

# RINGS AND MODULES

Manish Kumar, notes by Ramdas Singh

Fourth Semester

# Contents

1	RINGS	1
1.1	Properties and Maps . . . . .	1
1.1.1	Polynomials . . . . .	3
1.2	Ideals . . . . .	4
1.3	Other Rings . . . . .	6
1.4	Quotient Rings and Isomorphism Theorems . . . . .	7
1.5	Prime and Maximal Ideals . . . . .	9
1.5.1	Jacobson Radical and Nilradical . . . . .	11
1.6	Product of Rings . . . . .	12
1.6.1	Idempotents . . . . .	13
1.7	Generalizing Properties of Integers . . . . .	14
	Index	21

## Chapter 1

# 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

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (1.1)$$

$$(a + b) \cdot c = a \cdot c + b \cdot c. \quad (1.2)$$

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,

$$a \cdot 0_R = a \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R \implies a \cdot 0_R = 0_R \quad (1.3)$$

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

- Let  $a \in R$ . Then,

$$(-1_R \cdot a) + a = (-1_R + 1_R) \cdot a = 0_R \implies -1_R \cdot a = -a. \quad (1.4)$$

■

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  $\varphi : (R, +, \cdot) \rightarrow (S, \oplus, \odot)$  between two rings such that for all  $a, b \in R$ , we have

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

Most of the time, we shall drop  $\oplus$  and  $\odot$  when the context is clear. Some examples of ring homomorphisms include the map  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$  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  $\mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$  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  $\varphi : R \rightarrow S$  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  $\varphi : R \rightarrow S$  is bijective, then its inverse  $\varphi^{-1} : S \rightarrow R$  is a ring homomorphism. We look at some examples of rings and mappings.

**Example 1.7.** Let  $X$  be any set and let  $R := \{f : X \rightarrow \mathbb{R}\}$  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  $0 : X \rightarrow \mathbb{R}$  defined by  $0(x) = 0$  for all  $x \in X$ , and the multiplicative identity is the constant function  $1 : X \rightarrow \mathbb{R}$  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  $\varphi : R \rightarrow \mathbb{R}^n$  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 defines  $C^n([a, b], \mathbb{R})$  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  $\varphi : \mathbb{Z}[i] \rightarrow \mathbb{Z}^2$  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

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

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

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

and multiplication is defined as

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

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

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad (1.9)$$

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  $\iota : R \rightarrow R[x]$  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,

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

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  $\iota$  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  $R[x_1, x_2, \dots, x_n]$  for any  $n \in \mathbb{N}$ . For a countable number of indeterminates, one may define  $R[x_1, x_2, x_3, \dots]$  as the union  $\bigcup_{n=1}^{\infty} R[x_1, x_2, \dots, x_n]$ .

**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  $a_0 + a_1e + a_2e^2 + \cdots + a_ne^n$  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  $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[e]$  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  $f : R \rightarrow S$  be a ring homomorphism between two commutative rings with unity. Then, the kernel of  $f$ , defined as*

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

*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,

$$f(a + b) = f(a) + f(b) = 0_S + 0_S = 0_S, \quad (1.13)$$

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

$$f(r \cdot a) = f(r) \cdot f(a) = f(r) \cdot 0_S = 0_S, \quad (1.14)$$

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,

$$f(a - b) = f(a) - f(b) = 0_S, \quad (1.15)$$

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 collection of subrings of  $R$  containing the unity. 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*

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

*Proof.* Let  $S \subseteq I$ , a subset of an ideal. We claim that  $(S) \subseteq I$ . Let  $\alpha \in (S)$ . 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  $\{x_1, \dots, x_n\} \subseteq R$ , then  $I = (x_1, \dots, x_n) = Rx_1 + \cdots + Rx_n$  is the ideal generated by  $x_1, \dots, x_n$ . Let us look at some examples.

**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  $f : G \rightarrow k$  such that  $f(x) = 0$  for all but finitely many  $x \in G$ . Addition is defined pointwise as

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

and multiplication is defined as

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

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

If  $G$  is a finite group with  $G = \{e, x_2, \dots, x_n\}$  then  $R[G] = \{a_1e + a_2x_2 + \dots + a_nx_n \mid a_i \in \mathbb{C}\}$ . 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.,

$$R/I := \{a + I : a \in R\}. \quad (1.19)$$

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

$$(a + I) + (b + I) := (a + b) + I, \quad (1.20)$$

$$(a + I) \cdot (b + I) := (a \cdot b) + I. \quad (1.21)$$

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,

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

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

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

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  $\varphi : R \rightarrow S$  be a ring homomorphism. Let  $I = \ker \varphi$ . Then there exists a unique ring monomorphism  $\bar{\varphi} : R/I \rightarrow S$  such that  $\varphi = \bar{\varphi} \circ q$ , where  $q : R \rightarrow R/I$  is the quotient map. Moreover, if  $\varphi$  is surjective, then  $\bar{\varphi}$  is a ring isomorphism.*

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

$$\bar{\varphi}(a + I) = \varphi(a). \quad (1.24)$$

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,

$$\varphi(b) = \varphi(a + i) = \varphi(a) + \varphi(i) = \varphi(a) + 0_S = \varphi(a), \quad (1.25)$$

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

$$(\bar{\varphi} \circ q)(a) = \bar{\varphi}(a + I) = \varphi(a), \quad (1.26)$$

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

Now, suppose that  $\bar{\varphi}(a + I) = 0_S$  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,  $\bar{\varphi}$  is injective.

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

$$\bar{\varphi}(a + I) = \varphi(a) = s, \quad (1.27)$$

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

**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  $q : R \rightarrow R/I$ . 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.  $\blacksquare$

**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*

$$(S + I)/I \cong S/(S \cap I). \quad (1.28)$$

*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  $i : S \rightarrow R$  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  $\varphi : S \rightarrow (S + I)/I$  be the map  $\varphi = q \circ i$ , where  $q : S + I \rightarrow (S + I)/I$  is the quotient map. It is easy to verify that  $\varphi$  is a ring homomorphism with kernel

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

Moreover,  $\varphi$  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.  $\blacksquare$

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*

$$(R/J)/(I/J) \cong R/I. \quad (1.30)$$

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

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

Thus, by the first isomorphism theorem, we have the desired isomorphism.  $\blacksquare$

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  $\varphi : \mathbb{Z}[x] \rightarrow (\mathbb{Z}/5\mathbb{Z})[x]$  be the map defined by

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

where  $\bar{a}_i$  is the image of  $a_i$  in  $\mathbb{Z}/5\mathbb{Z}$  for all  $0 \leq i \leq n$ . It is easy to verify that  $\varphi$  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

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

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

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

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

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

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,

$$(a + I)(b + I) = (a \cdot b) + I = I, \quad (1.36)$$

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.  $\blacksquare$

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  $\varphi : \mathbb{Z}[x] \rightarrow \mathbb{Z}[i]$  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

$$f(x) = (x^2 + 1)q(x) + r(x), \quad (1.37)$$

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

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

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  $\iff \{J \mid I \subseteq J \subseteq R\} = \{I, R\}$   
 $\iff \{K \mid K \text{ is an ideal of } R/I\} = \{I/I, R/I\} \iff R/I \text{ is a field.}$  ■

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  $\Omega$  has an upper bound in  $\Omega$ , then  $\Omega$  has a maximal element. Let  $\mathcal{C}$  be a chain in  $\Omega$ . We claim that  $I_{\mathcal{C}} = \bigcup_{I \in \mathcal{C}} I$  is an upper bound of  $\mathcal{C}$  in  $\Omega$ . Certainly, for any  $I \in \mathcal{C}$ , we have  $I \subseteq I_{\mathcal{C}}$ . 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  $x + y \in J$  and  $r \cdot x \in J$  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,  $\Omega$  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  $a \in \mathbb{C}$ .

### 1.5.1 Jacobson Radical and Nilradical

February 5th.

**Definition 1.45.** The *Jacobson radical* of a non-zero ring  $R$  is defined as

$$\text{Jac}(R) = \bigcap_{\substack{\mathfrak{m} \subseteq R \\ \mathfrak{m} \text{ is a maximal ideal}}} \mathfrak{m}. \quad (1.39)$$

It is the interseciton of ideals, so it is also an ideal. The *nilradical* of  $R$  is defined as

$$\text{nil}(R) = \{x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{N}\}. \quad (1.40)$$

The following are some properties of the Jacobson radical and nilradical.

