Discrete Mathematics (BMS-05)

Unit –I (Set Theory)

BMS- 05 DISCRETE MATHEMATICS Number of Credits : 4

UNIT-I : Set Theory, Relation and Function: Definition of sets, Countable and uncountable sets, Venn Diagrams, Proofs of some general identities on sets. Definition and types of relation, composition of relation, equivalence relation, partial order relation. Function: Definition, types of function, one to one, into and onto function, inverse function, composition of functions.

UNIT-II Algebraic Structures: Definition, properties and types of algebraic structures, Semi groups, Monoid, Groups, Abelian group, properties of groups, Subgroups, Cyclic groups, Cosets, Factor group, Permutations groups, Normal subgroups, examples and standard results. Rings and fields: Definition and Standard results.

UNIT-III Graphs: Simple graph, multigraph, graph terminology, representation of graphs, Bipartite, regular, planar and connected graphs, connected components in a graph, Euler graphs, Hamiltonian path and circuits, graph colouring, chromatic number, chromatic polynomials. Tree: types and definition, rooted tree, properties of trees.

UNIT-IV Combinatorics: Basic counting Technique, Pigeon-hole principle, Discrete Numeric function, Recurrence relations and their solution, Generating function, Solution of recurrence relations by method of generating function.

Books & References

1. J.P. Tremblay and R. Manohar, Discrete Mathematical Structures with applications to computer science, Tata McGraw-Hill.

2. D. Narsingh, Graph Theory with application to engineering and computer science - Prentice Hall

3. V. Krishnamurthy, Combinatorics: Theory and applications -, East East-West Press PVT. LTD, 1985

Set Theory

- Set: Collection of objects (“elements”)
- $a \in A$ “a is an element of A”
  “a is a member of A”
- $a \notin A$ “a is not an element of A”
- $A = \{a_1, a_2, \ldots, a_n\}$ “A contains…”
- It does not matter how often the same element is listed.

Set Equality

- Two sets A and B are said to be equal if and only if they contain the same elements.

- Examples:

- A = {1, 2, 7, -3}, B = {7, 1, -3, 2} : $A = B$

- A = {dog, cat, horse},
  B = {cat, horse, squirrel, dog} $A \neq B$

A = {dog, cat, horse},
B = {cat, horse, dog, dog} $A = B$

Examples for Sets

- Natural numbers **N** = {0, 1, 2, 3, …}
- Integers **Z** = {…, -2, -1, 0, 1, 2, …}
- Positive Integers $\mathbf{Z}^+$ = {1, 2, 3, 4, …}
- Real Numbers **R** = {47.3, -12, π, …}

Examples for Sets

- $A = \varnothing$ "empty set/null set"
- $A = \{z\}$ Note: $z \in A$, but $z \neq \{z\}$
- $\mathbf{Q} = \{a/b \mid a \in \mathbf{Z}$ *and* $b \in \mathbf{Z}^+\}$, set of rational numbers
- $A = \{\{x, y\}\}$

  Note: $\{x, y\} \in A$, but $\{x, y\} \neq \{\{x, y\}\}$
- $A = \{x \mid P(x)$ is the .....}

  "set of all x such that P(x) is the..."
- $A = \{x \mid x \in \mathbf{N} ,\ x > 7\} = \{8, 9, 10, \ldots\}$

  "set builder notation"

Subsets

- $A \subseteq B$ "A is a subset of B"
- $A \subseteq B$ if and only if every element of A is also an element of B.

i.e.,

$$A \subseteq B \iff \forall x (x \in A \implies x \in B)$$

- Examples:

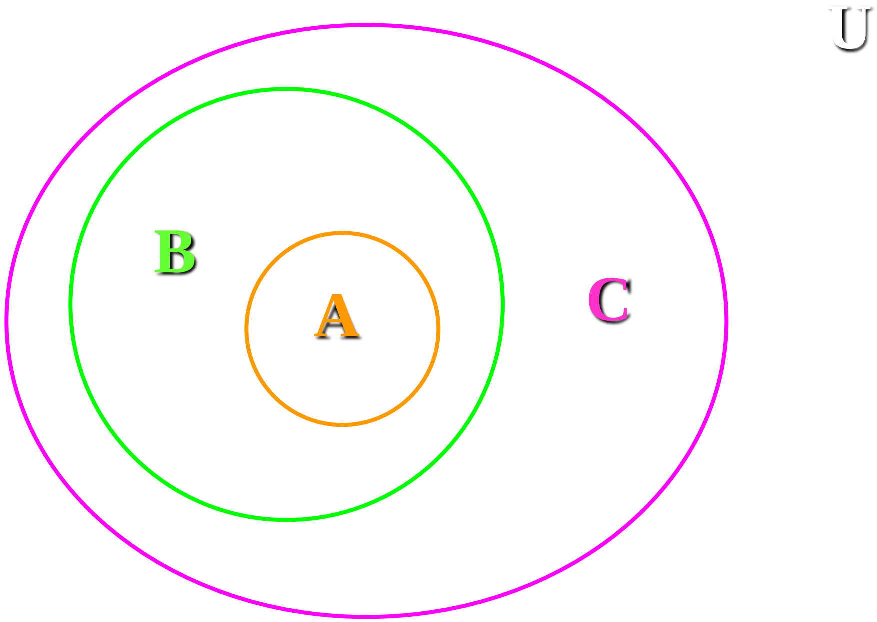
A = {3, 9}, B = {5, 9, 1, 3}, **$A \subseteq B$?** **true**

A = {3, 3, 3, 9}, B = {5, 9, 1, 3}, **$A \subseteq B$?** **true**

A = {1, 2, 3}, B = {2, 3, 4}, **$A \subseteq B$?** **false**

Subsets

- Useful rules:
- $A = B \Leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$
- $(A \subseteq B) \wedge (B \subseteq C) \Rightarrow A \subseteq C$ (see Venn Diagram)



Subsets

- Useful rules:
- $\emptyset \subseteq$ A for any set A
- A $\subseteq$ A for any set A

- Proper subsets:
- A $\subset$ B “A is a proper subset of B”
- A $\subset$ B $\Longleftrightarrow \forall x(x \in A \Longrightarrow x \in B)$ and $\exists x(x \in B \;\&\; x \notin$

Cardinality of Sets

- If a set A contains n distinct elements, $n \in \mathbf{N}$, then we call A a finite set with cardinality n.

- Examples:

- A = {Mercedes, BMW, Porsche}, $|A| = 3$

$B = \{1, \{2, 3\}, \{4, 5\}, 6\}$	**$|B| = 4$**
$C = \phi$	**$|C| = 0$**
$D = \{ x \in N \mid x \geq 1 \}$	**D is infinite!**

The Power Set

- P(A) “power set of A”
- P(A) = {B | B ⊆ A} (contains all subsets of A)

- Examples:

- A = {x, y, z}
- P(A) = {∅, {x}, {y}, {z}, {x, y}, {x, z}, {y, z}, {x, y, z}}

- A = ∅
- P(A) = {∅}
- Note: |A| = 0, |P(A)| = 1

The Power Set

- Cardinality of power sets:
- $| P(A) | = 2^{|A|}$
- Imagine each element in A has an “on/off” switch
- Each possible switch configuration in A corresponds to one element in 2^A

A	1	2	3	4	5	6	7	8
x	x	x	x	x	x	x	x	x
y	y	y	y	y	y	y	y	y
z	z	z	z	z	z	z	z	z

- For 3 elements in A, there are 2x2x2 = 8 elements in P(A)

Cartesian Product

- The ordered n-tuple $(a_1, a_2, a_3, \ldots, a_n)$ is an ordered collection of objects.

- Two ordered n-tuples $(a_1, a_2, a_3, \ldots, a_n)$ and $(b_1, b_2, b_3, \ldots, b_n)$ are equal if and only if they contain the same elements in the same order, i.e. $a_i = b_i$ for $1 \leq i \leq n$.

- The Cartesian product of two sets is defined as:

- $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

- Example: $A = \{x, y\}$, $B = \{a, b, c\}$

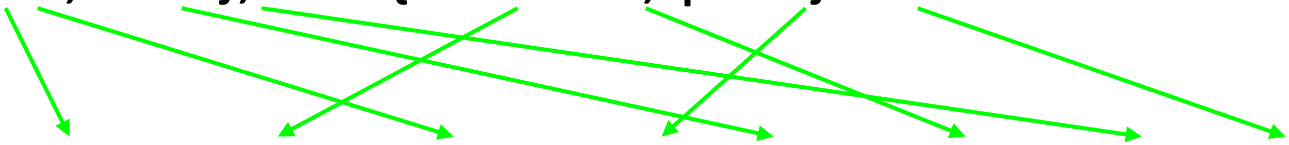
$A \times B = \{(x, a), (x, b), (x, c), (y, a), (y, b), (y, c)\}$

Cartesian Product

- The Cartesian product of two sets is defined as: A×B = {(a, b) | a∈A ∧ b∈B}

- Example:

- A = {good, bad}, B = {student, prof}



- A×B = { **(good, student), (good, prof), (bad, student), (bad, prof)**}

BxA = { (student, good), (prof, good), (student, bad), (prof, bad)}

Cartesian Product

- Note that:
- $A \times \emptyset = \emptyset$
- $\emptyset \times A = \emptyset$
- For non-empty sets A and B: $A \neq B \Leftrightarrow A \times B \neq B \times A$
- $|A \times B| = |A| \cdot |B|$
- The Cartesian product of two or more sets is defined as:
- $A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A \text{ for } 1 \leq i \leq n\}$

Set Operations

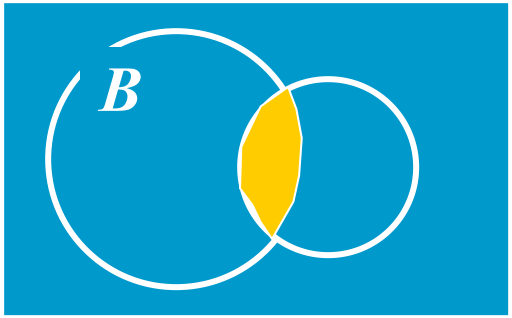
- Union: $A \cup B = \{x \mid x \in A \vee x \in B\}$
- Example: $A = \{a, b\}$, $B = \{b, c, d\}$
- $A \cup B = \{a, b, c, d\}$
- Intersection: $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- Example: $A = \{a, b\}$, $B = \{b, c, d\}$
- $A \cap B = \{b\}$

The *intersection* of two sets A and B is:

$$A \cap \mathrm{B} = \{\, x : x \in A \wedge x \in B \}$$

If A = {Charlie, Lucy, Linus}, and
B = {Lucy, Desi}, then

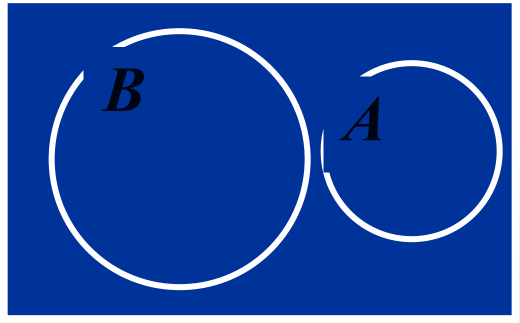
$A \cap B$ = {Lucy}



The *intersection* of two sets A and B is:

$$A \cap \mathrm{B} = \{ x : x \in A \wedge x \in B \}$$

If A = {x : x is a US president}, and
B = {x : x is in this room}, then
$A \cap B$ = {x : x is a Indian president in this room} = $\emptyset$



Sets whose intersection is empty are called *disjoint* sets

Set Operations

- Two sets are called disjoint if their intersection is empty, that is, they share no elements:
- $A \cap B = \varnothing$

- The difference between two sets A and B contains exactly those elements of A that are not in B:
- $A\text{-}B = \{x \mid x \in A \wedge x \notin B\}$

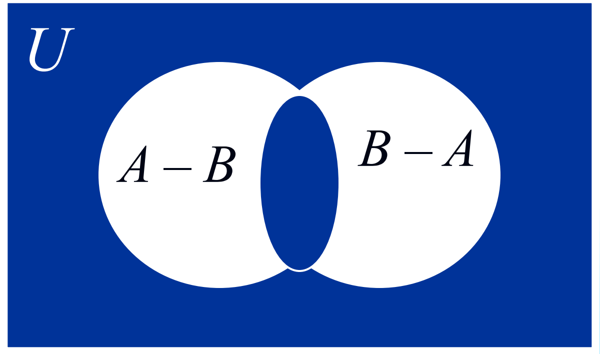
Example: $A = \{a, b\}$, $B = \{b, c, d\}$, $A\text{-}B = \{a\}$

The ***symmetric difference***, $A \oplus B$, is:

$$A \oplus B = \{ x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$$

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

$$= \{ x : x \in A \oplus x \in B\}$$

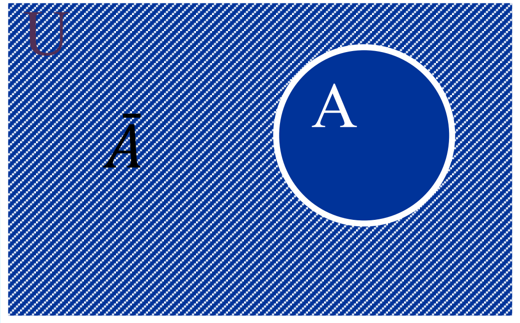


The *complement* of a set *A* is:

$$\bar{A} = \{x : x \notin A\}$$

If *A* = {*x* : *x* is not shaded}, then

$\bar{A} = \{x : x$ **is shaded**$\}$



$\overline{\varnothing} = U$

—and

$U = \varnothing$

- Identity

$$A \cap U = A$$

$$A \cup \varnothing = A$$

- Domination

$$A \cup U = U$$

$$A \cap \varnothing = \varnothing$$

- Idempotent

$$A \cup A = A$$

$$A \cap A = A$$

- ***Excluded Middle*** $A \cup \overline{A} = U$

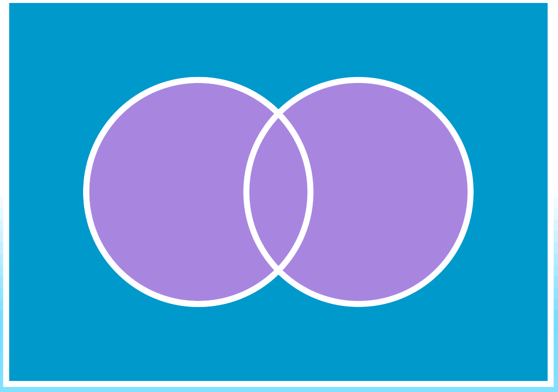
- ***Uniqueness*** $A \cap \bar{A} = \emptyset$

- ***Double complement*** $\overline{\overline{A}} = A$

Set Identities

- *DeMorgan's I* $\overline{A \cup B} = \bar{A} \cap \bar{B}$

- *DeMorgan's II* $\overline{A \cap B} = \bar{A} \cup \bar{B}$



Set Operations

- The complement of a set A contains exactly those elements under consideration that are not in A:
- A^c = U-A

- Example: U = **N(set of whole number)**

B = {250, 251, 252, …}

B^c = {0, 1, 2, …, 248, 249}

Set Identities

- Commutativity

$$A \cup B = B \cup A$$

$$A \cap B = B \cap A$$

- Associativity

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

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

- Distributivity

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

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

Problem1

❑ A computer Company must hire 20 programmers to handle system programming job and 30 programmers for applications programming. Of those hired, 5 are expected to perform job both types. How many programmers must be hired?

Sol: Let $A \rightarrow set\ of\ system\ programers\ hired, B \rightarrow set\ of\ applications\ programmers\ hired$.

Given $n(A) = 20, n(B) = 30, n(A \cap B) = 5.$ The number of programmers that must be hired is $n(A \cup B) = n(A) + n(B) - n\ (A \cap B)$ =20+30-5=45.

Problem2

- In a class of 25 students , 12 have taken Mathematics, 8 have taken Mathematics but not Biology. Find the number of students who have taken mathematics and biology and those who have taken biology but not mathematics.
- Let A&B be the sets of students who have taken Mathematics and Biology respectively, then A-B is there Is the set of students who have taken mathematics but not biology so ,

$n(A) = 12, n(A \cup B) = 25, n(A - B) = 8. As\ n(A - B) + n(A \cap B) = n(A), so$

$8 + n(A \cap B) = 12 \Rightarrow n(A \cap B)$ =4.

Now $n(A \cup B) = \mathrm{n(A) + n(B) - n(A} \cap B) \Rightarrow n(B) = 17.$

Also $n(B - A) + n(A \cap B) = n(B) \Rightarrow n(B - A) = 13.$

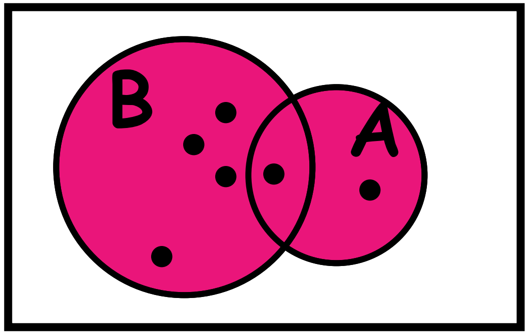
Set Theory - Inclusion/Exclusion

Example:
How many people are wearing a watch? a
How many people are wearing sneakers? b

How many people are wearing a watch OR sneakers? a + b

What's wrong?

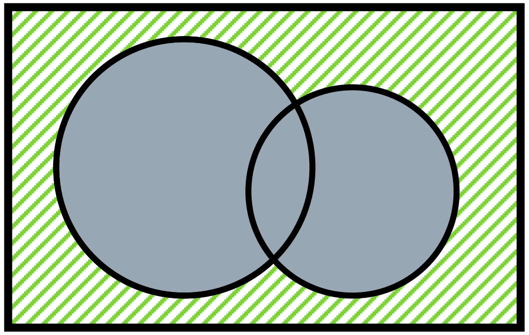
Wrong.



$$|A \cup B| = |A| + |B| - |A \cap B|$$

Set Theory - Inclusion/Exclusion

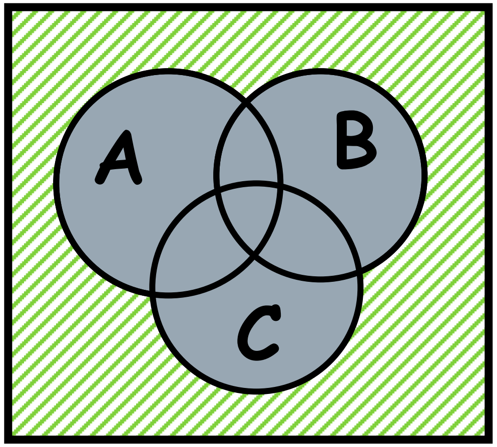
Example:
There are 217 students in a class.
157 are taking Maths.
145 are taking DM.
98 are taking both.
How many are taking neither?



217 - (157 + 145 - 98) = 13

Set Theory – Generalized Inclusion/Exclusion

Suppose we have:



And I want to know |A U B U C|

|A U B U C| = |A| + |B| + |C|
- |A ∩ B| - |A ∩ C| - |B ∩
C| + |A ∩ B ∩ C|

Prove that $\overline{A \cup B} = \bar{A} \cap \bar{B}$

$$x \in \overline{A \cup B} \Leftrightarrow x \notin A \cup B \Leftrightarrow x \notin A \wedge x \notin B$$
$$\Leftrightarrow x \in \bar{A} \wedge x \in \bar{B} \Leftrightarrow x \in \bar{A} \cap \bar{B}$$

Another Method

Prove that $\overline{A \cup B} = \bar{A} \cap \bar{B}$

using a membership table.

0 : x is not in the specified set

1 : otherwise

Haven't we seen this before?

A	B	$\bar{A}$	$\bar{B}$	$\bar{A} \cap \bar{B}$	$A \cup B$	$\overline{A \cup B}$
1	1	0	0	0	1	0
1	0	0	1	0	1	0
0	1	1	0	0	1	0
0	0	1	1	1	0	1

Set Operations

How can we prove $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$?

- Method I:

$x \in A \cup (B \cap C)$

$\Leftrightarrow x \in A \vee x \in (B \cap C)$

$\Leftrightarrow x \in A \vee (x \in B \wedge x \in C)$

$\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$

(distributive law for logical expressions)

$\Leftrightarrow x \in (A \cup B) \wedge x \in (A \cup C)$

$\Leftrightarrow x \in (A \cup B) \cap (A \cup C)$

Set Operations

- Method II: Membership table

- 1 means “x is an element of this set”

0 means “x is not an element of this set”

A	B	C	$B \cap C$	$A \cup (B \cap C)$	$A \cup B$	$A \cup C$	$(A \cup B) \cap (A \cup C)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	0
0	1	0	0	0	1	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

Prove that $\overline{A \cup (B \cap C)} = (\bar{C} \cup \bar{B}) \cap \bar{A}$

using known identities

$$\overline{A \cup (B \cap C)} = \bar{A} \cap (\overline{B \cap C})$$

$$= \bar{A} \cap (\bar{B} \cup \bar{C})$$

$$= (\bar{B} \cup \bar{C}) \cap \bar{A}$$

$$= (\bar{C} \cup \bar{B}) \cap \bar{A}$$

Introduction to Relations

Relations can be used to solve problems such as determining which pairs of cities are linked by airline flights in a network, or producing a useful way to store information in computer databases. Relationships between elements of sets occur in many contexts.

Introduction to Relations

Relationships between elements of sets are represented using a structure called relation.

Definition: Let A and B be sets. A relation R from A to B (a binary relation) is a subset of

$$\mathbf{A} \times \mathbf{B}$$

Cartesian Products and Relations

- **Definition 5.1:** For sets A, $B \subseteq U$, the *Cartesian product*, or *cross product*, of A and B is denoted by $A \times B$ and equals $\underline{\{(a, b) \mid a \in A, b \in B\}}$.
- We say that the elements of $A \times B$ are ***ordered pairs***. The following properties hold:
  - For $(a, b), (c, d) \in A \times B$, we have $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$.
  - If A, B are finite, it follows from the rule of product that $|A \times B| = |A| \bullet |B|$. We will have $|A \times B| = |B \times A|$, but not have $A \times B = B \times A$.
  - Although $A, B \subseteq U$, it is not necessary that $A \times B \subseteq U$.
  - If $n \in$ **Z**+, $n \geq 3$, and $A_1, A_2, \ldots, A_n \subseteq U$, then the (*n-fold*) *product* of $A_1, A_2, \ldots, A_n$ is denoted by $A_1 \times A_2 \times \ldots \times A_n$ and equals $\{(a_1,a_2,\ldots,a_n) \mid a_i \in A_i, 1 \leq i \leq n\}$.
  - The elements of $A_1 \times A_2 \times \ldots \times A_n$ are called ordered *n-tuples*.
  - If $(a_1,a_2,\ldots,a_n), (b_1,b_2,\ldots,b_n) \in A_1 \times A_2 \times \ldots \times A_n$, then $(a_1,a_2,\ldots,a_n) = (b_1,b_2,\ldots,b_n)$ if and only if $a_i = b_i$, for all $1 \leq i \leq n$.

e.g. If A={1,2} and B={a,b,c}, then

$$\mathbf{A \times B = \{(1,a),(1,b),(1,c),(2,a),(2,b),(2,c)\}}$$

Introduction to Relations

Definition: Let A and B be non-empty sets. A relation *R* from A and B is a subset of A x B.

We say that *a* is related to *b* by R

a *R* b

Lemma:

- For finite sets A, B with $|A| = m$ and $|B| = n$, there are 2^{mn} relations from A to B, including the empty relation and $A \times B$ itself. There are also 2^{nm} ($=2^{mn}$) relations from B to A, one of which is also ϕ and another of which is $B \times A$.

Relations and Their Properties

Use ordered pairs (*a*, *b*) to represent the relationship between elements of two sets.

- Example

Let ***A*** be the set of CS students in MMMUT

Let ***B*** be the set of courses,

Let ***R*** be the relation that consists of those pairs

(*a*, *b*) where *a* is a student enrolled in course *b*.

Then we may have

(Abhinav, DM), (Raj, Math) belonging to *R*.

Example:

Let A={0,1,2} and B={a,b}.

If R={(0,a), (0,b), (1,a), (2,b)}, then

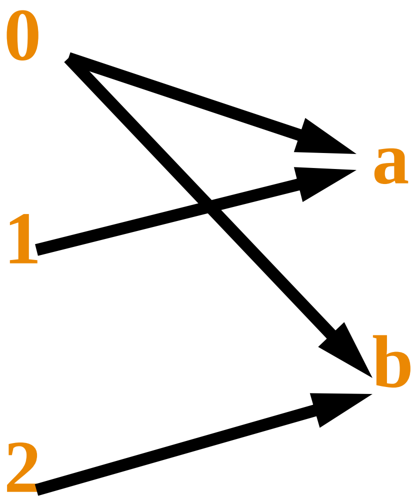
0 is related to a

but 1 is not related to b.

Relations can be represented graphically and in tabular form

R={(0,a), (0,b), (1,a), (2,b)}

Graphical method



Tabular form

R	a	b
0	X	X
1	X	
2		X

Relations on a Set

- **Relations from a set *A* to itself are of special interest.**

- **Definition: A relation on a set *A* is a relation from *A* to *A*.**
- Example

Let $A = \{1, 2, 3, 4\}$. Which ordered pairs are in the relation

$R = \{(a, b) : a \text{ divides } b\}$?

$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4),$
$(3, 3), (4, 4)\} \in A \times A$

Which of the following relations contain the ordered pairs (1, 1), (1, 2), (2, 1), (1, -1) or (2, 2) ?

$R_1 = \{(a, b) : a \leq b\}$

$\{(1, 1), (1, 2), (2, 2)\}$

$R_2 = \{(a, b) : a > b\}$

$\{(2, 1), (1, -1)\}$

$R_3 = \{(a, b) : a = b \text{ or } a = -b\}$

$\{(1, 1), (1, -1), (2, 2)\}$

Which of the following relations contain the ordered pairs (1, 1), (1, 2), (2, 1), (1, -1) or (2, 2) ?

$R_4 = \{(a, b) : a = b\}$

{(1, 1), (2, 2)}

$R_5 = \{(a, b) : a = b + 1\}$

{(2, 1)}

$R_6 = \{(a, b) : a + b \leq 3\}$.

{(1, 1), (1, 2), (2, 1), (1, -1)}

Combining Relations

Two relations from *A* to *B* can be combined using the set operations of union $\cup$, intersection $\cap$ and complement \\. Consider the following examples.

Example

Let $R_1 = \{(1, 1), (2, 2), (3, 3)\}$ and

$R_2 = \{(1, 1), (1, 2), (1, 3), (1,4)\}$

then :

$$R_1 \cup R_2 = \{(1, 1), (1, 2), (1, 3), (1,4), (2, 2), (3, 3)\}$$

$$R_1 \cap R_2 = \{(1, 1)\}$$

$$R_1 \setminus R_2 = \{(2, 2), (3, 3)\}$$

$$R_2 \setminus R_1 = \{(1, 2), (1, 3), (1,4)\}$$

Relations using matrices

Suppose that $A = \{1, 2, 3\}$ and $B =\{1, 2\}$. Let R be the relation from A to B such that it contains (a, b) if

$$a \in A, \quad b \in B, \text{ and } a > b.$$

What is the matrix representing R ?

Since $R = \{(2, 1), (3, 1), (3, 2)\}$, where $M_{i,j} = \begin{Bmatrix} 1, (x, y) \in R \\ 0, \quad (x, y) \notin R \end{Bmatrix}$,

then the logical matrix for R is $M_R = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$

Example

The binary relation *R* on the set {1, 2, 3, 4} is defined so that *aRb* holds if and only if *a* divides *b* evenly, with no remainder. For example, 2*R*4 holds because 2 divides 4 without leaving a remainder, but 3*R*4 does not hold because when 3 divides 4 there is a remainder of 1.

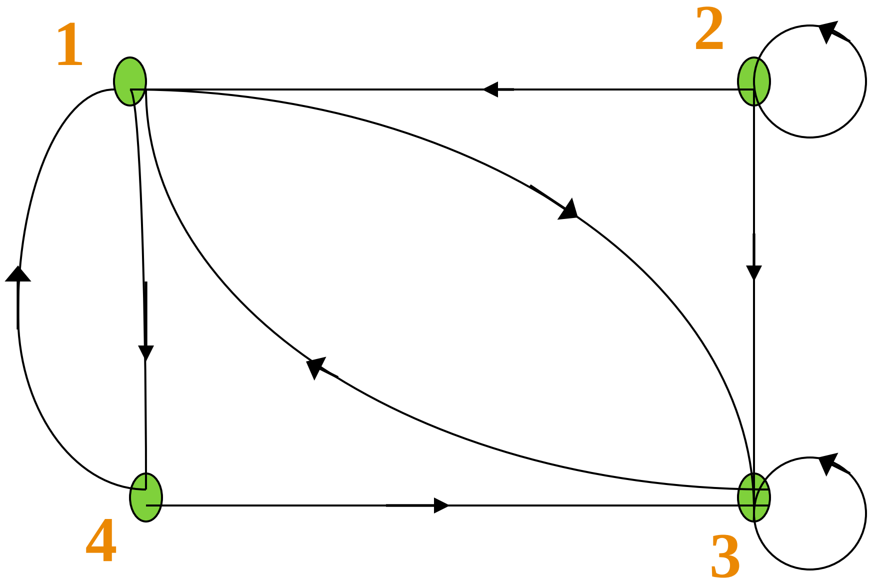
The following set is the set of pairs for which the relation *R* holds.

{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)}. The corresponding logical matrix is

$$M_R = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Relations using directed graphs

R = {(1,3), (1,4), (2,1), (2,2), (2,3), (3,1), (3,3), (4,1), (4,3)}



Properties of Binary Relations

The most direct way to express a relationship between two sets was to use ordered pairs. For this reason, sets of ordered pairs are called binary relations.

Reflexive Property of a Binary Relation

Definition:

A relation *R* on a set *A* is called *reflexive* if (*a*, *a*) $\in$ *R* for every element *a* $\in$ *A*.

Consider the following relations on {1, 2, 3, 4}. Which of these relations are reflexive?

R_1 = {(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)}

Not reflexive because 3 $\in$ A but (3,3) $\notin R_1$

R_2 = {(1, 1), (1, 2), (2, 1)}

Not reflexive because, say, 4 $\in$ A but (4, 4) $\notin R_2$

R_3 = {(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)}

Reflexive

R_4 = {(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)}

Not reflexive - (1, 1) ?

R_5 = {(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4),(3, 3), (3, 4), (4, 4)}

Reflexive - Why ?

R_6 = {(3, 4)}

Not Reflexive - Why ?

Symmetric Property of a Binary Relation

Definitions:

A relation R on a set A is called *symmetric* if for all $a, b \in A$, $(a, b) \in R$ implies $(b, a) \in R$.

Which of the relations are symmetric?

R_1 = {(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)}

Not symmetric - (3, 4) but no (4, 3)

R_2 = {(1, 1), (1, 2), (2, 1)}

Symmetric

R_3 = {(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)}

Symmetric

R_4 = {(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)}

Not symmetric - (2, 1) but no (1, 2)

R_5 = {(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)}

Not symmetric - (1, 3) but no (3, 1)

R_6 = {(3, 4)}

Not symmetric - (3, 4) but no (4, 3)

Transitive Property of a Binary Relation

Definition:

A relation *R* on a set *A* is called *transitive* if whenever (a, b) ∈ *R* and (b, c) ∈ *R* then

(a, c) ∈ *R*, for a, b, c ∈ *A*.

Which of the following relations are transitive?

R_1 = {(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)}

Not transitive

- (3, 4) & (4, 1) $\in R_1$ but (3, 1) $\notin R_1$

R_2 = {(1, 1), (1, 2), (2, 1)}

Not Transitive

- (2, 1) & (1, 2) $\in R_2$ but (2, 2) $\notin R_2$

$R_3 = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (3, 3), (4, 1), (4, 4)\}$

Not transitive

- (4, 1) & (1, 2) $\in R_3$ but (4, 2) $\notin R_3$

$R_4 = \{(2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$

Transitive

$R_5 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3, 4), (4, 4)\}$

Transitive

Equivalence Relation

Definition:

A relation *R* that is reflexive, symmetric and transitive on a set *A* is called *equivalence relation*

Consider a set A={1, 2 , 3 , 4 , 5 }

R_5 = {(1, 1), (1, 3), (1, 5), (2, 2), (2, 4), (3, 1), (3, 3), (3, 5), (4, 2), (4, 4), (5, 1), (5, 3), (5, 5)}

Is relation R_5 ia an equivalence relation on set A?

Yes, R_5 is an equivalence relation. Why ?

Consider a set A={a , b , c, d,}

R_6 = {(a, a), (b, c), (c, b), (d, d)}

Is relation R_6 is an equivalence relation on set A?

No, R_6 is an equivalence relation , Why ?

Partial ordering

- A relation R on a set S is called a partial ordering or *partial order* if it is:
  - reflexive
  - antisymmetric
  - transitive
- A set S together with a partial ordering R is called a *partially ordered set*, or *poset*, and is denoted by (S,R).

Example

- Let R be a relation on set A. Is R a partial order?

$$A = \{1,2,3,4\}$$

$$R = \{(1,1),(1,2),(1,3),(1,4),(2,2),$$
$$(2,3),(2,4),(3,3),(3,4),(4,4)\}$$

Example

- Is the “≥” relation is a partial ordering on the set of integers?
    - Since $a \geq a$ for every integer a, ≥ is reflexive
    - If $a \geq b$ and $b \geq a$, then $a = b$. Hence ≥ is anti-symmetric.
    - Since $a \geq b$ and $b \geq c$ implies $a \geq c$, ≥ is transitive.
    - Therefore “≥” is a partial ordering on the set of integers and (**Z**, ≥) is a poset.

Comparable/Incomparable

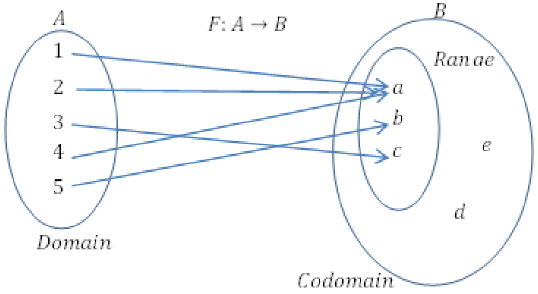
- The elements a and b of a poset (S, $\preccurlyeq$) are called *comparable* if either $a \preccurlyeq b$ or $b \preccurlyeq a$.
- The elements a and b of a poset (S, $\preccurlyeq$) are called *incomparable* if neither $a \preccurlyeq b$ nor $b \preccurlyeq a$.
- In the poset (**Z+**, **|**):
  - Are 3 and 9 comparable?
  - Are 5 and 7 comparable?

Total Order

- If every two elements of a poset $(S, \preccurlyeq)$ are comparable, then S is called a *totally ordered* or *linearly ordered* set and $\preccurlyeq$ is called a *total order* or *linear order*.
- The poset (**Z+**, ≤) is totally ordered.
  - Why?
- The poset (**Z+**, **|**) is not totally ordered.
  - Why?

Relation Vs Function

- A relation is a link between the elements of two sets. In a more formal setting, it can be described as a subset of the Cartesian product of two sets X and Y.
- Functions are a special type of relations. This special type of relation describes how one element is mapped to another element in another set or the same set. Every element of the set where each mapping starts must have an associated/linked element in the other set.
- The elements in the set where mapping starts can only be associated/linked to one and only one element in the other set
- The set from which the relation is mapped is known as the Domain. The set, where the relation is mapped into is known as the Codomain. The subset of elements in the codomain containing only the elements linked to the relation is known as the Range.



Functions: Definitions

A function $f : A \rightarrow B$ is given by a ***domain set*** A, a ***codomain set*** B, and a rule which for every element a of A, specifies a **unique** element $f(a)$ in B

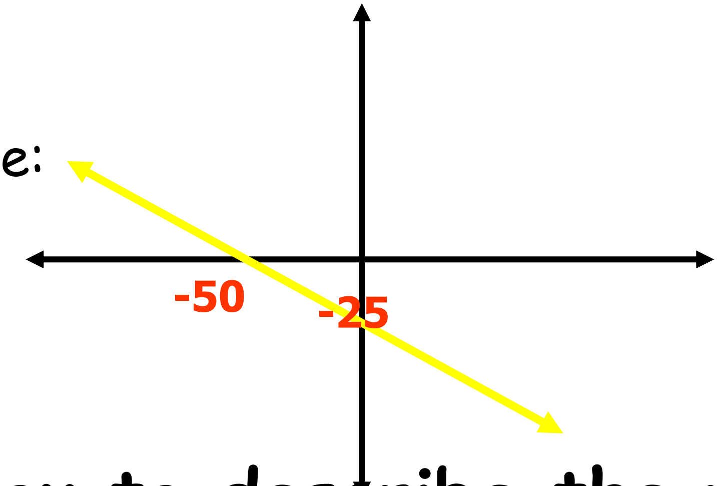
$f(a)$ is called the ***image*** of a, while a is called the ***pre-image*** of $f(a)$

The ***range*** (or ***image***) of f is defined by

$f(A) = \{f(a) \mid a \in A\}$.

Functions

Suppose we have:



And I ask you to describe the yellow function.

What's a function?

