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.

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 $X = \{1, 2, \dots, n\}$ 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 $\varphi(f) = (f(1), f(2), \dots, f(n))$ 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 $0 \le i \le n$ and $f(k) = 0$ for all $k > n$. For $0 \ne f \in R[x]$ as above with $a_n \ne 0_R$, 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 $n \ge 1$ 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,

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

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. ■

January 24th.

Let R be a ring with unity and R_i be a colelction of subrings of R containing the nuity. Then $\bigcap_i R_i$ is also a subring of R containing the unity. If I_j is a collection of ideals of R, then $\bigcap_j I_j$ is also an ideal of R. Thus, given any subset $S \subseteq R$, we may define the ideal generated.

Definition 1.17. Let R be a commutative ring with unity and $I \subseteq R$ be an ideal. Let $S \subseteq I$ be a set. We say S is a *generating set* of I if I is the smallest ideal containing S.

Proposition 1.18. *Let R be a commutative ring with unity and $S \subseteq R$ be any subset. Then, the ideal generated by S, denoted by (S), is given by*

$$(S) = \left\{ \sum_{i=1}^{n} r_i s_i : n \geq 0, r_i \in R, s_i \in S \text{ for all } 1 \leq i \leq n \right\}. \tag{1.16}$$

Proof. Let $S \subseteq I$, a subset of an ideal. We claim that $(S) \subseteq I$. Let $\alpha \in I$. THen, $\alpha = r_1 x_1 + \cdots + r_n x_n$ for some $n \geq 0$, $r_i \in R$ and $x_i \in S$ for all $1 \leq i \leq n$. Since I is an ideal, we have $r_i x_i \in I$ for all $1 \leq i \leq n$, and thus $\alpha \in I$. Therefore, $(S) \subseteq I$. ■

With this, we introduce the notation that if $\{x_1, \ldots, x_n\} \subseteq R$, then $I = (x_1, \ldots, x_n) = Rx_1 + \cdots + Rx_n$ is the ideal generated by $x_1, \ldots, x_n$. Let us look at some exmaples.

Example 1.19. In the ring $\mathbb{Z}$, $(2, 3) = \mathbb{Z}$ since $1 = 3 - 1 \cdot 2 \in (2, 3)$. More generally, for any $a, b \in \mathbb{Z}$, we have $(a, b) = \mathbb{Z}$ if and only if $\gcd(a, b) = 1$. Moreover, in $\mathbb{Z}$, every ideal can be generated by a single element; i.e., every ideal is of the form (n) for some $n \in \mathbb{Z}_{\geq 0}$.

Example 1.20. In $\mathbb{Z}[x]$, the ideal $(2, x)$ consists of all polynomials with integer coefficients where the constant term is even. That is, $(2, x) = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$.

Also note that a union of ideals need not be an ideal. For example, in $\mathbb{Z}$, the sets $2\mathbb{Z}$ and $3\mathbb{Z}$ are ideals, but their union $2\mathbb{Z} \cup 3\mathbb{Z}$ is not an ideal. This, however, calls for a more general construction.

Definition 1.21. Let R be a commutative ring with unity. If I_1, I_2 are two ideals, we then define their sum as $I_1 + I_2 = (I_1 \cup I_2)$.

It is easy to verify that $I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$. This definition may be extended to a finite number of ideals in the obvious way.

1.3 Other Rings

Definition 1.22. Let G be a group and k be a field. We define $R[G]$ to be the set of all functions $f : G \to k$ such that $f(x) = 0$ for all but finitely many $x \in G$. Addition is defined pointwise as

$$(f + g)(x) = f(x) + g(x) \quad \text{for all } x \in G, \tag{1.17}$$

and multiplication is defined as

$$(f \cdot g)(x) = \sum_{yz=x} f(y)g(z) = \sum_{y\in G} f(xy^{-1})g(y) \quad \text{for all } x \in G. \tag{1.18}$$

The ring $R[G]$ is called the *group ring* of G over k.

If G is a finite group with $G = \{e, x_2, \ldots, x_n\}$ then $R[G] = \{a_1 e + a_2 x_2 + \cdots + a_n x_n \mid a_i \in \mathbb{C}\}$. Verify that $R[G]$ is a ring with unity under the operations defined above. This ring, however, may not be commutative.

