Groups

Sets Definition

distinct

Finite

Infinite

In mathematics, a **set** is defined as a well-defined collection of objects. Sets are named and represented using capital letters. In the set theory, the elements that a set comprises can be any kind of thing: people, letters of the alphabet, numbers, shapes, variables, etc.

- Set of natural numbers, $\mathbb{N} = \{1, 2, 3, \ldots\}$
- Set of whole numbers, $W = \{0, 1, 2, 3, \ldots\}$
- Set of integers, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

Groups - Set of elements + some binary operation

{G, .}

↳ binary

Domain → Integers $G \to \{1, 2, 4, \ldots\}$

+

Sl No	Example	Property/Axiom	Generic Form
A1 1	$1+4=5 \in G$ $3+7=10 \in G$	Closure	$a \cdot b \in G$ $a \in G$ & $b \in G$
A2 2	$1+(2+4)=1+6=7$ $(1+2)+4=3+4=7$	Associativity	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
A3 3	$5+\underline{0}=5$ → identity $10+\underline{0}=10$	Identity	$a \cdot e = e \cdot a = a$
A4 4	$5+\underline{(-5)}=0$ → inverse $10+\underline{(-10)}=0$	Inverse	$a \cdot a' = a' \cdot a = e$
5	$4+5=9$ $5+4=9$	Commutative	$a \cdot b = b \cdot a$ } Abelian

Groups

A **group** G, sometimes denoted by $\{G, \cdot\}$, is a set of elements with a binary operation denoted by $\cdot$ that associates to each ordered pair (a, b) of elements in G an element $(a \cdot b)$ in G, such that the following axioms are obeyed:[1]

(A1) Closure: If a and b belong to G, then $a \cdot b$ is also in G.

(A2) Associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in G.

(A3) Identity element: There is an element e in G such that $a \cdot \mathrm{e} = \mathrm{e} \cdot a = a$ for all a in G.

(A4) Inverse element: For each a in G, there is an element a' in G such that $a \cdot a' = a' \cdot a = \mathrm{e}$.

If a group has a finite number of elements, it is referred to as a **finite group**, and the **order** of the group is equal to the number of elements in the group. Otherwise, the group is an **infinite group**.

Abelian Group

A group is said to be **abelian** if it satisfies the following additional condition:

(A5) Commutative: $a \cdot b = b \cdot a$ for all a, b in G.

A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$. The element a is said to **generate** the group G or to be a **generator** of G. A cyclic group is always abelian and may be finite or infinite.


THANK YOU!


LIKE
COMMENT
SHARE
SUBSCRIBE

Rings - Set of elements + two binary operation

$\{R, +, \times\}$

$\times$ - Closure - Associative - Identity - Inverse

Sl No	Example	Property/Axiom	Generic Form
1	$2 \in R$; $3 \in R$ $2 \times 3 = 6 \in R$	Closure	$a \times b \in R$
2	$2 \times (3 \times 4) = (2 \times 3) \times 4$	Associative	$(a \times b) \times c = a \times (b \times c)$
3	$2 \times (3 + 4) = (2 \times 3) + (2 \times 4)$	Distributive	$a \times (b + c) = (a \times b) + (a \times c)$
4	$2 \times 4 = 4 \times 2$	Commutative	$a \times b = b \times a$
5	$10 \times \underbrace{1}_{\text{identity}} = 10$	Identity	$a \times e = a$
6	$a \times b = 0 \Rightarrow a = 0$ or $b = 0$	No zero divisors	

A **ring** R, sometimes denoted by $\{R, +, \times\}$, is a set of elements with two binary operations, called *addition* and *multiplication*,[3] such that for all a, b, c in R the following axioms are obeyed.

(A1–A5) R is an abelian group with respect to addition; that is, R satisfies axioms A1 through A5. For the case of an additive group, we denote the identity element as 0 and the inverse of a as $-a$.

(M1) Closure under multiplication: If a and b belong to R, then ab is also in R.

(M2) Associativity of multiplication: $a(bc) = (ab)c$ for all a, b, c in R.

(M3) Distributive laws: $a(b + c) = ab + ac$ for all a, b, c in R.
$(a + b)c = ac + bc$ for all a, b, c in R.

A1-A4 — Group

A1—A5 — Abelian group

A1-A5+ M1-M4 } → Ring

In essence, a ring is a set of elements in which we can do addition, subtraction $[a - b = a + (-b)]$, and multiplication without leaving the set.

A ring is said to be **commutative** if it satisfies the following additional condition:

A1-A5+ M1-M6 } Integral domain

(M4) Commutativity of multiplication: $ab = ba$ for all a, b in R.

Next, we define an **integral domain**, which is a commutative ring that obeys the following axioms.

(M5) Multiplicative identity: There is an element 1 in R such that $a1 = 1a = a$ for all a in R.

(M6) No zero divisors: If a, b in R and $ab = 0$, then either $a = 0$ or $b = 0$.

} Integral domain


LIKE
COMMENT
SHARE
SUBSCRIBE


THANK YOU!

Fields - Set of elements + two binary operation

{F , + , x}

Ring

Sl No	Example inverse	Property/Axiom	Generic Form
1	$8 \times \frac{1}{8} = 1$ ↳ e	multiplicative inverse	$a \times a^{-1} = e$

A **field** F, sometimes denoted by $\{F, +, \times\}$, is a set of elements with two binary operations, called *addition* and *multiplication*, such that for all a, b, c in F the following axioms are obeyed.

(A1–M6) F is an integral domain; that is, F satisfies axioms A1 through A5 and M1 through M6.

(M7) Multiplicative inverse: For each a in F, except 0, there is an element a^{-1} in F such that $aa^{-1} = (a^{-1})a = 1$.

In essence, a field is a set of elements in which we can do addition, subtraction, multiplication, and division without leaving the set. Division is defined with the following rule: $a/b = a(b^{-1})$.

In gaining insight into fields, the following alternate characterization may be useful. A **field** F, denoted by $\{F, +\}$, is a set of elements with two binary operations, called *addition* and *multiplication*, such that the following conditions hold:

1. F forms an abelian group with respect to addition.
2. The nonzero elements of F form an abelian group with respect to multiplication.
3. The distributive law holds. That is, for all a, b, c in F,

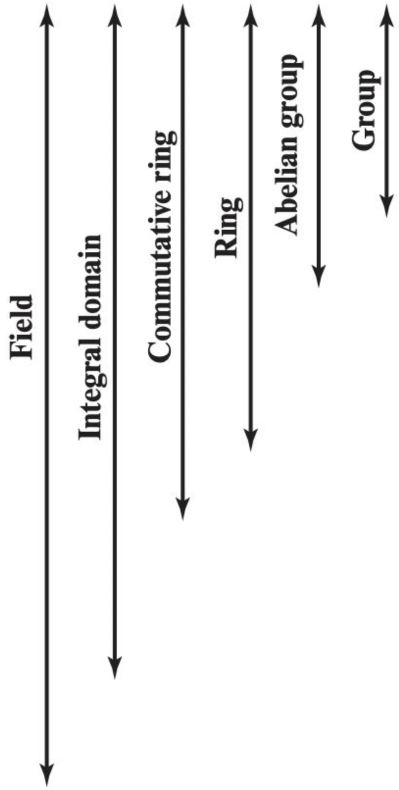
$$a(b + c) = ab + ac.$$

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


LIKE
COMMENT
SHARE
SUBSCRIBE


THANK YOU!

Groups, Rings and Fields



(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 $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Figure 5.2 Properties of Groups, Rings, and Fields


LIKE
COMMENT
SHARE
SUBSCRIBE


THANK YOU!