element belongs to S and the additive inverse of each element a in S belongs to S. Since addition is commutative and associative in R and S is a subset of R, addition is commutative and associative in S.

So, $(S,+)$ is by itself a commutative group.

So, $(S,+)$ is a subgroup of $(R,+)$

Again by (ii) S is closed under multiplication.

So, S is a subring of R by Theorem 2.1.3.

Theorem 2.1.5 Let S and T be two subrings of a ring R.

Then $S \cap T$ is a subring of R.

Proof: $S \cap T$ is non-empty subset of R as $0 \in S \cap T$

Let $p, q \in S \cap T \Rightarrow p, q \in S$ and $p, q \in T$

$\Rightarrow p-q \in S$ and $p \cdot q \in S$ as S is a subring of R

and $p-q \in T$ and $p \cdot q \in T$ as T is a subring

of R. So, $p-q \in S \cap T$ and $p \cdot q \in S \cap T$

Hence $S \cap T$ is a subring of R by Theorem 2.1.4.

Note 2.1.6 Union of two subrings may not be a subring of R.

For example, $(2\mathbb{Z}, +, \cdot)$ and $(3\mathbb{Z}, +, \cdot)$ are subrings of the ring $(\mathbb{Z}, +, \cdot)$ but $2\mathbb{Z} \cup 3\mathbb{Z}$ is not a subring of $(\mathbb{Z}, +, \cdot)$

Examples 2.1.7 (continued): 4. Subrings of the ring $(\mathbb{Z}, +, \cdot)$

Let $(S, +, \cdot)$ be a subring of the ring $(\mathbb{Z}, +, \cdot)$. Then $(S,+)$ must be a subgroup of the group $(\mathbb{Z}, +)$.

But all subgroups of the group $(\mathbb{Z}, +)$ are the groups $(m\mathbb{Z}, +)$ where m is an integer. Let us examine if $(m\mathbb{Z}, +, \cdot)$ is a subring of the ring $(\mathbb{Z}, +, \cdot)$

Case I $m = 0$ In this case $m\mathbb{Z} = \{0\}$ is the trivial subring

Case 2 $n \neq 0$, $n\mathbb{Z}$ is a non-empty subset of $\mathbb{Z}$ as $0 \in \mathbb{Z}$.
Let $a, b \in n\mathbb{Z}$ Then $a-b \in n\mathbb{Z}$ and $a.b \in n\mathbb{Z}$
So, $(n\mathbb{Z}, +, \cdot)$ is a subring of the ring $\mathbb{Z}$
Thus all the subrings of the ring $(\mathbb{Z}, +, \cdot)$ are $(n\mathbb{Z}, +, \cdot)$ where $n$ is an integer
(Note: Since the rings $(n\mathbb{Z}, +, \cdot)$ and $(-n\mathbb{Z}, +, \cdot)$ are identical, the totality of the subrings of the ring $(\mathbb{Z}, +, \cdot)$ can also be expressed as $(n\mathbb{Z}, +, \cdot)$ where $n$ is a non-negative integer.)

6. Subrings of the ring $\mathbb{Z}_n$. Let $(S, +, \cdot)$ be a subring of the ring $\mathbb{Z}_n$. Then the subgroup $(S, +)$ must be a subgroup of $(\mathbb{Z}_n, +)$. As the group $(\mathbb{Z}_n, +)$ is cyclic, all its subgroups are cyclic.

If $n$ be prime, $(\mathbb{Z}_n, +)$ has only two subgroups - the trivial subgroup $\{\bar{0}\}$ and the improper subgroup $(\mathbb{Z}_n, +)$
These are clearly the subrings of the ring $\mathbb{Z}_n$
Let $n$ be a composite number. For every divisor $d$ of $n$, there is one and only one subgroup of $(\mathbb{Z}_n, +)$ of order $d$. Let $m$ be a divisor (other than $n$) of $n$. Let $n = am$
Then $\bar{a} \in \mathbb{Z}_n$ and $\bar{a}$ generates a cyclic subgroup of order $m$. The elements of the subgroup are $\bar{a}, 2\bar{a}, \cdots, (m-1)\bar{a}$.
We prove that $S = \{\bar{a}, 2\bar{a}, \cdots, (m-1)\bar{a}\}$ is a subring of $\mathbb{Z}_n$.
$(S, +)$ is a subgroup of the group $(\mathbb{Z}_n, +)$
Let $x, y \in S$ Then $x = p\bar{a}$, $y = q\bar{a}$ for some integers $p, q$ satisfying $1 \leq p < m$, $1 \leq q < m$. Let $pqa = \lambda m + \mu$ where $\lambda$ and $\mu$ are integers with $0 \leq \mu < m$

Then $pqa^k = \lambda n + \mu a$, $0 \le \mu a < n$. This shows that $x.y \in S$

Consequently, $(S, +, \cdot)$ is a subring of the ring $\mathbb{Z}_n$

Some particular cases:

(1) Let $n = 6$, $S = \{\bar{2}, \bar{4}, \bar{0}\} \subset \mathbb{Z}_6$.

