Define Normal Subgroup of a group.

A Subgroup H of a group G is called a normal subgroup if and only if $aha^{-1} \in H$ $\forall h \in H$ and $\forall a \in G$.

Evidently H is a normal subgroup of G if $aHa^{-1} \subset H$.

Prove that a subgroup H of a group G is normal if and only if $aHa^{-1} = H$ $\forall a \in G$.

Proof, Suppose that H is a subgroup of a group G such that

$aHa^{-1} = H$

Now to prove that H is a normal subgroup of G

Now, $aHa^{-1} = H$ $\forall a \in G$

$\Rightarrow aHa^{-1} \subset H$ $\forall a \in G$

Hence H is a normal subgroup of G.

Converse

Let H be a normal subgroup of G.

then we have to prove $aHa^{-1} = H$ $\forall a \in G$.

Since H is a normal subgroup of G

then $aHa^{-1} \subseteq H$ $\forall a \in G$ ... (1)

$\because a \in G \Rightarrow a^{-1} \in G$

Therefore we get [replacing a by a^{-1} in eqn (1)]

$a^{-1}H(a^{-1})^{-1} \subseteq H$ $\forall a \in G$

$\Rightarrow a^{-1}Ha \subseteq H \quad \forall a \in G$

$\Rightarrow a(a^{-1}Ha)a^{-1} \subseteq aHa^{-1} \quad \forall a \in G$

$\Rightarrow (aa^{-1})H(aa^{-1}) \subseteq aHa^{-1} \quad \forall a \in G$

$\Rightarrow eHe \subseteq aHa^{-1} \quad \forall a \in G$

$\Rightarrow (eH)e \subseteq aHa^{-1} \quad \forall a \in G$

$\Rightarrow He \subseteq aHa^{-1} \quad \forall a \in G$

$\Rightarrow H \subseteq aHa^{-1} \quad \forall a \in G \ldots\ldots (2)$

From eqn (1) & (2) we Concluded that

$$aHa^{-1} = H$$

* Prove that every subgroup of an abelian group is a normal subgroup.

Proof: Let G be an abelian group and N be a subgroup of G.

To prove that N is a normal subgroup.

Since $N \subseteq G$

So, $n \in N \Rightarrow n \in G$

Again since G is abelian

So, $an = na \quad \forall a \in G$ and $\forall n \in N$.

Hence the set $\{an : n \in N\}$ = the set $\{na : n \in N\} \forall a \in G$

or $aN = Na \quad \forall a \in G$

Hence the subgroup N is a normal subgroup.

RING

Define ring →

A Let R be a nonempty set and $a, b, c \in R$ be arbitrary. Then the Set R with two binary operations '+' (addition) and '.' (multiplication) is Called a ring if the following postulates are Satisfied : →

For '+' (addition)

1. closure law : $a, b \in R \Rightarrow a+b \in R$
2. Associative law : $a, b, c \in R \Rightarrow (a+b)+c = a+(b+c)$
3. Commutative law : $a, b \in R \Rightarrow a+b = b+a$
4. Existence of identity element : $\exists$ an element $0 \in R$ (zero element) such that $a+0 = a \ \forall a \in R$
5. Existence of inverse element : For each element a in R there exists an element x in R such that $a+x = 0$

For '.' (multiplication)

6. closure law : $a, b \in R \Rightarrow a \cdot b \in R$.
7. Associative law : $a, b, c \in R \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$

For '+' and '.'

8. Distributive law : $a, b, c \in R \Rightarrow a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$

Ex → (a) The set of integers is a ring with '+' and '.'.

(b) The set $E = \{x \mid x = 2m, m \in Z\}$ is a ring under '+' and '.'.

The above stated definition of Ring is supposed to be less ostensible and implicit definition of ring.

We can also say that

A nonempty set R with two binary operations '+' (addition) and '.' (multiplication) is said to be a ring $(R, +, \cdot)$ if

(i) $(R, +)$ is an abelian group.
(ii) $(R, \cdot)$ is a semigroup.
and (iii) $(\cdot)$ multiplication is distributive over $(+)$ addition.