**Proposition 1.46.** *Let  $R$  be a ring. Then,*

1.  $\text{nil}(R)$  is an ideal of  $R$ .
2.  $\text{nil}(R) \subseteq \text{Jac}(R)$ .
3.  $x \in \text{Jac}(R)$  if and only if  $1 + ax$  is a unit for all  $a \in R$ .
4.  $\text{nil}(R) = \bigcap_{\substack{P \subseteq R \\ P \text{ is a prime ideal}}} P$ .

*Proof.* 1. Let  $x, y \in \text{nil}(R)$  and  $r \in R$ . Then, there exist  $m, n \in \mathbb{N}$  such that  $x^m = 0$  and  $y^n = 0$ . Thus,  $(x + y)^{m+n} = 0$  by the binomial theorem, so  $x + y \in \text{nil}(R)$ . Also,  $(r \cdot x)^m = r^m \cdot x^m = 0$ , so  $r \cdot x \in \text{nil}(R)$ . Therefore,  $\text{nil}(R)$  is an ideal of  $R$ .

2. Let  $x \in \text{nil}(R)$ . Then, there exists some  $n \in \mathbb{N}$  such that  $x^n = 0$ . Thus  $x^n$  belongs to every ideal of  $R$ , so in particular,  $x^n \in P$  for every prime ideal and  $x^n \in \mathfrak{m}$  for every maximal ideal. However,  $x^n \in P$  implies that  $x \in P$  since  $P$  is prime, and  $x^n \in \mathfrak{m}$  implies that  $x \in \mathfrak{m}$  since  $\mathfrak{m}$  is prime as well. Therefore,  $x$  belongs to every prime ideal and every maximal ideal, so  $x \in \text{Jac}(R)$ . Hence,  $\text{nil}(R) \subseteq \text{Jac}(R)$ .

3. For the forward implication, let  $x \in \text{Jac}(R)$  and  $a \in R$ . Note that  $ax$  cannot be a unit since it is contained in the (maximal) ideals  $\mathfrak{m}$ . Suppose  $1 + ax$  is *not* a unit. Then  $I = (1 + ax)$  is a proper ideal of  $R$ . If  $q : R \rightarrow R/I$  is the quotient map, and  $\bar{\mathfrak{m}}$  is a maximal ideal of  $R/I$ , then we claim that  $\mathfrak{m} = q^{-1}(\bar{\mathfrak{m}})$  is a maximal ideal of  $R$  containing  $I$ . Certainly,  $\mathfrak{m}$  is an ideal of  $R$  containing  $I$  by the proposition above. Also, if there exists some ideal  $J$  of  $R$  such that  $\mathfrak{m} \subsetneq J \subsetneq R$ , then  $I \subseteq J \subsetneq R$ , so  $q(J)$  is an ideal of  $R/I$  such that  $\bar{\mathfrak{m}} \subsetneq q(J) \subsetneq R/I$ , contradicting the maximality of  $\bar{\mathfrak{m}}$ . Thus,  $\mathfrak{m}$  is a maximal ideal of  $R$ . However, since  $x \in \text{Jac}(R)$ , we have  $x \in \mathfrak{m}$ , so  $ax \in I \subseteq \mathfrak{m}$ . This implies that  $1 = (1 + ax) - ax \in \mathfrak{m}$ , a contradiction. Therefore,  $1 + ax$  is a unit for all  $a \in R$ .

For the converse, suppose  $1 + ax$  is a unit for all  $a \in R$ . Let  $\mathfrak{m}$  be any maximal ideal of  $R$ . If  $x \notin \mathfrak{m}$ , then the ideal  $(\mathfrak{m}, x)$  properly contains  $\mathfrak{m}$ , so  $(\mathfrak{m}, x) = R$ . Thus, there exist  $m \in \mathfrak{m}$  and  $r \in R$  such that  $1 = m + r \cdot x$ . This implies that  $1 - r \cdot x = m \in \mathfrak{m}$ , contradicting the fact that  $1 - r \cdot x$  is a unit. Therefore,  $x \in \mathfrak{m}$ . Since  $\mathfrak{m}$  was an arbitrary maximal ideal, we have  $x \in \text{Jac}(R)$ .

4. It is clear that  $\text{nil}(R) \subseteq \bigcap_{P \text{ prime}} P$  since maximal ideals are prime ideals. For the converse inclusion, let  $x \in \bigcap_{P \text{ prime}} P$ . We claim that  $x$  is nilpotent. Suppose not. Then, the set  $S = \{x^n : n \in \mathbb{N}\}$  does not contain 0. Define the set  $\Omega = \{I \subseteq R \mid I \text{ is an ideal and } I \cap S = \emptyset\}$ . Inclusion  $\subseteq$  is a partial order on  $\Omega$ . Let  $\mathcal{C}$  be a chain in  $\Omega$  and let  $I = \bigcup_{J \in \mathcal{C}} J$ . We claim that  $I$  is an upper bound of  $\mathcal{C}$  in  $\Omega$ . It is an ideal since if  $z, y \in I$ , then  $z \in J_1$  and  $y \in J_2$  with  $J_1 \subseteq J_2$ . Thus,  $z, y \in J_1 \cup J_2$ , so  $z + y \in J_1 \cup J_2 \subseteq I$ . Also, for any  $r \in R$  and  $z \in I$ , we have  $z \in J$  for some  $J \in \mathcal{C}$ , so  $r \cdot z \in J \subseteq I$ . Therefore,  $I$  is an ideal. Moreover, if  $J \cap S = \emptyset$  for all  $J \in \mathcal{C}$  tells us  $I \cap S = \emptyset$ . Hence,  $I$  is a valid upper bound, and Zorn's lemma guarantess the existence of a maximal  $P$  in  $\Omega$ . We further claim that  $P$  is a prime ideal of  $R$ . Indeed,  $P \subsetneq R$  since  $P \cap S = \emptyset$ . Let  $uv \in P$  for some  $u, v \in R$ . If both  $u, v \notin P$ , then the ideals  $(P, u)$  and  $(P, v)$  properly contain  $P$ ; that is,  $au + y = x^n$  and  $bv + z = x^m$  for some  $a, b \in R, y, z \in P$ , and  $n, m \in \mathbb{N}$ . Thus,  $(au + y)(bv + z) = x^{n+m} \in S$ , but

$(au + y)(bv + z) = abuv + az + by + yz \in P$  since  $uv \in P$  and  $y, z \in P$ . This contradicts the fact that  $P \cap S = \emptyset$ . Therefore, either  $u \in P$  or  $v \in P$ , so  $P$  is a prime ideal. However, by construction,  $x$  is in every prime ideal of  $R$ , so  $x \in P$ , contradicting the fact that  $P \cap S = \emptyset$ . Hence,  $x$  is nilpotent, so  $x \in \text{nil}(R)$ . ■

February 6th.

Let us look at some examples.

**Example 1.47.** In  $\mathbb{Z}$ ,  $\text{nil}(\mathbb{Z}) = \{0\}$  since the only nilpotent element is 0. Also,  $\text{Jac}(\mathbb{Z}) = \{0\}$  since the intersection of all maximal ideals  $(p)$  for prime  $p$  is  $\{0\}$ . In the ring  $\mathbb{Z}/6\mathbb{Z}$ , the nilradical is  $\{0\}$  even though it is not an integral domain. The Jacobson radical is  $\{0\}$  as well since the maximal ideals are  $(2)$  and  $(3)$ , whose intersection is  $\{0\}$ .

**Example 1.48.** For a non-trivial example, let us look at the ring  $R = \mathbb{Z}/4\mathbb{Z}$ . The nilradical of  $R$  is  $\{0, 2\}$  since  $2^2 = 0$  in  $R$ . The Jacobson radical of  $R$  is also  $\{0, 2\}$  since the only maximal ideal of  $R$  is  $(2)$ . If we take  $R = \mathbb{Q}[x, y]/(x^2, y)$ , then  $\text{nil}(R) = (x)$  since  $x$  is nilpotent. The Jacobson radical of  $R$  is also  $(x)$ .

