Let us consider the set $R = \{0\}$ and define '+' and '.' by the following tables:

+	0
0	0

·	0
0	0

Then $(R, +, \cdot)$ is a ring called trivial ring.

A non-trivial ring R means R has at least two elements.

Theorem 2 If R be a non-trivial ring with unity 1 then $0 \neq 1$

Proof: Since R is a non-trivial ring there exists a non-zero element a in R. Let us assume that $0 = 1$

Then $a \cdot 0 = a \cdot 1 \Rightarrow 0 = a$, a contradiction. So, $0 \neq 1$ in R.

Units

Definition: In a non-trivial ring R with unity, an element a in R is said to be a unit if there exists an element b in R such that $a \cdot b = b \cdot a = 1$, 1 being the unity in R. b is said to be a multiplicative inverse of a.

Theorem 2 If a be a unit in a ring R, its multiplicative inverse is unique.

Proof: If possible, let b, c be two multiplicative inverses of a. Then $a \cdot b = b \cdot a = 1$ and $a \cdot c = c \cdot a = 1$, 1 being the unity in R. Now $b \cdot (a \cdot c) = (b \cdot a) \cdot c$ since multiplication is associative. This implies $b \cdot 1 = 1 \cdot c \Rightarrow b = c$. Hence the proof.

Field: Definition: A non-trivial ring F with unity is a field if each non-zero element is a unit and $a \cdot b = b \cdot a$ for all $a, b \in R$ (we say R is commutative)

So, a non-empty set F with at least two elements forms a field with respect to two binary operations denoted by '+' and '.', if

(i) $a + b \in F$ for all $a, b \in F$

(ii) $a + (b + c) = (a + b) + c$ for all $a, b, c \in F$

(iii) there exists an element, called the zero element and denoted by 0, in F such that $a+0 = 0+a = a$ for all $a \in F$

(iv) For each element a in F, there exists an element, denoted by $-a$, in F such that $a+(-a) = (-a)+a = 0$

(v) $a+b = b+a$ for all $a, b \in F$

(vi) $a.b \in F$ for all $a, b \in F$

(vii) $a.(b.c) = (a.b).c$ for all a, b, c in F

(viii) there exists an element, called the identity element and denoted by 1, in F such that $a.1 = 1.a = a$ for all a in F.

(ix) for each non-zero element a in F there exists an element, denoted by $\bar{a}^1$, in F such that $a.\bar{a} = \bar{a}.a = 1$.

(x) $a.b = b.a$ for all $a, b \in F$

(xi) $a.(b+c) = a.b + a.c$

The field is denoted by $(F, +, .)$ or F.

Examples: 1. The rings $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{C}, +, .)$ are familar examples of field. They are respectively called the field of rational numbers, the field of real numbers and the field of complex numbers.

2. The set $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ forms a commutative ring with unity under addition and multiplication. The multiplicative inverse of $a+b\sqrt{2}$ which is non-zero, (i.e., at least one of a and b is non-zero) is $\frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$ and this belongs to the set as $a^2-2b^2 \neq 0$ and $\frac{a}{a^2-2b^2} \in \mathbb{Q}$, $\frac{-b}{a^2-2b^2} \in \mathbb{Q}$. So, each non-zero element is a unit. So this set forms a field, denoted by $\mathbb{Q}[\sqrt{2}]$

Similarly, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, etc are fields.

Subring: Definition: A non-empty subset S of a ring $(R, +, .)$ is said to a subring of $(R, +, .)$ if S forms a ring under the binary operations '+' and '.' restricted to S.

Examples: 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 R forms a ring 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. $(\mathbb{Q}, +, \cdot)$ is a ring with unity, 1 being the unity. $(\mathbb{Z}, +, \cdot)$ is a subring of the ring $(\mathbb{Q}, +, \cdot)$

4. $\mathbb{Z} \times \mathbb{Z}$ is a ring under addition '+' and multiplication '.' 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, $(1,1)$ being the unity.

