1 Introduction to Rings

1.1 Basic Definitions and Examples

Definition.

1. A *ring* R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

   (a) $(R, +)$ is an abelian group,

   (b) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$,

   (c) the *distributive laws* hold in R: for all $a, b, c \in R$,

   $$(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c).$$

2. The ring R is *commutative* if multiplication is commutative.

3. The ring R is said to have an *identity* (or *contain a 1*) if there is an element $1 \in R$ with
$$1 \times a = a \times 1 = a \qquad \text{for all } a \in R.$$

Note.

1. We shall write ab rather than $a \times b$ for $a, b \in R$.

2. The additive identity of R will be denoted by 0

3. The additive of an element a will be denoted $-a$.

Note. $R = \{0\}$ is called the *zero ring*, denoted $R = 0$. $R = 0$ is the only ring where $1 = 0$. We will often exclude this ring by imposing the condition $1 \neq 0$.

Definition. A ring R with identity $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field*.

Proposition 1. Let R be a ring. Then

1. $0a = a0 = 0$ for all $a \in R$.

2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.

3. $(-a)(-b) = ab$ for all $a, b \in R$.

4. If R has an identity 1, then the identity is unique and $-a = -1(a)$.

Definition. Let R be a ring

1. A nonzero element a of R is called a *zero divisor* if there is a nonzero element b of R such that either $ab = 0$ or $ba = 0$.

2. Assume R has an identity $1 \neq 0$. An element u of R is called a *unit* in R if there is some v in R such that $vu = uv = 1$. The set of units in R is denoted $R^\times$.

Note.

1. $R^\times$ forms a group under multiplication and will be referred to as the *group of units* of R.

2. Using the above terminology a field is a commutative ring F with identity $1 \neq 0$ in which every nonzero element is a unit, i.e., $F^\times = F - \{0\}$.

Definition. A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

Proposition 2. Assume a, b and c are elements of any ring with a not a zero divisor. If $ab = ac$ then either $a = 0$ or $b = c$ (i.e., if $a \neq 0$ we can cancel the a's). In particular, if a, b, c are elements in an integral domain and $ab = ac$, then either $a = 0$ or $b = c$.

Corollary 3. Any finite integral domain is a field.

Definition. A *subring* of the ring R is a subgroup of R that is closed under multiplication.

Note. To show that a subset of a ring R is a subring it is enough to show that it is nonempty and closed under subtraction and under multiplication.

1.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings

Proposition 4. Let R be an integral domain and let $p(x), q(x)$ be nonzero elements of $R[x]$. Then

1. $\text{degree} p(x)q(x) = \text{degree} p(x) + \text{degree} q(x)$,

2. The units of $R[x]$ are just the units of R,

3. $R[x]$ is an integral domain.

1.3 Ring Homomorphisms and Quotient Rings

Definition. Let R and S be rings.

1. A *ring homomorphism* is a map $\varphi \colon R \to S$ satisfying

   (a) $\varphi(a + b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$ (so φ is a group homomorphism on the additive groups) and

   (b) $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

2. The *kernel* of the ring homomorphism φ, denoted $\ker\varphi$, is the set of elements of R that map to 0 in S. (i.e., the kernel of φ viewed as a homomorphism of additive groups).

3. A bijective ring homomorphism is called an *isomorphism*.

Proposition 5. Let R and S be rings and let $\varphi \colon R \to S$ be a homomorphism.

1. The image of φ is a subring of S.

2. The kernel of φ is a subring of R. Furthermore, if $\alpha \in \ker\varphi$ then $r\alpha$ and $\alpha r \in \ker\varphi$ for every $r \in R$, i.e., $\ker\varphi$ is closed under multiplication by elements from R.

Definition. Let R be a ring, let I be a subset of R and let $r \in R$.

1. $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$.
2. A subset I of R is a *left Ideal* of R if
   (a) I is a subring of R, and
   (b) I is closed under left multiplication by elements of R, i.e., $rI \subseteq I$ for all $r \in R$.