Definition 1.23. Let R be a ring and $x \in R$. x is termed *nilpotent* if there exists some $n \in \mathbb{N}$ such that $x^n = 0$. If R is commutative, $x \in R$ is called a *zero divisor* if there exists some $y \in R \setminus \{0\}$ such that $x \cdot y = 0$.

Note that nilpotents are zero divisors in a commutative ring, but the converse need not be true. For example, in the ring $\mathbb{Z}/6\mathbb{Z}$, the element $\bar{2}$ is a zero divisor since $\bar{2} \cdot \bar{3} = \bar{0}$, but it is not nilpotent since $\bar{2}^n \neq \bar{0}$ for all $n \geq 1$.

Definition 1.24. A commutative ring with unity R is called a *reduced ring* if it has no non-zero nilpotent elements. It is called an *integral domain* if it has no non-zero zero divisors.

Proposition 1.25. *Let R be an integral domain. Then, if $x, y \in R$ are such that $x \cdot y = 0$, then either $x = 0$ or $y = 0$.*

Proof. If $x \neq 0$, then since R is an integral domain, x is not a zero divisor. Thus, y must be 0. Similarly, if $y \neq 0$, then x must be 0. ■

Proposition 1.26. *Every integral domain is a reduced ring.*

Proof. Let R be an integral domain and let $x \in R$ be nilpotent. Then, there exists some $n \in \mathbb{N}$ such that $x^n = 0$. If $x \neq 0$, then since R is an integral domain, x is not a zero divisor. However, this contradicts the fact that $x^n = 0$. Thus, we must have $x = 0$, so R has no non-zero nilpotent elements. ■

January 29th.

In an integral domain R, if $ab = ac$ for some $a, b, c \in R$, then either $a = 0$ or $b = c$. Let us look at some examples of integral domains.

Example 1.27. The ring $\mathbb{Z}$ is an integral domain since it has no non-zero zero divisors. Similarly, the rings $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are integral domains as well. More generally, any field is an integral domain. Moreover, $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime.

Example 1.28. Note that R is an integral domain if and only if $R[x]$ is an integral domain.

Another small result is as follows: if R is an integral domain and R' is a subring of R containing the unity, then R' is also an integral domain. Some non-examples of integral domains include $\mathbb{Z}^2$, $C[0,1]$, $C^\infty[0,1]$, etc.

1.4 Quotient Rings and Isomorphism Theorems

From here on, we shall assume that all rings are commutative with unity unless otherwise stated.

Definition 1.29. Let R be a ring and I be an ideal of R. The *quotient ring* R/I is defined as the set of all cosets of I in R; i.e.,

$$R/I := \{a + I : a \in R\}. \tag{1.19}$$

Addition and multiplication in R/I are defined as follows: for all $a, b \in R$,

$$(a + I) + (b + I) := (a + b) + I, \tag{1.20}$$
$$(a + I) \cdot (b + I) := (a \cdot b) + I. \tag{1.21}$$

Of course, we must verify that these operations are well-defined. Note that I is a normal subgroup of $(R, +)$ since R is abelian under addition, so R/I is an abelian group under addition. We verify that multiplication is well-defined as follows: let $a, a', b, b' \in R$ such that $a + I = a' + I$ and $b + I = b' + I$. Then, there exist $i_1, i_2 \in I$ such that $a' = a + i_1$ and $b' = b + i_2$. Thus,

$$\begin{aligned}(a' \cdot b') + I &= ((a + i_1) \cdot (b + i_2)) + I = (a \cdot b + a \cdot i_2 + i_1 \cdot b + i_1 \cdot i_2) + I \\ &= (a \cdot b) + I,\end{aligned} \tag{1.22}$$

since $a \cdot i_2, i_1 \cdot b, i_1 \cdot i_2 \in I$. Therefore, multiplication is well-defined. Moreover, it is easy to verify that R/I is a ring with unity under these operations, where the additive identity is $0 + I$ and the multiplicative identity is $1 + I$. One also has the *quotient map* naturally defined as

$$q : R \to R/I, \quad q(a) = a + I \quad \text{for all } a \in R. \tag{1.23}$$

It is easy to verify that q is a ring epimorphism with kernel I. The most common example of a quotient ring is $\mathbb{Z}/n\mathbb{Z}$, which is isomorphic to the quotient ring $\mathbb{Z}/(n\mathbb{Z})$.