**Example 1.49.** For an example where the Jacobson radical is strictly larger than the nilradical, consider the power series ring  $R = \mathbb{Q}[[x]]$ . If  $f \in \mathbb{Q}[[x]]$ , then  $f$  is a unit if and only if the constant term of  $f$  is non-zero; if  $f = a_0(1 - g)$  where  $a_0 \in \mathbb{Q}$  and  $g \in (x)$ , then  $f^{-1} = a_0^{-1}(1 - g)^{-1}$ , where  $(1 - g)^{-1}$  is given by the geometric series expansion  $(1 - g)^{-1} = 1 + g + g^2 + \dots$ . Thus,  $\text{Jac}(R) = (x)$  since  $1 + ax$  is a unit for all  $a \in R$ . However,  $\text{nil}(R) = \{0\}$  since there are no non-zero nilpotent elements in  $R$ .

## 1.6 Product of Rings

Let  $R_1, R_2, \dots, R_n$  be rings. We can define the *product ring*  $R_1 \times R_2 \times \dots \times R_n$  as the set of all  $n$ -tuples  $(r_1, r_2, \dots, r_n)$  where  $r_i \in R_i$  for all  $1 \leq i \leq n$ , with addition and multiplication defined componentwise. It is easy to verify that  $R_1 \times R_2 \times \dots \times R_n$  is also a ring, and the unity is given by  $(1_{R_1}, 1_{R_2}, \dots, 1_{R_n})$ . The *projection map*  $p_i : R_1 \times R_2 \times \dots \times R_n \rightarrow R_i$  is defined by  $p_i(r_1, r_2, \dots, r_n) = r_i$  for all  $1 \leq i \leq n$ . It is, again, easy to verify that  $p_i$  is a surjective ring homomorphism with kernel  $R_1 \times \dots \times R_{i-1} \times \{0_{R_i}\} \times R_{i+1} \times \dots \times R_n$ . Conversely, the *inclusion map*  $e_i : R_i \rightarrow R_1 \times R_2 \times \dots \times R_n$  is defined by  $e_i(r) = (0_{R_1}, \dots, 0_{R_{i-1}}, r, 0_{R_{i+1}}, \dots, 0_{R_n})$  for all  $r \in R_i$ . It is easy to verify that  $e_i$  is an injective ring homomorphism with image  $\{0_{R_1}\} \times \dots \times \{0_{R_{i-1}}\} \times R_i \times \{0_{R_{i+1}}\} \times \dots \times \{0_{R_n}\}$ .

Regarding ideals, we have the following proposition.

**Proposition 1.50.** Let  $R_1, R_2, \dots, R_n$  be rings. Then, every ideal of the product ring  $R_1 \times R_2 \times \dots \times R_n$  is of the form  $I_1 \times I_2 \times \dots \times I_n$  where  $I_i$  is an ideal of  $R_i$  for all  $1 \leq i \leq n$ .

*Proof.* Let  $I$  be an ideal of  $R_1 \times R_2 \times \dots \times R_n$ . For each  $1 \leq i \leq n$ , let  $I_i = p_i(I)$ . We claim that each  $I_i$  is an ideal of  $R_i$  and  $I = I_1 \times I_2 \times \dots \times I_n$ . Let  $x_i, y_i \in I_i$  and  $r_i \in R_i$ . Then, there exist  $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in I$  such that  $p_i(x) = x_i$  and  $p_i(y) = y_i$ . Thus,  $x + y \in I$  since  $I$  is an ideal of the product ring, so  $x_i + y_i = p_i(x + y) \in I_i$ . Also,  $r_i \cdot x_i = p_i(e_i(r_i) \cdot x) \in I_i$  since  $e_i(r_i) \cdot x \in I$ . Therefore,  $I_i$  is an ideal of  $R_i$ .

Let us first show that  $I \supseteq I_1 \times I_2 \times \dots \times I_n$ . Let  $(a_1, a_2, \dots, a_n) \in I_1 \times I_2 \times \dots \times I_n$ . Let  $x^{(i)} \in I$  such that  $p_i(x^{(i)}) = a_i$  for all  $1 \leq i \leq n$ . Then  $e_i(1_{R_i}) \cdot x^{(i)} \in I$  since  $I$  is an ideal of the product ring, and so  $\sum_{i=1}^n e_i(1_{R_i}) \cdot x^{(i)} \in I$  as well. However,  $\sum_{i=1}^n e_i(1_{R_i}) \cdot x^{(i)} = (a_1, a_2, \dots, a_n)$ , so  $(a_1, a_2, \dots, a_n) \in I$ . Therefore,  $I \supseteq I_1 \times I_2 \times \dots \times I_n$ . For the converse inclusion  $I \subseteq I_1 \times I_2 \times \dots \times I_n$ , let  $(a_1, a_2, \dots, a_n) \in I$ . Then,  $a_i = p_i(a_1, a_2, \dots, a_n) \in I_i$  for all  $1 \leq i \leq n$ . Thus,  $(a_1, a_2, \dots, a_n) \in I_1 \times I_2 \times \dots \times I_n$ . Therefore,  $I = I_1 \times I_2 \times \dots \times I_n$ . ■

We now wish to study the prime ideals of the product ring.

**Proposition 1.51.** *Let  $R_1, R_2, \dots, R_n$  be rings. Then  $I \subseteq R_1 \times R_2 \times \dots \times R_n$  is a prime ideal if and only if  $p_i(I) = R_i$  for all  $1 \leq i \leq n$  except for one index  $1 \leq k \leq n$  such that  $p_k(I)$  is a prime ideal of  $R_k$ .*

*Proof.* For the forward direction, let  $I = I_1 \times \dots \times I_n$  (by the previous proposition), where  $I_i = p_i(I)$  is an ideal of  $R_i$ . Note that  $I$  is prime if and only if  $(R_1 \times \dots \times R_n)/I \cong R_1/I_1 \times \dots \times R_n/I_n$  is an integral domain. This implies that  $R_i/I_i$  is an integral domain for one index  $1 \leq k \leq n$  and  $R_i/I_i \cong \{0\}$  for all  $i \neq k$ . If it were otherwise, we could find two indices  $i \neq j$  such that  $R_i/I_i$  and  $R_j/I_j$  are both non-trivial, and  $e_i(1_{R_i}) + I$  and  $e_j(1_{R_j}) + I$  are two non-zero elements in  $R_1/I_1 \times \dots \times R_n/I_n$  whose product is zero, contradicting the fact that  $R_1/I_1 \times \dots \times R_n/I_n$  is an integral domain. Thus,  $p_i(I) = I_i = R_i$  for all  $i \neq k$ , and  $p_k(I) = I_k$  is a prime ideal of  $R_k$ .

Conversely, suppose that  $p_i(I) = R_i$  for all  $1 \leq i \leq n$  except for one index  $1 \leq k \leq n$  such that  $p_k(I)$  is a prime ideal of  $R_k$ . Then,  $(R_1 \times \dots \times R_n)/I \cong R_1/R_1 \times \dots \times R_k/p_k(I) \times \dots \times R_n/R_n \cong R_k/p_k(I)$  is an integral domain since  $p_k(I)$  is a prime ideal of  $R_k$ . Thus,  $I$  is a prime ideal of the product ring. ■

### 1.6.1 Idempotents

**Definition 1.52.** Let  $R$  be a ring. An element  $x \in R$  is called an *idempotent* if  $x^2 = x$ .

**Example 1.53.** Trivially, every ring has two idempotents, namely  $0_R$  and  $1_R$ . If  $R_1$  and  $R_2$  are rings, then  $(1, 1), (0, 0), (1, 0), (0, 1)$  are idempotents of the product ring  $R_1 \times R_2$ .

