MA3202

Algebra II

Spring 2022

Satvik Saha
19MS154

Indian Institute of Science Education and Research, Kolkata,
Mohanpur, West Bengal, 741246, India.

Contents

1 Rings

1.1 Basic definitions

Definition 1.1. A ring is a set R equipped with two binary operations, namely addition and multiplication, such that

1. $(R, +)$ is an abelian group.
   (a) $a + b \in R$ for all $a, b \in R$.
   (b) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.
   (c) $a + b = b + a$ for all $a, b \in R$.
   (d) There exists $0 \in R$ such that $a + 0 = a$ for all $a \in R$.
   (e) For each $a \in R$, there exists $-a \in R$ such that $a + (-a) = 0$.
2. $(R, \cdot)$ is a semi-group.
   (a) $a \cdot b \in R$ for all $a, b \in R$.
   (b) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
3. Multiplication distributes over addition.
   (a) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$.
   (b) $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ for all $a, b, c \in R$.

Remark. The following properties follow immediately,

1. $0 \cdot a = 0$ for all $a \in R$.
2. $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$ for all $a, b \in R$.
3. $(na) \cdot b = n(a \cdot b) = a \cdot (nb)$ for all $a, b \in R$.

Example. The integers $\mathbb{Z}$ form a ring, under the usual addition and multiplication.

Example. All fields, for instance the rational numbers $\mathbb{Q}$ or the real numbers $\mathbb{R}$, are rings.

Example. The integers modulo n, namely $\mathbb{Z}/n\mathbb{Z}$, form a ring.

Example. If R is a ring, then the algebra of polynomials $R[X]$ with coefficients from R form a ring.

Example. If R is a ring, then the $n \times n$ matrices $M_n(R)$ with entries from R form a ring.

Definition 1.2. If R is a ring and $(R, \cdot)$ is a monoid i.e. has an identity, then this identity is unique and called the unity of the ring R. Such a ring R is called a unit ring.

Example. The even integers $2\mathbb{Z}$ form a ring, but do not contain the identity.

Definition 1.3. If R is a ring and $(R, \cdot)$ is commutative, then R is called a commutative ring.

Definition 1.4. Let R be a unit ring. An element $a \in R$ is called a unit if there exists $b \in R$ such that $a \cdot b = 1 = b \cdot a$. This $b \in R$ is unique, and denoted by a^{-1}.

Example. The units in $\mathbb{Z}$ are $\{1, -1\}$.

Definition 1.5. Let R be a ring, and let $S \subseteq R$. We say S is a subring of R if the structure $(S, +, \cdot)$ is a ring, with addition and multiplication inherited from R.

Example. The rings $n\mathbb{Z}$ for $n \in \mathbb{N}$ are all subrings of $\mathbb{Z}$.