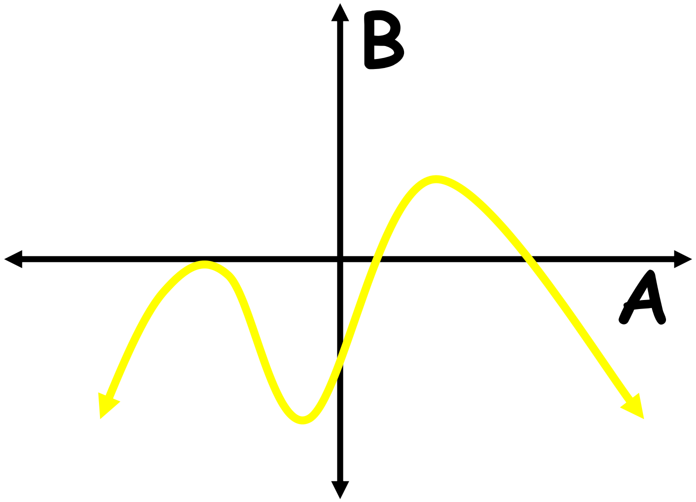
$y = f(x) = -(1/2)x - 25$

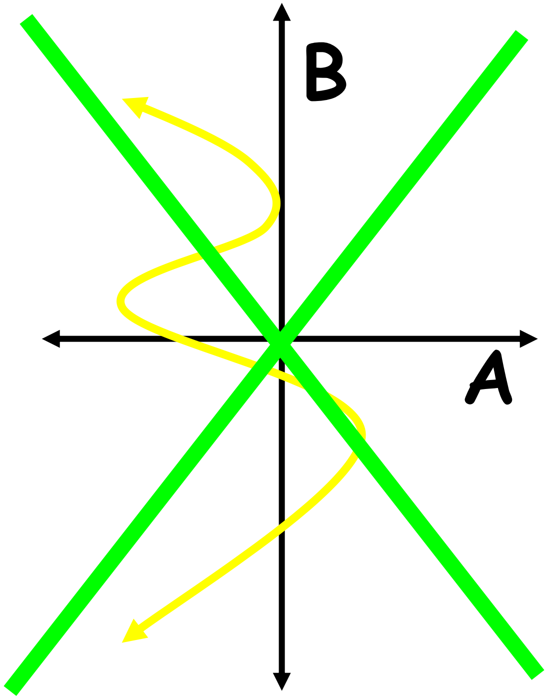
Notation: $f: R \to R,\ f(x) = -(1/2)x - 25$

domain

co-domain

Function or not?

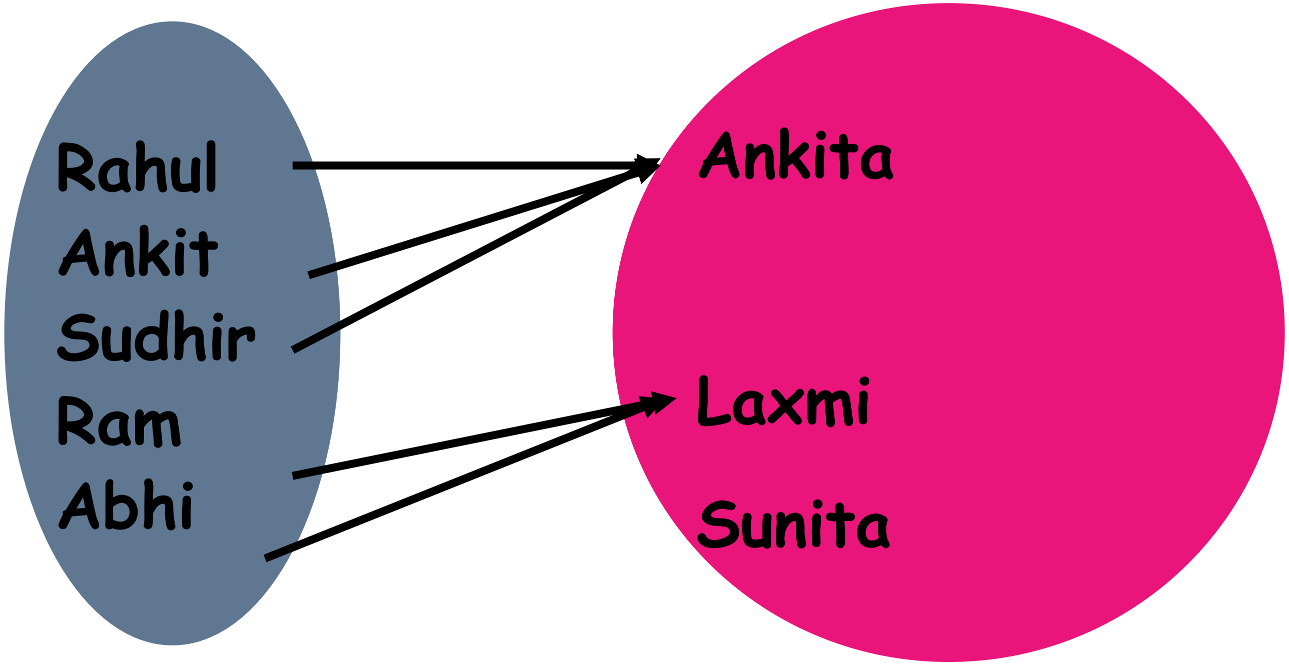




Functions: examples

A = {Rahul, Ankit, Sudhir, Ram, Abhi}
B = {Ankita, Laxmi, Sunita}

Let f: A → B be defined as f(a) = mother(a).

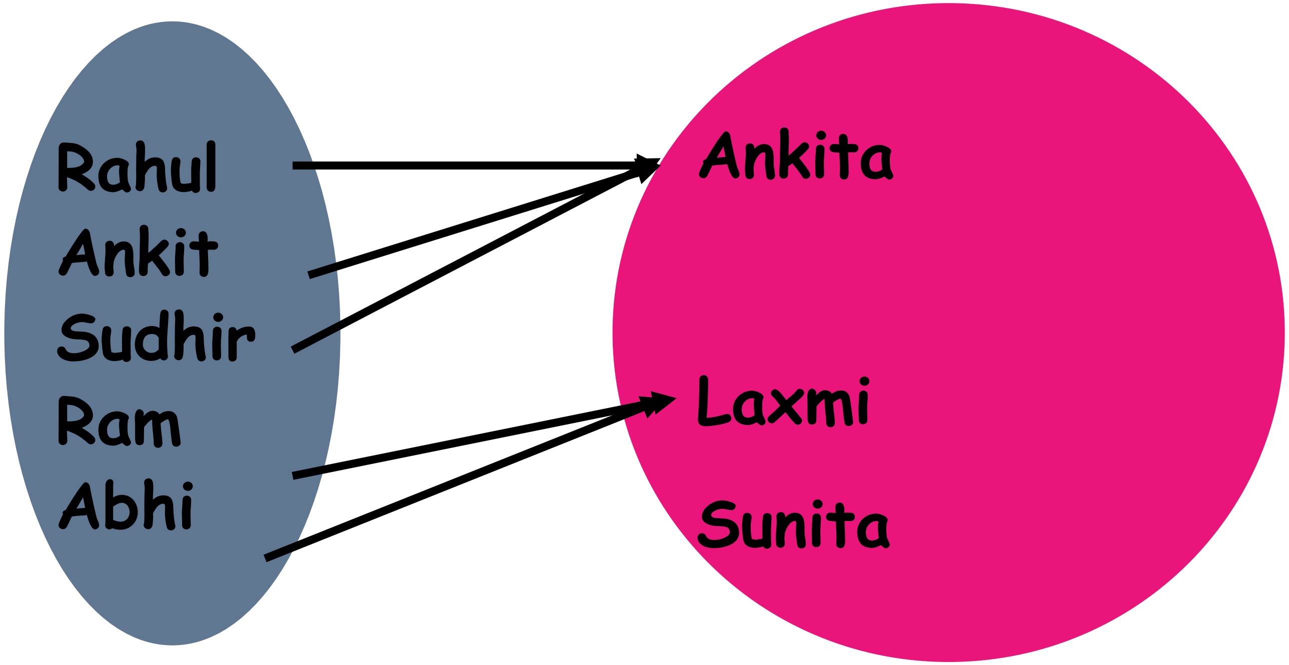


Functions - image set

For any set $S \subseteq A$, image(S) = $\{f(a) : a \in S\}$

image(S) = f(S)

So, image({Rahul, Ankit}) = {Ankita}, image(A) = B - {Sunita}

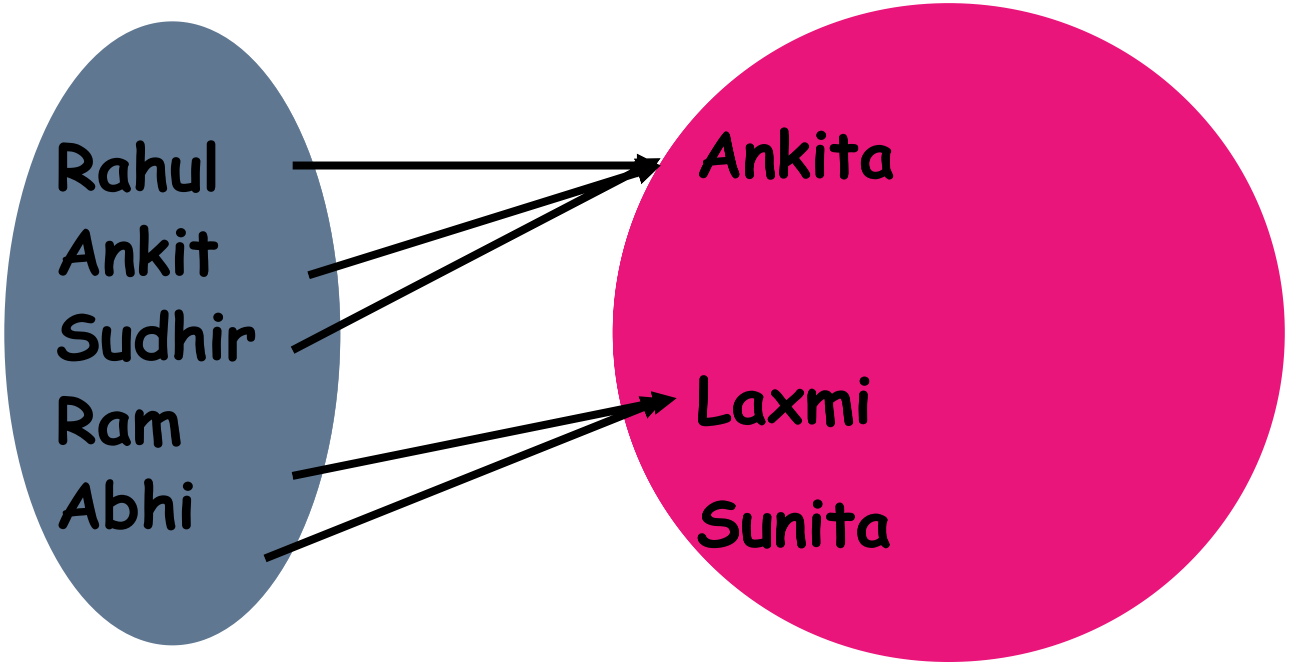


image(A) is also called range

Functions – preimage set

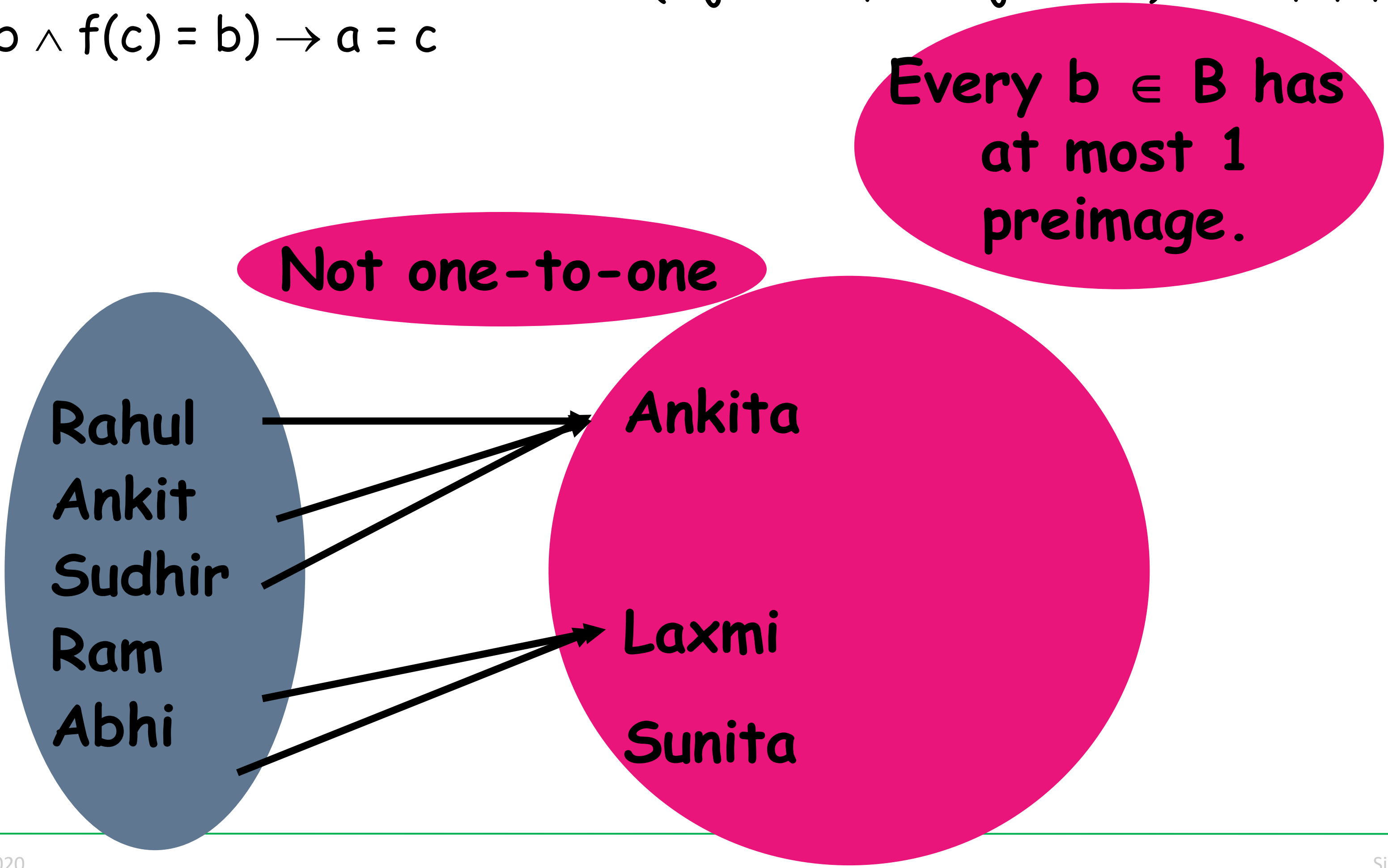
For any $S \subseteq B$, preimage(S) = $\{a \in A: f(a) \in S\}$ **preimage(S) = $f^{-1}(S)$**

So, preimage({Laxmi}) = {Ram, Abhi}, preimage(B) = A



Functions - injection

A function f: A $\rightarrow$ B is one-to-one (injective, an injection) if $\forall$a,b,c, (f(a) = b $\wedge$ f(c) = b) $\rightarrow$ a = c

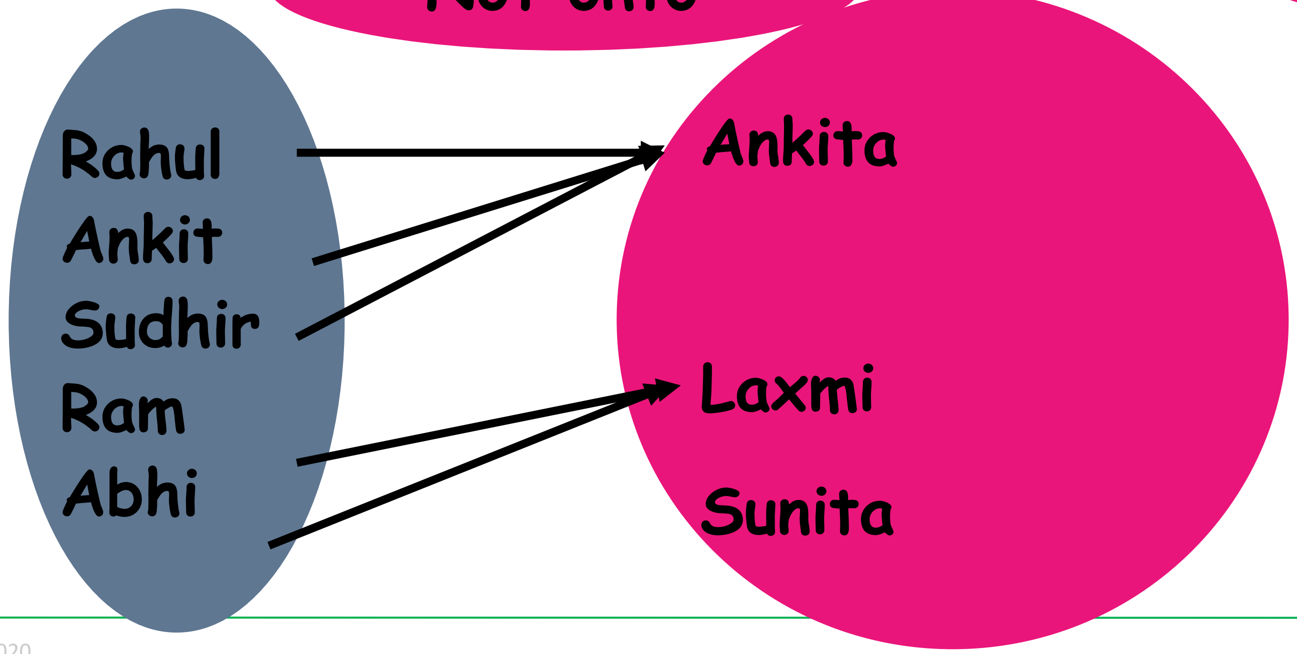


Functions - surjection

A function f: A → B is onto (surjective, a surjection) if $\forall b \in B, \exists a \in A$, f(a) = b

Every b ∈ B has at least 1 preimage.

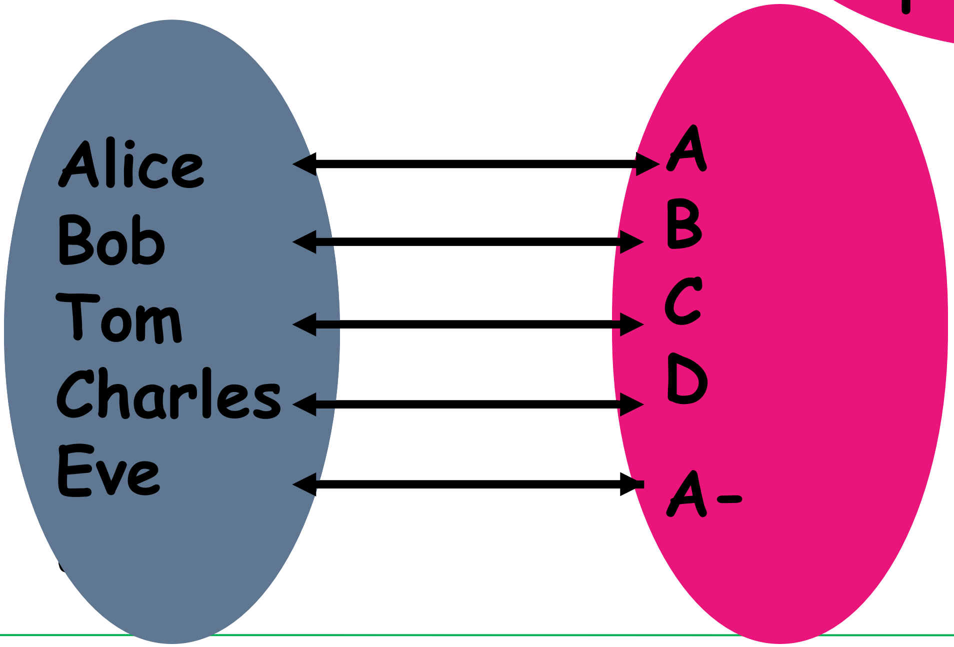
Not onto



Functions - bijection

A function f: A → B is bijective if it is one-to-one and onto.

Every b ∈ B has exactly 1 preimage.



An important implication of this characteristic: The preimage (f^{-1}) is a function!

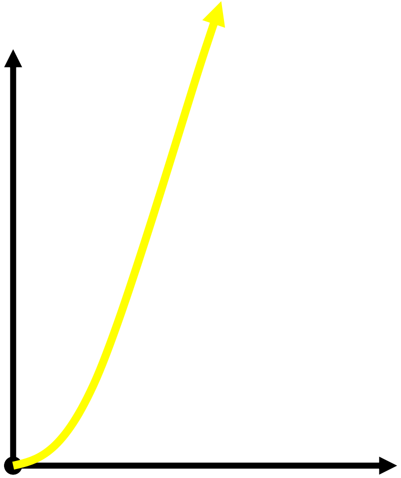
Functions - examples

Suppose f: $R^+ \rightarrow R^+$, $f(x) = x^2$.

Is f one-to-one? yes

Is f onto? yes

Is f bijective? yes



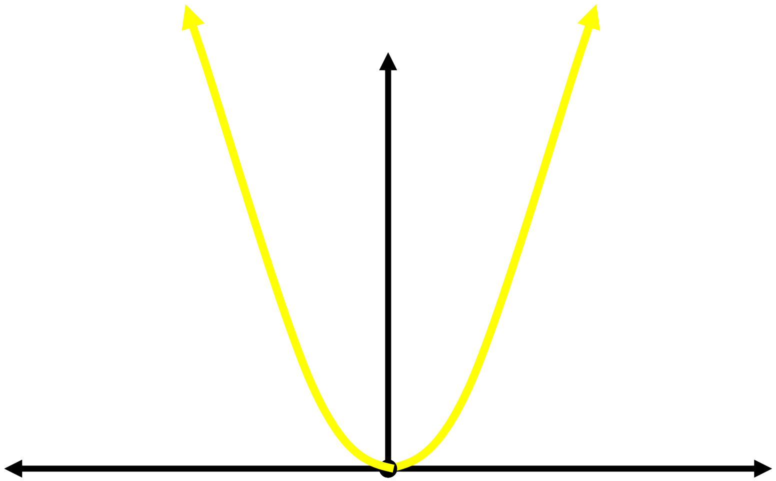
Functions - examples

Suppose f: R → R^+, $f(x) = x^2$.

Is f one-to-one? **no**

Is f onto? **yes**

Is f bijective? **no**



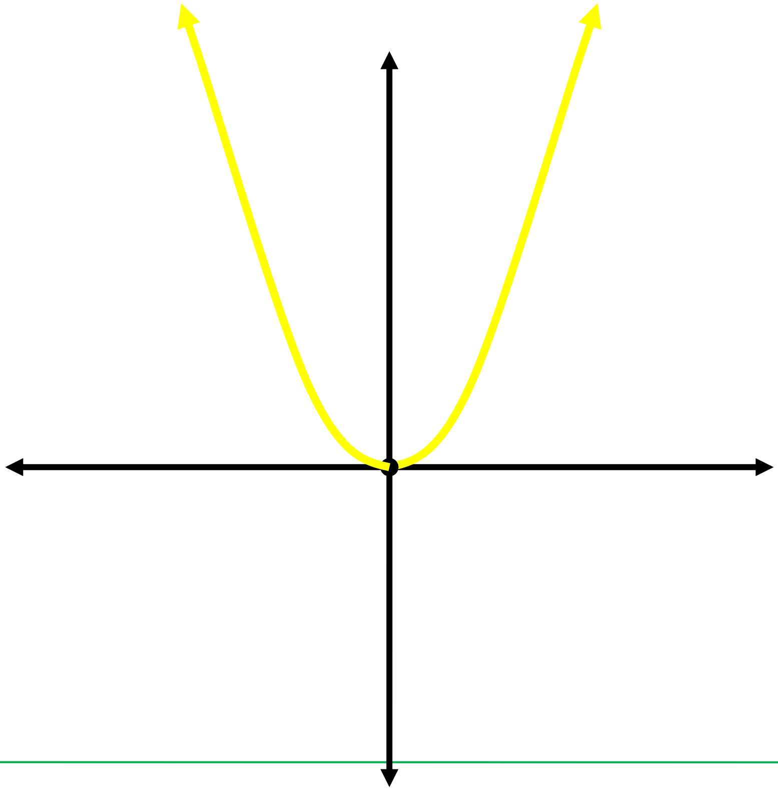
Functions - examples

Suppose f: R → R, $f(x) = x^2$.

Is f one-to-one? no

Is f onto? no

Is f bijective? no



Functions - examples

Q: Which of the following are 1-to-1, onto, a bijection? If f is invertible, what is its inverse?

1. $f : \mathbf{Z} \rightarrow \mathbf{R}$ is given by $f(x) = x^2$
2. $f : \mathbf{Z} \rightarrow \mathbf{R}$ is given by $f(x) = 2x$
3. $f : \mathbf{R} \rightarrow \mathbf{R}$ is given by $f(x) = x^3$
4. $f : \mathbf{Z} \rightarrow \mathbf{N}$ is given by $f(x) = |x|$
5. f : {people} → {people} is given by $f(x)$ = the father of x.

Operation

- **Sum**

  $(f + g)(x)=f(x) + g(x)$

Difference

$(f\text{-}g)(x) \ = f(x)\text{-}g(x)$

- **Product**

  $f(x) * g(x) = (f\ g)(x)$ $\longrightarrow f(x) \times g(x)$

  $= \left(\cancel{fg}\right)(x)$

- **Divide**

  (f/g)=$f(x)/g(x)$,

$$\left(\frac{f}{g}\right)(x) = \frac{f(x)}{g(x)} = \cancel{f[g(x)]}$$

$\boxed{\cancel{I(x) = R}}$

Special Type of Function

$I : A \to \underline{\underline{A}}$

Identity function

- Identity function maps each element from A to A. $I(\underline{x}) = \underline{\underline{x}}$

$\underline{\forall x \in A}$

Special Type of Function

Inverse function

An inverse function of $f: A \rightarrow B$ is $f^{-1}: B \rightarrow A$, given that *f* is a bijective function (onto and one-to-one).
Note that not all functions have the inverse function.

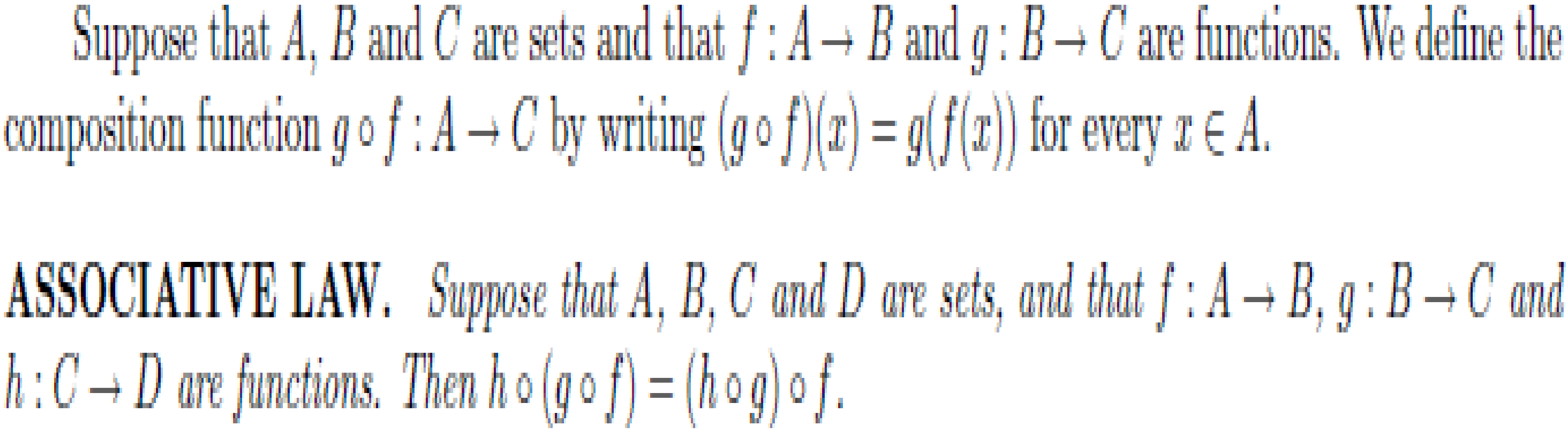
Special Type of Function

Invertible function

A function *f*: A→B is said to be invertible if its inverse relation, f^{-1} , is also a function.

Special Type of Function

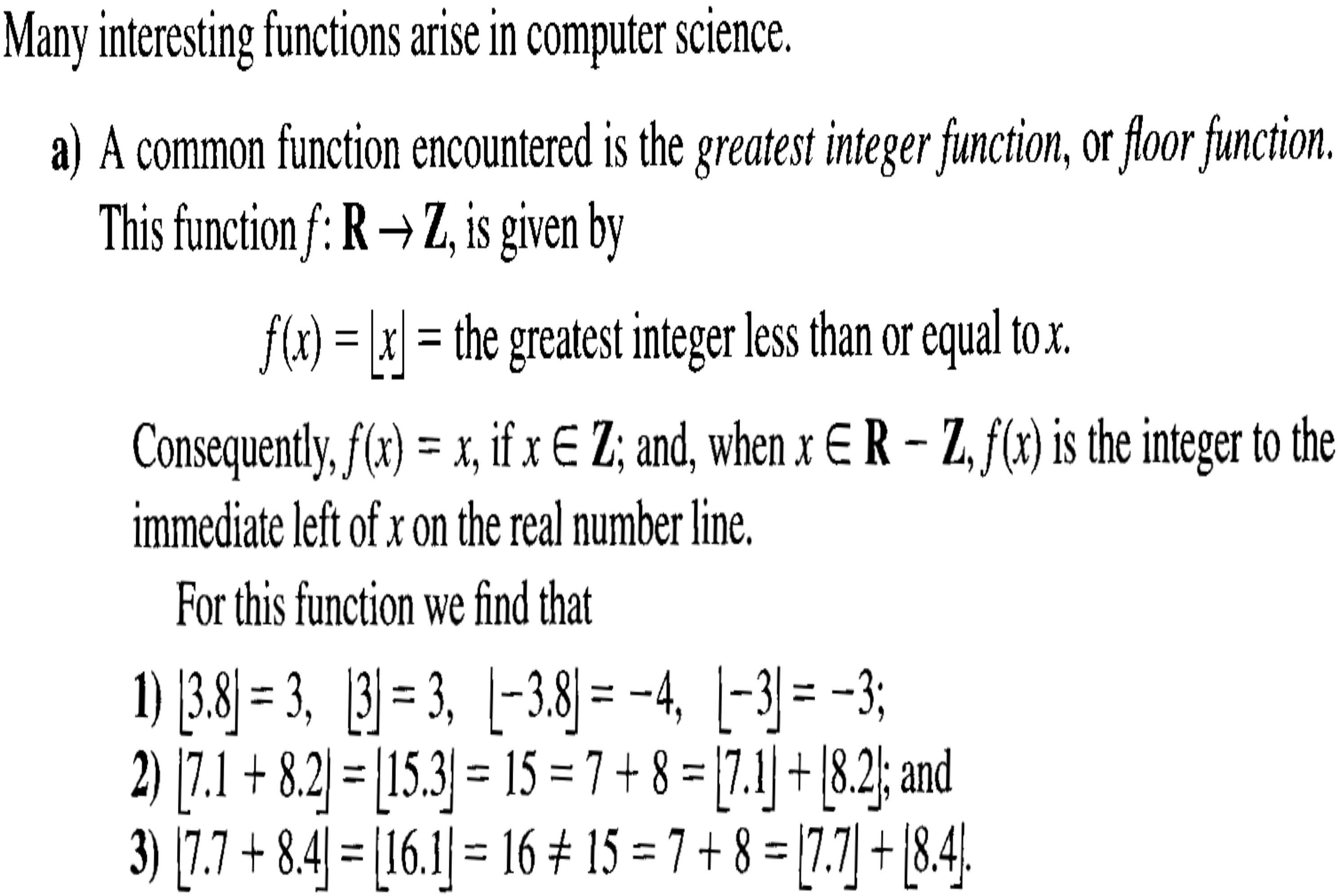
Composition function



Suppose that A, B and C are sets and that $f : A \to B$ and $g : B \to C$ are functions. We define the composition function $g \circ f : A \to C$ by writing $(g \circ f)(x) = g(f(x))$ for every $x \in A$.

ASSOCIATIVE LAW. *Suppose that A, B, C and D are sets, and that $f : A \to B$, $g : B \to C$ and $h : C \to D$ are functions. Then $h \circ (g \circ f) = (h \circ g) \circ f$.*

Example



Many interesting functions arise in computer science.

a) A common function encountered is the *greatest integer function*, or *floor function.* This function $f: \mathbf{R} \rightarrow \mathbf{Z}$, is given by

$$f(x) = \lfloor x \rfloor = \text{the greatest integer less than or equal to } x.$$

Consequently, $f(x) = x$, if $x \in \mathbf{Z}$; and, when $x \in \mathbf{R} - \mathbf{Z}$, $f(x)$ is the integer to the immediate left of x on the real number line.

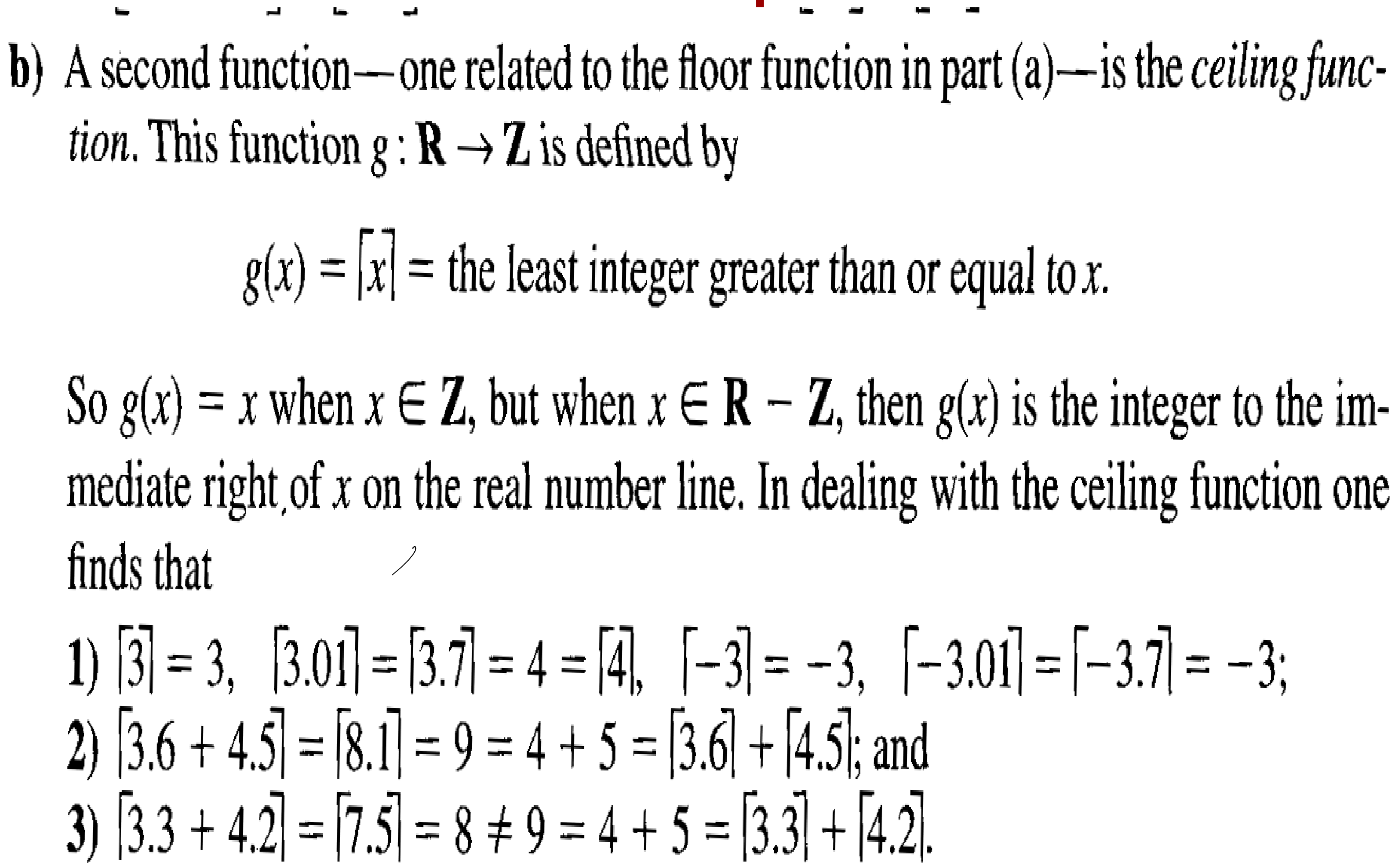
For this function we find that

1) $\lfloor 3.8 \rfloor = 3, \quad \lfloor 3 \rfloor = 3, \quad \lfloor -3.8 \rfloor = -4, \quad \lfloor -3 \rfloor = -3;$

2) $\lfloor 7.1 + 8.2 \rfloor = \lfloor 15.3 \rfloor = 15 = 7 + 8 = \lfloor 7.1 \rfloor + \lfloor 8.2 \rfloor$; and

3) $\lfloor 7.7 + 8.4 \rfloor = \lfloor 16.1 \rfloor = 16 \neq 15 = 7 + 8 = \lfloor 7.7 \rfloor + \lfloor 8.4 \rfloor$.

