence relation on the class of all groups.

Proof:

We simply show that $\approx$ is reflexive, symmetric, and transitive as follows.

1. Reflexive: If G is a group, then the identity mapping $I : G \to G$ is an isomorphism and thus $G \approx G$.

2. Symmetric: Assume that $G \approx H$. Then there is an isomorphism $f : G \to H$ which is a bijection. But then f^{-1} is a bijection as well. So, we need to show that f^{-1} is a homomorphism mapping. That is, $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$ for any $a, b \in H$. Let $f^{-1}(a) = x$ and $f^{-1}(b) = y$, then $a = f(x)$ and $b = f(y)$ and hence $ab = f(x)f(y) = f(xy)$. That is $f^{-1}(ab) = xy = f^{-1}(a)f^{-1}(b)$. Therefore, $H \approx G$.

3. Transitive: Let $G \approx H$ and $H \approx K$ with $f : G \to H$ and $g : H \to K$ are two isomorphisms. That is f and g are both bijection and hence $g \circ f : G \to K$ is a bijection as well. Also, for any $a, b \in G$, we have

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)\,(g \circ f)(b).$$

That is $G \approx K$.

Therefore, $\approx$ is an equivalence relation on the class of all groups.

Theorem 4.19.2

If p is a prime and G is a group of order p, then G is isomorphic to $\mathbb{Z}_p$.

Proof:

Let a be a nonidentity element of G. Then $\langle\, a \,\rangle \neq \{e\}$ is a subgroup of G. By Lagrange's Theorem, $\langle\, a \,\rangle = G$ and hence $G = \{e, a, a^2, \ldots, a^{p-1}\}$. Define $\theta : G \to \mathbb{Z}_p$ by $\theta(a^k) = [k]$. We next show that θ is an isomorphism.

1. θ is one-to-one: Let $\theta(a^{k_1}) = \theta(a^{k_2})$, then

$$[k_1] = [k_2] \text{ iff } k_1 \equiv k_2 \pmod{p} \text{ iff } p \mid (k_1 - k_2) \text{ iff } a^{k_1 - k_2} = e \text{ iff } a^{k_1} = a^{k_2}.$$

2. θ is onto: Let $[k] \in \mathbb{Z}_p$, then by the Division Algorithm $k = p \cdot q + r$; $0 \leq r < p$. Thus $a^k = (a^p)^q a^r = a^r \in G$. Then $\theta(a^k) = \theta(a^r) = [r] = [k] \in \mathbb{Z}_p$.

3. Let $a^m, a^n \in G$, then

$$\theta(a^m\, a^n) = \theta(a^{m+n}) = [m+n] = [m] \oplus [n] = \theta(a^m) \oplus \theta(a^n).$$

Therefore, θ is an isomorphism and hence $G \approx \mathbb{Z}_p$.

Theorem 4.19.3

Every cyclic group of order n is isomorphic to $\mathbb{Z}_n$.

Proof:

Assume that G is a cyclic group of order n. Let $G = \langle\, a \,\rangle = \{e, a, a^2, \cdots, a^{n-1}\}$. Define $\theta : G \to \mathbb{Z}_n$ by $\theta(a^k) = [k]$. Clearly, θ is a bijection. Furthermore,

$$\theta(a^k\ a^h) = \theta(a^{k+h}) = [k+h] = [k] \oplus [h] = \theta(a^k) \oplus \theta(a^h).$$

Therefore, ta is homomorphism and hence $G \approx \mathbb{Z}_n$.

Theorem 4.19.4

Every cyclic group of infinite order is isomorphic to $\mathbb{Z}$.

Proof:

Assume that G is a cyclic group of infinite order. There is $a \in G$ with $G = \langle\, a \,\rangle$. Define $\theta : G \to \mathbb{Z}$ by $\theta(a^k) = k$. Clearly, θ is a bijection. Furthermore,

$$\theta(a^k\ a^h) = \theta(a^{k+h}) = k + h = \theta(a^k) \oplus \theta(a^h).$$

Therefore, θ is homomorphism and hence $G \approx \mathbb{Z}$.

Theorem 4.19.5: Fundamental Theorem of Finite Abelian Groups

If G is a finite abelian group, then G is the direct product of cyclic groups of prime power order.