Example 1.30. In the ring $\mathbb{Q}[x]$, let $I = (x^2 - 2) = (x^2 - 2)\mathbb{Q}$. Then, the quotient $\mathbb{Q}[x]/(x^2 - 2)$ is indeed a quotient ring. It is also a field, and may be written as $\mathbb{Q}[\sqrt{2}]$. However, the quotient ring $\mathbb{R}[x]/(x^2 - 2)$ is not an integral domain since $(x - \sqrt{2} + I)(x + \sqrt{2} + I) = x^2 - 2 + I = I$.

We are now fit to show the isomorphism theorems for rings.

Theorem 1.31 (The *first isomorphism theorem* for rings)**.** *Let $\varphi : R \to S$ be a ring homomorphism. Let $I = \ker \varphi$. Then there exists a unique ring monomorphism $\overline{\varphi} : R/I \to S$ such that $\varphi = \overline{\varphi} \circ q$, where $q : R \to R/I$ is the quotient map. Moreover, if φ is surjective, then $\overline{\varphi}$ is a ring isomorphism.*

Proof. Define the map $\overline{\varphi} : R/I \to S$ as follows: for all $a + I \in R/I$, let

$$\overline{\varphi}(a + I) = \varphi(a). \tag{1.24}$$

We must verify that this map is well-defined. Let $a, b \in R$ such that $a + I = b + I$. Then, there exists some $i \in I$ such that $b = a + i$. Thus,

$$\varphi(b) = \varphi(a + i) = \varphi(a) + \varphi(i) = \varphi(a) + 0_S = \varphi(a), \tag{1.25}$$

so $\overline{\varphi}$ is well-defined. It is easy to verify that $\overline{\varphi}$ is a ring homomorphism. Also, for all $a \in R$,

$$(\overline{\varphi} \circ q)(a) = \overline{\varphi}(a + I) = \varphi(a), \tag{1.26}$$

so $\varphi = \overline{\varphi} \circ q$.

Now, suppose that $\overline{\varphi}(a + I) = 0_S$ for some $a + I \in R/I$. Then, $\varphi(a) = 0_S$, so $a \in I$. Thus, $a + I = I$, which is the additive identity in R/I. Therefore, $\overline{\varphi}$ is injective.

Finally, if φ is surjective, then for any $s \in S$, there exists some $a \in R$ such that $\varphi(a) = s$. Thus,

$$\overline{\varphi}(a + I) = \varphi(a) = s, \tag{1.27}$$

so $\overline{\varphi}$ is surjective as well. Therefore, $\overline{\varphi}$ is a ring isomorphism. ■

Proposition 1.32. *Let R be a ring and I be an ideal of R. Then there is a bijection between the set of all ideals of R containing I and the set of all ideals of the quotient ring R/I.*

Proof. We make use of the quotient map $q : R \to R/I$. Let J be an ideal of R such that $I \subseteq J$. The bijection is given by sending J to $J/I := q(J) = \{a + I : a \in J\}$, and sending K, an ideal of R/I, to $q^{-1}(K) = \{a \in R : q(a) \in K\}$. We first show that $q(J) = J/I$ is indeed an ideal of R/I, for J an ideal of R containing I. Let $x + I \in J/I$ and $r + I \in R/I$. Then, $(r + I)(x + I) = (r \cdot x) + I$. Since $x \in J$ and J is an ideal of R, we have $r \cdot x \in J$, so $(r + I)(x + I) \in J/I$. Also note that for all $x + I, y + I \in J/I$, we have $(x + I) + (y + I) = (x + y) + I \in J/I$ since $x, y \in J$ and J is an ideal of R. Thus, J/I is an ideal of R/I.