**Proposition 1.54.** *Let  $R$  be a ring and  $e \in R$  be an idempotent. Then  $1 - e$  is also an idempotent, and  $R \cong eR \times (1 - e)R$ .*

*Proof.* Note that  $(1 - e)e = e - e^2 = 0$ , and  $(1 - e)^2 = (1 - e)(1 - e) = 1 - e$ . To show the isomorphism, let  $\varphi : R \rightarrow eR \times (1 - e)R$  be defined by  $\varphi(r) = (er, (1 - e)r)$  for all  $r \in R$ . It is easy to verify that  $\varphi$  is a ring homomorphism. If we define  $\psi : eR \times (1 - e)R \rightarrow R$  by  $\psi(x, y) = x + y$  for all  $x \in eR$  and  $y \in (1 - e)R$ , then  $\psi$  is also a ring homomorphism. Moreover,  $\psi \circ \varphi(r) = \psi(er, (1 - e)r) = er + (1 - e)r = r$  for all  $r \in R$ , and  $\varphi \circ \psi(x, y) = \varphi(x + y) = (e(x + y), (1 - e)(x + y)) = (x, y)$  for all  $x \in eR$  and  $y \in (1 - e)R$ . Thus,  $\varphi$  is an isomorphism, so  $R \cong eR \times (1 - e)R$ . ■

*February 9th.*

An interesting consequence is the chinese remainder theorem, which is abstracted from the original number-theoretic version. For the below theorem, we define the product of two ideals  $I$  and  $J$  of a ring  $R$  as

$$IJ = \{a_1b_1 + \dots + a_nb_n \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}. \quad (1.41)$$

One may verify that  $IJ$  is an ideal of  $R$ . Moreover,  $IJ \subseteq I \cap J$  since  $a_ib_i \in I$  and  $a_ib_i \in J$  for all  $1 \leq i \leq n$ . However, it is not necessarily the case that  $IJ = I \cap J$ . For example, if  $R = \mathbb{Z}$  and  $I = (2)$  and  $J = (4)$ , then  $IJ = (8)$  but  $I \cap J = (4)$ .

**Theorem 1.55** (The *chinese remainder theorem*). *Let  $R$  be a ring, and  $I_1, I_2, \dots, I_k$  be ideals of  $R$  which are pairwise co-maximal; that is, for all  $1 \leq i \neq j \leq k$ , we have  $I_i + I_j = R$ . Then  $I_1 \cap I_2 \cap \dots \cap I_k = I_1 I_2 \dots I_k$ . Moreover, the natural homomorphism  $\varphi : R \rightarrow R/I_1 \times R/I_2 \times \dots \times R/I_k$  defined by  $\varphi(r) = (r + I_1, r + I_2, \dots, r + I_k)$  is surjective with kernel  $I_1 I_2 \dots I_k$ , so*

$$R/(I_1 I_2 \dots I_k) \cong R/I_1 \times R/I_2 \times \dots \times R/I_k. \quad (1.42)$$

We first determine how this abstract version of the chinese remainder theorem implies the original number-theoretic version. Let  $n_1, n_2, \dots, n_k$  be pairwise coprime positive integers, and let  $m = n_1 n_2 \dots n_k$ . Then, the ideals  $(n_1), (n_2), \dots, (n_k)$  of  $\mathbb{Z}$  are pairwise co-maximal since  $(n_i) + (n_j) = (1)$  for all  $1 \leq i \neq j \leq k$ . Thus, by the chinese remainder theorem, we have

$$\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}, \quad x \mapsto (x + n_1\mathbb{Z}, x + n_2\mathbb{Z}, \dots, x + n_k\mathbb{Z}) \quad (1.43)$$



is surjective with kernel  $(m)$ . That is, given any  $(a_1 + n_1\mathbb{Z}, a_2 + n_2\mathbb{Z}, \dots, a_k + n_k\mathbb{Z}) \in \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$ , there exists some integer  $x$  such that  $x \equiv a_i \pmod{n_i}$  for all  $1 \leq i \leq k$ , and any two such integers are congruent modulo  $m$ . Moreover, we have the isomorphism

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}. \quad (1.44)$$

*Proof.* We first show for  $k = 2$ . Let  $I_1$  and  $I_2$  be two ideals of  $R$  such that  $I_1 + I_2 = R$ . Then, there exist  $a \in I_1$  and  $b \in I_2$  such that  $a + b = 1$ . We already know that  $I_1 I_2 \subseteq I_1 \cap I_2$ , so we only need to show the converse inclusion. Let  $x \in I_1 \cap I_2$ . Then,  $x = x(a + b) = xa + xb \in I_1 I_2$  since  $xa \in I_1 I_2$  and  $xb \in I_1 I_2$ . Therefore,  $I_1 \cap I_2 = I_1 I_2$ . We now wish to show the natural map  $R \rightarrow R/I_1 \times R/I_2$  defined by  $r \mapsto (r + I_1, r + I_2)$  is surjective with kernel  $I_1 I_2$ . It is easy to verify that the map is a ring homomorphism. For surjectivity, since any element of  $R/I_1 \times R/I_2$  is of the form  $(r_1 + I_1, r_2 + I_2)$  for some  $r_1, r_2 \in R$ , we only show that  $(1 + I_1, 0 + I_2)$  and  $(0 + I_1, 1 + I_2)$  are in the image of the map. Since  $a \in I_1$ , we have  $a + I_1 = 0 + I_1$ , so  $\varphi(b) = (b + I_1, b + I_2) = (1 + I_1, 0 + I_2)$ . Similarly, since  $b \in I_2$ , we have  $b + I_2 = 0 + I_2$ , so  $\varphi(a) = (a + I_1, a + I_2) = (0 + I_1, 1 + I_2)$ . Therefore, the map is surjective. For the kernel, if  $r \in R$  is such that  $\varphi(r) = (r + I_1, r + I_2) = (0 + I_1, 0 + I_2)$ , then  $r \in I_1 \cap I_2 = I_1 I_2$ . Conversely, if  $r \in I_1 I_2$ , then  $r \in I_1 \cap I_2$ , so  $\varphi(r) = (0 + I_1, 0 + I_2)$ . Thus, the kernel of the map is  $I_1 I_2$ . For arbitrary  $k$ , we claim that  $I_1$  and  $I_2 \cdots I_k$  are co-maximal ideals. Since  $I_1$  and  $I_j$  are co-maximal for all  $2 \leq j \leq k$ , there exist  $x_j \in I_1$  and  $y_j \in I_j$  such that  $x_j + y_j = 1$  for all  $2 \leq j \leq k$ . Then

$$(x_2 + y_2)(x_3 + y_3) \cdots (x_k + y_k) = 1 \implies \alpha + y_2 y_3 \cdots y_k = 1 \quad (1.45)$$

where  $\alpha \in I_1$  since  $x_j \in I_1$  for all  $2 \leq j \leq k$ , and  $y_2 \cdots y_k \in I_2 \cdots I_k$ . Thus,  $I_1$  and  $I_2 \cdots I_k$  are co-maximal. Now induction can be applied on  $k$  to show  $I_1 \cap I_2 \cap \dots \cap I_k = I_1 I_2 \cdots I_k$ . To show surjectivity of the natural map  $R \rightarrow R/I_1 \times R/I_2 \times \dots \times R/I_k$ , we show  $e_j := (0 + I_1, \dots, 0 + I_{j-1}, 1 + I_j, 0 + I_{j+1}, \dots, 0 + I_k)$  is in the image of the map for all  $1 \leq j \leq k$ . Since  $I_j$  and  $I_1 \cdots I_{j-1} I_{j+1} \cdots I_k$  are co-maximal, there exist  $x \in I_j$  and  $y \in I_1 \cdots I_{j-1} I_{j+1} \cdots I_k$  such that  $x + y = 1$ . Then  $\varphi(y) = (y + I_1, y + I_2, \dots, y + I_k) = e_j$  since  $y \in I_i$  for all  $i \neq j$  and  $y + I_j = 1 + I_j$ . Therefore, the natural map is surjective with kernel  $I_1 I_2 \cdots I_k$ , so we have the desired isomorphism  $R/(I_1 I_2 \cdots I_k) \cong R/I_1 \times R/I_2 \times \dots \times R/I_k$ . ■

## 1.7 Generalizing Properties of Integers

February 12th.

The ring of integers has several properties, which we axiomatize as properties for more general rings.

