Sets, Groups and Relations

Krzysztof Sikora

February 27, 2018



Copyright © 2006 - 2018 by Krzysztof Sikora.
This work is made available under the terms of the Creative Commons Attribution-ShareAlike 4.0 license, `http://creativecommons.org/licenses/by-sa/4.0/`.
If you decide to use some of my concepts, I would like you to email me (krzyssikora@gmail.com) so that I will be able to notify you about major changes and new versions of the textbook. I would be happy to share some more of my materials with you. You will not have to pay anything for that. All I expect from you is that you accept the conditions of a free licence that are explained below.

- **Creative Commons** is a nonprofit organization that enables the sharing and use of creativity and knowledge through free legal tools. For this work I decided to use by-nc-sa licence.
- **Attribution** - You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **ShareAlike** - If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

Contents

1 Sets **4**
1.1 Elementary notions, definitions and properties 4

2 Relations **7**
2.1 Ordered pairs. Cartesian product. 7
2.2 Relations. 8
2.2.1 Properties of relations 8
2.2.2 Equivalence relations 9

3 Functions **13**
3.1 Injections, surjections and bijections 13
3.1.1 Injection 13
3.1.2 Surjection 14
3.1.3 Bijection 14
3.2 Composition of functions 15
3.3 Inverse function 16

4 Operations **21**
4.1 Binary operations 21
4.2 Operation tables 22
4.3 The identity and inverses 23
4.3.1 The identity element e 23
4.3.2 The inverse a^{-1} of an element a 24

5 Groups **27**
5.1 Axioms of a group 27
5.2 Groups of permutations 36
5.3 Order of an element, order of a group 39
5.4 Cyclic groups 41
5.5 Subgroups 43
5.5.1 Subgroup tests 44
5.6 Cosets 45
5.7 Lagrange's theorem 51

6 Homomorphism of groups **55**
6.1 Homomorphism 55
6.2 Isomorphism 58

Chapter 1

Sets

1.1 Elementary notions, definitions and properties

In axiomatic set theory a concept of a **set** is an example of a *primitive notion*, i.e. it is undefined. The *unique* set that contains no elements is called the **empty set** (*null set*), which is a *primitive notion*, too. In other words, existence of the empty set is an *axiom*.

DEFINITION 1.1 (subset)
A is a ***subset*** *of B* if and only if *every element of A is an element of B, i.e.*

$$A \text{ is a } \textbf{subset} \text{ of } B \quad \Leftrightarrow \quad ((x \in A) \Rightarrow (x \in B))$$

Additionally,
A is a ***proper subset*** *of B* if and only if *A is a subset of B but* $A \neq B$.

NOTATION.

$\emptyset$	*the empty set*
$n(A)$	*cardinality of set A (number of elements of set A)*
$A \subseteq B$	*A is a subset of B*
$A \subset B$	*A is a* ***proper subset*** *of B, i.e.* $(A \subseteq B) \vee (A \neq B)$
U	*a universal set (set of all elements considered)*

PROPERTIES.
For the empty set $\emptyset$ *and any set A:*

1. $n(\emptyset) = 0$

2. $\emptyset \subseteq A$

3. $A \neq \emptyset \Rightarrow A \not\subseteq \emptyset$

DEFINITION 1.2 (operations on sets)
Given the sets A and B the following operations are defined:

- $A \cup B$ - ***union*** *of A and B*
  $A \cup B = \{x | (x \in A) \vee (x \in B)\}$, *where "$\vee$" means "or"*
- $A \cap B$ - ***intersection*** *of A and B*
  $A \cap B = \{x | (x \in A) \wedge (x \in B)\}$, *where "$\wedge$" means "and"*
- $A \setminus B$ - ***difference*** *of A and B* *sometimes denoted as "$A - B$"*
  $A \setminus B = \{x | (x \in A) \wedge (x \notin B)\}$, *where "$x \notin B$" means "$\neg(x \in B)$"*

- A' - ***complement*** *of* A

  $A' = \boldsymbol{U} \setminus A,$ *where* $\boldsymbol{U}$ *is a universal set*

- $A \triangle B$ - ***symmetric difference*** *of* A *and* B

  $A \triangle B = (A \setminus B) \cup (B \setminus A)$ *or*

  $A \triangle B = \{x | ((x \in A) \wedge (x \notin B)) \vee ((x \in B) \wedge (x \notin A))\}$

PROPERTIES.

de Morgan's laws

- $(A \cup B)' = A' \cap B'$
- $(A \cap B)' = A' \cup B'$

distributive laws

- *the union of sets is distributive over intersection*

  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

- *the intersection of sets is distributive over union*

  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

- *the intersection of sets is distributive over the symmetric difference*

  $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$

associative laws

- *for union*

  $A \cup (B \cup C) = (A \cup B) \cup C$

- *for intersection*

  $A \cap (B \cap C) = (A \cap B) \cap C$

commutative laws

- *for union*

  $A \cup B = B \cup A$

- *for intersection*

  $A \cap B = B \cap A$

empty and universal sets

For any subset A *of a universal set* U*:*

- $U \cup A = U$
- $U \cap A = A$
- $\emptyset \cup A = A$
- $\emptyset \cap A = \emptyset$

other properties

$A \setminus B = A \cap B'$

Questions

In all questions, if you are to prove a statement you have to use set algebra and / or logic laws. Illustrations on Venn diagrams are not considered proofs.
If you want to show that a statement is false it is sufficient to show a counter-example.

Q1. List all subsets of set $\{1, 2, 3\}$.

Q2. How many k-element subsets does an n-element set have? $(k \in \{0, 1, 2, \ldots, n\})$
How many subsets does an n-element set have?

Q3. Let $S = \{0, 1, \ldots, 10, 11\}$. Let $S_n = \{x \in S |\ n \text{ divides } x\}$ for $n = 2, 3, 4, 6$. Find:

(i) $S_2 \cap S_3$
(ii) $S_4 \cap S_6$
(iii) $S_3 \cap S_6$
(iv) $(S_3 \cup S_2)'$
(v) $S_3 \cap S_2'$

Q4. Let $U = \{0, 1, 2, 3, 4, 5, 6\}$ and A and B be subsets of U. Let A contain all multiples of 2 and let B contain all multiples of 3. Let $P(X)$ denote a set of all subsets of a set X. Find:

(i) $n(P(A))$
(ii) $n(P(B))$
(iii) $P(A) \cap P(B)$
(iv) $n(P(A) \cup P(B))$

Q5. Is difference of sets associative?

Q6. Is union of sets distributive over difference?

Q7. Is intersection of sets distributive over difference?

Q8. Is difference of sets distributive over intersection?

Q9. Is difference of sets distributive over union?

Q10. Prove that for sets A and B: $A \triangle B = (A \cup B) \setminus (A \cap B)$.

Q11. Prove that for sets A and B: $(A \cup B)' \cap (A' \cup B')' = \emptyset$.

Q12. Prove that for sets A and B: $((A \cup B) \cap (A' \cup B'))' = (A \cap B) \cup (A \cup B)'$.

Q13. Prove that for sets A, B and C: $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Q14. Which of the following statements are equivalent for sets A and B?

(1) $A = B$
(2) $A \cup B = A \cap B$
(3) $A \setminus B = B \setminus A$
(4) $A \triangle B = \emptyset$

Chapter 2

Relations

2.1 Ordered pairs. Cartesian product.

DEFINITION 2.1 (ordered pair)
*An **ordered pair** is a collection of two objects such that one can be distinguished as the first element and the other as the second element.*[1]

NOTATION.
(a, b) *an ordered pair with first element a and second element b*

PROPERTIES.
- $(a, b) \neq (b, a)$
- $(a, b) = (c, d) \Rightarrow ((a = c) \wedge (b = d))$

EXAMPLE 2.2 (ordered pairs)
A point on a cartesian plane can be understood as an ordered pair of two real numbers.
A horizontal line in a cartesian plane defined by $y = 2$ can be understood as a set $\{(x, 2)|x \in \mathbb{R}\}$.

DEFINITION 2.3 (Cartesian product)
*The **Cartesian product** of two sets (A and B) is a set of pairs such that first element of each pair is an element of the first set (A) and second element of each pair is an element of the second set (B), i.e.*

$$\{(a, b)|a \in A, b \in B\}$$

NOTATION.
$A \times B \quad = \{(a, b)|a \in A, b \in B\}$
$A^2 \quad = A \times A$
and similarly
$A^3 \quad = A \times A^2 = A^2 \times A = A \times A \times A$ [2]
$A^n \quad = A \times A^{n-1} = A^{n-1} \times A$ *for* $n > 1$

EXAMPLE 2.4 (Cartesian product)
Let set X be a 13-element set:

$$X = \{A, K, Q, J, 10, 9, 8, 7, 6, 5, 4, 3, 2\}$$

and set Y be a 4-element set:

$$Y = \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\}.$$

[1] (non-obligatory) More formally, an ordered pair (a, b) may be defined as a set $\{a, \{a, b\}\}$.
[2] Operation $\times$ defined on sets is therefore assumed to be associative. Can that be assumed?

then the Cartesian product $X \times Y$ of those two sets is the 52-element set:

$$X \times Y = \{(A, \spadesuit), (K, \spadesuit), (Q, \spadesuit), \cdots, (2, \spadesuit), (A, \heartsuit), (K, \heartsuit), \cdots, (2, \clubsuit)\}.$$

EXAMPLE 2.5 ($\mathbb{R}^2$ and $\mathbb{R}^3$)
Cartesian plane is the Cartesian product $\mathbb{R} \times \mathbb{R}$ (or $\mathbb{R}^2$), where $\mathbb{R}$ is the set of real numbers. Three-dimensional cartesian space is the Cartesian product $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ (or $\mathbb{R}^3$).

2.2 Relations.

DEFINITION 2.6 (binary relation)
*We will define a **binary relation** R on elements of set S in two ways.*

1. *Formally, a **binary relation** R on elements of set S is a subset of the cartesian product $S \times S$. We will say that elements $s_1, s_2 \in S$ are in the relation R whenever $(s_1, s_2) \in R$.*[3]
2. *Informally, a **binary relation** R on elements of set S is a statement of* truth *or* false *for each pair of elements of set S.*

NOTATION.
For $a, b \in S$ if

- *$(a, b) \in R$ (according to definition **1**)* *or*
- *it is* true *that a and b are in the relation R (according to definition **2**)*

we write it as aRb.

EXAMPLE 2.7 (relation "<")
*Let $S = \{1, 2, 3\}$. The table below defines relation "<" ("is smaller than") on S according to definition **2**.*

	1	2	3
1	F	T	T
2	F	F	T
3	F	F	F

	b
a	T

*means that it is **TRUE** that $a < b$, while*

	b
a	F

*means that it is **FALSE** that $a < b$.*

In other words it is TRUE that $1 < 2, 1 < 3$ and that $2 < 3$ and no other numbers from S are in the relation "<".
*Using definition **1** we would state that $<= \{(1, 2), (1, 3), (2, 3)\}$. Note, that in definition **1** "<" describes a subset of $S \times S$.*

2.2.1 Properties of relations

DEFINITION 2.8 (reflexivity)
*Relation R defined on set S is **reflexive** $\Leftrightarrow$ for every $a \in S$ aRa.*

DEFINITION 2.9 (symmetry)
*Relation R defined on set S is **symmetric** $\Leftrightarrow$ for every $a, b \in S$ $(aRb) \Rightarrow (bRa)$.*

[3] This definition is non-obligatory.

Definition 2.10 (transitivity)
Relation R defined on set S is ***transitive*** $\Leftrightarrow$ *for every $a, b, c \in S$ $((aRb)$ and $(bRc)) \Rightarrow (aRc)$.*

Example 2.11 (properties of "$\geq$")
Relation "$\geq$" defined on $\mathbb{R}$ is:

- ***reflexive****, as for any $x \in \mathbb{R}$, $x \geq x$,*
- ***NOT symmetric****, as $(5 \geq 2) \not\Rightarrow (2 \geq 5)$,*
- ***transitive****, as $((a \geq b) \wedge (b \geq c)) \Rightarrow (a \geq c)$.*

Example 2.12 (empty relation)
Let $\sim$ be an ***empty relation*** *defined on a non-empty set X, i.e. for every $a, b \in X$ it is not true that $a \sim b$.*
Then $\sim$ is ***NOT reflexive*** *($x \sim x$ is never true), but it is* ***symmetric*** *and* ***transitive****.*

Example 2.13 (total relation)
Let $\asymp$ be a ***total relation*** *defined on a non-empty set X, i.e. for every $a, b \in X$ it is true that $a \asymp b$.*
Then $\asymp$ is ***reflexive****,* ***symmetric*** *and* ***transitive****.*

Example 2.14 (properties of relations)
The relation "has a common factor greater than 1 with" between integers greater than 1, is:

- ***reflexive***
- ***symmetric***
- ***NOT transitive****, as:*
  - *2 and 6 have a common factor greater than 1,*
  - *6 and 3 have a common factor greater than 1,*
  - *2 and 3 do not have a common factor greater than 1.*

2.2.2 Equivalence relations

Definition 2.15 (equivalence relation)
An ***equivalence relation*** *on a set X is a binary relation on X that is* ***reflexive****,* ***symmetric*** *and* ***transitive****, i.e. relation $\sim$ defined on X is an equivalence relation if and only if:*

- $\forall a \in X \quad a \sim a \quad$ *(reflexivity)*
- $\forall a, b \in X \quad (a \sim b) \Rightarrow (b \sim a) \quad$ *(symmetry)*
- $\forall a, b, c \in X \quad ((a \sim b) \wedge (b \sim c)) \Rightarrow (a \sim c) \quad$ *(transitivity)*

Example 2.16 (equivalence relations)
The following are examples of equivalence relations:

- *The equality ("=") relation between real numbers or sets.*
- *The relation "has the same birthday as" on the set of all human beings.*
- *The relation "is congruent to" on the set of all triangles.*
- *The relation "is similar to" on the set of all triangles.*

DEFINITION 2.17 (equivalence class)
*When $\sim$ is equivalence relation defined on set X, **equivalence class** of an element a is a set of all elements from X that are in relation $\sim$ with a.*
*Division of a set into equivalence classes is called a **partition** of a set. (An equivalence relation on a set induces a partition of the set into equivalence classes.)*

NOTATION.
Equivalence class of an element a under relation $\sim$ is usually denoted as $[a]$, i.e.

$$[a] = \{x | x \sim a\}$$

EXAMPLE 2.18 (equivalence classes)
For the relation "has the same birthday as" on the set of all human beings there are 366 equivalence classes. (Why?)

DEFINITION 2.19 (congruency modulo)
Let $a, b \in \mathbb{Z}$. Let $n \in \mathbb{Z}^+$. We say that a is congruent to b modulo n *and write it as*

$$a \equiv b \mod n$$

if and only if one of the following equivalent conditions is fulfilled:

1. *a and b give the same remainder when divided by n* — *or*
2. *$(a - b)$ is divisible by n*
   which is denoted as $n|(a - b)$ — *or*
3. *$a - b = nk$, where k is an integer*

Note: *"$a \equiv b \mod n$" denotes congruency relation while "$a \mod n$" denotes the remainder when a is divided by n.*

EXAMPLE 2.20 (congruency modulo)

- $30 \equiv 21 \mod 3$ — *[both numbers divisible by 3, the remainder is 0]*
- $19 \equiv 13 \mod 3$ — *[the remainder is 1]*
- $5 \equiv 8 \mod 3$ — *[the remainder is 2]*
- $-9 \equiv 0 \mod 3$ — *[the remainder is 0]*
- $-8 \equiv 1 \mod 3$ — *[the remainder is 1]*
- $-7 \equiv 2 \mod 3$ — *[the remainder is 2]*

PROPERTIES.

- *When dividing by $n \in \mathbb{Z}^+$ the possible remainders are $0, 1, 2, \ldots, n - 1$.*
- *Let $a \equiv b \mod n$ and $c \equiv d \mod n$. Let $k \in \mathbb{Z}$. Then:*
  (1) $a + c \equiv b + d \mod n$
  (2) $a - c \equiv b - d \mod n$
  (3) $ka \equiv kb \mod n$
- *$[a] = [b]$ whenever $a \sim b$*

Questions

Q1. Let the relation $\approx$ ("is approximately equal") be defined between real numbers as follows:

$$a \approx b \Leftrightarrow |a - b| < 0.01$$

Show that the relation is reflexive and symmetric but not transitive.

Q2. Explain why the relation "is the mother of" on the set of all human beings is not reflexive, not symmetric and not transitive.

Q3. Prove that $aRb \Leftrightarrow a \equiv b \mod 3$ defined for integers is an equivalence relation.

Q4. The relation R is defined on the non-negative integers a, b such that aRb if and only if

$$3^a \equiv 3^b \mod 10.$$

(i) Show that R is an equivalence relation.

(ii) By considering consecutive powers of 3 identify the equivalence classes.

(iii) Find the value of $3^{9999} \mod 10$.

Q5. The relation R is defined on the non-negative integers a, b such that aRb if and only if

$$a^2 \equiv b^2 \mod 10.$$

(i) Show that R is an equivalence relation.

(ii) By considering consecutive squares identify the equivalence classes.

(iii) Find the value of $(\underbrace{9999\ldots999}_{1111}+123)^2 \mod 10$.

Q6. Verify whether the relation $\sim$ defined below is an equivalence relation when it is defined on the set of:

(i) square matrices of the same order

(ii) invertible square matrices of the same order

$A \sim B \Leftrightarrow$

(a) $\det A = \det B$

(b) $(\det A)(\det B) = 0$

(c) $(\det A)(\det B) > 0$

(d) $(\det A)(\det B) < 0$

(e) $(\det A)(\det B) \neq 0$

Justify your answers.

Q7. Identify the partition of positive integers for relation $aRb \Leftrightarrow 3^a \equiv 3^b \mod 5$.

Q8. Let $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$. State whether the relation R is an equivalence relation. Justify your answers (prove that R is equivalence relation or show counter-example). For equivalence relations determine equivalence classes.
$(a, b)R(c, d) \Leftrightarrow$

(i) $a = c$

(ii) $d - b = 2(a - c)$

(iii) $a + b = c + d$

(iv) $(a - c)(a + c) = (d - b)(d + b)$

(v) $(a - b)(a + b) = (c - d)(c + d)$

(vi) $\max(|a|, |b|) = \max(|c|, |d|)$

(vii) $|a| + |b| = |c| + |d|$

(viii) $ad = bc$

What would happen if the last relation was defined on $\mathbb{R}^2 \setminus \{(0, 0)\}$ instead of $\mathbb{R}^2$?

