RINGS AND MODULES

Manish Kumar, notes by Ramdas Singh

Fourth Semester

Contents

1 INTRODUCTION TO RINGS 1
1.1 Properties and Maps 1
1.1.1 Polynomials 3
1.2 Ideals 4

Index 7

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.

January 23rd.

Definition 1.6. A ring homomorphism $\varphi : R \to S$ is termed a *ring monomorphism* if it is injective, a *ring epimorphism* if it is surjective, and a *ring isomorphism* if it is bijective. If there exists a ring isomorphism from R to S, then R and S are said to be *isomorphic*, denoted by $R \cong S$.

Note that if $\varphi : R \to S$ is bijective, then its inverse $\varphi^{-1} : S \to R$ is a ring homomorphism. We look at some examples of rings and mappings.

Example 1.7. Let X be any set and let $R := \{f : X \to \mathbb{R}\}$ be the set of all functions from X to $\mathbb{R}$. Then, $(R, +, \cdot)$ is a ring where addition and multiplication are defined pointwise; i.e., for all $f, g \in R$ and $x \in X$, $(f + g)(x) := f(x) + g(x)$ and $(f \cdot g)(x) := f(x) \cdot g(x)$. The additive identity is the zero function $0 : X \to \mathbb{R}$ defined by $0(x) = 0$ for all $x \in X$, and the multiplicative identity is the constant function $1 : X \to \mathbb{R}$ defined by $1(x) = 1$ for all $x \in X$. It is easy to verify that all ring axioms are

satisfied. Moreover, this ring is commutative and has unity. Note that $\mathbb{R}$ can be replaced by any ring S to form the ring of functions from X to S. In such a case, R is a (commutative) ring with unity if and only if S is a (commutative) ring with unity.
In the special case that $X = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, the ring R is isomorphic to the ring $(\mathbb{R}^n, +, \cdot)$ where addition and multiplication are defined component-wise. The isomorphism $\varphi : R \to \mathbb{R}^n$ is given by $\varphi(f) = (f(1), f(2), \ldots, f(n))$ for all $f \in R$.

Example 1.8. Continuing from the previous example, let $X = [a, b]$. Note that the R in this case is the set of all functions from the interval $[a, b]$ to $\mathbb{R}$, which is not a very manageable set. Thus, we may consider the subset $C([a, b], \mathbb{R}) \subseteq R$ consisting of all continuous functions from $[a, b]$ to $\mathbb{R}$. It is easy to verify that $C([a, b], \mathbb{R})$ is a subring of R. Similarly, one defined $C^n([a, b], \mathbb{R})$ to be the set of all n-times continuously differentiable functions from $[a, b]$ to $\mathbb{R}$, and $C^\infty([a, b], \mathbb{R})$ to be the set of all infinitely differentiable functions from $[a, b]$ to $\mathbb{R}$. Both of these are subrings of R as well.

Example 1.9. The set $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$ is a subring of the field $\mathbb{C}$. It is easy to verify that $\mathbb{Z}[i]$ is a ring with unity, but it is not a field since, for example, the element $1 + i$ does not have a multiplicative inverse in $\mathbb{Z}[i]$. Note that there is a natural bijection $\varphi : \mathbb{Z}[i] \to \mathbb{Z}^2$ defined by $\varphi(a + bi) = (a, b)$ for all $a + bi \in \mathbb{Z}[i]$, where $\mathbb{Z}^2$ has component-wise addition and multiplication. However, this map is not a ring isomorphism since it does not preserve multiplication; for example, $\varphi(i \cdot i) = \varphi(-1) = (-1, 0)$, but $\varphi(i) \cdot \varphi(i) = (0, 1) \cdot (0, 1) = (0, 1)$.

