4&5 Binary Operations and Relations. The Integers. (part I)

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

- To prove that $*$ is a binary operation on a set A

- To show that $*$ is <u>not</u> a binary operation on a set A

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*

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

EXAMPLE 3. *Using symbols complete the following*

(a) *A binary operation* $*$ *on* A *is* <u>*not*</u> **associative** *if*

(b) *A binary operation* $*$ *on* A *is* <u>*not*</u> **commutative** *if*

Identities

DEFINITION 4. *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 5. **(a)** 1 *is an identity element for* **Z**, **Q** *and* **R** *w.r.t. multiplication.*

(b) 0 *is an identity element for* **Z**, **Q** *and* **R** *w.r.t. addition.*

Inverses

DEFINITION 6. *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 7. *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 8. *Let $*$ be an 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 9. *Let $*$ be an 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 10. *Let $*$ be an 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.*

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

(d) *Discuss inverses.*

PROPOSITION 11. *Let $*$ be a binary operation on a nonempty set A. If e is an identity element on A then e is unique.*

Proof.

PROPOSITION 12. *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.

Closure

DEFINITION 13. *Let $*$ be a binary operation on a nonempty set A, and suppose that $S \subseteq A$. If $*$ is also a binary operation on S then we say that S is closed in A under $*$.*

EXAMPLE 14. *Let $*$ be a binary operation on A and let $S \subseteq A$. Using symbols complete the following*

(a) *S is closed in A under $*$ if and only if*

(a) *S is <u>not</u> closed in A under $*$ if*

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) $\mathbf{O}$

5.1: The Integers: Axioms and Basic Properties

`Operations on the set of integers`, $\mathbf{Z}$: *addition* and *multiplication* with the following properties:

A1. Addition is **associative**:

A2. Addition is **commutative**:

A3. $\mathbf{Z}$ has an **identity** element with respect to addition namely, the integer 0.

A4. Every integer x in $\mathbf{Z}$ has an **inverse** w.r.t. addition, namely, its negative $-x$:

A5. Multiplication is **associative**:

A6. Multiplication is **commutative**:

A7. $\mathbf{Z}$ has an **identity** element with respect to multiplication namely, the integer 1. (and $1 \neq 0$.)

A8. **Distributive Law:**

REMARK 16. We do not prove A1-A8. We take them as **axioms**: statements we *assume* to be true about the integers.

We use xy instead $x \cdot y$ and $x - y$ instead $x + (-y)$.

PROPOSITION 17. *Let* $a, b, c \in \mathbf{Z}$.

P1. *If* $a + b = a + c$ *then* $b = c$. *(cancellation law for addition)*

P2. $a \cdot 0 = 0 \cdot a = 0$.

P3. $(-a)b = a(-b) = -(ab)$

P4. $-(-a) = a$

P5. $(-a)(-b) = ab$

P6. $a(b - c) = ab - ac$

P7. $(-1)a = -a$

P8. $(-1)(-1) = 1$.

Proof

$\mathbf{Z}$ contains a subset $\mathbf{Z}^+$, called the **positive integers**, that has the following properties:

A9. Closure property: $\mathbf{Z}^+$ is closed w.r.t. addition and multiplication:

A10. Trichotomy Law: for all $x \in \mathbf{Z}$ exactly one is true:

PROPOSITION 18. *If* $x \in \mathbf{Z}$, $x \neq 0$, *then* $x^2 \in \mathbf{Z}^+$.

Proof.

COROLLARY 19. $\mathbf{Z}^+ = \{1, 2, 3, \ldots, n, n+1, \ldots\}$

Proof.

Inequalities (the order relation less than)

DEFINITION 20. *For $x, y \in \mathbf{Z}$, $x < y$ if and only $y - x \in \mathbf{Z}^+$.*

REMARK 21. If $x < y$, we can also write $y > x$. We can also write $x \leq y$ if $x < y$ or $x = y$. Similarly, $y \geq x$ if $y > x$ or $y = x$.

Note that $\mathbf{Z}^+ = \{n \in \mathbf{Z} | n > 0\}$.

EXAMPLE 22. *Let $x, y \in \mathbf{Z}$. Using symbols complete the following*

- $x < y \quad \Leftrightarrow$
- $x > y \quad \Leftrightarrow$
- $x < 0 \quad \Leftrightarrow$
- $x > 0 \quad \Leftrightarrow$

PROPOSITION 23. *Let $a, b \in \mathbf{Z}$.*

Q1. *Exactly one of the following holds: $a < b$, $b < a$, or $a = b$.*

Q2. *If $a > 0$ then $-a < 0$; if $a < 0$ then $-a > 0$.*

Q3. *If $a > 0$ and $b > 0$ then $a + b > 0$ and $ab > 0$.*

Q4. *If $a > 0$ and $b < 0$ then $ab < 0$.*

Q5. *If $a < 0$ and $b < 0$ then $ab > 0$.*

Proof.

PROPOSITION 24. *Let $a, b, c \in \mathbf{Z}$.*

Q6. *If $a < b$ and $b < c$ then $a < c$.*

Q7. *If $a < b$ and $a + c < b + c$.*

Q8. *If $a < b$ and $c > 0$ then $ac < bc$.*

Q9. *If $a < b$ and $c < 0$ then $ac > bc$.*

A11. The Well Ordering Principle Every nonempty subset on $\mathbf{Z}^+$ has a smallest element; that is, if S is a nonempty subset of Z^+, then there exists $a \in S$ such that $a \leq x$ for all $x \in S$.

PROPOSITION 25. *There is no integer x such that $0 < x < 1$.*

Proof.

COROLLARY 26. 1 *is the smallest element of* $\mathbf{Z}^+$.

COROLLARY 27. *The only integers having multiplicative inverses in* $\mathbf{Z}$ *are* ± 1.

5.2: Induction[1]

THEOREM 28. (`First Principle of Mathematical Induction`) *Let $P(n)$ be a statement about the positive integer n. Suppose that $P(1)$ is true. Whenever k is a positive integer for which $P(k)$ is true, then $P(k+1)$ is true. Then $P(n)$ is true for every positive integer n.*

Proof.

Paradox: All horses are of the same color.
Question: What's wrong in the following "proof" of G. Pólya?

$P(n)$: Let $n \in \mathbf{Z}^+$. Within any set of n horses, there is only one color.

Basic Step. If there is only one horse, there is only one color.

Induction Hypothesis. Assume that within any set of k horses, there is only one color.

Inductive step. Prove that within any set of $k+1$ horses, there is only one color.

Indeed, look at any set of $k+1$ horses. Number them: $1, 2, 3, ..., k, k+1$. Consider the subsets $\{1, 2, 3, ..., k\}$ and $\{2, 3, 4, ..., k+1\}$. Each is a set of only k horses, therefore within each there is only one color. But the two sets overlap, so there must be only one color among all $k+1$ horses.

[1]see also Chapter 1(Part III)