Theorem

let $(R,+,.)$ be a ring and let $(A,+,.)$, $(B,+,.)$ be two subrings of $(R,+,.)$. Then $(A\cap B,+,.)$ is a subring.

Proof

$0\in A$ and $0\in B$ (since A, B are subrings of R)

$\Rightarrow 0\in A\cap B$, implies that $A\cap B\neq\emptyset$.

let $a,b\in A\cap B$, implies $a,b\in A$ and $a,b\in B$

Thus $a\in A$ and $b\in A \Rightarrow a-b\in A$ and $a.b\in A$ (since A is subring of R) $\rightarrow$ ①

or $a,b\in B \Rightarrow a-b\in B$ and $a.b\in B$ (since B is a subring of R) $\rightarrow$ ②

From ① and ②, we get $a-b\in A\cap B$ and $a.b\in A\cap B$

Thus $A\cap B$ is a subring of $(R,+,.)$

- As a generalization of above theorem, we have

The intersection of any family $\{A_i\}_{i\in\Lambda}$, Λ is any index set of subring of a ring $(R,+,.)$ is a subring of $(R,+,.)$.

Remark

The union of two subrings of a ring $(R,+,.)$ need not be subring of R.

For example: Consider the ring $(\mathbb{Z},+,.)$ and the subrings $A=\{0,\mp2,\mp4,\dots\}$, $B=\{0,\mp3,\mp6,\mp9\dots\}$

$A\cup B=\{0,\mp2,\mp3,\mp4,\mp6,\dots\}$

Since $2 \in A \cup B$, $3 \in A \cup B$ but $3 - 2 = 1 \notin A \cup B$.
Thus $A \cup B$ is not subring.

Definition

let $(R, +, \cdot)$ be a ring, the set $\{x : x \in R \wedge x \cdot y = y \cdot x \quad \forall y \in R\}$ is called the center of R and denoted by Cent(R)

Remarks:

(1) If R is Comm. ring, then Cent(R) = R.

(2) Cent(R) is a subring of $(R, +, \cdot)$

Proof:

let $x_1, x_2 \in$ Cent(R)

1. $x_1 \cdot y = y \cdot x_1 \quad \forall y \in R \longrightarrow ①$
2. $x_2 \cdot y = y \cdot x_2 \quad \forall y \in R \longrightarrow ②$

Now, $\forall y \in R$ by ① and ② we get

$$(x_1 - x_2) \cdot y = x_1 y - x_2 y = y \cdot x_1 - y \cdot x_2 = y \cdot (x_1 - x_2)$$

$\therefore x_1 - x_2 \in$ Cent(R)

Similarly $x_1, x_2 \in$ Cent(R)

$$(x_1 \cdot x_2) \cdot y = x_1 \cdot (x_2 y) = x_1 \cdot (y x_2) = (x_1 y) \cdot x_2$$

$$= (y \cdot x_1) \cdot x_2 = y \cdot (x_1 x_2)$$

$\therefore x_1 x_2 \in$ Cent(R)

$\therefore$ Cent(R) is a subring of $(R, +, \cdot)$

Definition :

let $(R,+,\cdot)$ be a ring and let $a\in R$, $n\in Z_+$.

Then :

1. $na = a+a+\cdots+a$ (n-times)
2. $(-n)a = (-a)+(-a)+\cdots+(-a)$ (n-times)
3. $a^n = a\cdot a\cdot\cdots\cdot a$ (n-times)
4. If R has unity and a has multiplicative inverse a^{-1}, then $a^{-n} = a^{-1}\cdot a^{-1},\cdots,a^{-1}$

Example :

Consider the ring $(Z_8, +_8, \cdot_8)$

Fined $(2)\cdot\bar{3}$, $(-2)\cdot\bar{3}$, 7^{-2}

solution :

1. $(2)\bar{3} = \bar{3} +_8 \bar{3} = \bar{6}$

2. $(-2)\cdot\bar{3} = (-\bar{3})+(-\bar{3}) = \bar{5}+\bar{5} = \bar{2}$

3. $7^{-2} = (7^{-1})^2 = (\bar{7})^2 = \bar{7} \cdot_8 \bar{7} = \bar{1}$

Theorem :

let $(R,+,\cdot)$ be a ring. Then for $a,b\in R$ and arbitary integers m and n, the following hold

1. $(n+m)a = na+ma$
2. $(nm)a = n(ma)$
3. $n(a+b) = na+nb$
4. $n(a\cdot b) = (na)\cdot b = a\cdot(nb)$
5. $(na)\cdot(mb) = (nm)(a\cdot b)$

Proof :- 1

Case (i) $n\in Z_+$, $m\in Z_+$

$$na + ma = \underbrace{(a + a + \cdots + a)}_{n\text{ times}} + \underbrace{(a + a + \cdots + a)}_{m\text{ times}}$$

$$= \underbrace{a + a + a + \cdots + a + \cdots + a}_{(n+m)\text{ times}}$$

$$= (n+m)a$$

Case(ii): $n \in \mathbb{Z}, m = 0$

$$na + ma = na + 0.a = na = (n+0)a = (n+m)a$$

Case(iii): $n \in \mathbb{Z}_-, m \in \mathbb{Z}_-$ H.w.

Case(IV): $n \in \mathbb{Z}_+, m \in \mathbb{Z}_-$ H.w

Definition: مطلوب

Let $(R, +, \cdot)$ be a ring, if there exists a positive n s.t. $na = 0 \ \forall a \in R$, then the least positive integer with this property is Called characteristic of R (simply $ch(R)$).

If no such positive integer exists, implies $ch(R) = 0$

Examples:

1. Consider $(\mathbb{Z}, +, \cdot)$

$\forall a \in \mathbb{Z}$, only $na = \overset{\text{لازم}}{0}$, then $n = \overset{\text{لازم}}{0}$

$\therefore ch(\mathbb{Z}) = 0$

2. Each ring $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_e, +, \cdot)$

has chara. Zero.

3. Consider $(M_2(\mathbb{R}), +, \cdot)$

let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$

$\forall n \in \mathbb{Z}_+$; $nA = \begin{pmatrix} na & nb \\ nc & nd \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

if $A \neq 0_{2\times 2}$, then $ch(M_2(\mathbb{R})) = 0$

(4) Consider $(\mathbb{Z}_3, +_3, \cdot_3)$

$(3)\bar{1} = \bar{1} +_3 \bar{1} +_3 \bar{1} = \bar{0}$

$(3)\bar{2} = \bar{2} +_3 \bar{2} +_3 \bar{2} = \bar{0}$

$\therefore ch(\mathbb{Z}_3) = 3$

(4) let $X \neq \emptyset$, Consider $(P(X), \Delta, \cap)$
Zero element of this ring is $\emptyset$
let $A \in P(X)$
(1) $A = A \Delta A = \emptyset$
since $A \Delta A = (A/A) \cup (A/A) = \emptyset \cup \emptyset = \emptyset$ = Zero element

$\therefore ch(P(X), \Delta, \cap) = 2$

* problem: Prove or disprove
Let R be a ring and let S be a subring of R.

Then:
1. $ch(R) = ch(S)$
2. $ch(R) \neq ch(S)$

$ch(\mathbb{Z}_6) = 6$
but $A = \{\bar{0}, \bar{2}, \bar{4}\}$
The identity element of A is $\bar{4}$
Then $ch(A) = 3$
Since, $\bar{4} +_6 \bar{4} +_6 \bar{4} = \bar{0}$

Class