1.1.1 Polynomials

Let R be a ring. The polynomial ring in the variable x with coefficients from R is defined as follows:

Definition 1.10. The *polynomial ring* $R[x]$ is defined as

$$R[x] := \{f : \mathbb{N}_0 \to R \mid f(n) = 0 \text{ for all but finitely many } n \in \mathbb{N}_0\}. \tag{1.6}$$

The elements of $R[x]$ are called *polynomials* in the variable x with coefficients from R. For $f, g \in R[x]$ and $n \in \mathbb{N}_0$, addition is defined as

$$(f + g)(n) := f(n) + g(n) \quad \text{for all } n \in \mathbb{N}_0, \tag{1.7}$$

and multiplication is defined as

$$(f \cdot g)(n) := \sum_{k=0}^{n} f(k) \cdot g(n - k) \quad \text{for all } n \in \mathbb{N}_0. \tag{1.8}$$

Alternatively, a polynomial $f \in R[x]$ may be expressed in the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \tag{1.9}$$

where $a_i = f(i)$ for all $0 \leq i \leq n$ and $f(k) = 0$ for all $k > n$. For $0 \neq f \in R[x]$ as above with $a_n \neq 0_R$, the integer n is called the *degree* of f, denoted by $\deg(f)$. The degree of the zero polynomial is usually left undefined, or changed upon convention. Also note that $f \cdot g \in R[x]$ since $f \cdot g(k) = 0_R$ for all $k > \deg(f) + \deg(g)$.

Proposition 1.11. *For a ring R, the polynomial ring $R[x]$ is, indeed, a ring with unity under the operations defined above. If R is commutative, then so is $R[x]$. The map $\iota : R \to R[x]$ defined by $\iota(a) = f_a$ where $f_a(0) = a$ and $f_a(n) = 0_R$ for all $n \geq 1$ is a ring monomorphism.*

Proof. That $(R[x], +)$ forms an abelian group is clear. The associativity of multiplication is verified as

follows: let $f, g, h \in R[x]$ and $n \in \mathbb{N}_0$. Then,

$$((f \cdot g) \cdot h)(n) = \sum_{k=0}^{n} (f \cdot g)(k) \cdot h(n-k) = \sum_{k=0}^{n} \left(\sum_{j=0}^{k} f(j) \cdot g(k-j) \right) \cdot h(n-k)$$
$$= \sum_{j=0}^{n} f(j) \cdot \left(\sum_{k=j}^{n} g(k-j) \cdot h(n-k) \right) = \sum_{j=0}^{n} f(j) \cdot (g \cdot h)(n-j) = (f \cdot (g \cdot h))(n). \quad (1.10)$$

The distributive properties follow similarly. The unity in $R[x]$ is the polynomial $1_{R[x]}$ defined by $1_{R[x]}(0) = 1_R$ and $1_{R[x]}(n) = 0_R$ for all $n \geq 1$. Finally, it is easy to verify that ι is a ring homomorphism, and it is injective since $\iota(a) = \iota(b)$ implies that $a = b$. ■

With $R[x]$ established as a ring, we may consider a higher level of abstraction, by considering polynomials over this polynomial ring itself; that is, $(R[x])[y]$. Elements of this ring look like

$$f(x, y) = a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \cdots + a_{mn}x^m y^n, \quad (1.11)$$

where $a_{ij} \in R$ for all $i, j \geq 0$ and $a_{ij} = 0_R$ for all but finitely many pairs (i, j). We have already shown that $R[x]$ is a ring, so it follows that $(R[x])[y]$ is also a ring. This ring is usually denoted by $R[x, y]$. For $f \in R[x, y]$ as above with $a_{mn} \neq 0_R$, the degree of f is defined as $\deg(f) = m + n$. Similarly, one may define $R[x_1, x_2, \ldots, x_n]$ for any $n \in \mathbb{N}$. For a countable number of indeterminates, one may define $R[x_1, x_2, x_3, \ldots]$ as the union $\bigcup_{n=1}^{\infty} R[x_1, x_2, \ldots, x_n]$.

Example 1.12. Let $e \in \mathbb{R}$ be the Euler's number (or any transcendental number). Then $\mathbb{Z}[e] \subseteq \mathbb{C}$ is the smallest subring of $\mathbb{C}$ containing both $\mathbb{Z}$ and e. Here, $\mathbb{Z}[e]$ consists of all polynomials in e with integer coefficients; i.e., all elements of the form $a_0 + a_1 e + a_2 e^2 + \cdots + a_n e^n$ where $n \geq 0$ and $a_i \in \mathbb{Z}$. Since e is transcendental, there are no non-trivial polynomial relations among the powers of e with integer coefficients. Thus, the map $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[e]$ defined by $\varphi(f) = f(e)$ for all $f \in \mathbb{Z}[x]$ is a ring isomorphism.