Q9. Let $a, b \in \mathbb{R}$. State whether the relation R is an equivalence relation. Justify your answers (prove that R is equivalence relation or show counter-example). For equivalence relations determine equivalence classes.
$aRb \Leftrightarrow$

(i) $|a| = |b|$
(ii) $|a| > |b|$
(iii) $|a| \geq |b|$
(iv) $a^2 - a = b^2 - b$

Q10. Let $a, b \in \mathbb{C}$. State whether the relation R is an equivalence relation. Justify your answers (prove that R is equivalence relation or show counter-example). For equivalence relations determine equivalence classes.
$aRb \Leftrightarrow$

(i) $|a| = |b|$
(ii) $|a| \geq |b|$
(iii) $a = b + 2 - i$
(iv) $|a - b| = 5$
(v) $a = bi$
(vi) $|\arg(a^2) - \arg(b^2)| = \pi + 2\pi k, k \in \mathbb{Z}$
(vii) $Re(a) \times Im(b) = Re(b) \times Im(a)$
(viii) $a^2 - a = b^2 - b$

Chapter 3

Functions

3.1 Injections, surjections and bijections

DEFINITION 3.1 (domain, range)
Let $f : A \to B$ be a function. Then:

- *set A is called the* ***domain*** *of f,*
- *set B, a set of* possible *values of f is called the* ***codomain*** *of f,*
- *the* ***range*** *of f is a subset $f(A)$ of B that contains all* actual *values of f, i.e.*

$$f(A) = \{f(x) | x \in A\}$$

EXAMPLE 3.2 (domain, range)
Let $f : \mathbb{R} \to \mathbb{R}$ be defined $f(x) = x^2$.

- *the* ***domain*** *of f is $\mathbb{R}$,*
- *the* ***codomain*** *of f is $\mathbb{R}$,*
- *the* ***range*** *of f is $[0, +\infty[$,*

Let $g : [-2, +\infty] \to \mathbb{R}$ be defined $g(x) = x^2$.

- *the* ***domain*** *of g is $[-2, +\infty]$,*
- *the* ***codomain*** *of g is $\mathbb{R}$,*
- *the* ***range*** *of g is $[0, +\infty[$.*

3.1.1 Injection

DEFINITION 3.3 (injection)
A function $f : A \to B$ is called an ***injection*** *(or* ***"one-to-one"*** *or "injective function")* if and only if *it fulfils one of the following equivalent conditions:*

1. *Each argument $a \in A$ of function f has a* ***unique*** *value $b \in B$ assigned to a.*

2. *For every value $b \in B$ (codomain) there is at most one argument $a \in A$ such that $f(a) = b$.*

or more formally:

3. *For all $a_1, a_2 \in A$: $(a_1 \neq a_2) \Rightarrow (f(a_1) \neq f(a_2))$.*

4. *For all $a_1, a_2 \in A$: $(f(a_1) = f(a_2)) \Rightarrow (a_1 = a_2)$.*

Note. *Using the definition of a function both implications ($\Rightarrow$) in above conditions can be changed to equivalences ($\Leftrightarrow$).*

EXAMPLE 3.4 (injections)

- *For any set X, the identity function on X defined $f(x) = x$* ***is*** *injective.*

- *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$ **is** injective.*
- *Any linear function whose graph is not horizontal **is** injective.*
- *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ **is not** injective, because (for example) $f(2) = f(-2) = 4$.*
- *The function $f : [0, +\infty[\to \mathbb{R}$ defined by $f(x) = x^2$ **is** injective.*
- *The exponential function $x \to e^x$ **is** injective.*
- *The natural logarithm function $ln :]0, +\infty[\to \mathbb{R}$ defined: $x \mapsto \ln x$ **is** injective.*
- *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ **is** injective.*
- *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3 - x$ **is not** injective. (Why? Find a counter-example.)*

PROPERTIES.

- ***Horizontal line test***
  For real functions (both domain and codomain are subsets of the real number set), an injective function $f : \mathbb{R} \to \mathbb{R}$ is one whose graph is never intersected by any horizontal line more than once.
- *A function that is decreasing (or increasing) in its whole domain is injective.*

3.1.2 Surjection

DEFINITION 3.5 (surjection)
*A function $f : A \to B$ is called a **surjection** (or **"onto"** or "surjective fuction") if and only if it fulfils one of the following equivalent conditions:*

1. *Each element $b \in B$ of codomain is a value for at least one $a \in A$.*
2. *If $b \in B$ then there exists $a \in A$ such that $f(a) = b$. $(\forall\, b \in B\ \exists\, a \in A : f(a) = b)$*

***Note.** A surjective function is a function which uses all values from codomain. In other words, a function $f : A \to B$ is surjective if and only if its range $f(A)$ is equal to its codomain B.*

EXAMPLE 3.6 (surjections)

- *For any set X, the identity function on X defined $f(x) = x$ **is** surjective.*
- *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$ **is** surjective.*
  (For any y from codomain we can find $x = \frac{y-1}{2}$ in the domain.)
- *Any linear function whose graph is not horizontal **is** surjective.*
- *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ **is not** surjective, because (for example) there is no real number x such that $f(x) = -1$.*
- *The function $f : \mathbb{R} \to [0, +\infty[$ defined by $f(x) = x^2$ **is** surjective.*

3.1.3 Bijection

DEFINITION 3.7 (bijection)
*A function $f : A \to B$ is called a **bijection** (or "bijective fuction") if and only if it fulfils one of the following equivalent conditions:*

1. *f is both **injective** and **surjective**.*
2. *for every $b \in B$ there exists* exactly one *$a \in A$ such that $f(a) = b$.*

EXAMPLE 3.8 (bijections)

- *For any set X, the identity function on X defined $f(x) = x$ **is** bijective.*
- *The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$ **is** bijective.*
  *(For any y from codomain we can find the **unique** $x = \frac{y-1}{2}$ in the domain.)*

3.2 Composition of functions

DEFINITION 3.9 (composite function)

*For functions $f : A \to B$ and $g : B \to C$ a **composite function** $g \circ f : A \to C$ is defined:*

$$\forall x \in A \quad (g \circ f)(x) = g(f(x))$$

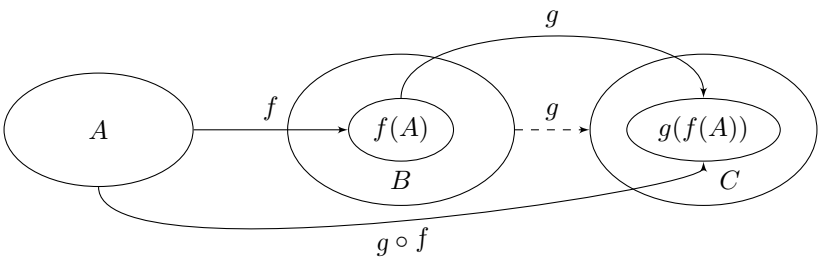


Figure 3.1: Composition of functions.

NOTATION.

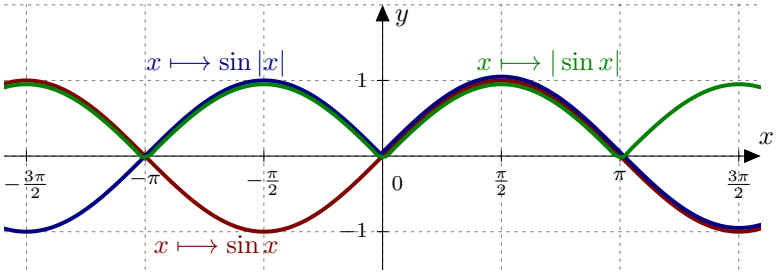
- *$g \circ f$ is read as "g circle f" or "g composed with f".*
- *when $A \subset B$ then $f : A \to B$ may compose with itself.*
  $f(f(x)) = f^2(x)$
  $f(f(f(x))) = f^3(x)$ *etc.*

EXAMPLE 3.10 (composite functions)

Suppose that an airplane's height at time t is given by the function $h(t)$ and that the oxygen concentration at height x is given by the function $c(x)$. Then $(c \circ h)(t)$ describes the oxygen concentration around the plane at time t.

PROPERTIES.

- *The composition of functions is always **associative**.*
  That is, if f, g, and h are three functions with domains and codomains as in the definition, then
  $$f \circ (g \circ h) = (f \circ g) \circ h.$$
- *(As a result the set of bijective functions $f : X \to X$ forms a group with respect to the composition operator. More on that in chapter 5.)*
- *In general, the composition of functions is **not commutative**.*
  That is for $f : A \to B$ and $g : C \to D$: $g \circ f \neq f \circ g$.
  (Note that $A = B = C = D$ for both compositions to be well defined.)



$(f \circ g)(x) \neq (g \circ f)(x)$ *for* $f(x) = \sin x$ *and* $g(x) = |x|$.

- *Derivatives of compositions can be found using the chain rule.*

3.3 Inverse function

DEFINITION 3.11 (inverse function)

For a function $f : A \to B$ *its* ***inverse*** f^{-1} *is a function*

$$f^{-1} : B \to A$$

such that:

- $(f^{-1} \circ f)(x) = x$ *for every* $x \in A$ *and*
- $(f \circ f^{-1})(x) = x$ *for every* $x \in B$

PROPERTIES.

- *Injections are invertible, however the inverses are defined on the injections' ranges only.*

If $f : X \to Y$ *is injective then there exists a function* $g : Y \to X$ *such that* $g(f(x)) = x$ *for every* $x \in X$*, that is* $g \circ f : X \to X$ *is identity function.*

Note. *g may not be the complete inverse of f, that is* $f \circ g : Y \to Y$ *may not be identity on* Y.

EXAMPLE 3.12 (inverse function)

- *Let* $f : [0, +\infty[\to \mathbb{R}$ *be defined by* $f(x) = \sqrt{x}$.
  Consider $g : R \to [0, +\infty[$ *defined by* $g(x) = x^2$.
  Then: $g \circ f : [0, +\infty[\to [0, +\infty[$ *defined is the identity on* $[0, +\infty[$. $g \circ f(x) = g(f(x)) = g(\sqrt{x}) = (\sqrt{x})^2 = x$
  On the other hand:
  $f \circ g : \mathbb{R} \to \mathbb{R}$ *defined is the identity on* $[0, +\infty[$ *only, not on* $\mathbb{R}$. $f \circ g(x) = f(g(x)) = f(x^2) = \sqrt{(x^2)} = |x|$

PROPERTIES.

- *Bijections are invertible.*

If $f : X \to Y$ *is bijective then there exists a function* $g : Y \to X$ *such that both* $g \circ f : X \to X$ *and* $f \circ g : Y \to Y$ *are identity functions.*

Questions

Q1. The functions f_k are defined for $k = 1, 2, 3, 4, 5$ as $f_k(x) = x^2$, where:

$$\begin{aligned} f_1 &: \mathbb{R} \to \mathbb{R}, \\ f_2 &: \mathbb{R} \to [0, +\infty[, \\ f_3 &: [0, +\infty[\to [0, +\infty[, \\ f_4 &: [0, +\infty[\to \mathbb{R}, \\ f_5 &:]-\infty, 0] \to [0, +\infty[. \end{aligned}$$

Verify which of the functions is injective, surjective and bijective. Find inverses of bijections.

Q2. Function $f :]-\infty, a] \to B$ is defined by $f(x) = x^2 - 8x + 11$.

(i) Find the largest value of a for which f is injective.

(ii) Find B for which f is surjective.

(iii) Find the equation of the inverse of f.

(iv) Sketch the graphs of both f and its inverse.

Q3. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = e^x - 2e^{-x} + 1$.

(i) Show that f is increasing in the whole domain.

(ii) Explain why f is onto $\mathbb{R}$.

(iii) Show that the function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = \ln(\frac{x-1+\sqrt{x^2-2x+9}}{2})$ is the inverse of f.

Q4. Consider the function $f :]-\infty, 0] \to [0, +\infty[$ defined by $f(x) = e^x + e^{-x} - 2$.

(i) Show that f is bijective.

(ii) Find the inverse of f.

Q5. Function $f : [-2, 2] \longrightarrow [-2, 2]$ is defined:

$$f(x) = \begin{cases} \frac{\sqrt{x+2}-4}{2} & \text{for } -2 \leq x < -1 \\ 2^x - 2 & \text{for } -1 \leq x \leq 2 \end{cases}$$

(i) Show that f is bijective.

(ii) Find the inverse of f.

Q6. Function $f : [-6, 6] \longrightarrow [-7, 1]$ is defined:

$$f(x) = \begin{cases} \frac{x^2+12x+1}{5} & \text{for } -6 \leq x \leq -1 \\ \frac{\ln(x+2)}{\ln 2} - 2 & \text{for } -1 < x \leq 6 \end{cases}$$

(i) Show that f is bijective.

(ii) Find the inverse of f.

Q7. Part A.
Let $f : [-5, 4] \longrightarrow [-7, 5]$ be defined:

$$f(x) = \begin{cases} x^2 + 10x + 18 & \text{for } -5 \leq x < -2 \\ -\frac{1}{2}x + 1 & \text{for } -2 \leq x \leq 4 \end{cases}$$

(i) Is f injective? Why?

(ii) Is f surjective? Why?

Part B.
Let $g : [-5, 4] \longrightarrow [-7, 5]$ be defined:

$$g(x) = \begin{cases} x^2 + 10x + 18 & \text{for } -5 \leq x < -2 \\ -\frac{1}{2}x + b & \text{for } -2 \leq x \leq 4 \end{cases}$$

Find the value of b for which g is a bijection.

Q8. Consider the function $f : \mathbb{R} \longrightarrow \mathbb{R}$ defined as follows:

$$f(x) = \begin{cases} -x^2 & \text{for } x < a \\ x & \text{for } x \geq a, \end{cases}$$

where a is a real constant.

(i) Find the values of a for which f is bijective.

(ii) Find the inverse of f for one value of a found before.

Q9. Consider the function $k : \mathbb{R} \longrightarrow \mathbb{R}$ defined as follows:

$$k(x) = \begin{cases} x + 2 & \text{for } x \leq a, \\ x^2 & \text{for } x > a \end{cases}$$

where a is a real constant.

(i) Find the value of a for which k is bijective.

(ii) Find the inverse of k.

Q10. Consider the function $g : [a, b] \longrightarrow [c, 6]$, where $a, b, c \in \mathbb{R}$ are constants defined as follows:

$$g(x) = \begin{cases} -\frac{1}{2}x - 2 & \text{for } a \leq x \leq -2 \\ x + 3 & \text{for } -2 < x \leq b \end{cases}$$

(i) Find the values of a, b and c for which g is bijective.

(ii) Find the inverse of g.

Q11. Find the largest possible number $a \in \mathbb{R}$ for which the function $h :]-\infty, a] \longrightarrow \mathbb{R}$ defined as $h(x) = x^3 - x$ is injective.

Q12. Consider the function $f : [0, 1] \longrightarrow [p, q]$, where $p, q \in \mathbb{R}$ are constants defined by

$$f(x) = 2x^4 - 4x^2 + 1$$

.

(i) Prove that f is injective.

(ii) Find the values of p and q for which f is surjective.

(iii) Find the inverse of f.

Q13. Part A.
Let $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be defined:

$$f(x, y) = (3y - 2x, 4x - 6y).$$

Show that f is not a surjection.
Part B.
Let $g : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be defined:

$$g(x, y) = (2x - y, x + 2y).$$

(i) Show that g is injective.

(ii) Show that g is surjective.

(iii) Find the inverse of g.

Q14. Let $f : [-2, 2] \longrightarrow [b, c]$ be defined:

$$f(x) = \begin{cases} -x^2 + 4x & \text{for } -2 \leq x \leq a \\ 2x^2 + 1 & \text{for } a < x \leq 2, \end{cases}$$

where a, b and c are real constants.

(i) Find the values of a, b and c for which f is bijective. Justify your answer.

(ii) Find the inverse of f.

Q15. Part A.

Let $f : \mathbb{R} \setminus \{0\} \times \mathbb{R} \setminus \{0\} \longrightarrow \mathbb{R}^2$ be defined:

$$f(x, y) = \left(\frac{3x - y}{x}, \frac{x + y}{y} \right).$$

Is f an injection? Justify your answer.

Part B.

Let $g : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ be defined:

$$g(x, y) = (4x - 5y, 3y - 2x).$$

(i) Show that g is injective.

(ii) Show that g is surjective.

(iii) Find the inverse of g.

Q16. Let $f :]-\infty, a] \longrightarrow \mathbb{R}$ be defined:

$$f(x) = \frac{2}{e^{x^2} + 1}.$$

(i) State the largest value of a for which f is injective.

(ii) State the range of f.

Let $g : \mathbb{R} \longrightarrow \mathbb{R}^+$ be defined:

$$g(x) = \begin{cases} \frac{2}{e^{x^2}+1} & \text{for } x \leq a \\ (x - b)^2 & \text{for } x > a, \end{cases}$$

where a is the value obtained above and b is a real constant.

(iii) Find the value of b for which g is bijective. Justify your answer.

(iv) Find the inverse of g.

Q17. Let $f : \mathbb{Z} \longrightarrow \mathbb{N}$ be defined:

$$f(x) = \left| \frac{4x - 1}{2} \right| - \frac{1}{2}.$$

Let $g : \mathbb{R} \longrightarrow \mathbb{R}$ be defined:

$$g(x) = x^3 + x.$$

Let $h : \mathbb{R}^2 \longrightarrow \mathbb{R}$ be defined:

$$h(x, y) = x^2 - y^2.$$

(i) Is f an injection? Is it a surjection? Justify your answer.

(ii) Is g an injection? Is it a surjection? Justify your answer.

(iii) Is h an injection? Is it a surjection? Justify your answer.

(iv) Find the inverse of f **OR** the inverse of g **OR** the inverse of h.

Q18. Let $f : A \to B$ and $g : B \to C$ be functions and let $h = g \circ f$.
Show that:

(i) if f and g are injective then h is injective, too,

(ii) if f and g are surjective then h is surjective, too,

(iii) if h is surjective then g is surjective, too,

(iv) if h is injective then f is injective, too.

Show by counter-example that the following statements are not true.

(v) if h is surjective then both f and g are surjective,

(vi) if h is injective then both f and g are injective, too.

