1. Rings and Ideals

Definition. A *ring*, R, is a non-empty set with two binary operations, addition (denoted $+$), and multiplication, (denoted $\cdot$ or with the $\cdot$ omitted), such that the following hold:

(1) $+$ and $\cdot$ are both commutative and associative;
(2) Both $+$ and $\cdot$ have identities, denoted 0 and 1 respectively.
(3) Additive inverses exist.
(4) Multiplication distributes over addition.

In general, multiplication in a ring need not be commutative nor have an identity, but for our purposes it always will.

Example. The set of integers, $\mathbb{Z}$, with standard addition and multiplication is a ring.

NOTE: In the sequel, R will denote a ring.

Definition. A subset $I \subseteq R$ is an *ideal* if the following hold:

(1) $a, b \in I \Rightarrow a + b \in I$.
(2) $a \in I, b \in R \Rightarrow a \cdot b \in I$.
(3) $0 \in I$.

Example. The sets $\{0\}$ and R are ideals in R.

Exercise. Show the set of even integers in $\mathbb{Z}$ is an ideal.

Exercise. Show that the intersection of ideals is an ideal.

Definition. For $X \subseteq R$, *the ideal generated by* X, denoted (X), is the smallest ideal in R containing X. An ideal generated by a finite set $\{r_1, r_2, \ldots, r_n\}$ is called *finitely generated* and is generally written $(r_1, r_2, \ldots, r_n)$. An ideal generated by a single element is called a *principal ideal*.

Exercise. For $X \subseteq R$, show $(X) = \{\sum_{i=1}^{n} r_i x_i : x_i \in X, r_i \in R, n \in \mathbb{Z}_{\geq 1}\}$.

Definition. For I and J ideals in R, let:

(1) $I + J = \{i + j : i \in I, j \in J\}$.
(2) $IJ = (\{ij : i \in I, j \in J\})$.

Exercise. Show that if I and J are ideals, then so is $I + J$.

Exercise. Let $I = (X)$, $J = (Y)$. Show that $IJ = (\{x \cdot y : x \in X, y \in Y\})$

Exercise. Give an example of a ring R and two ideals $I, J \subseteq R$ such that $\{ij : i \in I, j \in J\}$ is not an ideal.

Definition. Elements $a, b \in R$ are *zero-divisors* if they are non-zero but $ab = 0$. If R has no zero-divisors and $0 \neq 1$, then it is an *(integral) domain*.

Exercise. Show that $\mathbb{Z}/4\mathbb{Z}$ is not a domain.

Definition. A domain R in which all ideals are principal ideals is called a *principal ideal domain* or *PID*.

Exercise. Show that $\mathbb{Z}$ is a PID. (Hint: use the Euclidean algorithm.)

Definition. An ideal $I \subseteq R$ is *prime* if $I \neq R$ and $ab \in I \Rightarrow a \in I$ or $b \in I$.

Exercise. Show that, for $(n) \subseteq \mathbb{Z}$, the ideal (n) is prime if and only if n is a prime number.

Definition. A proper ideal $M \subsetneq R$ is *maximal* if for every ideal $I \supseteq M$, either $I = M$ or $I = R$. Note that R, itself, is not considered a maximal ideal.

Exercise. Show that every maximal ideal is prime.

2. Homomorphisms

Definition. For rings R, S, a mapping $\varphi : R \to S$ is a *ring homomorphism* if the following properties hold:

(1) $\varphi(r) \cdot \varphi(s) = \varphi(r \cdot s)$ for all $a, b \in R$.
(2) $\varphi(r) + \varphi(s) = \varphi(r + s)$ for all $a, b \in R$.
(3) $\varphi(1) = 1$.

Definition. A ring homomorphism is a *ring isomorphism* if it is bijective.

Exercise. Show that the inverse of a ring isomorphism is a ring homomorphism and therefore also a ring isomorphism.

Definition. Let $\varphi : R \to S$ be a ring homomorphism. The *kernel* of φ is the set

$$\ker(\varphi) = \{r \in R : \varphi(r) = 0\}.$$

The *image* of φ is the set

$$\mathrm{im}(\varphi) = \varphi(R) = \{s \in S : s = \varphi(r) \text{ for some } r \in R\}.$$

Exercise. Show that the kernel of ring homomorphism $\varphi : R \to S$ is an ideal in R.

3. Quotient Rings

Definition. A binary relation, $\sim$, on a set S is an *equivalence relation* if it is reflexive, symmetric, and transitive. That is, for all $a, b, c \in S$:

(1) $a \sim a$.
(2) $a \sim b \Rightarrow b \sim a$.
(3) $a \sim b$, $b \sim c \Rightarrow a \sim c$.