Example



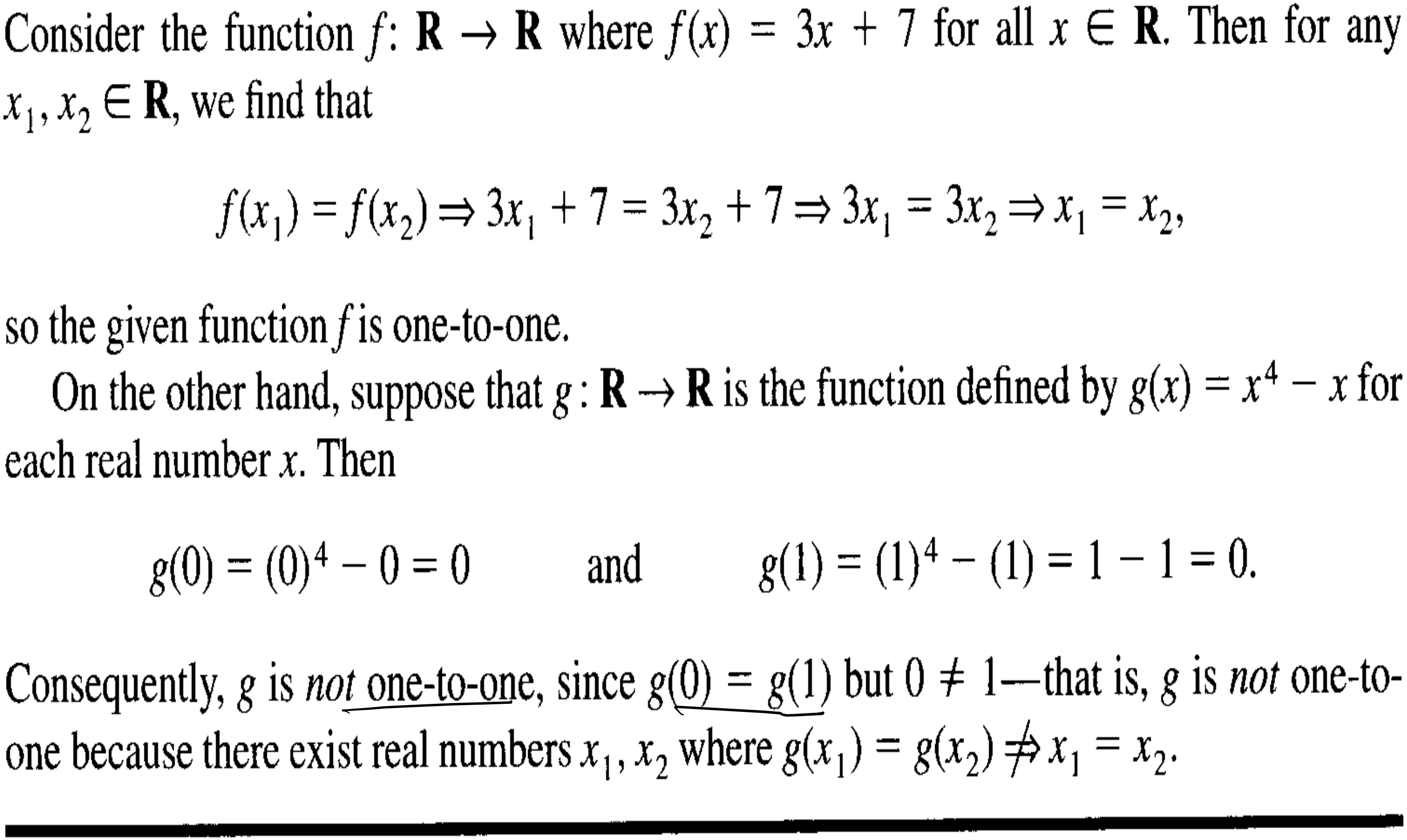
b) A second function—one related to the floor function in part (a)—is the *ceiling function*. This function $g : \mathbf{R} \to \mathbf{Z}$ is defined by

$$g(x) = \lceil x \rceil = \text{the least integer greater than or equal to } x.$$

So $g(x) = x$ when $x \in \mathbf{Z}$, but when $x \in \mathbf{R} - \mathbf{Z}$, then $g(x)$ is the integer to the immediate right of x on the real number line. In dealing with the ceiling function one finds that

1) $\lceil 3 \rceil = 3, \quad \lceil 3.01 \rceil = \lceil 3.7 \rceil = 4 = \lceil 4 \rceil, \quad \lceil -3 \rceil = -3, \quad \lceil -3.01 \rceil = \lceil -3.7 \rceil = -3;$
2) $\lceil 3.6 + 4.5 \rceil = \lceil 8.1 \rceil = 9 = 4 + 5 = \lceil 3.6 \rceil + \lceil 4.5 \rceil$; and
3) $\lceil 3.3 + 4.2 \rceil = \lceil 7.5 \rceil = 8 \neq 9 = 4 + 5 = \lceil 3.3 \rceil + \lceil 4.2 \rceil$.

Example



Consider the function f: $\mathbf{R} \to \mathbf{R}$ where $f(x) = 3x + 7$ for all $x \in \mathbf{R}$. Then for any $x_1, x_2 \in \mathbf{R}$, we find that

$$f(x_1) = f(x_2) \Rightarrow 3x_1 + 7 = 3x_2 + 7 \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2,$$

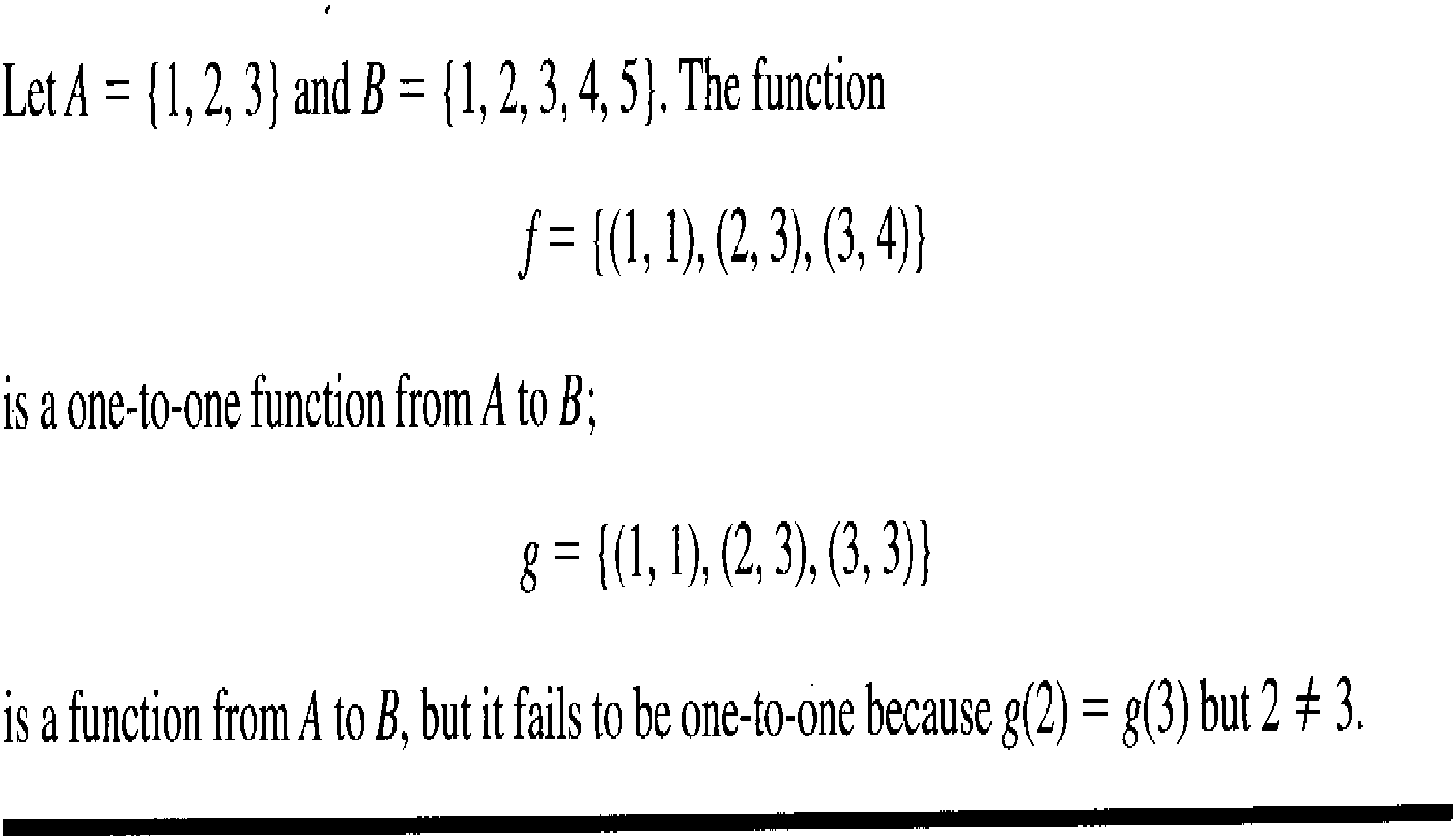
so the given function f is one-to-one.

On the other hand, suppose that $g : \mathbf{R} \to \mathbf{R}$ is the function defined by $g(x) = x^4 - x$ for each real number x. Then

$$g(0) = (0)^4 - 0 = 0 \qquad \text{and} \qquad g(1) = (1)^4 - (1) = 1 - 1 = 0.$$

Consequently, g is *not* one-to-one, since $g(0) = g(1)$ but $0 \neq 1$—that is, g is *not* one-to-one because there exist real numbers x_1, x_2 where $g(x_1) = g(x_2) \not\Rightarrow x_1 = x_2$.

Example



Let $A = \{1, 2, 3\}$ and $B = \{1, 2, 3, 4, 5\}$. The function

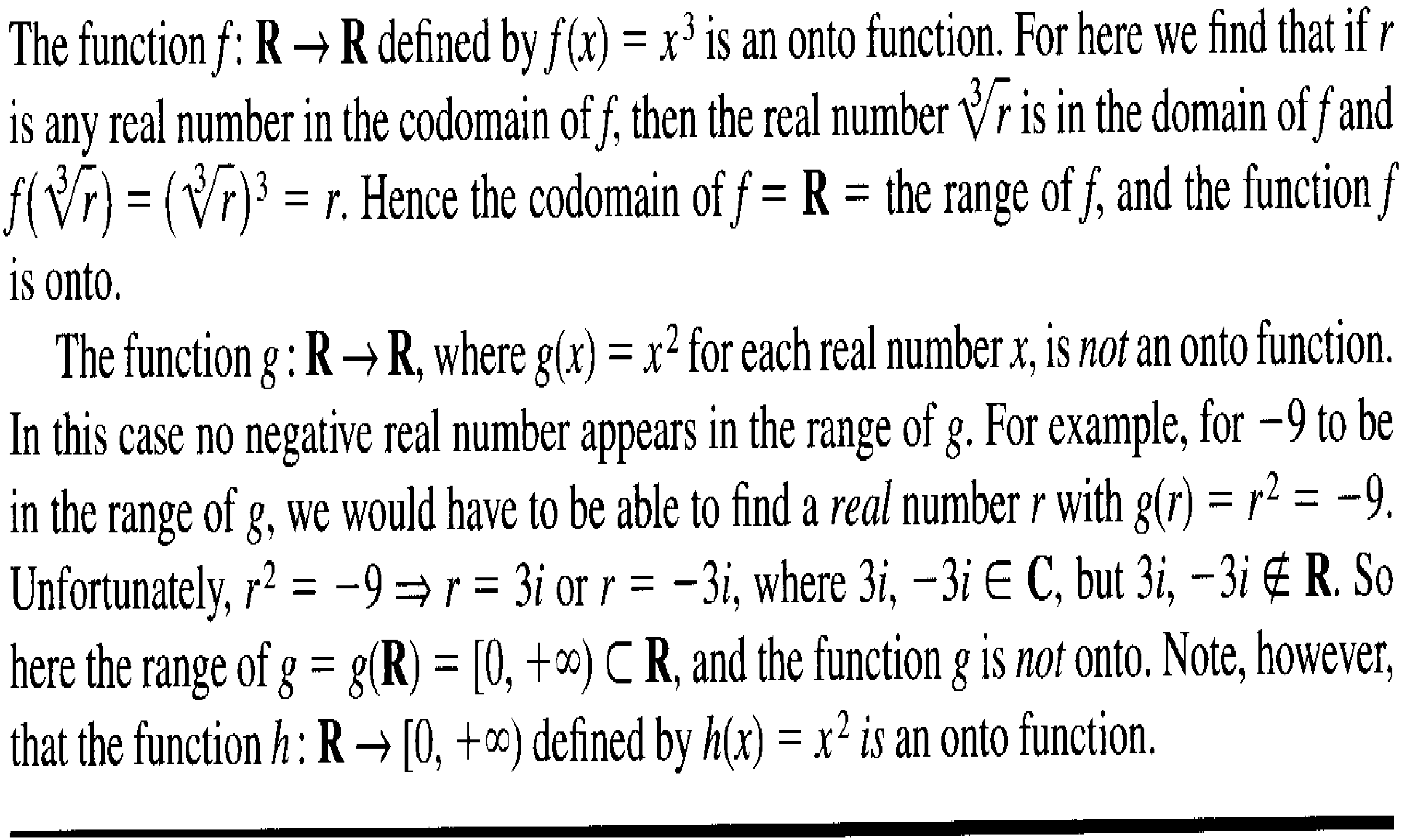
$$f = \{(1, 1), (2, 3), (3, 4)\}$$

is a one-to-one function from A to B;

$$g = \{(1, 1), (2, 3), (3, 3)\}$$

is a function from A to B, but it fails to be one-to-one because $g(2) = g(3)$ but $2 \neq 3$.

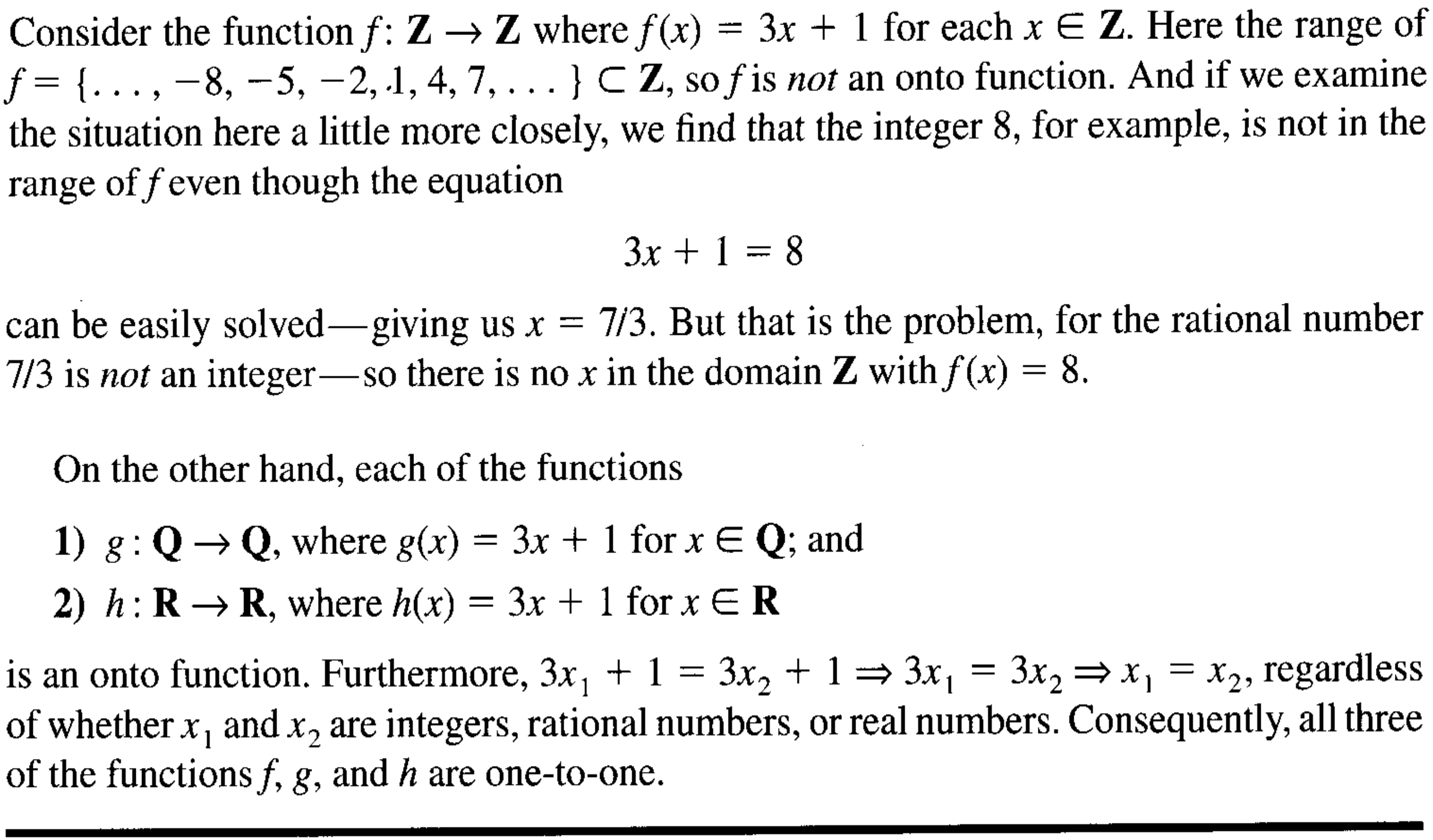
Example



The function $f: \mathbf{R} \to \mathbf{R}$ defined by $f(x) = x^3$ is an onto function. For here we find that if r is any real number in the codomain of f, then the real number $\sqrt[3]{r}$ is in the domain of f and $f(\sqrt[3]{r}) = (\sqrt[3]{r})^3 = r$. Hence the codomain of $f = \mathbf{R} =$ the range of f, and the function f is onto.

The function $g: \mathbf{R} \to \mathbf{R}$, where $g(x) = x^2$ for each real number x, is *not* an onto function. In this case no negative real number appears in the range of g. For example, for -9 to be in the range of g, we would have to be able to find a *real* number r with $g(r) = r^2 = -9$. Unfortunately, $r^2 = -9 \Rightarrow r = 3i$ or $r = -3i$, where $3i, -3i \in \mathbf{C}$, but $3i, -3i \notin \mathbf{R}$. So here the range of $g = g(\mathbf{R}) = [0, +\infty) \subset \mathbf{R}$, and the function g is *not* onto. Note, however, that the function $h: \mathbf{R} \to [0, +\infty)$ defined by $h(x) = x^2$ *is* an onto function.

Example



Consider the function $f\colon \mathbf{Z} \to \mathbf{Z}$ where $f(x) = 3x + 1$ for each $x \in \mathbf{Z}$. Here the range of $f = \{\ldots, -8, -5, -2, 1, 4, 7, \ldots\} \subset \mathbf{Z}$, so f is *not* an onto function. And if we examine the situation here a little more closely, we find that the integer 8, for example, is not in the range of f even though the equation

$$3x + 1 = 8$$

can be easily solved—giving us $x = 7/3$. But that is the problem, for the rational number 7/3 is *not* an integer—so there is no x in the domain $\mathbf{Z}$ with $f(x) = 8$.

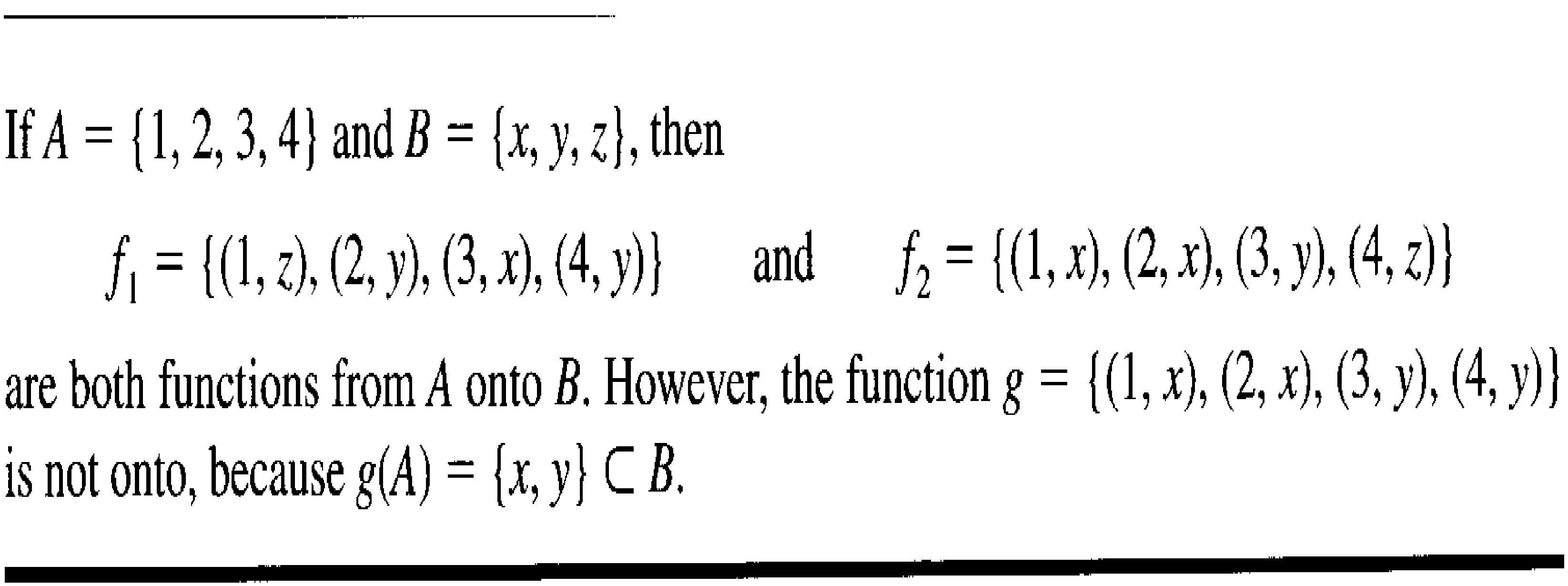
On the other hand, each of the functions

1) $g : \mathbf{Q} \to \mathbf{Q}$, where $g(x) = 3x + 1$ for $x \in \mathbf{Q}$; and

2) $h : \mathbf{R} \to \mathbf{R}$, where $h(x) = 3x + 1$ for $x \in \mathbf{R}$

is an onto function. Furthermore, $3x_1 + 1 = 3x_2 + 1 \Rightarrow 3x_1 = 3x_2 \Rightarrow x_1 = x_2$, regardless of whether x_1 and x_2 are integers, rational numbers, or real numbers. Consequently, all three of the functions f, g, and h are one-to-one.

Example



If $A = \{1, 2, 3, 4\}$ and $B = \{x, y, z\}$, then

$$f_1 = \{(1, z), (2, y), (3, x), (4, y)\} \qquad \text{and} \qquad f_2 = \{(1, x), (2, x), (3, y), (4, z)\}$$

are both functions from A onto B. However, the function $g = \{(1, x), (2, x), (3, y), (4, y)\}$ is not onto, because $g(A) = \{x, y\} \subset B$.

Example

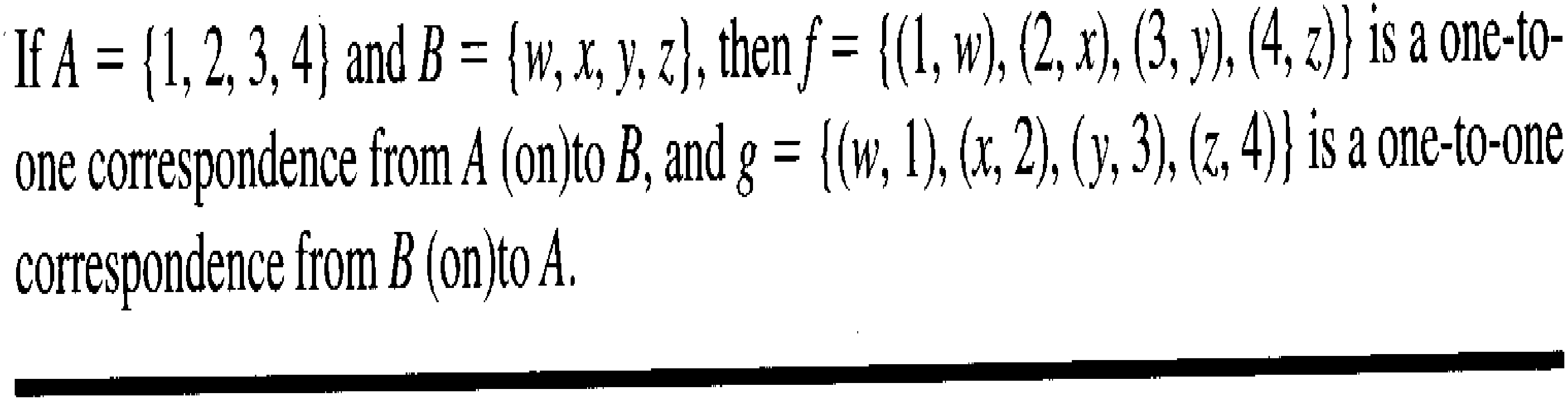
If $A = \{x, y, z\}$ and $B = \{1, 2\}$, then all functions $f: A \to B$ are onto except $f_1 = \{(x, 1), (y, 1), (z, 1)\}$, and $f_2 = \{(x, 2), (y, 2), (z, 2)\}$, the *constant* functions. So there are $|B|^{|A|} - 2 = 2^3 - 2 = 6$ onto functions from A to B.

In general, if $|A| = m \geq 2$ and $|B| = 2$, then there are $2^m - 2$ onto functions from A to B. (Does this formula tell us anything when $m = 1$?)

5.6 Function Composition and Inverse Functions

- In this section we study a method for combining two functions into a single function. Then we develop the concept of the inverse (of a function) for functions.
- **Definition 5.15:** If f:$A \to B$, then f is said to be *bijective*, or to be a *one-to-one correspondence*, if f is both one-to-one and onto.

Example

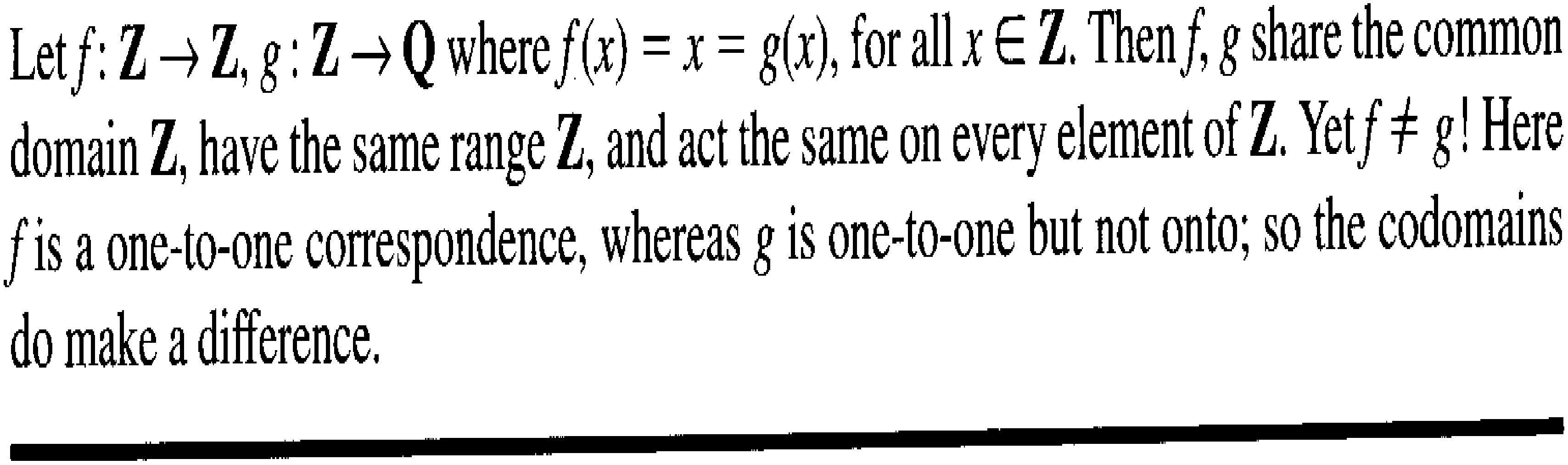


If $A = \{1, 2, 3, 4\}$ and $B = \{w, x, y, z\}$, then $f = \{(1, w), (2, x), (3, y), (4, z)\}$ is a one-to-one correspondence from A (on)to B, and $g = \{(w, 1), (x, 2), (y, 3), (z, 4)\}$ is a one-to-one correspondence from B (on)to A.

Definition

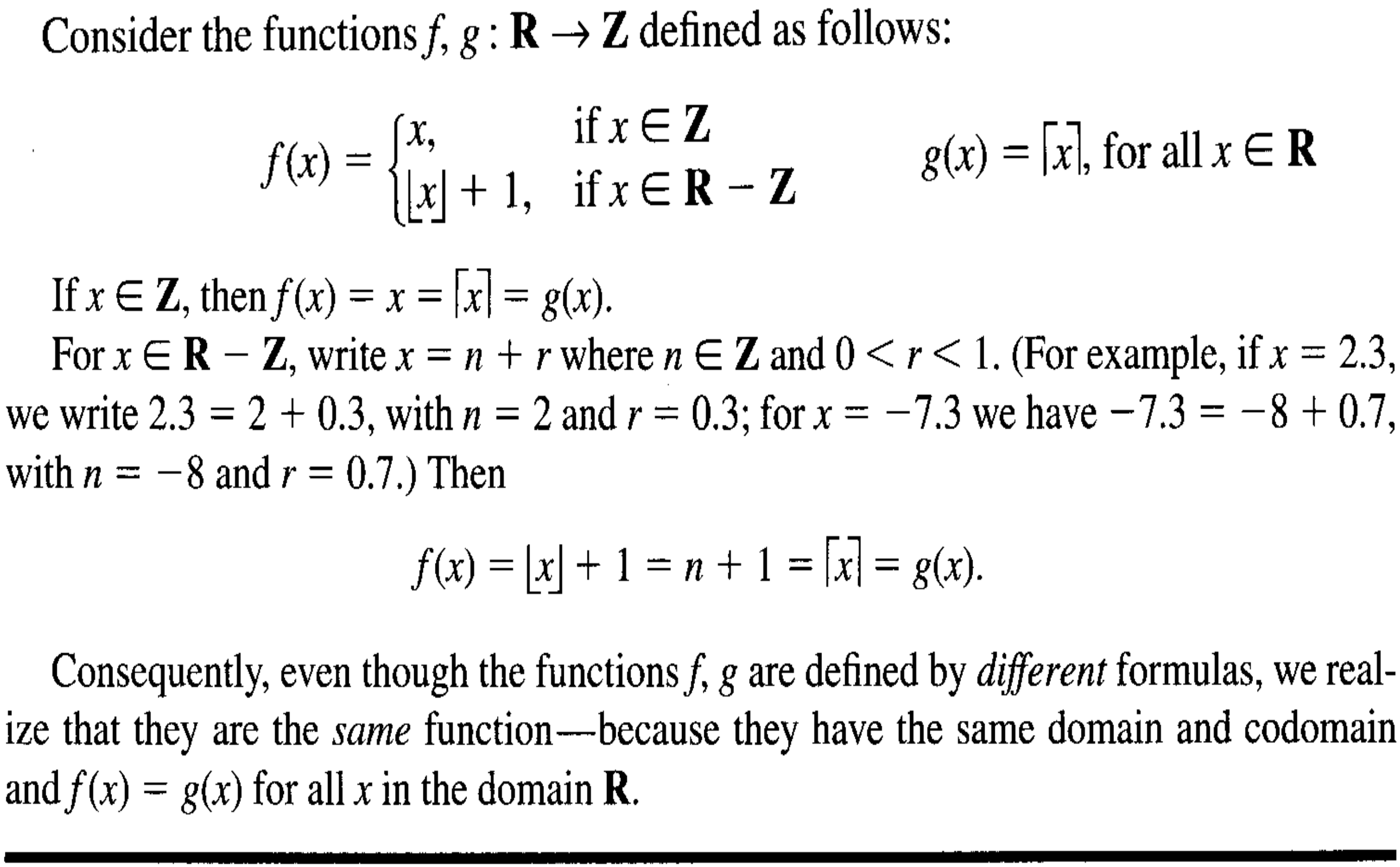
- **Definition 5.16:** The function I_A: $A \rightarrow A$, defined by $I_A(a) = a$ for all $a \in A$, is called the *identity function* for A.
- **Definition 5.17:** If f, g: $A \rightarrow B$, we say that f and g are *equal* and write $f = g$, if $f(a) = g(a)$ for all $a \in A$.

Example



Let $f : \mathbf{Z} \to \mathbf{Z}$, $g : \mathbf{Z} \to \mathbf{Q}$ where $f(x) = x = g(x)$, for all $x \in \mathbf{Z}$. Then f, g share the common domain $\mathbf{Z}$, have the same range $\mathbf{Z}$, and act the same on every element of $\mathbf{Z}$. Yet $f \neq g$! Here f is a one-to-one correspondence, whereas g is one-to-one but not onto; so the codomains do make a difference.

Example



Consider the functions $f, g : \mathbf{R} \to \mathbf{Z}$ defined as follows:

$$f(x) = \begin{cases} x, & \text{if } x \in \mathbf{Z} \\ \lfloor x \rfloor + 1, & \text{if } x \in \mathbf{R} - \mathbf{Z} \end{cases} \qquad g(x) = \lceil x \rceil, \text{ for all } x \in \mathbf{R}$$

If $x \in \mathbf{Z}$, then $f(x) = x = \lceil x \rceil = g(x)$.

For $x \in \mathbf{R} - \mathbf{Z}$, write $x = n + r$ where $n \in \mathbf{Z}$ and $0 < r < 1$. (For example, if $x = 2.3$, we write $2.3 = 2 + 0.3$, with $n = 2$ and $r = 0.3$; for $x = -7.3$ we have $-7.3 = -8 + 0.7$, with $n = -8$ and $r = 0.7$.) Then

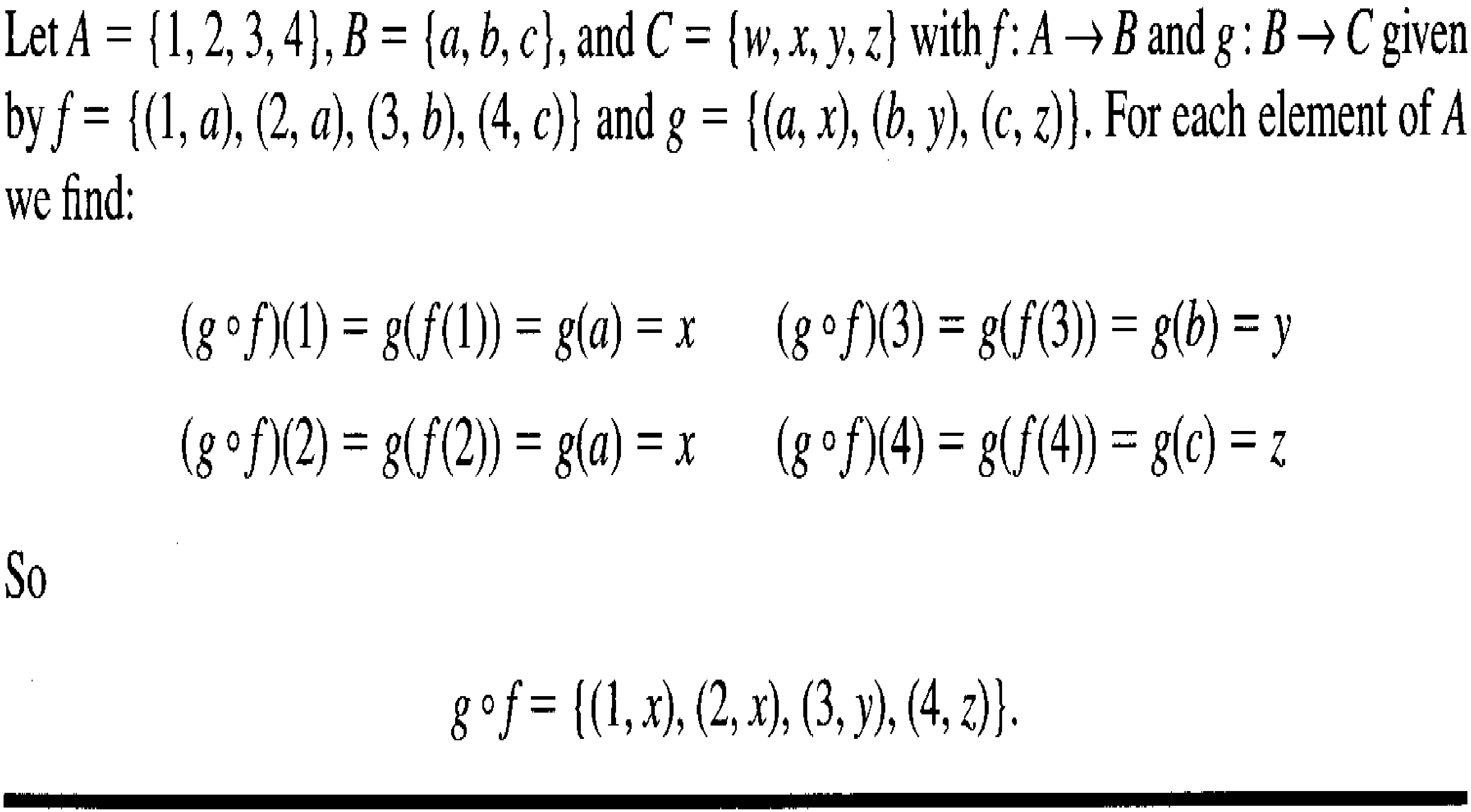
$$f(x) = \lfloor x \rfloor + 1 = n + 1 = \lceil x \rceil = g(x).$$

Consequently, even though the functions f, g are defined by *different* formulas, we realize that they are the *same* function—because they have the same domain and codomain and $f(x) = g(x)$ for all x in the domain $\mathbf{R}$.

Definition

- If f: $A \to B$ and g: $B \to C$, we define the *composite function*, which is denoted $g \circ f$: $A \to C$, by $g \circ f(a) = g(f(a))$, for each $a \in A$.