Moreover, if $G \approx A_1 \times A_2 \times \cdots \times A_s$ and $G \approx B_1 \times B_2 \times \cdots \times B_t$, where each A_i and each B_j is cyclic of prime order, then $s = t$ and after suitable relabeling of subscripts, $|\,A_i\,| = |\,B_i\,|$ for $1 \leq i \leq s$.

Example 4.19.1

If p is a prime, then there are five isomorphism classes of abelian groups of order p^4. Give one group from each class.

Solution:

Clearly, $p^4 = p^3 \cdot p = p^2 \cdot p^2 = p^2 \cdot p \cdot p = p \cdot p \cdot p \cdot p$. Thus, we have

$$\mathbb{Z}_{p^4}; \mathbb{Z}_{p^3} \times \mathbb{Z}_p; \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}; \mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p; \text{ and } \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p.$$

Example 4.19.2

List the isomorphism class representatives of abelian groups of order 125.

Solution:

Clearly, $125 = 5^3 = 5^2 \cdot 5 = 5 \cdot 5 \cdot 5$. Thus, we have

$$\mathbb{Z}_{5^3}; \mathbb{Z}_{5^2} \times \mathbb{Z}_5; \text{ and } \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5.$$

Example 4.19.3

List the isomorphism class representatives of abelian groups of order 200.

Solution:

Clearly, $200 = 2^3 \cdot 5^2 = 2^3 \cdot 5 \cdot 5 = 2^2 \cdot 2 \cdot 5^2 = 2^2 \cdot 2 \cdot 5 \cdot 5 = 2 \cdot 2 \cdot 2 \cdot 5^2 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$. Thus, we have

$$\mathbb{Z}_{2^3} \times \mathbb{Z}_{5^2};\ \mathbb{Z}_{2^3} \times \mathbb{Z}_5 \times \mathbb{Z}_5;\ \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2};\ \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5;$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2};\ \text{and } \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5.$$

Exercise 4.19.1

Solve the following exercises from the book at pages 101:

- 19.15 – 19.18.

Chapter

5 Group Homomorphisms

Section 5.21: Homomorphism of Groups. Kernels

Remark 5.21.1

Every isomorphism is a homomorphism, but not (necessary) vice versa.

Definition 5.21.1

If $\theta : G \to H$ is a homomorphism, then the **kernel** of θ is the set of all elements $a \in G$ such that $\theta(a) = e_H$. That is

$$\ker\theta = \{a \in G \,:\, \theta(a) = e_H\}\,.$$

Example 5.21.1

Let $\theta : \mathbb{Z} \to \mathbb{Z}$ be defined by $\theta(a) = 2a$ for all $a \in \mathbb{Z}$. Discuss 1) homomorphismity of θ. 2) Is θ onto, 3) Is θ 1-1, and 4) Find $\ker\theta$.

Solution:

1. Clearly, $\theta(a+b) = 2(a+b) = 2a + 2b = \theta(a) + \theta(b)$ and hence θ is a homomorphism.
2. θ is not onto $\mathbb{Z}$ since there is no element $a \in \mathbb{Z}$ with $\theta(a) = 3$ for instance.
3. $\theta(a) = \theta(b)$ implies $2a = 2b$ and hence $a = b$. Thus, θ is 1-1.
4. $\ker\theta = \{a \in \mathbb{Z} \,:\, \theta(a) = 2a = 0\} = \{0\}$.

$\square$

Example 5.21.2

For any positive integer n, define $\theta : \mathbb{Z} \to \mathbb{Z}_n$ by $\theta(a) = [a]$ for each $a \in \mathbb{Z}$. Show that θ is a homomorphism, find $\ker\theta$, and is θ an isomorphism? Explain.

Solution:

Clearly for any $a, b \in \mathbb{Z}$ we have $\theta(a+b) = [a+b] = [a] \oplus [b] = \theta(a) \oplus \theta(b)$.

Thus, θ is a homomorphism. Also, $\ker\theta = \{a \in \mathbb{Z} : \theta(a) = [a] = [0]\} = \{k \cdot n : k \in \mathbb{Z}\}$.

Moreover, θ is not isomorphism since it is not one-to-one, for instance $\theta(0) = \theta(n) = [0]$.

Theorem 5.21.1

If $\theta : G \to H$ is a homomorphism and $A \leq G$, then $\theta(A) \leq H$ where $\theta(A) = \{\theta(a) : a \in A\}$, the image of A under θ.

Proof:

We prove the statement by showing the three conditions of a subgroup as follows:

$\mathcal{S}_1$: Closure: Let $\theta(a), \theta(b) \in \theta(A)$, then $\theta(a)\theta(b) = \theta(ab) \in \theta(A)$ since $ab \in A$.

$\mathcal{S}_2$: Identity: $\theta(e_G) = e_H \in \theta(A)$ since $e_G \in A$.

$\mathcal{S}_3$: Inverse: Let $\theta(a) \in \theta(A)$, then $\theta(a^{-1}) = \theta(a)^{-1} \in \theta(A)$ since $a^{-1} \in A$.

Therefore, $\theta(A) \leq H$.

Exercise 5.21.1

Q.21.10: If $\theta : G \to H$ is a homomorphism and $B \leq H$, then $\theta^{-1}(B) \leq G$, where $\theta^{-1}(B) = \{g \in G : \theta(g) \in B\}$, the inverse image of B under θ.

Solution:

$\mathcal{S}_1$: Closure: Let $g_1, g_2 \in \theta^{-1}(B)$, then $\theta(g_1), \theta(g_2) \in B$. Thus

$$\theta(g_1)\theta(g_2) = \theta(g_1 g_2) \in B \;\Rightarrow\; g_1 g_2 \in \theta^{-1}(B).$$

$\mathcal{S}_2$: Identity: Clearly $\theta(e_G) = e_H \in H$ and hence $e_G \in \theta^{-1}(B)$.

$\mathcal{S}_3$: Inverse: Let $g \in \theta^{-1}(B)$, then $\theta(g) \in B$. Therefore, $\theta(g)^{-1} = \theta(g^{-1}) \in B$. Hence $g^{-1} \in \theta^{-1}(B)$.

Therefore, $\theta^{-1}(B) \leq G$.

Theorem 5.21.2

If $\theta : G \to H$ is a homomorphism, then $\ker\theta \leq G$. Moreover, θ is 1-1 if and only if $\ker\theta = \{e_G\}$.

Proof:

We show the three conditions of a subgroup as follows:

$\mathcal{S}_1$: Closure: Let $a, b \in \ker\theta$, then $a, b \in G$ with $\theta(a) = \theta(b) = e_H$. Thus, $\theta(ab) = \theta(a)\,\theta(b) = e_H\, e_H = e_H$. Thus $ab \in \ker\theta$.

$\mathcal{S}_2$: Identity: Clearly $e_G \in \ker\theta$ since $\theta(e_G) = e_H$.

$\mathcal{S}_3$: Inverse: Let $a \in \ker\theta$ then $a, a^{-1} \in G$. Thus

$$\theta(a^{-1}) = \theta(a)^{-1} = e_H^{-1} = e_H \;\Rightarrow\; a^{-1} \in \ker\theta.$$

Therefore, $\ker\theta \leq G$. Next We show the if and only if statement:

„ $\Rightarrow$ ": Assume that θ is 1-1. Since $e_G \in \ker\theta \leq G$ and the identity is unique then $\ker\theta = \{e_G\}$.

„ $\Leftarrow$ ": Assume that $\ker\theta = \{e_G\}$. If $a, b \in G$ with $\theta(a) = \theta(b)$, then $\theta(a)\theta(b)^{-1} = e_H$ and hence $\theta(a)\theta(b^{-1}) = e_H$ and thus $\theta(ab^{-1}) = e_H$. Therefore, $ab^{-1} \in \ker\theta$ which implies that $ab^{-1} = e_G$. Hence $a = b$. Therefore θ is 1-1.

Example 5.21.3

Consider the homomorphism $\theta : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ defined by $\theta(x) = 8x$ for all $x \in \mathbb{Z}_{10}$. Find the $\ker\theta$.

Solution:

$\ker\theta = \{0, 5\}$ since $\theta(0) = \theta(5) = 40 = 0$ while for instance $\theta(3) = 24 = 4 \neq 0$ and hence $3 \notin \ker\theta$.

Definition 5.21.2

A subgroup N of a group G is called **normal subgroup** of G if $gng^{-1} \in N$ for all $n \in N$ and all $g \in G$. In that case, we write $N \lhd G$.

Example 5.21.4

Show that every subgroup of an abelian group is a normal subgroup.

Solution:

If N is a subgroup of an abelian group G, then for all $n \in N$ and for all $g \in G$,

$$gng^{-1} = gg^{-1}n = n \in N.$$

Thus $N \lhd G$.