$(S, +)$ is a subgroup of the group $(\mathbb{Z}_6, +)$. The multiplication table

| $\cdot$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |
|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |

shows that the set $S$ is closed under multiplication. So, $S$ is a subring of $\mathbb{Z}_6$. $\bar{4}$ is the unity element in the subring, while $\bar{1}$ is the unity in $\mathbb{Z}_6$. Every non-zero element in the subring is a unit

Theorem 2.1.8 Let $\{S_\alpha : \alpha \in I\}$ be a collection of subrings of a ring $R$. Then $S = \bigcap_{\alpha \in I} S_\alpha$ is a subring of $R$.

Proof: For each $\alpha \in I$, $0 \in S_\alpha$. So $0 \in S$ and $S$ is non-empty. Now let $a, b \in S$. Then $a, b \in S_\alpha$ for each $\alpha \in I$. Since $S_\alpha$ is a subring, $a - b, ab \in S_\alpha$. So, $a - b, ab \in S$. So, $S$ is a subring of $R$ by Theorem 2.1.4

Definition 2.1.9 Let $R$ be a ring. Define

$$C(R) = \{a \in R : xa = ax \text{ for all } x \in R\}$$

$C(R)$ is called the centre of $R$.

Note that $C(R) = R$ if and only if $R$ is commutative.

Theorem 2.1.9 The centre of a ring $R$ is a subring of $R$.

Proof: We have $C(R) \neq \phi$ as $0 \in C(R)$. Let $a, b \in C(R)$

Then $xa = ax$ and $xb = bx$ for all $x \in R$. This implies

$x(a - b) = (a - b)x$ for all $x \in R$. So, $a - b \in C(R)$.

Moreover $xab = axb = abx$ for all $x \in R$. So, $ab \in C(R)$

So, $C(R)$ is a subring of $R$ by Theorem 2.1.4.

**Definition 2.1.10 (Subfield).** A non-empty set $K$ of a field $F$ is said to be a subfield of $F$ if the elements of $K$ form a field with respect to the binary operations on $F$ restricted to $K$.

**Theorem 2.1.11** Let $S$ be a subset of a field $F$. Then $S$ is a subfield of $F$ if and only if $S$ satisfies the following conditions

(i) $o(S) \geq 2$

(ii) $a - b \in S$ for all $a, b \in S$

(iii) $ab^{-1} \in S$ for all $a \in S$ and $b \in S - \{0\}$

**Proof:** Let $S$ be a subfield of $F$. Then $S$ is a subring of $F$ and so, $S$ is non-empty and satisfies (ii). Then $0 \in S$. Also by definition $1 \in S$ and $0 \neq 1$. So, $o(S) \geq 2$

Now Since $S$ is a subfield of $F$, for any $b \in S - \{0\}$, we have $b^{-1} \in S$, So, for any $a \in S$, $ab^{-1} \in S$ as $S$ is a subring of $F$ which implies (iii).

Conversely, let $S$ be a subset of $F$ which satisfies (i), (ii) and (iii). By (i) $S$ is non-empty and $\exists$ a non-zero element, say $a$ in $S$. Then by (iii) $aa^{-1} = 1 \in S$. Now let $a, b \in S$ so that $b \neq 0$. Then $b^{-1} = 1b^{-1} \in S$ and so $ab = a(b^{-1})^{-1} \in S$ by (iii) Also for any $a, b \in S$, $a - b \in S$ by (ii). So, $S$ is a subring of $F$, $1 \in S$ and for any $b \in S - \{0\}$, $b^{-1} \in S$. So, $S$ is a subfield of $F$.

**Theorem 2.1.12** Let $\{S_\alpha : \alpha \in I\}$ be a collection of subfield of a field $F$. Then $S = \bigcap_{\alpha \in I} S_\alpha$ is also a subfield of $F$.