Example



Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c\}$, and $C = \{w, x, y, z\}$ with $f : A \to B$ and $g : B \to C$ given by $f = \{(1, a), (2, a), (3, b), (4, c)\}$ and $g = \{(a, x), (b, y), (c, z)\}$. For each element of A we find:

$$(g \circ f)(1) = g(f(1)) = g(a) = x \qquad (g \circ f)(3) = g(f(3)) = g(b) = y$$

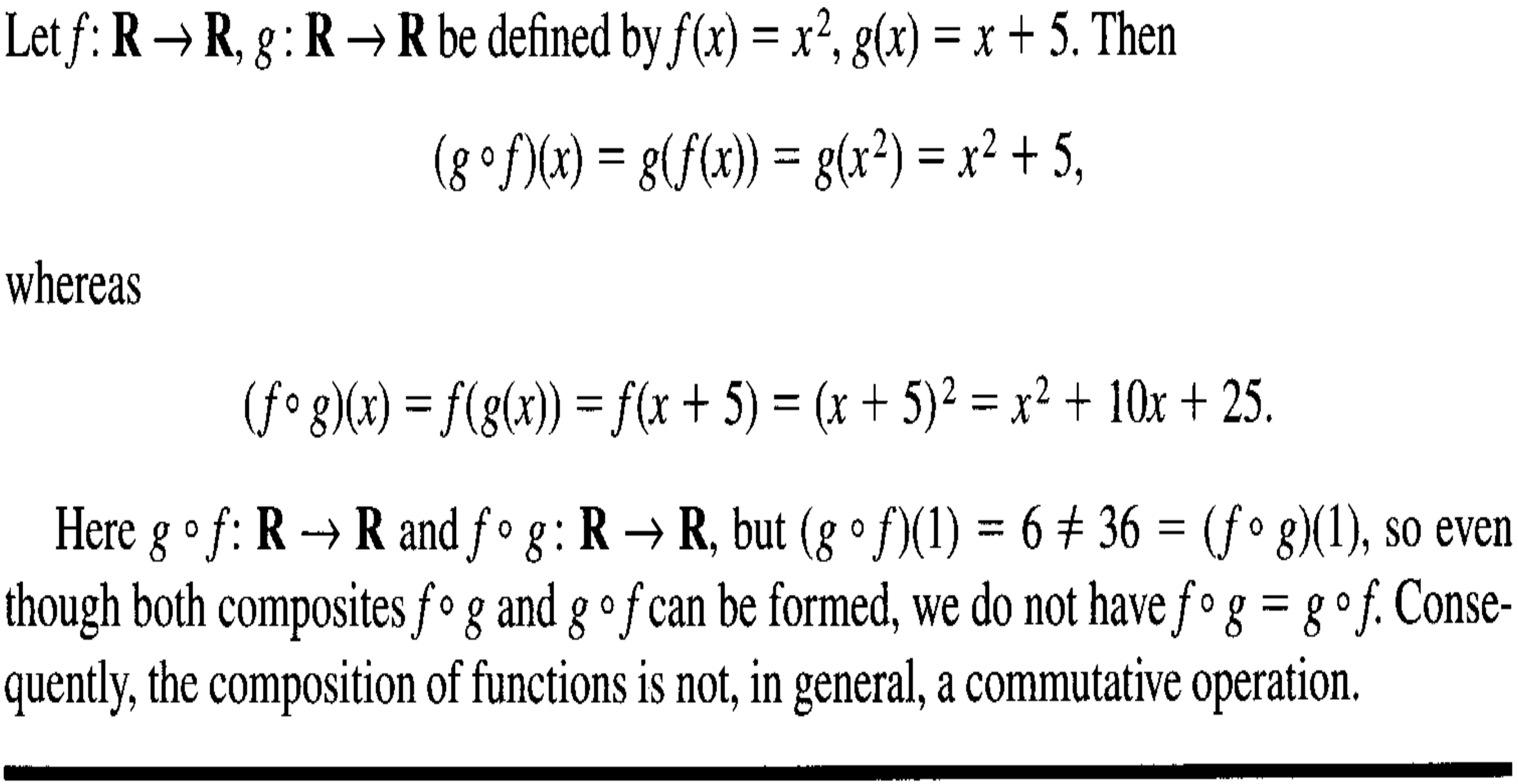
$$(g \circ f)(2) = g(f(2)) = g(a) = x \qquad (g \circ f)(4) = g(f(4)) = g(c) = z$$

So

$$g \circ f = \{(1, x), (2, x), (3, y), (4, z)\}.$$

Example

- For any f: $A \to B$, we observe that $f \circ I_A = f = I_B \circ f$.



Let $f: \mathbf{R} \to \mathbf{R}$, $g: \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = x^2$, $g(x) = x + 5$. Then

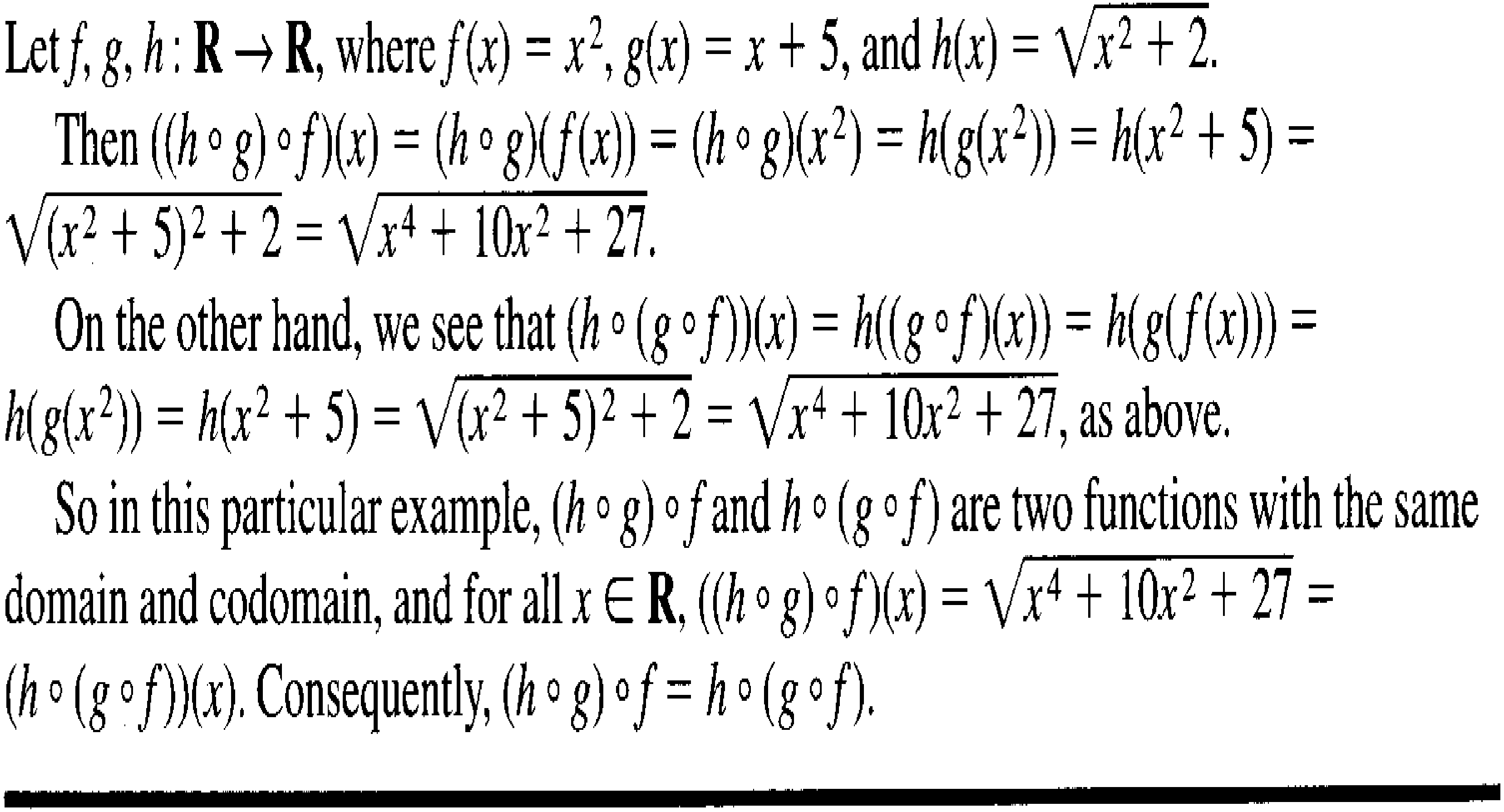
$$(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 5,$$

whereas

$$(f \circ g)(x) = f(g(x)) = f(x + 5) = (x + 5)^2 = x^2 + 10x + 25.$$

Here $g \circ f: \mathbf{R} \to \mathbf{R}$ and $f \circ g: \mathbf{R} \to \mathbf{R}$, but $(g \circ f)(1) = 6 \neq 36 = (f \circ g)(1)$, so even though both composites $f \circ g$ and $g \circ f$ can be formed, we do not have $f \circ g = g \circ f$. Consequently, the composition of functions is not, in general, a commutative operation.

Example 5.55: page 252.



Let $f, g, h: \mathbf{R} \to \mathbf{R}$, where $f(x) = x^2$, $g(x) = x + 5$, and $h(x) = \sqrt{x^2 + 2}$.

Then $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = (h \circ g)(x^2) = h(g(x^2)) = h(x^2 + 5) = \sqrt{(x^2 + 5)^2 + 2} = \sqrt{x^4 + 10x^2 + 27}$.

On the other hand, we see that $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = h(g(x^2)) = h(x^2 + 5) = \sqrt{(x^2 + 5)^2 + 2} = \sqrt{x^4 + 10x^2 + 27}$, as above.

So in this particular example, $(h \circ g) \circ f$ and $h \circ (g \circ f)$ are two functions with the same domain and codomain, and for all $x \in \mathbf{R}$, $((h \circ g) \circ f)(x) = \sqrt{x^4 + 10x^2 + 27} = (h \circ (g \circ f))(x)$. Consequently, $(h \circ g) \circ f = h \circ (g \circ f)$.

.

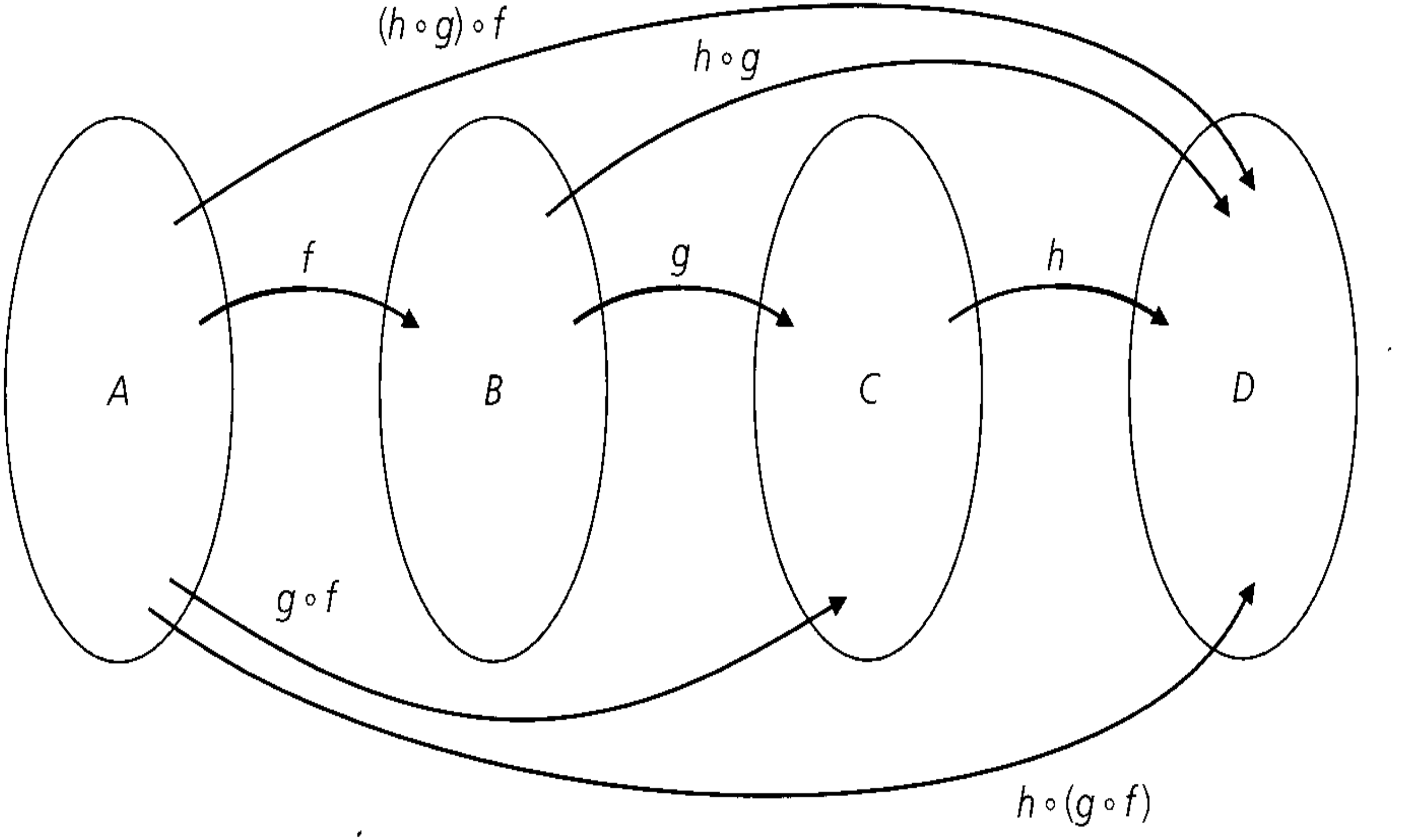
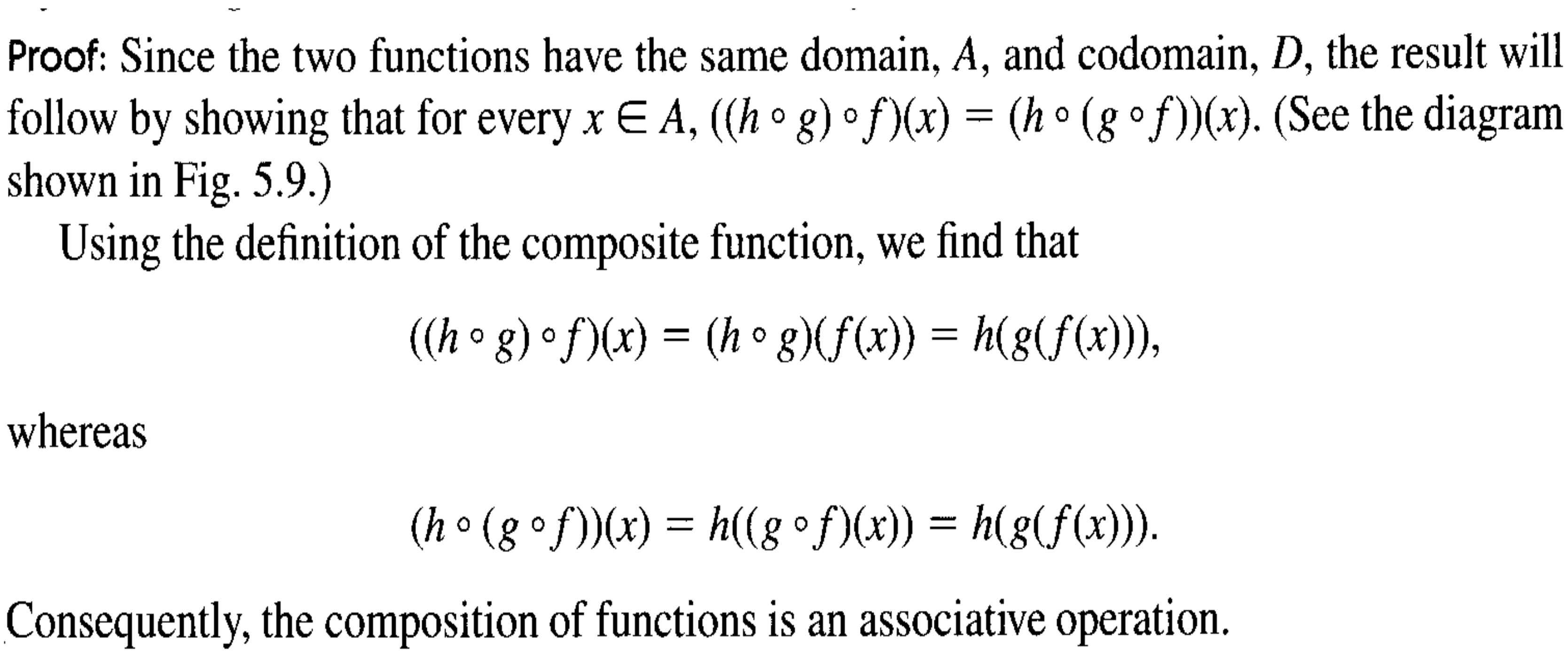


Figure 5.9

Theorem 5.6:

- If $f: A \to B$, $g: B \to C$, and $h: C \to D$, then $(h\circ g)\circ f = h\circ(g\circ f)$.



Proof: Since the two functions have the same domain, A, and codomain, D, the result will follow by showing that for every $x \in A$, $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$. (See the diagram shown in Fig. 5.9.)

Using the definition of the composite function, we find that

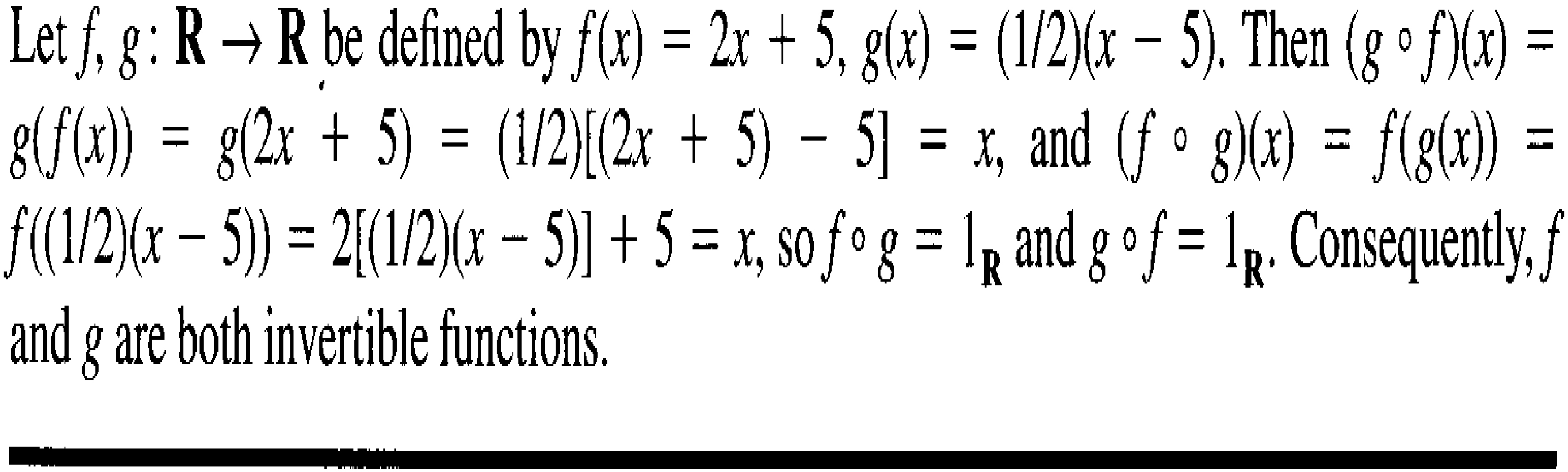
$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))),$$

whereas

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

Consequently, the composition of functions is an associative operation.

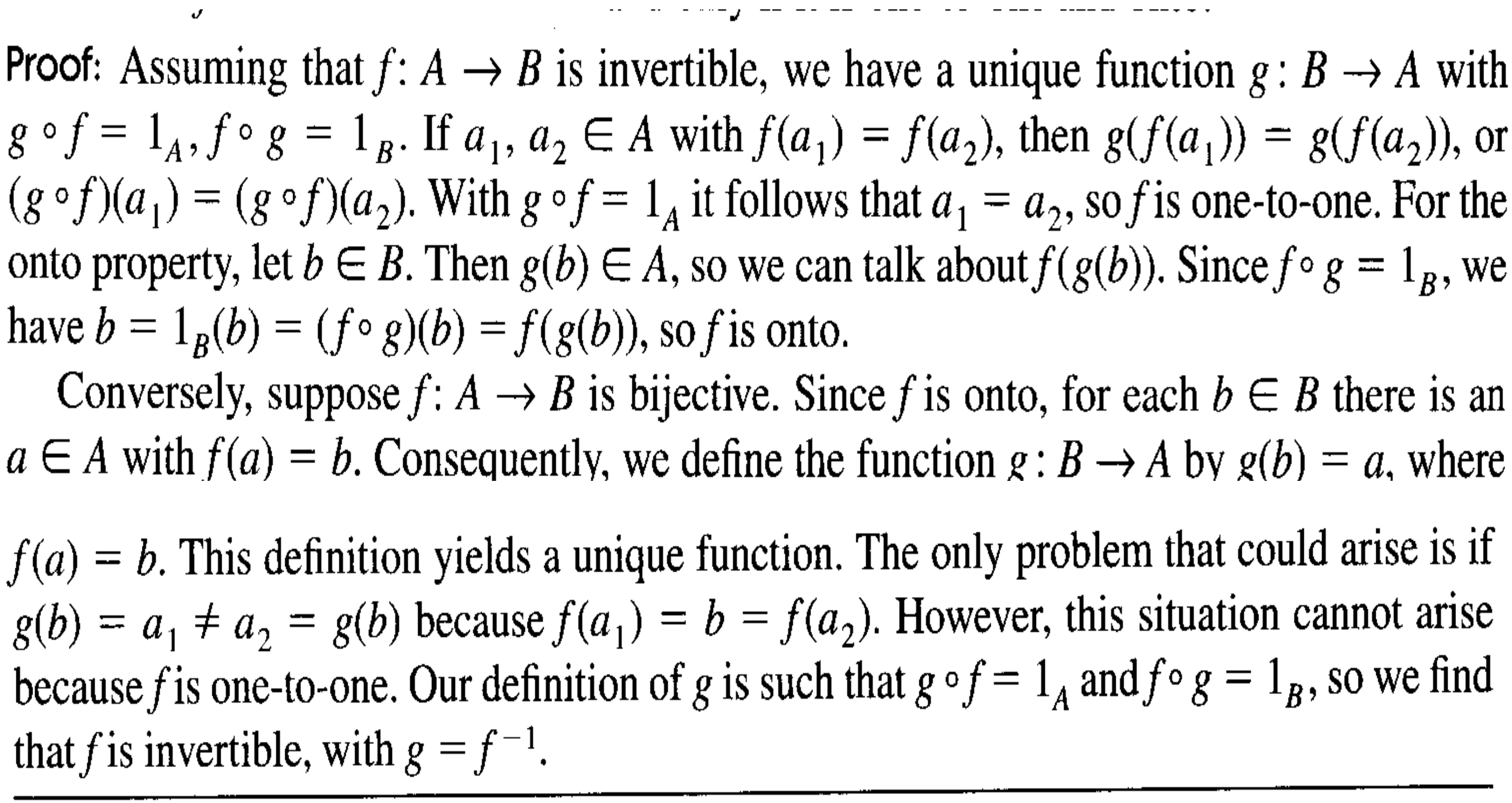
Example



Let $f, g : \mathbf{R} \to \mathbf{R}$ be defined by $f(x) = 2x + 5$, $g(x) = (1/2)(x - 5)$. Then $(g \circ f)(x) = g(f(x)) = g(2x + 5) = (1/2)[(2x + 5) - 5] = x$, and $(f \circ g)(x) = f(g(x)) = f((1/2)(x - 5)) = 2[(1/2)(x - 5)] + 5 = x$, so $f \circ g = 1_{\mathbf{R}}$ and $g \circ f = 1_{\mathbf{R}}$. Consequently, f and g are both invertible functions.

Theorem

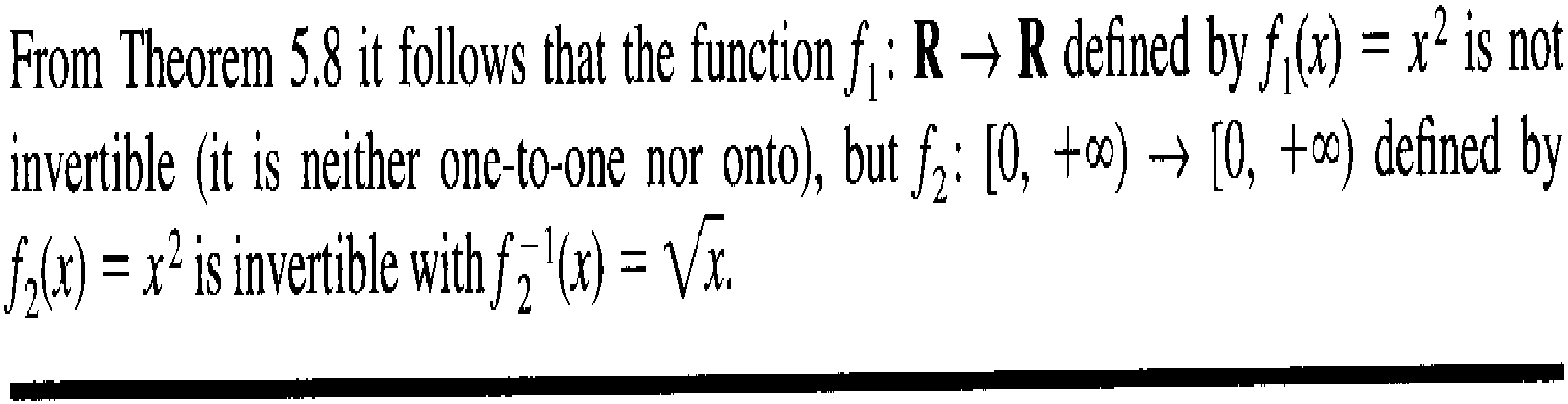
- A function *f*: *A* → *B* is invertible if and only if it is one-to-one and onto.



Proof: Assuming that $f: A \to B$ is invertible, we have a unique function $g: B \to A$ with $g \circ f = 1_A, f \circ g = 1_B$. If $a_1, a_2 \in A$ with $f(a_1) = f(a_2)$, then $g(f(a_1)) = g(f(a_2))$, or $(g \circ f)(a_1) = (g \circ f)(a_2)$. With $g \circ f = 1_A$ it follows that $a_1 = a_2$, so f is one-to-one. For the onto property, let $b \in B$. Then $g(b) \in A$, so we can talk about $f(g(b))$. Since $f \circ g = 1_B$, we have $b = 1_B(b) = (f \circ g)(b) = f(g(b))$, so f is onto.

Conversely, suppose $f: A \to B$ is bijective. Since f is onto, for each $b \in B$ there is an $a \in A$ with $f(a) = b$. Consequently, we define the function $g: B \to A$ by $g(b) = a$, where $f(a) = b$. This definition yields a unique function. The only problem that could arise is if $g(b) = a_1 \neq a_2 = g(b)$ because $f(a_1) = b = f(a_2)$. However, this situation cannot arise because f is one-to-one. Our definition of g is such that $g \circ f = 1_A$ and $f \circ g = 1_B$, so we find that f is invertible, with $g = f^{-1}$.

Example

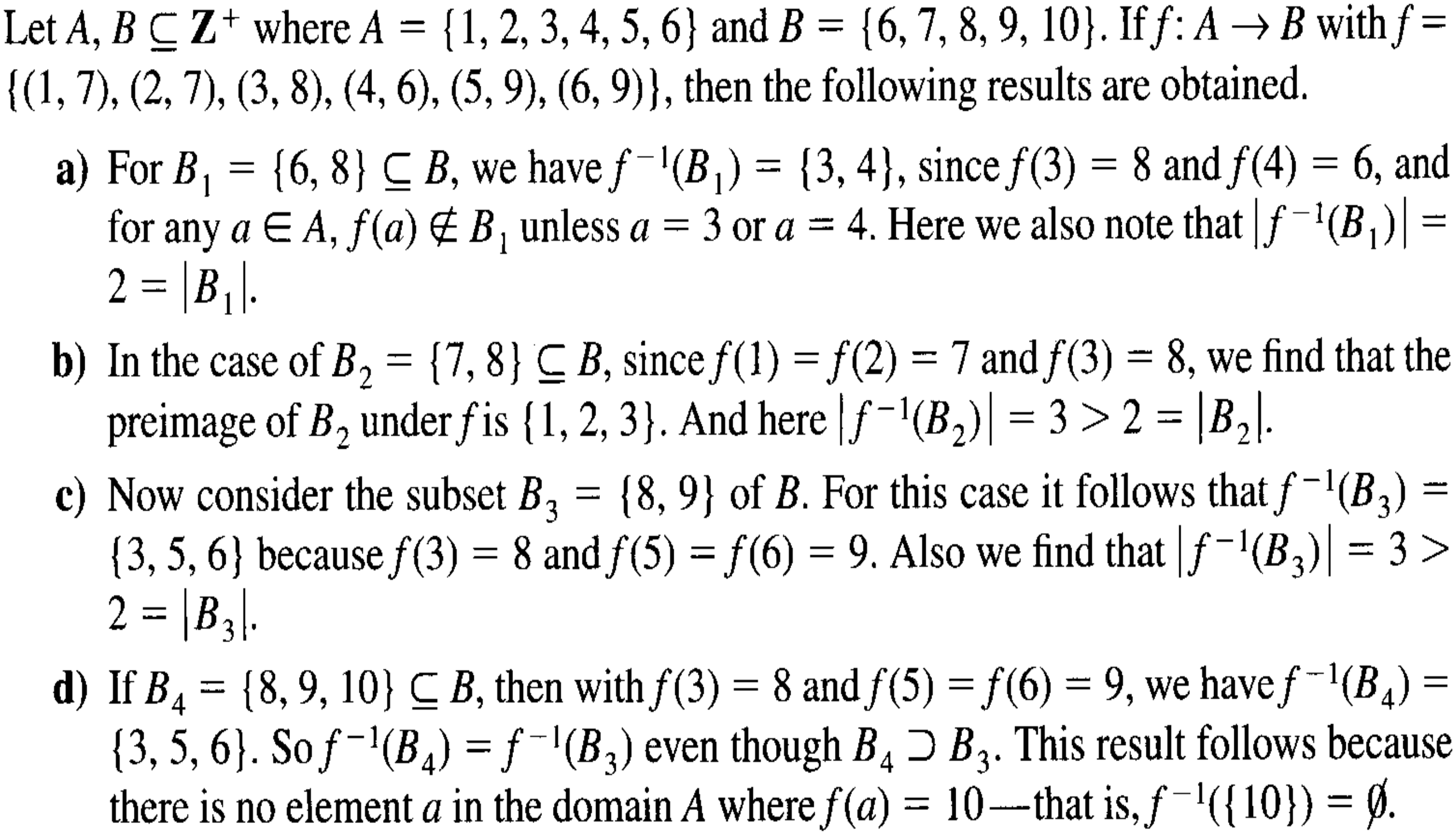


From Theorem 5.8 it follows that the function $f_1 : \mathbf{R} \rightarrow \mathbf{R}$ defined by $f_1(x) = x^2$ is not invertible (it is neither one-to-one nor onto), but $f_2 : [0, +\infty) \rightarrow [0, +\infty)$ defined by $f_2(x) = x^2$ is invertible with $f_2^{-1}(x) = \sqrt{x}$.

Theorem

- if f: $A \to B$, g: $B \to C$ are invertible functions, then $g \circ f$: $A \to C$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Example



Let $A, B \subseteq \mathbf{Z}^+$ where $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{6, 7, 8, 9, 10\}$. If $f: A \rightarrow B$ with $f = \{(1, 7), (2, 7), (3, 8), (4, 6), (5, 9), (6, 9)\}$, then the following results are obtained.

a) For $B_1 = \{6, 8\} \subseteq B$, we have $f^{-1}(B_1) = \{3, 4\}$, since $f(3) = 8$ and $f(4) = 6$, and for any $a \in A$, $f(a) \notin B_1$ unless $a = 3$ or $a = 4$. Here we also note that $|f^{-1}(B_1)| = 2 = |B_1|$.

b) In the case of $B_2 = \{7, 8\} \subseteq B$, since $f(1) = f(2) = 7$ and $f(3) = 8$, we find that the preimage of B_2 under f is $\{1, 2, 3\}$. And here $|f^{-1}(B_2)| = 3 > 2 = |B_2|$.

c) Now consider the subset $B_3 = \{8, 9\}$ of B. For this case it follows that $f^{-1}(B_3) = \{3, 5, 6\}$ because $f(3) = 8$ and $f(5) = f(6) = 9$. Also we find that $|f^{-1}(B_3)| = 3 > 2 = |B_3|$.

d) If $B_4 = \{8, 9, 10\} \subseteq B$, then with $f(3) = 8$ and $f(5) = f(6) = 9$, we have $f^{-1}(B_4) = \{3, 5, 6\}$. So $f^{-1}(B_4) = f^{-1}(B_3)$ even though $B_4 \supset B_3$. This result follows because there is no element a in the domain A where $f(a) = 10$—that is, $f^{-1}(\{10\}) = \emptyset$.

Example

Let f: $\mathbf{R} \to \mathbf{R}$ be defined by

$$f(x) = \begin{cases} 3x - 5, & x > 0 \\ -3x + 1, & x \le 0. \end{cases}$$

a) Determine $f(0)$, $f(1)$, $f(-1)$, $f(5/3)$, and $f(-5/3)$.

b) Find $f^{-1}(0)$, $f^{-1}(1)$, $f^{-1}(-1)$, $f^{-1}(3)$, $f^{-1}(-3)$, and $f^{-1}(-6)$.

c) What are $f^{-1}([-5, 5])$ and $f^{-1}([-6, 5])$?

a) $f(0) = -3(0) + 1 = 1$ $\quad$ $f(5/3) = 3(5/3) - 5 = 0$

$f(1) = 3(1) - 5 = -2$ $\quad$ $f(-5/3) = -3(-5/3) + 1 = 6$

$f(-1) = -3(-1) + 1 = 4$

b)
$$\begin{aligned} f^{-1}(0) &= \{x \in \mathbf{R} \mid f(x) \in \{0\}\} = \{x \in \mathbf{R} \mid f(x) = 0\} \\ &= \{x \in \mathbf{R} \mid x > 0 \text{ and } 3x - 5 = 0\} \cup \{x \in \mathbf{R} \mid x \le 0 \text{ and } -3x + 1 = 0\} \\ &= \{x \in \mathbf{R} \mid x > 0 \text{ and } x = 5/3\} \cup \{x \in \mathbf{R} \mid x \le 0 \text{ and } x = 1/3\} \\ &= \{5/3\} \cup \emptyset = \{5/3\} \end{aligned}$$

[Note how the horizontal line $y = 0$—that is, the x-axis—intersects the graph in Fig. 5.11 only at the point $(5/3, 0)$.]

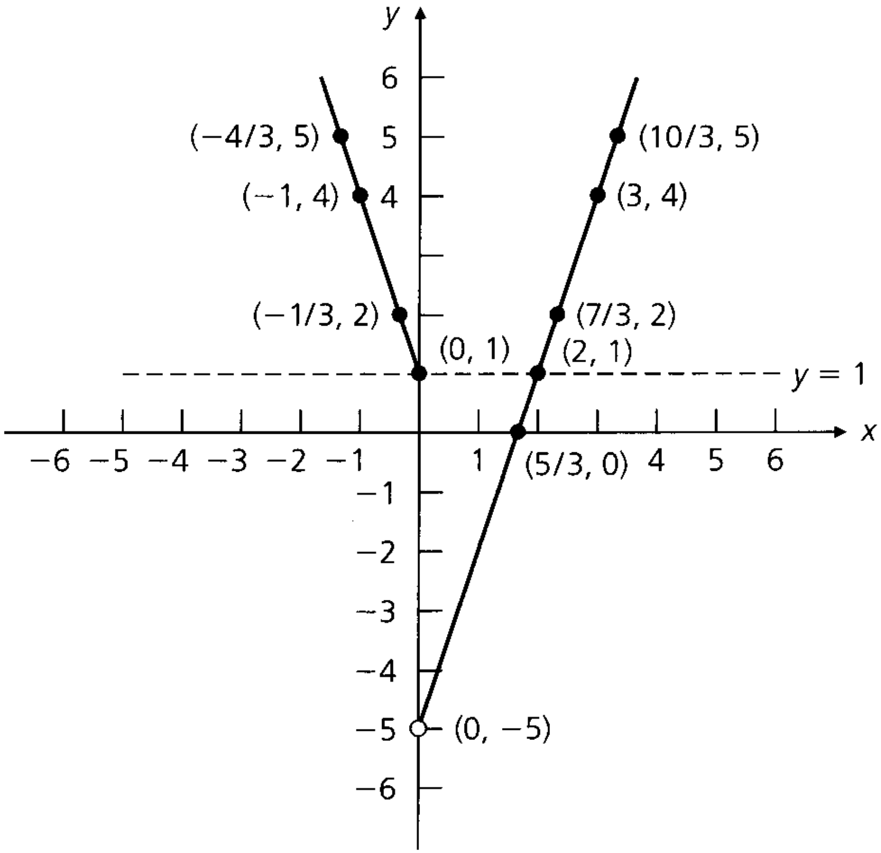


Figure 5.11

Example

$$
\begin{aligned}
f^{-1}(1) &= \{x \in \mathbf{R} \mid f(x) \in \{1\}\} = \{x \in \mathbf{R} \mid f(x) = 1\} \\
&= \{x \in \mathbf{R} \mid x > 0 \text{ and } 3x - 5 = 1\} \cup \{x \in \mathbf{R} \mid x \leq 0 \text{ and } -3x + 1 = 1\} \\
&= \{x \in \mathbf{R} \mid x > 0 \text{ and } x = 2\} \cup \{x \in \mathbf{R} \mid x \leq 0 \text{ and } x = 0\} \\
&= \{2\} \cup \{0\} = \{0, 2\}
\end{aligned}
$$

[Here we note how the dashed line $y = 1$ intersects the graph in Fig. 5.11 at the points (0, 1) and (2, 1).]

$$
\begin{aligned}
f^{-1}(-1) &= \{x \in \mathbf{R} \mid x > 0 \text{ and } 3x - 5 = -1\} \cup \{x \in \mathbf{R} \mid x \leq 0 \text{ and } -3x + 1 = -1\} \\
&= \{x \in \mathbf{R} \mid x > 0 \text{ and } x = 4/3\} \cup \{x \in \mathbf{R} \mid x \leq 0 \text{ and } x = 2/3\} \\
&= \{4/3\} \cup \emptyset = \{4/3\}
\end{aligned}
$$

$$
f^{-1}(3) = \{-2/3, 8/3\} \qquad f^{-1}(-3) = \{2/3\}
$$

Example

$f^{-1}(3) = \{-2/3, 8/3\}$ $\qquad$ $f^{-1}(-3) = \{2/3\}$

$$\begin{aligned} f^{-1}(-6) &= \{x \in \mathbf{R} \mid x > 0 \text{ and } 3x - 5 = -6\} \cup \{x \in \mathbf{R} \mid x \leq 0 \text{ and } -3x + 1 = -6\} \\ &= \{x \in \mathbf{R} \mid x > 0 \text{ and } x = -1/3\} \cup \{x \in \mathbf{R} \mid x \leq 0 \text{ and } x = 7/3\} \\ &= \emptyset \cup \emptyset = \emptyset \end{aligned}$$

c) $f^{-1}([-5, 5]) = \{x \mid f(x) \in [-5, 5]\} = \{x \mid -5 \leq f(x) \leq 5\}$.

