

Theorem: If a ring has a unity then it is unique.

Pf: ~~of the ring has no~~

Let R be a ring with unity or identity. Suppose both e and e' are identities of R . Then

$$ae = a \text{ for all } a \in R \quad \text{--- (I)}$$

$$\text{and } e'a = a \text{ for all } a \in R \quad \text{--- (II)}$$

Taking $a = e'$ in (I) we get

$$e'e = e'$$

Taking $a = e$ in (II) we get

$$e'e = e$$

Thus both e' and e are equal to $e'e$ and so they are equal to each other. Hence $e = e'$.

Theorem: If a ring element has an inverse then it is unique.

pf: Let a be an element of a ring R and ~~a has~~ let inverse of a exist.

To show inverse of a is unique.

Suppose b and c are two inverses of a . Then

$$ab = e \quad \text{and} \quad ac = e, \text{ where } e \text{ is the identity element of } R$$

$$\therefore ab = ac$$

$$\Rightarrow a^{-1}(ab) = a^{-1}(ac)$$

$$\Rightarrow (a^{-1}a)b = (a^{-1}a)c$$

$$\Rightarrow eb = ec$$

$$\Rightarrow b = c$$

Hence a ~~has~~ ^{has} unique inverse.

Subring: Defn.

A subset S of a ring R is a subring of R if S is itself a ring with the operations of R .

Theorem (Subring Test)

A nonempty subset S of a ring R is a subring iff S is closed under subtraction and multiplication i.e. iff $a-b$ and ab are in S whenever a and b are in S .

Pf: Let S be a subring of R and let $a, b \in S$.
Then by definition of subring S itself
~~a ring~~. ~~So $a+b \in S$ and $ab \in S$.~~

a ring ~~with~~ under addition and multiplication. So $a+b \in S$ and $ab \in S$.

Also S is a ring so $\langle S, + \rangle$ is an additive abelian group. So for $b \in S$,
 $\exists -b \in S$ s.t. $b + (-b) = 0$; 0 is the additive identity of S .
 $\therefore a - b = a + (-b) \in S$.

Conversely let S be such that for all $a, b \in S$,
 $a-b \in S$ and $ab \in S$.

Now $a-b \in S$, $\forall a, b \in S$.

$\Rightarrow S$ is a subgroup of $\langle R, + \rangle$.

Thus S is closed under the addition composition in R and is an abelian group under the induced addition.

Also $ab \in S \quad \forall a, b \in S$.

Since all the elements of S are also elements of R so associativity, ^{N.B. multiplication} and distributivity hold in S since they hold in R . Hence S is a ring.

$\Rightarrow S$ is a subring of R .

Ex. $\{0\}$ and R are subrings of any ring R . $\{0\}$ is called trivial subring of R .

Pf. Let $S = \{0\}$. S contains only one element which is 0.

Since $0 - 0 = 0 \in S$ and $0 \cdot 0 = 0 \in S$

$\therefore S$ is a ~~subring of R~~ subring of R $[\because a \cdot 0 = 0, \forall a \in R]$
 $\Rightarrow \{0\}$ is a subring of R

Next let $S = R$. Let $a, b \in S = R$.

Since $S = R$ is a ring so $\langle S, + \rangle = \langle R, + \rangle$ is an additive abelian group. So $S = R$ is a subgroup of itself. By subgroup test for $a, b \in S = R$, $a - b \in S = R$.

Also $S = R$ is closed under multiplication so for $a, b \in S = R$, $ab \in S = R$.

$\therefore S = R$ is a subring of R .

Ex: $\{0, 2, 4\}$ is a subring of the ring $\mathbb{Z}_6$, the integers modulo 6.

Soln: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, let $S = \{0, 2, 4\}$

$+$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

$\times$	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

clearly S is closed under addition and multiplication modulo 6. i.e. if $a, b \in S$ then $a \times b \in S$.

From the 1st table it is clear that 0 is the additive identity element. Also additive inverses of 0, 2 and 4 are 0, 4 and 2 respectively. Since all the elements of S are also elements of R and R is a ring so S is associative under addition as $\langle R, + \rangle$ is an additive group which implies R is associative under addition.

