We can generalise this ring. Let R be a ring with unity. Let $M_n(R)$ be the set of all $n\times n$ matrices with entries from R. Then $(M_n(R), +, \cdot)$ is a ring where $+$ is the matrix addition and $\cdot$ is the matrix multiplication (They are defined as in the same way as in $\mathbb{R}$ as the ring R has a addition $+$ and multiplication $\cdot$). This ring is called the ring of matrices over the ring R.

Note 1.1.5: If for a ring $R=\{0\}$, then ring R is called a trivial ring.

Theorem 1.1.6. Let R be a ring. Then

(i) $a\cdot 0 = 0\cdot a = 0$ for all $a\in R$, 0 being the zero element in R;

(ii) $a(-b) = (-a)b = -(ab)$ for all $a, b\in R$;

(iii) $(-a)(-b) = ab$ for all $a, b \in R$.

Proof: (i) $a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$

~~or, $a\cdot 0 + 0 = a\cdot 0 + a\cdot 0$ (As 0 is the additive identity)~~

or, $a\cdot 0 + a\cdot 0 = a\cdot 0 + 0$ (As 0 is the additive identity)

or, $a\cdot 0 = 0$ (by left cancellation law)

Similarly, $0\cdot a = 0$.

(ii) $a(-b) + ab = a(-b+b) = a\cdot 0 = 0$

So, $a(-b) = -ab$

Similarly, $(-a)b + ab = (-a+a)b = 0\cdot b = 0$

So, $(-a)b = -ab$

Hence, $a(-b) = (-a)b = -ab$

(iii) $(-a)(-b) = -(-a)b = -(-(ab)) = ab$ (using (ii) and as $-(-x)=x$)

The following results are easy applications of distributive laws:

Theorem 1.1.7 Let R be a ring and $a, b, c, d\in R$. Then

(i) $(a+b)(c+d) = ac+bc+ad+bd$

(ii) $(a-b)(c-d) = ac-bc-ad+bd$

(iii) $(a+b)^2 = a^2+ab+ba+b^2$

(iv) $(a-b)^2 = a^2-ab-ba+b^2$

(v) $(a+b)(a-b) = a^2-ab+ba-b^2$

Proof: Exercise.

Note 1.1.8 One should note that the condition: $a+b=b+a$ in the definition of a ring is redundant in the case of a ring with unity. If R be the ring with unity 1, then using distributive laws, we have $(a+b)(1+1) = (a+b)1 + (a+b)1 = a+b+a+b$ and also $(a+b)(1+1) = a(1+1) + b(1+1) = a+a+b+b$. So, we have

$$a+a+b+b = a+b+a+b$$

So, by cancellation law, $a+b = b+a$

Now in any ring, 0 is an element satisfying $0^2 = 0$ and any ring with unity 1, 1 is another element satisfying $1^2 = 1$. In general we define the following

Definition 1.1.9 An element x in a ring R is called an idempotent element if $x^2 = x$

Example: In $M_3(\mathbb{R})$, the ring of real square matrices of order 3, the following matrices are idempotent elements:

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{bmatrix}$$

There are rings in which every element is idempotent

Definition 1.1.9 A ring R is called a Boolean ring if every element of R is an idempotent element, i.e., $x^2 = x$ for all $x \in R$.

We prove the following interesting properties of a Boolean ring:

Theorem 1.1.10 Let R be a Boolean ring. Then

(i) $x + x = 0$ for all $x \in R$

(ii) $xy = yx$ for all $x, y \in R$

Proof: (i) Let $x \in R$. Then $-x \in R$ and so $x = x^2 = (-x)^2$ [As $(-a)(-b) = ab$] $= -x$. So, $x + x = 0$

(ii) Let $x, y \in R$. Then $x+y = (x+y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$

So, $xy = x + y - x - y - yx = -yx$. But since $yx \in R$, we have $yx = -yx$ by (i). So, $xy = yx$ for all $x, y \in R$.

Theorem 1.1.11 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 $0 = 1$, Then $a \cdot 0 = a.1$ and this implies $0 = a$, a contradiction. So, $0 \neq 1$.

Definition 1.1.12 Let R be a non-trivial ring with unity 1. Then an element $u \in R$ is called a unit (or invertible) if there exists $v \in R$ such that $uv = vu = 1$. v is said to be a multiplicative inverse of u.