On the other hand, we show that $q^{-1}(K)$ is an ideal of R for K an ideal of R/I. Let $x, y \in q^{-1}(K)$. Then, $q(x), q(y) \in K$, so $q(x + y) = q(x) + q(y) \in K$ since K is an ideal of R/I. Thus, $x + y \in q^{-1}(K)$. Also, for any $r \in R$ and $x \in q^{-1}(K)$, we have $q(r), q(x) \in R/I$ and $q(x) \in K$, so $q(r \cdot x) = q(r) \cdot q(x) \in K$ since K is an ideal of R/I. Thus, $r \cdot x \in q^{-1}(K)$. Therefore, $q^{-1}(K)$ is an ideal of R. Also, if $x \in I$, then $q(x) = x + I = I$, which is the additive identity in R/I and thus belongs to every ideal of R/I. Therefore, $I \subseteq q^{-1}(K)$.

To show that the maps are inverses of each other is left as an exercise. ■

Theorem 1.33 (The *second isomorphism theorem* for rings)**.** *Let R be a ring, and let $S \subseteq R$ be a subring containing the unity. Let I be an ideal of R. Then, $S + I = \{s + i : s \in S, i \in I\}$ is a subring of R containing the unity, $S \cap I$ is an ideal of S, and there is a ring isomorphism*

$$(S + I)/I \cong S/(S \cap I). \tag{1.28}$$

Proof. Let $\alpha, \beta \in S + I$. Then $\alpha = s + x$ and $\beta = s' + y$ for some $s, s' \in S$ and $x, y \in I$. Thus, $\alpha + \beta = (s + s') + (x + y) \in S + I$ since S is a subring and I is an ideal. Also, $\alpha \cdot \beta = (s + x)(s' + y) = ss' + sy + xs' + xy \in S + I$ since $ss' \in S$, $sy, xs', xy \in I$. Therefore, $S + I$ is a subring of R containing the unity.

Note that the inclusion map $i : S \to R$ is a ring homomorphism. Thus, by the proposition above, $S \cap I = i^{-1}(I)$ is an ideal of S. Also, $I \subseteq S + I$ is an ideal of $S + I$. Now let $\varphi : S \to (S + I)/I$ be the map $\varphi = q \circ i$, where $q : S + I \to (S + I)/I$ is the quotient map. It is easy to verify that φ is a ring homomorphism with kernel

$$\ker \varphi = \{a \in S \mid q \circ i(a) = I\} = \{a \in S \mid a + I = I\} = S \cap I. \tag{1.29}$$

Moreover, φ is surjective since for any $s + i + I \in (S + I)/I$ where $s \in S$ and $i \in I$, we have $\varphi(s) = s + I = s + i + I$. Thus, by the first isomorphism theorem, we have the desired isomorphism. ■

January 30th.

Theorem 1.34 (The *third isomorphism theorem* for rings)**.** *Let R be a ring, and let $J \subseteq I$ be two ideals of R. Then, $I/J = \{a + J : a \in I\}$ is an ideal of the quotient ring R/J, and there is a ring isomorphism*

$$(R/J)/(I/J) \cong R/I. \tag{1.30}$$

Proof. Let $q_R : R \to R/J$ be the quotient map, and $q_{R/J} : R/J \to (R/J)/(I/J)$ be the quotient map. Thus, the composition $\varphi = q_{R/J} \circ q_R : R \to (R/J)/(I/J)$ is a surjective ring homomorphism. The kernel of φ is given by

$$\ker \varphi = \{x \in R \mid \varphi(x) = J + I/J\} = \{x \in R \mid q_R(x) \in I/J\} = \{x \in R \mid x + J \in I/J\} = I. \tag{1.31}$$

Thus, by the first isomorphism theorem, we have the desired isomorphism. ■

We look at some applications of the isomorphism theorems.

Example 1.35. Let $I = (5) \subseteq \mathbb{Z}[x]$. We claim that $\mathbb{Z}[x]/5\mathbb{Z}[x] \cong (\mathbb{Z}/5\mathbb{Z})[x]$. To see this, we make use of the first isomorphism theorem. Let $\varphi : \mathbb{Z}[x] \to (\mathbb{Z}/5\mathbb{Z})[x]$ be the map defined by

$$\varphi\left(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\right) = \bar{a}_0 + \bar{a}_1x + \bar{a}_2x^2 + \cdots + \bar{a}_nx^n, \tag{1.32}$$

where $\bar{a}_i$ is the image of a_i in $\mathbb{Z}/5\mathbb{Z}$ for all $0 \le i \le n$. It is easy to verify that φ is a surjective ring homomorphism with kernel $5\mathbb{Z}[x]$. Thus, by the first isomorphism theorem, we have the desired isomorphism.