Chapter 4

Operations

4.1 Binary operations

DEFINITION 4.1 (binary operation)
*A **binary operation** $*$ on a set S is a function:*

$$* : S \times S \to A.$$

NOTATION.
$*(a, b) = a * b$

PROPERTIES.

- ***Closure***. $*$ *is closed when* $A \subseteq S$.
- ***Associativity***. $*$ *is associative if for any* a, b, c *from* S*:*

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

- ***Distributivity***. $*$ *is distributive over* $\sim$ *if for any* a, b, c *from* S*:*

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

- ***Commutativity***. $*$ *is commutative if for any* a, b *from* S*:*

$$a * b = b * a$$

EXAMPLE 4.2 (properties of standard operations)

- *Addition of numbers* ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$)
  ▷ *(closed, associative, commutative)*
- *Multiplication of numbers* ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$)
  ▷ *(closed, associative, distributive over addition, commutative)*
- *Subtraction of numbers over natural numbers*
  ▷ *(not closed, not associative, not commutative)*
- *Subtraction of numbers over* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
  ▷ *(closed, not associative, not commutative)*
- *Addition of matrices of the same order*
  ▷ *(closed, associative, commutative)*
- *Multiplication of square matrices of the same order*
  ▷ *(closed, associative, distributive over addition, not commutative)*
- *Composition of functions*
  ▷ *(closed, associative, not commutative)*

4.2 Operation tables (Cayley tables)

Cayley table is a representation of a binary operation $\oplus : S \times S \to S$ defined on a set S.

Example 4.3 (addition modulo 4)

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Example 4.4 (Cayley table)

$\odot$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	d	b	c
b	b	c	e	d	a
c	c	d	a	e	b
d	d	b	c	a	e

The table in example 4.3 shows results of addition modulo 4:

$$\oplus : \{0,1,2,3\} \times \{0,1,2,3\} \to \{0,1,2,3\}.$$

$a \oplus b = (a + b) \mod 4$ is the remainder when $a + b$ is divided by 4.

Definition 4.5 (Latin square property)

*An operation table is said to have the **Latin square property** when each element of the set appears exactly once in each row and each column inside the table.*
More precisely, if $(G, *)$ is a set with binary operation and a and b are elements of G, then there exists a unique element x of G such that $a * x = b$, and a unique element y of G such that $y * a = b$.

Note. Both tables shown above have the **Latin square property**.
(In the example 4.3 above:
for $a = 2$ and $b = 3$, $x = 1$ and $y = 1$, as $2 * 1 = 3$ and $1 * 2 = 3$.)

Example 4.6 (Latin square)

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Example 4.7 (not Latin square)

$\odot$	1	3	5	7	9
1	1	3	5	7	9
3	3	9	5	1	7
5	5	5	5	5	5
7	7	1	5	9	3
9	9	7	5	3	1

The example 4.6 above shows results of multiplication modulo 5 on a set $\{1, 2, 3, 4\}$.
The example 4.7 above shows results of multiplication modulo 10 on a set $\{1, 3, 5, 7, 9\}$.
Note that the table in example 4.6 has a Latin square property while the one in example 4.7 does not.

Questions

Q1. Determine whether or not the set of numbers in the form $a + b\sqrt{2}$, where $a, b \in \mathbb{Z}$ is closed under multiplication.

Q2. Determine whether or not the set of 2×2 matrices of the type $\begin{pmatrix} t & 1-t \\ 1+t & -t \end{pmatrix}$, $t \in \mathbb{R}$ is closed under matrix multiplication.

Q3. Given that p and q are real, show that the set of matrices of the form $\begin{pmatrix} p & -q \\ q & p \end{pmatrix}$ is closed under matrix multiplication and that the operation is commutative on this set.

Q4. The binary operation $*$ is defined by $a * b = \frac{a+b}{ab}$, where $a, b \in \mathbb{R} \setminus \{0\}$.

(i) Is the operation commutative?

(ii) Is the operation associative?

Q5. The binary operation $*$ is defined by $a * b = \frac{a}{b}$, where $a, b \in \mathbb{R} \setminus \{0\}$. Show that $*$ is neither commutative nor associative.

4.3 The identity and inverses

4.3.1 The identity element e

DEFINITION 4.8 (identity)

Let $(S, *)$ be a set S with a binary operation $*$ on it.
An element e of S is called:

- *a left identity if $e * a = a$ for all a in S, and*
- *a right identity if $a * e = a$ for all a in S.*

If e is both a left identity and a right identity, then it is called a two-sided identity, or simply the ***identity****.*

EXAMPLE 4.9 (identities)

set	***operation***	***identity***
real numbers	*multiplication*	1
real numbers	*addition*	0
$n \times n$ matrices	*multiplication*	*identity matrix*
$n \times n$ matrices	*addition*	*zero matrix*
real functions	*composition*	*identity function $e(x) = x$*
real numbers	*subtraction*	***no identity***
real numbers	*division*	***no identity***

THEOREM 4.10 (Uniqueness of identity)

For given set and a binary operation defined on the set there exists at most one identity.

PROOF.

Suppose that e and f are two identities in $(S, *)$.
Then for all a in S (1) $a * e = a$ and (2) $e * a = a$
and (3) $a * f = a$ and (4) $f * a = a$
From (1) for $a = f$: (5) $f * e = f$
From (4) for $a = e$: (6) $f * e = e$
From (5) and (6): $f = f * e = e$, that is $f = e$.

□

Questions

Q6. Let operation $\triangle$ be defined on real numbers as follows:

$$x \triangle y = x + y - 1$$

Find the identity for the operation.

Q7. Let operation $*$ be defined on real numbers as follows:

$$x * y = xy - x - y + 2$$

Find the identity for the operation.

Q8. Let operation $\circ$ be defined on real numbers as follows:

$$x \circ y = \frac{x}{y+2}$$

(i) Find the right identity for $\circ$.

(ii) Show that $\circ$ has no left identity.

Q9. Let operation $\star$ be defined on real numbers as follows:

$$x \star y = \frac{xy}{x+y}$$

Show that $\star$ has no identity.

Q10. The binary operation $*$ is defined by $a * b = \frac{a+b}{ab}$, where $a, b \in \mathbb{R} \setminus \{0\}$. Does the operation have the identity?

4.3.2 The inverse a^{-1} of an element a

DEFINITION 4.11 (inverse)

Let $(S, *)$ be a set S with a binary operation $*$ on it.
Let e be the identity of $(S, *)$.

- *if $b * a = e$ then b is called a left inverse of a,*
- *if $a * b = e$ then b is called a right inverse of a.*

*If b is both a left inverse and a right inverse of a, then it is called a two-sided inverse, or simply the **inverse**.*
*An element with the inverse in S is called **invertible** in S.*

DEFINITION 4.12 (left-cancelation property)

Left-cancelation property
*An element a in $(S, *)$ has the **left-cancellation property** (or is **left-cancellative**) if for all b and c in S*
$a * b = a * c$ always implies $b = c$.

DEFINITION 4.13 (right-cancelation property)

Right-cancelation property
*An element a in $(S, *)$ has the **right-cancellation property** (or is **right-cancellative**) if for all b and c in S*
$b * a = c * a$ always implies $b = c$.

EXAMPLE 4.14 (inverses)

set	***operation***	***element***	***inverse***
$\mathbb{R} \setminus \{0\}$	*multiplication*	x	$\frac{1}{x}$
$\mathbb{R}$	*addition*	x	$-x$
$n \times n$ *matrices*	*multiplication*	A, $\det A \neq 0$	*inverse matrix* A^{-1}
$n \times n$ *matrices*	*addition*	A	$-A$
bijective functions	*composition*	f	*inverse function* f^{-1}

THEOREM 4.15 (Uniqueness of inverse)

For given set, a binary operation defined on the set and an element of the set there exists at most one inverse of the element.

Proof.

Suppose that b and c are two inverses of a in $(S, *)$.
Let e be the identity in S.

Then		(1)	$a * b = e$	and	(2)	$b * a = e$
	and	(3)	$a * c = e$	and	(4)	$c * a = e$
From (1) and (3):			$a * b = e = a * c$			
i.e.:			$a * b = a * c$			
and then			$b * (a * b) = b * (a * c)$			
		$\Leftrightarrow$	$(b * a) * b = (b * a) * c$			
from (2)			$e * b = e * c$			
so eventually			$b = c$			

□

Note that $*$ has to be associative.

Theorem 4.16 (Inverse of 2 elements)

Let $a, b \in S$ and let $*$ be a binary operation defined on S. Then

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

Proof. $(a * b) * (b^{-1} * a^{-1}) = a * (b * b^{-1}) * a^{-1} = a * e * a^{-1} = a * a^{-1} = e$
Similarly $(b^{-1} * a^{-1}) * (ab) = e$, so $(b^{-1} * a^{-1})$ is the inverse of (ab). □

Corollary 4.17 (Inverse of more than 2 elements)

Let $a_1, a_2, \dots a_n \in S$ and let $*$ be a binary operation defined on S. Then

$$(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * \cdots * a_2^{-1} * a_1^{-1}$$

Proof. It can be easily shown by the mathematical induction. □

Definition 4.18 (involute function)

*An **involute** function is a* self-inverse *function, i.e. a function f that fulfils one of the following equivalent conditions:*

I. *$f(x) = f^{-1}(x)$ for every x from the domain of f,*

II. *$(f \circ f)(x) = x$ for every x from the domain of f.*[1]

Properties.

- *Graphs of involute real functions are self-symmetrical in line $y = x$.*
- *An involute real function has at most one zero.*

Example 4.19 (involute functions)

- *$e : x \longmapsto x$ defined on any non-empty set is an involute function,*
- *$x \longmapsto \frac{1}{x}$ and $x \longmapsto -\frac{1}{x}$ are involute functions,*
- *$x \longmapsto k - x$, where $k \in \mathbb{R}$ is a constant is an involute function.*

Questions

Q11. Given that p and q are real, consider the set of matrices of the form $\begin{pmatrix} p & -q \\ q & p \end{pmatrix}$.

(i) State in terms of p and q the condition that an elementof the set has the inverse.

(ii) Write down the element(-s) of the set which is self-inverse.

[1] the condition requires the domain of f and the range of f to be the same set

(iii) Write down the element(-s) of the set which has no inverse.

Q12. Show the tables of addition and multiplication modulo 5 of the set $\{0, 1, 2, 3, 4\}$.
State

(i) the identity elements under both operations,

(ii) the inverses of 3 and of 4 under both operations.

If $p \in \{0, 1, 2, 3, 4\}$ solve, in modulo 5 arithmetic,

(iii) $p + 2 = 1$,

(iv) $p \times p = 1$.

Q13. The operation $\odot$ is defined on the set of complex numbers $\mathbb{C}$ as follows:
For $z_1 = x_1 + iy_1$ and $z_2 = x_2 + iy_2$: $z_1 \odot z_2 = x_1x_2 + iy_1y_2$.
Determine the identity element.

Q14. Let $f(x) = \frac{ax+b}{cx+d}, x \in \mathbb{R} \setminus \{-\frac{d}{c}\}$. Show that f is a self-inverse (involute) function if **either** f can be expressed as $f(x) = \pm x$ **or** $d = -a$.

Q15. For each of sets S under given operation:

(i) construct the Cayley table,

(ii) find the identity,

(iii) list inverses of all elements.

(1) $S = \{0, 1, 2, 3\}$ under addition modulo 4,

(2) $S = \{0, 1, 2, 3\}$ under multiplication modulo 4,

(3) $S = \{0, 2, 4, 6, 8, 10, 12\}$ under addition modulo 14,

(4) $S = \{1, 3, 5, 9, 11, 13\}$ under multiplication modulo 14.

Chapter 5

Groups

5.1 Axioms of a group

DEFINITION 5.1 (group)
A set G under a given operation $*$ is called a ***group*** *if the following four conditions are fulfilled:*

1. *G is closed under $*$,*

2. *$*$ is associative,*

3. *G contains an identity element,*

4. *each element in G has an inverse in G.*

EXAMPLE 5.2 (group)
Set $S = \{1, i, -1, -i\}$ under multiplication is a group.

PROOF.

1. The table below shows closure:

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

2. multiplication of numbers is associative.

3. $1 \in S$ is the identity.

4. Each element has an inverse in S:

element	1	i	-1	$-i$
inverse	1	$-i$	-1	i

i.e. i and $-i$ are inverses while 1 and -1 are *self-inverses*.

□

PROPERTIES.

- *A group has exactly one identity element.*
- *Every element has exactly one inverse.*
- *A "division" can be performed on groups; that is, given elements a and b of the group G, there is exactly one solution x in G to the equation $x * a = b$ and exactly one solution y in G to the equation $a * y = b$.*
- *The inverse of a product is the product of the inverses in the opposite order:*

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

THEOREM 5.3 (Latin square property for groups)

(1) The operation table of a group is a Latin square (has a Latin square property).

(2) A Latin square operation table does not have to be a group table.

PROOF.

(1) Let us assume otherwise, i.e. there is a row (or equivalently a column) in the operation table for a group $(G, *)$ in which an element of G appears at least twice.
Hence there exist three elements a, b and c in group $(G, *)$ such that $b \neq c$ and $a * b = a * c$

$*$	$\dots$	b	$\dots$	c	$\dots$
$\vdots$		$\vdots$		$\vdots$	
a	$\dots$	x	$\dots$	x	$\dots$
$\vdots$		$\vdots$		$\vdots$	

(or equivalently $b * a = c * a$ for a column). Then:

$$\begin{aligned} a * b &= a * c \\ a^{-1} * (a * b) &= a^{-1} * (a * c) && \text{(as there exists } a^{-1} \in G) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c && (* \text{ is associative}) \\ (e) * b &= (e) * c && (e \text{ is the identity in } G) \\ b &= c, \end{aligned}$$

which shows by contradiction that the table must be Latin square.

(2) Consider the two operation tables below.

table 1

$*$	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	1
3	3	4	5	1	2
4	4	5	1	2	3
5	5	1	2	3	4

table 2

$\circ$	1	2	3	4	5
1	1	2	3	4	5
2	3	4	5	1	2
3	2	3	4	5	1
4	4	5	1	2	3
5	5	1	2	3	4

Table 1 shows a group while table 2 does not. Why? Which of the axioms is not satisfied? (Finish the proof yourself.) □

Note. The group shown in table 1 in the proof above is actually the only possible 5-element group. The reasons for that will be explained later in section 5.7.

DEFINITION 5.4 (Abelian group)
A group $(G, *)$ is called ***Abelian*** *(or* ***commutative****) when $a * b = b * a$ for all $a, b \in G$.*

NOTATION.
$a * b = ab$ *(*multiplicative *notation)*

Note.
The *multiplicative* notation is sometimes confusing.

EXAMPLE 5.5 (multiplicative notation)
Consider a group of integers under addition. Then:

- *ab means $a + b$*
- *$2^5 = 2 + 2 + 2 + 2 + 2 = 10$ (i.e. it is actually 2×5)*
- *$2^{-1} = -2$*

EXAMPLE 5.6 (elementary groups)

- *$\mathbb{R}$ under addition - an Abelian group*
- *$\mathbb{Q}$ under addition - an Abelian group*
- *$\mathbb{Z}$ under addition - an Abelian group*
- *$\mathbb{C}$ under addition - an Abelian group*
- *$\mathbb{Z}$ under multiplication - not a group*
- *$\mathbb{Q}$ under multiplication - not a group*
- *$\mathbb{Q}^+$ under multiplication - an Abelian group*
- *matrices of the same order under addition - an Abelian group*
- *2×2 invertible matrices under multiplication - nonabelian group*
- *integers under addition modulo n - an Abelian group*
- *invertible functions under composition of functions - nonabelian group*

EXAMPLE 5.7 ($\mathbb{Z}_n$ group)
Let operation $\oplus$ be defined on set $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$ as addition modulo n*:*

$$a \oplus b = (a + b) \mod n$$

Then:

- *$\mathbb{Z}_n$ is* closed *under $\oplus$*
- *$\oplus$ is* associative *as the addition is,*
- *$0 \in \mathbb{Z}_n$ is the* identity
- *each element in $\mathbb{Z}_n$ has the inverse in $\mathbb{Z}_n$: $k^{-1} = n - k$*

EXAMPLE 5.8 (Group of vectors in $\mathbb{R}^2$)
Let $\vec{i} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\vec{j} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Then $\mathbb{R}^2$ defined as follows:

$$\mathbb{R}^2 = \{x\vec{i} + y\vec{j} |\ x, y \in \mathbb{R}\}$$

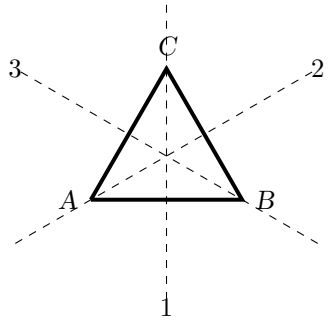
forms a group under addition of vectors. (Why?)

Note: the example can be extended to higher dimensions.

