RINGS AND MODULES

Manish Kumar, notes by Ramdas Singh

Fourth Semester

Contents

Chapter 1

INTRODUCTION TO RINGS

January 19th.

Of course, we begin with the definition of a ring.

Definition 1.1. A *ring* is a triple $(R, +, \cdot)$ where R is a set, and $+$ and $\cdot$ are binary operations on R such that the following axioms are satisfied:

- $(R, +)$ is an abelian group. The identity element of this group is denoted by 0_R, and the (additive) inverse of an element $a \in R$ is denoted by $-a$.
- The property of *associativity* of $\cdot$ holds; i.e., for all $a, b, c \in R$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- The property of *distributivity* of $\cdot$ over $+$ holds; i.e., for all $a, b, c \in R$, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c, \tag{1.1}$$

$$(a + b) \cdot c = a \cdot c + b \cdot c. \tag{1.2}$$

Rings may be written simply as R instead of the triple. The ring R is termed a *ring with unity* if there exists an element $1_R \in R$ such that for all $a \in R$, we have $1_R \cdot a = a \cdot 1_R = a$. Some examples of rings with unity include $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $M_n(\mathbb{R})$ with the usual addition and multiplication. A ring R is said to be a *commutative ring* if for all $a, b \in R$, we have $a \cdot b = b \cdot a$. Examples of commutative rings include $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, but $M_n(\mathbb{R})$ is not commutative for $n \geq 2$. Lastly, a commutative ring R with unity is termed a *field* if every non-zero element of R has a multiplicative inverse; i.e., for every $a \in R \setminus \{0_R\}$, there exists an element $b \in R$ such that $a \cdot b = b \cdot a = 1_R$. Examples of fields include $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, but $\mathbb{Z}$ is not a field.

Example of rings without unity include $2\mathbb{Z}$ with the usual addition and multiplication, and the set of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$ that vanish at 0, with the usual addition and multiplication of functions. Another class of rings we previously studied was $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$, with the usual addition and multiplication modulo n. This ring has unity, but is a field if and only if n is prime.

Definition 1.2. Let R be a ring with unity. An element $a \in R$ is called a *unit* if there exists an element $b \in R$ such that $a \cdot b = b \cdot a = 1_R$.

For example, in the ring $\mathbb{Z}/n\mathbb{Z}$, an element $\bar{a}$ is a unit if and only if $\gcd(a, n) = 1$. The set of all units in a ring R with unity is denoted by $R^\times$. It can be easily verified that $(R^\times, \cdot)$ is an abelian group.

1.1 Properties and Maps

Some basic properties may be inferred.

Proposition 1.3. *Let R be a ring with unity. Then,*

- 1_R *is the unique multiplicative identity in* R.
- $1_R \cdot 0_R = 0_R$. *In general,* $a \cdot 0_R = 0_R$ *for all* $a \in R$.
- $-1_R \cdot a = -a$ *for all* $a \in R$.

Proof.

- This is left as an exercise to the reader.
- $1_R \cdot 0_R = 1_R$ is trivial since 1_R is the multiplicative identity. For the general case, let $a \in R$. Then,

$$a \cdot 0_R = a \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R \implies a \cdot 0_R = 0_R \tag{1.3}$$

  by the addition of $-(a \cdot 0_R)$ on both sides.

- Let $a \in R$. Then,

$$(-1_R \cdot a) + a = (-1_R + 1_R) \cdot a = 0_R \implies -1_R \cdot a = -a. \tag{1.4}$$

■

The subscript R in 0_R and 1_R may be dropped when the context is clear. We move on to some special maps.

Definition 1.4. A *ring homomorphism* is a map $\varphi : (R, +, \cdot) \to (S, \oplus, \odot)$ between two rings such that for all $a, b \in R$, we have

$$\varphi(a + b) = \varphi(a) \oplus \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \odot \varphi(b). \tag{1.5}$$

Most of the time, we shall drop $\oplus$ and $\odot$ when the context is clear. Some examples of ring homomorphisms include the map $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\varphi(a) = \bar{a}$ for all $a \in \mathbb{Z}$, and the inclusion map from $\mathbb{Z}$ to $\mathbb{Q}$. Non-examples include $n \mapsto -n$ from $\mathbb{Z}$ to $\mathbb{Z}$, and the determinant map from $M_n(\mathbb{R})$ to $\mathbb{R}$.

Let $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ be the ring where addition and multiplication are defined component-wise. Then the map $Z \to \mathbb{Z} \times \mathbb{Z}$ defined by $a \mapsto (a, 0)$ is a ring homomorphism since it preserves both addition and multiplication. However, the unity of $\mathbb{Z}$ is mapped to $(1, 0)$, which is not the unity of $\mathbb{Z} \times \mathbb{Z}$. Thus, ring homomorphisms need not map unity to unity.

Definition 1.5. Let R be a ring with $S \subseteq R$ a subset. Then, S is called a *subring* of R if $(S, +, \cdot)$ is itself a ring with the operations inherited from R.

Again, even if R has unity, a subring S need not have the same unity as R or even a unity at all.

Index