Proof: By Theorem 2.1.8, we have that S is a subring. Now since $1 \in S_\alpha$ for each $\alpha \in I$, we have $1 \in S$. Let $b \in S$ so that $b \neq 0$. Then $b \in S_\alpha - \{0\}$, so $b^{-1} \in S_\alpha$ for all $\alpha \in I$. Thus $b^{-1} \in S$. Hence S is a subfield of F.

Examples: 1. $(\mathbb{R}, +, \cdot)$ is a field and $(\mathbb{Q}, +, \cdot)$ is a field. So, $(\mathbb{Q}, +, \cdot)$ is a subfield of $(\mathbb{R}, +, \cdot)$.

2. Let $\mathbb{Q}[\sqrt{2}]$ be the subset of $\mathbb{R}$ defined by $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$

Then $o(\mathbb{Q}[\sqrt{2}]) \geq 2$ as $0, 1 \in \mathbb{Q}[\sqrt{2}]$

Let $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Then $a, b, c, d \in \mathbb{Q}$

$$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \quad \ldots (i)$$

Let $p + q\sqrt{2}$ be a non-zero element of $\mathbb{Q}[\sqrt{2}]$. Then $(p, q) \neq (0, 0)$, $(p + q\sqrt{2})^{-1} = \frac{p}{p^2 - 2q^2} + \frac{-q\sqrt{2}}{p^2 - 2q^2} \in \mathbb{Q}[\sqrt{2}]$, since $p^2 - 2q^2 \neq 0$ for rational p, q when $(p, q) \neq (0, 0)$ and

$\frac{p}{p^2 - 2q^2} \in \mathbb{Q}$, $\frac{-q}{p^2 - 2q^2} \in \mathbb{Q}$.

$$(a + b\sqrt{2})(p + \sqrt{2})^{-1} = \frac{ap - 2bq}{p^2 - 2q^2} + \frac{bp - aq}{p^2 - 2q^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \quad \ldots (ii)$$

From (i) & (ii) it follows that $\mathbb{Q}[\sqrt{2}]$ is a subfield of $\mathbb{R}$.

Worked out Exercises 2.1.12

1. Suppose in a ring R, $e \in R$ is idempotent. Show that $eRe = \{exe : x \in R\}$ is a subring of R with unity e.

Solution: We have $e^2 = e$. Then $e = eee \in eRe$ So, $eRe \neq \phi$

Let $x, y \in eRe$. Then $x = ere$, $y = ese$ for some $r, s \in R$. Now $x - y = ere - ese = e(r - s)e \in eRe$ as $r - s \in R$ and $xy = ereese$ $= erese \in eRe$ as $rs \in R$. So, eRe is a subring of R.

Also $ex = e \cdot ere = ere = x$. Similarly $xe = x$ So, e is the unity in eRe.

2. Let $S = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$ where $\bar{n}$ denotes the equivalence class of n modulo 10. Prove that S is a subring of $\mathbb{Z}_{10}$ with the usual operations of $\mathbb{Z}_{10}$. Also show that S has a multiplicative identity which is different from that of $\mathbb{Z}_{10}$.

Solution: Let $\bar{i}, \bar{j} \in S$. Then i, j are even. Let $\bar{k} = \bar{i} - \bar{j}$ and $\bar{n} = \bar{i}\bar{j}$ where $0 \le k, n < 10$. Then $i - j \equiv k \pmod{10}$ and $ij \equiv n \pmod{10}$, that is, $i - j = k + 10k_1$, $ij = n + 10k_2$ for some integers k_1, k_2. This implies that k and n are both even. Hence $\bar{i} - \bar{j}, \bar{i}\bar{j} \in S$ and so, S is a subring of $\mathbb{Z}_{10}$.

3. Show that the field $(\mathbb{Q}, +, \cdot)$ has no proper subfield.

Solution: Let S be a subfield of $\mathbb{Q}$. Then $1 \in S$. Since S is a subring, we also have $-1 \in S$. Let $x \in \mathbb{Q}$. Then $\exists\ p, q \in \mathbb{Z}$ and $q > 0$ such that $x = \frac{p}{q}$, now if $p = 0$, then $x = 0$ and $0 \in S$, as S is a subring. If $p > 0$ then $p = 1 + 1 + \cdots + 1$ (p times) and so $p \in S$, Again, if $p < 0$ then $p = (-1) + (-1) + \cdots + (-1)$ ($|p|$ times). So, $p \in S$. Similarly $q \in S$ and since S is a subfield, $\frac{1}{q} \in S$ But $\frac{1}{q} = \frac{1}{q}$ in $\mathbb{Q}$. Then $p, \frac{1}{q} \in S$. So, $x = \frac{p}{q} = p\frac{1}{q} \in S$. So, $\mathbb{Q} \subseteq S$. Hence $S = \mathbb{Q}$ which implies that $\mathbb{Q}$ has no proper subfield.