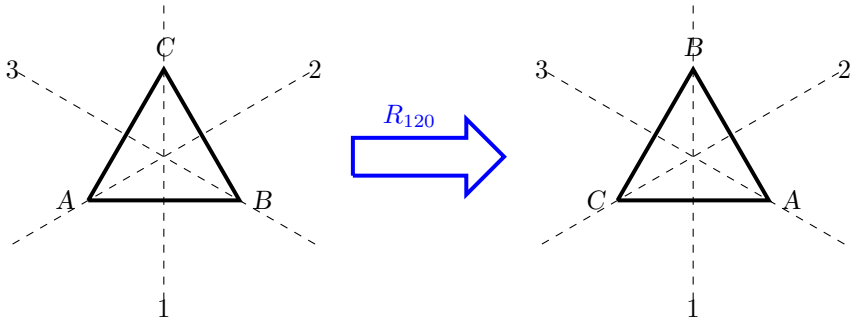
EXAMPLE 5.9 (Group of transformations of a plane under composition of transformations)
The group $(G, \circ)$ *generated by* rotations, reflections, enlargements *and* translations.
$\circ$ *is composition of transformations. (The composition* $T_2 \circ T_1$ *denotes* T_1 *followed by* T_2*.)*

- G *is* closed *under* $\circ$
- $\circ$ *is* associative
- G *contains an* identity *element the identity transformation*
- *each element in* G *has the inverse in* G*:*
  - *for a rotation: rotation about the same point with opposite angle*
  - *for a reflection: the same reflection*
  - *for an enlargement with scale factor* k*: an enlargement with scale factor* $\frac{1}{k}$
  - *for composition* $T_2 \circ T_1$*:* $(T_2 \circ T_1)^{-1} = (T_1)^{-1} \circ (T_2)^{-1}$

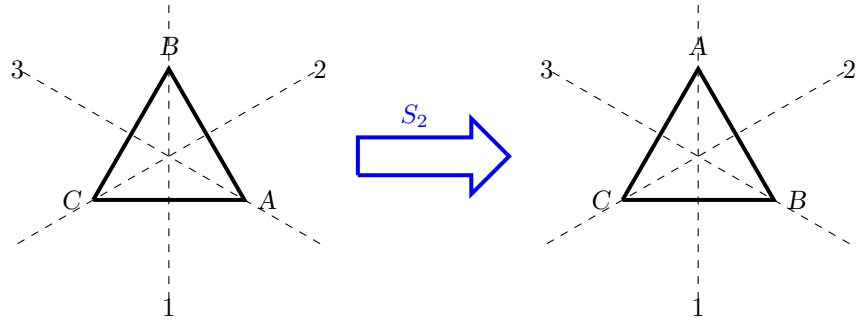
EXAMPLE 5.10 (Symmetries of an equilateral triangle under composition)
Let us consider an equilateral triangle:



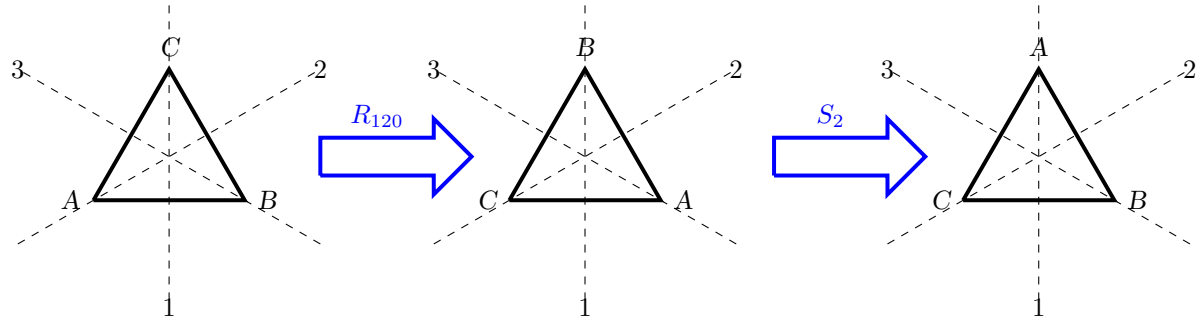
The group consists of I*, the identity, two anticlockwise rotations:* R_{120} *and* R_{240} *about the centre of triangle by* 120° *and* 240° *respectively and three reflections:* S_1*,* S_2 *and* S_3 *in lines 1, 2 and 3 respectively.*
The diagram below shows triangle ABC *changed by* R_{120}*:*



The diagram below shows triangle CAB *changed by* S_2*:*



Hence the composition $S_2 \circ R_{120}$ works as follows:



i.e. $S_2 \circ R_{120} = S_3$. Similarly all other compositions can be obtained.

$\circ$	I	R_{120}	R_{240}	S_1	S_2	S_3
I	I	R_{120}	R_{240}	S_1	S_2	S_3
R_{120}	R_{120}	R_{240}	I	S_3	S_1	S_2
R_{240}	R_{240}	I	R_{120}	S_2	S_3	S_1
S_1	S_1	S_2	S_3	I	R_{120}	R_{240}
S_2	S_2	S_3	S_1	R_{240}	I	R_{120}
S_3	S_3	S_1	S_2	R_{120}	R_{240}	I

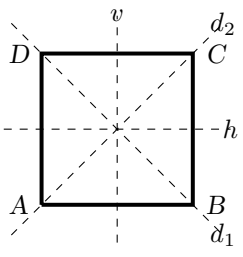
To show that set $G = \{I, R_{120}, R_{240}, S_1, S_2, S_3\}$ under composition of transformations is a group we have to check the four axioms:

1. *the table shows that G is closed under $\circ$,*
2. *$\circ$ is associative, as is composition of functions,*
3. *$I \in G$ is the identity,*
4. *each element in G has an inverse in G: $(R_{120})^{-1} = R_{240}$, $(R_{240})^{-1} = R_{120}$ while I and all reflections are self-inverses.*

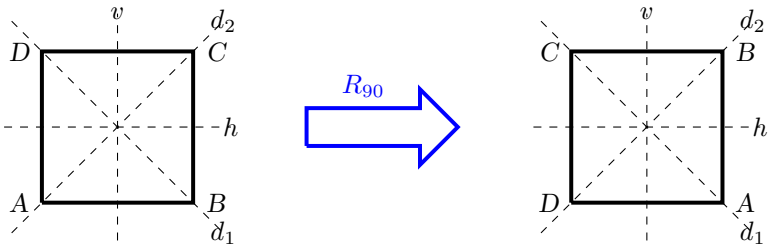
***Note** that the group is **not Abelian**.*

EXAMPLE 5.11 (Symmetries of a square under composition)

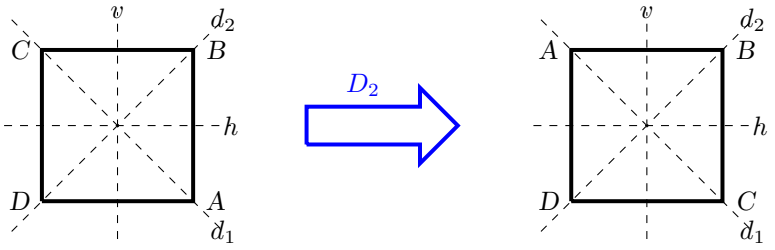
Let us consider a square:



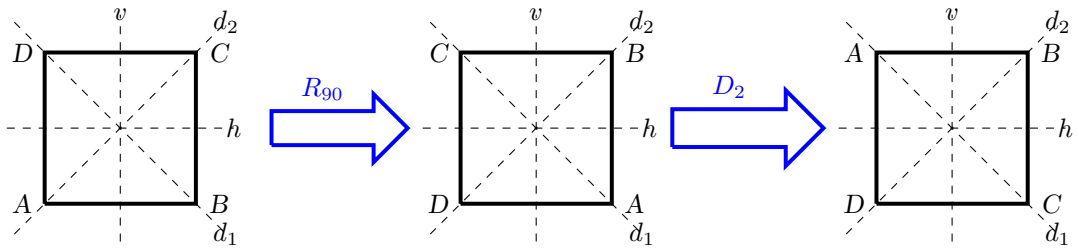
The group consists of I, the identity, three anticlockwise rotations: R_{90}, R_{180} and R_{270} about the centre of a square by 90°, 180° and 270° respectively and four reflections: H, V, D_1 and D_2 in lines h, v, d_1 and d_2 respectively.
The diagram below shows square $ABCD$ changed by R_{90}:



The diagram below shows square $DABC$ changed by D_2:



Hence the composition $D_2 \circ R_{90}$ works as follows:



i.e. $D_2 \circ R_{90} = H$. Similarly all other compositions can be obtained.

$\circ$	I	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
I	I	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
R_{90}	R_{90}	R_{180}	R_{270}	I	D_1	D_2	H	V
R_{180}	R_{180}	R_{270}	I	R_{90}	H	V	D_2	D_1
R_{270}	R_{270}	I	R_{90}	R_{180}	D_2	D_1	V	H
V	V	D_2	H	D_1	I	R_{180}	R_{270}	R_{90}
H	H	D_1	V	D_2	R_{180}	I	R_{90}	R_{270}
D_1	D_1	V	D_2	H	R_{90}	R_{270}	I	R_{180}
D_2	D_2	H	D_1	V	R_{270}	R_{90}	R_{180}	I

The proof that all four axioms of a group hold is left for the reader.

EXAMPLE 5.12 (Symmetries of a rectangle under composition)
The group consists of identity, 2 reflections, 1 rotation.

Questions

Q1. Given that the set $\{1, 2, 3, 4\}$ forms a group under operation $*$ copy and complete the operation table below.

$*$	1	2	3	4
1	3	1	4	2
2				
3				
4				

Find the solution set of the equations

(i) $x * x = 3$,

(ii) $(4 * x) * 1 = 3$.

Q2. (i) Show that the set of real numbers $\mathbb{R}$, excluding a single number, forms a group under the operation $\bigtriangledown$ defined as

$$a \bigtriangledown b = a + b - ab$$

and determine the number which must be excluded from $\mathbb{R}$.

(ii) Find the inverse of 7 in this group, and hence solve the equation $7 \bigtriangledown x = 13$.

(iii) The binary operation $\bigtriangleup$ in the set $\mathbb{R}$ of real numbers is defined by

$$a \bigtriangleup b = a + b + ab.$$

Show that $\mathbb{R}$ under $\bigtriangleup$ does not form a group. Give a reason for that.

Q3. Display the operation table for the set $S = \{0, 1, 2, 3, 4\}$ under the operation $*$, where $a * b = (ab + b) \mod 5$.

(i) Evaluate $(2 * 3) * 4$ and $2 * (3 * 4)$.

(ii) Determine which of the axioms of a group holds for the set S under $*$.

(iii) Find the solution set, under $*$, of the equations

I. $x * x = 0$

II. $(x * x) * x = 3$

Q4. The operation $*$ is defined on the set $S = \{0, 1, 2, 3, 4\}$ by $a * b = (a + b + 4ab) \mod 5$.

(i) Display the operation table for S under $*$.

(ii) Given that $*$ is associative, explain why $*$ on S still does not form a group.

T is the largest subset of S which does form a group under $*$.

(iii) List the elements of T and state

I. the identity,

II. the inverse of each element.

(iv) Given that $x \in T$ and that $x * x * x = 3$ find x.

Q5. Part A.
The operation $*$ is defined on the set of integers by $a*b = a+b+ab$. Show that $*$ is associative.
Part B.
The operation $\circ$ is defined on the set $S = \{0, 1, 2, 3, 4\}$ by $a \circ b = (a + b + ab) \mod 5$.

(i) Display the operation table for S under $\circ$.

(ii) Explain why $\circ$ on S does not form a group.

(iii) Write down each subset of S which forms a group under $\circ$.

Q6. Let $S = \{(x, y) \in \mathbb{R}^2 | \ x \neq 0\}$.
For $(x_1, y_1), (x_2, y_2) \in S$, the operation $*$ is defined by

$$(x_1, y_1) * (x_2, y_2) = (x_1 x_2, y_1 x_2 + y_2)$$

(i) Evaluate $(4,3) * (2,1)$.

(ii) Find the identity element.

(iii) Find the inverse of (a,b).

(iv) Find $((a,b) * (c,d)) * (e,f)$.

(v) Determine whether or not the operation $*$ on S forms a group.

Q7. Consider set G that consists of four functions:

$$e(x) = x \qquad p(x) = -x$$
$$q(x) = \frac{1}{x} \qquad r(x) = -\frac{1}{x}$$

under $\circ$, a composition of functions.

(i) Create a Cayley table for $(G, \circ)$.

(ii) Show that $(G, \circ)$ is a group.

(iii) Is the group Abelian? Why?

Q8. Consider set G that consists of four functions:

$$e(x) = x \qquad p(x) = \frac{2}{2-x}$$
$$q(x) = \frac{x-2}{x-1} \qquad r(x) = \frac{2x-2}{x}$$

under $\circ$, a composition of functions. Show that $(G, \circ)$ is a group. Is it Abelian?

Q9. Consider set G that consists of six functions:

$$e(x) = x \qquad s(x) = \frac{1}{x}$$
$$p(x) = 1 - x \qquad t(x) = \frac{1}{1-x}$$
$$q(x) = 1 - \frac{1}{x} \qquad u(x) = \frac{x}{x-1}$$

under $\circ$, a composition of functions.

(i) Create a Cayley table for $(G, \circ)$.

(ii) Show that $(G, \circ)$ is a group.

(iii) Is the group Abelian? Why?

Q10. Find the smallest set of functions G that contains a function $f(x) = \frac{2x-3}{x-1}$ and forms a group under composition of functions. Show it is a group.

Q11. Find the smallest set of functions G that contains a function $f(x) = \frac{1+x}{1-x}$ and forms a group under composition of functions. Show it is a group.

Q12. Find the smallest set of functions G that contains a function $f(x) = \frac{5x+7}{-3x-4}$ and forms a group under composition of functions. Show it is a group.

Q13. Let $G = \{p, q, r, s\}$ be a set of four functions, where $p : x \longmapsto \frac{x}{x-1}$ and $q : x \longmapsto \frac{x-2}{x-1}$. The set forms a group under $\circ$ - composition of functions.

(i) Find the functions r and s and show the group table.

(ii) Find $f, g \in G$ such that:

I. $(q \circ f) \circ p = q$
II. $(g \circ p) \circ g = p$

Q14. Consider matrices of the form $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ where $a, b \in \mathbb{R}$ and $ab \neq 0$. Show that a set of such matrices forms a group under matrix multiplication.

Q15. Consider matrices of the form $\begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & -c & b \end{pmatrix}$ where $a, b, c \in \mathbb{R} \setminus \{0\}$. Show that a set of such matrices forms a group under matrix multiplication.

Q16. Consider matrices of the form $\begin{pmatrix} a & b \\ 0 & a+2b \end{pmatrix}$ where $a, b \in \mathbb{R}$. Show that a set of such matrices forms a group under matrix multiplication if $a \neq 0$ and $a \neq -b$.

Q17. Consider the following two sets of matrices:

$$M = \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

and

$$S = \left\{ I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, D = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, E = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

Which of the two sets forms a group under matrix multiplication?

Q18. The three matrices:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \text{ and } B$$

form a group under the operation of matrix multiplication. Find the matrix B and write the group table.

Q19. Part A.
Let e, a and b be three distinct elements of group G, where e is the identity. They satisfy the equations

$$a^3 = b^2 = e \text{ and } ab = ba^2$$

(i) Explain why G is non-commutative.

(ii) Prove that

$$ba^2b = a \text{ and } a^2ba = ab$$

Part B.
The functions a, b and e are given by

$$a(x) = \frac{x+3}{-x-2},$$
$$b(x) = \frac{-x}{x+1},$$
$$e(x) = x.$$

(i) Show that they satisfy the condition $ab(x) = ba^2(x)$.

(ii) Show that they satisfy the condition $a^3(x) = b^2(x) = e(x)$.

(iii) Copy and complete the following group table, expressing all elements in the table in terms of those in the 0^{th} row and 0^{th} column.

$\circ$	e	a	b	ab	ba	a^2
e	e	a				
a	a		ab			
b		ba	e			
ab						
ba						
a^2						

Q20. Which of the following sets under the given operation forms a group? For each set which you decide does **not** form a group, give a reason for your answer. You may assume that the following operations are associative:

- addition of numbers,
- multiplication of numbers,
- addition of matrices,
- multiplication of matrices,
- composition of functions.

(1) the set $\{1, i, -1, -i\}$ under multiplication,

(2) the set $\left\{1, -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right\}$ under multiplication,

(3) the set $\left\{\pm 1, \pm\left(\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right)\right\}$ under multiplication,

(4) the set $\{0, 1, 2, 3\}$ under addition modulo 4,

(5) the set $\{0, 1, 2, 3, 4, 5\}$ under addition modulo 6,

(6) the set $\{1, 2, 3, 4, 5\}$ under multiplication modulo 6,

(7) the set $\{1, 2, 5, 7\}$ under mutiplication modulo 8,

(8) the set $\{1, 5, 7, 11\}$ under mutiplication modulo 12,

(9) the set of non-negative integers under addition,

(10) the set of non-zero integers under multiplication,

(11) the set of positive rational numbers under multiplication,

(12) the set of 2×2 matrices excluding $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ under matrix multiplication,

(13) the set of matrices $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 7 \\ -3 & -5 \end{pmatrix}, \begin{pmatrix} -5 & -7 \\ 3 & 4 \end{pmatrix}\right\}$ under matrix multiplication.

5.2 Groups of permutations

DEFINITION 5.13 (permutation)

Permutation *is a bijective function from set* $\{1, 2, 3, \ldots, n\}, n \in \mathbb{N}$ *onto itself.*

EXAMPLE 5.14 (identity permutation)

$e : \{1, 2, 3, \ldots, n\} \longrightarrow \{1, 2, 3, \ldots, n\}$ *defined by* $e(x) = x$ *is the identity permutation.*

NOTATION.

A permutation $p : \{1, 2, 3, 4, 5\} \longrightarrow \{1, 2, 3, 4, 5\}$ *such that:*

$$p(1) = 3, p(2) = 4, p(3) = 1, p(4) = 5, p(5) = 2$$

is usually denoted as:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

DEFINITION 5.15 (cycle)

*A **cycle** of a permutation $p : \{1, 2, 3, \ldots, n\} \longrightarrow \{1, 2, 3, \ldots, n\}$ is a sequence $u_1, u_2, \ldots, u_k$, where:*

1. $\{u_1, u_2, u_3, \ldots, u_k\} \subseteq \{1, 2, 3, \ldots, n\}$
2. $u_m \neq u_s$ *for* $m \neq s$
3. $\forall\, m \in \{1, 2, 3, \ldots, k-1\}\ p(u_m) = u_{m+1}$ *and* $p(u_k) = u_1$

EXAMPLE 5.16 (cycles)

Permutation $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ *consists of two cycles:*

- $1 \to 3 \to 1$
- $2 \to 4 \to 5 \to 2$

NOTATION.

1. *Permutation* $p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$ *can be written in a **cycle** form:*

$$(1\ 3)\ (2\ 4\ 5)$$

2. *Permutation* $q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$ *can be written as*

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

Sometimes it is simplified to $(1\ 2\ 4)$*, i.e. cycles consisting of 1 element are ommited.*
The exception to this is the identity permutation $e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ *which is simply written as* (1) *or* $()$*.*

EXAMPLE 5.17 (group of permutations of 3 elements)

Let us consider a group S_3 *of permutations of three elements:* $\{1, 2, 3\}$*. The permutations are:*

permutation	*cycle notation*	
$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$(1)\ (2)\ (3)$	*or* (1) *or* $()$
$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$(1\ 2\ 3)$	
$p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$(1\ 3\ 2)$	
$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$(1)\ (2\ 3)$	*or* $(2\ 3)$
$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$(1\ 3)\ (2)$	*or* $(1\ 3)$
$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$(1\ 2)\ (3)$	*or* $(1\ 2)$

Permutations are composed in the same way as other functions. So for example:

$$p_4 p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{matrix} p_1 \\ \\ p_4 \end{matrix} \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = p_5$$

Similarly all other compositions can be obtained.
The table below shows all results.

$\circ$	e	p_1	p_2	p_3	p_4	p_5
e	e	p_1	p_2	p_3	p_4	p_5
p_1	p_1	p_2	e	p_5	p_3	p_4
p_2	p_2	e	p_1	p_4	p_5	p_3
p_3	p_3	p_4	p_5	e	p_1	p_2
p_4	p_4	p_5	p_3	p_2	e	p_1
p_5	p_5	p_3	p_4	p_1	p_2	e

Compare the table above with the one in example 5.10.
What can you see?

NOTATION.
S_n denotes a group of permutations of an n-element set $\{1, 2, \ldots, n\}$.

Questions

Q21. Consider the set of the following permutations:

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \qquad r = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$
$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} \qquad s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$
$$q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} \qquad t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

(i) Write the permutations in cycle form.

(ii) Show that the set forms a group under composition of permutations.

Q22. Find the smallest set of permutations of $\{1, 2, 3, 4\}$ that contains permutation (1 3 4) and that forms a group under composition of permutations.

Q23. Find the smallest set of permutations of $\{1, 2, 3, 4, 5\}$ that contains permutation ((1 2 5) (3 4)) and that forms a group under composition of permutations.

Q24. Permutation (1 2 3) $\in S_4$ is a 3-element cycle while permutation (2 3) $\in S_4$ is a 2-element cycle.

(i) How many 2-element cycles are there in S_4?

(ii) How many 3-element cycles are there in S_4?

(iii) How many 3-element cycles are there in S_5?

(iv) How many 3-element cycles are there in S_n, $n \geq 3$?

Q25. Let $p = (1\ 3\ 4)(2\ 5)$ and $q = (2\ 5\ 4)$ be elements of S_5.

(i) Express both p and q as a composition of 2-element cycles (i.e. cycles like (1 2) where only 2 elements swap).

(ii) Is the composition unique? Why?

5.3 Order of an element, order of a group

DEFINITION 5.18 (order of a group)
order of a group
The **order** *of a finite group $(G, *)$ is the number of elements of set G.*

NOTATION.
Ord(G) or $|G|$

DEFINITION 5.19 (order of an element)
order of an element
The **order** *of an element a of a group $(G, *)$ is the* ***smallest positive*** *integer n such that $a^n = e$, where e is the identity.*

NOTATION.
ord(a) or $|a|$

PROPERTIES.

- $ord(a) = 1 \Leftrightarrow a = e$
- $ord(a) = 2 \Leftrightarrow a^{-1} = a$
- $ord(a) = Ord(G) \Leftrightarrow \forall\, b \in G\ \exists\, n \in \mathbb{N}\ b = a^n$

EXAMPLE 5.20 (orders)

- *In a group of symmetries of an equilateral triangle (example 5.10):*
  - $ord(I) = 1$
  - $ord(R_{120}) = ord(R_{240}) = 3$
  - $ord(S_1) = ord(S_2) = ord(S_3) = 2$
- *In a group of permutations of three elements (example 5.17):*

permutation	*cycle notation*	*order*
$e = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	(1) (2) (3)	*1*
$p_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	(1 2 3)	*3*
$p_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	(1 3 2)	*3*
$p_3 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	(1) (2 3)	*2*
$p_4 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	(1 3) (2)	*2*
$p_5 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	(1 2) (3)	*2*

- *the order of a permutation* $\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&1&5&4&7&8&6\end{pmatrix} = ((1\ 2\ 3)\ (4\ 5)\ (6\ 7\ 8))$ *is equal to* $LCM(2,3) = 6$.
- *in a group of* $\{0,1,2,3,4\}$ *under addition modulo 5:*
  - *ord* $0 = 1$,

– $ord\ 1 = ord\ 2 = ord\ 3 = ord\ 4 = 5$

- *in a set of* $\{1, \omega, \omega^2\}$ *- complex roots of unity under multiplication:* $ord\ 1 = 1, ord\ \omega = ord\ \omega^2 = 3$

THEOREM 5.21 (order of inverse)
Let a *be an element of group* $(G, *)$*. Then* $ord\ (a) = ord\ (a^{-1})$.

PROOF. Let $n = ord\ (a)$. Then n is the smallest positive integer such that $a^n = e$, the identity. Hence:

$$e = e^n = (a * a^{-1})^n \overset{(*)}{=} a^n * (a^{-1})^n = e * (a^{-1})^n = (a^{-1})^n$$

(Why does the equality $(*)$ hold?)
It shows that $(a^{-1})^n = e$, so the order of a^{-1} is n or a factor of n. However, if $ord\ (a^{-1}) = k < n$ then analogically to the method above we can show that $a^k = e$ which contradicts the assumption that n is the smallest positive integer such that $a^n = e$. □

Questions

Q26. Find the order of the pointed element in the given set under the given operation.

set	**operation**	**element**
$\{1, i, -1, -i\}$	multiplication	i
$\left\{1, -\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right\}$	multiplication	$-\frac{1}{2} + i\frac{\sqrt{3}}{2}$
$\left\{\pm 1, \pm\left(\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right)\right\}$	multiplication	$\frac{1}{2} - i\frac{\sqrt{3}}{2}$
$\{0, 1, 2, 3\}$	addition modulo 4	3
$\{0, 1, 2, 3, 4, 5\}$	addition modulo 6	3
$\{1, 5, 7, 11\}$	mutiplication modulo 12	7
$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}4 & 7\\ -3 & -5\end{pmatrix}, \begin{pmatrix}-5 & -7\\ 3 & 4\end{pmatrix}\right\}$	matrix multiplication	$\begin{pmatrix}4 & 7\\ -3 & -5\end{pmatrix}$

Q27. What is the order of function $f(x) = \frac{3x-7}{9x+6}$ under composition of functions?

Q28. What is the order of function $f(x) = \frac{-3x-7}{x+2}$ under composition of functions?

Q29. Find the orders of all elements of the group of symmetries of a square shown in example 5.11.

Q30. Find the order of the permutations $p = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 2 & 4 & 7 & 5 & 1 & 6 & 3 & 8\end{pmatrix}$ and $q = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 4 & 8 & 6 & 7 & 5 & 3 & 1 & 2\end{pmatrix}$ under composition of permutations.

Q31. The operation $*$ is defined on set $S = \{1, 2, 3, 4\}$ by the following table.

$*$	1	2	3	4
1	2	4	1	3
2	4	3	2	1
3	1	2	3	4
4	3	1	4	2

(i) State the identity element and the inverse of each element.
(ii) Find the order of each element.
(iii) Find the solutions of the equations.

I. $x * x = 3$
II. $x * (x * 1) = 4$

Consider also set $T = \{1, i, -1, -i\}$ under multiplication.

(iv) Find the order of each element of T.

(v) Make up a bijective function $f : S \longrightarrow T$ such that for every $s \in S$ $ordf(s) = ord\ s$.

(vi) Construct an operation table for T arranging the elements of T in the following order: $f(1), f(2), f(3), f(4)$.

(vii) What can you say about the two operation tables?

Q32. Let $\mathbb{Z}_n$ denote the set of integers $\{0, 1, 2, \ldots, n-1\}$. For $x, y \in \mathbb{Z}_n$ let us define operations $\oplus_n$ and $\otimes_n$ by

$$x \oplus_n y = x + y \mod n$$
$$x \otimes_n y = x \times y \mod n.$$

(i) Write down the operation tables for $\mathbb{Z}_5$ under both operations.

(ii) Show that $\mathbb{Z}_5$ under $\oplus_5$ is a group and that $\mathbb{Z}_5$ under $\otimes_5$ is not.

(iii) Which number should be removed from $\mathbb{Z}_5$ so that the remaining set froms a group under $\otimes_5$?

(iv) Does $\mathbb{Z}_4$, with the same number removed and under operation $\otimes_4$ form a group? Why?

(v) What are the orders of:

1. $3 \in \mathbb{Z}_5$ under $\oplus_5$?
2. $3 \in \mathbb{Z}_5$ under $\otimes_5$?
3. $3 \in \mathbb{Z}_8$ under $\oplus_8$?

(vi) Show that $\mathbb{Z}_9$ has only one proper subgroup.

Q33. Let $(G, *)$ be a group, where $G = \{e, a, b, c\}$, $ord\ (e) = 1$ and $ord\ (a) = ord\ (b) = ord\ (c) = 2$. Create the group table.

5.4 Cyclic groups

DEFINITION 5.22 (generator)

*A **generator** of a **finite** group G is an element a of the group such that all other elements of G can be written as a^n where n is a positive integer.* [1]
*More generally, a **generator** of a group G is an element a such that the smallest subgroup of G containing a is the whole group.*

DEFINITION 5.23 (cyclic group)

*A **cyclic** group is one that contains a generator.*

EXAMPLE 5.24 (cyclic groups)

- *If $G = \{e, g, g^2, g^3, g^4, g^5\}$ where $g^6 = e$ is the identity then G is cyclic.*
- *G shown above is the same as $\{0, 1, 2, 3, 4, 5\}$ under addition modulo 6.*
- *The group of n^{th} roots of unity - cyclic group of order n.*
- *Rotations of n-sided polygon - cyclic group of order n.*

[1] Or an for additive notation.

- $G = \{e, g, g^2, g^3, \ldots, g^{n-1}\}$ *where* $g^n = e$ *is the identity is a cyclic group of order* n.

PROPERTIES.

- *Every cyclic group* G *is* isomorphic *(essentially the same) as:*
  $\mathbb{Z}_n = (\{0, 1, 2, \ldots, n-1\},$ *addition modulo* $n)$ *when* G *is finite or*
  $\mathbb{Z}$, *the additive group of all integers* *when* G *is infinite.*

- *One of generators of* $\mathbb{Z}_n$ *is 1. The group* $\mathbb{Z}$ *has 2 generators:* 1 *and* -1.

THEOREM 5.25 (cyclic and Abelian groups)
All cyclic groups are Abelian.

PROOF. Let $(G, *)$ be a cyclic group with generator g. Let $a, b \in G$. Then

$$\begin{aligned} \exists m, k \in \mathbb{Z}^+ : \quad & a = g^m \\ \text{and} \quad & b = g^k \end{aligned}$$

and hence:

$$\begin{aligned} a * b = g^m * g^k = \\ = g^{m+k} = \text{ (associativity)} \\ = g^k * g^m = \\ = b * a \end{aligned}$$

□

Questions

Q34. Let $\mathbb{Z}_8$ be the group of numbers $\{0, 1, 2, 3, 4, 5, 6, 7\}$ under $\oplus$ - addition modulo 8. Complete the following table. In the first row of the table circle the generators of $\mathbb{Z}_8$.

a	0	1	2	3	4	5	6	7
a^2								
a^3								
a^4								
a^5								
a^6								
a^7								
a^8								
ord a								

List all possible subgroups of $\mathbb{Z}_8$ with the following orders. In each subgroup circle its generators.

1: .....

2: .....

3: .....

4: .....

6: .....

8: .....

Q35. Consider set $\mathbb{Z}_2 \times \mathbb{Z}_3$ with operation $\square$ defined:

$$(a,b)\square(c,d) = ((a+c) \mod 2, (b+d) \mod 3)$$

(i) Prove that set $\mathbb{Z}_2 \times \mathbb{Z}_3$ forms a group under $\square$. Show a group table.

(ii) State orders of all elements.

(iii) Is the group cyclic? List all generators.

(iv) Solve the equation $(1,2)\square(x,y) = (0,1)$.

5.5 Subgroups

DEFINITION 5.26 (subgroup)
*Given a group $(G,*)$ we say that a subset H of G is a **subgroup** of G if H also forms a group under $*$.*

DEFINITION 5.27 (proper subgroup)
*A subgroup $H \subseteq G$ is called **proper** when $H \neq \{e\}$ and $H \neq G$.*

THEOREM 5.28 (subgroup of a cyclic group)
A subgroup of a cyclic group is cyclic, too.

PROOF. Let G be a group and $H \subseteq G$ its subgroup. Let g be a generator of G. As all elements of G but e, the identity can be expressed as positive integer powers of g or their inverses, so do all elements of H. Let k be the smallest positive integer such that $g^k \in H$. We will show that g^k is a generator in H, i.e. for any $x \in H$ if $x \neq e$ then there exists $m \in \mathbb{Z} \setminus \{0\}$ such that $x = (g^k)^m$.
Let us assume otherwise. Then there exists $x \in H$ such that $x \neq e$ and $x = g^s, s \in \mathbb{Z}$ (as $x \in G$) but s is not divisible by k.
Let $r = s \mod k, r \neq 0$. As $g^s \in H$ and $g^k \in H$ so $(g^k)^{-1} \in H$ and in consequence (by closure) $g^r \in H$. However $r = s \mod k$, so $0 < r < k$ which contradicts the assumption that k was the smallest positive integer such that $g^k \in H$. Such r and s cannot therefore exist. $\square$

EXAMPLE 5.29 (subgroup of $\mathbb{Z}_6$)

- *$\{0,2,4\}$ is a subgroup of $\{0,1,2,3,4,5\}$ under addition modulo 6.*
- *$\{0,2,4\}$ under addition modulo 6 is isomorphic (essentially the same) as $\{0,1,2\}$ under addition modulo 3.*

EXAMPLE 5.30 (subgroup of $\mathbb{Z}_8$)
Consider $\mathbb{Z}_8$ i.e. the set $\{0,1,2,3,4,5,6,7\}$ under $\oplus$ - addition modulo 8. Rearrainging the order of elements of the set into $\{0,2,4,6,1,3,5,7\}$ the following Cayley table can be formed:

$\oplus$	0	2	4	6	1	3	5	7
0	0	2	4	6	1	3	5	7
2	2	4	6	0	3	5	7	1
4	4	6	0	2	5	7	1	3
6	6	0	2	4	7	1	3	5
1	1	3	5	7	2	4	6	0
3	3	5	7	1	4	6	0	2
5	5	7	1	3	6	0	2	4
7	7	1	3	5	0	2	4	6

This group has two proper subgroups: $J = \{0,4\}$ and $H = \{0,2,4,6\}$, where J is also a subgroup of H. The Cayley table for H is the top-left quadrant of the Cayley table for G. The group G is cyclic, and so are its subgroups.

EXAMPLE 5.31 (Alternating groups)
The example is not very important for our course, it will be shown, however, as it can serve as an illustration of the Lagrange's theorem (5.51).
$A_n \subseteq S_n$ is the subgroup of even *permutations of n elements. A permutation is even when it can be expressed as a composition of an even number of 2-element cycles. It can be shown that:*

1. *although such a composition is not unique, an even permutation cannot be expressed as a composition of an odd number of 2-element cycles,*
2. *the number of odd permutations is equal to the number of even premutations, i.e.* $n(A_n) = \frac{n(S_n)}{2} = \frac{n!}{2}$,
3. $A_3 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$.

Try to show that A_3 is as shown above. Can you see why A_3 is a subgroup of S_3 (or more generally A_n is a subgroup of S_n). Why a set of odd permutations is not a group?

5.5.1 Subgroup tests

THEOREM 5.32 (subgroup test 1)
Suppose G is a group and H is a ***non-empty*** *subset of G. H is a subgroup of G if*

$$ab^{-1} \in H \text{ whenever } a, b \in H. \qquad (*)$$

PROOF. For the proof we have to check that the frour axioms of a group hold for H.

1. As $H \neq \emptyset$, there exists $a \in H$. Applying $(*)$ for a and a: $aa^{-1} = e \in H$, so there is the **identity** in H.
2. Applying $(*)$ for e and a: $ea^{-1} = a^{-1} \in H$, so for every $a \in H$ its **inverse** is in H, too.
3. From **2.** if $a, b \in H$ then $a^{-1}, b^{-1} \in H$.
   Thus applying $(*)$ for a and b^{-1}: $a(b^{-1})^{-1} = ab \in H$, so for $a, b \in H$, $ab \in H$, too, which shows **closure**.
4. The operation in group G is **associative**, so it is in a subset.

Hence, as all four axioms hold for H, H is a group. □

THEOREM 5.33 (subgroup test 2)
Suppose G is a ***finite*** *group and H is a* ***non-empty*** *subset of G. H is a subgroup of G if H is* ***closed*** *under the group operation.*

PROOF. As H is non-empty, let $a \in H$. Let $n = n(H)$.
Let $T = \{a, a^2, a^3, \ldots, a^n, a^{n+1}\}$.
H is closed $\therefore T \subseteq H$ and thus $n(T) \leq n$.
Therefore there are k and m such that:

$$\begin{aligned} & 1 \leq k < m + k \leq n + 1 \\ \text{and} \qquad & a^k = a^{m+k} \\ & a^k = a^m a^k \\ & a^m = e \text{ - identity in } G. \end{aligned}$$

As $1 \leq m \leq n$, $e = a^m \in T \therefore e \in H$. **(1)**
As $e = a^m = aa^{m-1}, a^{-1} = a^{m-1} \in H$ **(2)**
The group operation is associative and **(3)**
H is closed under the operation **(4)**
therefore conditions **(1)**-**(4)** show that all axioms of the group are fulfilled for H. □

Questions

Q36. Find all proper subgroups of the group of symmetries of a triangle described in example 5.10.

Q37. Find all proper subgroups of the group of symmetries of a square described in example 5.11.

Q38. List all subgroups of $\mathbb{Z}_{12}$.

Q39. Consider set $S^1 = \{z \in \mathbb{C} |\ |z| = 1\}$.

(i) Show that S^1 forms a group under multiplication.

(ii) Show that $G = \{z \in S^1 |\ \arg(z) = \frac{k\pi}{20}, k \in \mathbb{Z}\}$ is a subgroup of S^1.

(iii) Show that $H = \{z \in S^1 |\ \arg(z) \in \mathbb{Q}\}$ is a subgroup of S^1.

Q40. Consider S_5, a group of permutations of 5 elements. Let G, subset of S_5 consist of permutations that permute numbres $\{1, 2, 3\}$ and $\{4, 5\}$. (i.e. no number from $\{1, 2, 3\}$ changes into 4 or 5.)

(i) Find $n(G)$.

(ii) Is G a subgroup of S_5?

Q41. Suppose G is a group and H is a **non-empty** subset of G. Show that H is a subgroup of G if $ab^{-1} \in H$ whenever $a, b \in H$.