   Similarly I is a *right ideal* if (a) holds and in place of (b) one has

   (b)' I is closed under right multiplication by elements from R, i.e., $Ir \subseteq I$ for all $r \in R$.
3. A subset I that is both a left ideal and a right ideal is called an *ideal* (or, for added emphasis, a *two-sided ideal*) of R.

Proposition 6. Let R be a ring and let I be an ideal of R. Then the (additive) quotient group R/I is a ring under the binary operations:

$$(r + I) + (s + I) = (r + s) + I \qquad \textit{and} \qquad (r + I) \times (s + I) = (rs) + I$$

for all $r, s \in R$. Conversely, if I is any subgroup such that the above operations are well defined, then I is an ideal of R.

Definition. When I is an ideal of R the ring R/I with the operations in the previous proposition us called the *quotient ring* of R by I.

Theorem 7. 1. (The First Isomorphism Theorem for Rings) If $\varphi\colon R \to S$ is a homomorphism of rings, then the kernel of φ is an ideal of R, the image of φ is a subring of S and $R/\ker\varphi$ is isomorphic as a ring to $\varphi(R)$.

2. If I is any ideal of R, then the map

$$R \to R/I \qquad \text{defined by} \qquad r \mapsto r + I$$

is a surjective ring homomorphism with kernel I (this homomorphism is called the *natural projection* of R onto R/I). Thus every ideal is the kernel of a ring homomorphism and vice versa.

Theorem 8. Let R be a ring.

1. (The Second Isomorphism Theorem for Rings) Let A be a subring and let B be an ideal of R. Then $A + B = \{a + b \mid a \in A, b \in B\}$ is a subring of R, $A \cap B$ is an ideal of A and $(A + B)/B \cong A/(A \cap B)$.
2. (The Third Isomorphism Theorem for Rings) Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$.

3. (The Fourth or Lattice Isomorphism Theorem for Rings) Let I be an ideal of R. The correspondence $A \leftrightarrow A/I$ is an inclusion preserving bijective between the set of subrings A of R that contain I and the set of subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

Definition. Let I and J be ideals of R.

1. Define the *sum* of I and J by $I + J = \{a + b \mid a \in I, b \in J\}$.

2. Define the *product* of I and J, denoted by IJ, to be the set of all finite sums of elements of the form ab with $a \in I$ and $b \in J$.

3. For any $n \geq 1$, define the n^{th} *power* of I, denoted I^n, to be the set consisting of all finite sums of elements of the form $a_1 a_2 \cdots a_n$ with $a_i \in I$ for all i. Equivalently, I^n is defined inductively by defining $I^1 = I$ and $I^n = II^{n-1}$ for $n = 2, 3, \ldots$.

1.4 Properties of Ideals

Throughout this section R is a ring with identity $1 \neq 0$.

Definition. Let A be any subset of the ring R.

1. Let (A) denote the smallest ideal of R containing A, called *the ideal generated by* A.

2. Let RA denote the set of all finite sums of elements of the form ra with $r \in R$ and $a \in A$ i.e., $RA = \{r_1 a_2 + r_2 a_2 + \ldots + r_n a_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$

   (where the convention is $RA = 0$ if $A = \emptyset$).

   Similarly, $AR = \{a_1 r_2 + a_2 r_2 + \ldots + a_n r_n \mid r_i \in R, a_i \in A, n \in \mathbb{Z}^+\}$ and

   $RAR = \{r_1 a_2 r_1' + r_2 a_2 r_2' + \ldots + r_n a_n r_n' \mid r_i, r_i' \in R, a_i \in A, n \in \mathbb{Z}^+\}$

3. An ideal generated by a single element is called a *principal ideal.*

4. An ideal generated by a finite set is called a *finitely generated ideal.*

Note. When $A = \{a\}$ or $\{a_1, a_2, \ldots\}$, etc. we shall simply write (a) or $(a_1, a_2, \ldots)$ for (A), respectively.

Note.

1. Analogous to subgroups generated by subsets of a group (section 2.4), we have

$$(A) = \bigcap_{\substack{I \text{ an ideal} \\ A \subseteq I}} I$$

2. RAR is the ideal generated by A.

3. If R is commutative then $RA = AR = RAR = (A)$.

Proposition 9. Let I be an ideal of R.

