Definition 17.1

A *ring* is set R equipped with two binary operations:

- *addition*, denoted $a + b$
- *multiplication*, denoted $a \cdot b$

satisfying the following properties:

1) R taken with addition is an abelian group (with the identity element $0 \in R$).
2) Multiplication is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in R$.
3) For any $a, b, c \in R$ we have $(a + b)c = ac + bc$ and $a(b + c) = ab + ac$.

Definition 17.2

We say that a ring R is *commutative* if $ab = ba$ for any $a, b \in R$.

We say that R is a *ring with unity* if there is an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

Example. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with the usual addition and multiplication are commutative rings rings with unity.

Example. $\mathbb{Z}_n$ with the addition and multiplication modulo n is a commutative ring with unity.

Example. Let $M_n(\mathbb{R})$ denote the set of $n \times n$ matrices with coefficients in $\mathbb{R}$. This is ring with addition and multiplication given by the usual addition and multiplication of matrices. This is a ring with unity (given by the identity matrix), but it is not commutative. In the same way with can define rings $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$ and $M_n(\mathbb{C})$ of $n \times n$ matrices with integer, rational and complex coefficients.

Example. Let R be a commutative ring. By $R[x]$ we denote the ring of polynomials with coefficients in R. Elements of $R[x]$ are polynomials of the form

$$p(x) = a_0 + a_1 x + \ldots + a_n x_n$$

where $a_i \in R$ and $n \geq 0$. Addition and multiplication are the usual addition and multiplication of polynomials. The ring $R[x]$ is commutative if R is commutative If R is a ring with unit $1 \in R$ then $R[x]$ is a ring with unity given by the polynomial $p(x) = 1$.

Example. In a similar way as in the last example, from any ring R we obtain a ring $R[x_1, \ldots, x_m]$ of polynomials of m variables.

Example Let S denote the set of all polynomials

$$p(x) = 0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

such that $a_i \in \mathbb{Z}$, $n \geq 1$. The set S is a commutative ring with the usual addition and multiplication of polynomials, but it does not have a unity.

Theorem 17.3

If a ring R has a unity, the the unity is unique.

Proof. Assume that $1, 1'$ are two unities in R, so that

$$1 \cdot a = a \cdot 1 = a \quad \text{and} \quad 1' \cdot a = a \cdot 1' = a$$

for all $a \in R$. Then $1 = 1 \cdot 1' = 1'$. □

Theorem 17.4

If a ring R. For any $a, b \in R$ we have:

1) $0 \cdot a = a \cdot 0 = 0$.

2) $a(-b) = (-a)b = -(ab)$.

3) $(-a)(-b) = ab$

4) if R has a unity $1 \in R$ then $(-1)a = a(-1) = -a$.

Proof. **1)** We have

$$0 \cdot a = (0 + 0)a = 0 \cdot a + 0 \cdot a$$

Subtracting $0 \cdot a$ from both sides we obtain $0 \cdot a = 0$. By the same argument, $a \cdot 0 = 0$.

2) We have
$$a(-b) + ab = a(b - b) = a \cdot 0 = 0$$

Thus $a(-b) = -ab$. In the same way, $a(-b) = -(ab)$

3) Using part 2) we obtain (-a)(-b) = -(a(-b)) = -(-(ab)) = ab

4) We have

$$0 = 0 \cdot a = (1 + (-1))a = 1 \cdot a + (-1)a = a + (-1)a$$

Thus $(-1)a = -a$. Similarly, $a(-1) = -a$. $\square$

Definition 17.5

Let R be a ring. A *subring* of R is a subset $S \subseteq R$ such that S is a ring with respect to the addition and multiplication in R.

Example. $\mathbb{Z}$ is a subring of $\mathbb{Q}$.

Example. Let $2\mathbb{Z}$ denote the set of even integers. Then $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

Theorem 17.6

Let R be a ring. A subset $S \subseteq R$ is a subring of R if and only if the following conditions are satisfied:

1) $0 \in S$

2) if $a, b \in S$ then $a + b \in S$ and $ab \in S$

3) if $a \in S$ then $(-a) \in S$

Definition 17.7

The *direct product* of rings R_1, R_1 is a ring $R_1 \times R_2$ defined as follows:

- Elements of $R_1 \times R_1$ are ordered tuples (a_1, a_2) where $a_i \in R_i$
- Addition and multiplication are given by

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1,\ a_2 + b_2)$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1,\ a_2 b_2)$$

Note. If $R_1, R_2, \ldots, R_n$ are rings that the direct product $R_1 \times R_2 \times \ldots R_n$ is defined analogously as as in Definiton 17.7.