**Definition 1.56.** Let  $R$  be an integral domain. Let  $N : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  be a function such that for all  $a, b \in R \setminus \{0\}$ , there exists  $q, r \in R$  such that  $a = bq + r$  and either  $r = 0$  or  $N(r) < N(b)$ . Then, we say that  $R$  is a *euclidean domain* with respect to the euclidean function  $N$ .

Of course, the ring of integers  $\mathbb{Z}$  is a euclidean domain with respect to the euclidean function  $N : \mathbb{Z} \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  defined by  $N(n) = |n|$  for all  $n \in \mathbb{Z} \setminus \{0\}$ . We know this to satisfy the condition that given any  $a, b \in \mathbb{Z} \setminus \{0\}$ , there exist  $q, r \in \mathbb{Z}$  such that  $a = bq + r$  and  $0 \leq r < |b|$ . If  $k$  denotes a field, then  $k[x]$  is a euclidean domain with respect to the euclidean function  $N : k[x] \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  defined by  $N(f) = \deg(f)$  for all  $f \in k[x] \setminus \{0\}$ . We know this to satisfy the condition that given any  $f, g \in k[x] \setminus \{0\}$ , there exist  $q, r \in k[x]$  such that  $f = gq + r$  and either  $r = 0$  or  $\deg(r) < \deg(g)$ .

**Example 1.57.** A *valuation map* on a field  $k$  is a surjective map  $v : k \rightarrow \mathbb{Z} \cup \{\infty\}$  such that  $v(0) = \infty$ ,  $v(ab) = v(a) + v(b)$  and  $v(a + b) \geq \min\{v(a), v(b)\}$  for all  $a, b \in k$ . If  $v$  is a valuation map on  $k$ , then  $R_v = \{x \in k : v(x) \geq 0\}$  is a valid ring with respect to the usual addition and multiplication on  $k$  termed the *valuation ring*. Moreover,  $R_v$  is a euclidean domain with respect to the euclidean function  $N : R_v \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  defined by  $N(x) = v(x)$  for all  $x \in R_v \setminus \{0\}$ . To show that  $N$  satisfies the condition in the definition of euclidean domain, let  $a, b \in R_v \setminus \{0\}$ . If  $v(a) < v(b)$ , then we can take  $q = 0$  and  $r = a$ . If  $v(a) \geq v(b)$ , then we can take  $q = a/b$  so that  $v(a/b) = v(a) - v(b) \geq 0$ , so  $q \in R_v$ , and  $r = a - bq = 0$ . Therefore,  $R_v$  is a euclidean domain with respect to the euclidean function  $N$ .

**Definition 1.58.** Let  $R$  be an integral domain. We say that  $R$  is a *principal ideal domain* if every ideal of  $R$  is principal; that is, for every ideal  $I$  of  $R$ , there exists some  $a \in R$  such that  $I = (a)$ .



In other words, every ideal of  $R$  is generated by a single element. The ring of integers  $\mathbb{Z}$  is a principal ideal domain since every ideal of  $\mathbb{Z}$  is of the form  $(n)$  for some  $n \in \mathbb{Z}$ . More trivially,  $\mathbb{Q}$  and  $\mathbb{R}$  are principal ideal domains since the only ideals of  $\mathbb{Q}$  and  $\mathbb{R}$  are the zero ideal and the whole ring. Generally, we can show the following proposition.

**Proposition 1.59.** *Let  $R$  be a euclidean domain. Then  $R$  is a principal ideal domain.*

*Proof.* Let  $N : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  be a euclidean function on  $R$ . Let  $I$  be an ideal of  $R$ . If  $I = \{0\}$ , then  $I = (0)$  is principal. Else, let  $x \in I$  be such that  $N(x) = \min\{N(y) : y \in I \setminus \{0\}\}$ . We claim that  $I = (x)$ . It is clear that  $(x) \subseteq I$  since  $x \in I$  and  $I$  is an ideal. For the converse inclusion, let  $y \in I \setminus \{0\}$ . Then, there exist  $q, r \in R$  such that  $y = xq + r$  and either  $r = 0$  or  $N(r) < N(x)$ . If  $r = 0$ , then  $y = xq \in (x)$ . If  $r \neq 0$ , then  $r = y - xq \in I$ , contradicting the choice of  $x$  since  $N(r) < N(x)$ . Therefore, we must have  $r = 0$ , so  $y \in (x)$ . Thus,  $I = (x)$  is principal. ■

**Definition 1.60.** Let  $R$  be a ring. A non-zero element  $x \in R$  is called a *prime element* if the ideal  $(x)$  generated by  $x$  is a non-zero prime ideal of  $R$ . A non-zero element  $x \in R$  is called an *irreducible element* if  $x$  is not a unit and whenever  $x = ab$  for some  $a, b \in R$ , then either  $a$  or  $b$  is a unit.

That is, if  $x \mid ab$ , then  $x \mid a$  or  $x \mid b$  for all  $a, b \in R$  (note that  $x \mid a$  means there exists  $c \in R$  such that  $a = cx$ ) for a prime  $x$ . For example, in  $\mathbb{Z}$ , the prime elements and irreducible elements are exactly the prime numbers and their negatives. In  $k[x]$  where  $k$  is a field, the prime elements and irreducible elements are exactly the irreducible polynomials.

**Proposition 1.61.** *Let  $R$  be an integral domain. Then every prime element of  $R$  is irreducible.*

*Proof.* Let  $x = ab$  for  $a, b \in R$ . Then  $x \mid ab$ , so  $x \mid a$  or  $x \mid b$  since  $x$  is prime. If  $x \mid a$ , then there exists some  $c \in R$  such that  $a = cx$ . Thus,  $x = ab = cxb$ , so  $(1 - cb)x = 0$ . Since  $R$  is an integral domain and  $x \neq 0$ , we must have  $cb = 1$ , so  $b$  is a unit. If  $x \mid b$ , then there exists some  $d \in R$  such that  $b = dx$ . Thus,  $x = ab = adx$ , so  $(1 - ad)x = 0$ . Since  $R$  is an integral domain and  $x \neq 0$ , we must have  $ad = 1$ , so  $a$  is a unit. Therefore, either  $a$  or  $b$  is a unit, so  $x$  is irreducible. ■

Note that in a field, there are no prime elements. In a valuation ring,  $x$  is a prime element if and only if  $v(x) = 1$ .

**Proposition 1.62.** *Let  $R$  be a principal ideal domain. Then every irreducible element of  $R$  is prime.*

*Proof.* Consider  $I = (x)$ . Let  $\mathfrak{m}$  be a maximal ideal of  $R$  containing  $I$ . Since  $R$  is a principal ideal domain,  $\mathfrak{m} = (a)$  for some  $a \in R$ . Since  $I \subseteq \mathfrak{m}$ , we have  $x \in (a)$ , so there exists some  $b \in R$  such that  $x = ab$ . Since  $x$  is irreducible, either  $a$  or  $b$  is a unit. If  $a$  is a unit, then  $\mathfrak{m} = (a) = R$ , contradicting the fact that  $\mathfrak{m}$  is a maximal ideal. Thus,  $b$  is a unit and  $a = b^{-1}x$ . Thus  $\mathfrak{m} = (a) = (b^{-1}x) \subseteq (x) = I$ . Since  $\mathfrak{m}$  is a maximal ideal containing  $I$ , we must have  $\mathfrak{m} = I$ . Therefore,  $I$  is a prime ideal, so  $x$  is a prime element. ■

**Corollary 1.63.** *In a principal ideal domain, every non-zero prime ideal is a maximal ideal.*

**Definition 1.64.** Let  $R$  be a ring, and  $a, b \in R$ . We say that  $d \in R$  is a *greatest common divisor* of  $a$  and  $b$ , and we write  $d = \gcd(a, b)$ , if  $d \mid a$  and  $d \mid b$ , and if there exists some  $d' \in R$  such that  $d' \mid a$  and  $d' \mid b$ , then  $d' \mid d$ .

Note that the gcd here may not be unique. For example, in  $\mathbb{Z}$ , the gcd of 6 and  $-9$  is 3 and  $-3$ .

