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 f 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.*

EXAMPLE 10. [1] *Let $*$ be a binary operation on the set $M_2(\mathbf{R})$ of all 2×2 matrices defined by*

$$\forall A_1, A_2 \in M_2(\mathbf{R}), \quad A_1 * A_2 = A_1 + A_2.$$

(a) *Prove that the operation is binary.*

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

[1] se Appendix at the end of the Chapter.

(c) *Determine whether the operation has identities.*

(d) *Discuss inverses.*

EXAMPLE 11. *Let* $*$ *be a binary operation on the set* $M_2(\mathbf{R})$ *of all* 2×2 *matrices defined by*

$$\forall A_1, A_2 \in M_2(\mathbf{R}), \quad A_1 * A_2 = A_1 A_2.$$

(a) *Prove that the operation is binary.*

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

(c) *Show that the matrix* $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *is an identity element w.r.t.* $*$.

(d) *Discuss inverses (Use the following FACT: "A matrix is invertible if and only if its derminant does not equal to zero").*

PROPOSITION 12. *Let* $*$ *be a binary operation on a nonempty set* A*. If* e *is an identity element on* A *then* e *is unique.*

Proof.

PROPOSITION 13. *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 14. *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 15. *Determine whether the following subsets of $\mathbf{Z}$ are closed in $\mathbf{Z}$ under addition and multiplication.*

(a) $\mathbf{Z}^+$

(b) $\mathbf{E}$

(c) $\mathbf{O}$

EXAMPLE 16. *Determine whether the following subsets of $M_2(\mathbf{R})$ is closed in $M_2(\mathbf{R})$ under matrix addition and multiplication:*

$$S = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{R}) |\ a = d. \right\}$$

4.2: Equivalence Relations

DEFINITION 17. *A* **relation** *R on a set A is a subset of $A \times A$. If $(a, b) \in R$, we write aRb.*

EXAMPLE 18. *On the set* $\mathbf{R}$ *one can define aRb by $a < b$. Then, for example,*

EXAMPLE 19. *On the power set $P(\mathbf{Z})$ one can define R by ARB if $|A| = |B|$.*

Properties of Relations

DEFINITION 20. *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, ten $a = b$.*

.

DEFINITION 21. *A relation R on a set A is called an* **equivalence relation** *if it is reflexive, symmetric, and transitive.*

EXAMPLE 22. *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 23. *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 24. *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 25. When R is an equivalence relation, it is common to write $a \sim b$ instead of aRb, read "a is equivalent to b."

EXAMPLE 26. *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 27. The above relation is called **congruence** mod n, and usually written

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

Equivalence Classes

DEFINITION 28. *If R is an equivalence relation on a set A, and $a \in A$, then the set*

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

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

EXAMPLE 29. *Define aRb on* $\mathbf{Z}$ *by $2|a-b$. (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 30. *Define aRb on* $\mathbf{Z}$ *by $n|a-b$. (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 31. *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 32. *Let $\mathcal{R}$ be a partition of a nonempty set A. Define a relation R_1 on A by aR_1b if a and b are in the same element of the partition $\mathcal{R}$. Then R_1 is an equivalence relation on A.*

Proof.

Conclusion: Theorems 31 and 32 imply that there is a bijection between the set of all equivalence relations of A and the set of all partitions on A.

EXAMPLE 33. *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 34. *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 35. *For all $X, Y \in P(A)$ define R by $X \subseteq Y$. Then R is a partial ordering of $P(A)$.*

DEFINITION 36. *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 37. $\leq$ *is a linear ordering of* $\mathbf{R}$

EXAMPLE 38. *Discuss when the relation from Example 35 is a linear ordering.*

EXAMPLE 39. *(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?*

Appendix: Matrices and Matrix Multiplication

1. An $m \times n$ (this is often called the size or dimension of the matrix) matrix is a table with m rows and n columns and the entry in the i-th row and j-th column is denoted by a_{ij}:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

2. A matrix is usually denoted by a capital letter and its elements by small letters : a_{ij} = entry in the ith row and jth column of A.