Q42. Suppose G is a **finite** group and H is a **non-empty** subset of G. Show that H is a subgroup of G if H is **closed** under the group operation.

5.6 Cosets

DEFINITION 5.34 (coset)

Let G be a group and H be a subgroup of G.
Let g be an element of G. Then

$$gH = \{gh |\ h \in H\} \text{ is a } \textbf{left } H\textbf{-coset } \text{of } g \text{ in } G \text{ and}$$
$$Hg = \{hg |\ h \in H\} \text{ is a } \textbf{right } H\textbf{-coset } \text{of } g \text{ in } G.$$

g is called a ***representative*** *of a coset.*

NOTATION.

G/H - a set of left H-cosets
$H\backslash G$ - a set of right H-cosets

PROPERTIES.

- *H is both left and right H-coset of e, as $H = eH = He$,*
- *if $g \in H$ then $gH = Hg = H$,*
- *if $gH = H$ or $Hg = H$ then $g \in H$.*

EXAMPLE 5.35 (cosets in $\mathbb{Z}$)

Let $H = 3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$ be a subgroup of $\mathbb{Z}$. Then $2 + H = 5 + H = H + 5 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$. In fact, for every $n \in \mathbb{Z}$, $n + H = H + n$ as addition is commutative.
***Note**, that additive notation was used in the example, not multiplicative (i.e. $n + H$ instead of nH).*

EXAMPLE 5.36 (cosets in a group of symmetries of a triangle)
Let $G = \{I, R_{120}, R_{240}, S_1, S_2, S_3\}$ be the group of symmetries of an equilateral triangle discussed in example 5.10. Let us consider a subgroup $H = \{I, R_{120}, R_{240}\}$ of G. Then:

- $R_{120}H = H$
- $HR_{120} = H$
- $S_1H = \{S_1, S_2, S_3\}$
- $HS_1 = \{S_1, S_2, S_3\}$

***Note**, that $S_1H = HS_1$ which is not always the case. Consider a subgroup $K = \{I, S_1\}$. Then:*

- $R_{120}K = \{R_{120}, S_3\}$
- $KR_{120} = \{R_{120}, S_2\}$

EXAMPLE 5.37 (cosets in S_3 - group of permutations)
Let S_3 be a group of permutations of 3 elements described in example 5.17.
Let $H = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}$. Let $p = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ and $q = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$. Then:

- $pH = \left\{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\}$,
- $Hp = \left\{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}$,
- $qH = \left\{\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\}$.

It can be observed that:

- *$pH \neq Hp$ so an element can have different left and right H-cosets,*
- *$pH = qH$ so different elements can have the same left H-cosets,*
- *cosets are usually not subgroups.*

THEOREM 5.38 (cosets in Abelian groups)
If G is an Abelian group, $H \subseteq G$ is a subgroup and $g \in G$ then the left coset of H in G is the same as the right coset of H in G, i.e. $gH = Hg$.

PROOF. G is Abelian, so $gh = hg$ for every $g, h \in G$. Hence:
$gH = \{gh |\ h \in H\} = \{hg |\ h \in H\} = Hg$ □

NOTATION.
For additive groups (i.e. groups under addition) additive notation is usually used:

- *$g + H$ instead of gH,*
- *$H + g$ instead of Hg.*

EXAMPLE 5.39 (cosets in $\mathbb{Z}_9$)
Let $G = \mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ under $\oplus$ addition modulo 9.
Let $H = \{0, 3, 6\}$. Then:

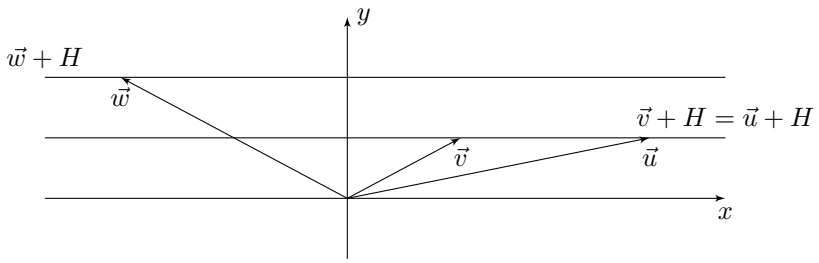
$$\begin{array}{lcl} 0 + H = 3 + H = 6 + H = & H & = H + 6 = H + 3 = H + 0 \\ 1 + H = 4 + H = 7 + H = & \{1, 4, 7\} & = H + 7 = H + 4 = H + 1 \\ 2 + H = 5 + H = 8 + H = & \{2, 5, 8\} & = H + 8 = H + 5 = H + 2 \end{array}$$

EXAMPLE 5.40 (cosets in vector group $\mathbb{R}^2$)

Let $\mathbb{R}^2$ be the vector group described in example 5.8.
Let $H = \{x\vec{i} \mid x \in \mathbb{R}\}$ be the x-axis.
The left H-cosets of $\vec{v} \in \mathbb{R}^2$ is

$$\vec{v} + H = \{\vec{v} + k\vec{i} \mid k \in \mathbb{R}\},$$

which is a line parallel to the x-axis (see the diagram below).



EXAMPLE 5.41 (solutions of systems of linear equations)

Consider a system of m linear equations of n variables. The system can be written in the form $A\vec{x} = \vec{b}$ where A is an $m \times n$ matrix, $\vec{b} \in \mathbb{R}^m$ and $\vec{x} \in \mathbb{R}^n$ is an unknown vector.
Let us consider the solution set of an equation where the right side equals $\vec{0}$:

$$H = \{\vec{x} \in \mathbb{R}^n \mid A\vec{x} = \vec{0}\}.$$

H is a group under vector addition, so a subgroup of $\mathbb{R}^n$.
Now, if $\vec{x}_0$ is a solution of $A\vec{x} = \vec{b}$, the general solution is a coset $\vec{x}_0 + H$ in $\mathbb{R}^n$, as:

$$\begin{aligned} A\vec{x} = \vec{b} &\Leftrightarrow A\vec{x} = A\vec{x}_0 \\ &\Leftrightarrow A(\vec{x} - \vec{x}_0) = \vec{0} \\ &\Leftrightarrow \vec{x} - \vec{x}_0 \in H \\ &\Leftrightarrow \vec{x} \in \vec{x}_0 + H. \end{aligned}$$

EXAMPLE 5.42 (illustration of example 5.41)

Let $A = \begin{pmatrix} 2 & 4 & -1 \\ 3 & 1 & -2 \end{pmatrix}$ *and* $\vec{b} = \begin{pmatrix} 3 \\ 8 \end{pmatrix}$.
Let us consider a system of equations:

$$\begin{cases} 2x + 4y - z = 3 \\ 3x + y - 2z = 8 \end{cases}$$

which can be written in a matrix form:

$$\begin{pmatrix} 2 & 4 & -1 \\ 3 & 1 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 8 \end{pmatrix}$$
$$\Leftrightarrow \quad A\vec{x} = \vec{b}$$

Now $\vec{x}_0 = \begin{pmatrix} 5 \\ -1 \\ 3 \end{pmatrix}$ *is a solution of*

$$A\vec{x} = \vec{b},$$

while the solutions of $A\vec{x} = \vec{0}$ are $H = \left\{ k \begin{pmatrix} 7 \\ -1 \\ 10 \end{pmatrix} \middle| \; k \in \mathbb{R} \right\}$, *so all solutions of $A\vec{x} = \vec{b}$ are*

$$\vec{x}_0 + H = \left\{ \begin{pmatrix} 5 \\ -1 \\ 3 \end{pmatrix} + k \begin{pmatrix} 7 \\ -1 \\ 10 \end{pmatrix} \middle| \; k \in \mathbb{R} \right\}$$

THEOREM 5.43 (intersection of cosets)

- *If two left H-cosets have a common element, then they are equal*
- *Two left H-cosets that are not equal are disjoint, i.e. have no common element.*

PROOF. Let $x \in g_1H$ and $x \in g_2H$, i.e. there are $h_1, h_2 \in H$ such that

$$x = g_1h_1 = g_2h_2$$

This implies $g_1 = g_2h_2h_1^{-1}$.
Let us take any $h \in H$ and consider an element g_1h of g_1H:

$$g_1h = (g_2h_2h_1^{-1})h = g_2(h_2h_1^{-1}h) \in g_2H$$

Thus $g_1H \subseteq g_2H$. Analogically, $g_2H \subseteq g_1H$. □

THEOREM 5.44 (left coset as right coset)

Let G be a group, H its subgroup and $g \in G$.
There exists a subgroup $K \subseteq G$ such that $gH = Kg$.

PROOF. $gH = gHe = gH(g^{-1}g) = (gHg^{-1})g$, so let $K = gHg^{-1}$.
We will show that K is a group.
As associativity is obvious, we are to prove that K is closed, $e \in K$ and if $g \in K$ then $g^{-1} \in K$, too.

Closure.
Let $a, b \in K$.
Then there exist $a_1, b_1 \in H$ such that:

$$a = ga_1g^{-1}$$
$$b = gb_1g^{-1}$$

Then
$ab = (ga_1g^{-1})(gb_1g^{-1}) = ga_1(g^{-1}g)b_1g^{-1} = ga_1(e)b_1g^{-1} = ga_1b_1g^{-1} = g(a_1b_1)g^{-1}$
As H is a group, $a_1b_1 \in H$, so $ab = g(a_1b_1)g^{-1} \in gHg^{-1} = K$.
Identity.

$$\begin{aligned} e \in H, \text{ so } geg^{-1} &\in K \\ \therefore gg^{-1} &\in K \\ \therefore e &\in K \end{aligned}$$

Inverse.
If $a \in K$ then $a = ghg^{-1}$ for a certain $h \in H$.

$$\begin{aligned} \text{And then } a^{-1} &= (ghg^{-1})^{-1} = \\ &= (g^{-1})^{-1}(h)^{-1}(g)^{-1} = \qquad (\text{as } (ab)^{-1} = b^{-1}a^{-1} \text{ (theorem 4.16)}) \\ &= (g)h^{-1}(g^{-1}) \end{aligned}$$

As $h^{-1} \in H$, $a^{-1} = (g)(h^{-1})(g^{-1}) \in K$. □

THEOREM 5.45 (coset as an equivalence class)

Let G be a group and H its subgroup.
There exists an equivalence relation R on G such that for every $x, y \in G$:

$$xRy \Leftrightarrow (\exists\ g \in G :\ x, y \in gH)$$

COROLLARY 5.46

Let G be a group and H its subgroup. Then the (distinct) left cosets of H in G form a partition of G, i.e.

1. $\forall\ g_1, g_2 \in G\ (g_1 \neq g_2) \Rightarrow (g_1 H \cap g_2 H = \emptyset)$

2. $\bigcup_{g \in G} gH = G$ *(i.e.* $\forall\ a \in G\ \exists\ g \in G :\ a \in gH$*)*

Proof of theorem 5.45. Let $\sim$ be relation on G defined by:

$$x \sim y \ \Leftrightarrow\ x^{-1}y \in H$$

We will show that $\sim$ is an equivalence relation and then that $\sim$ is actually the same relation as R.
Firstly, $\sim$ is **reflexive**, as

$$\forall\ x \in G\ x^{-1}x = e \in H, \text{ so } x \sim x$$

Secondly, $\sim$ is **symmetric**, as if $x, y \in G$

$$(x \sim y) \Leftrightarrow (x^{-1}y \in H) \Leftrightarrow ((x^{-1}y)^{-1} \in H) \Leftrightarrow (y^{-1}x \in H) \Leftrightarrow (y \sim x)$$

Thirdly, $\sim$ is **transitive**, as if $x, y, z \in G$

$$(x \sim y) \wedge (y \sim z) \Leftrightarrow (x^{-1}y, y^{-1}z \in H) \Rightarrow ((x^{-1}y)(y^{-1}z) \in H) \Rightarrow (x^{-1}(yy^{-1})z \in H) \Rightarrow (x^{-1}z \in H) \Rightarrow (x \sim z)$$

It should be now shown that

$$(x^{-1}y \in H) \Leftrightarrow\ (\exists\ g \in G :\ x, y \in gH) \tag{5.1}$$

Let us then see that:

$$\begin{aligned} &\exists\ g \in G :\ x, y \in gH \\ \Leftrightarrow\ &\exists\ g \in G, h_x, h_y \in H :\ x = gh_x, y = gh_y \\ \Leftrightarrow\ &\exists\ g \in G, h_x, h_y \in H :\ x^{-1} = (h_x)^{-1}g^{-1}, y = gh_y \end{aligned}$$

And then

$$x^{-1}y = (h_x)^{-1}g^{-1}gh_y = (h_x)^{-1}h_y$$

As both $(h_x)^{-1} \in H$ and $h_y \in H$, $x^{-1}y \in H$, which shows the $\Leftarrow$ implication of (5.1).
For the $\Rightarrow$ implication of (5.1) let us firstly see that

$$(x^{-1}y \in H) \Leftrightarrow ((x^{-1}y)^{-1} \in H) \Leftrightarrow (y^{-1}x \in H) \tag{5.2}$$

Let us now consider any element $h \in H$. Let

$$g = yh^{-1}. \tag{5.3}$$

Then $g^{-1} = hy^{-1}$ and hence

$$g^{-1}x = hy^{-1}x. \tag{5.4}$$

We obtained therefore:

$$\begin{cases} y = gh & \text{from (5.3)} \\ x = ghy^{-1}x & \text{from (5.4)} \end{cases} \tag{5.5}$$

As by (5.2) $y^{-1}x \in H$, so does $hy^{-1}x \in H$. Let $h_2 = hy^{-1}x \in H$ and let us rearrange (5.5) into

$$\begin{cases} y = gh & \text{where } g \in G, h \in H \\ x = gh_2 & \text{where } h_2 \in H \end{cases}$$

which finishes the proof of the $(\Rightarrow)$ implication of equivalence (5.1). □

EXAMPLE 5.47 (cosets in $\mathbb{Z}$ as equivalence classes)
Let $H = 3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$ be a subgroup of $\mathbb{Z}$.
Consider relation defined for $a, b \in \mathbb{Z}$ as:

$$a \equiv b(\mod 3) \Leftrightarrow (3|(a-b))$$

The H-cosets in $\mathbb{Z}$ are equivalence classes of the relation:

$$\begin{aligned} 0 + H &= \{\dots, -6, -3, 0, 3, 6, \dots\} = [0], \\ 1 + H &= \{\dots, -5, -2, 1, 4, 6, \dots\} = [1], \\ 2 + H &= \{\dots, -4, -1, 2, 5, 7, \dots\} = [2]. \end{aligned}$$

***Note** that*

$$\mathbb{Z} = (0 + H) \cup (1 + H) \cup (2 + H).$$

A similar example can be shown for congruence modulo relation in $\mathbb{Z}_n$.

EXAMPLE 5.48 (partition of vector group $\mathbb{R}^2$)
Let $\mathbb{R}^2$ be the vector group defined in example 5.8. Let H be the x-axis, the subgroup with cosets shown in example 5.40. Then:

$$\mathbb{R}^2 = \bigcup_{k \in \mathbb{R}} \left(\begin{pmatrix} 0 \\ k \end{pmatrix} + H \right)$$

THEOREM 5.49 (left coset size)
Let H be a subgroup of the group G.
For every $g \in G$ there exists a bijection $f : gH \longrightarrow H$.
In particular, when H is finite,

$$n(gH) = H.$$

COROLLARY 5.50 (right coset size)
A similar theorem can be formed for right cosets.

PROOF OF THEOREM 5.49. The function f can be defined as follows:
for $gh \in gH$, $f(gh) = g^{-1}gh = (g^{-1}g)h = h \in H$. The function is a bijection (why?) whose inverse is defined as $f^{-1}(h) = gh$. □

Questions

Q43. For $H = \{0, 4, 8\}$ list all H-cosets in $\mathbb{Z}_{12}$.

Q44. Let $H = \{I, S_1\}$ be a subgroup of the group of symmetries of an equilateral triangle from example 5.10. List all:

(i) left H-cosets,

(ii) right H-cosets.

Q45. Let $K = \{I, R_{180}, V, H\}$ be a subgroup of the group of symmetries of a square from example 5.11. List all:

(i) left K-cosets,

(ii) right K-cosets.

Q46. Let G be the multiplicative group of complex solutions of the equation $z^6 = 1$. Let H be a set of solutions of $z^3 = 1$.

(i) Show that H is a subgroup of G.

(ii) Find all H-cosets in G.

(iii) Define an equivalence relation whose equivalence classes are H-cosets.

Q47. Let G be a set of functions $\{x \mapsto x, x \mapsto -x, x \mapsto \frac{1}{x}, x \mapsto -\frac{1}{x}\}$. Let H be a subset of G: $H = \{x \mapsto x, x \mapsto -x\}$.

(i) Show that G is a group and H its subgroup.

(ii) Find all H-cosets in G.

(iii) Define an equivalence relation whose equivalence classes are H-cosets.

Q48. Consider the multiplicative group of non-zero real numbers $(\mathbb{R} \setminus \{0\}, \times)$.

(i) Show that $\mathbb{Q} \setminus \{0\}$, $\mathbb{R}^+$ and $\mathbb{Q}^+$ are subgroups of the group.

(ii) Find all cosets of $\mathbb{R}^+$.

(iii) Show that the relation S defined on $\mathbb{R} \setminus \{0\}$ by

$$xSy \;\Leftrightarrow\; xy > 0$$

is an equivalence relation.

(iv) Show that the cosets of $\mathbb{R}^+$ are the equivalence classes of S.

Q49. Let $H = \{0, 3, 6, 9\}$ be a subgroup of $\mathbb{Z}_{12}$. Define an equivalence relation whose classes are H-cosets in $\mathbb{Z}_{12}$.

Q50. Let S_3 be a group of permutations of 3 elements. Let $H = \{(1), (1\ 2)\}$.

(i) Copy the table below and complete it with all left and right H-cosets.

g	gH	Hg
(1)		
(12)		
(13)		
(23)		
(123)		
(132)		

(ii) Define an equivalence relation whose classes are equal to left H-cosets.

5.7 Lagrange's theorem

THEOREM 5.51 (Joseph-Luis Lagrange, 1770)
The order of any subgroup is a factor of the order of the group itself.

Note. Lagrange did not prove the theorem. He discussed some special cases. The theorem was proven by Carl Friedrich Gauss in 1801.

COROLLARY 5.52 (to Lagrange's theorem)
The order of any element is a factor of the order of the group.