1. $I = R$ if and only if I contains a unit.

2. Assume R is commutative. Then R is a field if and only if its only ideals are 0 and R.

Corollary 10. If R is a field then any nonzero ring homomorphism from R into another ring is an injection.

Definition. An ideal M is an arbitrary ring S is called a *maximal ideal* if $M \neq S$ and the only ideals containing M are M and S, i.e., there is no ideal I such that $M \subsetneq I \subsetneq S$.

Proposition 11. In a ring with identity every proper ideal is contained in a maximal ideal.

Proposition 12. Assume R is commutative. The ideal M is maximal if and only if the quotient ring R/M is a field.

Definition. Assume R is commutative. An ideal P is called a *prime ideal* if $P \neq R$ and whenever the product ab of two elements $a, b \in R$ is an element of P, then at least one of a and b is an element of P.

Proposition 13. Assume R is commutative. Then the ideal P is a prime ideal in R if and only if the quotient ring R/P is an integral domain.

Corollary 14. Assume R is commutative. Every maximal ideal of R is a prime ideal.

1.5 Rings of Fractions

Theorem 15. Let R be a commutative ring. Let D be any nonempty subset of R that does not contain 0, does not contain any zero divisors, and is closed under multiplication (i.e., $ab \in D$ for all $a, b \in D$). Then there is a commutative ring Q with 1 such that Q contains R as a subring and every element of D is a unit in Q. The ring Q has the following additional properties.

1. Every element of Q is of the form rd^{-1} for some $r \in R$ and $d \in D$. In particular, if $D = R - \{0\}$ then Q is a field.
2. (uniqueness of Q) The ring Q is the "smallest" ring containing R in which all elements of D becomes units, in the following sense. Let S be any commutative ring with identity and let $\varphi\colon R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in S for every $d \in D$. Then there is an injective homomorphism $\Phi\colon Q \to S$ such that $\Phi|_R = \varphi$. In other words, any ring containing an isomorphic copy of R in which all elements of D become units must also contain an isomorphic copy of Q.

Definition. Let R, D and Q be as in Theorem 15.

1. The ring Q is called the *ring of Fractions* of D with respect to R and is denoted $D^{-1}R$.
2. If R is an integral domain and $D = R - \{0\}$, Q is called the *field of fractions* or *quotient field* of R.

Note. If A is a subset of a field F, then the intersection of all the subfields of F containing A is a subfield of F and is called the *subfield generated by* A.

Corollary 16. Let R be an integral domain and let Q be the field of fractions of R. If a field F contains a subring R' isomorphic to R then the subfield of F generated by R' is isomorphic to Q.

1.6 The Chinese Remainder Theorem

Assume unless otherwise stated that all rings are commutative with identity $1 \neq 0$.

Definition. The ideals A and B of the ring R are said to be *comaximal* if $A + B = R$.

Theorem 17. (Chinese Remainder Theorem) Let $A_1, A_2, \ldots, A_k$ be ideals in R. The map

$$R \to R/A_1 \times R/A_2 \times \cdots \times R/A_k \qquad \text{defined by} \qquad r \mapsto (r + A_1, r + A_2, \ldots, r + A_k)$$

is a ring homomorphism with kernel $A_1 \cap A_2 \cap \ldots \cap A_k$. If for each map $i, j \in \{1, 2, \ldots, K\}$ with $i \neq j$ the ideals A_i and A_j are comaximal, then this map is surjective and $A_1 \cap A_2 \cap \ldots \cap A_k = A_1 A_2 \cdots A_k$, so

$$R/(A_1 A_2 \cdots A_k) = R/(A_1 \cap A_2 \cap \ldots \cap A_k) \cong R/A_1 \times R/A_2 \times \cdots \times R/A_k.$$

Corollary 18. Let n be a positive integer and let $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be its factorization into powers of distinct primes. Then

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}),$$

as rings, so in particular we have the following isomorphism of multiplicative groups:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times.$$