4. Let $\omega \neq 1$ be a root of $x^3 = 1$. Prove that $T = \{a + b\omega \in \mathbb{C} : a, b \in \mathbb{Q}\}$ where $\mathbb{C}$ is the field of complex numbers, is a subfield of $\mathbb{C}$

Solution: We first note that $0 = 0 + 0\omega \in T$ and $1 = 1 + 0\omega \in T$. Then $o(T) \ge 2$ Next let $x, y \in T$. Then $x = a + b\omega$ and $y = c + d\omega$ for some $a, b, c, d \in \mathbb{Q}$. So,

$x-y = (a-c)+(b-d)\omega \in T$. Finally for $y \neq 0$,

$$xy^{-1} = (a+b\omega)(c+d\omega)^{-1}$$

$$= \frac{a+b\omega}{c+d\omega} = \frac{(a+b\omega)(c+d\omega^2)}{(c+d\omega)(c+d\omega^2)} = \frac{ac+bc\omega+ad\omega^2+bd}{c^2+cd(\omega^2+\omega)+d^2}$$

$$= \frac{ac+bd-ad+(bc-ad)\omega}{c^2-cd+d^2} = \frac{ac+bd-ad}{c^2-cd+d^2} + \frac{bc-ad}{c^2-cd+d^2}\omega \in T$$

Note that $c+d\omega \neq 0$, $c+d\omega^2 = \overline{c+d\omega} \neq 0$ and hence $c-cd+d^2 = (c+d\omega)(c+d\omega^2) \neq 0$. So, by Theorem 2.1.11, T is a subfield of $\mathbb{C}$.

3.1 Ideals of a ring

Definition 3.1.1 A subring S of ring R is said to be

(i) a left ideal of R if $a \in S, r \in R \Rightarrow r.a \in S$;

(ii) a right ideal of R if $a \in S, r \in R \Rightarrow a.r \in S$;

(iii) a both sided ideal (or an ideal) of R if $a \in S, r \in R \Rightarrow r.a \in S$ and $a.r \in S$.

Let R be a ring. Then the improper subring R is an ideal of R. This ideal is called the improper ideal of R. All other ideals are called proper ideals of R.

The subring $\{0\}$ is also an ideal of R. This is called the trivial ideal of R or the null ideal of R.

Theorem 3.1.2 A non-empty subset S of a ring $(R, +, \cdot)$ is an ideal of R if and only if

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

(ii) $a \in S, r \in R \Rightarrow r.a \in S$ and $a.r \in S$

Proof: Let S be an ideal of R. Then S is a subring of R with the property that $a \in S$ and $r \in R \Rightarrow a.r \in S$ and $r.a \in S$. Since $(S,+)$ is a subgroup of $(R,+)$. So, both the conditions (i) and (ii) are satisfied.

Conversely, let S be a non-empty subset of R where (i) and (ii) both hold. Let $a \in S, b \in S$ Then by (ii) $a \in S, b \in S \Rightarrow a \in S, b \in R$
$\Rightarrow a.b \in S$. So, S is a non-empty subset of R such that $(S,+)$ is a subgroup of R and $a \in S, b \in S \Rightarrow a.b \in S$

Hence S is a subring of R, by Theorem 2.1.3

Since S is a subring of R such that (ii) holds. So, S is an ideal of R.

Theorem 3.1.3 Let $(R,+,\cdot)$ be a ring and S be a non-empty subset of R. Then S is an ideal of R if and only if

(i) $a \in S, b \in S \Rightarrow a-b \in S$ and

(ii) $a \in S, r \in R \Rightarrow r.a \in S$ and $a.r \in S$

Proof: Let S be an ideal of R. Then S is a subring of R such that $a \in S, r \in R \Rightarrow r.a \in S$, and $a.r \in S$.

Since S is a ring $a \in S, b \in S \Rightarrow a-b \in S$

So, both the conditions (i) and (ii) hold.

Conversely, let S be a non-empty subset of R such that (i) and (ii) both hold.

Since (i) holds, $(S,+,\cdot)$ is a subgroup of $(R,+)$.

Since (ii) holds, $a \in S, b \in S \Rightarrow a \in S, b \in R \Rightarrow a.b \in S$

So, S is a non-empty subset of R such that $(S,+)$ is a subgroup of $(R,+)$ and $a \in S, b \in S \Rightarrow a.b \in S$.

Hence S is a subring by Theorem 2.1.3. Since S is a subring of R and (ii) holds, S is an ideal of R.

Examples: 1. Let n be an integer. Then $n\mathbb{Z}$ is an ideal of the ring $\mathbb{Z}$, the ring of all integers.

For any integer n, $n\mathbb{Z}$ is a subring of $\mathbb{Z}$

Case 1. Let $n=0$. Then $n\mathbb{Z}$ is the null ideal $\{0\}$

Case 2. Let $n \neq 0$. Let $S = n\mathbb{Z}$. Let $p, q \in S$