**Proposition 1.65.** *Let  $R$  be a ring, and  $a, b \in R$  such that  $(a, b)$  is a principal ideal. Then the gcd of  $a$  and  $b$  exists, and if  $(d) = (a, b)$ , then  $d$  is a gcd of  $a$  and  $b$ . Moreover,  $d = ax + by$  for some  $x, y \in R$ .*

*Proof.* If  $(a, b) = (d)$ , then  $d \mid a$  and  $d \mid b$ . If  $d' \in R$  is such that  $d' \mid a$  and  $d' \mid b$ , then  $(a, b) \subseteq (d')$ , so  $(d) \subseteq (d')$ , so  $d' \mid d$ . Thus,  $d$  is a gcd of  $a$  and  $b$ . Since  $(d) = (a, b)$ , there exist  $x, y \in R$  such that  $d = ax + by$ . ■

Of course, the notion of gcd exists for  $\mathbb{Z}$ . As another example, look at this ring  $\mathbb{Q}[x, y]$ . By inspection, 1 is a gcd of  $x$  and  $y$ , since  $1 \mid x$  and  $1 \mid y$ , and if  $d' \in \mathbb{Q}[x, y]$  is such that  $d' \mid x$  and  $d' \mid y$ , then  $d' \in \mathbb{Q}$ , so  $d' \mid 1$ . In fact, any  $a \in \mathbb{Q}^\times$  is a gcd of  $x$  and  $y$ .

February 13th.

**Example 1.66.** Consider the rings  $\mathbb{Z}[i]$  and  $\mathbb{Z}[\sqrt{-3}]$ . The ring  $\mathbb{Z}[i]$  is a euclidean domain with respect to the euclidean function  $N : \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  defined by  $N(a + bi) = a^2 + b^2$  for all  $a + bi \in \mathbb{Z}[i] \setminus \{0\}$ . Indeed, given any  $\alpha = a + ib, \beta = c + id \in \mathbb{Z}[i]$ , for  $a, b, c, d \in \mathbb{Z}$ , we wish to find  $\gamma, r \in \mathbb{Z}[i]$  such that  $\alpha = \beta\gamma + r$  and either  $r = 0$  or  $N(r) < N(\beta)$ . Consider

$$\frac{\alpha}{\beta} = \frac{(a + ib)(c - id)}{(c + id)(c - id)} = u + iv \quad (1.46)$$

where  $u, v \in \mathbb{Q}$ . So there exist  $p, q \in \mathbb{Z}$  such that  $|p - u| \leq 1/2$  and  $|q - v| \leq 1/2$ . Thus,

$$\alpha = \beta(u + iv) = \beta(p + iq) + \beta((u - p) + i(v - q)) = \beta(p + iq) + r \quad (1.47)$$

where  $N(r) = N(\beta)N((u - p) + i(v - q)) \leq N(\beta)\frac{1}{2} < N(\beta)$ . Thus,  $\gamma = p + iq$  and  $r = \beta((u - p) + i(v - q))$  satisfy the required condition. Therefore,  $\mathbb{Z}[i]$  is a euclidean domain, so  $\mathbb{Z}[i]$  is a principal ideal domain. Thus,  $\mathbb{Z}[i]$  is a principal ideal domain, so every irreducible element of  $\mathbb{Z}[i]$  is prime. In particular,  $1 + i$  is an irreducible element of  $\mathbb{Z}[i]$ , so  $1 + i$  is prime.

On the other hand, the ring  $\mathbb{Z}[\sqrt{-3}]$  is not a principal ideal domain; consider  $I = (2, 1 + \sqrt{-3})$ . We show that  $I \cap \mathbb{Z} = (2)$ . Since  $2 \in I$ , we have  $(2) \subseteq I \cap \mathbb{Z}$ . For the converse inclusion, let  $x \in I \cap \mathbb{Z}$ . Then, there exist  $r, s \in \mathbb{Z}[\sqrt{-3}]$  such that  $x = r(1 + \sqrt{-3}) + s2$ . Since  $x$  is also an integer, we can write  $x = \alpha(1 + \sqrt{-3}) + 2\beta$  where  $\alpha \in \mathbb{Z}[-\sqrt{-3}]$  and  $\beta \in \mathbb{Z}$ . But this means that  $\alpha(1 + \sqrt{-3})$  must be an integer, so taking norms gives  $(x - 2\beta)^2 = \alpha\bar{\alpha}4$ , so  $4 \mid (x - 2\beta)^2$ , so  $2 \mid x - 2\beta$ , so  $2 \mid x$ . Thus,  $x \in (2)$ , so  $I \cap \mathbb{Z} = (2)$ . Hence,  $I \subsetneq \mathbb{Z}[\sqrt{-3}]$ . If  $I$  were principal, then  $I = (a + b\sqrt{-3})$  for some  $a, b \in \mathbb{Z}$ . If  $b = 0$ , then  $I = (a)$  implies  $I = 2\mathbb{Z}[\sqrt{-3}]$  which makes the contradiction  $1 + \sqrt{-3} \notin 2\mathbb{Z}[\sqrt{-3}]$ ;  $b$  has to be non-zero. We must have, as  $2 \in I$ ,  $2 = (a + b\sqrt{-3})(c + d\sqrt{-3})$  for some  $c, d \in \mathbb{Z}$ . Taking norms gives  $4 = (a^2 + 3b^2)(c^2 + 3d^2)$ . Since  $b \neq 0$ ,  $b = \pm 1$  and  $a = \pm 1$  must be the only possibilities. This again must mean that  $c^2 + 3d^2 = 1$  which implies  $c = \pm 1$  and  $d = 0$ . But this gives  $2 = \pm(1 \pm \sqrt{-3})$ , which is nonsense. Hence  $I$  cannot be principal.

A more general result states that if  $D \equiv 1 \pmod{4}$  and  $D$  is square-free, then  $\mathbb{Z}[\sqrt{D}]$  cannot be a principal ideal domain.

**Proposition 1.67.** *Let  $R$  be a ring such that  $R[x]$  is a principal ideal domain. Then  $R$  is a field.*

*Proof.* Since  $R \subseteq R[x]$  is a subring,  $R$  is an integral domain. Let  $\varphi : R[x] \rightarrow R$  be the evaluation homomorphism defined by  $\varphi(f) = f(0)$  for all  $f \in R[x]$ . This map is surjective. Moreover,  $\ker \varphi = (x) \subseteq R[x]$ . So  $R[x]/(x) \cong R$ , implying that  $R[x]/(x)$  is an integral domain and  $(x)$  is a prime ideal. We had shown that any non-zero prime ideal in a principal ideal domain is maximal, so  $(x)$  is maximal. Thus,  $R[x]/(x) \cong R$  is a field, so  $R$  is a field. ■

**Definition 1.68.** For a ring  $R$ , the map  $N : R \rightarrow \mathbb{Z}_{\geq 0}$  is called a *Dedekind-Hasse norm* if  $N(0) = 0$ , and for all  $a, b \in R \setminus \{0\}$ , either  $b \mid a$  or there exists  $0 \neq r \in (a, b)$  such that  $N(r) < N(b)$ .

**Proposition 1.69.** *If  $R$  is an integral domain that admits a Dedekind-Hasse norm, then  $R$  is a principal ideal domain. The converse also holds.*

*Proof.* Let  $I \subseteq R$  be an ideal. Let  $x \in I \setminus \{0\}$  be such that  $N(x)$  is the least among  $\{N(y) \mid y \in I, y \neq 0\}$ .  $(x) \subseteq I$  is clear. Let  $y \in I \setminus \{0\}$ . So either  $x \mid y$  or there exists  $0 \neq r \in (x, y)$  such that  $N(r) < N(x)$ . This, however, is a contradiction to the choice of  $x$ . Hence  $x \mid y$  and  $y \in (x)$ . Thus,  $I = (x)$  is principal. ■

**Example 1.70.** The ring  $\mathbb{Z}[(1 + \sqrt{-19})/2]$  is a principal ideal domain but not a euclidean domain. Note that  $N : \mathbb{Z}[\omega = (1 + \sqrt{-19})/2] \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  defined by  $a + b\omega \mapsto a^2 + ab + 5b^2$  is a Dedekind-Hasse norm.

