Group Theory

Dr. Smita Agrawal
Assistant Professor, CSED
TIET, Patiala
smita.agrawal@thapar.edu

Contents

- Sets with 2 Binary Operations
- Ring
- Commutative Ring
- Commutative Ring
- Field
- Examples

Sets with 2 Binary Operations

- Let S be a set with 2 binary operations $*$ and o.

a) Axioms $1-5$ refer to $*$ axioms.

b) Axioms $6, 7, 8$ *and* 10 are simply the axioms $1, 2, 3$ *and* 5 for the binary operation o.

c) Axiom 9: If S under $*$ satisfies the axioms $1-5$, then for every a in S, with $a \neq e$, $\exists$ a unique element a' in S such that

$$a' o\, a = a\, o\, a' = e'$$

where, e' is the identity element corresponding to o.

d) Axiom 11: Distributivity

for $a, b, c \in S$

$$a\, o\, (b * c) = (a\, o\, b) * (a\, o\, c)$$

Ring

- A set S with 2 binary operations $*$ and o is called a ring if:

a) It is an abelian group with respect to $*, and$

b) Operation o satisfies the closure, associativity and distributivity axioms (i.e. axioms $6, 7$ and 11).

Commutative Ring

- A ring is called a commutative ring if the commutativity axiom is satisfied for operation *o*.

Commutative Ring with Unity

- A commutative ring with unity is a commutative ring that satisfies the identity axiom for operation o.

Field

- A field is a set with 2 binary operations $*$ and o, if it satisfies all the axioms from $1 - 11$.

Examples

1. Set Z with addition and multiplication (in place of $*$ and o) is a commutative ring with unity.

   Here, the identity element with respect to addition is 0, and the identity element with respect to multiplication is 1.

2. The set of all 2×2 matrices with matrix addition and multiplication is a ring with identity, but it is not a field.

3. The set of all rational numbers (i.e. of the form a/b where a is an integer and $b \neq 0$) is a field.

   Here, identity element with respect to multiplication is 1. The inverse of a/b, $a/b \neq 0$, is b/a.

Examples (Cont..)

4. The power set $P(S)$ of a set with 2 binary operations $\cup$ and $\cap$ is neither a group nor a ring. It is also not a field.

Because here, the axioms satisfied by $\cup$ and $\cap$ are $1, 2, 3, 5, 6, 7, 8, 10$ *and* 11.

But it is an abelian monoid with respect to operations $\cup$ and $\cap$.

Q: Consider the ring $Z_{10} = \{0, 1, 2, -----, 9\}$ of integer modulo 10.

$m = 10$

addition mod 10.
multiplication mod 10.

a) Find the units of Z_{10}.

b) Find -3, -8 and 3^{-1}.

c) Let $f(x) = 2x^2 + 4x + 4$. Find the roots of $f(x)$ over Z_{10}.

Ans. a) Those integers that are relatively prime to the modulus $m = 10$ are the units of Z_{10}.

$\therefore$ Units are $1, 3, 7, 9$.

b) find -3, -8 and 3^{-1}.

-3 ↓ additive inverse of 3

3^{-1} ↓ multiplicative inverse of 3.

$\underline{a} + \underline{(-a)} = e = \underline{0}$

$(3 +_{10} 7) = 0$

$-3 = 7$

$(8 +_{10} 2) = 0$

$-8 = 2$

$aa^{-1} = e = 1$

$3 \times_{10} 7 = 1$

$3^{-1} = 7$

c) $f(x) = 2x^2 + 4x + 4 \mod 10$

$f(0) = 4 \mod 10 = 4$

$f(1) = 10 \mod 10 = 0$

$f(2) = 20 \mod 10 = 0$

$f(3) = 4$

$f(4) = 2$

$f(5) = 4$

$f(6) = 0$

$f(7) = 0$

$f(8) = 4$

$f(9) = 0$

$\therefore$ Roots are 1, 2, 6, 7 and 9.

$p \to q \equiv \neg p \vee q$

$p \to q \equiv$

Inverse

Converse

Contrapositive

$\neg q \to \neg p$