Definition. An equivalence relation $\sim$ on S partitions S into disjoint subsets of the form $[a] = \{s \in S : s \sim a\}$, called *equivalence classes*. The subset $[a]$, frequently abbreviated to a is called *the equivalence class of* a.

Exercise. Show that for any ideal $I \subseteq R$, $\sim$ defined by $(a \sim b) \iff (a - b) \in I$ is an equivalence relation. Here $a - b = a + (-b)$, where $-b$ is the additive inverse of b.

Definition. For a ring R and an equivalence relation $\sim$ on R, the *quotient* $R/\sim$, pronounced "R mod $\sim$", is the set of all equivalence classes of elements of R. For an ideal $I \subseteq R$, the *quotient ring* R/I is $R/\sim$ where $\sim$ is defined by $(a \sim b) \iff (a - b) \in I$.

Exercise. For an ideal $I \subseteq R$, show that R/I is a ring under the operations $[a]+[b] = [a+b]$ and $[a] \cdot [b] = [a \cdot b]$. Note that you will need to show that these operations are well-defined.

Exercise. An ideal $I \subseteq R$ is prime if and only if R/I is a domain.

Definition. A *field*, k, is a ring such that for all non-zero $a \in k$ there exists a multiplicative inverse of a in k, and $0 \neq 1$.

Example. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Z}/p\mathbb{Z}$ for p a prime are fields. $\mathbb{Z}$ is not a field.

Exercise. An ideal $I \subseteq R$ is maximal if and only if R/I is a field.

Exercise. Let $\varphi : R \to S$ be a ring homomorphism. Define $\psi : R/\ker(\varphi) \to S$ by $\psi(r) = \varphi(r)$ for all $r \in R/\ker(\varphi)$. Show ψ is injective.

4. Polynomial Rings

Definition. A *polynomial over* R is an expression of the form

$$p = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

where each *coefficient*, a_i, is an element of R and where x is a formal symbol. The *degree* of p is d provided $a_d \neq 0$. The collection of all polynomials is the *ring of polynomials over* R, denoted $R[x]$. The ring structure is given by

$$\left(\sum_i a_i x^i\right) + \left(\sum_i b_i x^i\right) = \sum_i (a_i + b_i) x^i$$

and

$$\left(\sum_i a_i x^i\right)\left(\sum_i b_i x^i\right) = \sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k.$$

Define the *polynomial ring in n variables,* $x_1, \ldots, x_n$, by $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$.

Theorem 4.1. *Let $f, g \in k[x]$, where k is a field and $g \neq 0$. Then there exist $q, r \in k[x]$, where* $\deg(r) < \deg(g)$ *such that $f = qg + r$.*

Exercise. For any field k, the polynomial ring $k[x]$ is a principal ideal domain. (Hint: given a non-zero ideal $I \subseteq k[x]$, choose a non-zero element $f \in I$ of least degree. Using the quotient-remainder theorem, just cited, show that $I = (f)$.)

Exercise. Let $f \in k[x]$ and suppose $f(a) = 0$ for some $a \in k$. Show that $x - a$ divides f, i.e., there exists $q \in k[x]$ such that $f = (x-a)q$. Use this to show that a non-zero polynomial $f \in k[x]$ has at most $\deg(f)$ zeroes.

Definition. A field k is *algebraically closed* if every polynomial $f \in k[x]$ of degree at least 1 has a zero in k, i.e., there exists $a \in k$ such that $f(a) = 0$.

Example. $\mathbb{R}$ and $\mathbb{Z}/p\mathbb{Z}$ for p prime are not algebraically closed. $\mathbb{C}$ is algebraically closed.

5. Exact Sequences

Definition. A sequence of rings, $\{R_i\}$, and ring homomorphisms $\{\varphi_i : R_i \to R_{i+1}\}$, is *exact at* R_i if $\mathrm{im}(\varphi_{i-1}) = \ker(\varphi_i)$. The sequence is *exact* if it is exact at every R_i except for the first and last.

Definition. A *short exact sequence* is an exact sequence with only 5 rings, beginning and ending with the trivial ring, i.e., the one with only a single element, denoted 0:

$$0 \longrightarrow A \xrightarrow{\varphi} B \xrightarrow{\psi} C \longrightarrow 0$$

Exercise. Show the following facts about a short exact sequence as above:

(1) φ is injective.
(2) ψ is surjective.
(3) C is isomorphic to B/A.

Exercise. Short exact sequences can be defined identically for vector spaces and linear mappings, instead of rings and ring homomorphisms. Given a short exact sequence of vector spaces:

$$0 \longrightarrow V'' \longrightarrow V \longrightarrow V' \longrightarrow 0$$

show $\dim(V) = \dim(V') + \dim(V'')$.