Chapter III. Rings

Section III.1. Rings and Homomorphisms

Note. In this section, we introduce rings and define “field.” Rings will play a large role in our eventual study of the insolvability of the quintic because polynomials will be elements of rings.

Definition III.1.1. A *ring* is a nonempty set $R$ together with two binary operations (denoted + and multiplication) such that:

(i) $(R, +)$ is an abelian group.

(ii) $(ab)c = a(bc)$ for all $a, b, c \in R$ (i.e., multiplication is associative).

(iii) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (left and right distribution of multiplication over $+$).

If in addition,

(iv) $ab = ba$ for all $a, b \in R$,

then $R$ is a *commutative ring*. If $R$ contains an element $1_R$ such that

(v) $1Ra = a1_R = a$ for all $a \in R$,

then $R$ is a *ring with identity* (or *unity*).

Note. An obvious “shortcoming” of rings is the possible absence of inverses under multiplication.
Note. We adopt the standard notation from \((R, +)\). We denote the \(+\) identity as 0 and for \(n \in \mathbb{Z}\) and \(a \in R\), \(na\) denotes the obvious repeated addition (see Definition I.1.8).

Theorem III.1.2. Let \(R\) be a ring. Then

(i) \(0a = a0 = 0\) for all \(a \in R\).

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

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

(iv) \((na)b = a(nb) = n(ab)\) for all \(n \in \mathbb{Z}\) and for all \(z, b \in R\).

(v) For all \(a_i, b_j \in R\),

\[
\left( \sum_{i=1}^{n} a_i \right) \left( \sum_{j=1}^{m} b_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j.
\]

Definition III.1.3. A nonzero element \(a\) in the ring \(R\) is a left (respectively, right) zero divisor if there exists a nonzero \(b \in R\) such that \(ab = 0\) (respectively, \(ba = 0\)). A zero divisor is an element of \(R\) which is both a left and right zero divisor.

Lemma III.1.A. A ring has no zero divisors if and only if left or right cancellation hold in \(R\) (that is, for all \(a, b, c \in R\) with \(a \neq 0\), if either \(ab = ac\) or \(ba = ca\) then \(b = c\)).
**Definition III.1.4.** An element $a$ in a ring $R$ with identity is *left invertible* (respectively, *right invertible*) if there exists $c \in R$ (respectively, $b \in R$) such that $ca = 1_R$ (respectively, $ab = 1_R$). The element $c$ (respectively, $b$) is a *left* (respectively, *right*) *inverse* of $a$. An element $a \in R$ that is both left and right invertible is *invertible* and is called a *unit*.

**Note.** If $a$ has a left inverse $c$ and a right inverse $b$ then $ca = 1_R = ab$ and so $b = 1_Rb = (ca)b = c(ab) = c1_R = c$. The set of all units in a ring $R$ with identity forms a group under multiplication (Exercise III.1.A)—you have seen an example of this before when considering the group $(\mathbb{R}^*, \cdot)$, for example.

**Definition III.1.5.** A commutative ring $R$ with identity $1_R$ and no zero divisors is an *integral domain*. A ring $D$ with identity $1_D \neq 0$ in which every nonzero element is a unit is a *division ring*. A *field* is a commutative division ring.

**Note.** A ring $R$ with identity is a division ring if and only if the nonzero elements of $R$ form a group under multiplication (Exercise III.1.B). Every field $F$ is an integral domain since $ab = 0$ and $a \neq 0$ imply that $b = 1_Fb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$.

**Example.** The integers $\mathbb{Z}$ form an integral domain. The ring $2\mathbb{Z}$ is a commutative ring without identity. Examples of fields are $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. The set of all $n \times n$ matrices with entries from $\mathbb{Q}$ (or $\mathbb{R}$ or $\mathbb{C}$) form a noncommutative ring with identity. The units here are the nonsingular matrices.
Example. For $p$ prime, $\mathbb{Z}_p$ is a field. If $n$ is not prime, then $\mathbb{Z}_n$ is a commutative ring with unity. The divisors of zero are those equivalence classes whose representatives, $1, 2, \ldots, n - 1$, are not relatively prime with $n$.

Example. Let $G$ be a multiplicative group and $R$ a ring. We now define a ring $R(G)$ called the group ring of $G$ over $R$. Let $R(G)$ be the additive abelian group $\sum_{g \in G} R$ (one copy of $R$ for each $g \in G$) where we require all but finitely many entries in a “$|G|$-tuple” to be 0. So for $x \in R(G)$, say $x = \{r_g\}_{g \in G}$ where the nonzero $r_g$ are $r_{g_1}, r_{g_2}, \ldots, r_{g_n}$, denote $x$ as the formal sum

$$r_{g_1}g_1 + r_{g_2}g_2 + \cdots + r_{g_n}g_n = \sum_{i=1}^{n} r_{g_i}g_i.$$  

In the formal sum, we allow some of the $r_{g_i}$ to be zero and some of the $g_i$ to be repeated. So an element of $R(G)$ can be written as a formal sum in different ways (for example, $r_{g_1}g_1 + 0g_2 = r_{g_1}g_1$ and $r_{g_1}g_1 + s_{g_1}g_1 = (r_{g_1} + s_{g_1})g_1$). We define addition on $R(G)$ as

$$\sum_{i=1}^{n} r_{g_i}g_i + \sum_{i=1}^{n} s_{g_i}g_i = \sum_{i=1}^{n} (r_{g_i} + s_{g_i})g_i$$

(where zero coefficients are inserted so that the formal sums involve exactly the same indices $g_1, g_2, \ldots, g_n$). Define multiplication on $R(G)$ as

$$\left(\sum_{i=1}^{n} r_{g_i}g_i\right) \left(\sum_{j=1}^{m} s_{g_j}h_j\right) = \sum_{i=1}^{n} \sum_{j=1}^{m} (r_{g_i} s_{g_j})(g_i h_j).$$

Notice that $r_{g_i} s_{h_j}$ make sense since it is a product in ring $R$. Product $g_i h_j$ makes sense since it is a product in multiplicative group $G$. We claim

- $R(G)$ is a group under addition and multiplication as defined.
III.1. Rings and Homomorphism

- $R(G)$ is commutative if and only if both $R$ and $G$ are commutative.
- If $R$ has identity $1_R$ and $G$ has identity $e$ then $1_R e$ is the identity of $R(G)$.

