integers and $1 < p < m$, $1 < q < m$. Let 1 be the unity in R. Since $\text{char } R = m$, m is the least positive integer for which $m1 = 0$ but $m1 = (p1)(q1)$. Since R contains no divisor of zero, either $p1 = 0$ or $q1 = 0$.

$p1 = 0 \Rightarrow$ char R is either p or less than p.

$q1 = 0 \Rightarrow$ char R is either q or less than q.

In either case, $\text{char } R = m$ is contradicted. So, m is not a composite number. Since m is neither 1 nor composite, m is a prime number.

If, however, there is no positive integer n for which $n1 = 0$ holds, then $\text{char } R = 0$. This completes the proof.

Note 1.1.38 As field is an integral domain, the characteristic of a field is either zero or a prime number.

Worked out Exercises 1.1.39 : 1. Prove that the ring of matrices $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ is a field.

Proof : Let $S = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$. $(S, +, \cdot)$ is a ring with unity, the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ being the unity in S.

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ -q & p \end{pmatrix} \in S$. Then

$$AB = \begin{pmatrix} ap - bq & aq + bp \\ -(aq + bp) & ap - bq \end{pmatrix} \quad \text{and} \quad BA = \begin{pmatrix} pa - qb & pb + qa \\ -(pb + qa) & pa - qb \end{pmatrix}$$

So, $AB = BA$ for all $A, B \in S$

Hence S is commutative ring with unity. Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ be a non-zero element of S. Then $(a, b) \neq (0, 0)$ and so, $\det A = a^2 + b^2 \neq 0$. Hence A^{-1} exists and $A^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in S$

So, each non-zero element of S is a unit. Hence $(S, +, \cdot)$ is a field.

2. Find the elements in $\mathbb{Z}_{12}$ which are zero divisors.

Solution: We have, in $\mathbb{Z}_{12}$, $\bar{0} = \bar{2}\cdot\bar{6} = \bar{3}\cdot\bar{4} = \bar{8}\cdot\bar{3} = \bar{9}\cdot\bar{4} = \bar{10}\cdot\bar{6}$. So, $\bar{2}, \bar{3}, \bar{4}, \bar{6}, \bar{8}, \bar{9}$ and $\bar{10}$ are zero divisors of $\mathbb{Z}_{12}$. For $k = 1, 5, 7$ or 11, $\bar{k}$ is a unit in $\mathbb{Z}_{12}$, as in these cases $\gcd(k, 12) = 1$. So, these elements are not divisors of zero.

3. Is there any integral domain which has six elements?

Solution: Let R be an integral domain and $o(R) = 6$, then $(R, +)$ is an abelian group of order 6. Then $(R, +)$ is cyclic. Suppose it is generated by $a \in R$. Then $2a, 3a \neq 0$ but $2a \cdot 3a = 6a^2 = 0$ as the order of $(R, +)$ is 6. So R has divisors of zero, a contradiction. So, there is no integral domain of order 6.

4. Suppose R is a ring with unity 1 such that R has no zero divisors. Prove that 0 and 1 are the only idempotent elements in R.

Solution: Let $a \in R$ such $a^2 = a$. Then $a(a-1) = a^2 - a = 0$. Since R has no zero divisors, we have $a = 0$ or $a = 1$. So, 0 and 1 are the only idempotent elements in R. —

5. Let R be a ring with no zero divisors. If $a, b \in R$ be such that $a^m = b^n$ and $a^n = b^n$, where m, n are relatively prime positive integers, then show that $a = b$.

Solution: ~~Let R be a ring~~ First note that, since R has no divisor of zero, if any one of a, b is zero, then the other is also zero. So, suppose $a, b \neq 0$. Now since m, n are relatively prime integers, there are integers x, y such that $mx + ny = 1$. Let $x \geq 0$ and $y \leq 0$ (Since $m, n > 0$, neither $x, y > 0$ nor $x, y < 0$ is possible). Then $a^{mx} = b^{mx}$ which implies $a^{1-ny} = b^{1-ny}$

Again, $a^{-ny} = b^{-ny} = c$(say). Then $ac = bc$ or $(a-b)c = 0$. Certainly $c \neq 0$ as $a \neq 0$ and R has no divisors of zero. So $a - b = 0$ or $a = b$. The proof for the case $x \leq 0$, $y \geq 0$ is similar.

2.1 Subrings and Subfields.

Definition 2.1.1 A non-empty subset S of a ring $(R, +, \cdot)$ is called a subring of R if S forms a ring under the composition $+$ and $\cdot$ restricted to S.

Examples 2.1.2 : 1. Let R be a ring. Then R itself can be considered as a subring of R. This is said to be the improper subring of R.

The zero element of forms a subring of R by itself. This is said to be the trivial subring of R.

2. $(\mathbb{Z}, +, \cdot)$ is a ring with unity. $(2\mathbb{Z}, +, \cdot)$ is a subring of the ring $(\mathbb{Z}, +, \cdot)$ but the subring does not contain the unity.

3. $\mathbb{Z} \times \mathbb{Z}$ is a ring under addition $+$ and multiplication $\cdot$ defined by $(a, b) + (c, d) = (a+c, b+d)$ and $(a, b) \cdot (c, d) = (ac, bd)$ for (a, b), $(c, d) \in \mathbb{Z} \times \mathbb{Z}$. It is a commutative ring with unity $(1, 1)$.

Let us consider the subset S of $\mathbb{Z} \times \mathbb{Z}$ given by $S = \{(a, 0) : a \in \mathbb{Z}\}$

Then S forms a ring under addition and multiplication restricted to S. So, S is a subring of $\mathbb{Z} \times \mathbb{Z}$.

$(1, 0)$ is the unity in S, since $(1, 0) \cdot (a, 0) = (a, 0)$ for all $(a, 0) \in S$.

So, the unity in a subring S is different from the unity in the ring $\mathbb{Z} \times \mathbb{Z}$. Let us consider the subset T of $\mathbb{Z} \times \mathbb{Z}$ given by $T = \{(a, a) : a \in \mathbb{Z}\}$. Then T is a subring of $\mathbb{Z} \times \mathbb{Z}$

$(1, 1)$ is the unity in the subring T and it is the same as the unity in the ring $\mathbb{Z} \times \mathbb{Z}$.

Theorem 2.1.3 Let $(R, +, \cdot)$ be a ring. A non-empty subset S of R forms a subring of R if and only if

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

(ii) S is closed under multiplication

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

Conversely, let the conditions (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 and the distributive laws hold in S. But these are hereditary properties and since they hold in R, they hold in the subset S. So, S is a subring.

Theorem 2.1.4. Let $(R, +, \cdot)$ be a ring and S be a non-empty subset of R. Then S is a subring of R if and only if

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

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

So, both the conditions hold.

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

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

and $0 \in S, a \in S \Rightarrow 0 - a \in S \Rightarrow -a \in S$

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 $+$, the additive identity