

## Chapter 1

# Introduction to Rings and Fields

## 1.1. THE DEFINITION AND SOME EXAMPLES OF RINGS

**Definition 1.1.1** (Rings). A **ring**  $(R, +, \cdot, 0, 1)$  is a set of at least two elements (0 and 1 are distinct) such that  $(R, +, 0)$  is a commutative group,  $(R, \cdot, 1)$  is a **monoid** and  $\cdot$  is distributive with respect to  $+$ . To be precise, a ring must satisfy the following axioms.

- (1) The addition  $+$  is associative.
- (2) The element 0 is the additive identity.
- (3) Every element has an additive inverse.
- (4) The addition  $+$  is commutative.
- (5) The multiplication  $\cdot$  is associative.
- (6) The element 1 is the multiplicative identity. (The multiplicative identity is usually called the **unity**.)
- (7)  $a \cdot (b + c) = a \cdot b + a \cdot c$  for all  $a, b$  and  $c \in R$ .
- (8)  $(b + c) \cdot a = b \cdot a + c \cdot a$  for all  $a, b$  and  $c \in R$ .

If in addition that  $(R, \cdot, 1)$  is commutative we say  $(R, +, \cdot, 0, 1)$  or simply  $R$  is a **commutative ring**. A ring which is not commutative is called a **noncommutative ring**.

*Remark.* (1) We usually write  $ab$  for  $a \cdot b$ .

(2) Multiplication is assumed to be performed before addition.

(3) Remember that Cancellation Law holds for  $+$  but not for  $\cdot$ .

(4) In some textbooks one does not require a ring to contain 1 or to contain at least 2 elements. Hence the set of all even integers or the set  $\{0\}$  qualify as examples of rings in those textbooks but not in our class. (Jacobson called the rings without unity *rngs* in his classic *Basic Algebra I*.)

**Example 1.1.2.** (1)  $\mathbb{C}$ ,  $\mathbb{R}$ ,  $\mathbb{Q}$  and  $\mathbb{Z}$  are all examples of commutative rings, while  $\mathbb{N}$  or  $\mathbb{Z}_+$  are not rings.

(2) For each  $n$ ,  $\mathbb{Z}_n$  is a commutative ring. In  $\mathbb{Z}_6$  we have

$$\bar{2} \cdot \bar{3} = \bar{2} \cdot \bar{0} = \bar{0}.$$

The Cancellation law does not hold for multiplication in  $\mathbb{Z}_6$ .

(3)  $\mathbb{C}[x]$ ,  $\mathbb{R}[x]$ ,  $\mathbb{Q}[x]$  and  $\mathbb{Z}[x]$  are commutative rings.

(4) Let  $M_n(\mathbb{R})$  be the set of all  $n \times n$  square matrices. In the course of Linear Algebra we have seen that it is a *noncommutative* ring. It is also easy to see that  $M_n(\mathbb{Z})$  is also a noncommutative ring.

(4) Let  $R$  be the set of all continuous functions from  $\mathbb{R}$  to  $\mathbb{R}$ . This is a commutative ring.

(5) Let  $R = \mathbb{Z}^n$ . We knew from last semester that the coordinate-wise addition makes  $(R, +, (0, 0, \dots, 0))$  an abelian group. We can also define a coordinate-wise multiplication on  $R$ :

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n).$$

It is easy to see that  $(1, 1, \dots, 1)$  is the multiplicative identity and that  $R$  is a commutative ring.

Next Let's give a list of very basic properties of rings.

**Proposition 1.1.3.** *Let  $R$  be a ring and  $a, b, c \in R$ . Then*

- (1)  $a0 = 0a = 0$ ;
- (2)  $(-1)a = a(-1) = -a$ ;
- (3)  $a(-b) = (-a)b = -ab$ ;
- (4)  $(-a)(-b) = ab$ ;
- (5)  $(a - b)c = ac - bc$  and  $c(a - b) = ca - cb$ .

**Definition 1.1.4.** We say an element  $u$  of a ring  $R$  is a **unit** or is **invertible** if there exists  $v$  in  $R$  such that  $uv = vu = 1$ .

*Remark.* (1) 0 is not a unit.

- (2) 1 is an unit.
- (3) The product of two units is still a unit.
- (4) The inverse of a unit is unique.

**Definition 1.1.5.** The set  $U(R) = \{u \in R : u \text{ is a unit}\}$  is a group. It is called the **group of units** of  $R$ .

**Example 1.1.6.** (1)  $U(\mathbb{Z}) = \{1, -1\}$ .

- (2)  $U(\mathbb{Z}_n) = \{\bar{k} \in \mathbb{Z}_n : (k, n) = 1\}$ . See Proposition 1.1.7
- (3) Inside  $(M_n(\mathbb{R}), \cdot)$  there are two important subgroups. One is what we call the **general linear group**

$$GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}.$$

The other is the **special linear group**,

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A = 1\},$$

which is a subgroup of  $GL_n(\mathbb{R})$ . The group of units  $U(M_n(\mathbb{R})) = GL_n(\mathbb{R})$ .

**Proposition 1.1.7.** *In  $\mathbb{Z}_n$ , the element  $\bar{k}$  is a unit if and only if  $k$  and  $n$  are relatively prime.*

**Definition 1.1.8.** Let  $n$  be an integer greater than 1. Define the **Euler function** to be

$$\varphi(n) = |\{k \in \mathbb{Z}_+ : k < n, (k, n) = 1\}|.$$

For example,  $\varphi(1) = 0$ ,  $\varphi(2) = 1$ ,  $\varphi(3) = 2$ ,  $\varphi(4) = 2$ , etc. Obviously,

$$|\mathbb{Z}_n| = \varphi(n).$$

**Corollary 1.1.9** (Euler). *If  $k$  is an integer prime to the positive inter  $n$ , then*

$$k^{\varphi(n)} \equiv 1 \pmod{n}.$$

Fermat's little Theorem is a special case of this Corollary.

**Corollary 1.1.10** (Fermat). *If  $p$  is a prime integer and  $k$  is an integer not divisible by  $p$  then*

$$k^{p-1} \equiv 1 \pmod{p}.$$

*Consequentially, for any integer  $k$  we have*

$$k^p \equiv k \pmod{p}.$$

**Definition 1.1.11.** A ring is called a **division ring** or a **skew field** if every nonzero element of  $R$  is a unit. A commutative division ring is called a **field**.

**Example 1.1.12.** (1)  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  and  $\mathbb{Z}_p$ ,  $p$  prime, are all examples of fields while  $\mathbb{Z}$  or  $\mathbb{Z}_9$  is not.

- (2) The set of **rational functions** over  $\mathbb{R}$

$$\mathbb{R}(x) = \left\{ \frac{g(x)}{f(x)} : f(x), g(x) \in \mathbb{R}, f(x) \neq 0 \right\}$$

is a field. Similarly, other sets of rational functions over various fields, for example,  $\mathbb{C}(x)$ , and  $\mathbb{Q}(x)$  are also fields.

**Example 1.1.13.** (1) Check that

$$\begin{aligned}\mathbb{Z}[\sqrt{2}] &= \{a_0 + a_1\sqrt{2} + a_2\sqrt{2}^2 + \cdots + a_n\sqrt{2}^n : n \in \mathbb{N}, a_1, a_2, \dots, a_n \in \mathbb{Z}\} \\ &= \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}\end{aligned}$$

is a commutative ring. Find all the units of  $\mathbb{Z}[\sqrt{2}]$ .

(2) Check that  $\mathbb{Q}[\sqrt{2}]$  is a field.

The homework problem set will provide an example of a division ring.

**Definition 1.1.14.** Let  $R$  be a ring and let  $a \in R$ . We say  $a$  is a **(left) zero divisor** if  $ab = 0$  for some  $b \neq 0$ . **Right zero divisor** is defined similarly. We say  $a$  is a **nonzerodivisor**, or simply **NZD**, if  $a$  is not a zero divisor.

*Remark.* (1) To check  $a$  is a NZD we simply need to check that  $ab = 0$  implies  $b = 0$ .

(2) In a ring, 0 is always a zero divisor while 1 is never a zero divisor. In fact, all units are NZD's. The product of two NZD's is a NZD.

**Example 1.1.15.** In  $\mathbb{Z}_6$ , the elements  $\bar{0}, \bar{2}, \bar{3}, \bar{4}$  are zero divisors while  $\bar{1}, \bar{5}$  are NZD's.