* Define Commutative ring with examples.

A nonempty set R with two binary operations addition $(+)$ and multiplication $(\cdot)$ is called a Commutative ring if the following postulates are satisfied :—

(i) $a+b \in R \ \forall \ a, b \in R$ (Closure law)
(ii) $(a+b)+c = a+(b+c) \ \forall a, b, c \in R$ (Associative law)
(iii) R has a 0 zero element as an identity element i.e. $a+0 = 0+a = a \ \forall a \in R$ (Identity law for addition)
(iv) For every $a \in R \ \exists$ an element $x \in R$ such that
$a+x = x+a = 0$ (additive inverse)

(V) $a+b = b+a \quad \forall\ a,b \in R$ (Commutative law)

(VI) $a \cdot b \in R \quad \forall\ a,b \in R$ (Closure law)

(VII) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall\ a,b,c \in R$ (Associative law for multiplication)

(VIII) $a \cdot (b+c) = a \cdot b + a \cdot c$
$\forall\ a,b,c \in R$
$(b+c) \cdot a = b \cdot a + c \cdot a$ (distributive laws)

(IX) $a \cdot b = b \cdot a \quad \forall\ a,b \in R$ (Commutative law)

Examples →

(1) The set of even integers is a commutative ring under ordinary addition and multiplication without unity.

(2) The set of real numbers is a Commutative ring under ordinary addition and multiplication.

★ Define ring with unity.

~~At first we will define ring then~~

A ring R with multiplication unit element (identity element) is called a ring with unity or ring with identity element such that

$$a \cdot 1 = 1 \cdot a = a \quad \forall\ a \in R.$$

Examples →

(1) The set of integers is a Commutative ring with unity element under ordinary addition and multiplication.

(2) The set of real numbers is a Commutative ring with unity under ordinary addition and multiplication.

* Define ring without unity

At first we will define ring then if the identity element for multiplication does not exist is ring R then R is called a ring without unity.

Examples

(1) The set of all $n \times n$ matrices of even integral elements is a ring without unity, with respect to addition and multiplication operation.

(2) The set of even integers (whether zero or positive or negative) is a ring without unity under ordinary addition and multiplication.

Ring with Zero divisors.

If two non zero elements a and b i.e. $(a \neq 0, b \neq 0)$ of a ring R exist in such a way that either

$$ab = 0 \quad \text{or} \quad ba = 0$$

then the ring R is said to be a ring with zero divisors and a, b are called divisors of zero.

Ring without Zero divisors.

A ring R is without zero divisors if the product of no two non zero elements of R is zero, i.e. if $ab = 0 \Rightarrow a = 0, b = 0$ we can say that if in a ring R ∃ non zero elements a and b such that $ab = 0$ then R is said to be a ring with zero divisors.

Uniqueness of Unity in a Ring with Unity

* Prove that the unity in a ring is unique.

Proof → Let $(R, +, \cdot)$ be a ring with unity. To show that unity in the ring R is unique.

Suppose that R is not unique, so R possesses more than one unity element.

Let e and e' be two unity elements in R.

$$e \neq e'$$

Now $a \cdot e = e \cdot a = a \quad \forall a \in R \quad \ldots (1)$

and $a \cdot e' = e' \cdot a = a \quad \forall a \in R \quad \ldots (2)$

$\because e' \in R$, replacing a by e' in (1)

$$e'e = ee' = e' \quad \ldots (3)$$

$\because e \in R$, replacing a by e in (2)

$$ee' = e'e = e \quad \ldots (4)$$

So we get $e' = e$

Thus we observe that unity in a ring is unique.

* Prove that a ring R is without zero divisor iff the cancellation laws for multiplication hold in R.

Proof → Let R be a ring without zero divisors under the operation multiplication and addition.

