# Math 2070 Week 8

Commutative Rings, Integral Domains, Fields

## 8.1 Commutative Rings

**Definition 8.1.** A ring $R$ is said to be **commutative** if $ab = ba$ for all $a, b \in R$.

**Example 8.2.** For a fixed natural number $n > 1$, the ring of $n \times n$ matrices with integer coefficients, under the usual operations of addition and multiplication, is not commutative.

**Example 8.3.** Let $m$ be a natural number greater than 1. Let $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. Recall that for any integer $n \in \mathbb{Z}$, there exists a unique $\overline{n} \in \mathbb{Z}_m$, such that $n \equiv \overline{n} \mod m$. More precisely, $\overline{n}$ is the remainder of the division of of $n$ by $m$: $n = mq + r$. We equip $\mathbb{Z}_m$ with addition $+_m$ and multiplication $\times_m$ defined as follows: For $a, b \in \mathbb{Z}_m$, let:

$$a +_m b = \overline{a + b},$$
$$a \times_m b = \overline{a \cdot b},$$

where the addition and multiplication on the right are the usual addition and multiplication for integers.

**Claim 8.4.** *With addition and multiplication thus defined, $\mathbb{Z}_m$ is a commutative ring.*

*Proof of Claim 8.4.*

1. For $a, b \in \mathbb{Z}_m$, we have $a +_m b = \overline{a+b} = \overline{b+a} = b +_m a$, since addition for integers is commutative. So, $+_m$ is commutative.

2. For any $r_1, r_2 \in \mathbb{Z}$, by Claim 6.17 and Theorem 6.19 , we have

$$r_1 \equiv \overline{r_1} \mod m, \quad r_2 \equiv \overline{r_2} \mod m,$$

and:

$$\overline{r_1 + r_2} \equiv r_1 + r_2 \equiv \overline{r_1} + \overline{r_2} \equiv \overline{\overline{r_1} + \overline{r_2}} \mod m.$$

For $a, b, c \in \mathbb{Z}_m$, we have:

$$\begin{aligned} a +_m (b +_m c) &= a +_m \overline{b + c} \\ &= \overline{a + \overline{b + c}} \\ &= \overline{\overline{a} + \overline{b + c}} \\ &= \overline{a + (b + c)} \end{aligned}$$

But $a+(b+c)$ is equal to $(a+b)+c$, since addition for integers is associative. Hence, the above expression is equal to:

$$\begin{aligned} \overline{(a + b) + c} &= \overline{\overline{(a + b)} + \overline{c}} \\ &= \overline{\overline{a + b} + c} \\ &= \overline{(a +_m b) + c} \\ &= (a +_m b) +_m c. \end{aligned}$$

We conclude that $+_m$ is associative.

---

3. **Exercise:** We can take 0 to be the additive identity element.

4. For each nonzero element $a \in \mathbb{Z}_m$, we can take the additive inverse of $a$ to be $m - a$. Indeed, $a +_m (-a) = \overline{a + (m - a)} = \overline{m} = 0$.

5. By the same reasoning used in the case of addition, for $r_1, r_2 \in \mathbb{Z}$, we have

$$\overline{r_1 r_2} \equiv r_1 r_2 \equiv \overline{r_1} \cdot \overline{r_2} \equiv \overline{\overline{r_1} \cdot \overline{r_2}} \mod m.$$

For $a, b, c \in \mathbb{Z}_m$, we have:

$$a \times_m (b \times_m c) = a \times_m \overline{bc} = \overline{\overline{a} \cdot \overline{bc}} = \overline{a(bc)},$$

which by the associativity of multiplication for integers is equal to:

$$\overline{(ab)c} = \overline{\overline{ab} \cdot \overline{c}} = \overline{ab} \times_m c = (a \times_m b) \times_m c.$$

So, $\times_m$ is associative.

6. **Exercise:** We can take $1$ to be the multiplicative identity.

7. For $a, b \in \mathbb{Z}_m$, $a \times_m b = \overline{a \cdot b} = \overline{b \cdot a} = b \times_m a$. So $\times_m$ is commutative.

8. Lastly, we need to prove distributativity. For $a, b, c \in \mathbb{Z}_m$, we have:

$$\begin{aligned} a \times_m (b +_m c) &= \overline{\overline{a} \cdot \overline{b + c}} \\ &= \overline{a \cdot (b + c)} \\ &= \overline{ab + ac} \\ &= \overline{\overline{ab} + \overline{ac}} \\ &= a \times_m b +_m a \times_m c. \end{aligned}$$

   It now follows from the distributativity from the left, proven above, and the commutativity of $\times_m$, that distributativity from the right also holds:

$$(a +_m b) \times_m c = a \times_m c + b \times_m c.$$

□

## 8.2 Integral Domains, Units

**Definition 8.5.** A nonzero commutative ring $R$ is an **integral domain** if the product of two nonzero elements is always nonzero.

