1 Introduction to Rings

1.1 Basic Definitions and Examples

Definition.

1. A *ring* R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

   (a) $(R, +)$ is an abelian group,

   (b) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$,

   (c) the *distributive laws* hold in R: for all $a, b, c \in R$,

   $$(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c).$$

2. The ring R is *commutative* if multiplication is commutative.

3. The ring R is said to have an *identity* (or *contain a 1*) if there is an element $1 \in R$ with
$$1 \times a = a \times 1 = a \qquad \text{for all } a \in R.$$

Note.

1. We shall write ab rather than $a \times b$ for $a, b \in R$.

2. The additive identity of R will be denoted by 0

3. The additive of an element a will be denoted $-a$.

Note. $R = \{0\}$ is called the *zero ring*, denoted $R = 0$. $R = 0$ is the only ring where $1 = 0$. We will often exclude this ring by imposing the condition $1 \neq 0$.

Definition. A ring R with identity $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field*.

Proposition 1. Let R be a ring. Then

1. $0a = a0 = 0$ for all $a \in R$.

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

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

4. If R has an identity 1, then the identity is unique and $-a = -1(a)$.

Definition. Let R be a ring

1. A nonzero element a of R is called a *zero divisor* if there is a nonzero element b of R such that either $ab = 0$ or $ba = 0$.

2. Assume R has an identity $1 \neq 0$. An element u of R is called a *unit* in R if there is some v in R such that $vu = uv = 1$. The set of units in R is denoted $R^{\times}$.

Note.

1. $R^\times$ forms a group under multiplication and will be referred to as the *group of units* of R.

2. Using the above terminology a field is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^\times = F - \{0\}$.

Definition. A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

Proposition 2. Assume a, b and c are elements of any ring with a not a zero divisor. If $ab = ac$ then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$ we can cancel the a's). In particular, if a, b, c are elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

Corollary 3. Any finite integral domain is a field.

Definition. A *subring* of the ring R is a subgroup of R that is closed under multiplication.

Note. To show that a subset of a ring R is a subring it is enough to show that it is nonempty and closed under subtraction and under multiplication.

1.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings