Definition. Let R be a nonempty set and "+", "." be two binary operations defined on R such that:

1. (R, +) is an abelian group.
2. (R, .) is a semigroup.
3. The operation "." is distributive on the operation "+", then the ordered triple (R, +, .) is said to be ***ring***.

Definitions.

1. A ring (R, +, .) is said to be commutative if a.b = b.a for all a, b ∈R.
2. A ring R is said to be ring with identity if there exists 1∈ R such that a.1 = 1.a = a for all a in R.
3. An element a ∈ R (R is a ring) is said to be invertible if there exists b ∈ R such that a.b = b.a = 1.

Notations.

1. 0 is the identity element of the group (R, +).
2. 1 is the identity element of the semigroup (R, .) (if it exists).
3. –a is the inverse element of a in the group (R, +).
4. a^{-1} is the inverse element of a in (R, .) (if a^{-1} exists).

Remark. We will refer to (R, +, .) by only R.

Examples.

1. (ℤ, +, .) is a commutative ring with identity 1 for that:
   a. (ℤ, +) is an abelian group (**why?)**
   b. (ℤ, .) is a semigroup (**why?)**
   c. For all a, b, c ∈ R, :
      a.(b+c) = a.b + a.c

(b+c).a = b.a + c.a

∴ $\mathbb{Z}$ is ring

Now, for all a, b ∈ $\mathbb{Z}$, 1.a = a.1 = a

∴ $\mathbb{Z}$ is ring with identity and for all a, b ∈ $\mathbb{Z}$, a.b = b.a

∴ $\mathbb{Z}$ is commutative ring with identity.

2. $2\mathbb{Z}, 4\mathbb{Z}, \ldots, n\mathbb{Z} (n \neq 1)$ is a commutative ring with identity.
3. $4 \in 4\mathbb{Z}$ but $a^{-1} \notin 4\mathbb{Z}$ such that $4.a^{-1} = a^{-1}.4 = 1$.

   ∴ 4 has no inverse
4. ($\mathbb{C}$, +, .), ($\mathbb{R}$, +, .), ($\mathbb{Q}$, +, .) and (M_{22}, +, .) are rings (where M_{22} is the set of all 2x2 matrix).

Theorem. Let R be a ring, then for all a, b, c ∈ R :

1. If the identity element exists, the it is unique.

   If the inverse element a^{-1} (for all a ∈R) exists, then it is unique. .2
3. a.0 = 0.a = 0
4. a.(-b) = (-a) . b = - (a.b)
5. (-a).(-b) = a.b
6. a. (b - c) = a.b – a.c
7. (b – c) . a = b.a – c.a

Remarks.

1. A ring R is said to be trivial if R = {0}
2. A ring R is said to be nontrivial if R ≠ {0}
3. Let R be a ring with identity. If R is not trivial, then 1≠ 0.

   Proof. Since R≠ {0}, then if 1 = 0, ∃ 0 ≠ a ∈ R such that a = a.1 = a.0 = 0 c!

∴ 1≠0

4. If R is a ring, $n \in \mathbb{Z}^+$, $x \in R$, then:

   $nx = \underbrace{x + x + \ldots + x}_{n-times}$

   $(-n)x = \underbrace{(-x) + (-x) + \ldots + (-x)}_{n-times}$

$x^n = \underbrace{x \,.\, x \,.\, \ldots \,.\, x}_{n-times}$

Theorem. Let

$$R^* = \{a \in R \mid a \text{ has inverse}\}$$

be a set of all unite element of a ring R, then $(R^*, .)$ is a group

1. $R^* \neq \emptyset$ $(1 \in R^*)$.
2. If $a, b \in R^*$, then $\exists\ a^{-1}, b^{-1} \in R^*$ such that

$$a.a^{-1} = a^{-1}.a = 1 \text{ and } b.\,b^{-1} = b^{-1}.b = 1$$

also,

$$ab(b^{-1}\,a^{-1}) = a(b\,b^{-1})\,a^{-1} = a(1)\,a^{-1} = a\,a^{-1} = 1$$

$$b^{-1}\,a^{-1}(ab) = b^{-1}(\,a^{-1}\,a)b = b^{-1}\,(1)\,b = b^{-1}\,b = 1$$

$\therefore$ $b^{-1}\,a^{-1}$ is the inverse element of ab in R^*.

$$\therefore b^{-1}\,a^{-1} \in R^*$$

$\therefore$ R^* is closed under "."

3. $(R^*, .)$ is associative(prove that)

$$\therefore (R^*, .) \text{ is group}$$

Examples.