1.2 Ideals

Definition 1.13. Let R be a commutative ring with unity. A subset $I \subseteq R$ is called an *ideal* of R if the following conditions hold:

- for all $a, b \in I$, we have $a + b \in I$,
- for all $a \in I$ and $r \in R$, we have $r \cdot a \in I$.

Note that the first condition implies that $(I, +)$ is a subgroup of $(R, +)$. Some examples of ideals include the set $\{0_R\}$, the ring R itself, and the set $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ for any $n \in \mathbb{Z}_{\geq 0}$ as an ideal of the ring $\mathbb{Z}$. A non-example is $\mathbb{Z}$ in $\mathbb{R}$; it is a subring, but not an ideal since, for example, $1 \in \mathbb{Z}$ but $\pi \cdot 1 = \pi \notin \mathbb{Z}$. Note that if $1_R \in I$, then $I = R$.

Example 1.14. Let us look at ideals of $\mathbb{R}$. Trivially, $\{0\}$ and $\mathbb{R}$ are ideals of $\mathbb{R}$. We claim that these are the only ideals of $\mathbb{R}$. To see this, let I be any ideal of $\mathbb{R}$ such that $I \neq \{0\}$. Then, there exists some $a \in I$ such that $a \neq 0$. Since $\mathbb{R}$ is a field, a has a multiplicative inverse $a^{-1} \in \mathbb{R}$. Thus, $1 = a^{-1} \cdot a \in I$, which implies that $I = \mathbb{R}$. In fact, this argument shows that in any field, the only ideals are the zero ideal and the field itself.

Example 1.15. We examine ideals of $\mathbb{Z}$. From group theory, we know that every subgroup of $(\mathbb{Z}, +)$ is of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}_{\geq 0}$, so $n\mathbb{Z}$ are the only candidates for ideals of $\mathbb{Z}$. In fact, each $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ since for all $a, b \in n\mathbb{Z}$, we have $a + b \in n\mathbb{Z}$, and for all $a \in n\mathbb{Z}$ and $r \in \mathbb{Z}$, we have $r \cdot a \in n\mathbb{Z}$. Thus, the ideals of $\mathbb{Z}$ are precisely the sets $n\mathbb{Z}$ for $n \in \mathbb{Z}_{\geq 0}$, and $\mathbb{Z}$.

Proposition 1.16. *Let $f : R \to S$ be a ring homomorphism between two commutative rings with unity. Then, the* kernel *of f, defined as*

$$\ker f := \{a \in R \mid f(a) = 0_S\}, \tag{1.12}$$

is an ideal of R. Moreover, f is a ring monomorphism if and only if $\ker f = \{0_R\}$.

Proof. Let $a, b \in \ker f$ and $r \in R$. Then,

$$f(a+b) = f(a) + f(b) = 0_S + 0_S = 0_S, \tag{1.13}$$

so $a + b \in \ker f$. Also,

$$f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0_S = 0_S, \tag{1.14}$$

so $r \cdot a \in \ker f$. Thus, $\ker f$ is an ideal of R.

Now, suppose that f is a ring monomorphism. Let $a \in \ker f$. Then, $f(a) = 0_S = f(0_R)$. Since f is injective, we have $a = 0_R$, so $\ker f = \{0_R\}$. Conversely, suppose that $\ker f = \{0_R\}$. Let $a, b \in R$ such that $f(a) = f(b)$. Then,

$$f(a-b) = f(a) - f(b) = 0_S, \tag{1.15}$$

so $a - b \in \ker f$. Thus, $a - b = 0_R$, which implies that $a = b$. Therefore, f is injective. ■

Index

associativity, 1

commutative ring, 1

degree, 3
distributivity, 1

field, 1

ideal, 4
isomorphic, 2

kernel, 5

polynomial ring, 3
polynomials, 3

ring, 1
ring epimorphism, 2
ring homomorphism, 2
ring isomorphism, 2
ring monomorphism, 2
ring with unity, 1

subring, 2

unit, 1