3. Two matrices are said to be **equal** if they are the same size and each corresponding entry is equal.

4. Special Matrices:

   - A **square** matrix is any matrix whose size (or dimension) is $n \times n$ (i.e. it has the same number of rows as columns.) In a square matrix the diagonal that starts in the upper left and ends in the lower right is often called the **main diagonal.**
   - The **zero** matrix is a matrix all of whose entries are zeroes.
   - The **identity** matrix is a square $n \times n$ matrix, denoted I_n, whose main diagonal consists of all 1's and all the other elements are zero:

$$I_n = \begin{pmatrix} 1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & 1 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & 1 \end{pmatrix}$$

   - The **diagonal** matrix is a square $n \times n$ matrix of the following form

$$\begin{pmatrix} \lambda_1 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & \lambda_2 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot & \lambda_n \end{pmatrix}$$

   - **Column matrix** (=column vector) and the **row matrix** (=row vector) are those matrices that consist of a single column or a single row respectively:

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 & y_2 & \dots & y_n \end{pmatrix}$$

     Note that an n-dimensional column vector is an $n \times 1$ matrix, and an n-dimensional row vector is an $1 \times n$ matrix.

   - **Transpose of a Matrix**: If A is an $m \times n$ matrix with entries a_{ij} , then A^T is the $n \times m$ matrix with entries a_{ji}.
     A^T is obtained by interchanging rows and columns of A.

5. **Matrix Arithmetic**

- The **sum** or difference of two matrices of the same size is a new matrix of identical size whose entries are the sum or difference of the corresponding entries from the original two matrices. Note that we cant add or subtract entries with different sizes.
- The **scalar multiplication** by a constant gives a new matrix whose entries have all been multiplied by that constant.
- If A, B, and C are matrices of the *same* size, then
  (a) $A + B = B + A$ (Commutative Law)
  (b) $(A + B) + C = A + (B + C)$ (Associative Law)
- **Matrix multiplication**: If Y is a row matrix of size $1 \times n$ and X is a column matrix of size $n \times 1$ (see above), then the **matrix product** of Y and X is defined by

$$YX = \begin{pmatrix} y_1 & y_2 & y_3 & \cdots & y_n \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = y_1x_1 + y_2x_2 + y_3x_3 + \cdots + y_nx_n$$

- If A is an $m \times p$ matrix and matrix B is $p \times n$, then the product AB is an $m \times n$ matrix, and its element in the ith row and jth column is the product of the ith row of A and the jth column of B.
- RULE for multiplying matrices:
  The column of the 1st matrix must be the same size as the row of the 2nd matrix.

6. *Example.*

(a) Given

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ -1 & -2 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & -2 \\ 3 & 4 \\ 1 & 2 \end{pmatrix}$$

Compute $A - 2B$.

(b) Let $A = \begin{pmatrix} 1 & 2 & -3 & 0 & -1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 2 & 0 & 1 & -1 \end{pmatrix}$. Find BA^T.

(c) *Example.* Given

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ -1 & -2 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & -2 \\ 3 & 4 \end{pmatrix}$$

Compute AB and BA when it is possible.

(d) Compute $\begin{pmatrix} 1 & 2 & 5 \\ 3 & 2 & -3 \\ 4 & 3 & 9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

7. FACTS and LAWS FOR MATRIX MULTIPLICATION: If the size requirements are met for matrices A, B and C, then
   - $AB \neq BA$ (NOT always Commutative)[2]
   - $A(B + C) = AB + AC$ (always Distributive)
   - $(AB)C = A(BC)$ (always Associative)
   - $AB = 0$ does not imply that $A = 0$ or $B = 0$.
   - $AB = AC$ does not imply that $B = C$.
   - $I_n A = AI_n = A$ for any square matrix A of size n.

Determinant

8. Determinant of a matrix is a function that takes a square matrix and converts it into a number.
9. Determinant of 2×2 matrix:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

10. **Matrix Inverse**. Let A be a square matrix of size n. A square matrix, A^{-1}, of size n, such that $AA^{-1} = I_n$ (or , equivalently, $A^{-1}A = I_n$) is called an **inverse matrix**.
11. A^{-1} in the case $n = 2$: If $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ then

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

12. *FACT*: A^{-1} exists if and only if $\det A \neq 0$.

[2]Since the multiplication of matrices is NOT commutative, you MUST multiply left to right.