**Definition 1.1.16.** A ring in which no nonzero element is a zero divisor is called a **domain**. A commutative domain is called an **integral domain**.

*Remark.* (1) In a domain,  $ab \neq 0$  if  $a, b \neq 0$ . If  $ab = 0$  then  $a = 0$  or  $b = 0$ .

(2) Fields are integral domains. Division Rings are domains.

**Example 1.1.17.**  $\mathbb{Z}$  and  $\mathbb{R}[x]$  are integral domains. All fields are integral domains. All division rings are domains.  $\mathbb{Z}^2$  is not an integral domain, and so are  $\mathbb{Z}^n$  for all  $n \geq 2$ .

**Proposition 1.1.18.** For all  $n \geq 2$ ,  $\mathbb{Z}_n$  is an integral domain if and only if  $n$  is a prime.

*Remark.* In fact  $\mathbb{Z}_p$ ,  $p$  prime, is a field. See also Proposition 1.1.21.

**Theorem 1.1.19.** Let  $a$  be a NZD. Then  $ab = ac$  (or  $ba = ca$ ) would imply  $b = c$ .

**Corollary 1.1.20.** In a domain we have that  $ab = ac$  (or  $ba = bc$ ) implies that  $a = 0$  or  $b = c$ .

**Proposition 1.1.21.** Every finite integral domain is a field.

At last we use an example to demonstrate the complication of zero divisors.

**Example 1.1.22.** Solve  $x^2 - x - 2 = 0$  in  $\mathbb{Z}_{10}$ .

**Definition 1.1.23.** Let  $R$  be a ring and let  $a \in R$ . We say  $a$  is a **nilpotent** element if  $a^n = 0$  for some  $n \in \mathbb{Z}_+$ .

**Definition 1.1.24.** We say  $R$  is a **reduced** ring if  $R$  is a ring without any nonzero nilpotent elements. In other words, in a reduced ring  $a^n = 0$  for some positive integer  $n$  implies that  $a = 0$ .

**Example 1.1.25.** (1)  $\mathbb{Z}$  is a reduced ring.

(2)  $M_n(\mathbb{Z})$  is not a reduced ring. For example, the matrix  $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$  is a nonzero nilpotent element in  $M_n(\mathbb{Z})$ .

(3) Which of  $\mathbb{Z}_8, \mathbb{Z}_6, \mathbb{Z}_{12}$  is a reduced ring?

## 1.2. SUBRINGS AND SUBFIELDS

**Definition 1.2.1.** We say that a subset  $R'$  of a ring  $R$  is a **subring** if  $R'$  is a ring itself with the same unity under the inherited addition and multiplication. When  $R$  and  $R'$  are fields we may also say that  $R'$  is a **subfield** of  $R$ .

**Example 1.2.2.** (1) The ring  $\mathbb{Z}$  is a subring of  $\mathbb{Q}$ . The ring  $\mathbb{Q}$  is a subring of  $\mathbb{R}$ . The ring  $\mathbb{R}$  is a subring of  $\mathbb{C}$ .

The field  $\mathbb{Q}$  is a subfield of  $\mathbb{R}$ . The field  $\mathbb{R}$  is a subfield of  $\mathbb{C}$ .

(2) The field  $\mathbb{Q}$  is a subfield of  $\mathbb{Q}[\sqrt{2}]$ .

(3) The ring  $M_n(\mathbb{Z})$  is a subring of  $M_n(\mathbb{R})$ .

(4) The set

$$R = \{(a, 0) : a \in \mathbb{Z}\}$$

is a subset of  $\mathbb{Z}^2$  and is a ring itself, but it is not a subring of  $\mathbb{Z}^2$  since they do not share the same unity.

**Theorem 1.2.3.** Let  $R$  be a ring and  $R'$  be a subset of  $R$ . Then the following three conditions are equivalent.

- (1)  $R'$  is a subring of  $R$ .
- (2)  $1 \in R'$  and  $a + b, -a, ab \in R'$  for all  $a, b \in R$ .
- (3)  $1 \in R'$  and  $a - b, ab \in R'$  for all  $a, b \in R$ .