Thus $\langle S, +_6 \rangle$ is a group. Hence S is a subgroup of itself. So by subgroup test for $a, b \in S$, $a - b \in S$.

$\Rightarrow S$ is a subring of R

ie. $\{0, 2, 4\}$ is a subring of Z_6 .

Ex. The set of Gaussian integers $Z[i] = \{a + bi \mid a, b \in Z\}$ is a subring of the complex numbers C .

Soln. $Z[i] = \{a + bi \mid a, b \in Z\}$.
clearly $Z[i] \subseteq C$.

Let $x = a + bi$, $y = c + di \in Z[i]$,
 $a, b, c, d \in Z$.

Then $x \bar{y} = (a + bi) \overline{(c + di)} = (a - bi)(c + di) = (ac - bd) + (ad + bc)i$
 $\in Z[i]$ since $ac - bd, ad + bc \in Z$.

And $xy = (a + bi)(c + di) = (ac - bd) + (ad + bc)i \in Z[i]$
since $ac - bd, ad + bc \in Z$.

$\therefore Z[i]$ is a subring of C .

Ex: Let R be the ring of all real-valued functions of a single real variable under pointwise addition and multiplication. The subsets S of R of functions whose graphs pass through the origin forms a subring of R .

Soln: $R = \{ f \mid f: \mathbb{R} \rightarrow \mathbb{R} \}$

for $f, g \in R$

$$(f+g)(x) = f(x) + g(x), \quad \forall x \in \mathbb{R}$$

$$(fg)(x) = f(x)g(x).$$

$$S = \{ f \mid f: \mathbb{R} \rightarrow \mathbb{R} \text{ and } f(0) = 0 \}.$$

To show S is a subring of R .

Let $f, g \in S$. Then f, g are real valued functions of a single real variable and $f(0) = 0$ and $g(0) = 0$.

~~Now~~ $(f+g)(0) = f(0) + g(0) = 0 + 0 = 0$

and $(fg)(0) = f(0) \cdot g(0) = 0 \cdot 0 = 0.$

clearly $f+g, fg$ ~~are~~ functions from $\mathbb{R}$ to $\mathbb{R}$. Hence $f+g, fg \in S$

$\Rightarrow S$ is closed under pointwise addition and multiplication of functions.

Also $g \in S \Rightarrow g \in R$ i.e. g is a real valued function. $\Rightarrow (-1)g = -g$ is also a real valued function and

$$\Leftrightarrow (-g)(0) = ((-1)g)(0) = (-1)g(0) = (-1) \cdot 0 = 0.$$

$$\Rightarrow -g \in S.$$

Thus $f, g \in S \Rightarrow f, -g \in S$

$$\therefore f + (-g) = f - g \in S. \quad [\because S \text{ is closed under addition}]$$

Thus $f, g \in S \Rightarrow f + g \in S$ and $f - g \in S$

Hence S is a subring of R .

Ex. The set $\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ of diagonal matrices is a subring of the ring of all 2×2 matrices over $\mathbb{Z}$.

Sol. Let $R = \left\{ \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \mid a_1, b_1, c_1, d_1 \in \mathbb{Z} \right\}$

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$$

clearly $S \subseteq R$.

Let $x = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $y = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in S$
where $a, b, c, d \in \mathbb{Z}$.

Then $x - y = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} - \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$

$$= \begin{bmatrix} a - c & 0 - 0 \\ 0 - 0 & b - d \end{bmatrix}$$

$$= \begin{bmatrix} a - c & 0 \\ 0 & b - d \end{bmatrix} \in S$$

Since $a, b, c, d \in \mathbb{Z} \Rightarrow a - c, b - d \in \mathbb{Z}$

Also $xy = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$

$$= \begin{bmatrix} ac + 0 & 0 + 0 \\ 0 + 0 & 0 + bd \end{bmatrix}$$

$$= \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in S$$

$\therefore a, b, c, d \in \mathbb{Z} \Rightarrow ac, bd \in \mathbb{Z}$

Hence S is a subring of R