PROOF OF LAGRANGE'S THEOREM (THEOREM 5.51).
The full proof will not be shown here. It is based on the observation that

$$n(G) = n(G/H) \times n(H).$$

To prove the above one needs to show that for any $g \in G$ and H - subgroup of G: $n(gH) = n(H)$. This can be proven by showing that a function between two H-cosets $f : aH \mapsto bH$, where $a, b \in G$ defined by $f(x) = ba^{-1}x$ is bijective. □

PROOF OF COROLLARY TO LAGRANGE'S THEOREM (COROLLARY 5.52).
Let n be the order of an element a of a group $(G, *)$, that is $a^n = e$.

Consider a set $H = \{e, a, a^2, a^3, \ldots, a^{n-1}\}$.
H is a cyclic subgroup of G. The order of H is n.
From Lagrange's theorem n is a factor of $n(G)$. □

THEOREM 5.53 (groups of prime order)
Let $(G, *)$ be a group such that $n(G) = p$ is prime. Then:

1. *G is cyclic,*
2. *G has no proper subgroups,*
3. *G is Abelian.*

PROOF. The group has p elements out of which exactly one (the identity) is of order 1. By corollary 5.52 all other elements are of order p. It means they are generators, so G is cyclic and hence (by theorem 5.25) Abelian.
Then by Lagrange's theorem (5.51) any subgroup is either of order 1 or p, i.e. there are no proper subgroups. □
Note.
Be carefull with groups under operations modulo p, the prime number. While $\mathbb{Z}_p$, the additive groups are cyclic, the theorem says nothing about the multiplicative group, as its order is $p - 1$.

EXAMPLE 5.54 (orders of subgroups)

- *Group of permutations of 3 elements is of order 6 ($3! = 6$).*
  Possible orders of elements of the group are 1, 2, 3 and 6.
  (Find elements of the order 1, 2 and 3. Why there is no element of the order 6?)
- *Possible orders of subgroups and elements of the group $\mathbb{Z}_8$ are 1, 2, 4, 8. There are proper subgroups of the order 1, 2 and 4. There are elements of the order 1, 2, 4, 8.*

EXAMPLE 5.55 (converse of Lagrange's theorem)
The Lagrange's theorem states that an order of a subgroup divides the order of the group.
The question is:

given a factor of the order of the group,
is there a subgroup of that size?

No, not always. Although it is true for some groups (including all cyclic groups) but false in general.
The smallest counterexample is the alternating group $A_4 \subseteq S_4$, of even permutations of 4 elements (see example 5.31). It does have subgroups of order 1, 2, 3, 4 and 12 but there is no subgroup of order 6.
Suppose otherwise, that H is a subgroup of A_4 of order 6. We will show that squares of all elements from A_4 are in H. Let g be any element of A_4.

- *if $g \in H$ then obviously $g^2 \in H$, too, as H is a subgroup, so the operation is closed on H,*
- *if $g \notin H$ then $gH \neq H$. As $n(H) = 6$ so $n(gH) = 6$ (by theorem 5.49). Then (by theorem 5.43) H and gH are disjoint. As $n(A_4) = 12$ these are the only H-cosets. In consequence either $g^2 \in gH$ or $g^2 \in H$. If $g^2 \in gH$ then $g \in H$ which contradicts the assumption. Thus finally $g^2 \in H$.*

Having shown that squares of all elements from A_4 are in H, we can calculate the number of squares. Firstly, the identity is a square (of itself). Secondly, all 3-element cycles are squares (i.e. $(a\ b\ c) = (a\ c\ b)^2$). The number of 3-cycles in A_4 is 8 (why?). Finally, there are at least 9 elements of H, so $n(H)$ cannot be 6.

Note. Although it can be shown that A_n does not have a subgroup o order $\frac{1}{2}n(A_n) = \frac{n!}{4}$, there is no simple distinction between the groups that satisfy the converse of the Lagrange's theorem and these that do not.

THEOREM 5.56 (binomial coefficients are integers)
Let $n \geq 1$ and $0 \leq r \leq n$. Then the ratio

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

is an integer.

PROOF. The theorem obviously works for $r = 0$ and $r = n$. We will show it for $0 < r < n$.
Let us consider a subset of S_n, a group of permutations that consist of permutations that permute $\{1, 2, \ldots, r\}$ and $\{r+1, \ldots, n\}$. There are $r!(n-r)!$ such permutations.
It can be easily seen that a set of such permutations forms a group under the composition of permutations, so a subgroup of S_n. By the Lagrange's theorem the order of this subgroup divides the order of S_n, so $\frac{n!}{r!(n-r)!}$ is an integer. □

Questions

Q51. The permutations e, a, b and c are defined by $e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ and $c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. The operation is composition of permutations.

(i) Given that $p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ find another permutation q such that $\{e, p, q, a, b, c\}$ form a group.

(ii) Show the group table.

(iii) Determine, with clear explanation, whether or not the group is commutative.

(iv) List all proper subgroups of the group.

Q52. The set $S = \{1, 2, 4, 7, 8, 11, 13, 14\}$ forms a group under multiplication modulo 15.

(i) Write down the group table.

(ii) Given that the set $\{1, 2, a, b\}$ is a subgroup of S, find a and b.

(iii) Find one of the subgroups of S that also has four elements and includes 4, but not 2.

(iv) What is the order of the largest element in your answer to (iii)?

Q53. Consider set $G = \{1, 2, 3, 4, 5, 6\}$ under multiplication modulo 7.

(i) Show that G forms a group under the given operation.

(ii) Determine the orders of all elements of G.

(iii) Write down a subgroup of G which contains 2 elements and one which contains 3 elements.

Q54. (i) Let T be a set $\{x \in \mathbb{Q} |\ x \neq 0 \wedge x \neq 1\}$. Given that $f_1(x) = x$, $f_2(x) = 1 - x$ and $f_3(x) = \frac{1}{x}$, obtain expressions for $f_4(x)$, $f_5(x)$ and $f_6(x)$ if $f_4 = (f_2 \circ f_3)$, $f_5 = (f_3 \circ f_2)$ and $f_6 = (f_3 \circ f_4)$.

(ii) Given that the set $\{f_1, f_2, f_3, f_4, f_5, f_6\}$ forms a group with respect to $\circ$ - composition of functions construct the group table.

(iii) Determine the order of each element of the group.

(iv) List all proper subgroups.

Q55. The transpose of a matrix A which is denoted A^T is a matrix formed from A by switching rows into columns, i.e. if $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ then $A^T = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$.

(i) Prove that if A and B are 2×2 matrices then $(AB)^T = B^T A^T$.

(ii) Prove that if A is non-singular 2×2 matrix then $(A^T)^{-1} = (A^{-1})^T$.

(iii) Find eight different 2×2 matrices in which each of the elements is either -1, 0 or 1 and which satisfy $AA^T = I$, the identity matrix.

(iv) Assuming that these eight matrices form a group under matrix multiplication, find its all proper subgroups.

Q56. (i) Prove by induction, that if $n \in \mathbb{Z}^+$ and $p \in \mathbb{R}$,

$$\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & np \\ 0 & 1 \end{pmatrix}$$

(ii) Assuming that matrix multiplication is associative, prove that the set S of matrices of the form $\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$, $p \in \mathbb{R}$ forms a group under matrix multiplication.

(iii) Determine, with reasons, whether or not the following subsets of S form subgroups.

(1) the subset of $S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \right\}$,

(2) the subset of S for which $p \in \mathbb{Z}$,

(3) the subset of S for which $-1 \leq p \leq 1$.

Q57. Let p and q be prime numbers. Show that any proper subgroup of a group of order pq is cyclic.

Q58. *You may like to use the following result by Étienne Bézout:*
Let $n, k \in \mathbb{Z}$ such that $gcd(n, k) = 1$ (i.e. n and k are relatively prime). Then there exist $l, m \in \mathbb{Z}$ such that

$$kl + nm = 1$$

Let G be a finite group, $n(G) = n$. Let k be an integer relatively prime to n. Show that the function $f : G \longrightarrow G$ defined for $g \in G$ by $f(g) = g^k$ is invertible.

Chapter 6

Homomorphism of groups

6.1 Homomorphism

DEFINITION 6.1 (homomorphism)
Let $(G, *)$ and $(H, \bullet)$ be two groups.
A ***homomorphism*** *is a function $f : G \longmapsto H$ such that for every $a, b \in G$:*

$$f(a * b) = f(a) \bullet f(b)$$

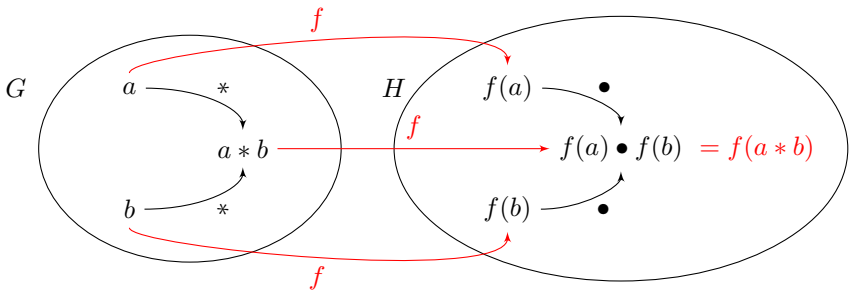


Figure 6.1: Group homomorphism.

EXAMPLE 6.2 (homomorphism $\mathbb{Z}_6$ into $\mathbb{Z}_9$)
Consider two groups:

$$\mathbb{Z}_6 = (\{0, 1, 2, 3, 4, 5\}, \oplus_6), \qquad \text{where } a \oplus_6 b = (a + b) \mod 6 \text{ and}$$
$$\mathbb{Z}_9 = (\{0, 1, 2, 3, \ldots, 7, 8\}, \oplus_9), \qquad \text{where } a \oplus_9 b = (a + b) \mod 9$$

Let $f : \mathbb{Z}_6 \longmapsto \mathbb{Z}_9$ be defined by:

$$f(x) = (3x) \mod 9$$

The values of f are as follows:

x	0	1	2	3	4	5
$f(x)$	0	3	6	0	3	6

Note *that f is neither* injective *nor* surjective.
Let us have a look at the group table for $\mathbb{Z}_6$ - domain of f and the table for range of f.

$\oplus_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\oplus_9$	0	3	6	0	3	6
0	0	3	6	0	3	6
3	3	6	0	3	6	0
6	6	0	3	6	0	3
0	0	3	6	0	3	6
3	3	6	0	3	6	0
6	6	0	3	6	0	3

The same colour-pattern in both tables show the property that defines homomorphism.

$$f(a * b) = f(a) \bullet f(b)$$

Let us have a closer look at:

$$f(1) = 3 \qquad f(2) = 6 \qquad f(3) = 0$$

$\oplus_6$	$\cdots$	2
$\vdots$	$\ddots$	$\vdots$
1	$\cdots$	3

$\oplus_9$	$\cdots$	6
$\vdots$	$\ddots$	$\vdots$
3	$\cdots$	0

$$\begin{aligned} 0 &= 3 \oplus_9 6 \\ f(3) &= f(1) \oplus_9 f(2) \\ f(1 \oplus_6 2) &= f(1) \oplus_9 f(2) \end{aligned}$$

THEOREM 6.3 (homomorphism preserves identity and inverses)

Let $f : G \longmapsto H$ be homomorphism between groups $(G, *)$ and $(H, \bullet)$. Let e_G and e_H be the identities in G and H respectively. Then:

1. $f(e_G) = e_H$,
2. *for all $a \in G$:* $f(a^{-1}) = (f(a))^{-1}$.

PROOF.

1.

For all $a, b \in G$: $f(a * b) = f(a) \bullet f(b)$. Consider $b = e_G$.

So for all $a \in G$: $f(a * e_G) = f(a) \bullet f(e_G)$,

That is: $f(a) = f(a) \bullet f(e_G)$

left-cancelling: $(f(a))^{-1} \bullet f(a) = (f(a))^{-1} \bullet [f(a) \bullet f(e_G)]$

associativity: $e_H = [(f(a))^{-1} \bullet f(a)] \bullet f(e_G)$

$e_H = e_H \bullet f(e_G)$

$e_H = f(e_G)$

2.

For all $a, b \in G$: $f(a * b) = f(a) \bullet f(b)$. Consider $b = a^{-1}$.

Then: $f(a * a^{-1}) = f(a) \bullet f(a^{-1})$

$f(e_G) = f(a) \bullet f(a^{-1})$

from **(1.)**: $e_H = f(a) \bullet f(a^{-1})$

left-cancelling: $(f(a))^{-1} \bullet e_H = (f(a))^{-1} \bullet [f(a) \bullet f(a^{-1})]$

associativity: $(f(a))^{-1} = [(f(a))^{-1} \bullet f(a)] \bullet f(a^{-1})$

$(f(a))^{-1} = e_H \bullet f(a^{-1})$

$(f(a))^{-1} = f(a^{-1})$

□

Definition 6.4 (kernel and image)
Let $f : G \longmapsto H$ be homomorphism between groups $(G, *)$ and $(H, \bullet)$.
*The **kernel** of f is a set of elements of G that are mapped onto the identity in H:*

$$\ker(f) = \{a \in G |\ f(a) = e_H\}$$

*The **image** of f is a set of elements of H that are values of f:*

$$\mathrm{im}(f) = \{x \in H |\ \exists a \in G :\ f(a) = x\}$$

Theorem 6.5 (kernel of homomorphism as a subgroup)
Let $f : G \longmapsto H$ be homomorphism between groups $(G, *)$ and $(H, \bullet)$.
Then $\ker(f)$ is a subgroup of G.

Proof.

1. operation in G is **associative**, so it is in $\ker(f)$, too.
2. the **identity** $e_G \in \ker(f)$ as $f(e_G) = e_H$.
3. Let $a \in \ker(f)$. Then $f(a) = e_H$. To check if **inverse** of a is in $\ker(f)$ let us consider

$$\begin{aligned} f(a^{-1}) &= (f(a))^{-1} = && \text{(homomorphism preserves inverses)} \\ &= (e_H)^{-1} = \\ &= e_H && \text{i.e. } a^{-1} \in \ker(f) \end{aligned}$$

4. Let now $a, b \in \ker(f)$, i.e. $f(a) = f(b) = e_H$. Then

$$f(a * b) = f(a) \bullet f(b) = e_H \bullet e_H = e_H$$

so $(a * b) \in \ker(f)$, too, which shows **closure**.

The four conditions above show that $\ker(f)$ is a group, so a subgroup of G. □

Theorem 6.6 (image of homomorphism as a subgroup)
Let $f : G \longmapsto H$ be homomorphism between groups $(G, *)$ and $(H, \bullet)$.
Then $\mathrm{im}(f)$ is a subgroup of H.

Proof.

1. operation in H is **associative**, so it is in $\mathrm{im}(f)$, too.
2. the **identity** $e_H \in \mathrm{im}(f)$ as $e_H = f(e_G)$.
3. Let $x \in \mathrm{im}(f)$. There exists $a \in G$ such that $f(a) = x$. As $f(a^{-1}) = (f(a))^{-1} = x^{-1}$, so the **inverse** of x, $x^{-1} \in \mathrm{im}(f)$, too.
4. Let $x, y \in \mathrm{im}(f)$. There exist $a, b \in G$ such that $f(a) = x$ and $f(b) = y$.
   $f(a) \bullet f(b) = f(a * b)$, so $f(a) \bullet f(b) \in \mathrm{im}(f)$, which shows **closure**.

The four conditions above show that $\mathrm{im}(f)$ is a group, so a subgroup of H. □

Example 6.7 (properties of homomorphism $\mathbb{Z}_6 \to \mathbb{Z}_9$)
Consider groups and homomorphism from example 6.2.

- $f(0) = 0$, *so f preserves identity,* *(theorem 6.3, **(1.)**)*
- *The table below shows that the inverses are preserved under f:* *(theorem 6.3, **(2.)**)*

x	0	1	2	3	4	5
$f(x)$	0	3	6	0	3	6
$(f(x))^{-1}$	0	6	3	0	6	3

x^{-1}	0	5	4	3	2	1
$f(x^{-1})$	0	6	3	0	6	3

- $\ker(f) = \{0, 3\}$ *which is a subgroup in* $\mathbb{Z}_6$, *(theorem 6.5)*
- $\mathrm{im}(f) = \{0, 3, 6\}$ *which is a subgroup in* $\mathbb{Z}_9$. *(theorem 6.6)*

Questions

Q1. Let $f : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_8$ be defined by $f(x) = 2x$. Show that f is a homomorphism. Find its image.

Q2. Let $f : \mathbb{Z}_8 \longrightarrow \mathbb{Z}_4$ be defined by $f(x) = (x \mod 4)$. Show that f is a homomorphism. Find its kernel.

Q3. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}_3$ be defined by $f(x) = (x \mod 3)$. Show that f is a homomorphism. Find its kernel.

Q4. Let $f : \mathbb{Z} \longrightarrow \mathbb{Z}_8$ be defined by $f(x) = (2x \mod 8)$. Show that f is a homomorphism. Find its kernel and image.

Q5. Consider the function $f : \mathbb{R} \longrightarrow \mathbb{R} \setminus \{0\}$ defined by $f(x) = e^x$.

(i) Show that f is a homomorphism of the additive group of real numbers into the multiplicative group of non-zero real numbers.

(ii) Find the kernel of f.

(iii) Find the image of f.

Q6. Consider the function $f : \mathbb{R}^+ \longrightarrow \mathbb{C} \setminus \{0\}$ defined by $f(x) = x^i$.

(i) Show that f is a homomorphism of group $(\mathbb{R}^+, \times)$ into group $(\mathbb{C} \setminus \{0\}, \times)$.

(ii) Find the kernel of f.

(iii) Show that the image of f is a subgroup of $\mathbb{C} \setminus \{0\}$.

Q7. Consider the function $f : \mathbb{C} \longrightarrow \mathbb{C} \setminus \{0\}$ defined by $f(z) = e^z$.

(i) Show that f is a homomorphism of the additive group of complex numbers into the multiplicative group of non-zero complex numbers.

(ii) Show that f is surjective but not injective.

(iii) Find the kernel of f and show it is a cyclic subgroup of $(\mathbb{C}, +)$.

(iv) Find the image of f.

Q8. Let M be the set of 2×2 invertible matrices. Let S be the set of 2×2 matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ such that $a, b \in \mathbb{R}$ and $a^2 + b^2 \neq 0$.

(i) Show that M forms a group under matrix multiplication.

(ii) Show that S is a subgroup of M.