1. Let X be a nonempty set and P(X) denote the collection of all subset of X. then each of (P(X), ∪,∩) and (P(X), ∩,∪) is not ring (because neither (P(X), ∩) nor (P(X), ∪) form group(**prove that**?)).
2. Let X be a nonempty set and (R, +, .) be an arbitrary ring. Let map(X, R) be the set of all mapping from X into R

$$map(X, R) = \{f|\ f: X \to R\}$$

define for a ∈ X:

$$(f+g)\ (a) = f(a) + g(a)$$

$$(f.g)\ (a) = f(a)\ .\ g(a)$$

then, (map(X, R), +, .) is a ring with 1.

<u>Proof.</u>

a) map(X, R) = ∅ (∃ 0 : X→R such that 0(a) = 0 for all a ∈ R).
b) 0 is zero map (additive identity)
c) 1 is the constant map (if R has 1, then f(a) = 1 for all a ∈ R).
d) –f is the additive inverse map of (f +(-f)(x) = 0(x)

3. Let R = C[0,1] = {f: [0,1] → R| f is continuous} then (R, +, .) = (C[0, 1], +, .) is a ring.

<u>Proof.</u>

a) (R, +) is an abelian group (prove ?)
b) Distributive lows

$$\begin{aligned}[f.(g+h)]\ (x) &= [f.g + f.h](x)\\ &= (f.g)(x) + (f.h)(x)\\ &= f(x)\ g(x) + f(x)\ h(x)\\ &= g(x)f(x) + h(x).\ f(x)\\ &= [g.f + h.f](x)\\ &= [(g+h)f](x)\end{aligned}$$

∴ (R, +, .) is a ring

4. The ordered triple $(\mathbb{Z}_n, +_n, \cdot_n)$ forms a commutative ring with identity 1.

   Proof. for all $\bar{a}, \bar{b} \in \mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$

   Firstly, $\bar{a} +_n \bar{b}$ = [a]$+_n$[b]= [a+b] = $\overline{a+b}$

   $\bar{a} \cdot_n \bar{b}$ = [a]$\cdot_n$[b]= [a.b] = $\overline{a.b}$

   a) $(\mathbb{Z}_n, +_n)$ is an abelian group (prove?)
   b) $(\mathbb{Z}_n, \cdot_n)$ is a semigroup (prove?)
   c) $(\bar{a} \cdot_n (\bar{b} +_n \bar{c}))$ = ….= $\bar{a} \cdot_n \bar{b} +_n \bar{a} \cdot_n \bar{c}$

      also, $(\bar{b} +_n \bar{c}) \cdot_n \bar{a}$ = ….= $\bar{b} \cdot_n \bar{a} +_n \bar{c} \cdot_n \bar{a}$

For examples:

$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

$\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$

$\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

Definition. The ring $((R_1 \, x \, R_2), \oplus, \otimes)$ is said to be direct product to the two rings R_1 and R_2.

Remark. The ring R is commutative if and only if for all a ∈ R, $a = a^2$

Proof. ∵ a+b ∈ R , then

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

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

∴ ab + ba = 0 → ab = - ba = $(-ba)^2$ = ba

∴ ab = ba

∴ R is a commutative ring

Definition. Let R be a ring, then R is said to be ***Boolean*** ring if $x^2 = x$ for all x ∈ R.

Remark. Every Boolean ring is a commutative ring. but the **converse is not true** in general.

Homework. Give an example to show that the converse of the previous remark is not true in general

Definitions. Let R be a ring and a be element in R, then a is said to be:

1. **Idempotent** element if $a^2 = a$.
2. **Nilpotent** element if $a^n = 0$ for $n > 0$.
3. **Unite** element if $\exists$ b $\in$ R such that ab = ba = 1.

Examples.

1. In $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ the idempotent elements are only 1, 0.
2. In 2 $\mathbb{Z}$ the idempotent element is 0
3. In $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, the nilpotent element is 0.
4. In $\mathbb{Z}$, the unites elements are 1, -1
5. In $\mathbb{Q}, \mathbb{R}$ the unites elements are every nonzero element
6. $(P(X), \Delta, \cap)$ is a Boolean ring with identity $\emptyset$

SUBRINGS

Definition. (subring)

Let (R, + , .) be a ring and $\emptyset \neq S \subseteq R$. then (S, +, .) is said to be subring of R ($S \leq R$) if (S, +, .) is ring itself.

Remarks.

1. If $S \leq R$ such that R has 1, then it is not necessary that S has 1.

Example. ($2\mathbb{Z}$, +, .) is a subring of the ring of integers ($\mathbb{Z}$, +, .) and ($2\mathbb{Z}$, +, .) is a ring without identity although ($\mathbb{Z}$, +, .) has identity.

2. Both ring and one of its subrings possess identity but they are different.

   Example. the ring $(\mathbb{Z}_6, +_6, \cdot_6)$ has 1 but the subring $(\{\bar{0}, \bar{2}, \bar{4}\}, +_4, \cdot_4)$ of $(\mathbb{Z}_6, +_6, \cdot_6)$ of $\mathbb{Z}_6$has an identity $\bar{4}$.