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 $\mathbb{Z} \times \mathbb{Z}$. Here $(1,0)$ is the unity in S, as $(1,0) \cdot (a,0) = (a,0) \cdot (1,0) = (a,0)$ for all $(a,0) \in S$.

Here we see that the unity in the subring S is different from the unity in the ring $\mathbb{Z} \times \mathbb{Z}$.

Now we state a theorem without proofs.

Theorem3 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) $a \in S, b \in S \Rightarrow a \cdot b \in S$

Subfield : Definition: A non-empty subset K of a field $(F, +, \cdot)$ is said to be a subfield of $(F, +, \cdot)$ if K forms a field with respect to the binary operations $(+)$ and $(\cdot)$ restricted to K.

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

2. $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is the subset $\mathbb{R}$. $\mathbb{Q}[\sqrt{2}]$ is a subfield of the field $(\mathbb{R}, +, \cdot)$

We state a theorem without proof.

Theorem 4 Let F be a field. A non-empty subset K is a subfield of F if and only if

(i) $a \in K, b \in K \Rightarrow a - b \in K$

(ii) $a \in K, 0 \neq b \in K \Rightarrow a \cdot b^{-1} \in K$

Some worked examples: [Note: In a ring R, a non-zero element a is said to be a divisor of zero if there exists a non-zero element b in R such that $a \cdot b$ or a non-zero element c in R such that $c \cdot a = 0$. In the first case, a is said to be a left divisor of zero and in the second case, a is said to be a right divisor of zero.

If, however, R is a commutative ring, every left divisor of zero is also a right divisor of zero and conversely. Thus there is no distinction between left and right divisors of zero in a commutative ring.

Examples: 1. $(\mathbb{Z}, +, \cdot)$ contains no divisor of zero

2. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ Contain no divisors of zero.

3. In the ring $M_2(\mathbb{R})$, $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 2 & 6 \\ -1 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

So, $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ is a left divisor of zero and $\begin{pmatrix} 2 & 6 \\ -1 & -3 \end{pmatrix}$ is a right divisor of zero. Here $\begin{pmatrix} 2 & 6 \\ -1 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 14 & 28 \\ -7 & -14 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$]

1. Show that the set of matrices $S = \left\{ \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ form a ring with respect matrix addition and multiplication. Show that S contains divisors of zero and does not contain unity

Solution: Here $(S, +)$ forms a additive commutative group where $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the zero element in S.

Let $A = \begin{pmatrix} 2x & 0 \\ 0 & 2y \end{pmatrix}$ and $B = \begin{pmatrix} 2x' & 0 \\ 0 & 2y' \end{pmatrix}$ $x, y, x', y' \in \mathbb{Z}$

Then $AB = \begin{pmatrix} 2.2x^{a}x' & 0 \\ 0 & 2.2yy' \end{pmatrix} = \begin{pmatrix} 2x'' & 0 \\ 0 & 2y'' \end{pmatrix}$ where $x'' = 2xx' \in \mathbb{Z}$ and $y'' = 2yy' \in \mathbb{Z}$

So $AB \in S$. Also matrix multiplication is associative So, multiplication is associative in S.

Also both the distributive laws for any matrix ~~[illegible]~~, where all the additions and products are defined.

So, both the distributive Laws hold in S.

So, $(S, +, \cdot)$ is a ring. Let $E = \begin{pmatrix} 2x & 0 \\ 0 & 2y \end{pmatrix}$ in S be the unity. Then $AE = EA = A$ for all A in S

Let $A = \begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix}$ Then $AE = A$ gives

$4ax = 2a$, $4by = 2b$ So, $x = \frac{1}{2}$ and $y = \frac{1}{2}$ for, $a \neq 0$ and $b \neq 0$ As $x, y \notin \mathbb{Z}$ $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin S$

So, S does not contain the unity.

$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 4 \end{pmatrix}$ are two non-zero elements of S

and $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

This shows that S contains divisors of zero.

2. Show that the set of matrices $S = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ is a ring with respect to matrix ~~multiplication~~ addition and multiplication. Show that S contains divisors of zero.

