

Chapter 4: Binary Operations and Relations

4.1: Binary Operations

DEFINITION 1. A **binary operation** $*$ on a nonempty set A is a function from $A \times A$ to A .

Addition, subtraction, multiplication are binary operations on \mathbf{Z} .

Addition is a binary operation on \mathbf{Q} because

Division is NOT a binary operation on \mathbf{Z} because

Division is a binary operation on

Classification of binary operations by their properties

Associative and Commutative Laws

DEFINITION 2. A binary operation $*$ on A is **associative** if

$$\forall a, b, c \in A, \quad (a * b) * c = a * (b * c).$$

A binary operation $*$ on A is **commutative** if

$$\forall a, b \in A, \quad a * b = b * a.$$

Identities

DEFINITION 3. If $*$ is a binary operation on A , an element $e \in A$ is an **identity element** of A w.r.t $*$ if

$$\forall a \in A, \quad a * e = e * a = a.$$

EXAMPLE 4. 1 is an identity element for \mathbf{Z} , \mathbf{Q} and \mathbf{R} w.r.t. multiplication.

0 is an identity element for \mathbf{Z} , \mathbf{Q} and \mathbf{R} w.r.t. addition.

Inverses

DEFINITION 5. Let $*$ be a binary operation on A with identity e , and let $a \in A$. We say that a is **invertible** w.r.t. $*$ if there exists $b \in A$ such that

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

If b exists, we say that b is an **inverse** of a w.r.t. $*$ and write $b = a^{-1}$.

Note, inverses may or may not exist.

EXAMPLE 6. Every $x \in \mathbf{Z}$ has inverse w.r.t. addition because

$$\forall x \in \mathbf{Z}, \quad x + (-x) = (-x) + x = 0.$$

However, very few elements in \mathbf{Z} have multiplicative inverses. Namely,

EXAMPLE 7. Let $*$ be a binary operation on \mathbf{Z} defined by

$$\forall a, b \in \mathbf{Z}, \quad a * b = a + 3b - 1.$$

(a) Prove that the operation is binary.

(b) Determine whether the operation is associative and/or commutative. Prove your answers.

(c) Determine whether the operation has identities.

(d) Discuss inverses.

EXAMPLE 8. Let $*$ be a binary operation on the power set $P(A)$ defined by

$$\forall X, Y \in P(A), \quad X * Y = X \cap Y.$$

(a) Prove that the operation is binary.

(b) Determine whether the operation is associative and/or commutative. Prove your answers.

(c) Determine whether the operation has identities.

(d) Discuss inverses.

EXAMPLE 9. Let $*$ be a binary operation on $F(A)$ defined by

$$\forall f, g \in F(A), \quad f * g = f \circ g.$$

(a) Prove that the operation is binary.

(b) Determine whether the operation is associative and/or commutative. Prove your answers.

(c) Determine whether the operation has identities.

(d) Discuss inverses.

PROPOSITION 10. *Let $*$ be a binary operation on a nonempty set A . If e is an identity element on A then e is unique.*

Proof.

PROPOSITION 11. *Let $*$ be an associative binary operation on a nonempty set A with the identity e , and if $a \in A$ has an inverse element w.r.t. $*$, then this inverse element is unique.*

Proof. See Exercise 12.

Closure

DEFINITION 12. *Let $*$ be a binary operation on a nonempty set A , and suppose that $X \subseteq A$. If $*$ is also a binary operation on X then we say that X is closed in A under $*$.*

EXAMPLE 13. *Determine whether the following subsets of \mathbf{Z} are closed in \mathbf{Z} under addition and multiplication.*

(a) \mathbf{Z}^+

(b) \mathbf{E}

(c) \mathbf{O}

4.2: Equivalence Relations

DEFINITION 14. A **relation** R on a set A is a subset of $A \times A$. If $(a, b) \in R$, we write aRb .

EXAMPLE 15. On the set \mathbf{R} one can define aRb by $a < b$. Then, for example,

EXAMPLE 16. On the power set $P(\mathbf{Z})$ one can define R by ARB if $|A| = |B|$.

Properties of Relations

DEFINITION 17. Let R be a relation on a set A . We say:

1. R is **reflexive** if $aRa, \forall a \in A$.
2. R is **symmetric** if $\forall a, b \in A$, if aRb then bRa .
3. R is **transitive** if $\forall a, b, c \in A$, if aRb and bRc , then aRc .
4. R is **antisymmetric** if $\forall a, b \in A$, if aRb and bRa , then $a = b$.

DEFINITION 18. A relation R on a set A is called an **equivalence relation** if it is reflexive, symmetric, and transitive.

EXAMPLE 19. Let R be the relation on \mathbf{Z} defined by aRb if $a \leq b$. Determine whether it is reflexive, symmetric, transitive, or antisymmetric.

EXAMPLE 20. Let R be the relation on \mathbf{R} defined by aRb if $|a - b| \leq 1$ (that is a is related to b if the distance between a and b is at most 1.) Determine whether it is reflexive, symmetric, transitive, or antisymmetric.

EXAMPLE 21. Let R be the relation on \mathbf{Z} defined by aRb if $a + 3b \in \mathbf{E}$. Show that R is an equivalence relation.

REMARK 22. When R is an equivalence relation, it is common to write $a \sim b$ instead of aRb , read “ a is equivalent to b .”

EXAMPLE 23. Let $n \in \mathbf{Z}^+$. Define aRb on \mathbf{Z} by $n|a - b$. (In particular, if $n = 2$ the aRb means $a - b$ is _____). Show that R is an equivalence relation.

REMARK 24. The above relation is called **congruence** modulo n , and usually written

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

Equivalence Classes

DEFINITION 25. If R is an equivalence relation on a set A , and $a \in A$, then the set

$$[a] = \{x \in A \mid x \sim a\}$$

is called the **equivalence class** of a . Elements of the same class are said to be **equivalent**.

EXAMPLE 26. Define aRb on \mathbf{Z} by $2 \mid a - b$. (In other words, R is the relation of congruence mod 2 on \mathbf{Z} .)

(a) What integers are in the equivalence class of 6?

(b) What integers are in the equivalence class of 25?

(c) How many distinct equivalence classes there? What are they?

EXAMPLE 27. Define aRb on \mathbf{Z} by $n \mid a - b$. (In other words, R is the relation of congruence mod n on \mathbf{Z} .)

(a) How many distinct equivalence classes there? What are they?

(b) Show that the set of these equivalence classes forms a partition of \mathbf{Z} .

THEOREM 28. *If R is an equivalence relation on a nonempty set A , then the set of equivalence classes on R forms a partition on A .*

Proof.

So, any equivalence relation on a set A leads to a partition of A . In addition, any partition of A gives rise to an equivalence relation on A .

THEOREM 29. *Let $\mathcal{P}(A)$ be a partition of a nonempty set A . Define a relation R on A by aRb if a and b are in the same element of the partition. Then R is an equivalence relation on A .*

Proof.

Conclusion: Theorems 28 and 29 imply that there is a bijection between the set of all equivalence relations of A and the set of all partitions on A .

EXAMPLE 30. *Let R be the relation on \mathbf{Z} defined by aRb if $a + 3b \in \mathbf{E}$. By one of the above examples, R is an equivalence relation. Determine all equivalence classes for R .*

Partial and linear ordering

Recall that aRb defined by $a \leq b$, $a, b \in \mathbf{R}$, is not an equivalence relation. Why?

DEFINITION 31. A relation R on a set A is called a **partial ordering** on A if R is reflexive, transitive and antisymmetric.

If A is a set and there exists a partial ordering on A , then we say that A is a **partially ordered set**.

EXAMPLE 32. Let A be a set. For all $X, Y \in P(A)$ define R by $X \subseteq Y$. Then R is a partial ordering of $P(A)$.

DEFINITION 33. Let A be a set and R be a partial ordering on A . We say that R is a **linear ordering** on A if for all $a, b \in A$ either aRb , or bRa .

EXAMPLE 34. \leq is a linear ordering of \mathbf{R}

EXAMPLE 35. *Discuss when the relation from Example 32 is a linear ordering.*

EXAMPLE 36. *(cf. Example 17(c).) Let R be a relation on a set A . If R is both symmetric and antisymmetric, does it follow that R is reflexive?*