Theorem 5.21.3

If G and H are groups and $\theta : G \to H$ is a homomorphism, then $\ker \theta \lhd G$.

Proof:

Recall that $\ker \theta \leq G$. Let $n \in \ker \theta$ and $g \in G$, then $\theta(n) = e_H$. So

$$\theta(gng^{-1}) = \theta(g)\theta(n)\theta(g^{-1}) = \theta(g)e_H\theta(g^{-1}) = \theta(g)\theta(g^{-1}) = e_H.$$

Thus $gng^{-1} \in \ker \theta$ and hence $\ker \theta \lhd G$.

Remark 5.21.2

Let H be a subgroup of a group G. Then H is normal subgroup of G iff for all $g \in G$

$$gH = Hg \iff gHg^{-1} = H \iff H = g^{-1}Hg.$$

Example 5.21.5

Let $H = \{e, (1\ \ 2)\} \leq S_3$. Is $H \lhd S_3$? Explain.

Solution:

Note that,

$$eH = \{e, (1\ \ 2)\} = He = \{e, (1\ \ 2)\}$$
$$(1\ \ 2)H = \{e, (1\ \ 2)\} = H(1\ \ 2) = \{e, (1\ \ 2)\}$$
$$(1\ \ 3)H = \{(1\ \ 3), (1\ \ 2\ \ 3)\} \neq H(1\ \ 3) = \{(1\ \ 3), (1\ \ 3\ \ 2)\}$$

Therefore, H is not a normal subgroup of S_3.

Exercise 5.21.2

Show that $H = \{e, (1 \;\; 2 \;\; 3), (1 \;\; 3 \;\; 2)\} \lhd S_3$. [Hint: Simply show that for all $g \in S_3$, we have $gH = Hg$].

Example 5.21.6

Show that $H = \{0, 3\} \lhd (\mathbb{Z}_6, +)$.

Solution:

One way to show the statement: H is a subgroup of $\mathbb{Z}_6$ which is an abelian group and hence H is normal subgroup.

Another way to show the statement: Show that H is a normal subgroup by showing that $g + H = H + g$ for all $g \in \mathbb{Z}_6$.

Exercise 5.21.3

Solve the following exercises from the book at pages 109 - 110:

- 21.2,
- 21.5 – 21.10,
- 21.34.

Section 5.22: Quotient Groups

Theorem 5.22.1

Let H be a subgroup of a group G. The left cosets of H in G with multiplication is well defined by $aH\,bH = ab\,H$ if and only if $aH = Ha$ for all $a, b \in G$.

Theorem 5.22.2

Let N be a normal subgroup of a group G, and let G/N denote the set of all left cosets of N in G. Then $G/N = \{gN : g \in G\}$ under the binary operation $(g_1N)(g_2N) = g_1g_2N$ is a group.

This group is called the **quotient group** (or factor group) of G by N. Moreover,

$$|\,G/N\,| = \frac{|\,G\,|}{|\,N\,|} := \big[G : H\big].$$

Proof:

We show that G/N is a group by showing the following three conditions:

$\mathcal{G}_1$: Associative: If $a, b, c \in G$, then

$$aN(bNcN) = aN(bcN) = (a(bc))N = ((ab)c)N = (ab)NcN = (aNbN)cN.$$

$\mathcal{G}_2$: Identity: Clearly, the identity element is $eN \in G/N$.

$\mathcal{G}_3$: Inverse: For any element $gN \in G/N$, the inverse is $g^{-1}N \in G/N$.

Example 5.22.1

Let $H = \langle\, 2\,\rangle$. Show that $H \lhd \mathbb{Z}_{12}$. Find the order of $\mathbb{Z}_{12}/H$. Is $\mathbb{Z}_{12}/H \approx \mathbb{Z}_2$? Explain.

Solution:

Note that $H = \{0, 2, 4, 6, 8, 10\}$.

- Since $\mathbb{Z}_{12}$ is abelian, then $H \lhd \mathbb{Z}_{12}$.
- Note that $\mathbb{Z}_{12}/H$ is a quotient group and hence $|\,\mathbb{Z}_{12}/H\,| = \frac{12}{6} = 2$.
- Clearly $\mathbb{Z}_{12}/H = \{a + H : a \in \mathbb{Z}_{12}\} = \{H, 1 + H\} \approx \mathbb{Z}_2$.

Example 5.22.2

Consider $N = \{e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\} \lhd S_3$. Find S_3/N.