(Case 1) $x > 0$: $\quad -5 \leq 3x - 5 \leq 5$

$0 \leq 3x \leq 10$

$0 \leq x \leq 10/3$—so we use $0 < x \leq 10/3$.

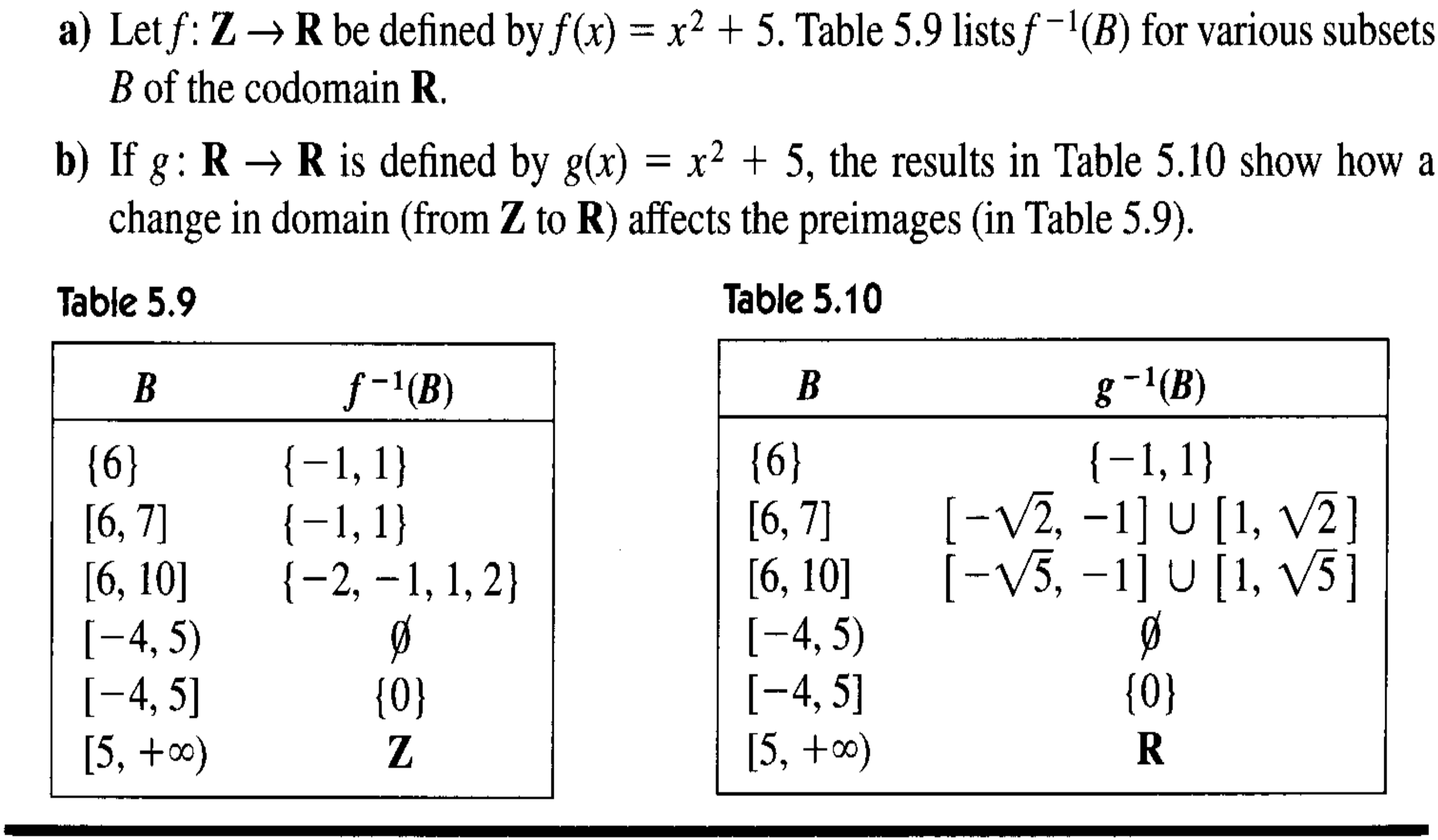
(Case 2) $x \leq 0$: $\quad -5 \leq -3x + 1 \leq 5$

$-6 \leq -3x \leq 4$

$2 \geq x \geq -4/3$—here we use $-4/3 \leq x \leq 0$.

Hence $f^{-1}([-5, 5]) = \{x \mid -4/3 \leq x \leq 0 \text{ or } 0 < x \leq 10/3\} = [-4/3, 10/3]$. Since there are no points (x, y) on the graph (in Fig. 5.11) where $y \leq -5$, it follows from our prior calculations that $f^{-1}([-6, 5]) = f^{-1}([-5, 5]) = [-4/3, 10/3]$.

Example



a) Let $f : \mathbf{Z} \rightarrow \mathbf{R}$ be defined by $f(x) = x^2 + 5$. Table 5.9 lists $f^{-1}(B)$ for various subsets B of the codomain $\mathbf{R}$.

b) If $g : \mathbf{R} \rightarrow \mathbf{R}$ is defined by $g(x) = x^2 + 5$, the results in Table 5.10 show how a change in domain (from $\mathbf{Z}$ to $\mathbf{R}$) affects the preimages (in Table 5.9).

Table 5.9

B	$f^{-1}(B)$
$\{6\}$	$\{-1, 1\}$
$[6, 7]$	$\{-1, 1\}$
$[6, 10]$	$\{-2, -1, 1, 2\}$
$[-4, 5)$	$\emptyset$
$[-4, 5]$	$\{0\}$
$[5, +\infty)$	$\mathbf{Z}$

Table 5.10

B	$g^{-1}(B)$
$\{6\}$	$\{-1, 1\}$
$[6, 7]$	$[-\sqrt{2}, -1] \cup [1, \sqrt{2}]$
$[6, 10]$	$[-\sqrt{5}, -1] \cup [1, \sqrt{5}]$
$[-4, 5)$	$\emptyset$
$[-4, 5]$	$\{0\}$
$[5, +\infty)$	$\mathbf{R}$

Cardinality

Definition: The *cardinality* of a set *A* is said to be equal to the cardinality of a set *B*, denoted by

$$|A| = |\mathrm{B}|,$$

if and only if there is a one-to-one correspondence (*i.e.*, a bijection) from *A* to *B*.

- If there is a one-to-one function (*i.e.*, an injection) from *A* to *B*, the cardinality of *A* is less than or the same as the cardinality of *B* and we write $|A| \leq |B|$.

Cardinality

- **Definition**: A set A that has the same cardinality as the set N of natural numbers is called a ***countable set***. A set that is not countable is *uncountable*.
- The set of real numbers **R** is an uncountable set.
- When an infinite set is countable (*countably infinite*) its cardinality is $\aleph_0$ (where ℵ is aleph, the 1st letter of the Hebrew alphabet). We write $|S| = \aleph_0$ and say that S has cardinality “aleph null.”

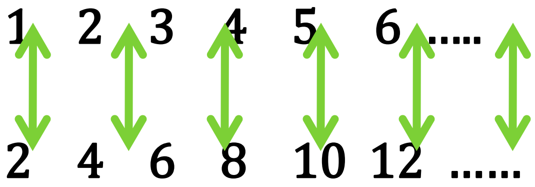
Showing that a Set is Countable

- An infinite set is countable if and only if it is possible to list the elements of the set in a sequence (indexed by the positive integers) i.e if there is one to one correspondence with the set of Natural numbers
- The reason for this is that a one-to-one correspondence *f* from the set of positive integers to a set *S* can be expressed in terms of a sequence $a_1, a_2, \ldots, a_n, \ldots$ where $a_1 = f(1)$, $a_2 = f(2), \ldots, a_n = f(n), \ldots$

Showing that a Set is Countable

Example 1: Show that the set of positive even integers E is countable set.

Solution: Let $f(x) = 2x$.



1 2 3 4 5 6 …..

2 4 6 8 10 12 ……

Then f is a bijection from **N** to E since f is both one-to-one and onto. To show that it is one-to-one, suppose that $f(n) = f(m)$. Then $2n = 2m$, and so $n = m$. To see that it is onto, suppose that t is an even positive integer. Then $t = 2k$ for some positive integer k and $f(k) = t$.

Showing that a Set is Countable

Example 2: Show that the set of integers Z is countable.

Solution: Can list in a sequence:

$0, 1, -1, 2, -2, 3, -3$,……….

Or can define a bijection from N to Z:

- **When *n* is even:** $f(n) = n/2$
- **When *n* is odd:** $f(\mathrm{n}) = -(n-1)/2$

$$\text{i.e. } f(n) = \begin{cases} \frac{n}{2} & \text{, When } n \text{ is even} \\ \frac{-(n-1)}{2} & \text{, When } n \text{ is odd} \end{cases}$$

The Positive Rational Numbers are Countable

- **Definition**: A *rational number* can be expressed as the ratio of two integers *p* and *q* such that $q \neq 0$.
  - ¾ is a rational number
  - $\sqrt{2}$ is not a rational number.

Example 3: Show that the positive rational numbers are countable.

Solution: The positive rational numbers are countable since they can be arranged in a sequence:

$$r_1, r_2, r_3, \ldots$$

The next slide shows how this is done. →

The Positive Rational Numbers are Countable

The set of rational numbers R is also countable.

- *Proof*: in two steps.

a) ***Card(N) ≤ Card(R)****, because each natural number is rational*: *N* ⊆ *R.*

b) Now we construct a mapping of *N* **onto** *R* (*surjection N onto R*), by which we prove that ***Card(R) ≤ Card(N)***:

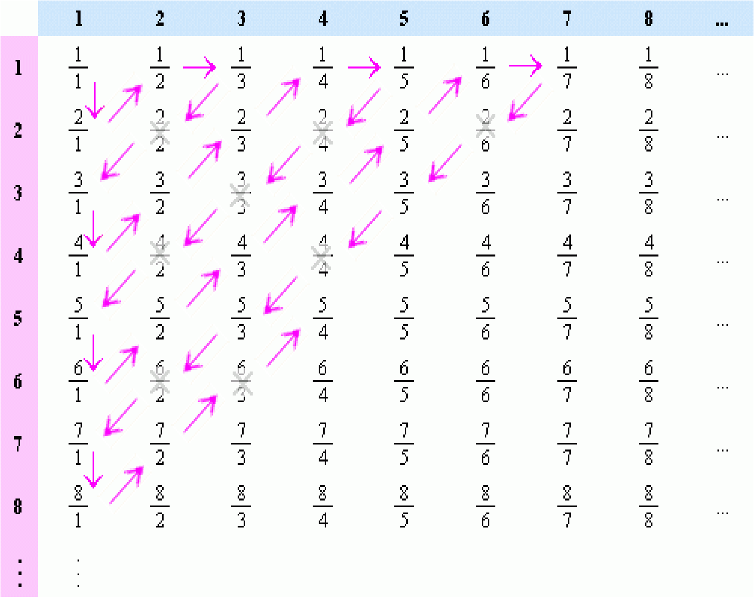
1 2 3 4 5 6 …

1/1 2/1 1/2 1/3 2/2 3/1 …

But, in the table there are repeating rationales, hence the mapping is not one-to-one. However, no rational number is omitted, therefore it is a mapping of N ***onto R (surjection).***

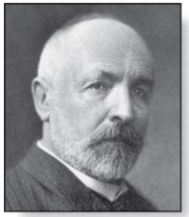
Card(N) = Card(R).

First column *q* = 1.
Second column *q* = 2. etc.



	1	2	3	4	5	6	7	8	...
1	$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{5}$	$\frac{1}{6}$	$\frac{1}{7}$	$\frac{1}{8}$	⋯
2	$\frac{2}{1}$	$\cancel{\frac{2}{2}}$	$\frac{2}{3}$	$\cancel{\frac{2}{4}}$	$\frac{2}{5}$	$\cancel{\frac{2}{6}}$	$\frac{2}{7}$	$\frac{2}{8}$	⋯
3	$\frac{3}{1}$	$\frac{3}{2}$	$\cancel{\frac{3}{3}}$	$\frac{3}{4}$	$\frac{3}{5}$	$\frac{3}{6}$	$\frac{3}{7}$	$\frac{3}{8}$	⋯
4	$\frac{4}{1}$	$\cancel{\frac{4}{2}}$	$\frac{4}{3}$	$\cancel{\frac{4}{4}}$	$\frac{4}{5}$	$\frac{4}{6}$	$\frac{4}{7}$	$\frac{4}{8}$	⋯
5	$\frac{5}{1}$	$\frac{5}{2}$	$\frac{5}{3}$	$\frac{5}{4}$	$\frac{5}{5}$	$\frac{5}{6}$	$\frac{5}{7}$	$\frac{5}{8}$	⋯
6	$\frac{6}{1}$	$\cancel{\frac{6}{2}}$	$\cancel{\frac{6}{3}}$	$\frac{6}{4}$	$\frac{6}{5}$	$\frac{6}{6}$	$\frac{6}{7}$	$\frac{6}{8}$	⋯
7	$\frac{7}{1}$	$\frac{7}{2}$	$\frac{7}{3}$	$\frac{7}{4}$	$\frac{7}{5}$	$\frac{7}{6}$	$\frac{7}{7}$	$\frac{7}{8}$	⋯
8	$\frac{8}{1}$	$\frac{8}{2}$	$\frac{8}{3}$	$\frac{8}{4}$	$\frac{8}{5}$	$\frac{8}{6}$	$\frac{8}{7}$	$\frac{8}{8}$	⋯
⋮	⋮								

The Real Numbers are Uncountable



Georg Cantor
(1845-1918)

Example: Show that the set of real numbers in [0,1] is uncountable.

Solution: The method is called the Cantor diagonalization argument and is a proof by contradiction.

- Suppose [0,1] is countable. Then all the real numbers between 0 and 1 can be listed in order $r_1, r_2, r_3, \ldots$ .Let the decimal representation of this listing be

$$\begin{aligned} r_1 &= 0.d_{11}d_{12}d_{13}d_{14}d_{15}d_{16}\ldots \\ r_2 &= 0.d_{21}d_{22}d_{23}d_{24}d_{25}d_{26}\ldots \\ r_3 &= 0.d_{31}d_{32}d_{33}d_{34}d_{35}d_{36}\ldots \\ &\vdots \end{aligned}$$

Where each d_{ii} *is one of the number of the set*$\{0,1,2,3,\ldots.9\}$($e.g. r_1 = 0.35765312$)
Form a new real number with the decimal expansion $c = 0.b_1b_2b_3b_4 \ldots\ldots\ldots$

where $b_i = \begin{cases} 1, if\ d_{ii} = 9 \\ 9 - d_{ii}, if\ d_{ii} = 0,1,..8 \end{cases}$.

5. *For all i. For those numbers which can be expressed in two different decimal expansions. e.g. ½ =0.5000000=0.49999999, we choose the expansion which ends with nine. This means we have a unique representation for all numbers. Clearly the numbers* $0.b_1b_2b_3\ldots.$ Is a real number between 0 and 1 that does not have trailing 0's. Now the real number c is not equal to any of $r_1, r_2, r_3 \ldots.$ $(Note\ it)$. Since there is a real number c between 0 and 1 that is not in the list which contradicts the assumption that the set is countably infinite. Hence [0,1] is uncountable.

Unit –II
(Group and Ring Theory)

Unit II (Group and Ring Theory)

- 1 Group
- 2 Subgroup
- 3 Homomorphism, Isomorphism
- 4 Cyclic Group
- 5 Lagrange Theorem
- 6 Normal Subgroup
- 7 Factor Group
- 8 Permutation Group
- 9 Rings and Field

Group

- Definition 16.1

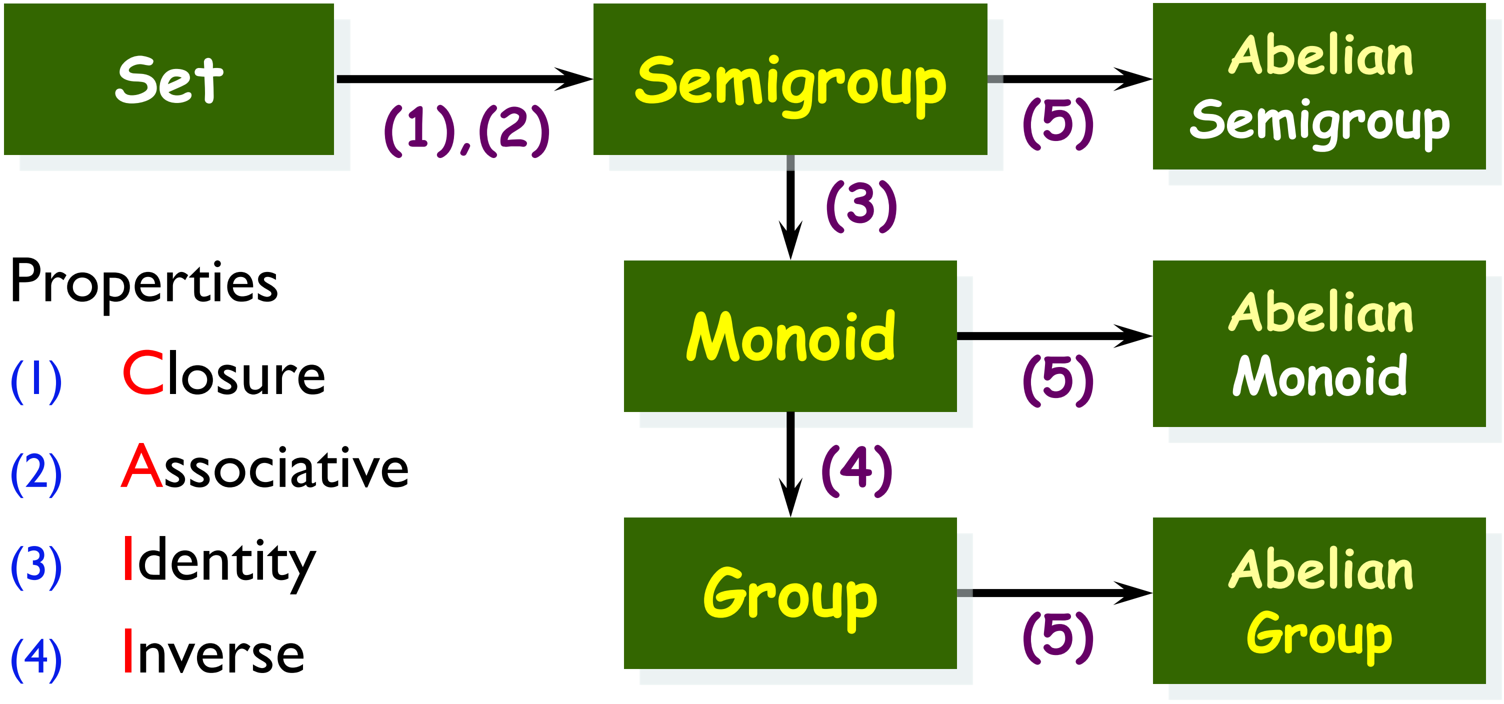
If G is a nonempty set and □ is a binary operation on G, then $<G,*>$ is called a *group* if the following conditions are satisfied.

1. For all $a,b \in G$, $a * b \in G$ (Closure of under *)
2. For all a, b, $c \in G$, $(a * b) * c = a * (b * c)$. (Associative)
3. There exists $e \in G$ with $e *a = a * e = a$ for all $a \in G$. (Existence of an Identity)
4. For each $a \in G$, there is an elements $a´ \in G$ such that $a´ * a = a * a´ = e$. (Existence of Inverses)

Abelian Group

- Abelian Group

5. A group $<G,*>$ is abelian if $*$ is commutative.
   i.e., $a * b = b * a$ for all $a, b \in G$.



Set

(1),(2)

Semigroup

(5)

Abelian Semigroup

(3)

Monoid

(5)

Abelian Monoid

(4)

Group

(5)

Abelian Group

Properties

(1) Closure

(2) Associative

(3) Identity

(4) Inverse

(5) Commutative

- The set of Real Numbers R for binary addition is group(why?)
- The Set of on zero real numbers R* for the binary operation x is a group.
- The set of positive integers Z^+ is not a group with respect to addition.
- The fourth roots of unity {1,-1,i,-i} from a group under multiplication. (Draw multiplication table)

$*$	1	-1	$\mathbf{i}$	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	I	$-i$	I	1
$-i$	$-i$	I	$-i$	-1

Z_n ={0,1 ,2 ,….n-1} modulo n

- The group Z_n uses only the integers from 0 to *n* - 1. Its basic operation is addition, which ends by reducing the result modulo *n*; that is, taking the integer remainder when the result is divided by *n*.

$$\begin{aligned} & 10 + 12 \, mod \, 15 \\ = & \ 22 \, mod \, 15 \\ = & \ 7 \end{aligned}$$

- $<Z_n ,+>$ is an abelian group.

Draw Multiplication Table

Associative ?

Identity : 0

Inverse exists in Z_n.

- (-a) for all a in Z_n
- We can also subtract element in Z_n.
- We define a-b in Z_n to be (a + (-b)) mod *n*.

Commutative?

Example : $< Z_n^*, \cdot >$, the integers coprime (relatively prime) to n from the set $\{0,1,2, \ldots n-1\}$ $of\ n$ non-negative integers form a group under multiplication modulo n, called the multiplicative group of integers modulo n

- Theorem :

  If n is any positive integer,

  $<Z_n^*, \cdot>$ is an abelian group.

- Example : The multiplication table of Z_9^* is

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

$< Z_9^*, \cdot >$

1) Closed

2) Associative

3) Identity

4) Inverse

5) Commutative

Properties of Groups

- For every group G,

(1) the identity of G is unique.

(2) the inverse of each element of G is unique.

(3) if $a, b, c \in G$, and $ab = ac$ → $b = c$

(Left-cancellation property)

(4) if $a, b, c \in G$, and $ba = ca$ → $b = c$

(Right-cancellation property)

(Notation) $a * b \rightarrow ab$

Properties of Groups

(**Proof**)

(1) If e_1, e_2 are both identities in G,

then $e_1 = e_1e_2 = e_2$

(2) Let $a \in G$ and suppose that b, c are both inverses of a,

then $b = be = b(ac) = (ba)c = ec = c$

(Note)

The properties (3),(4) imply that each group element appears exactly once in each row and each column of the table for a finite group

Properties of Groups

- Example : $< Z_9^*, \cdot >$,

$$ab = ac \rightarrow b = c \,, \qquad ba = ca \rightarrow b = c$$

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Properties of Groups

- Cancellation Laws hold in Group

  $ab = ac$ ➔ $b = c$, $ba = ca$ ➔ $b = c$ *For all a,b in G.*

Proof) In the first case multiply each member on the left by a^{-1} and use associativity.

$ab = ac$ ➔ $a^{-1}ab=a^{-1}ac$ ➔ $(a^{-1}a)b=(a^{-1}a)c$ ➔ $b = c$

- Show that in a group G show that $(a^{-1})^{-1} = a \; and \; (ab)^{-1} = b^{-1}a^{-1}$.
- Proof 2: Let $e \in G, then \; a * a^{-1} = e = a * a^{-1} \Rightarrow (a^{-1})^{-1} * (a^{-1})^{-1} = e$

$\Rightarrow a^{-1} * a = (a^{-1}) * (a^{-1})^{-1}$

$\Rightarrow a = (a^{-1})^{-1}$.

Also $a, b \in G \Rightarrow a^{-1}, b^{-1} \in G \; and \; ab \in G$

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

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

Hence we have the result.

- 1Prove that if $a^2 = a$, then $a = e$, a being the element of group.
- 2 Show that if every element has its own inverse in a group G then group G is abelian.
- Proof 2: It is given that $a = a^{-1}\ \forall\ a \in G$ hence

$if\ a \in G, b \in G\ then\ ab \in G\ and$ we have

$$ab = (ab)^{-1}$$

$$\Rightarrow ab = b^{-1}a^{-1}$$

$\Rightarrow ab = ba\ \forall a, b \in G$.

Order of Group

- Definition For every group G the number of elements in G is called the *order of* G and is denoted by $|G|$.

  When the number of elements in a group is not finite we say that G has infinite order.

  For all $n \in Z^+$, $|<Z_n, +>| = n$.

  $|<Z_p^*, \cdot>| = p-1$.

- Notice that $|<Z_n^*, \cdot>| = \phi(n)$.

Subgroup

- Definition Let G be a group and $G \supseteq H \neq \varnothing$.

  If H is a group under the binary operation on G, then we call H a subgroup of G.

  (Examples)

  - □ Every group G has $\{e\}$ and G as subgroup.
    - These are trivial subgroups of G.
  - □ $G = \langle Z_6, + \rangle$, $H = \{0,2,4\}$
  - □ The group $\langle Z, + \rangle$ is a subgroup of $\langle Q, + \rangle$, which is a subgroup of $\langle R, + \rangle$.

Examples

$< \{e\}, □ >$

1) Closed

   $e □ e = e$

2) Associative
3) Identity
4) Inverse
5) Commutative

$G = <Z_6 ,+> , H = \{0,2,4\}$

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Subgroup Condition (I)

- Theorem I

If H is a nonempty subset of a group G, then H is a subgroup of G ⇔

(a) for all $a, b \in H, ab \in H$, (closed) and

(b) for all $a \in H, a^{-1} \in H$. (inverse)

❑ Proof : (Necessary Condition)

Let H is subgroup of G. Hence H is group.

and $a, b \in H \Rightarrow ab \in H$ and $a^{-1} \in H$.

(Sufficient Condition)

Assume that (a) and (b) are true, then again associative law holds in H as all elements of H are in G.

Now we must show that identity exists in H.

$$As\ a \in H\ , a^{-1} \in \ \ H, hence\ by\ part\ (a)$$

$$aa^{-1} = e \in H.$$

Hence sufficient conditions are satisfied.

Subgroup Condition (II)

- Theorem 2

If G is a group and $G \supseteq H \neq \varnothing$ with H finite,
then H is a subgroup of G ↔
H is closed under the binary operation on G.

$G = \langle Z_6, + \rangle$, $H = \{0,2,4\}$

+	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

identity inverse

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

distinct

Subgroup Condition (II)

(proof of ←)

- If $a \in H$, then $aH = \{ah \mid h \in H\} \subseteq H$ because of the closure condition. By the left-cancellation in G, if $h_1 \neq h_2$, then $ah_1 \neq ah_2$. So $|aH| = |H|$ and furthermore $aH = H$.
- If $a \in H$, then there exists $b \in H$ with $ab = a$. Therefore there exist an identity element e in H.
- Since $e \in aH$, there is an element $c \in H$ such that $ac = e$. Therefore, each element of H has its inverse in H.
- From the theorem 1, H is a subgroup of G.

Direct Product of Groups

- Theorem 3

Let $<G, \square>$ and $<H, *>$ be groups.

Define the operation $\cdot$ on $G \times H$ by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \square g_2, h_1 * h_2)$$

Then $<G \times H, \cdot>$ is a group and is called the direct product of G and H.

(Example)On $G = <Z_2, +> \times <Z_9^*, \cdot>$,

- (0,2) × (1,7) = (0+1, 2·7) = (1,5)
- G is a group of order 12(=2x6).
- Identity is (0,1) and Inverse of (1,2) is (1,5).

Powers of Elements

- Definition of a^n

For a group G, $a \in G$ and $n \in Z$,

$a^0 = e$, $a^1 = a$, $a^2 = aa$, $a^{n+1} = a^n a$,

$a^{-n} = (a^{-1})^n$, $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$

- ❑ Examples for $< Z_4 , + >$

  $[3]^2=[3]+[3]=[6]=[2]$, $[3]^{-2}=[3^{-1}]^2=[1]^2=[2]$

  $[3]^2\,[3]^{-2} =[2][2]=[4]=[0]= [3]^0 =[3]^{2-2}$

- $(ab)^n = a^n b^n$?

$(ab)^n = (ab)(ab)(ab) \cdots (ab) = aa \cdots abb \cdots b = a^n b^n$

, if it is abelian.

Homomorphism

Definition 16.4

If $<G, \square>$ and $<H, *>$ are groups and $f : G \rightarrow H$, then f is called a group homomorphism if for all $a, b \in G$, $f(a \square b) = f(a) * f(b)$.

(Example)

Consider $<Z, +>$ and $<Z_4, +>$. Define $f : Z \rightarrow Z_4$ by

$$f(x) = [x] = \{ x+4k \mid k \in Z \}.$$

For all $a, b \in Z$, $f(a+b) = [a+b] = [a]+[b] = f(a)+f(b)$.

$$f(7+5) = [7+5] = [12] = [0] = [7] + [5] = f(7)+f(5)$$

Endomorphism, Automorphism

- **Endomorphism** is a morphism (or homomorphism) from a mathematical object to itself.
  - Example) an endomorphism of a vector space V is a linear map f:V → V
  - In group G, f: G → G is a group endomorphism
  - In a set S, endomorphism is a function from a set S into itself.
- **Automorphism** is an invertible endomorphism.
  - There exists a bijective function. That is, one-to-one correspondence.
  - The set of all automorphism is a subgroup of Endomorphism.
- **Isomorphism**
  - Bijective
  - Is a morphism f:X→Y in a category for which there exists an "inverse" f^{-1} :Y→X, with the property that both f^{-1} f=id_X and f f^{-1} =id_Y.
- **(Homo)morphism**
  - A structure-preserving map between two algebraic structures (such as groups, rings, or vector spaces).

Properties of Homomorphism

- Theorem 16.5

Let $<G, □>$ and $<H, *>$ be groups with respective identities e_G, e_H. If $f : G \rightarrow H$ is a homomorphism, then

(1) $f(e_G) = e_H$ (2) $f(a^{-1}) = [f(a)]^{-1}$ for all $a \in G$

(3) $f(a^n) = [f(a)]^n$ for all $a \in G$ and all $n \in Z$

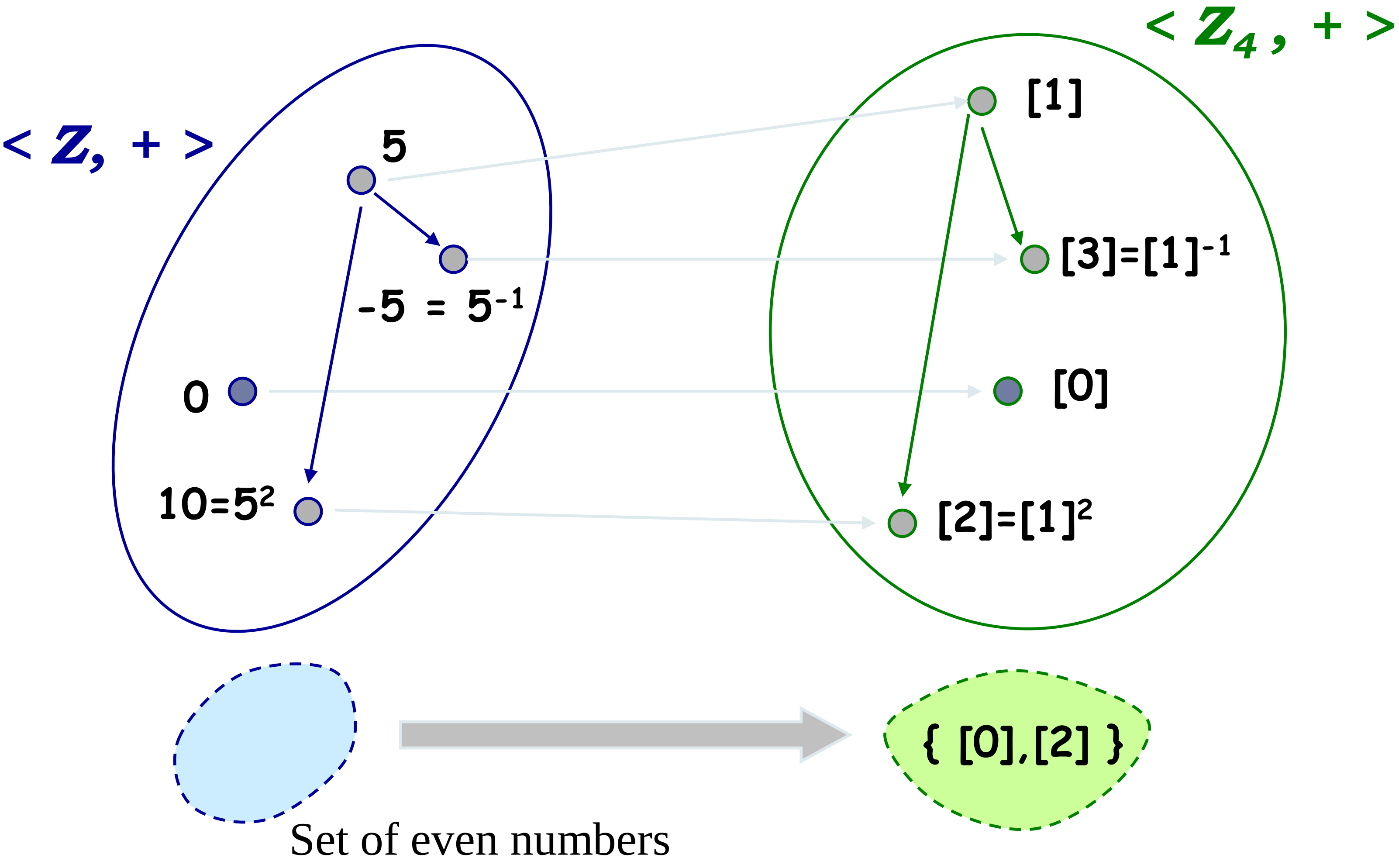
(4) $f(S)$ is a subgroup of H for each subgroup S of G

- ❑ For the example $f : Z \rightarrow Z_4$,

  $f(0) = [0]$,
  $f(5^{-1}) = f(-5) = [-5] = [3] = [1]^{-1} = [5]^{-1} = [f(5)]^{-1}$,
  $[f(5)]^3 = [5]^3 = [5]+[5]+[5] = [5+5+5] = [5^3] = f(5^3)$

Properties of Homomorphism

An Example $f : Z \rightarrow Z_4$



Set of even numbers

Isomorphism

- Definition 16.5

If $f : <G ,\square> \rightarrow <H, *>$ is a homomorphism, we call f an isomorphism if it is one-to-one and onto.

In this case G, H are said to be isomorphic groups.

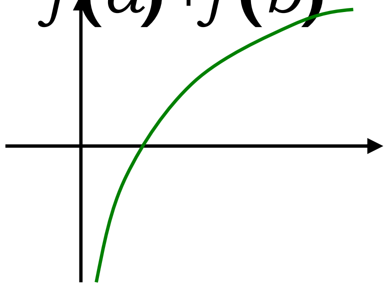
(Example)

Let $f : <R^{+} , \cdot> \rightarrow <R ,+>$ where $f(x) = \mathbf{log}_{10}(x)$

For all a, $b \in R^{+}$,

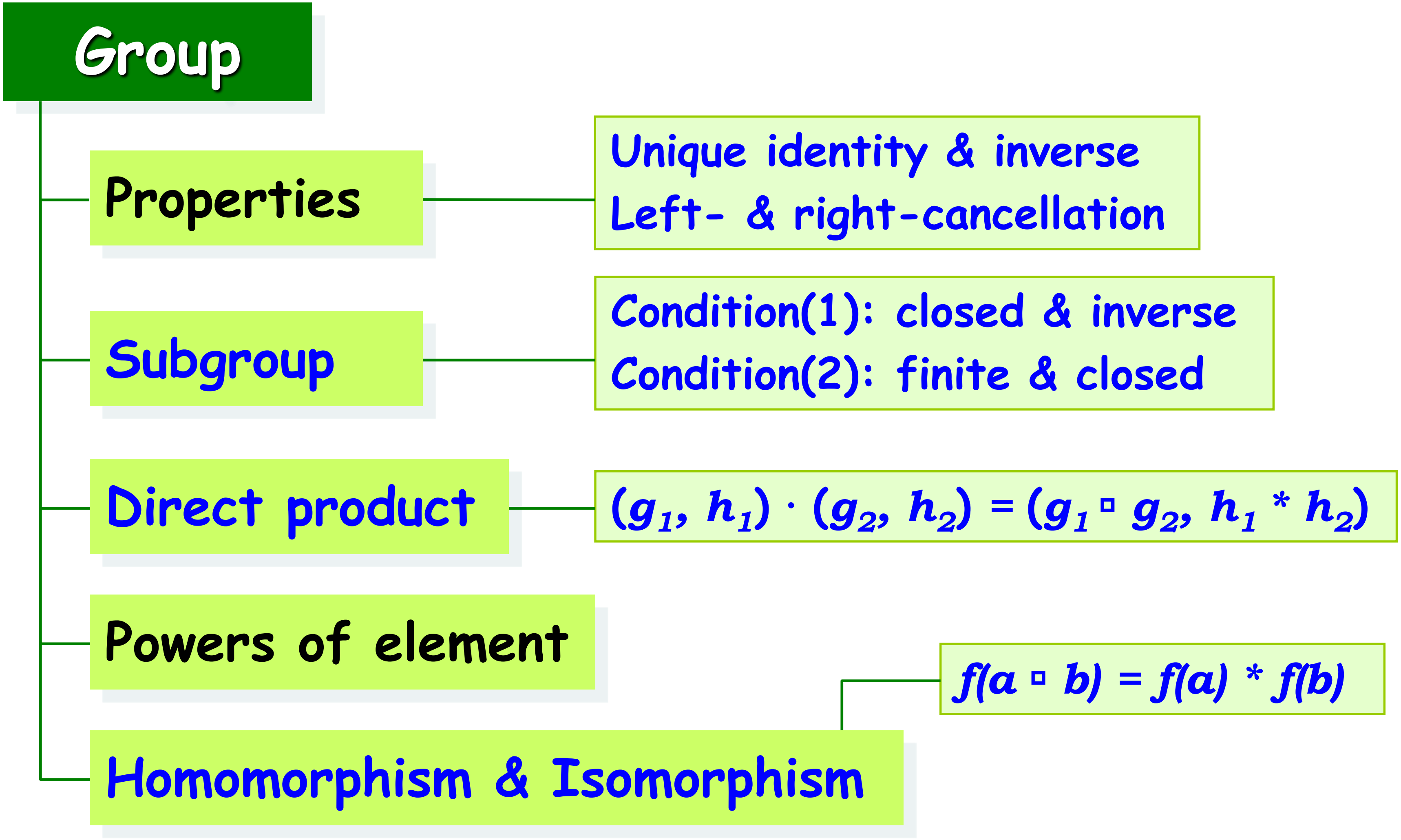
$f(ab) = \mathbf{log}_{10}(ab) = \mathbf{log}_{10}(a) + \mathbf{log}_{10}(b) = f(a)+f(b)$

This function is one-to-one and onto.



