Arkansas Tech University
MATH 4033: Elementary Modern Algebra
Dr. Marcel B. Finan

25 Integral Domains. Subrings

In Section 24 we defined the terms **unitary rings** and **commutative rings.** These terms together with the concept of **zero divisors** discussed below are used to define a special type of ring known as an **integral domain.**
Let R be a ring. Then, by Theorem 24.1(ii), we have $a0 = 0a = 0$ for all $a \in R$. This shows that if a product is zero then one of the factors is 0. The converse is not always true. For example, in $\mathbb{Z}_{10}$, [2] and [5] are nonzero elements with $[2] \odot [5] = [0]$. The following definition singles out those rings where a product of two (additive) nonidentity elements is the zero element.

Definition 25.1
Let R be a commutative ring. An element $a \in R, a \neq 0$ is called a **zero divisor** *in R if there exists an element $b \in R, b \neq 0$ such that $ab = 0$.*

Example 25.1
1. The ring of integers $\mathbb{Z}$ has no zero divisors.
2. The elements [2] and [5] are zero divisors in $\mathbb{Z}_{10}$.■

Remark 25.1
Definition 25.1 is restricted to elements in a commutative ring. It is possible to have noncommutative rings where $ab = 0$ but $ba \neq 0$. Indeed, the ring of all 2×2 matrices is noncommutative. Moreover, we have

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

The following definition shows that zero divisors can not exist in an integral domain.

Definition 25.2
A commutative ring with unity $e \neq 0$ and no zero divisors is called an **integral domain.**

Remark 25.2
The requirement $e \neq 0$ means that the ring has at least two elements, the zero element and the unity element.

Example 25.2
1. $\mathbb{Z}$,$\mathbb{Q}$, and $\mathbb{R}$ are all integral domains.
2. The set E of evens integers is not an integral domain since it has no unity element.
3. $\mathbb{Z}_{10}$ is not an integral domain since [2] and [5] are zero divisors.
4. The ring $\mathcal{M}$ of all 2×2 matrices is not an integral domain for two reasons: first, the ring is noncommutative, and second, it has zero divisors. (See Remark 25.1■

Example 25.2(4), shows that $\mathbb{Z}_{10}$ is a commutative ring with unity but is not an integral domain since [2] and [5] are zero divisors. Note that $10 = 2 \times 5$. We can generalize this fact to any composite number n. So if $n = rs$ where $r, s > 1$, then $[r] \odot [s] = [rs] = [n] = [0]$ so that $[r]$ and $[s]$ are zero divisors of $\mathbb{Z}_n$. That is, $\mathbb{Z}_n$ is not an integral domain.
The next result provides a condition on n so that $\mathbb{Z}_n$ is an integral domain.

Theorem 25.1
For $n > 1$, $\mathbb{Z}_n$ has no zero divisors if and only if n is prime.

Proof.
Suppose first that n is prime. Let $[a] \odot [b] = [0]$ in $\mathbb{Z}_n$ with $[a] \neq [0]$. We will show that $[b] = [0]$ in $\mathbb{Z}_n$. Since $[a] \odot [b] = [0]$ then $[ab] = [0]$ and this implies that $n|ab$. Since $[a] \neq [0]$ then $n \not| a$. Since n is prime then by Lemma 13.3, we must have $n|b$. That is, $[b] = [0]$. Therefore, $\mathbb{Z}_n$ has no zero divisors, and is an integral domain.
Conversely, suppose that $\mathbb{Z}_n$ is an integral domain. Assume that n is not prime. As pointed out in the discussion preceding the theorem, $\mathbb{Z}_n$ is not an integral domain, a contradiction. Hence, n must be prime.■

An important consequence of the absence of zeros in an integral domain is that the cancellation law for multiplication must hold.

Theorem 25.2
If $a, b,$ and c are elements in integral domain D such that $a \neq 0$ and $ab = ac$, then $b = c$.

Proof.
Since $ab = ac$ then $a(b - c) = 0$ with $a \neq 0$ in D. But D is an integral domain so we must have $b - c = 0$ or $b = c$.■

The converse of the previous theorem is also true.

Theorem 25.3
If D is a commutative ring with unity $e \neq 0$ such that the cancellation property holds then D is an integral domain.

Proof.
Suppose that for all $a, b, c \in D, ab = ac$ and $a \neq 0$ implies $b = c$. We will show

that D has no zero divisors. Let $a, b \in D$ be such that $ab = 0$ with $a \neq 0$. Since $a0 = 0$ then $ab = a0$. By the cancellation law, $b = 0$. This shows that D has no zero divisors, so D is an integral domain.■

The notion of subring is the abvious analogue of the notion of subgroup.

Definition 25.3
A subring of a ring R is any subset $S \subseteq R$ which forms a ring with respect to the operation of R.