Solution:

Clearly, $S_3/N = \{aN : a \in S_3\}$, but since $|\,S_3/N\,| = \frac{6}{3} = 2$, we conclude that

$$S_3/N = \{N, (1\ \ 2)N\}, \quad \text{where} \quad (1\ \ 2)N = \{(1\ \ 2), (1\ \ 3), (2\ \ 3)\}.$$

Theorem 5.22.3

If G is a group with a normal subgroup N, then the mapping $\theta : G \to G/N$ defined by $\theta(a) = aN$ for each $a \in G$ is a homomorphism of G onto G/N, and $\ker\theta = N$. It is called the natural homomorphism.

Proof:

Clearly the mapping θ is well defined and onto G/N. If $a, b \in G$, then

$$\theta(ab) = abN = aNbN = \theta(a)\theta(b).$$

Thus θ is a homomorphism. Finally, if $a \in G$, then

$$a \in \ker\theta \Leftrightarrow \theta(a) = aN = eN = N,$$

because eN is the identity element of G/N. Therefore, $a \in \ker\theta$ if and only if $aN = N$ and hence if and only if $a \in N$.

Theorem 5.22.4

Let G be a group with a normal subgroup N. Let G/N be a quotient group. Then,

1. If G is finite, then $|\,G/N\,| = \frac{|\,G\,|}{|\,N\,|}$.
2. If G is cyclic, then G/N is cyclic.
3. If G is abelian, then G/N is abelian.
4. If a has a finite order in G, then the order of aN in G/N divides the order of a.

Theorem 5.22.5

Every quotient group of a cyclic group is cyclic.

Proof:

Let G/N be a quotient group of a cyclic group G. Assume that $G = \langle a \rangle$ for some $a \in G$. If $g \in G$, then $g = a^n$ for some $n \in \mathbb{Z}$ since G is cyclic. Hence $gN = a^nN = (aN)^n$ for any element $gN \in G/N$. Thus, $G/N = \langle aN \rangle$ and so G/N is cyclic.

Theorem 5.22.6

If H and K are normal subgroups of a group G, then $H \cap K \lhd G$.

Proof:

For all $g \in G$ and for all $x \in H \cap K$, we have $x \in H$ and $x \in K$; hence $gxg^{-1} \in H$ and $gxg^{-1} \in K$ and hence $gxg^{-1} \in H \cap K$. Therefore, $H \cap K$ is normal.

Theorem 5.22.7

If H and K are normal subgroup of a group G and $H \cap K = \{e\}$, then $hk = kh$ for all $h \in H$ and $k \in K$.

Proof:

Let $g = hkh^{-1}k^{-1} \in G$. But K is normal and hence $hkh^{-1} \in K$ and $k^{-1} \in K$ and thus $g = hkh^{-1}k^{-1} \in K$. Also H is normal and hence $h^{-1} \in H$ which implies that $kh^{-1}k^{-1} \in H$ and hence $g = hkh^{-1}k^{-1} \in H$. Therefore, $g \in H \cap K = \{e\}$; hence $g = e$ and hence $hk = kh$ for all $h \in H$ and $k \in K$.

Example 5.22.3

Prove that if $N \lhd G$ and H is any subgroup of G, then $N \cap H \lhd H$.

Solution:

Note that $N \cap H \leq G$ and $N \cap H \subseteq H$ implies that $N \cap H \leq H$. Let $h \in H$ and $x \in N \cap H$. Then $x \in N$ and $x \in H$ and $h^{-1} \in H$ and hence $hxh^{-1} \in H$ since $H \leq G$. Also $hxh^{-1} \in N$ since $N \lhd G$. Therefore, $hxh^{-1} \in N \cap H$. That is $N \cap H \lhd H$.

Theorem 5.22.8: The Fundamental Homomorphism Theorem

Let G and H be groups and let $\theta : G \to H$ be a homomorphism from G onto H with $\ker\theta = K$. Then the mapping $\Phi : G/K \to H$ defined by $\Phi(aK) = \theta(a)$ for each $aK \in G/K$ is an isomorphism of G/K onto H. Therefore, $G/K \approx H$.

Proof:

Onto: Clearly Φ is onto H since θ is onto H. For any $h \in H$ there is $a \in G$ such that $\theta(a) = h = \Phi(aK)$ for $aK \in G/K$.