**Theorem 1.2.4.** Let  $F$  be a field and  $F'$  be a subset of  $F$ . Then the following three conditions are equivalent.

- (1)  $F'$  is a subfield of  $F$ .
- (2)  $1 \in F'$  and  $a + b, -a, ab, a^{-1}$  (if  $a \neq 0$ )  $\in F'$  for all  $a, b \in F'$ .
- (3)  $1 \in F'$  and  $a - b, a^{-1}b$  (if  $a \neq 0$ )  $\in F'$  for all  $a, b \in F'$ .

**Corollary 1.2.5.** Let  $R$  be a ring and let  $\{R_i : i \in \Lambda\}$  be a nonempty collection of subrings of  $R$ . Then  $\bigcap_{i \in \Lambda} R_i$  is a subring of  $R$ .

**Corollary 1.2.6.** Let  $F$  be a field and let  $\{F_i : i \in \Lambda\}$  be a nonempty collection of subfields of  $F$ . Then  $\bigcap_{i \in \Lambda} F_i$  is a subfield of  $F$ .

### 1.3. IDEALS

**Definition 1.3.1.** Let  $R$  be a ring. A nonempty subset  $I$  of  $R$  is called a **left** (or **right**) **ideal** of  $R$  if

- (1)  $0 \in I$  (to ensure  $I$  is nonempty),
- (2)  $a + b \in I$  for all  $a, b \in I$ ,
- (3)  $ra$  (or  $ar$ )  $\in I$  for all  $r \in R$  and  $a \in I$ .

A **two-sided** ideal is an ideal which is both left and right.

*Remark.* (1) The ideal  $(I, +, 0)$  is a subgroup of  $(R, +, 0)$ .

(2) The adjectives *left* and *right* describes the position of the coefficient  $r$  on  $I$ .

(3) By an ideal we mean a left, or right or two-sided ideal. When  $R$  is a commutative ring, all ideals are two-sided. We will be mostly interested in ideals in commutative rings.

(4) While  $0$  is always in an ideal, the unity is seldom in there.

**Lemma 1.3.2.** Let  $R$  be a ring and let  $I$  be an ideal of  $R$ . If  $1 \in I$  then  $I = R$ . In fact, if  $I$  contains a unit then  $I = R$ .

**Definition 1.3.3.** Let  $I$  be an ideal of  $R$ . If  $I = R$  we say  $I$  is the **unit ideal**. If  $I = \{0\}$  we say  $I$  is the **trivial ideal**. We say  $I$  is a **proper** ideal if  $I \subsetneq R$ .

**Example 1.3.4.** (1) In a division ring or in a field the only ideals are the unit ideal and the trivial ideal.

(2) In the ring  $\mathbb{Z}$  the subset

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

is an ideal for all  $n \in \mathbb{Z}$ .

**Example 1.3.5.** Consider the ring  $M_2(\mathbb{Z})$ . Show that

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

is a left ideal, but not a right ideal.

*Remark.* For the rest of the course all ideals will be assumed to be *left* ideals unless otherwise noted. Note that all results regarding left ideals can be translated symmetrically to those of right ideals. However the results regarding left ideals will be adequate for our purpose since we will be mainly dealing with commutative rings.

**Proposition 1.3.6.** Let  $R$  be a ring and let  $\{I_i : i \in \Lambda\}$  be a nonempty collection of ideals of  $R$ . Then  $\bigcap_{i \in \Lambda} I_i$  is an ideal of  $R$ .

**Definition 1.3.7.** Let  $S$  be a subset of a ring  $R$ . We define  $(S)$  to be the intersection of all ideals of  $R$  containing  $S$ . If you want to distinguish between left and right ideals, you can use  $(S)_l$  and  $(S)_r$ . We say that  $(S)$  is the **ideal generated by  $S$** . If an ideal  $I = (S)$  we say that the set  $S$  **generates  $I$**  or  $S$  is a **generating set of  $I$** .

*Remark.* (1) From Proposition 1.3.6, we know that  $(S)$  is the smallest ideal of  $R$  containing  $S$ .

(2)  $(\phi) = \{0\}$ .

(3) When  $S$  is a finite set  $\{a_1, a_2, \dots, a_n\}$  we also use  $(a_1, a_2, \dots, a_n)$  to denote  $(S)$ .