**Proposition 1.71.** *Let  $R$  be a euclidean domain but not a field. Then it contains a ‘universal side divisor’; that is, there exists a non-zero non-unit  $u \in R$  such that for all non-zero  $x \in R$ , there exists  $q \in R$  satisfying that  $r = x - qu$  is either 0 or a unit*

*Proof.* Let  $u \in R \setminus \{0\}$  be such that  $N(u)$  is least among all non-zero non-unit elements of  $R$ . We claim that  $u$  satisfies this property. Let  $x \in R \setminus \{0\}$ . Then there exist  $q, r \in R$  such that  $x = qu + r$  satisfying either  $r = 0$  or  $N(r) < N(u)$ . Since  $u$  is a non-unit,  $N(u) > 0$ , so  $N(r) < N(u)$  implies that  $r$  is a unit. Thus,  $r = x - qu$  is either 0 or a unit, so the claim holds. ■

One may check that  $\mathbb{Z}[(1 + \sqrt{-19})/2]$  has no universal side division, and  $\pm 1$  are the only units in the ring.

**Definition 1.72.** Let  $R$  be an integral domain. We say that  $R$  is a *unique factorization domain* if for all non-zero non-unit  $x \in R$ ,  $x$  can be written as  $x = p_1 \cdots p_n$  for some  $n \geq 1$  and  $p_i$  irreducibles, and if  $x = p_1 \cdots p_n = q_1 \cdots q_m$  for some  $m \geq 1$  and irreducibles  $q_j$ , then  $n = m$  and, after reordering,  $p_i = u_i q_i$  for some unit  $u_i$  for all  $1 \leq i \leq n$ .

For example, both  $\mathbb{Z}$  and  $k[x]$  where  $k$  is a field are UFDs. As a small definition,  $x, y \in R$  are termed *associates* if  $x = uy$  for some unit  $u \in R$ . Again, in  $\mathbb{Z}$ ,  $-n$  and  $n$  are associates, and in  $\mathbb{Q}[x]$ ,  $f$  and  $cf$  for some  $c \in \mathbb{Q}^\times$  are associates. Lastly, in  $\mathbb{Z}[i]$ ,  $n, -n, ni, -ni$  are all associates for any  $n \in \mathbb{Z}$ . Thus the above definition is saying that the factorization of  $x$  into irreducibles is unique up to reordering and up to associates. For non-examples,  $\mathbb{Z}[\sqrt{5}]$  is an integral domain but not a unique factorization domain since  $-4 = -2 \cdot 2 = (1 + \sqrt{5})(1 - \sqrt{5})$  are two distinct factorizations of  $-4$  into irreducibles, and the irreducibles  $2, 1 + \sqrt{5}, 1 - \sqrt{5}$  are not associates of each other.

February 16th.

**Example 1.73.** As a more concrete example of a non-UFD, consider the quotient ring  $\bar{R} = \mathbb{Q}[x, y, z, w]/(xy - zw)$ . Suppose  $\bar{x} = \bar{f}\bar{g}$  for some  $\bar{f}, \bar{g} \in \bar{R}$ . Then  $x - fg \in (xy - zw)$  unless  $x - fg = 0$ . Since  $xy - zw$  is irreducible in  $\mathbb{Q}[x, y, z, w]$ , we must have  $x \mid f$  or  $x \mid g$ . If  $x \mid f$ , then  $\bar{f}$  is a unit in  $\bar{R}$ , so  $\bar{x}$  is irreducible. Similarly, if  $x \mid g$ , then  $\bar{g}$  is a unit in  $\bar{R}$ , so  $\bar{x}$  is irreducible. Thus,  $\bar{x}$  is irreducible. By symmetry,  $\bar{y}, \bar{z}, \bar{w}$  are also irreducible. However, we have the two distinct factorizations  $\bar{x}\bar{y} = \bar{z}\bar{w}$  into irreducibles, and the irreducibles  $\bar{x}, \bar{y}, \bar{z}, \bar{w}$  are not associates of each other since they are all of degree one. Therefore,  $\bar{R}$  is not a unique factorization domain.

**Theorem 1.74.** *Let  $R$  be a principal ideal domain. Then  $R$  is a unique factorization domain.*

*Proof.* Let  $x \in R$  be a non-zero non-unit. We show that  $x$  can be written as a product of irreducibles. Let  $\mathfrak{m}$  be a maximal ideal of  $R$  containing  $(x)$ . Since  $R$  is a principal ideal domain,  $\mathfrak{m} = (p_1)$  for some  $p_1 \in R$ . Thus,  $p_1$  is a prime element, so  $p_1$  is irreducible. If  $x = p_1 x_1$  for some  $x_1 \in R$ , then we can repeat the process for  $x_1$ . If  $x_1$  is a unit, then we are done. Else, we can repeat the process for  $x_1$  to get a prime element  $p_2$  such that  $x_1 = p_2 x_2$  for some  $x_2 \in R$ . We can keep repeating this process; we claim that it must terminate after finitely many steps. If not, then we have an infinite sequence of ideals  $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$ . Let  $I = \bigcup_{n \geq 0} (x_n)$ . Then  $I$  is an ideal of  $R$ . Since  $R$  is a principal ideal domain,  $I = (y)$  for some  $y \in R$ . Thus,  $y \in I$  implies that  $y \in (x_r)$  for some  $r \geq 0$ , so  $y = ux_r$  for some  $u \in R$ . Also,  $x_r = p_{r+1} x_{r+1}$  for some  $p_{r+1} \in R$  and  $x_{r+1} \in R$ , so  $y = up_{r+1} x_{r+1}$ . Also, since  $x_{r+1} = vy$  for some  $v \in R$ , we have  $y = up_{r+1} vy$ , so  $(1 - up_{r+1}v)y = 0$ . Since  $R$  is an integral domain and  $y \neq 0$ , we must have  $up_{r+1}v = 1$ , so  $p_{r+1}$  is a unit, contradicting the fact that  $p_{r+1}$  is a prime element. Therefore, the

process must terminate after finitely many steps, so  $x$  can be written as a product of irreducibles (note that the last terminating unit may be absorbed into the previous prime element to make it irreducible).

To show uniqueness upto reordering, and associates, let  $x = p_1 \cdots p_n = q_1 \cdots q_m$  for some  $m \geq 1$  and irreducibles  $q_j$ . Since  $p_1$  is irreducible and  $R$  is a principal ideal domain,  $p_1$  is prime, so  $p_1 \mid q_1 \cdots q_m$  implies that  $p_1 \mid q_{i_1}$  for some  $1 \leq i_1 \leq m$ . Since  $q_{i_1}$  is irreducible,  $p_1$  and  $q_{i_1}$  are associates, so  $p_1 = u_1 q_{i_1}$  for some unit  $u_1$ . We can reorder the  $q_j$ 's so that  $i_1 = 1$ , giving us  $p_1 = u_1 q_1$ . Cancellation gives us  $p_2 \cdots p_n = u_1 q_2 \cdots q_m$ ; we can repeat the same process to get  $p_2 = u_2 q_2$  for some unit  $u_2$ , and so on. After repeating this process, we get  $p_i = u_i q_i$  for some unit  $u_i$  for all  $1 \leq i \leq n$ . By symmetry argument, we also get  $q_j = v_j p_j$  for some unit  $v_j$  for all  $1 \leq j \leq m$ . Thus,  $n = m$  and  $p_i = u_i q_i$  for some unit  $u_i$  for all  $1 \leq i \leq n$ , so the factorization of  $x$  into irreducibles is unique up to reordering and up to associates. ■

**Proposition 1.75.** *Let  $R$  be a unique factorization domain. Then an element is irreducible if and only if it is prime.*

*Proof.* We already know that every prime element is irreducible in any integral domain. For the converse, let  $x$  be an irreducible element of  $R$ . Let  $x \mid ab$  for some  $a, b \in R$ . There then exists some  $y \in R$  such that  $ab = xy$ . Let  $a = p_1 \cdots p_n$  and  $b = q_1 \cdots q_m$ , and  $y = r_1 \cdots r_k$  be the factorizations of  $a, b, y$  into irreducibles. Then  $p_1 \cdots p_n q_1 \cdots q_m = r_1 \cdots r_k x$ . Since  $x$  is irreducible,  $x$  must be an associate of some  $p_i$  or some  $q_j$ , so  $x \mid a$  or  $x \mid b$ . Thus,  $x$  is prime. ■

**Theorem 1.76.** *Let  $R$  be a principal ideal domain. Then  $R$  has a Dedekind-Hasse norm.*

*Proof.* Let  $x \in R \setminus \{0\}$ . Define  $N : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  as follows: if  $x$  is a unit,  $N(x) = 1$ . Otherwise, write  $x = p_1 \cdots p_n$  for some  $n \geq 1$  and irreducibles  $p_i$ , and define  $N(x) = 2^n$ . Verify that  $N$  is a Dedekind-Hasse norm. ■

February 19th.