1-1: We show that Φ is 1-1 iff $\ker\Phi = \{eK\}$. Let $aK \in \ker\Phi$, then $\Phi(aK) = \theta(a) = e_H$ and hence $a \in \ker\theta = K$ iff $aK = K = eK$. Thus, $\ker\Phi = \{eK\}$ and hence Φ is 1-1.

homomorphism: For any $a, b \in G$, we have:

$$\Phi(aK\, bK) = \Phi(ab\, K) = \theta(ab) = \theta(a)\,\theta(b) = \Phi(aK)\,\Phi(bK).$$

Therefore, $G/K \approx H$.

Example 5.22.4

For integer $n \geq 2$, show that $\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}_n$; or similarly $\mathbb{Z}/\langle\, n\,\rangle \approx \mathbb{Z}_n$.

Solution:

Let $G = \mathbb{Z}$ and $H = \mathbb{Z}_n$ and $K = n\mathbb{Z} = \langle\, n\,\rangle$. Let $\theta : \mathbb{Z} \to \mathbb{Z}_n$ be defined by $\theta(a) = [a]$ which is onto homomorphism. Also, we know that $\ker\theta = \{x \in \mathbb{Z} : [x] = [0]\} = \{nk : k \in \mathbb{Z}\} = n\mathbb{Z} = \langle\, n\,\rangle = K$. Therefore, by the Fundamental Homomorphism Theorem, we get $G/K \approx H$.

Exercise 5.22.1

Solve the following exercises from the book at pages 114:

- 22.5 – 22.6.

The Index

Symbols

ϕ-function ... 60

A

abelian group ... 20
alternating group ... 36
associative ... 12
associative law ... 12

B

bijection ... 4
binary operation ... 10
 closed ... 10
 closure ... 10

C

Cartesian product ... 10
Cayley table ... 11
center ... 38
centralizaer ... 38
closed ... 10
closure ... 10
codomain ... 3
common
 divisor ... 56
commutative ... 12
commutative law ... 12
Composition ... 6
congruence ... 43, 47
congruence class ... 48
congruent ... 47
coset ... 79
 left ... 79
 right ... 79
cycle ... 29
 disjoint ... 29
cyclic ... 67
cyclic decomposition ... 29
cyclic group ... 88
cyclic subgroup ... 68

D

direct product ... 75
direct product group ... 75
disjoint cycle ... 29
divides ... 47
divisibility ... 43
divisible ... 47
division algorithm ... 47, 50
domain ... 3

E

equivalence ... 43
 class ... 44
 relation ... 43
equivalence class ... 44
equivalence relation ... 43
Euclidean algorithm ... 56
Euler ϕ-function ... 60
Euler phi-function ... 60

F

factor group 111

factorization 60

function 3

  one-to-one 3

  onto 3

G

generator 68

  order 69

greatest common divisor 56

group 19, 65

  abelian 20

  alternating group 36

  cyclic 67, 88

  direct product 75

  factor 111

  generator 68

  homomorphism 105

  infinite 22

  isomorphism 95

  kernel 105

  non-abelian 20

  normal 107

  order 22

    infinite 22

  quotient 111

  subgroup 32

  symmetric 27

H

homomorphism 105

  natural 112

I

identity 13

image 3

improper subgroup 33

index 88

inverse 13

isomorphism 95

K

k-cycle 29

kernel 105

L

Lagrange's Theorem 88

least integer principle 49

left coset 79

M

mapping 3

  bijection 4

  identity 7

  inverse 8

  invertible 6, 8

modulo 53

N

natural homomorphism 112

non-abelian group 20

normal 107

O

operation

  associative 12

  binary 10

    associative 12

    commutative 12

- commutative 12
order 22, 69

P

partition 44
permutation 27
- cycle 29
- cyclic 29
- cyclic decomposition 29
- even 35
- k-cycle 29
- multiplication 27
- odd 35
- transposition 35

phi-function 60
preimage 3
product
- Cartesian 10, 75

proper subgroup 33

Q

quotient group 111

R

reflexive 43
relation 43
- equivalence 43
- reflexive 43
- symmetric 43
- transitive 43

right coset 79

S

subgroup 32
- center 38
- centralizer 38
- cyclic 68
- improper 33
- index 88
- normal 107
- proper 33
- trivial 33

symmetric 43
symmetric group 27
- identity 28
- inverse 28

T

table 11
- Cayley 11

transitive 43
transposition 35
trivial subgroup 33