Let $a, b, c \in R$ such that $a \neq 0$, $ab = ac$

We have, $a \cdot b = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0$

Here R is without zero divisors
So, $a \cdot (b-c) = 0$ and
$a \neq 0 \Rightarrow b - c = 0$
i.e. $b = c$
Thus the left cancellation law for multiplication holds in R.
Similarly we can prove that the right cancellation law for multiplication also holds in R.
Now we have to show that R is without zero divisors.
Suppose that cancellation laws hold for multiplication hold in R.
Let $ab = 0$, $a \neq 0$, $b \neq 0$
Then we have
$ab = a0$, since $a0 = 0$
Now $a \neq 0$, $ab = a0 \Rightarrow b = 0$
(by left cancellation law)
So this is a contradiction
Hence R is without zero divisors.

Define idempotent of an element of a ring.
An element a of a Ring $(R, +, \cdot)$ is said to be idempotent if
$aa = a$ i.e. $\boxed{a^2 = a}$

(4) If in a ring $x^2 = x \ \forall\ x \in R$ then prove that R is a commutative ring. 455

Ans) As $x \in R$
so $-x \in R$

$\therefore (-x)^2 = -x$
or $(-x)(-x) = -x$ [$\because (-a)(-b) = ab$ in a ring (property of ring)]
or $xx = -x$
or $x^2 = -x \ \forall\ x \in R$ ... (1)

But Given that
$x^2 = x \ \forall\ x \in R$ .. (2)

From (1) & (2)
$x = -x$ $\therefore ab = -(ab)$ ... (3)

Again let $a, b \in R \Rightarrow a+b \in R$
$\therefore (a+b)^2 = a+b$ [as $x^2 = x \ \forall\ x \in R$]
or $(a+b)(a+b) = a+b$
or $a(a+b) + b(a+b) = a+b$ [By distributive law of a ring]
or $a^2 + ab + ba + b^2 = a+b$
or $a + ab + ba + b = a+b$ [$\because a^2 = a,\ b^2 = b$ as $x^2 = x \ \forall x \in R$]
or $ab + ba = 0$ [By left and right cancellation laws for addition]

So ba is the additive inverse of ab.
$\therefore -(ab) = ba$ ..... (4)

By (3) & (4) we get
$ab = ba \ \forall\ a, b \in R$
So R is a Commutative ring.

* Prove that a ring R is Commutative if and only if (iff) $(a+b)^2 = a^2+2ab+b^2$, for all $a,b \in R$ where a^2 we mean $a \cdot a$.

Proof: Let the ring R be Commutative

then $a \cdot b = b \cdot a \quad \forall\ a, b \in R$ ---(1)

Now $(a+b)^2 = (a+b)\cdot(a+b)$ [Distributive law]

$= a(a+b) + b\cdot(a+b)$ [Distributive law]

$= a\cdot a + a\cdot b + b\cdot a + b\cdot b$ [from (1)]

$= a^2 + a\cdot b + a\cdot b + b^2$

$= a^2 + 2ab + b^2$

So $(a+b)^2 = a^2+2ab+b^2$, when Ring R is Commutative.

Again Let $(a+b)^2 = a^2+2ab+b^2 \quad \forall\ a,b \in R$ --- (2)

Now to prove R is Commutative we will have to show that $a\cdot b = b\cdot a \quad \forall\ a, b \in R$

Here $(a+b)^2 = a^2+2ab+b^2$

or $(a+b)(a+b) = a^2+2ab+b^2$

or $a\cdot(a+b) + b\cdot(a+b) = a^2+2ab+b^2$ [Distributive law]

or $a\cdot a + a\cdot b + b\cdot a + b\cdot b = a^2+2ab+b^2$ ["]

or $a^2 + a\cdot b + b\cdot a + b^2 = a^2 + a\cdot b + a\cdot b + b^2$

or $b\cdot a = a\cdot b$ [By Cancellation laws]

Hence if $(a+b)^2 = a^2+2ab+b^2 \quad \forall\ a,b \in R$

then $a\cdot b = b\cdot a$.

So ring R is Commutative.

Thus a ring R is Commutative if and only if $(a+b)^2 = a^2+2ab+b^2 \quad \forall\ a,b \in R$