Example 1.36. Let $(x) \subseteq \mathbb{Z}[x]$. We claim that $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. To see this, we make use of the second isomorphism theorem. Let $S = \mathbb{Z} \subseteq \mathbb{Z}[x]$. Then, $S + (x) = \mathbb{Z}[x]$ since for any $f(x) \in \mathbb{Z}[x]$, we have $f(x) = f(0) + (f(x) - f(0)) \in S + (x)$. Also, $S \cap (x) = \{0\}$ since the only constant polynomial in (x) is the zero polynomial. Thus, by the second isomorphism theorem, we have

$$\mathbb{Z}[x]/(x) \cong S/(S \cap (x)) = S/\{0\} \cong \mathbb{Z}. \tag{1.33}$$

Example 1.37. Again, let $I = (x^2 - 4, 2) \subseteq \mathbb{Z}[x]$. We claim the isomorphism

$$\mathbb{Z}[x]/(x^2 - 4, 2) \cong \mathbb{Z}/2\mathbb{Z}[x]/(x^2). \tag{1.34}$$

To see this, we make use of the third isomorphism theorem. Let $J = (2) \subseteq I$. Then, by the third isomorphism theorem, we have

$$\mathbb{Z}[x]/I \cong (\mathbb{Z}[x]/J)/(I/J) \cong (\mathbb{Z}/2\mathbb{Z})[x]/(x^2 - 4 + J) = (\mathbb{Z}/2\mathbb{Z})[x]/(x^2), \tag{1.35}$$

since $x^2 - 4 + J = x^2 + J$ in $(\mathbb{Z}/2\mathbb{Z})[x]$.

1.5 Prime and Maximal Ideals

Definition 1.38. Let R be a ring. An ideal $P \subseteq R$ is called a *prime ideal* if $P \neq R$ and for all $a, b \in R$ such that $a \cdot b \in P$, we have either $a \in P$ or $b \in P$.

Of course, the most common example of a prime ideal is (0_R) in an integral domain R. Another example is $(p) = p\mathbb{Z}$ in $\mathbb{Z}$ for any prime p. Note that if R is a field, then the only prime ideal of R is (0_R).

Theorem 1.39. *Let I be an ideal of a ring R. Then, I is a prime ideal if and only if the quotient ring R/I is an integral domain.*

Proof. Suppose that R/I is an integral domain. Let $a, b \in R$ such that $a \cdot b \in I$. Then,

$$(a + I)(b + I) = (a \cdot b) + I = I, \tag{1.36}$$

which is the zero element in R/I. Since R/I is an integral domain, either $a + I = I$ or $b + I = I$, which implies that either $a \in I$ or $b \in I$. Thus, I is a prime ideal. If we now suppose that I is a prime ideal, let $a + I, b + I \in R/I$ such that $(a + I)(b + I) = (a \cdot b) + I = I$. This implies that $a \cdot b \in I$, so either $a \in I$ or $b \in I$. Thus, either $a + I = I$ or $b + I = I$, so R/I is an integral domain. ■

One can also show that there is the natural bijection between ideals of R/I and ideals of R containing I restricts to a bijection between prime ideals of R/I and prime ideals of R containing I.

Example 1.40. We can use this theorem to show (x^2+1) is a prime ideal of $\mathbb{Z}[x]$. Indeed, look at the ring homomorphism $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[i]$ defined by $\varphi(f) = f(i)$ for all $f \in \mathbb{Z}[x]$. For the kernel, let $f \in \ker\varphi$. By the division algorithm, there exist unique $q, r \in \mathbb{Z}[x]$ such that

$$f(x) = (x^2+1)q(x) + r(x), \tag{1.37}$$

where either $r(x) = 0$ or $\deg r < 2$. Plugging in $x = i$ gives $f(i) = 0 = r(i)$. The only way an at most linear polynomial $r(x)$ can be 0 at $x = i$ is if r is the zero polynomial. Hence, $\ker\varphi = (x^2+1)$. Since $\mathbb{Z}[i]$ is an integral domain, by the first isomorphism theorem, we have

$$\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i] \tag{1.38}$$

showing that (x^2+1) is a prime ideal of $\mathbb{Z}[x]$.

