Subrings:

A non-empty subset of a ring R is called a subring of R if it is a ring under induced operations from the whole ring R.

For example:-

(i) Any ring R has atleast two subrings R and $\{0\}$.

(ii) $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ is a subring of $(\mathbb{R}, +, \cdot)$

(iii) $(2\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{Z}, +, \cdot)$

(iv) $(m\mathbb{Z}, +, \cdot)$ where m is any integer is a subring of $(\mathbb{Z}, +, \cdot)$

Results:

① Let $(R, +, \cdot)$ be a ring. A non-empty subset S of R forms a subring of R iff

(i) $(S, +)$ is a subgroup of the group $(R, +)$;

(ii) S is closed under multiplication.

Proof:- Let S be a ring of R. Then both the conditions (i) and (ii) are satisfied.

Conversely, let the condition (i) and (ii) be satisfied in S.

Since (i) holds, $(S, +)$ is a commutative group

Since (ii) holds, S is closed under multiplication.

We need only to verify that multiplication is associative on S and the distributive laws holds in S.

But these are hereditary properties and since they hold in R, they hold in the subset S.

Therefore S is a subring.

② A non-empty subset S of a ring R is a subring of R iff

(i) $a - b \in S$, $\forall\ a, b \in S$.

(ii) $a \cdot b \in S$, $\forall\ a, b \in S$.

Proof: Let S be a subring of R and let $a \in S$, $b \in S$. Since S is a ring, $a \in S, b \in S$.

$\Rightarrow a \in S, -b \in S$

$\Rightarrow a + (-b) \in S$

$\Rightarrow a - b \in S$

Also, $a \in S, b \in S \Rightarrow a.b \in S$, since S is a ring.

Therefore both the conditions hold.

Conversely, let a non-empty subset S of R be such that both the conditions holds.

Using (i), $a \in S, a \in S \Rightarrow a - a \in S$ i.e $0 \in S$.

and $0 \in S, a \in S \Rightarrow 0 - a \in S$, i.e $-a \in S$.

Also $a \in S, b \in S \Rightarrow a \in S, -b \in S \Rightarrow a - (-b) \in S$

$\Rightarrow a + b \in S$.

Thus S is closed under addition (+), the additive identity element belongs to S and the additive inverse of each element in S belongs to S.

Since addition is associative and commutative on R and S is a subset of R, so addition is associative and commutative on S.

Thus (S, +) is by itself a commutative group and therefore (S, +) is a sub-group of the group (R, +)

By (ii) S is closed under multiplication.

Therefore, S is a subring of R.