Example 25.3
The set E of even integers is a subring of all integers. The set of integers is a subring of the ring of rational numbers. The set of rational numbers is a subring of the ring of all real numbers. The set of all real numbers is a subring of the ring of complex numbers.■

As in groups, we can reduce the number of axioms one has to check when proving that something is a subring.

Theorem 25.4
Let R be a ring and S a subset of R. Then S is a subring of R if and only if

(i) $S \neq \emptyset$;
(ii) For all $a, b \in S$ we have $a - b \in S$ and $ab \in S$.

Proof.
Suppose first that S is a subring of R. Then S being a ring itself, it must contain the zero element of R. Thus, $S \neq \emptyset$. Now, let $a, b \in S$. Since S is a ring then $(S, +)$ is a group so that $a - b \in S$. Also, S is closed with respect to multiplication so that $ab \in S$.
Conversely, suppose that S is a subset of R satisfying conditions (i) and (ii). Since S is nonempty and $a - b \in S$ for all $a, b \in S$ then by Theorem 7.5, $(S, +)$ is a group. By (ii), S is closed with respect to multiplication. Since multiplication is associative in R and S is closed then multiplication is associative when restricted to S. Thus, S is a ring and hence a subring of R.■

Example 25.4
Consdier the subset of the ring $\mathcal{M}$ of all 2×2 matrices:

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

We will show that S is a subring of $\mathcal{M}$. Since the zero matrix is in S then $S \neq \emptyset$. Since

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} a-d & b-e \\ 0 & c-f \end{pmatrix} \in S$$

and

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ 0 & f \end{pmatrix} = \begin{pmatrix} ad & ae+bf \\ 0 & cf \end{pmatrix} \in S$$

then by Theorem 25.4, S is a subring of $\mathcal{M}$.■

Review Problems

Exercise 25.1
Find the zero divisors of $\mathbb{Z}_6$.

Exercise 25.2
Verify that $([2],[0])$ *is a zero divisor in* $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Exercise 25.3
Which elements of $\mathbb{Z} \times \mathbb{Z}$ *are zero divisors?*

Exercise 25.4
Prove that if an element a *in a ring* R *has a multiplicative inverse in* R*, then* a *is not a zero divisor in* R.

Exercise 25.5
Show that a zero divisor can not have a multiplicative inverse.

Exercise 25.6
Let R *be a commutative ring with unity* e*. Let* $a \in R$ *be such that* $a^n = 0$ *for some* $n \in \mathbb{N}$*. Prove that* a *is either 0 or a zero divisor.*

Exercise 25.7
Let D *be an integral domain. Show that if* $a \in D$ *such that* $a^2 = a$ *and* $a \neq e$ *then* a *is a zero divisor.*

Exercise 25.8
Let R *be a commutative ring. For each* $a \in R$ *let* $H_a = \{x \in R : ax = 0\}$*. Show that for all* $x, y \in H_a$*, we have* $xy \in H_a$.

Exercise 25.9
Show that $\mathbb{Z}[\sqrt{2}]$ *(Exercise 24.3) is an integral domain.*

Exercise 25.10
Show that the ring $\mathcal{M}(\mathbb{R})$ *of all mappings from* $\mathbb{R}$ *to* $\mathbb{R}$ *is not an integral domain.(See Exercise 24.4.)*

Exercise 25.11
State and prove a theorem giving a necessary and sufficient condition for a subset of an integral domain to be an integral domain.

Exercise 25.12
Prove that if D *is an integral domain and* $a^2 = e$ *then* $a = \pm e$.

Exercise 25.13
Let R *and* S *be integral domains. Prove that* $R \times S$ *is also an integral domain.*

Exercise 25.14
Let R *be a ring with unity* e*. Let* S *be the collection of all elements in* R *with multiplicative inverse. Prove that* $(S, \cdot)$ *is a group.*

Exercise 25.15
Let R be a commutative ring with unity e such that every nonzero element of R has a multiplicative inverse. Show that R is an integral domain.

Exercise 25.16
Let $C(\mathbb{R})$ denote the collection of all continuous functions from $\mathbb{R}$ to $\mathbb{R}$. Show that $C(\mathbb{R})$ is a subring of $\mathcal{M}(\mathbb{R})$.

Exercise 25.17
Prove that $\{(a, a) : a \in R\}$ is a subring of $R \times R$.

Exercise 25.18
Let R be a ring with identity e and S a subring of R such that $e \in S$. Prove that if u is a unit in S then u is a unit in R. Show by an example that the converse is false.

Exercise 25.19
The **center** *of a ring R is defined to be $\{c \in R : cr = rc \ \forall r \in R\}$. Prove that the center of a ring is a subring. What is the center ofa commutative ring?*

Exercise 25.20
Let $\mathcal{C}$ be the collection of all subrings of a ring R. Prove that $\cap_{H \in \mathcal{C}} H$ is a subring of R.

Exercise 25.21
Show that the set

$$S = \left\{ \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} \right\}$$

is not a subring of the ring $\mathcal{M}$ of all 2×2 matrices.