**Proposition 1.77.** *Let  $R$  be a unique factorization domain. If  $a, b \in R$  are non-zero, then  $\gcd(a, b)$  exists. If  $a$  or  $b$  is a unit, then  $\gcd(a, b)$  is a unit. Moreover, if  $a$  and  $b$  are non-units, then there exist irreducibles  $p_1, \dots, p_r$  such that  $a = p_1^{e_1} \cdots p_r^{e_r}$  and  $b = p_1^{f_1} \cdots p_r^{f_r}$  for some  $e_i, f_i \geq 0$  for all  $1 \leq i \leq r$ , and  $\gcd(a, b) = p_1^{\min\{e_1, f_1\}} \cdots p_r^{\min\{e_r, f_r\}}$ .*

*Proof.* If  $a$  or  $b$  is a unit, then  $\gcd(a, b)$  is a unit since any unit divides any element. So we may assume that  $a$  and  $b$  are non-units. Since  $R$  is a unique factorization domain, there exist irreducibles  $p_1, \dots, p_r$  such that  $a = p_1^{e_1} \cdots p_r^{e_r}$  and  $b = p_1^{f_1} \cdots p_r^{f_r}$  for some  $e_i, f_i \geq 0$  for all  $1 \leq i \leq r$ . Let  $d = p_1^{\min\{e_1, f_1\}} \cdots p_r^{\min\{e_r, f_r\}}$ . Then  $d \mid a$  and  $d \mid b$ . If  $d' \in R$  is such that  $d' \mid a$  and  $d' \mid b$ , then there exist some irreducibles  $q_1, \dots, q_s$  such that  $d' = q_1^{g_1} \cdots q_s^{g_s}$  for some  $g_i \geq 0$  for all  $1 \leq i \leq s$ . Since  $d' \mid a$ , we have that each irreducible factor of  $d'$  must be an associate of some irreducible factor of  $a$ , so after reordering, we can write  $d' = p_1^{g'_1} \cdots p_r^{g'_r}$  where each  $g'_i \geq 0$ . Since  $d' \mid b$ , we have that each irreducible factor of  $d'$  must be an associate of some irreducible factor of  $b$ , so after reordering, we can write  $d' = p_1^{g''_1} \cdots p_r^{g''_r}$  where each  $g''_i \geq 0$ . Thus, after reordering, we can write  $d' = p_1^{g'''_1} \cdots p_r^{g'''_r}$  where  $g'''_i = \min\{g'_i, g''_i\} \leq \min\{e_i, f_i\}$  for all  $1 \leq i \leq r$ . Thus,  $d' \mid d$ . Therefore,  $d$  is a gcd of  $a$  and  $b$ . ■

**Proposition 1.78.** *Let  $R$  be an integral domain. Then  $R$  is a unique factorization domain if and only if every irreducible element of  $R$  is prime and any increasing chain of principal ideals in  $R$  stabilizes.*

*Proof.* For the forward implication, if we have already shown that every irreducible element of  $R$  is prime. Let  $(x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \cdots$  be a strictly increasing chain of principal ideals in  $R$ . If  $x_1$  is a unit, then  $(x_1) = R$ , contradicting the fact that  $(x_1) \subsetneq (x_2)$ . If  $x_1 = 0$ , then  $x_2 \neq 0$  so we may assume that  $x_1$  is a non-zero non-unit. Since  $R$  is a unique factorization domain, we can uniquely factor  $x_1$  as  $x_1 = p_1 \cdots p_n$  for some  $n \geq 1$  and irreducibles  $p_i$ . Since  $x_1 \in (x_2)$ ,  $x_1 = x_2 y$  for some  $y \in R$ . Also  $(x_1) \subsetneq (x_2)$  implies that  $y$  is not a unit. Let  $x_2 = q_1 \cdots q_m$  and  $y = r_1 \cdots r_k$  be the factorizations of  $x_2$  and  $y$  into irreducibles. Then by the uniqueness of factorization,  $n = m + k$  and since  $y$  is not a unit,  $k \geq 1$ , so  $m < n$ . Thus,  $x_2$  has strictly less irreducible factors than  $x_1$ . We can repeat the same process for  $x_2$  to get that  $x_3$  has

strictly less irreducible factors than  $x_2$ , and so on. Since the number of irreducible factors is a non-negative integer, this process must terminate after finitely many steps giving a  $x_n$  that is a unit, contradicting the fact that  $(x_n) \subsetneq (x_{n+1})$ . Therefore, any increasing chain of principal ideals in  $R$  stabilizes.

For the converse implication, let  $x \in R$  be a non-zero non-unit. The result is trivial if  $x$  is irreducible, so we may assume that  $x$  is not an irreducible. We claim that there exists an irreducible  $p_1 \in R$  such that  $x = p_1 y$  for some  $y \in R$ . Since  $x$  is not irreducible, there exist  $x_1, y_1 \in R$  such that  $x = x_1 y_1$  and neither  $x_1$  nor  $y_1$  is a unit. If  $x_1$  is irreducible, then we can take  $p_1 = x_1$  and  $y = y_1$ . Else, we can repeat the same process for  $x_1$  to get  $x = x_2 y_2 y_1$  for some non-units  $x_2, y_2 \in R$ . We can keep repeating this process; we claim that it must terminate after finitely many steps. If not, then we have an infinite sequence of ideals  $(x) \subsetneq (x_1) \subsetneq (x_2) \subsetneq \cdots$ . This contradicts the fact that any increasing chain of principal ideals in  $R$  stabilizes. Therefore, the process must terminate after finitely many steps, so there exists an irreducible  $p_1 \in R$  such that  $x = p_1 y$  for some  $y \in R$ . If  $y$  is a unit, then we are done. Else, we can repeat the same process for  $y$  to get  $x = p_1 p_2 y_2$  for some irreducible  $p_2$  and some  $y_2 \in R$ . We can keep repeating this process; we claim that it must terminate after finitely many steps. If not, then we have an infinite sequence of ideals  $(x) \subsetneq (p_1) \subsetneq (p_1 p_2) \subsetneq \cdots$ . This contradicts the fact that any increasing chain of principal ideals in  $R$  stabilizes. Therefore, the process must terminate after finitely many steps, so  $x$  can be written as a product of irreducibles. The uniqueness follows from the same proof as that of the theorem that a principal ideal domain is a unique factorization domain. ■



# Index

- associates, 17
- associativity, 1
- chinese remainder theorem, 13
- commutative ring, 1
- Dedekind-Hasse, 16
- degree, 3
- distributivity, 1
- euclidean domain, 14
- field, 1
- first isomorphism theorem, 7
- generating set, 5
- greatest common divisor, 15
- group ring, 6
- ideal, 4
- idempotent, 13
- inclusion map, 12
- integral domain, 6
- irreducible element, 15
- isomorphic, 2
- Jacobson radical, 11
- kernel, 5
- maximal ideal, 10
- nilpotent, 6
- nilradical, 11
- polynomial ring, 3
- polynomials, 3
- prime element, 15
- prime ideal, 9
- principal ideal domain, 14
- product ring, 12
- projection map, 12
- quotient map, 7
- quotient ring, 7
- reduced ring, 6
- ring, 1
- ring epimorphism, 2
- ring homomorphism, 2
- ring isomorphism, 2
- ring monomorphism, 2
- ring with unity, 1
- second isomorphism theorem, 8
- subring, 2
- third isomorphism theorem, 8
- unique factorization domain, 17
- unit, 1
- universal side divisor, 17
- valuation map, 14
- valuation ring, 14
- zero divisor, 6