3. Some subring has an identity, but the entire ring does not.

   Example. Th ring R = $\mathbb{Z}\ x\ 2\mathbb{Z}$ has no identity while the subring s = $\mathbb{Z}x\{0\}$ is a subring of R with identity (1,0).

Theorem. A nonempty subset (S, +,.) of a ring R is said to be subring if and only if:

1. a-b ∈ S
2. a.b ∈ S

   for all a,b, ∈ S

example. The $\mathbb{Z}_e$ forms a subring of integer ring . for that

$2n – 2m = 2(n\text{-}m) \in \mathbb{Z}e$

$2n.2m= 4(n.m) = 2(2n.m) = 2(2nm) \in \mathbb{Z}_e$

Examples.

1. If R = ($\mathbb{Z}$, +, .) and H_n= ($n\mathbb{Z}$, +, .), then H_n is a subring of R ($H_n \leq$ R) for all n ∈ $\mathbb{Z}^+$.
2. If R = ($\mathbb{R}$, +, .), then $\mathbb{Q}\sqrt{p},\ \mathbb{Z}\sqrt{p}, \mathbb{Z}, \mathbb{Q},\ H_n$ are subrings of the ring R with the same binary operations "+" and "."(p prime number).
3. For each ring R, there are two trivial subrings R and {0}.
4. $2\mathbb{Z}_6$ is a subring of $\mathbb{Z}_6$($2\mathbb{Z}_6\ \leq\ \mathbb{Z}_6$) and $n\mathbb{Z}_6\ \leq\ \mathbb{Z}_6$.
5. Each of

$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z} \right\}$ and $T = \left\{ \begin{pmatrix} n & 0 \\ m & l \end{pmatrix} \middle| \, n, m, l \in \mathbb{Z} \right\}$ subring of

$M_2(\mathbb{Z}) = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} \middle| \, x, y, z, w \in \mathbb{Z} \right\}$ where

$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix}$.

Theorem. If S_1, S_2 are subrings of R, then so is $S_1 \cap S_2$.

Proof. Suppose S_1 and S_2 are subrings of R. then $0 \in S_1 \wedge 0 \in S_2$, then $S_1 \cap S_2 \neq \emptyset$.

Now, for all $x, y \in S_1 \cap S_2 \rightarrow x, y \in S_1 \wedge x, y \in S_2$

1. $x - y \in S_1 \wedge x - y \in S_2 \rightarrow x - y \in S_1 \cap S_2$
2. $x.y \in S_1 \wedge x.y \in S_2 \rightarrow x . y \in S_1 \cap S_2$

$\therefore S_1 \cap S_2$ is a subring of R

Remark. If S_1, S_2 are subrings of R, then not necessary $S_1 \cup S_2$ is a subring of R.

Example. $2\mathbb{Z}$, $3\mathbb{Z}$ subring of $\mathbb{Z}$ while $2\mathbb{Z} \cup 3\mathbb{Z} \nleq \mathbb{Z}$ since $3, 2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$ while $3-2 = 1 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.

Definition. Let R be a ring . A set

$$\text{center } R = \{x \in R \mid xr = rx, \forall r \in R\}$$

is said to be center of the ring R.

Remarks.

1. Cent(R) $\neq \emptyset$.
2. A ring R is commutative iff cent(R) = R.
3. Cent(R) is a subring of R.

Proof. H.W

Definition. let R be a ring and a ∈ R. the set

$$C(a) = \{w \in R \mid wa = aw\}$$

Is called the centralizer of x.

Remarks.

1. $C(a) \neq \emptyset$ ($a.a=a.a \to a \in C(a)$).
2. C(a) is a subring of R.
3. $Cent(R) = \bigcap_{a \in R} C(a)$

Proof. 1. H.W.

Proof 2.

a. $C(a) \neq \emptyset$ and C(a) subset of R.
b. Let x, y ∈ C(a), then xa = ax and ya = ay.

Then $(x-y)(a) = xa-ya = ax-ay = a(x - y) \to x-y \in C(a)$

$(xy)(a) = x(ya) = x(ay) = (xa)y = (ax)y = a(xy) \to xy \in C(a)$

∴ C(a) is a subring of R

Examples.

1. $Cent(\mathbb{Z}_4) = \mathbb{Z}_4$
2. $Cent(\mathbb{Z}_n) = \mathbb{Z}_n$
3. $Cent(\mathbb{Z}) = \mathbb{Z}$

∴ the ring $\mathbb{Z}_n$ and $\mathbb{Z}$ are commutative

H.W. find $Cent(M_{22}(\mathbb{Z}))$?