Proof: Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ and $B = \begin{pmatrix} a' & b' \\ 2b' & a' \end{pmatrix}$, $a, b, a', b' \in \mathbb{R}$

Then $A+B = \begin{pmatrix} a+a' & b+b' \\ 2(b+b') & a+a' \end{pmatrix} = \begin{pmatrix} a'' & b'' \\ 2b'' & a'' \end{pmatrix}$ where $a'' = a+a' \in \mathbb{R}$,

$b'' = b+b' \in \mathbb{R}$ Then $A+B \in S$. As matrix addition is associative in $\mathbb{R}$, so, it is associative in S.

Here $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{R}$, taking $a=0$, $b=0$ in $\mathbb{R}$

and let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \in S$

Then $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$

So, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the additive identity in $\mathbb{R}$

Let $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \in S$. Then consider the matrix $\begin{pmatrix} -a & -b \\ 2(-b) & -a \end{pmatrix} \in S$

and $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} + \begin{pmatrix} -a & -b \\ 2(-b) & -a \end{pmatrix} = \begin{pmatrix} -a & -b \\ 2(-b) & -a \end{pmatrix} + \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

So, $\begin{pmatrix} -a & -b \\ 2(-b) & -a \end{pmatrix}$ is the inverse of $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ in S.

As matrix addition is commutative, it is commutative in S.

So, $(S,+)$ is a commutative group

Let $A = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$ and $B = \begin{pmatrix} a' & b' \\ 2b' & a' \end{pmatrix}$ be in S

Where $a, b, a', b' \in \mathbb{R}$

Then $A.B = \begin{pmatrix} aa'+2bb' & ab'+ba' \\ 2a'b+2ab' & 2bb'+aa' \end{pmatrix} = \begin{pmatrix} a'' & b'' \\ 2b'' & a'' \end{pmatrix} \in S$

Where $a'' = aa'+2bb' \in \mathbb{R}$, $b'' = a'b+ab' \in \mathbb{R}$.

As matrix multiplication is associative, it is associative in S. As both distributive laws hold for any matrices, it both the laws hold in S. So, $(S,+,\cdot)$ is ring

Let $A = \begin{pmatrix} \sqrt{2} & 1 \\ 2 & \sqrt{2} \end{pmatrix}$ and $B = \begin{pmatrix} -\sqrt{2} & 1 \\ 2 & -\sqrt{2} \end{pmatrix}$ Then $A, B \in S$

$A.B = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. So, S contains divisors of zero.

Exercises: 1. Let $(R, +, \cdot)$ be a ring Define $a - b = a + (-b)$, $a, b \in R$. Prove that

(i) $a \cdot (b - c) = a \cdot b - a \cdot c$

(ii) $(b - c) \cdot a = b \cdot a - c \cdot a$ for a, b, c in R.

Some more worked out problems:

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.

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

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $B = \begin{pmatrix} p & q \\ -q & p \end{pmatrix} \in S$ $(\text{i.e., } a, b, p, q \in \mathbb{R})$

Then $A.B = \begin{pmatrix} ap - bq & aq + bp \\ -bp - aq & -bq + ap \end{pmatrix}$

$B.A = \begin{pmatrix} pa - qb & pb + qa \\ -qa - pb & -qb + pa \end{pmatrix}$

So, $A.B = B.A$ for all $A, B \in S$

So, $(S, +, \cdot)$ is a commutative ring with unity.

Let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ be a non-zero element of S

Then $(a, b) \neq (0, 0)$ (i.e not both of a and b be zero)

So, $\det A = a^2 + b^2 \neq 0$. Hence A^{-1} exists

and $A^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \frac{a}{a^2 + b^2} & -\frac{b}{a^2 + b^2} \\ \frac{b}{a^2 + b^2} & \frac{a}{a^2 + b^2} \end{pmatrix} \in S$

So, each non-zero element of the ring is a unit.

Hence $(S, +, \cdot)$ is a field.