Therefore, f is an isomorphism.

?



Group

Properties

Unique identity & inverse

Left- & right-cancellation

Subgroup

Condition(1): closed & inverse

Condition(2): finite & closed

Direct product

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \square g_2, h_1 * h_2)$

Powers of element

Homomorphism & Isomorphism

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

Cyclic Group

- Definition A group G is called cyclic if there is an element $x \in G$ such that for each $a \in G$, $a = x^n$ for some $n \in Z$. Such element x is called a generator (or primitive element) for G.

  - ❑ Given a group G, if $a \in G$ consider the set $S = \{a^k \mid k \in Z\}$. S is a subgroup of G, because it is closed and satisfies the inverse property. (Refer to theorem 2)

    This subgroup is called the subgroup generated by a and is designated by $<a>$.

Order of Elements

- Definition If G is a group and $a \in G$, the order of a, denoted by $ord(a)$, is $|<a>|$. (If $|<a>|$ is infinite, we say that a has infinite order.)

subgroup generated by a

- Theorem Let $a \in G$ with $ord(a) = n$.

If $k \in Z$ and $a^k = e$, then $n \mid k$.

$Proof$: $As\ a^k = e, a^n = e, n\ is\ least\ .\ Hence\ k > n$. Now by division algorithm we have $k = nq + r$, for $0 \le r < n$.

Now $a^k = a^{qn+r} = a^r$, $but\ a^k = e, so\ we\ must\ have\ r = 0$

Therefore, $k = nq\ and\ this\ implies\ n\ divies\ k\ i.e., n|k$.

Example

- Group H = $<Z_4,+>$ ∴ **Cyclic Group**

: [1] and [3] generate H

$[0]^1 = [0]^2 = [0]^3 = [0]^4 = [0] \rightarrow <0> = \{0\}$

$[1]^1 = [1], [1]^2 = [1]+[1] = [2],$
$[1]^3 = [3], [1]^4 = [4] = [0] = e \rightarrow <1> = Z_4$

$[2]^1 = [2], [2]^2 = [2]+[2] = [4] = [0],$
$[2]^3 = [6] = [2], [2]^4 = [8] = [0] = e \rightarrow <2> = \{0,2\}$

$[3]^1 = [3], [3]^2 = [3]+[3] = [6] = [2],$
$[3]^3 = [9] = [1], [3]^4 = [12] = [0] = e \rightarrow <3> = Z_4$

Example

- Group $<Z_4,+>$

Order 4는 4를 나눔

$[1]^1 = [1], [1]^2 = [1]+[1] = [2],$

$[1]^3 = [3], [1]^4 = [4] = [0] = e \rightarrow <1> = Z_4$

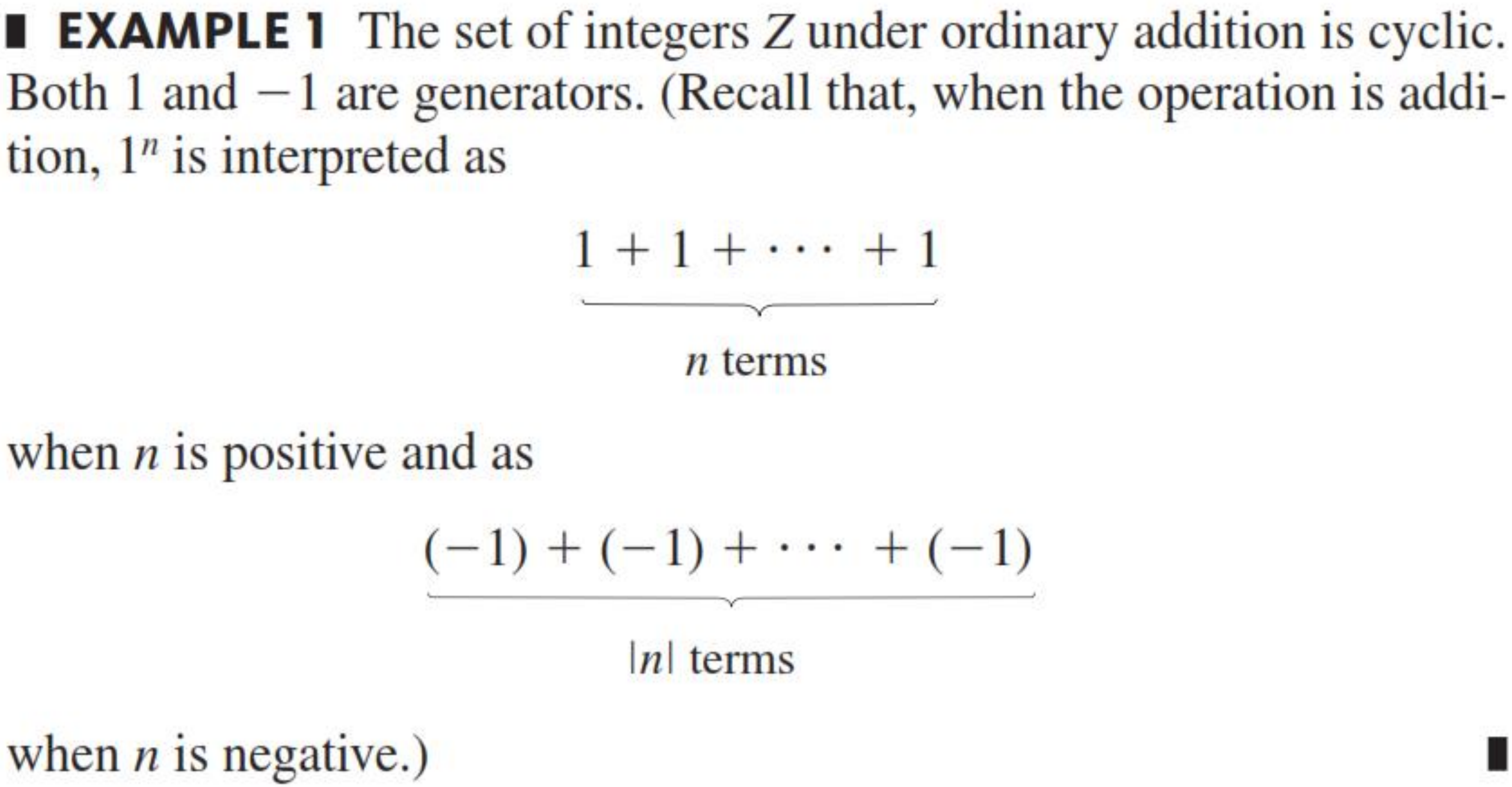
$ord\,[1] = 4.$

$[2]^1 = [2], [2]^2 = [2]+[2] = [4] = [0],$

$[2]^3 = [6] = [2], [2]^4 = [8] = [0] = e \rightarrow <2> = \{0,2\}$

$ord\,[2] = 2.$

Properties of Cyclic Groups



EXAMPLE 1 The set of integers *Z* under ordinary addition is cyclic. Both 1 and -1 are generators. (Recall that, when the operation is addition, 1^n is interpreted as

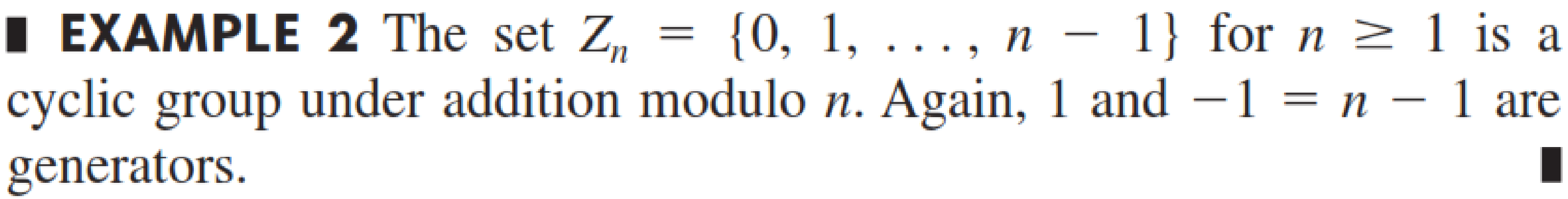
$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}}$$

when n is positive and as

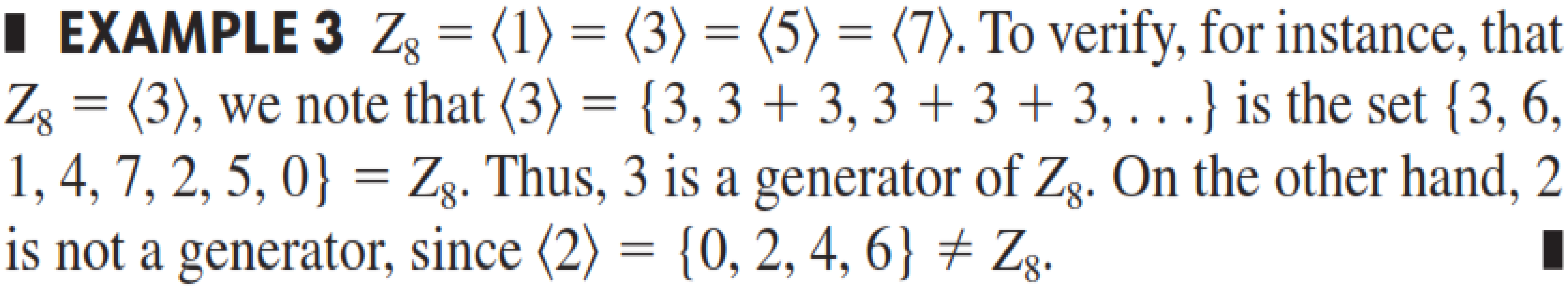
$$\underbrace{(-1) + (-1) + \cdots + (-1)}_{|n| \text{ terms}}$$

when n is negative.) ∎

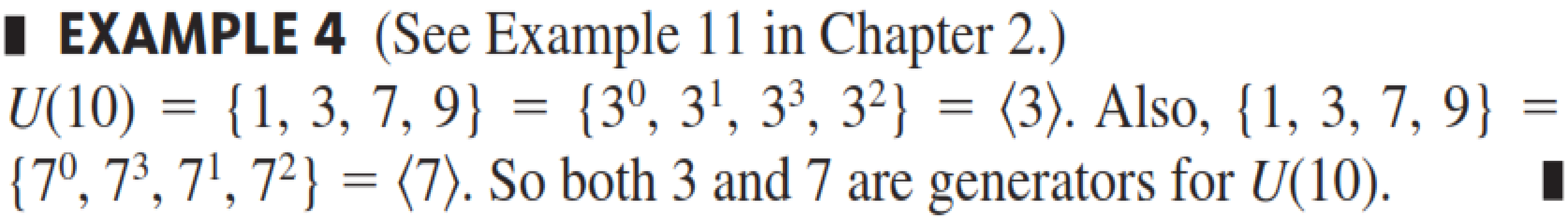
More Examples



▮ **EXAMPLE 2** The set $Z_n = \{0, 1, \ldots, n - 1\}$ for $n \geq 1$ is a cyclic group under addition modulo n. Again, 1 and $-1 = n - 1$ are generators. ▮

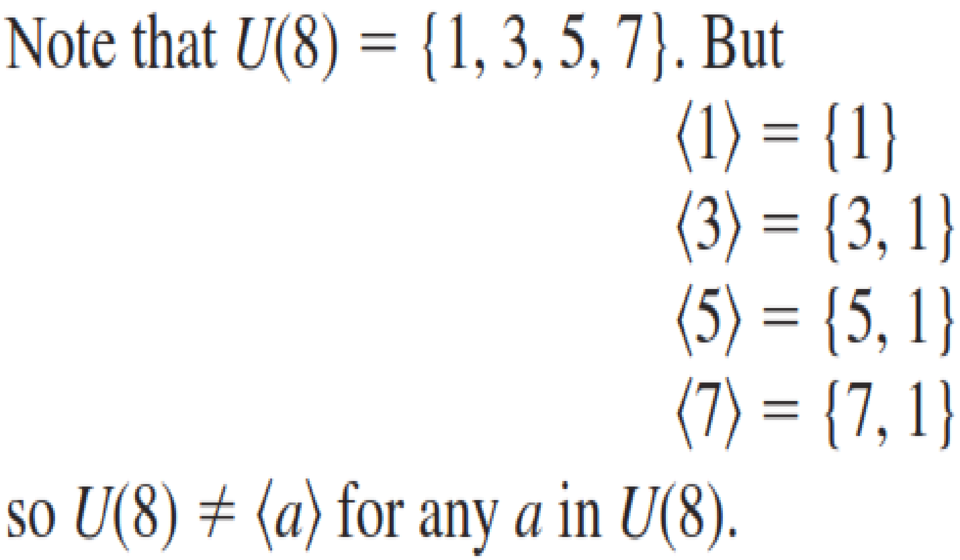


▮ **EXAMPLE 3** $Z_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$. To verify, for instance, that $Z_8 = \langle 3 \rangle$, we note that $\langle 3 \rangle = \{3, 3 + 3, 3 + 3 + 3, \ldots\}$ is the set $\{3, 6, 1, 4, 7, 2, 5, 0\} = Z_8$. Thus, 3 is a generator of Z_8. On the other hand, 2 is not a generator, since $\langle 2 \rangle = \{0, 2, 4, 6\} \neq Z_8$. ▮



▮ **EXAMPLE 4** (See Example 11 in Chapter 2.) $U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^3, 3^2\} = \langle 3 \rangle$. Also, $\{1, 3, 7, 9\} = \{7^0, 7^3, 7^1, 7^2\} = \langle 7 \rangle$. So both 3 and 7 are generators for $U(10)$. ▮

More Examples



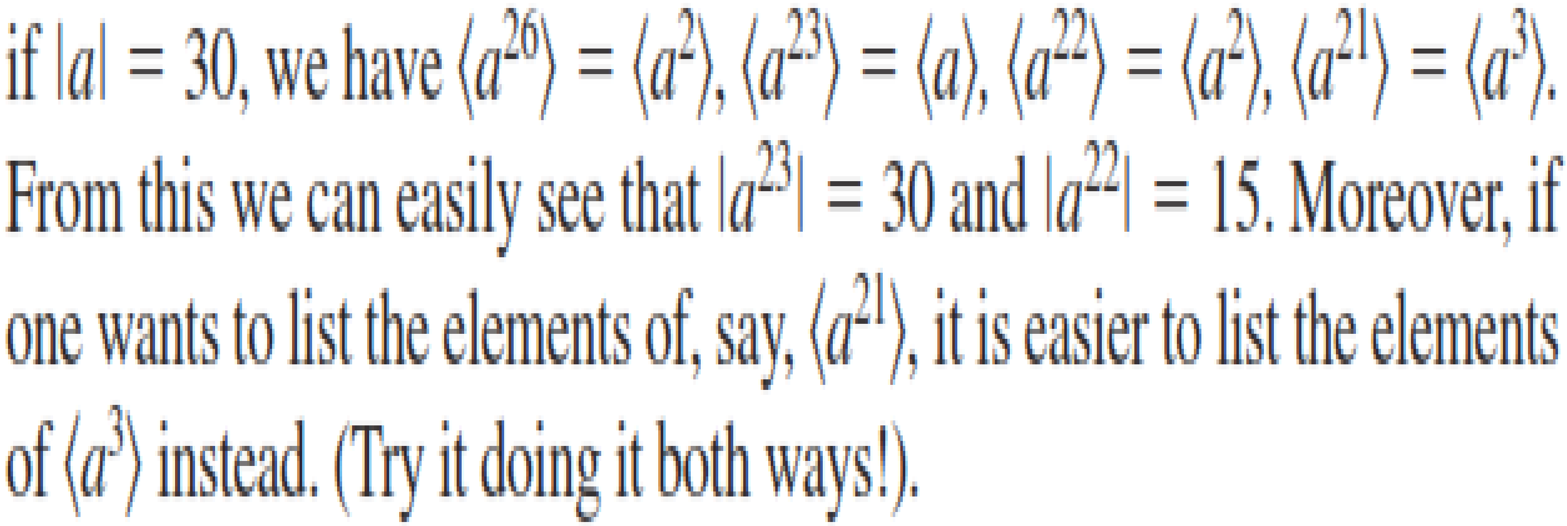
Note that $U(8) = \{1, 3, 5, 7\}$. But

$$\begin{aligned}\langle 1\rangle &= \{1\}\\ \langle 3\rangle &= \{3, 1\}\\ \langle 5\rangle &= \{5, 1\}\\ \langle 7\rangle &= \{7, 1\}\end{aligned}$$

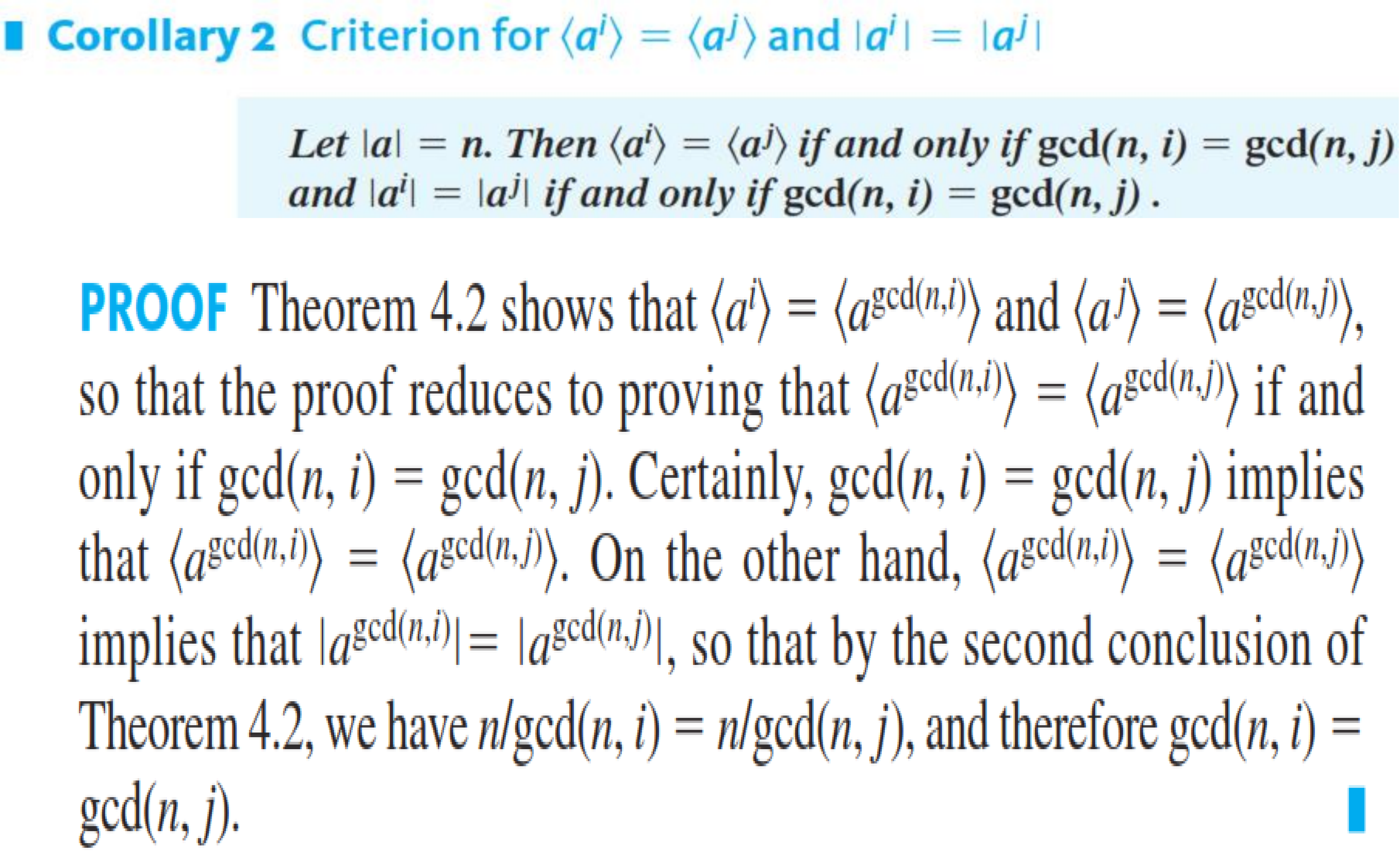
so $U(8) \neq \langle a\rangle$ for any a in $U(8)$.

Therefore, U(8) is not cyclic.

Example:



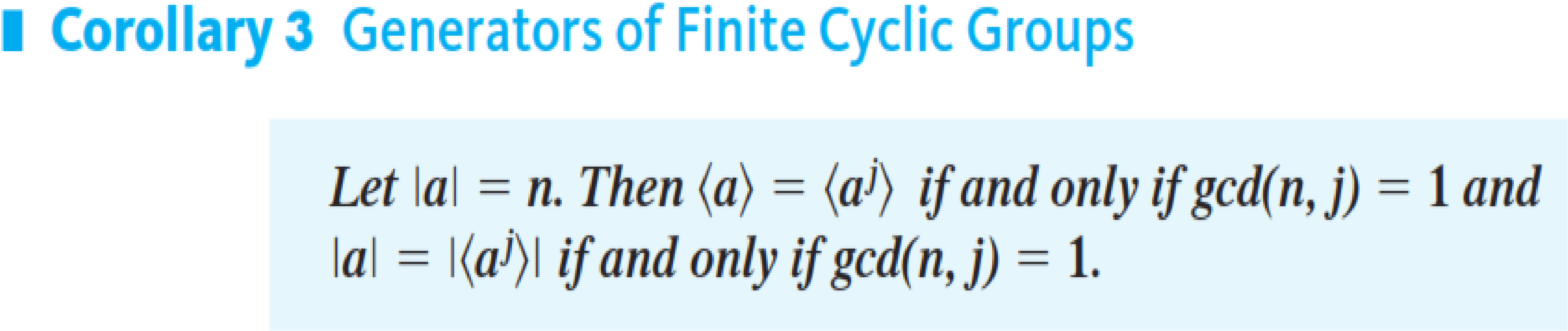
if $|a| = 30$, we have $\langle a^{26}\rangle = \langle a^{2}\rangle$, $\langle a^{23}\rangle = \langle a\rangle$, $\langle a^{22}\rangle = \langle a^{2}\rangle$, $\langle a^{21}\rangle = \langle a^{3}\rangle$. From this we can easily see that $|a^{23}| = 30$ and $|a^{22}| = 15$. Moreover, if one wants to list the elements of, say, $\langle a^{21}\rangle$, it is easier to list the elements of $\langle a^{3}\rangle$ instead. (Try it doing it both ways!).



Corollary 2 Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$

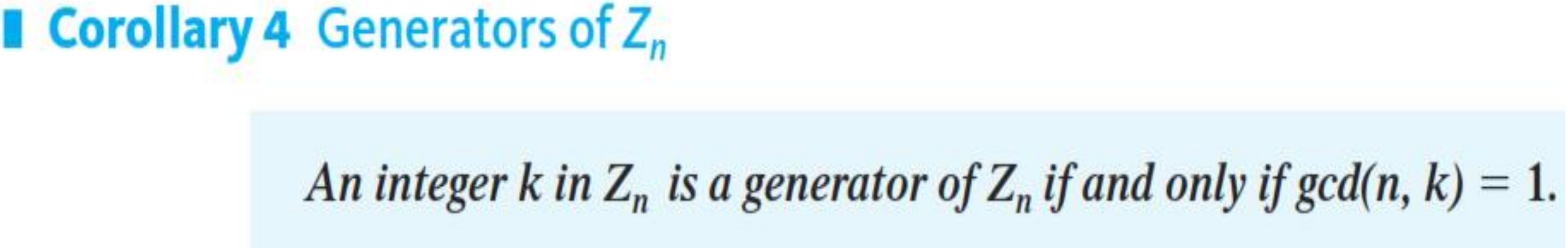
Let $|a| = n$. *Then* $\langle a^i \rangle = \langle a^j \rangle$ *if and only if* $\gcd(n, i) = \gcd(n, j)$ *and* $|a^i| = |a^j|$ *if and only if* $\gcd(n, i) = \gcd(n, j)$.

PROOF Theorem 4.2 shows that $\langle a^i \rangle = \langle a^{\gcd(n,i)} \rangle$ and $\langle a^j \rangle = \langle a^{\gcd(n,j)} \rangle$, so that the proof reduces to proving that $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$. Certainly, $\gcd(n, i) = \gcd(n, j)$ implies that $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$. On the other hand, $\langle a^{\gcd(n,i)} \rangle = \langle a^{\gcd(n,j)} \rangle$ implies that $|a^{\gcd(n,i)}| = |a^{\gcd(n,j)}|$, so that by the second conclusion of Theorem 4.2, we have $n/\gcd(n, i) = n/\gcd(n, j)$, and therefore $\gcd(n, i) = \gcd(n, j)$. ▮



Corollary 3 Generators of Finite Cyclic Groups

Let $|a| = n$. *Then* $\langle a \rangle = \langle a^j \rangle$ *if and only if* $\gcd(n, j) = 1$ *and* $|a| = |\langle a^j \rangle|$ *if and only if* $\gcd(n, j) = 1$.



Corollary 4 Generators of Z_n

An integer k in Z_n is a generator of Z_n if and only if $\gcd(n, k) = 1$.

Theorems for Cyclic Groups

- Theorem Let G be a cyclic group.

  If $|G|$ is infinite, then G is isomorphic to $<Z,+>$.

  If $|G| = n > 1$, then G is isomorphic to $<Z_n,+>$.

- Theorem Every subgroup of cyclic group is cyclic.

  ❑ In $<Z_4,+>$,

  $<1> = Z_4 = \{0,1,2,3\}, \quad <2> = \{0,2\}$

  $S = \{1,3\}$?

Not subgroup

- Theorem Every Cyclic group is abelian.
- Proof: Let $G =< a \geq \{a^n | n \in Z\}$

Let $x, y \in G$, then $\exists$ integers r and s such that $x = a^r, y = a^s$, hence $xy = a^{r+s} = a^{s+r} = a^s a^r = yx$, G is abelian.

Eg: 1. S_3 (Symmetric group of order 6), D_4 (Dihedral group of order 8) are not cyclic as they are non abelian.

2. Abelian group need not to be cyclic e.g. Klein 4-group is abelian but not cyclic.

Theorem 4.3 Fundamental Theorem of Cyclic Groups

- A subgroup of a cyclic group is cyclic.
- If |<a>|=n, then the order of any subgroup of <a> divides n.
- For each +ve integer k, where

  k divides n, the group <a> has exactly one subgroup of order k, namely $< a^{n/k} >$

- *The subgroups of Z are exactly* nZ *for* n=0,1,2,...., *Every subgroup of a cyclic group is cyclic.*

Proof.

The main tools used in this proof are the division algorithm and the Principle of Well-Ordering. Let G be a cyclic group generated by a and suppose that H is a subgroup of G. If $H = \{e\}$, then trivially H is cyclic. Suppose that H contains some other element g distinct from the identity. Then g can be written as a^n for some integer n. Since H is a subgroup, $g^{-1} = a^{-n}$ must also be in H. Since either n or $-n$ is positive, we can assume that H contains positive powers of a and n>0. Let m be the smallest natural number such that $a^m \in H$. Such an m exists by the Principle of Well-Ordering. We claim that $h = a^m$ is a generator for H. We must show that every $h' \in H$ can be written as a power of h. Since $h' \in H$ and H is a subgroup of G, $h' = a^k$ for some integer k. Using the division algorithm, we can find numbers q and r such that $k = mq + r$ where $0 \leq r < m$; hence,

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r.$$

So $a^r = a^k h^{-q}$. Since a^k and h^{-q} are in H, a^r must also be in H. However, m was the smallest positive number such that a^m was in H; consequently, $r = 0$ and so $k = mq$. Therefore, $h' = a^k = a^{mq} = h^q$and H is generated by h.

- *Let* G *be a cyclic group of order* n *and suppose that* a *is a generator for* G. *Then* $a^k = e$ *if and only if* n *divides* k.
- *Proof.*

First suppose that $a^k = e$. By the division algorithm, $k = nq + r$where $0 \le r < n$; hence,

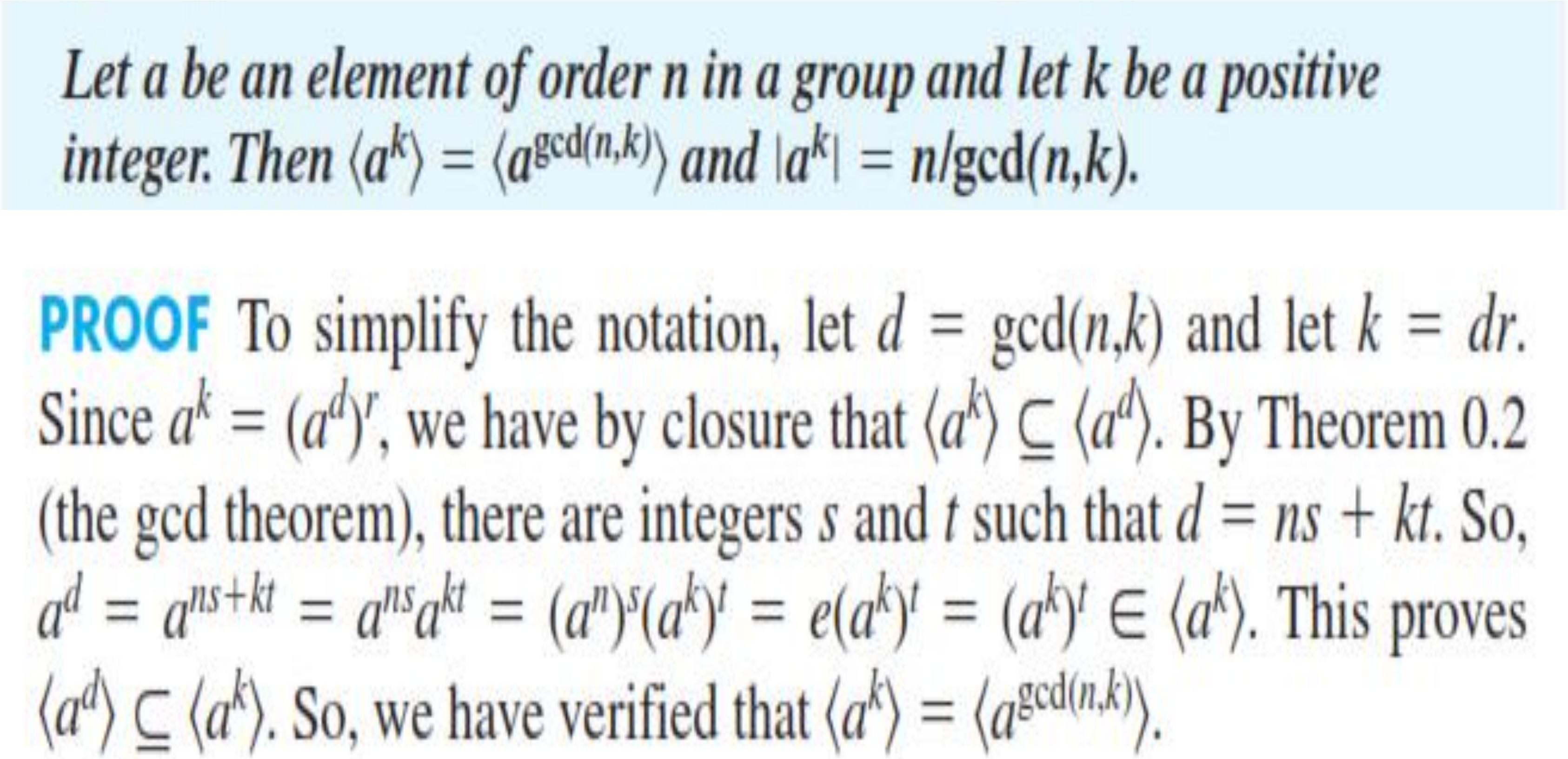
$$e = a^k = a^{nq+r} = a^{nq}\, a^r = ea^r = a^r$$

Since the smallest positive integer m such that $a^m = e$ is n, r=0. =0.

- Conversely, if n divides k, then $k = ns$ for some integer s. Consequently,
- $a^k = a^{ns} = (a^n)^s = e^s = s.$

- **Theorem** *Let* G *be a cyclic group of order* n *and suppose that* $a \in G$ *is a generator of the group. If* $b = a^k$, *then the order of* b *is* n/d, *where*, $d = \gcd(k, n)$.

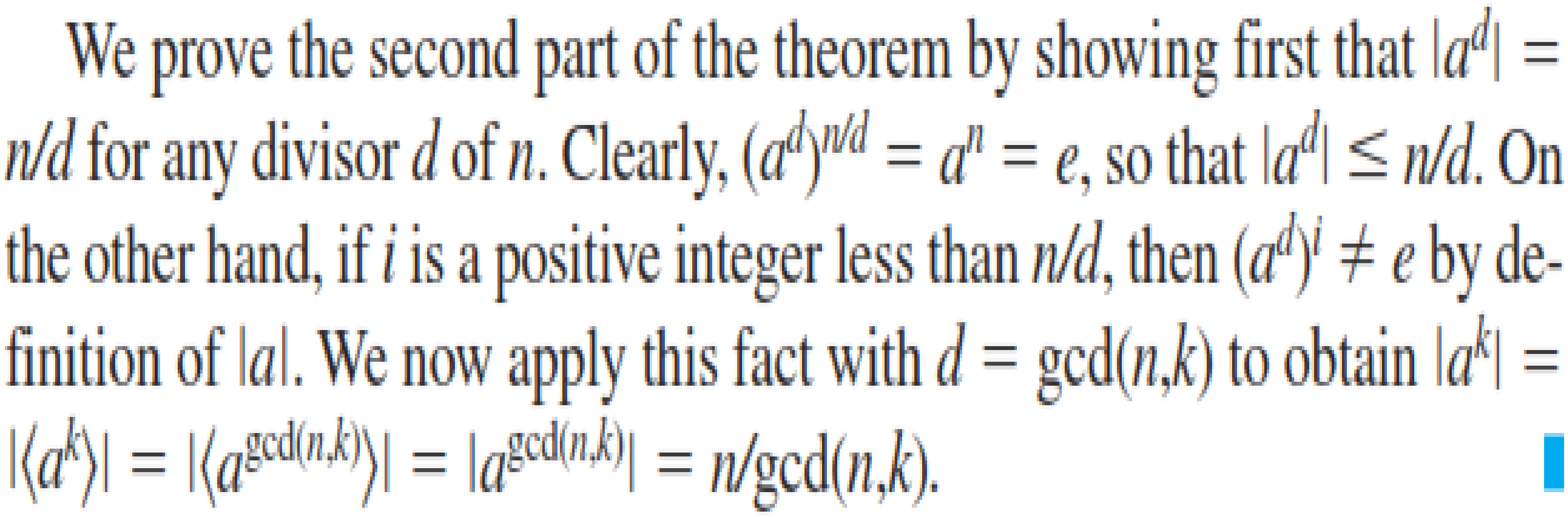
Theorem 4.2 $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$



Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ *and* $|a^k| = n/\gcd(n,k)$.