Theorem 1.1.13 Let u be a unit in a ring R, its multiplicative inverse is unique.

Proof: If possible, let v, w be two multiplicative inverses of u.

Then $uv = vu = 1$ and $uw = wu = 1$, 1 being the unity in R.

Now $v(uw) = (vu)w$, since multiplication is associative

So, $v.1 = 1.w$ or, $v = w$ and this prove the uniqueness.

Note 1.1.13 The multiplicative inverse of u is denoted by u^{-1}. So, if u be a unit in a ring R, $u^{-1} \in R$ and $uu^{-1} = u^{-1}u = 1$

<u>Examples</u>: 1. In the ring $(\mathbb{Z}, +, \cdot)$, 1 and -1 are the only units.

2. In the ring $(\mathbb{Q}, +, \cdot)$, each non-zero element is a unit.

3. In the ring $(\mathbb{Z}_6, +, \cdot)$, $\bar{1}.\bar{1} = \bar{1}$, $\bar{5}.\bar{5} = \bar{1}$, $\bar{1}$ and $\bar{5}$ are units.

4. In the ring $(\mathbb{Z}_5, +, \cdot)$, each non-zero element is a unit.

5. In the ring $M_2(\mathbb{R})$, every non-singular 2×2 matrix is a unit.

Theorem 1.1.14 In a non-trivial ring R, the zero element is not a unit in R.

Proof: <u>Case 1</u>: Let R be a non-trivial ring without unity. So, no element in R is a unit in R. So, 0 is not a unit in R.

<u>Case 2</u>: Let R be a non-trivial ring with unity 1. If possible, let 0 be a unit in R. Then 0^{-1} exists in R and $0.0^{-1} = 0^{-1}.0 = 1$

But $0.0^{-1} = 0^{-1} \cdot 0 = 0$ by the property of 0 (by Theorem 1.1.6 (i))

So, $1=0$, a contradiction to the fact that R is a non-trivial ring with unity 1. So, 0 is not a unit in R.

Theorem 1.1.15 Let R be a ~~ring~~ non-trivial ring with unity 1. Then the set of units of R forms a group

Proof: Let U be the set of units of R. We shall show that $(U,\cdot)$ is a subgroup of the semigroup $(R,\cdot)$. Now $U \neq \phi$ as $1 \in U$. Also if $u \in U$, then there exists $u^{-1} \in R$ such that

$u u^{-1} = u^{-1} u = 1$. This implies $u^{-1} \in U$. Further, if $u, v \in U$, then $uv(v^{-1}u^{-1}) = u(vv^{-1})u^{-1} = u.1.u^{-1} = uu^{-1} = 1$. Similarly, $(v^{-1}u^{-1})(uv) = v^{-1}(u^{-1}u)v = v^{-1}.1.v = v^{-1}v = 1$. So, uv is a unit and $(uv)^{-1} = v^{-1}u^{-1}$. Thus U has an identity element 1 and for each element $u \in U$, there exists an inverse $u^{-1} \in U$ of u; also U is closed under multiplication. So, $(U,\cdot)$ is a subgroup of $(R,\cdot)$

Note 1.1.16 We now give the definition of integral multiples of an element in a non-trivial ring. Let R be a non-trivial ring and $a \in R$. Then for any integer n, we define na as follows:

$$
\begin{aligned}
na &= (a+a+\cdots+a) \text{ (added } n \text{ times), when } n>0 \\
&= ((-a)+(-a)+\cdots+(-a)) \text{ (added } -n \text{ times), when } n<0 \\
&= 0 \text{ (the zero element in } R\text{), when } n=0
\end{aligned}
$$

It follows easily from the definition that if $m, n \in \mathbb{Z}$,

(i) $(m+n)a = ma + na$ for all $a \in R$

(ii) $m(a+b) = ma + mb$ for all $a, b \in R$

If R be a ring with unity 1 and $a \in R$, then

$$na = (n1)\cdot a \quad \text{where } n \in \mathbb{Z} \text{ and } n>0$$

Definition 1.1.17 An element x in a ring R is said to be a nilpotent element if $x^n = 0$ for some positive integer n.

Example: In the ring $M_2(\mathbb{R})$, the matrix $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is a nilpotent element as $A^2 = 0 = [$