**Example.** Let $S = \{1, i, j, k\}$. Let $K$ be the additive abelian group $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$ and write the elements of $K$ as formal sums $(a_0, a_1, a_2, a_3) = a_0 1 + a_1 i + a_2 j + a_3 k$. We often drop the “1” in “$a_0 1$” and replace it with just $a_0$. Addition in $K$ is as expected:

$$(a_0+a_1i+a_2j+a_3k) + (b_0+b_1i+b_2j+b_3k) = (a_0+b_0) + (a_1+b_1)i + (a_2+b_2)j + (a_3+b_3)k.$$ 

We turn $K$ into a ring by defining multiplication as

$$(a_0 + a_1 i + a_2 j + a_3 k)(b_0 + b_1 i + b_2 j + b_3 k) = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3) + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)i + (a_0b_2 + a_2b_0 + a_3b_1 - a_1b_3)j + (a_0b_3 + a_3b_0 + a_1b_2 - a_2b_1)k.$$ 

This product can be interpreted by considering:

(i) multiplication in the formal sum is associative,

(ii) $ri = ir$, $rj = jr$, $rk = kr$ for all $r \in \mathbb{R}$,

(iii) $i^2 = j^2 = k^2 = ijk = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

We claim that $K$ is a noncommutative division ring where $(a_0 + a_1i + a_2j + a_3k)^{-1} = \frac{a_0}{d} - \frac{a_1}{d}i - \frac{a_2}{d}j - \frac{a_3}{d}k$ where $d = a_0^2 + a_1^2 + a_2^2 + a_3^2$. $K$ is called the division ring of real quaternions. You may have encountered the quaternions as a multiplicative group of order 8 with elements $\pm 1, \pm i, \pm j, \pm k$. See my Introduction to Modern Algebra (MATH 4127/5127) notes.
The real quaternions division ring may also be interpreted as a subring of the ring of all $2 \times 2$ matrices over $\mathbb{C}$ (see Exercise III.1.8).

**Note.** In a ring, we use the usual notation $na$ for repeated addition and $a^n$ for repeated multiplication, where $n \in \mathbb{Z}$. Recall that for $k, n \in \mathbb{Z}$ with $0 \leq k \leq n$, the binomial coefficient is $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

**Theorem III.1.6.** Binomial Theorem.

Let $R$ be a ring with identity, $n \in \mathbb{N}$, and $a, b, a_1, a_2, \ldots, a_s \in R$.

(i) If $ab = ba$ then $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.

(ii) If $a_i a_j = a_j a_i$ for all $i$ and $j$, then

$$(a_1 + a_2 + \cdots + a_s)^n = \sum \frac{n!}{i_1!i_2!\cdots i_s!} a_1^{i_1}a_2^{i_2}\cdots a_s^{i_s}$$

where the sum is over all $s$-tuples $(i_1, i_2, \ldots, i_n)$ where $i_1 + i_2 + \cdots + i_s = n$.

**Definition III.1.7.** Let $R$ and $S$ be rings. A function $f : R \to S$ is homomorphism of rings provided that for all $a, b \in R$ we have

$$f(a + b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b).$$

The kernel of a homomorphism of rings $f : R \to S$ is $\text{Ker}(f) = \{ r \in R \mid f(r) = 0 \}$. 
Note. If $f : R \to S$ is a ring homomorphism where $1_R$ and $1_S$ are multiplicative identities in $R$ and $S$ respectively, then it is not necessary that $f(1_R) = 1_S$; see Exercises III.1.15 and III.1.16.

Note. Just as we did for groups, we can define for rings: monomorphism (one to one homomorphism), epimorphism (onto homomorphism), isomorphism, and automorphism.

**Definition III.1.8.** Let $R$ be a ring. If there is a least positive integer $n$ such that $na = 0$ for all $a \in R$, then $R$ has *characteristic* $n$. If no such $n$ exists, then $R$ is said to have *characteristic zero*.

Note. The following result (part (ii)) shows that the characteristic of a ring with unity can by found by considering unity only.

**Theorem III.1.9.** Let $R$ be a ring with identity $1_R$ and characteristic $n > 0$.

(i) If $\varphi : \mathbb{Z} \to R$ is the map given by $m \mapsto m1_R$, then $\varphi$ is a homomorphism of rings, with kernel $\langle n \rangle = \{kn \mid k \in \mathbb{Z}\} = n\mathbb{Z}$.

(ii) $n$ is the least positive integer such that $n1_R = 0$.

(iii) If $R$ has no zero divisors (in particular, if $R$ is an integral domain) then $n$ is prime.
Theorem III.1.10. Every ring $R$ may be embedded in a ring $S$ with identity (that is, there is a one to one homomorphism mapping $R$ into $S$). The ring $S$ (which is not unique) may be chosen to be either of characteristic zero or of the same characteristic as $R$.