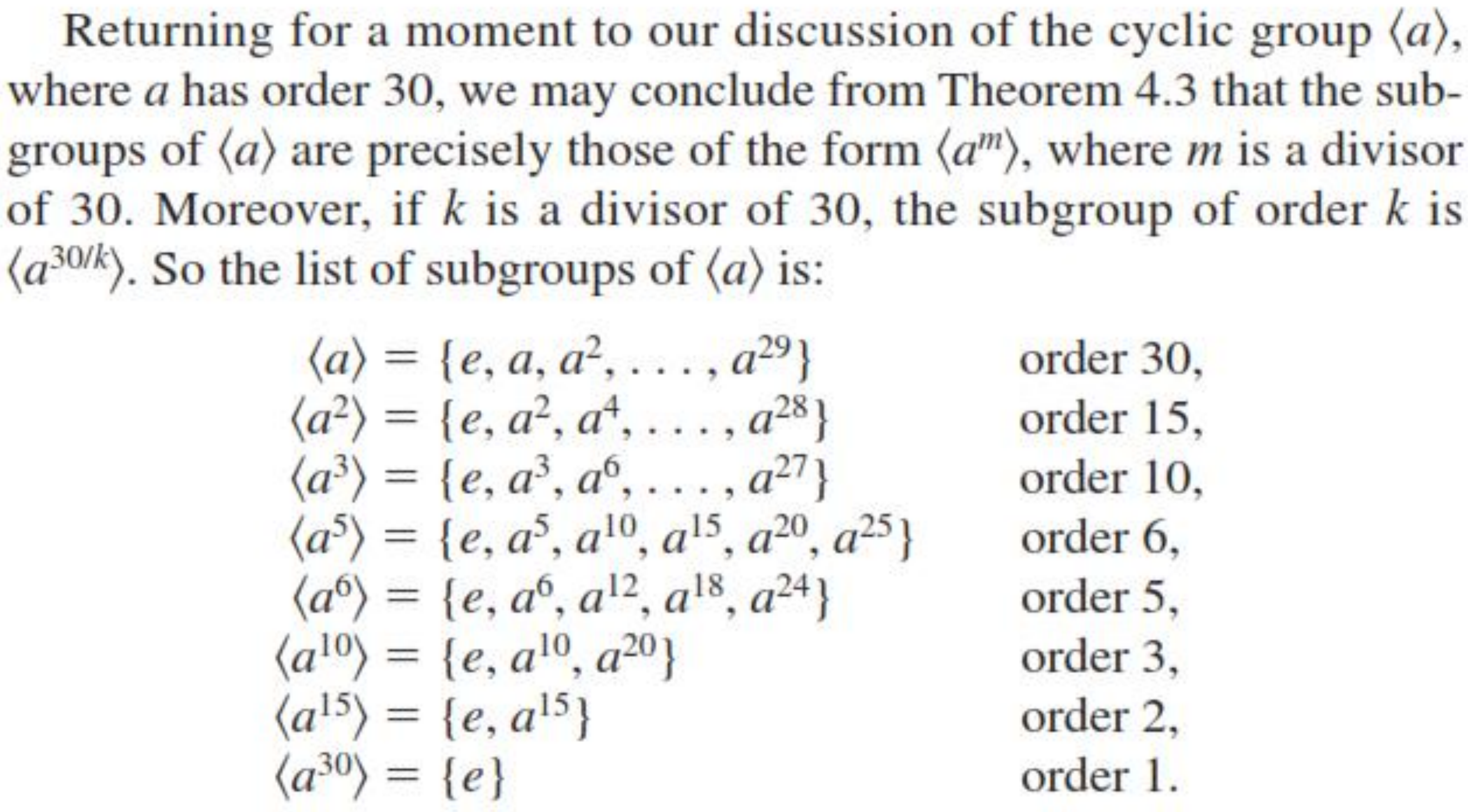
PROOF To simplify the notation, let $d = \gcd(n,k)$ and let $k = dr$. Since $a^k = (a^d)^r$, we have by closure that $\langle a^k \rangle \subseteq \langle a^d \rangle$. By Theorem 0.2 (the gcd theorem), there are integers s and t such that $d = ns + kt$. So, $a^d = a^{ns+kt} = a^{ns}a^{kt} = (a^n)^s(a^k)^t = e(a^k)^t = (a^k)^t \in \langle a^k \rangle$. This proves $\langle a^d \rangle \subseteq \langle a^k \rangle$. So, we have verified that $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

Proof; continue



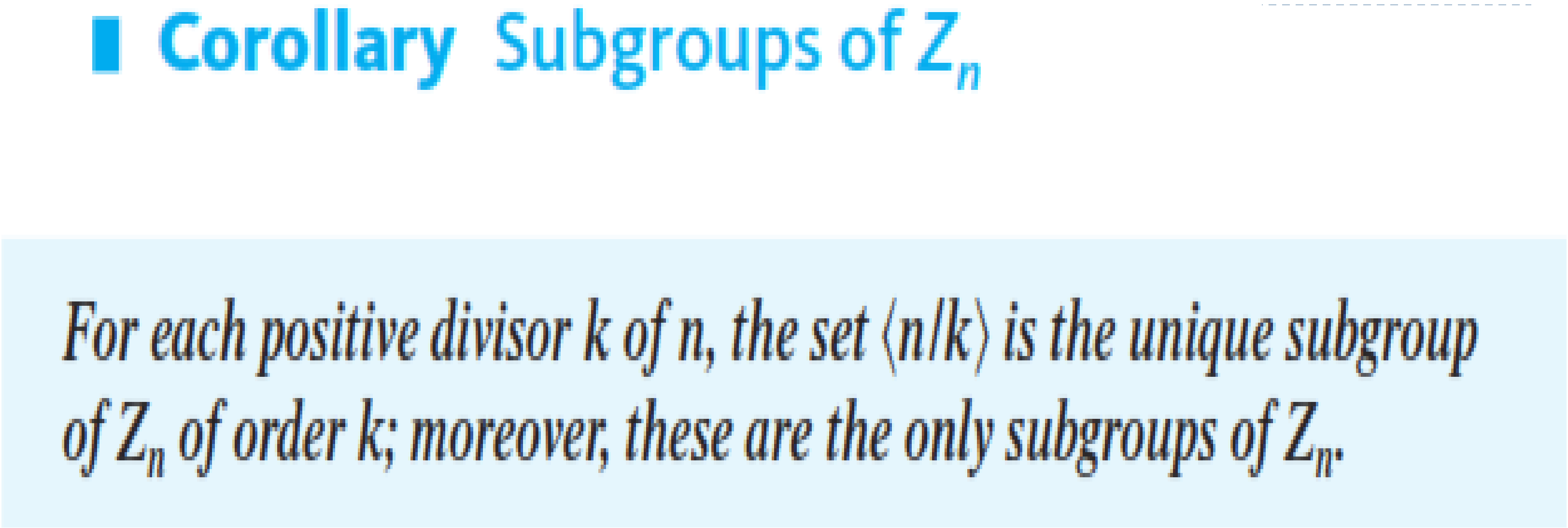
We prove the second part of the theorem by showing first that $|a^d| = n/d$ for any divisor d of n. Clearly, $(a^d)^{n/d} = a^n = e$, so that $|a^d| \le n/d$. On the other hand, if i is a positive integer less than n/d, then $(a^d)^i \ne e$ by definition of $|a|$. We now apply this fact with $d = \gcd(n,k)$ to obtain $|a^k| = |\langle a^k \rangle| = |\langle a^{\gcd(n,k)} \rangle| = |a^{\gcd(n,k)}| = n/\gcd(n,k)$. ■

Example



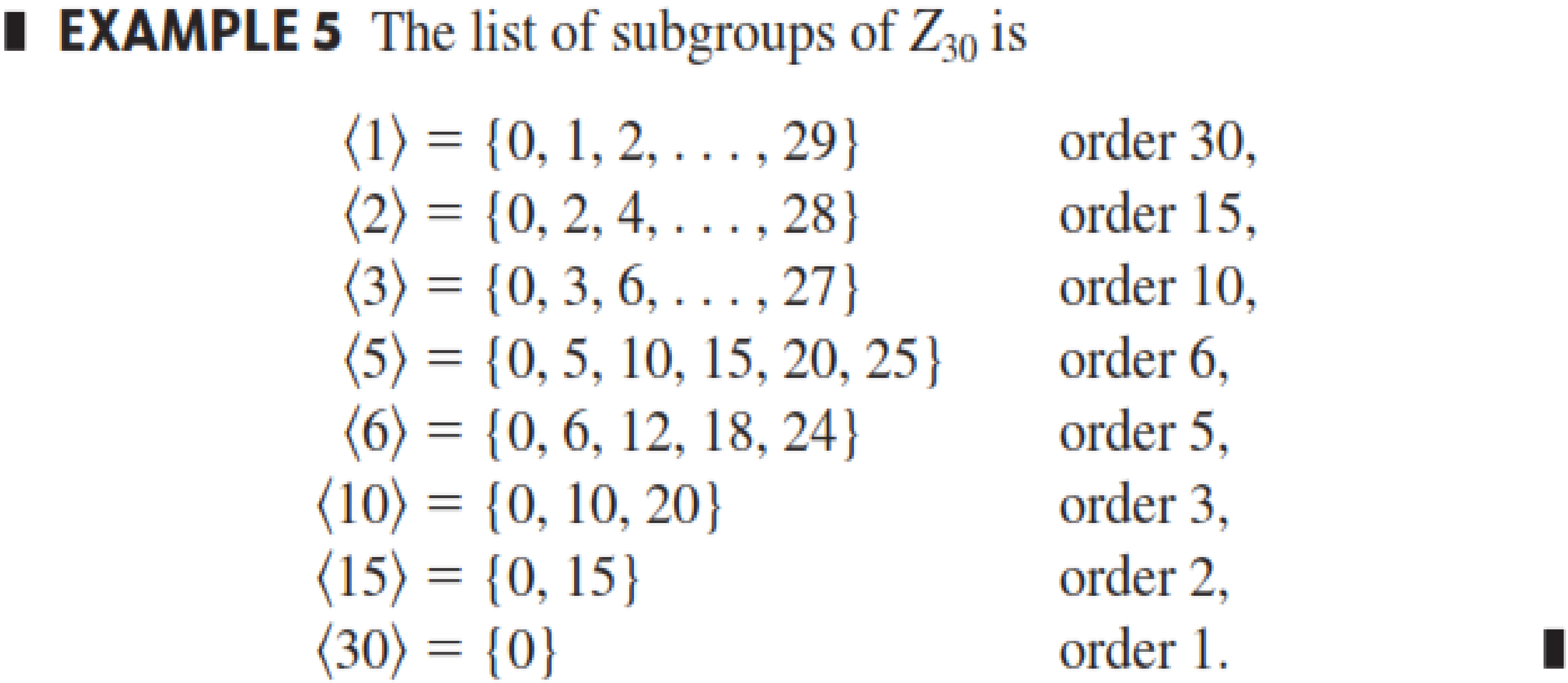
Returning for a moment to our discussion of the cyclic group $\langle a \rangle$, where a has order 30, we may conclude from Theorem 4.3 that the subgroups of $\langle a \rangle$ are precisely those of the form $\langle a^m \rangle$, where m is a divisor of 30. Moreover, if k is a divisor of 30, the subgroup of order k is $\langle a^{30/k} \rangle$. So the list of subgroups of $\langle a \rangle$ is:

$$
\begin{aligned}
\langle a \rangle &= \{e, a, a^2, \ldots, a^{29}\} && \text{order } 30, \\
\langle a^2 \rangle &= \{e, a^2, a^4, \ldots, a^{28}\} && \text{order } 15, \\
\langle a^3 \rangle &= \{e, a^3, a^6, \ldots, a^{27}\} && \text{order } 10, \\
\langle a^5 \rangle &= \{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}\} && \text{order } 6, \\
\langle a^6 \rangle &= \{e, a^6, a^{12}, a^{18}, a^{24}\} && \text{order } 5, \\
\langle a^{10} \rangle &= \{e, a^{10}, a^{20}\} && \text{order } 3, \\
\langle a^{15} \rangle &= \{e, a^{15}\} && \text{order } 2, \\
\langle a^{30} \rangle &= \{e\} && \text{order } 1.
\end{aligned}
$$



Corollary Subgroups of Z_n

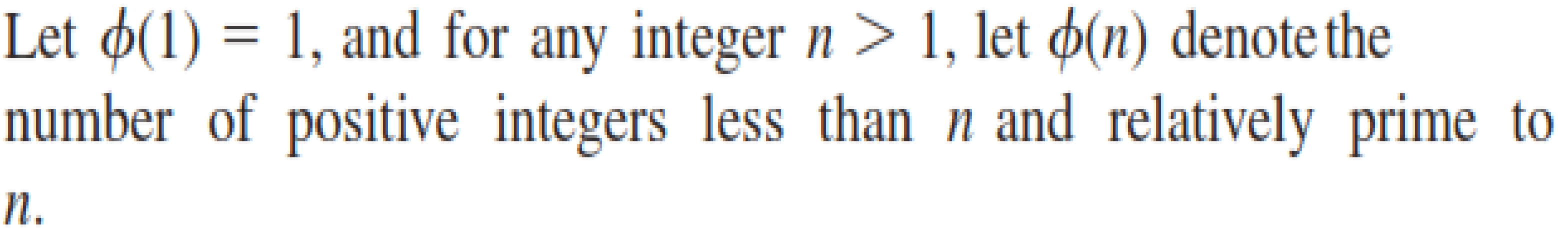
For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of Z_n of order k; moreover, these are the only subgroups of Z_n.



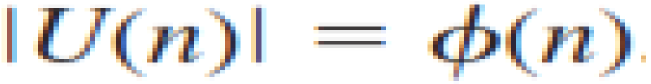
EXAMPLE 5 The list of subgroups of Z_{30} is

$$\begin{array}{rll}
\langle 1\rangle = \{0, 1, 2, \ldots, 29\} & & \text{order } 30, \\
\langle 2\rangle = \{0, 2, 4, \ldots, 28\} & & \text{order } 15, \\
\langle 3\rangle = \{0, 3, 6, \ldots, 27\} & & \text{order } 10, \\
\langle 5\rangle = \{0, 5, 10, 15, 20, 25\} & & \text{order } 6, \\
\langle 6\rangle = \{0, 6, 12, 18, 24\} & & \text{order } 5, \\
\langle 10\rangle = \{0, 10, 20\} & & \text{order } 3, \\
\langle 15\rangle = \{0, 15\} & & \text{order } 2, \\
\langle 30\rangle = \{0\} & & \text{order } 1.
\end{array}$$

■ Euler phi function



Let $\phi(1) = 1$, and for any integer $n > 1$, let $\phi(n)$ denote the number of positive integers less than n and relatively prime to n.



$$|U(n)| = \phi(n).$$

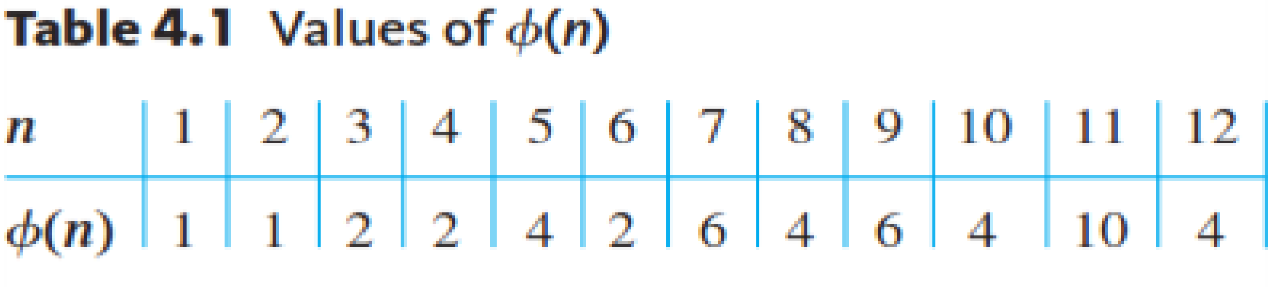
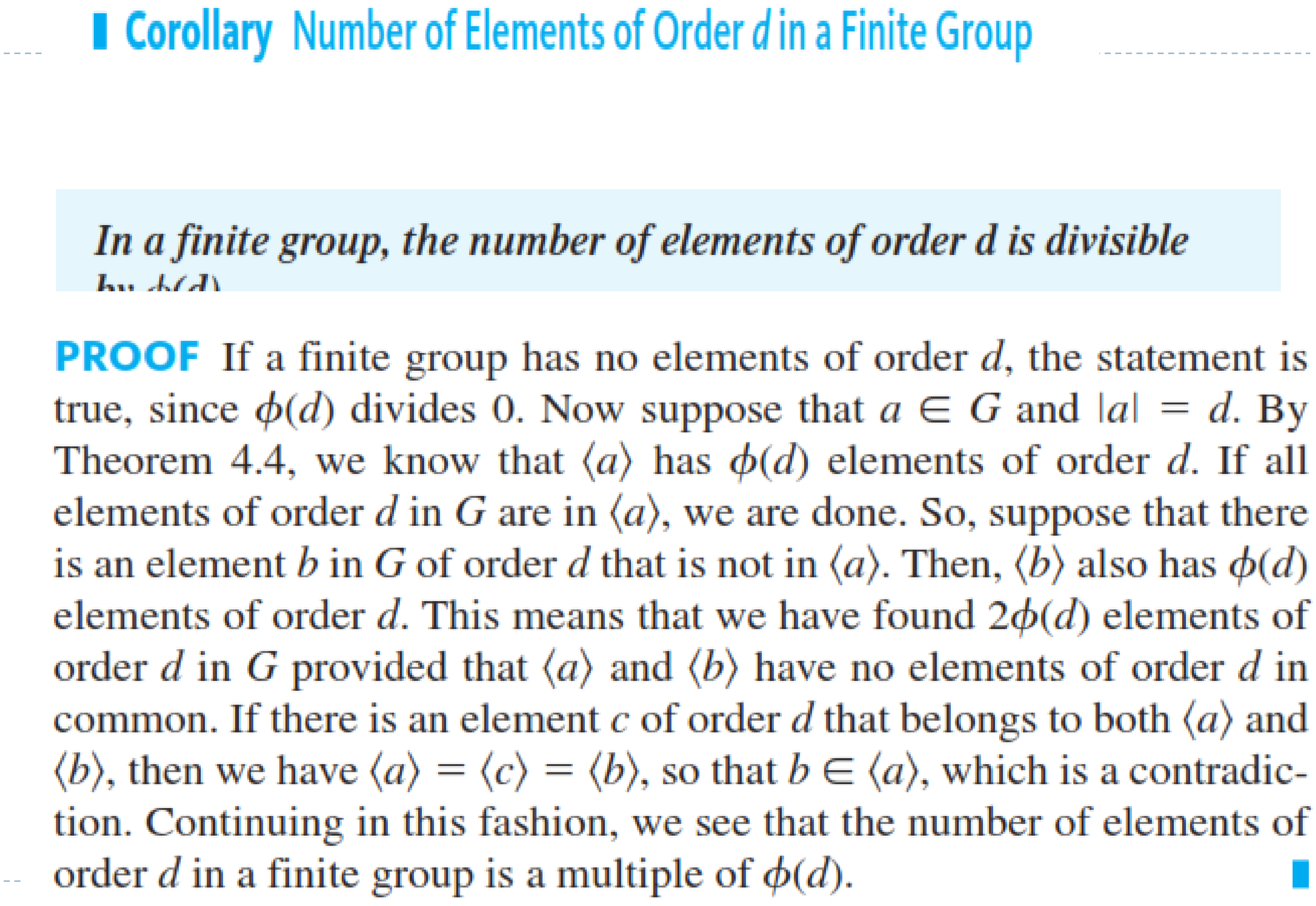


Table 4.1 Values of $\phi(n)$

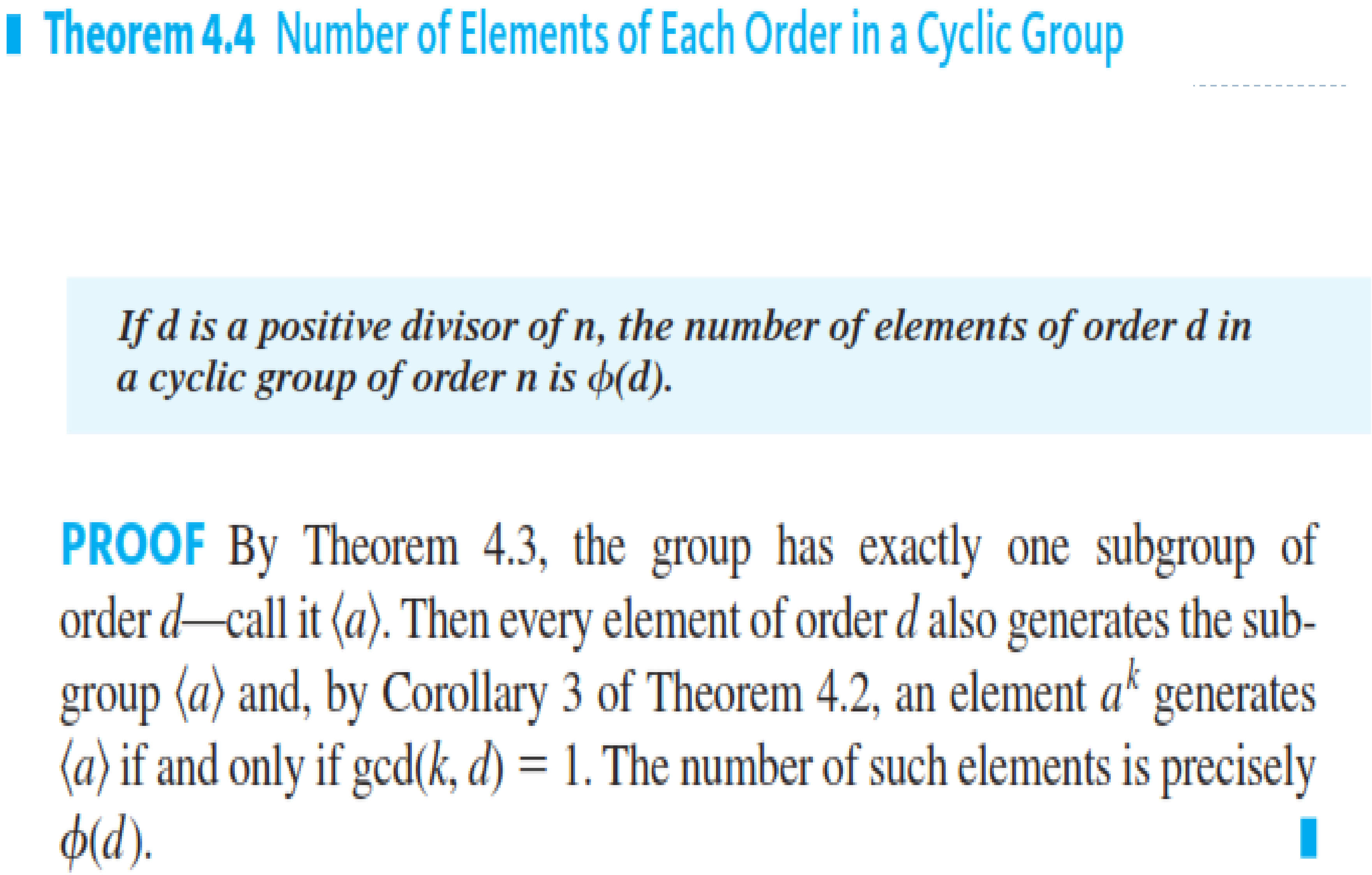
n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4



Corollary Number of Elements of Order d in a Finite Group

In a finite group, the number of elements of order d is divisible by $\phi(d)$.

PROOF If a finite group has no elements of order d, the statement is true, since $\phi(d)$ divides 0. Now suppose that $a \in G$ and $|a| = d$. By Theorem 4.4, we know that $\langle a \rangle$ has $\phi(d)$ elements of order d. If all elements of order d in G are in $\langle a \rangle$, we are done. So, suppose that there is an element b in G of order d that is not in $\langle a \rangle$. Then, $\langle b \rangle$ also has $\phi(d)$ elements of order d. This means that we have found $2\phi(d)$ elements of order d in G provided that $\langle a \rangle$ and $\langle b \rangle$ have no elements of order d in common. If there is an element c of order d that belongs to both $\langle a \rangle$ and $\langle b \rangle$, then we have $\langle a \rangle = \langle c \rangle = \langle b \rangle$, so that $b \in \langle a \rangle$, which is a contradiction. Continuing in this fashion, we see that the number of elements of order d in a finite group is a multiple of $\phi(d)$. ▮



Theorem 4.4 Number of Elements of Each Order in a Cyclic Group

If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\phi(d)$.

PROOF By Theorem 4.3, the group has exactly one subgroup of order d—call it $\langle a \rangle$. Then every element of order d also generates the subgroup $\langle a \rangle$ and, by Corollary 3 of Theorem 4.2, an element a^k generates $\langle a \rangle$ if and only if $\gcd(k, d) = 1$. The number of such elements is precisely $\phi(d)$. ▮

How to find $\phi(n)$

For any prime number p,

$$\phi(p^n) = p^n - p^{n-1}$$

If m, n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$

Example: find the Euler function value for each of the following numbers: n=81, n=100

The subgroup lattice

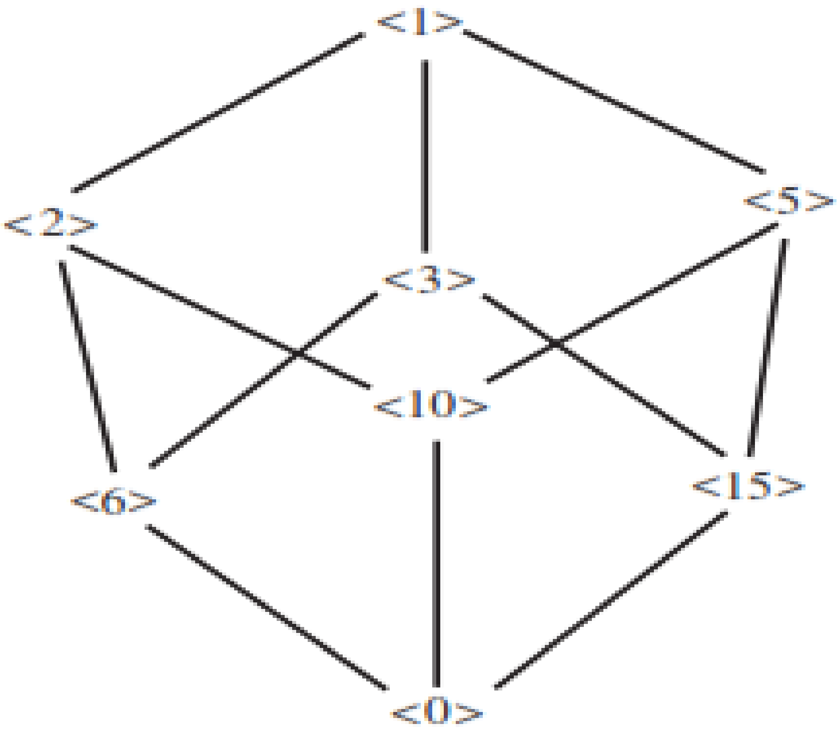


Figure 4.2 Subgroup lattice of Z_{30}.

Lagrange Theorem

- Lagrange's Theorem

  If G is a finite group of order n with H a subgroup of order m, then m divides n.

  → The order of every subgroup H of G divides the order of G

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

Coset

- Let H be a subgroup of a group G and $a \in G$.

$Ha = \{ ha \mid h \in H \}$ --- right coset of H generated by a

$aH = \{ ah \mid h \in H \}$ --- left coset of H generated by a

Klein group

- $K_4 = \{1, a, b, ab\}$, $|a| = |b| = 2$, $ab = ab$

Let $H = \{1, a\}$

right cosets

$H1 \quad = H$

$Ha \quad = \{a, a^2\} = \{a, 1\} = H$

$Hb \quad = \{b, ab\}$

$H(ab) = \{ab, a^2\mathrm{b}\} = \{ab, b\} = Hb$

Theorem

- Let H be a subgroup of G, $a,b \in G$.

  (1) $Ha = H$ iff $a \in H$

  (2) If $a \in Hb$,then $Ha = Hb$

  (3) Either $Ha \cap Hb = \phi$ or $Ha = Hb.$

- Note that Ha may not be equal to aH.

Example

- $G = \langle a \rangle$ with $|a| = 6$, find coset of $H = \langle a^3 \rangle$ and $K = \langle a^2 \rangle$
- Solution:

$$H = \{1, a^3\} = Ha^3$$
$$Ha = \{a, a^4\} = Ha^4$$
$$Ha^2 = \{a^2, a^5\} = Ha^5$$

$$K = \{1, a^2, a^4\}$$
$$= Ka^2 = Ka^4$$
$$Ka = \{a, a^3, a^5\}$$
$$= Ka^3 = Ka^5$$

Lemma

- Let H be a finite subgroup of a group G.

  Then $|H| = |Ha| = |aH|$ for all $a \in G$.

- Proof:
  - Let $f: H \to Ha$ with $f(h) = ha.$
  - Then f is a bijection. So $|H| = |Ha|$.
  - Similarly, $|H| = |aH|$.

Example

- Let H be the subgroup of Z_6 consisting of the elements 0 and 3. The cosets are

$$0+H=3+H=\{0,3\}$$
$$1+H=4+H=\{1,4\}$$
$$2+H=5+H=\{2,5\}.$$

We will always write the cosets of subgroups of Z and Z_n with the additive notation we have used for cosets here. In a commutative group, left and right cosets are always identical.

Example

- Let H be the subgroup of S_3 defined by the permutations {(1),(123),(132)}.The left cosets of H are
$$(1)H = (123)H = (132) = \{(1), (123), (132)\}$$
$(12)H = (13)H = (23)H = \{(12), (13), (23)\}$.The right cosets of H are exactly the same as the left cosets:
$$H(1) = H(123) = H(132) = \{(1), (123), (132)\}$$
$$H(12) = H(13) = H(23) = \{(12), (13), (23)\}.$$
- It is not always the case that a left coset is the same as a right coset. Let K be the subgroup of S_3 defined by the permutations $\{(1), (12)\}$.Then the left cosets of K are
$$(1)K = (12)K = \{(1), (12)\}$$
$$(13)K = (123)K = \{(13), (123)\}$$
$$(23)K = (132)K = \{(23), (132)\};$$
However, the right cosets of K are
$$K(1) = K(12) = \{(1), (12)\}$$
$$K(13) = K(132) = \{(13), (132)\}$$
$$K(23) = K(123) = \{(23), (123)\}.$$

Theorem: Let H *be a subgroup of a group* G*. Then the left cosets of* H *in* G *partition* G*. That is, the group* G *is the disjoint union of the left cosets of* H *in* G*.*

- Let g_1H and g_2H be two cosets of H in G. We must show that either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$. Suppose that $g_1H \cap g_2H \neq \emptyset$ and $a \in g_1H \cap g_2H$. Then by the definition of a left coset, $a = g_1h_1 = g_2h_2$ for some elements h_1 and h_2 in H.

Hence, $g_1 = g_2h_2h_1^{-1}\ or\ g_1 \in g_2H$. Hence , $g_1H = g_2H$.

Normal subgroup

- A **normal subgroup** is a subgroup that is invariant under conjugation by any element of the original group : H is normal if and only if $gHg^{-1} = H$ for any $g \in G$. Equivalently, a subgroup H of G is normal if and only if gH = Hg for any $g \in G$.

Theorem

- Let K be a normal subgroup of G and let $G/K=\{K a|a\in K\}$. Then G/K is a group under $Ka\cdot Kb=Kab$.

- The group G/K of all cosets of K in G is called the quotient group (or factor group) of G by K.

- Example: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

Quotient group

- A **quotient group** is defined as G/N for some normal subgroup *N* of *G*, which is the set of cosets of *N* w.r.t. *G*, equipped with the operation ∘ satisfying $(gN) \circ (hN) = (gh)N$ for all $g, h \in G$. This definition is the reason that *N* must be normal to define a quotient group; it holds because the chain of equalities

$$(gN)(hN) = g(Nh)N = g(hN)N = (gh)(NN) = (gh)N$$

holds, where $g(Nh)N = g(hN)N$ utilizes the fact that $Nh = hN$ for any *h* (true iff N is normal, by definition).

- For example, consider the subgroup $H = \{0, 2, 4, 6\}\ of\ G = Z_8\ (which\ is\ an\ additive\ group)$. The left cosets are

$$\{0 + h \mid h \in H\} = \{2 + h \mid h \in H\} = \{4 + h \mid h \in H\} = \{6 + h \mid h \in H\}$$
$$= \{0, 2, 4, 6\}$$
$$\{1 + h \mid h \in H\} = \{3 + h \mid h \in H\} = \{5 + h \mid h \in H\} = \{7 + h \mid h \in H\}$$
$$= \{1, 3, 5, 7\}$$

so $\frac{G}{H} = \{\{0, 2, 4, 6\}, \{1, 3, 5, 7\}\}$ .This can be more cleanly written as $\frac{G}{H} = \{0 + H, 1 + H\}$ which is isomorphic to $\{0,1\}$ or the cyclic group C_2 .

Theorem

- Let K be a normal subgroup of a finite group G. Then $|G/K|=|G|/|K|=[G:K]$

Basic facts

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

(1) $Ka=Kb$ if and only if $ab^{-1}\in K$.

(2) $Ka=K$ if and only if $a\in K$.

(3) $Ka \cdot Kb = Kab$.

(4) $K=K1$ is the identity of G/K.

(5) $(Ka)^{-1}=Ka^{-1}$.

(6) $(Ka)^{k}=Ka^{k}$ for all $k\in\mathbb{Z}$.

Example

- $G=\langle a\rangle, |a|=12, \ K=\langle a^4\rangle$

The cosets are

$$K=\{1,a^4,a^8\}$$

$$Ka=\{a,a^5,a^9\}=Ka^5=Ka^9$$

$$Ka^2=\{a^2,a^6,a^{10}\}=Ka^6=Ka^{10}$$

$$Ka^3=\{a^3,a^7,a^{11}\}=Ka^7=Ka^{11}$$

$$G/K=\langle Ka\rangle \cong C_4$$

The Cayley table

G/K	K	Ka	Ka^2	Ka^3
K	K	Ka	Ka^2	Ka^3
Ka	Ka	Ka^2	Ka^3	K
Ka^2	Ka^2	Ka^3	K	Ka
Ka^3	Ka^3	K	Ka	Ka^2

Example

- Let $K=\{\varepsilon,(12)(34),(13)(24),(14)(23)\}$. Show that K is normal subgroup of A_4 . Find A_4/K and write down the Cayley table.
- Solution:
  - $A_4 = K \cup \{(123),(132),(124),(142),(134),(143),(234),(243)\}$
  - $K\varepsilon=\varepsilon K=K$
  - $(123)K=K(123)=\{(123),(243),(142),(134)\}$
  - $(132)K=K(132)=\{(132),(143),(234),(124)\} = [K(123)]^2$
  - $A_4/K=\langle K(123)\rangle$

A_4/K	K	$K(123)$	$K(132)$
K	K	$K(123)$	$K(132)$
$K(123)$	$K(123)$	$K(132)$	K
$K(132)$	$K(132)$	K	$K(123)$

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

1. $ghg^{-1} \in H$ for all $g \in G$ and $h \in H$.
2. $gHg^{-1} = H$ for all $g \in G$.
3. $gH = Hg$ for all $g \in G$.

(1) => (2) Suppose that H is a subgroup of G such that $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. Then $gHg^{-1} = \{ghg^{-1} \mid h \in H\} \subseteq H$ for all $g \in G$. We claim that actually $gHg^{-1} = H$. We must show that $H \subseteq gHg^{-1}$ for all $g \in G$.

Let $h \in H$. Replacing g by g^{-1} in the relation $ghg^{-1} \in H$, we obtain $g^{-1}h(g^{-1})^{-1}$
$= g^{-1}hg = h_1$ where $h_1 \in H$.
Consequently, $h = gh_1g^{-1} \in gHg^{-1}$, and we are done.

(3) => (2) Suppose that $gH = Hg$ for all $g \in G$. Then $gh = h_1g$, so $ghg^{-1} \in H$ for all $g \in G$ and all $h \in H$. By the preceding paragraph, this means that $gHg^{-1} = H$ for all $g \in G$.

(2) => (3) Conversely, if $gHg^{-1} = H$ for all $g \in G$, then $ghg^{-1} = h_1$ so $gh = h_1g \in Hg$, and $gH \subseteq Hg$. But also, $g^{-1}Hg = H$ giving $g^{-1}hg = h_2$, so that $hg = gh_2$ and $Hg \subseteq gH$.

Lagrange's Theorem

Proposition

Proposition

Let H *be a subgroup of* G *with* $g \in G$ *and define a map* ϕ:*H*→*gH by* $\phi(h) = gh$.*The map* ϕ *is bijective; hence, the number of elements in* H *is the same as the number of elements in* gH.

Proof.

We first show that the map ϕ *is one to one. Suppose that* $\phi(h_1) = \phi(h_2)$ *for elements* $h1, h2 \in H$. *We must show that* $h1 = h2$, *but* $\phi(h1) = gh_1$ *and* $\phi(h2) = gh2$. So $gh1 = gh2$, and by left cancellation $h1 = h2$. To show that φ is onto is easy. By definition every element of gH is of the form gh *for some* $h \in H$ *and* $\phi(h) = gh$.

Theorem Lagrange.

Let G be a finite group and let H be a subgroup of G. Then $\frac{|G|}{|H|} = [G: H]$ is the number of distinct left cosets of H *in* G. In particular, the number of elements in H must divide the number of elements in G.

Proof.

The group G is partitioned into $[G: H]$ distinct left cosets. Each left coset has $|H|$ elements; therefore, $|G| = [G: H]|H|$.

Lagrange Theorem

- Corollary Every group of prime order is cyclic.

Let p be a prime and G be a group such that |G|=p. Then G contains more than one element.

Let $g \in G$ such that $g \neq eG$ Then ⟨g⟩ contains more than one element.

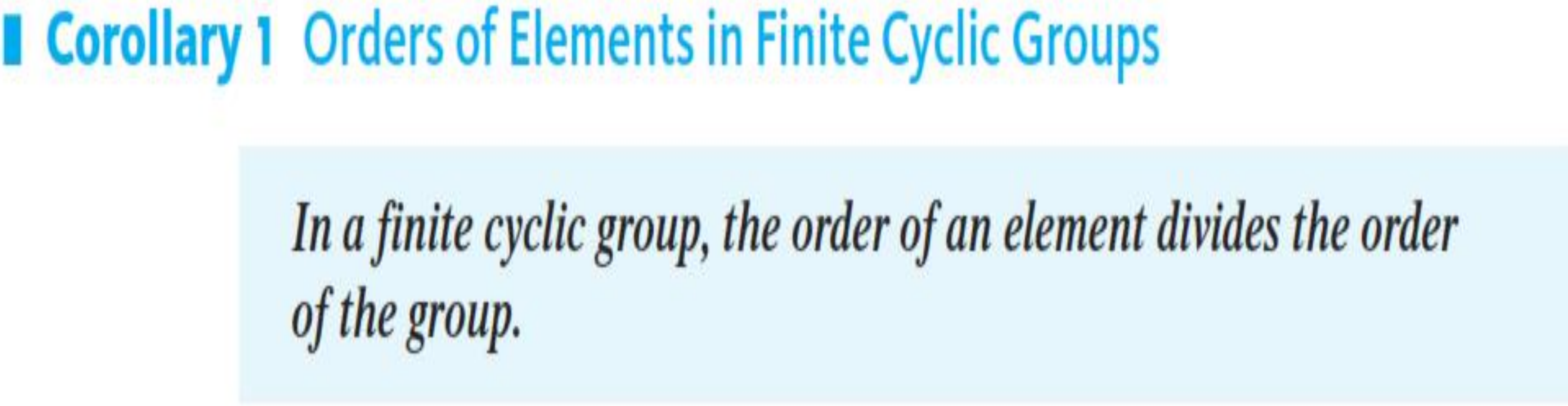
Since $|\langle g\rangle| \ \leq \ |G|$, by Lagrange's theorem, $|\langle g\rangle|$ divides p.

Since $|\langle g\rangle| > 1$ and $|\langle g\rangle|$ divides a prime, $|\langle g\rangle| = p = |G|$. Hence, $\langle g\rangle = G. It\ follows\ that\ G\ is\ cyclic.$

A prime number is a positive integer p>1 that has no positive integer divisors other than 1 and p itself.

Lagrange's Theorem (2nd Proof)

- Proof:
  - ➢ Suppose $Ha_1, \ldots\ldots\ldots, Ha_k$ are distinct cosets of H in G.
  - ➢ Then $k=[G:H]$ and $|Ha_1|+\ldots\ldots\ldots+|Ha_k| = |G|$.
  - ➢ This implies $k|H| = |G|$ since $|H| = |Ha_i|$ for each i.
  - ➢ So $|G| = |H|[G:H]$.



Corollary 1 Orders of Elements in Finite Cyclic Groups

In a finite cyclic group, the order of an element divides the order of the group.