(4) If  $S_1 \subseteq S_2$  then  $(S_1) \subseteq (S_2)$ .

**Definition 1.3.8.** We will write  $\sum_{i=1}^k a_i$ , the sum over  $\{a_1, a_2, \dots, a_k\}$ , for  $a_1 + a_2 + \dots + a_k$ . By convention, the sum over an empty set is defined to be 0.

**Theorem 1.3.9.** Let  $R$  be a ring and  $S$  be a subset of  $R$ . Then

$$(S)_l = \left\{ \sum_{i=1}^k r_i s_i : k \in \mathbb{N}, r_i \in R, s_i \in S \right\}.$$

*Remark.* Thanks to the theorem above we often write  $(a_1, a_2, \dots, a_n)_l$  as

$$Ra_1 + Ra_2 + \dots + Ra_n,$$

or in the case of right ideals, as

$$a_1R + a_2R + \dots + a_nR.$$

Of course when  $R$  is a commutative ring the two notation would make no difference. In the case of commutative rings it is often very common to see an ideal  $I$  written as

$$IR = \{ir : i \in I, r \in R\}.$$

This notation makes an emphasis on the ring which is sometimes very useful.

Now let's give a short discussion on the union of two ideals.

**Proposition 1.3.10.** Let  $I$  and  $J$  be ideals of a ring  $R$ . Then  $I \cup J$  is an ideal of  $R$  if and only if either  $I \subseteq J$  or  $J \subseteq I$ .

From the proposition above we see that  $I \cup J$  is usually not an ideal. Next we find the ideal generated by the  $I \cup J$ , the smallest ideal containing both  $I$  and  $J$ .

**Proposition 1.3.11.** Let  $I$  and  $J$  be ideals of a ring  $R$ . Then

$$I + J = \{i + j \in R : i \in I, j \in J\}$$

is an ideal of  $R$  and that  $I + J = (I \cup J)$ .

**Corollary 1.3.12.** Let  $I_1, I_2, \dots, I_n$  be ideals of  $R$ . Then

$$I_1 + I_2 + \dots + I_n = \{i_1 + i_2 + \dots + i_n : i_j \in I_j \text{ for all } j = 1, 2, \dots, n\}$$

is an ideal of  $R$  and is  $(I_1 \cup I_2 \cup \dots \cup I_n)$ .

**Corollary 1.3.13.** Let  $I$  be an ideal of a ring  $R$  and  $a$  an element of  $R$ . We have that  $a \in I$  if and only if  $(a) + I = I$ .

*Remark.* Observe that the notation  $Ra_i$  in Theorem 1.3.9 denotes the principal ideal generated by  $a_i$ . The notation does coincide with the notation in the previous corollary. Theorem 1.3.9 tells us that  $Ra_1 + Ra_2 + \dots + Ra_n$  is the smallest ideal containing  $a_1, a_2, \dots, a_n$ . The previous corollary tells us that  $Ra_1 + Ra_2 + \dots + Ra_n$  is the smallest ideal containing the ideals  $Ra_1, Ra_2, \dots, Ra_n$ . We conclude that

$$(a_1, a_2, \dots, a_n) = (a_1) + (a_2) + \dots + (a_n).$$

**Definition 1.3.14.** An ideal which can be generated by a finite set is called a **finitely generated** ideal. An ideal which can be generated by a single element is called a **principal** ideal.

**Example 1.3.15.** Inside the ring  $\mathbb{Z}$ , the ideal of all multiples of 6 can be written as  $(6)$ ,  $\mathbb{Z}6$  or  $6\mathbb{Z}$ . This is a principal ideal.

**Lemma 1.3.16.** Let  $R$  be a commutative ring and let  $(a)$  and  $(b)$  be two nonzero principal ideals of  $R$ . Then  $(a) \subseteq (b)$  if and only if  $b|a$ .

Let's investigate the ideals of  $\mathbb{Z}$ .