(iii) Define a homomorphism $f : \mathbb{C} \setminus \{0\} \longrightarrow M$ such that its image is S. Show clearly that function f has required properties.

6.2 Isomorphism

DEFINITION 6.8 (isomorphism)

*An **isomorphism** is a bijective homomorphism.*
or more precisely:

*Let $(G, *)$ and $(H, \bullet)$ be two groups. An **isomorphism** is a function $f : G \longmapsto H$ such that:*

- *f is bijective*
- *for every $a, b \in G$: $f(a * b) = f(a) \bullet f(b)$*

*The groups G and H are called **isomorphic**.*

PROPERTIES.

*Let $(G,*)$ and $(H,\bullet)$ be two **finite** groups and $f: G \longrightarrow H$ be an isomorphism. Then:*

- $n(G) = n(H)$
- *Cayley tables of G and H show the same pattern (arrangement) of elements, if the elements are displayed in an appropriate order, i.e. position of an element of one group in a table is the same as position of its value under isomorphism in the other table.*

EXAMPLE 6.9 (isomorphism with $\mathbb{Z}_4$)

Consider groups:

- *set $G = \{1, i, -1, -i\}$ under multiplication, and*
- *$\mathbb{Z}_4$ of numbers $\{0,1,2,3\}$ under $\oplus_4$ - addition modulo 4.*

Compare two operation tables for G with a table for $\mathbb{Z}_4$:

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

The isomorphism $f: \mathbb{Z}_4 \longrightarrow G$ is $f(n) = i^n$, i.e.

n	0	1	2	3
$f(n)$	1	i	-1	$-i$

which is supported by the same pattern in the top tables.

THEOREM 6.10 (inverse of isomorphism)

Let $(G,*)$ and $(H,\bullet)$ be two groups and $f: G \longrightarrow H$ be an isomorphism. Then $f^{-1}: H \longrightarrow G$ is an isomorphism, too.

PROOF. It is obvious that f^{-1} exists and is bijective. It has to be shown that for all $c, d \in H$:

$$f^{-1}(c \bullet d) = f^{-1}(c) * f^{-1}(d)$$

Let $a = f^{-1}(c)$ and $b = f^{-1}(d)$ (or equivalently $c = f(a)$ and $d = f(b)$).

f is an isomorphism, so:	$f(a*b) = f(a) \bullet f(b)$
and thus:	$f^{-1}(f(a*b)) = f^{-1}(f(a) \bullet f(b))$
as $f^{-1}(f(x)) = x$ for all x	$a*b = f^{-1}(f(a) \bullet f(b))$
as $a = f^{-1}(c)$ and $b = f^{-1}(d)$	$f^{-1}(c) * f^{-1}(d) = f^{-1}(f(a) \bullet f(b))$
as $c = f(a)$ and $d = f(b)$	$f^{-1}(c) * f^{-1}(d) = f^{-1}(c \bullet d)$

□

EXAMPLE 6.11 (isomorphisms)

- *The groups $\mathbb{R}$ under addition and $\mathbb{R}^+ =]0, +\infty[$ under multiplication are isomorphic. The isomorphism is $f: \mathbb{R} \longrightarrow \mathbb{R}^+$ defined: $f(x) = e^x$.*
- *All finite cyclic groups are isomorphic to $\mathbb{Z}_n$, all infinite cyclic groups are isomorphic to $\mathbb{Z}$.*
- *Group $\mathbb{Z}_2 \times \mathbb{Z}_3$ under $*$ defined: $(a,b)*(c,d) = ((a+c) \mod 2, (b+d) \mod 3)$ is isomorphic with $\mathbb{Z}_6$ under addition modulo 6. The isomorphism is: $f((a,b)) = (3a + 4b) \mod 6$. The isomorphism could be written in the table:*

(a,b)	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
$f((a,b))$	0	4	2	3	1	5

Construct Cayley tables for both groups to see the isomorphism.

- *The Cartesian product of two cyclic groups is cyclic if and only if their orders are coprime.*

THEOREM 6.12 (isomorphism preserves orders)
Let $(G,*)$ and $(H,\bullet)$ be two groups and $f: G \longrightarrow H$ be an isomorphism. Then

$$\forall\ a \in G:\ \ ord(a) = ord(f(a))$$

LEMMA 6.13
Let $(G,*)$ and $(H,\bullet)$ be two groups and $f: G \longrightarrow H$ be an isomorphism. Let n be a positive integer. Then for all $x \in G$:

$$(f(x))^n = f(x^n)$$

i.e.

$$\underbrace{f(x) \bullet f(x) \bullet \cdots \bullet f(x)}_{n \text{ times}} = f(\underbrace{x * x * \cdots * x}_{n \text{ times}})$$

PROOF OF LEMMA. The proof can be easily conducted from the isomorphism property $f(a*b) = f(a) \bullet f(b)$ by mathematical induction. □

PROOF OF THEOREM 6.12. Let $a \in G$ and $n = ord(a)$, i.e. n is the smallest positive integer such that $a^n = e_G$ - the identity in G.

$$\begin{aligned} e_H = f(e_G) = & \qquad \text{(theorem 6.3\textbf{(1.)})} \\ = f(a^n) = & \qquad \text{(n is the order of a)} \\ = (f(a))^n & \qquad \text{(lemma)} \end{aligned}$$

Hence $(f(a))^n = e_H$. It must be shown that n is smallest positive integer with this property. Assume otherwise, there exists order of $f(a)$ smaller than n, i.e. $k \in \mathbb{Z}$ such that $0 < k < n$ and $(f(a))^k = e_H$. Then, as $f^{-1}: H \longrightarrow G$ is an isomorphism (theorem 6.10):

$$\begin{aligned} e_G = f^{-1}(e_H) = & \qquad \text{(theorem 6.3\textbf{(1.)})} \\ = f^{-1}((f(a))^k) = & \qquad \text{(k is the order of $f(a)$)} \\ = f^{-1}(f(a^k)) = & \qquad \text{(lemma)} \\ = a^k & \end{aligned}$$

This shows that $a^k = e_G$ which contradicts the assumption that order of a was equal n. □

Questions
Note.
*To prove that groups G and H are **isomorphic** you have to define a function $f: G \longrightarrow H$, show it is bijective and show it fulfils the isomorphism / homomorphism property. For finite groups the property can be explained by showing that there is an arrangement of the group tables that shows the same pattern.*
*To prove that two groups are **not isomorphic** it is sufficient to show that no bijective function can preserve inverses or orders.*

Q9. Consider S_4 - a group of permutations of 4 elements under composition of permutations.

(i) Find G, a subgroup of S_4 of order 3. Is the subgroup isomorphic to $\mathbb{Z}_3$? Does it hold for any subgroup of order 3?

(ii) Find H, a subgroup of S_4 such that $n(H) = 4$ and H is not isomorphic to $\mathbb{Z}_4$.

Q10. Function $e(x) = x$ together with 4 other functions forms a group under composition of functions. Show that this group is isomorphic to additive group $\mathbb{Z}_5$.

Q11. (i) Show that there is no 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $a, b, c, d \in \mathbb{R}$ such that $A^2 = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$.

(ii) Let P represent reflection in the line $y = -x$. Given that P is one of a set of four transformations $\{P, Q, R, S\}$ forming a group G under composition of transformations, describe geometrically the transformations Q, R and S and display the operation table for G.

(iii) Determine, giving reasons, whether or not G is isomorphic to the group defined by the table below.

$\times$	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

(iv) Determine orders of all elements of both groups.

Q12. Consider the following groups:

- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under $\oplus$ - addition modulo 4,
- $A = \{0, 3, 6, 9\}$ under $\oplus_{12}$ - addition modulo 12,
- $B = \{e, f, g, h\}$ - set of functions under composition of functions, where:
  - $e(x) = x$,
  - $f(x) = -x$,
  - $g(x) = \frac{1}{x}$,
  - $h(x) = -\frac{1}{x}$,
- $C = \{1, -1, i, -i\}$ under multiplication,
- $D = \{1, 2, 3, 4\}$ under $\otimes$ - multiplication modulo 5,
- $E = \{1, 3, 5, 7\}$ under $\otimes$ - multiplication modulo 8,
- $F = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ under multiplication of matrices,
- $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$ under multiplication of matrices.

(i) Show that A is isomorphic to $\mathbb{Z}_4$.

(ii) Show that B is not isomorphic to $\mathbb{Z}_4$.

(iii) Show that C is isomorphic to $\mathbb{Z}_4$.

(iv) Show that F and G are not isomorphic.

(v) Copy and complete the table below. The tick ($\surd$) means that the groups are isomorphic, the cross ($\times$) means that they are not.

	A	B	C	D	E	F	G	$\mathbb{Z}_4$
A	$\surd$							$\surd$
B		$\surd$						$\times$
C			$\surd$					$\surd$
D				$\surd$				
E					$\surd$			
F						$\surd$	$\times$	
G						$\times$	$\surd$	
$\mathbb{Z}_4$	$\surd$	$\times$	$\surd$					$\surd$

Q13. Consider the following groups:

- $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ under $\oplus$ - addition modulo 6,
- $A = \{0, 2, 4, 6, 8, 10\}$ under $\oplus_{12}$ - addition modulo 12,
- $B = \{e, p, q, s, t, u\}$ - set of functions under composition of functions, where:

$$e(x) = x \qquad s(x) = \frac{1}{x}$$
$$p(x) = 1 - x \qquad t(x) = \frac{1}{1-x}$$
$$q(x) = 1 - \frac{1}{x} \qquad u(x) = \frac{x}{x-1},$$

- $C = \left\{\pm 1, \pm\left(\frac{1}{2}i \pm \frac{\sqrt{3}}{2}\right)\right\}$ under multiplication,
- $D = \{1, 2, 3, 4, 5, 6\}$ under $\otimes$ - multiplication modulo 7,
- $E = \{1, 3, 5, 9, 11, 13\}$ under $\otimes$ - multiplication modulo 14,
- $F = \mathbb{Z}_2 \times \mathbb{Z}_3$ under $\odot$ - operation defined for $(a, b), (c, d) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ as follows:

$$(a, b) \odot (c, d) = ((a + c) \mod 2, (b + d) \mod 3),$$

- $G = \left\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}, \pm \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}\right\}$ under multiplication of matrices,
- S_3 - group of permutations of 3 elements under composition of permutations.

(i) Show that A is isomorphic to $\mathbb{Z}_6$.

(ii) Show that B is not isomorphic to $\mathbb{Z}_6$.

(iii) Show that B is isomorphic to S_3.

(iv) Show that C is isomorphic to $\mathbb{Z}_6$.

(v) Show that S_3 and G are not isomorphic.

(vi) Copy and complete the table below. The tick ($\surd$) means that the groups are isomorphic, the cross ($\times$) means that they are not.

	A	B	C	D	E	F	G	$\mathbb{Z}_6$	S_3
A	$\surd$							$\surd$	
B		$\surd$						$\times$	$\surd$
C			$\surd$					$\surd$	
D				$\surd$					
E					$\surd$				
F						$\surd$			
G							$\surd$		$\times$
$\mathbb{Z}_6$	$\surd$	$\times$	$\surd$					$\surd$	
S_3		$\surd$					$\times$		$\surd$

Q14. Show that $f : \mathbb{R}^+ \to \mathbb{R}$ defined by $f(x) = \ln x$ is an isomorphism of groups $(\mathbb{R}^+, \times)$ and $(\mathbb{R}, +)$.

Q15. (i) Show that sets $G = \{e^{in} |\ n \in \mathbb{Z}\}$ and $H = \{e^{ix} |\ x \in \mathbb{R}\}$ form groups under multiplication.

(ii) Show that G is isomorphic to $(\mathbb{Z}, +)$.

(iii) Show that H is not isomorphic to $(\mathbb{R}, +)$.

List of definitions

1.1 Definition (subset) . . . 4
1.2 Definition (operations on sets) . . . 4

2.1 Definition (ordered pair) . . . 7
2.3 Definition (Cartesian product) . . . 7
2.6 Definition (binary relation) . . . 8
2.8 Definition (reflexivity) . . . 8
2.9 Definition (symmetry) . . . 8
2.10 Definition (transitivity) . . . 9
2.15 Definition (equivalence relation) . . . 9
2.17 Definition (equivalence class) . . . 10
2.19 Definition (congruency modulo) . . . 10

3.1 Definition (domain, range) . . . 13
3.3 Definition (injection) . . . 13
3.5 Definition (surjection) . . . 14
3.7 Definition (bijection) . . . 14
3.9 Definition (composite function) . . . 15
3.11 Definition (inverse function) . . . 16

4.1 Definition (binary operation) . . . 21
4.5 Definition (Latin square property) . . . 22
4.8 Definition (identity) . . . 23
4.11 Definition (inverse) . . . 24
4.12 Definition (left-cancelation property) . . . 24
4.13 Definition (right-cancelation property) . . . 24
4.18 Definition (involute function) . . . 25

5.1 Definition (group) . . . 27
5.4 Definition (Abelian group) . . . 29
5.13 Definition (permutation) . . . 36
5.15 Definition (cycle) . . . 37
5.18 Definition (order of a group) . . . 39
5.19 Definition (order of an element) . . . 39
5.22 Definition (generator) . . . 41
5.23 Definition (cyclic group) . . . 41
5.26 Definition (subgroup) . . . 43
5.27 Definition (proper subgroup) . . . 43
5.34 Definition (coset) . . . 45

6.1 Definition (homomorphism) . . . 55
6.4 Definition (kernel and image) . . . 57
6.8 Definition (isomorphism) . . . 58

List of theorems

4.10 Theorem (Uniqueness of identity) . . . 23
4.15 Theorem (Uniqueness of inverse) . . . 24
4.16 Theorem (Inverse of 2 elements) . . . 25
4.17 Corollary (Inverse of more than 2 elements) . . . 25

5.3 Theorem (Latin square property for groups) . . . 28
5.21 Theorem (order of inverse) . . . 40
5.25 Theorem (cyclic and Abelian groups) . . . 42
5.28 Theorem (subgroup of a cyclic group) . . . 43
5.32 Theorem (subgroup test 1) . . . 44
5.33 Theorem (subgroup test 2) . . . 44
5.38 Theorem (cosets in Abelian groups) . . . 46
5.43 Theorem (intersection of cosets) . . . 48
5.44 Theorem (left coset as right coset) . . . 48
5.45 Theorem (coset as an equivalence class) . . . 48
5.46 Corollary . . . 48
5.49 Theorem (left coset size) . . . 50
5.50 Corollary (right coset size) . . . 50
5.51 Theorem (Joseph-Luis Lagrange, 1770) . . . 51
5.52 Corollary (to Lagrange's theorem) . . . 51
5.53 Theorem (groups of prime order) . . . 52
5.56 Theorem (binomial coefficients are integers) . . . 53

6.3 Theorem (homomorphism preserves identity and inverses) . . . 56
6.5 Theorem (kernel of homomorphism as a subgroup) . . . 57
6.6 Theorem (image of homomorphism as a subgroup) . . . 57
6.10 Theorem (inverse of isomorphism) . . . 59
6.12 Theorem (isomorphism preserves orders) . . . 60

List of examples

2.2 Example (ordered pairs) . . . 7
2.4 Example (Cartesian product) . . . 7
2.5 Example ($\mathbb{R}^2$ and $\mathbb{R}^3$) . . . 8
2.7 Example (relation "$<$") . . . 8
2.11 Example (properties of "$\geq$") . . . 9
2.12 Example (empty relation) . . . 9
2.13 Example (total relation) . . . 9
2.14 Example (properties of relations) . . . 9
2.16 Example (equivalence relations) . . . 9
2.18 Example (equivalence classes) . . . 10
2.20 Example (congruency modulo) . . . 10

3.2 Example (domain, range) . . . 13
3.4 Example (injections) . . . 13
3.6 Example (surjections) . . . 14
3.8 Example (bijections) . . . 15
3.10 Example (composite functions) . . . 15
3.12 Example (inverse function) . . . 16

4.2 Example (properties of standard operations) . . . 21
4.3 Example (addition modulo 4) . . . 22
4.4 Example (Cayley table) . . . 22
4.6 Example (Latin square) . . . 22
4.7 Example (not Latin square) . . . 22
4.9 Example (identities) . . . 23
4.14 Example (inverses) . . . 24
4.19 Example (involute functions) . . . 25

5.2 Example (group) . . . 27
5.5 Example (multiplicative notation) . . . 29
5.6 Example (elementary groups) . . . 29
5.7 Example ($\mathbb{Z}_n$ group) . . . 29
5.8 Example (Group of vectors in $\mathbb{R}^2$) . . . 29
5.9 Example (Group of transformations of a plane under composition of transformations) 30
5.10 Example (Symmetries of an equilateral triangle under composition) . . . 30
5.11 Example (Symmetries of a square under composition) . . . 31
5.12 Example (Symmetries of a rectangle under composition) . . . 32
5.14 Example (identity permutation) . . . 36
5.16 Example (cycles) . . . 37
5.17 Example (group of permutations of 3 elements) . . . 37
5.20 Example (orders) . . . 39
5.24 Example (cyclic groups) . . . 41

5.29 Example (subgroup of $\mathbb{Z}_6$) . . . 43
5.30 Example (subgroup of $\mathbb{Z}_8$) . . . 43
5.31 Example (Alternating groups) . . . 44
5.35 Example (cosets in $\mathbb{Z}$) . . . 45
5.36 Example (cosets in a group of symmetries of a triangle) . . . 46
5.37 Example (cosets in S_3 - group of permutations) . . . 46
5.39 Example (cosets in $\mathbb{Z}_9$) . . . 46
5.40 Example (cosets in vector group $\mathbb{R}^2$) . . . 47
5.41 Example (solutions of systems of linear equations) . . . 47
5.42 Example (illustration of example 5.41) . . . 47
5.47 Example (cosets in $\mathbb{Z}$ as equivalence classes) . . . 50
5.48 Example (partition of vector group $\mathbb{R}^2$) . . . 50
5.54 Example (orders of subgroups) . . . 52
5.55 Example (converse of Lagrange's theorem) . . . 52

6.2 Example (homomorphism $\mathbb{Z}_6$ into $\mathbb{Z}_9$) . . . 55
6.7 Example (properties of homomorphism $\mathbb{Z}_6 \to \mathbb{Z}_9$) . . . 57
6.9 Example (isomorphism with $\mathbb{Z}_4$) . . . 59
6.11 Example (isomorphisms) . . . 59