Another notion is the maximal ideal.

Definition 1.41. Let R be a ring. An ideal $M \subseteq R$ is called a *maximal ideal* if $M \neq R$ and there are no ideals I of R such that $M \subsetneq I \subsetneq R$.

That is, if J is an ideal such that $M \subseteq J$, then either $J = M$ or $J = R$. For example, in $\mathbb{Z}$, the ideals $(p) = p\mathbb{Z}$ for prime p are maximal ideals. Note that if R is a field, then the only maximal ideal of R is (0_R). In fact, it may be shown that R is a field if and only if (0) and R are the only ideals.

February 2nd.

Theorem 1.42. *Let I be an ideal of a ring R. Then, I is a maximal ideal if and only if the quotient ring R/I is a field.*

Proof. We work with a set of equivalences. $I \subseteq R$ is a maximal ideal $\iff \{J \mid I \subseteq J \subseteq R\} = \{I, R\}$ $\iff \{K \mid K \text{ is an ideal of } R/I\} = \{I/I, R/I\} \iff R/I$ is a field. ■

A neat corollary of this theorem is that every maximal ideal is a prime ideal. Indeed, if M is a maximal ideal of R, then R/M is a field, and thus an integral domain. Therefore, by the previous theorem, M is a prime ideal. Another theorem guarantees the existence of maximal ideals.

Theorem 1.43. *Every non-zero ring has at least a maximal ideal.*

This theorem, though true in many common cases, requires Zorn's lemma for a general proof.

Proof. Let $(\Omega, \subseteq)$ be the set of all proper ideals of a ring R, ordered by inclusion. Note that $R \supsetneq (0) \in \Omega$, so $\Omega \neq \emptyset$. Zorn's lemma states that if every chain in Ω has an upper bound in Ω, then Ω has a maximal element. Let $\mathcal{C}$ be a chain in Ω. We claim that $I_{\mathcal{C}} = \bigcup_{I \in \mathcal{C}} I$ is an upper bound of $\mathcal{C}$ in Ω. Certainly, for any $I \in \mathcal{C}$, we have $I \subseteq J$. Also, we must verify that $I_{\mathcal{C}}$ is a proper ideal of R.

Let $x, y \in I_{\mathcal{C}}$, and $r \in R$. Then there exist two ideals $I, J \in \mathcal{C}$ such that $x \in I$ and $y \in J$. Since $\mathcal{C}$ is a chain, without loss of generality, suppose that $I \subseteq J$. Thus, $x, y \in J$, so $x + y \in R$ and $r \cdot x \in R$ since J is an ideal of R. Therefore, $I_{\mathcal{C}}$ is an ideal of R. Also, if $I_{\mathcal{C}} = R$, then $1_R \in I_{\mathcal{C}}$, so there exists some ideal $I \in \mathcal{C}$ such that $1_R \in I$. This implies that $I = R$, which contradicts the fact that I is a proper ideal. Thus, $I_{\mathcal{C}}$ is a proper ideal of R, so $I_{\mathcal{C}} \in \Omega$. Therefore, by Zorn's lemma, Ω has a maximal element, which is a maximal ideal of R. ■

Example 1.44. In $\mathbb{C}[x]$, the ideal (x) is maximal since $\mathbb{C}[x]/(x) \cong \mathbb{C}$, which is a field. However, (x^2) is not maximal since $(x^2) \subsetneq (x)$. Another reasoning is that $\mathbb{C}[x]/(x^2)$ is not a field since $(x + (x^2)) \cdot (x + (x^2)) = x^2 + (x^2) = 0 + (x^2)$; it is not an integral domain either, so (x^2) is not even prime. In fact, the maximal ideals of $\mathbb{C}[x]$ are precisely of the form $(x - a)$ for some $a \in \mathbb{C}$.

Index