**Proposition 1.3.17.** Let  $I = (a_1, a_2)$  where  $a_1, a_2 \in \mathbb{Z}$ , and let  $d$  be the greatest zero divisor of  $a_1$  and  $a_2$ , denoted  $\text{g.c.d.}(a_1, a_2)$ . Then  $I = (d)$ . In general,

$$I = (a_1, a_2, \dots, a_n) = (\text{g.c.d.}(a_1, a_2, \dots, a_n))$$

From this proposition we see that all finitely generate ideals in  $\mathbb{Z}$  are principal ideals. The next theorem tells us what happens in the general case.

**Theorem 1.3.18.** *Every ideal in  $\mathbb{Z}$  is a principal ideal. Hence every ideal in  $\mathbb{Z}$  is of the form  $n\mathbb{Z}$ .*

**Example 1.3.19.** In  $\mathbb{Z}$  find  $(12) + (20)$  and  $(12) \cap (20)$ .

**Definition 1.3.20.** Let  $R$  be a ring. An ideal  $P$  of  $R$  is called a **prime ideal** if  $P$  is proper and if for all  $ab \in P$  we have either  $a \in P$  or  $b \in P$ .

*Remark.* The following conditions are the the equivalent criterions for prime ideals.

- (1)  $ab \in P \implies a \in P$  or  $b \in P$ .
- (2)  $a, b \notin P \implies ab \notin P$ .

**Definition 1.3.21.** Let  $R$  be a ring. We say an ideal  $M$  is called a **maximal ideal** if  $M$  is proper and if  $M$  is maximal with respect to inclusion of ideals. In other words, if an ideal  $N$  is such that  $M \subseteq N \subseteq R$  then  $N = R$  or  $N = M$ .

**Definition 1.3.22.** Let  $I$  be an ideal of a ring  $R$ . We say  $I$  is a **radical ideal** if  $a^n \in I$  for some positive integer  $n$  implies  $a \in I$ .

**Example 1.3.23.** Identify all the prime ideals and maximal ideals in  $\mathbb{Z}$ . Identify all radical ideals.

**Proposition 1.3.24.** *Let  $I$  be an ideal of a commutative ring  $R$ . Then*

$$\sqrt{I} = \{a \in R : a^n \in I \text{ for some positive interger } n\}$$

*is a radical ideal.*

**Definition 1.3.25.** The ideal  $\sqrt{I}$  is called the **radical ideal of  $I$** .

**Example 1.3.26.** In  $\mathbb{Z}$  find  $\sqrt{(24)}$ .

#### 1.4. QUOTIENT RINGS

For this section we will assume all rings are commutative.

Let  $R$  be a commutative ring and let  $I$  be an ideal. Remember that by definition  $(R, +, 0)$  is an (abelian) additive group and  $I$  is a subgroup of  $R$ . Also remember that  $R/I$  denotes the quotient group modulo  $I$ . The elements of  $R/I$  are of the form

$$a + I, \quad a \in R.$$

It has a natural addition:

$$(a + I) + (b + I) = (a + b) + I, \quad a, b \in R,$$

which makes  $R/I$  an additive group with the additive identity  $I$ .

**Lemma 1.4.1.** *There is a natural binary operation*

$$(a + I)(b + I) = (ab) + I, \quad a, b \in R,$$

*on  $R/I$ . This gives a multiplication on  $R/I$ .*

**Theorem 1.4.2.** *Let  $R$  be an commutative ring and  $I$  be an ideal of  $R$ . The natural addition and multiplication makes  $(R/I, +, \cdot, I, 1 + I)$  into a commutative ring.*

**Definition 1.4.3.** The ring  $R/I$  is called **the quotient ring of  $R$  modulo the ideal  $I$** .

*Remark.* For  $a \in R$  the coset  $a + I$  is often denoted as  $\bar{a}$ .

**Example 1.4.4.** The ring  $\mathbb{Z}_n$  is the same as the quotient ring  $\mathbb{Z}/(n)$ .

**Proposition 1.4.5.** *Let  $R$  be a commutative ring and let  $I$  be an ideal of  $R$ . The following statements are true.*

- (1)  $R/I$  is an integral domain if and only if  $I$  is a prime ideal.
- (2)  $R/I$  is a field if and only if  $I$  is a maximal ideal.
- (3)  $R/I$  is a reduced ring if and only if  $I$  is a radical ideal.

**Corollary 1.4.6.** *In a commutative ring all maximal ideals are prime ideals, and all prime ideals are radical ideals.*