Example (1)

- In $<Z_{15}^{*}, \cdot>$, $ord(2)$ = 4 and $ord(4)$ = 2.

k a	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	2	4	8	1	2	4	8	1
4	4	1	4	1	4	1	4	1
7	7	4	13	1	7	4	13	1
8	8	4	2	1	8	4	2	1
11	11	1	11	1	11	1	11	1
13	13	4	7	1	13	4	7	1
14	14	1	14	1	14	1	14	1

Table of Powers, a^k

Example (2)

- In $<Z_{11}{}^*, \cdot>$, $|Z_{11}{}^*| = 10$

k a	1	2	3	4	5	6	7	8	9	10
1	①	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	①
3	3	9	5	4	①	3	9	5	4	1
4	4	5	9	3	①	4	5	9	3	1
5	5	3	4	9	①	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	①
7	7	5	2	3	10	4	6	9	8	①
8	8	9	6	4	10	3	2	5	7	①
9	9	4	3	5	①	9	4	3	5	1
10	10	①	10	1	10	1	10	1	10	1

Table of Powers, a^k

Example (3)

Every group of prime order is cyclic.

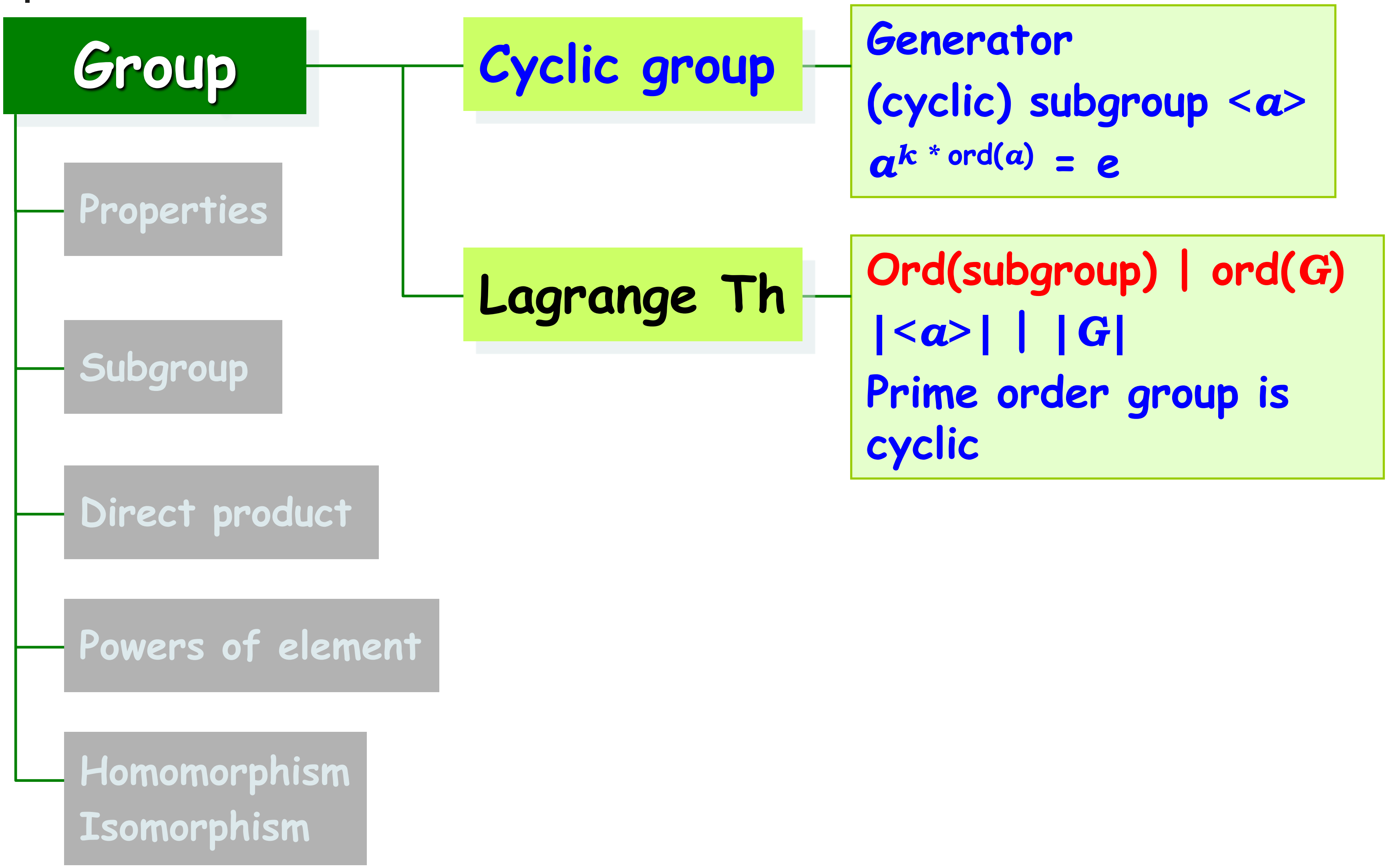
- In $<Z_5,+>$, $|Z_5| = 5$

Note that the number 5 is prime.

a k	1	2	3	4	5
0	0	0	0	0	0
1	1	2	3	4	0
2	2	4	1	3	0
3	3	1	4	2	0
4	4	3	2	1	0

Table of Powers, a^k

A group G is called cyclic if there exists an element g in G such that G = { g^n | n is an integer }.



Group

Properties

Subgroup

Direct product

Powers of element

Homomorphism
Isomorphism

Cyclic group

Generator

(cyclic) subgroup $<a>$

$a^{k * \mathrm{ord}(a)} = e$

Lagrange Th

Ord(subgroup) | ord(G)

$|<a>| \mid |G|$

Prime order group is cyclic

?

- Lagrange's Theorem

H is a subgroup of G

$$|G| = k\,|H|$$

$< Z_{15}^*, \cdot >$

8

$< \{1, 4\}, \cdot >$

2

·	1	4
1	1	4
4	4	1

·	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
4	4	8	1	13	2	14	7	11

$k = 4$?

Euler Theorem

- Euler Theorem

For each $n \in Z^{+}$, $n > 1$, and each $a \in Z$, if gcd(a,n) = 1, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

For any integer $n > 1$,

$$a^{\phi(n)} \equiv 1 \ (mod\ n) \text{ for all } a \in Z_n^*.$$

(Proof)

Z_n^* is a multiplicative group of order $\phi(n)$.

Example

- In $<Z_{15}^{*}, \cdot>$, $a^{\phi(n)} \equiv 1 \ (mod\ n)$.

$\phi(15)=8$

a \ k	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	2	4	8	1	2	4	8	1
4	4	1	4	1	4	1	4	1
7	7	4	13	1	7	4	13	1
8	8	4	2	1	8	4	2	1
11	11	1	11	1	11	1	11	1
13	13	4	7	1	13	4	7	1
14	14	1	14	1	14	1	14	1

Table of Powers, a^k

Fermat Theorem

- Fermat Theorem

If p is prime, $a^p \equiv a \pmod{p}$ for each $a \in Z$.

If p is prime,

$$a^p \equiv a \ (mod\ p) \text{ for all } a \in Z_p^*.$$

If p is prime,

$$a^{p-1} \equiv 1 \ (mod\ p) \text{ for all } a \in Z_p^*.$$

Example

- In $<Z_{11}{}^{*}, \cdot>$, $a^{p-1} \equiv 1 \ (mod\ p)$ & $a^{p} \equiv a \ (mod\ p)$

$\phi(11)=10$

k a	1	2	3	4	5	6	7	8	9	10	11
1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1	2
3	3	9	5	4	1	3	9	5	4	1	3
4	4	5	9	3	1	4	5	9	3	1	4
5	5	3	4	9	1	5	3	4	9	1	5
6	6	3	7	9	10	5	8	4	2	1	6
7	7	5	2	3	10	4	6	9	8	1	7
8	8	9	6	4	10	3	2	5	7	1	8
9	9	4	3	5	1	9	4	3	5	1	9
10	10	1	10	1	10	1	10	1	10	1	10

Table of Powers, a^k

# of Generators

- Theorem

If p is prime, then

Z_p* is a cyclic group of order p-1.

The number of generators for Z_p* is $\phi(p-1)$.

- Example

In Z_{11}*, there are $\phi(11-1) = \phi(10) = 4$ generators.

  - Generators : 2, 6, 7, 8

Example

- In $<Z_{11}^*,\cdot>$, $\phi(p-1) = 4$.

# of generators

k a	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

Table of Powers, a^k

Permutation of a Set

- Let A be the set { *1, 2, …, n* }.
  A **permutation** on A is a function
  $$f : A \to A$$
  that is both one-to-one and onto.

- The set of all permutations on A is denoted by S_n

- A permutation is represented by a matrix :
  $$f = \begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & & f(n) \end{bmatrix}$$

Examples of Permutation

- Let A be the set { $1, 2, 3, 4, 5$ }

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{bmatrix}$$

$$g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{bmatrix}$$

f and g are elements of S_5

Product of Permutations

- The product of f and g is the composition function $f \circ g$

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & \downarrow & \\ 3 & 5 & 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 4 & 2 & 5 & 3 & 1 \end{bmatrix}$$

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & ? & ? & ? & ? \end{bmatrix}$$

- An element f of S_n is a cycle (r-cycle) if there exists

$$\{ i_1, i_2, \cdots, i_r \} \subseteq \{ 1, 2, \cdots, n \}$$

such that

$$f(i_1) = i_2 \text{ , } f(i_2) = i_3 \text{ , } \cdots \text{ , } f(i_{r-1}) = i_r \text{ , } f(i_r) = i_1$$

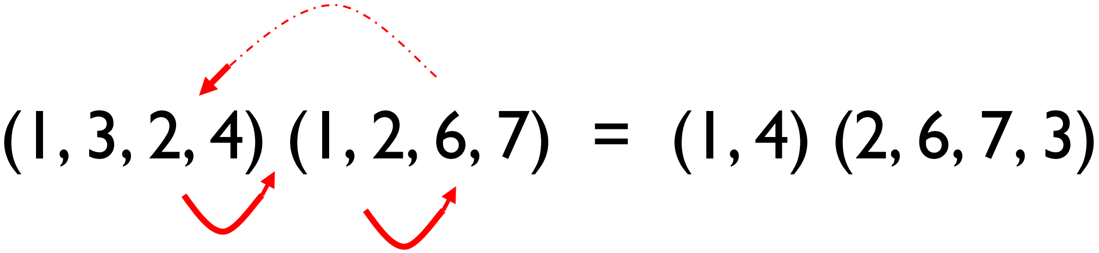
$$\text{and } f(m) = m \text{ for all other } m \notin \{ i_1, i_2, \cdots, i_r \}$$

Cycles will be written simply as $(i_1, i_2, \ldots , i_r)$

Example : $$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & \downarrow & \downarrow & \\ 3 & 2 & 4 & 1 & 5 \end{bmatrix} = \mathbf{(1, 3, 4)}$$

Product of Cycles

- If (1, 3, 2, 4) and (1, 2, 6, 7) are two cycles in S_7 we have



$$(1, 3, 2, 4)\ (1, 2, 6, 7) = (1, 4)\ (2, 6, 7, 3)$$

- **Note that (1, 4) (2, 6, 7, 3) is a product of disjoint cycles**

Permutations and cycles

- Every permutation can be written as a product of disjoint cycles. For example

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 2 & 6 & 7 & 4 & 9 & 1 & 5 \end{bmatrix}$$

We have

1 → 3 → 2 → 8 → 1
4 → 6 → 4
5 → 7 → 9 → 5

We can easily verify that

f = (1, 3, 2, 8)(4, 6)(5, 7, 9)

Transpositions : A special kind of cycles

- A 2-cycle such as (3, 7) is called a *transposition*

- **Every cycle can be written as a product of transposition :**

  $$(i_1, i_2, \ldots , i_r) = (i_1, i_r)(i_1, i_{r-1}) \ldots (i_1, i_3)(i_1, i_2)$$

  For example,

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

Permutations and transpositions

- Since every permutation can be expressed as a product of (disjoint) cycles, every permutation can be expressed as a product of transpositions
For example,

$$f=\begin{bmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 3 & 8 & 2 & 6 & 7 & 4 & 9 & 1 & 5\end{bmatrix}$$

$$=(1,3,2,8)(4,6)(5,7,9)$$

$$=(1,8)(1,2)(1,3)(4,6)(5,9)(5,7)$$

Product of Transposition

- Theorem If a permutation f is expressed as a product of p transpositions and also a product of q transpositions, then p and q are either both even or both odd.

- Definition A permutation that can be expressed as a product of an even number of transpositions is called an even permutation, and is called an odd permutation if it can be expressed a product of odd transpositions

Even, Odd Permutations

- Observe that (1,3,2,4)(1,7,6,2) = (1,7,6,4)(2,3)
  So, we can write this permutation as two different product of transpositions :
  (1,3,2,4)(1,7,6,2) = (1,4)(1,2)(1,3)(1,2)(1,6)(1,7)
  (1,7,6,4)(2,3) = (1,4)(1,6)(1,7)(2,3)

- **Note that (1,2)(1,2) is an expression of the identity mapping, so identity is an even permutation**

Permutation of a Set

- Let A be the set { *1, 2, …, n* }.
  A **permutation** on A is a function
  $$f : A \to A$$
  that is both one-to-one and onto.

- The set of all permutations on A is denoted by S_n

- A permutation is represented by a matrix :
  $$f = \begin{bmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & & f(n) \end{bmatrix}$$

Examples of Permutation

- Let A be the set { *1, 2, 3, 4, 5* }

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{bmatrix}$$

$$g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{bmatrix}$$

f and g are elements of S_5

Product of Permutations

- The product of *f* and *g* is the composition function $f \circ g$

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{bmatrix}$$

$$f \circ g = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & ? & ? & ? & ? \end{bmatrix}$$

Cycles : A special kind of Permutation

- An element f of S$_n$ is a cycle (r-cycle) if there exists

$$\{\, i_1, i_2, \cdots, i_r \,\} \subseteq \{\, 1, 2, \cdots, n \,\}$$

such that

$$f(i_1) = i_2 \,,\, f(i_2) = i_3 \,, \cdots ,\, f(i_{r-1}) = i_r \,,\, f(i_r) = i_1$$

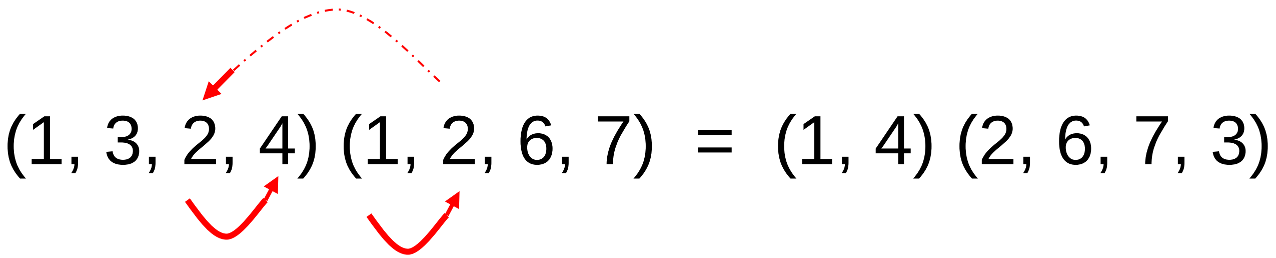
$$\text{and } f(m) = m \text{ for all other } m \notin \{ i_1, i_2, \cdots, i_r \}$$

Cycles will be written simply as (i_1, i_2, ... , i_r)

Example : $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & \downarrow & \downarrow & \\ 3 & 2 & 4 & 1 & 5 \end{bmatrix}$ = (1, 3, 4)

Product of Cycles

- If (1, 3, 2, 4) and (1, 2, 6, 7) are two cycles in S_7 we have



$$(1, 3, 2, 4)\,(1, 2, 6, 7) \;=\; (1, 4)\,(2, 6, 7, 3)$$

- Note that (1, 4) (2, 6, 7, 3) is a product of disjoint cycles

Permutations and cycles

- Every permutation can be written as a product of disjoint cycles. For example

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 2 & 6 & 7 & 4 & 9 & 1 & 5 \end{bmatrix}$$

We have

$$1 \rightarrow 3 \rightarrow 2 \rightarrow 8 \rightarrow 1$$
$$4 \rightarrow 6 \rightarrow 4$$
$$5 \rightarrow 7 \rightarrow 9 \rightarrow 5$$

We can easily verify that

f = (1, 3, 2, 8)(4, 6)(5, 7, 9)

Example

- Compute στ and τσ if $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$.
- Sol:

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

$$\nparallel$$

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

- Note that $\sigma\tau \neq \tau\sigma$ in general.

Transpositions : A special kind of cycles

- A 2-cycle such as (3, 7) is called a *transposition*

- Every cycle can be written as a product of transposition :

$$(i_1, i_2, \ldots , i_r) = (i_1, i_r)(i_1, i_{r-1}) \ldots (i_1, i_3)(i_1, i_2)$$

For example,

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

Transposition

- A cycle of length 2 is called a transposition.
- Thus each transposition δ has the form $\delta=(m, n)$, where $m\neq n$.

$$(1\ 2)(2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3)$$

Permutations and transpositions

- Since every permutation can be expressed as a product of (disjoint) cycles, every permutation can be expressed as a product of transpositions
  For example,

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 8 & 2 & 6 & 7 & 4 & 9 & 1 & 5 \end{bmatrix}$$

$$= (1,3,2,8)(4,6)(5,7,9)$$

$$= (1,8)(1,2)(1,3)(4,6)(5,9)(5,7)$$

- A permutation σ is called even or odd according as it can be written in some way as the product of an even or odd number of transpositions.

- The set of all even permutations in S_n is denoted A_n and is called the alternating group of degree n.

Product of Transposition

- Theorem 4.3 If a permutation f is expressed as a product of p transpositions and also a product of q transpositions, then p and q are either both even or both odd.

- Definition 4.4 A permutation that can be expressed as a product of an even number of transpositions is called an **even permutation**, and is called an **odd permutation** if it can be expressed a product of odd transpositions

Example

$$(1, 2, 3) = (1, 2)(2, 3)$$

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

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

$$(1, 2, 3, 4, 5, 6) = (1, 2)(2, 3)(3, 4)(4, 5)(5, 6)$$

Example

- Determine the parity of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 6 & 1 & 7 & 8 & 2 & 9 & 3 \end{pmatrix}$$

- Solution:
  - ➢We have σ = (1, 5, 7, 2, 4)(3, 6, 8, 9)

    =(1,5)(5,7)(7,2)(2,4)(3,6)(6,8)(8,9)
  - ➢So σ is odd because it has a product of 7 transpositions.

Identity permutation

- The identity permutation ε in S_n is defined as

$$\varepsilon = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

- In other words, $\varepsilon(k)=k$ holds for every $k\in X_n$.
- It is easy to verify that $\varepsilon\sigma=\sigma=\sigma\varepsilon$ holds for all $\sigma\in S_n$.

inverse

- If $\sigma\in S_n$, the fact that $\sigma: X_n\to X_n$ is one-to-one and onto implies that a uniquely determined permutation $\sigma^{-1} : X_n\to X_n$ exists (called the inverse of σ), which satisfies

  $\sigma(\sigma^{-1}(k))=k$ and $\sigma^{-1}(\sigma(k))=k$, for all $k\in X_n$.

Example

- Find the inverse of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 8 & 3 & 2 & 5 & 6 & 7 \end{pmatrix}$$ in S_8.

- Sol:

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

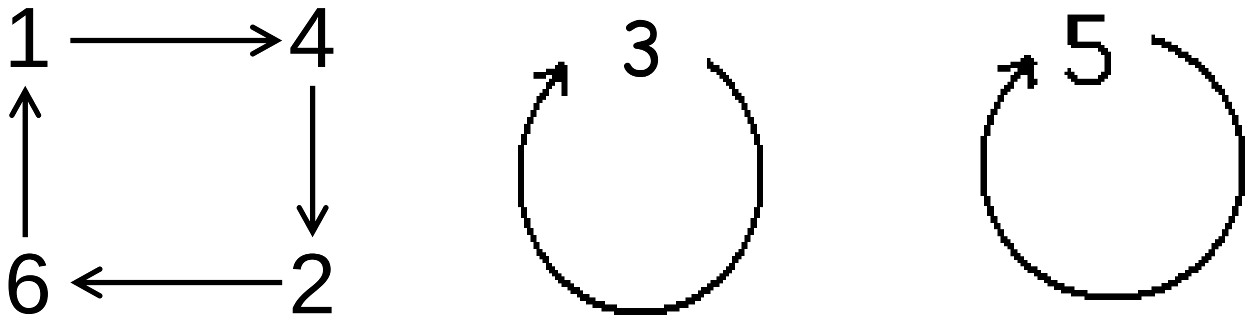
Example

- The set S_n of all permutations of $\{1,2,\cdots,n\}$ is a group under composition, called the symmetric group of degree n.

- Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix}$$ in S_6.

The action of σ is described graphically as:



Example

- Factor

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 5 & 12 & 2 & 1 & 9 & 11 & 4 & 3 & 7 & 10 & 13 & 8 & 6 \end{pmatrix}$$

as a product of (pairwise) disjoint cycles.

σ=(1, 5, 9, 7, 4)(2, 12, 8, 3)(6, 11, 13)

Example

- Find the order of $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}.$

- Solution:

$$\sigma = (1, 2, 3)(4, 5)$$

$$|\sigma| = 6$$

$$= \mathrm{lcm}(2, 3)$$

Example

- Find the order of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 5 & 7 & 9 & 14 & 10 & 11 & 12 & 8 & 3 & 13 & 2 & 6 & 4 & 1 \end{pmatrix}.$$

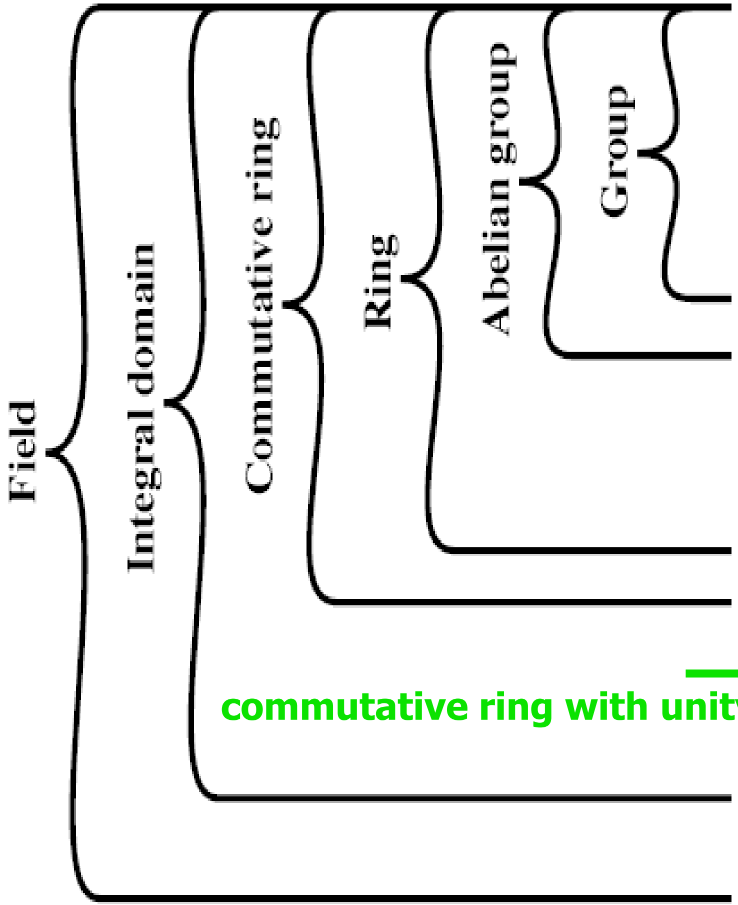
- Solution:

$$\sigma = (1,5,10,13,4,14)(2,7,12,6,11)(3,9)$$

$$|\sigma| = \mathrm{lcm}(6,5,2) = 30.$$

Ring Theory

- 1 Ring
- 2 Integral Domain & Field
- 3 Ring Properties



Field

Integral domain

Commutative ring

Ring

Abelian group

Group

commutative ring with unity

(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and a 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Ring Structure

- Def

Let R be a nonempty set on which we have two closed binary operations, denoted by + and $\cdot$. Then $(R,+,\cdot)$ is a ring if for all $a,b,c \in R$, the following conditions are satisfied:

a) $a + b = b + a$

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

c) $\exists\ z\ (\in R)$ such that $a + z = z + a = a$

d) For each $a \in R$, $\exists\ b$ with $a + b = b + a = z$

Abelian group

e) $a\cdot(b\cdot c) = (a\cdot b)\cdot c \rightarrow a(bc) = (ab)c = abc$ associative

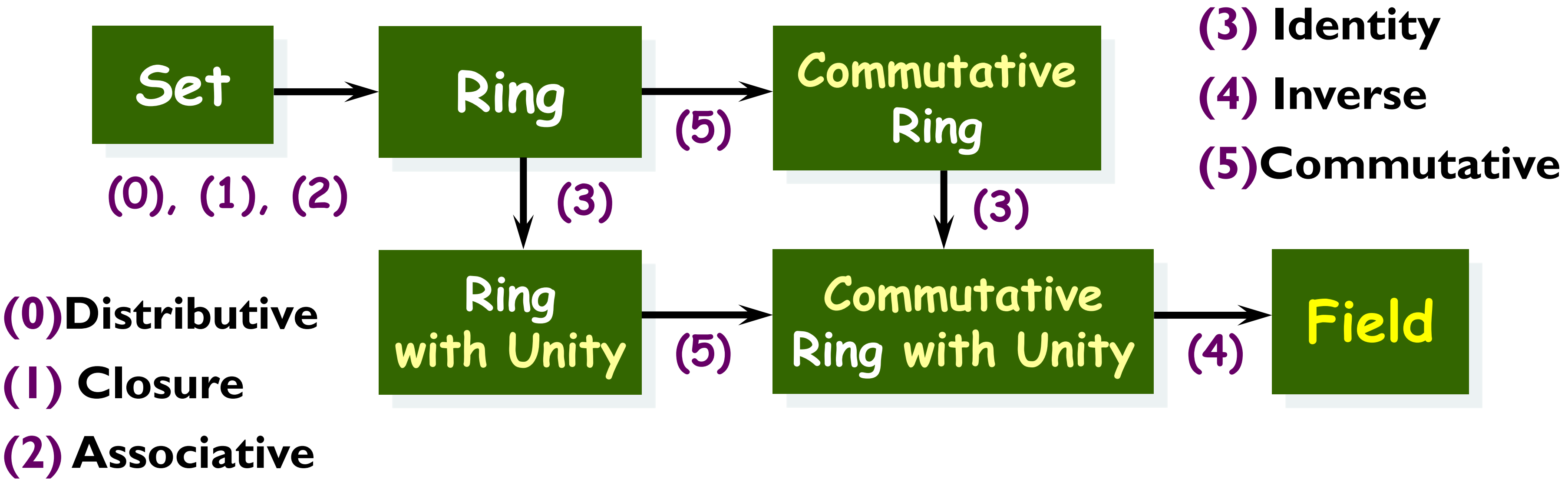
f) $a\cdot(b+c) = a\cdot b + a\cdot c$ and $(b+c)\cdot a = b\cdot a + c\cdot a$

distributive

Examples

Under the ordinary addition and multiplication, Z, Q, R, and C are rings.

Let $M_{2,2}(Z)$ be the set of all 2X2 matrices with integer entries. Then it is a ring under the ordinary matrix addition and matrix multiplication.



Commutative Ring with Unity

- Let $(R,+,\cdot)$ be a ring.

  Commutative Ring : $ab = ba$ for all $a,b \in R$

  Ring with Unity :

  $\exists\ u\ (\in R)$ such that $au = ua = a$ and

  $u \neq z$ for all $a \in R$. The u is called

  a unity or multiplicative identity.

  Commutative Ring with Unity :

  a commutative ring that has the unity.

  Note that the unity is unique.

An Example

- $(Z,\oplus,\otimes)$; $x\oplus y = x+y-1$ and $x\otimes y = x+y-xy$

1) $\oplus$ and $\otimes$ are closed operators.

2) $\oplus$ is commutative and associative.

3) $\exists$ a zero element (additive identity) $z=1$ for $\oplus$.

$$x\oplus 1 = 1\oplus x = x+1-1 = x$$

4) The additive inverse of x is $2-x$.

$$x\oplus(2-x) = (2-x)\oplus x = x+(2-x)-1 = 1$$

5) $(Z,\oplus,\otimes)$ satisfies the associative law of $\otimes$ and the distributive law of $\otimes$ over $\oplus$.

6) Unity (multiplicative identity) 0:

$$x\otimes u = x+u-xu = x \rightarrow u = 0\ (\neq z)$$

Ring with unity

Zero Element ?

- ∃ a zero element (additive identity) $z = 1$ for ⊕.

$$x \oplus 1 = 1 \oplus x = x + 1 - 1 = x$$

Which one is true ?

- $\oplus : K \times K \to K$

Identity element e for ⊕ in K

$$e \oplus a = a \oplus e = a \text{ for all } a \in K$$

Zero element z for ⊕ in K

$$z \oplus a = a \oplus z = z \text{ for all } a \in K$$

Zero Element ?

- zero element can be defined as followings
  (depending on the context)
  (1) additive identity
  (2) absorbing element
  - let (*S*,*) be a set *S* with a binary operation * on it. A **zero element** is an element *z* such that for all *s* in *S*, *z***s*=*s***z*=*z*.
  - *z***s*=*z* : left zero
  - *s***z*=*z* : right zero

Another Example

- U = {1,2} and R = P(U) (power set)

A+B = A Δ B = { x | x∈A or x∈B, but not both }

A·B = A ∩ B = intersection of sets A,B ⊆ U

+	ϕ	{1}	{2}	U
ϕ	ϕ	{1}	{2}	U
{1}	{1}	ϕ	U	{2}
{2}	{2}	U	ϕ	{1}
U	U	{2}	{1}	ϕ

·	ϕ	{1}	{2}	U
ϕ	ϕ	ϕ	ϕ	ϕ
{1}	ϕ	{1}	ϕ	{1}
{2}	ϕ	ϕ	{2}	{2}
U	ϕ	{1}	{2}	U

Additive Identity : ϕ

Additive Inverse : itself

Unity : U

Commutative

{1},{2} : proper divisors of zero

Ref) Proper divisors of zero

(Ex.) $< Z_6, +, \cdot >$

➔ **Not Field**

Unit : Invertible element of ring R ~ No zero divisor

+	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

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

proper divisors of zero

Unit

If $\forall$a,b $\in$ R, $ab = z \;\Rightarrow a = z$(additive identity,0) or $b = z$, then R is said to have no proper divisors of zero (zero divisor).

Multiplicative Inverse & Unit

- Def

Let R be a ‘ring with unity u’.

If $a \in R$ and there exist $b \in R$ such that $ab = ba = u$, then

b is called a multiplicative inverse of a and

a is called a unit of R.

(The b is also a unit of R.)

That is, a unit in a ring *R* is an invertible element o

Integral Domain & Field

- Def

Let R be a commutative ring with unity. Then

(a) R is called an integral domain if R has no proper divisors of zero.

(b) R is called a field if every nonzero element of R is a unit (= invertible !).

- ❑ $(Z,+,\cdot)$: an integral domain but not field

  (only 1 and -1 are units.) $2 * \frac{1}{2} = 1$

- ❑ $(Q,+,\cdot), (R,+,\cdot), (C,+,\cdot)$: integral domain & field

An Example

Let $M_{2,2}(Z)$ be the set of all 2x2 matrices with integer entries. Is it an integral domain under the ordinary matrix addition and matrix multiplication ?

No. Because it is not a commutative ring with unity.

$AB = 0 \rightarrow A = 0$ or $B = 0$?

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

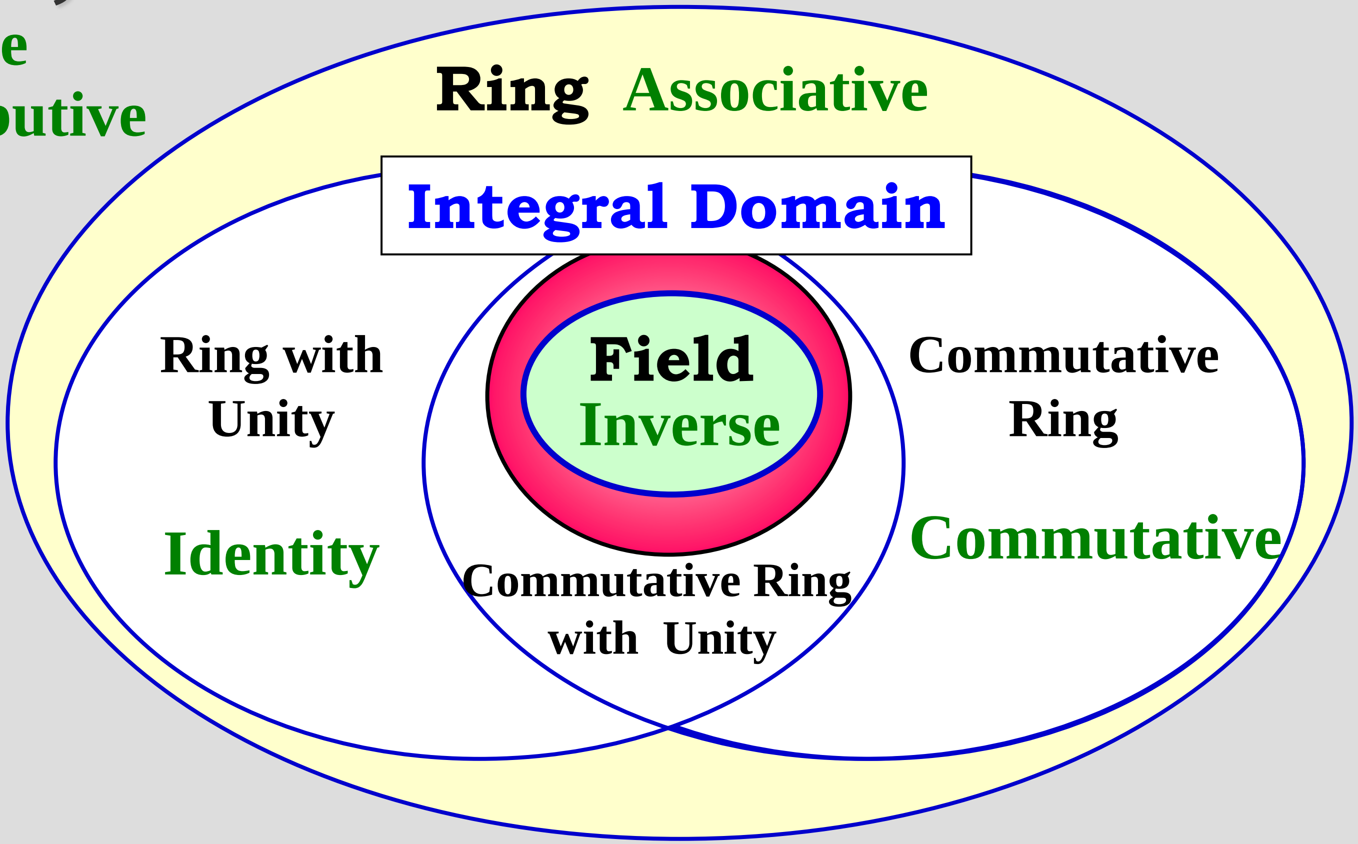
$CA = CB \rightarrow A = B$? $\qquad A^2 = I \rightarrow A = \pm I$?

from Ring to Field

$< K, \oplus, \otimes >$

Closure

Distributive



Ring Associative

Integral Domain

Ring with Unity

Identity

Field

Inverse

Commutative Ring

Commutative

Commutative Ring with Unity

Ring Properties (1)

- Theorem 1

  In any ring $(R,+,\cdot)$,

  (a) the zero element z is unique, and

  (b) the additive inverse of each ring element is unique.

  (Notation) $-a$ = additive inverse of a

- Theorem 2 (Cancellation of Addition)

  For all a, b, $c \in R$,

  (a) $a + b = a + c$ ➔ $b = c$, and

  (b) $b + a = c + a$ ➔ $b = c$.

Ring Properties (2)

- Theorem 3

  For any ring $(R,+,\cdot)$ and any $a \in R$, we have $az = za = z$.

(Proof)

$$a\cancel{z} + z = az = a(z + z) = \cancel{a}z + az$$

By the cancellation law, $z = az$.

Similarly, $za = z$.

Ring Properties (3)

- Theorem 4

  Given a ring $(R,+,\cdot)$, for all $a, b \in R$,

  (a) $-(-a) = a$

  (b) $a(-b) = (-a)b = -(ab)$

  (c) $(-a)(-b) = ab$

(Proof of (b))

$\boldsymbol{ab + a(-b) = a[b + (-b)] = az = z}$ **&**

$\boldsymbol{ab + (-a)b = [a + (-a)]b = zb = z.}$

From the uniqueness of additive inverse,

$\boldsymbol{a(-b) = -(ab) = (-a)b.}$

Ring Properties (4)

- Theorem 5

For a ring $(R,+,\cdot)$,

(a) if R has a unity, then it is unique, and

(b) if R has a unity, and x is a unit of R, then the multiplicative inverse of x is unique.

(Proof)

If u and v are unity's of R, then $u = uv = v$. Thus the unity is unique.

Let a and b are multiplicative inverses of x. Then $a = au = a(xb) = (ax)b = ub = b$. Therefore, ...

Ring Properties (5)

- Theorem 6

  Let $(R,+,\cdot)$ be a commutative ring with unity. Then R is an integral domain if and only if, for all $a,b,c \in R$ where $a \neq z$, $ab = ac$ ➔ $b = c$. (cancellation of multiplication)

- Theorem 7

  If $(F,+,\cdot)$ is a field, then it is an integral domain.

(Proof)

Let a ($\neq z$), $b \in F$ with $ab = z$. Then a has the unique inverse a^{-1}. $a^{-1}(ab) = a^{-1}z$ ➔ $b = z$.

Hence F has no proper divisors of zero.

Ring Properties (6)

- Theorem 8

A finite integral domain $(D,+,\cdot)$ is a field.

(Proof)

Let $D = \{d_1, d_2,\ldots, d_n\}$.

$dD = \{dd_1, dd_2,\ldots, dd_n\}$, for $d \in D$ and $d \neq z$.

From closure and multiplicative cancellation, $dd_i \neq dd_j$ and $dD = D$. Then, $dd_k = u$ for some $1 \leq k \leq n$ and any d is a unit of D. Therefore, $(D,+,\cdot)$ is a field.

THANK YOU