**Definition 8.6.** A nonzero element $r$ in a ring $R$ is called a **zero divisor** if there exists nonzero $s \in R$ such that $rs = 0$ or $sr = 0$.

**Note.** A nonzero commutative ring $R$ is an integral domain if and only if it has no zero divisors.

**Example 8.7.** Since $2, 3 \neq 0$ in $\mathbb{Z}_6$, but $2 \times_6 3 = \bar{6} = 0$, the ring $\mathbb{Z}_6$ is not an integral domain.

**Claim 8.8.** *A commutative ring $R$ is an integral domain if and only if the* **cancellation law** *holds for multiplication. That is: Whenever $ca = cb$ and $c \neq 0$, we have $a = b$.*

*Proof of Claim 8.8.* Suppose $R$ is an integral domain.
If $ca = cb$, then by distributativity $c(a - b) = c(a + -b) = 0$.
Since $R$ is an integral domain, we have either $c = 0$ or $a - b = 0$.
So, if $c \neq 0$, we must have $a = b$.

Conversely, suppose cancellation law holds. It suffices to show that whenever we have $a, b \in R$ such that $ab = 0$ and $a \neq 0$, then we must have $b = 0$.

By a previous result we know that $0 = a0$. So, $ab = a0$, which by the cancellation law implies that $b = 0$. □

**Note.** If every nonzero element of a commutative ring has a multiplicative inverse, then that ring is an integral domain:

$$ca = cb \implies c^{-1}ca = c^{-1}cb \implies a = b.$$

However, a nonzero element of an integral domain does not necessarily have a multiplicative inverse.

**Example 8.9.** The ring $\mathbb{Z}$ is an integral domain, for the product of two nonzero integers is nonzero. So, the cancellation law holds for $\mathbb{Z}$, but the only nonzero elements in $\mathbb{Z}$ which have multiplicative inverses are $\pm 1$.

**Example 8.10.** The ring $\mathbb{Q}[x]$ is an integral domain.

**Exercise 8.11.** Show that: For $m > 1$, $\mathbb{Z}_m$ is an integral domain if and only if $m$ is a prime.

**Example 8.12.** Consider $R = C[-1, 1]$, the ring of all continuous functions on $[-1, 1]$, equipped with the usual operations of addition and multiplication for functions.

Let:

$$f(x) = \begin{cases} -x, & -1 \leq x \leq 0, \\ 0, & 0 < x \leq 1. \end{cases} \quad , \quad g(x) = \begin{cases} 0, & -1 \leq x \leq 0, \\ x, & 0 < x \leq 1. \end{cases}$$

Then $f$ and $g$ are nonzero elements of $R$, but $fg = 0$.

So $R$ is not an integral domain.

**Definition 8.13.** We say that an element $r \in R$ is a **unit** if it has a multiplicative inverse; i.e. there is an element $r^{-1} \in R$ such that $rr^{-1} = r^{-1}r = 1$.

**Example 8.14.** Consider $4 \in \mathbb{Z}_{25}$. Since $4 \cdot 19 = 76 \equiv 1 \mod 25$, we have $4^{-1} = 19$ in $\mathbb{Z}_{25}$. So, 4 is a unit in $\mathbb{Z}_{25}$.

On the other hand, consider $10 \in \mathbb{Z}_{25}$. Since $10 \cdot 5 = 50 \equiv 0 \mod 25$, we have $10 \cdot 5 = 0$ in $\mathbb{Z}_{25}$. If $10^{-1}$ exists, then by the associativity of multiplication, we would have:

$$5 = (10^{-1} \cdot 10) \cdot 5 = 10^{-1} \cdot (10 \cdot 5) = 10^{-1} \cdot 0 = 0,$$

a contradiction. So, 10 is not a unit in $\mathbb{Z}_{25}$.

**Claim 8.15.** *Let $m \in \mathbb{N}$ be greater than one. Then, $r \in \mathbb{Z}_m$ is a unit if and only if $r$ and $m$ are relatively prime; i.e. $gcd(r, m) = 1$.*

*Proof of Claim 8.15.* Suppose $r \in \{0, 1, 2, \ldots, m-1\}$ is a unit in $\mathbb{Z}_m$, then there exists $r^{-1} \in \mathbb{Z}_m$ such that $r \cdot r^{-1} \equiv 1 \mod m$.

In other words, there exists $x \in \mathbb{Z}$ such that $r \cdot r^{-1} - 1 = mx$, or $r \cdot r^{-1} - mx = 1$. This implies that if there is an integer $d$ such that $d|r$ and $d|m$, then $d$ must also divide 1. Hence, the GCD of $r$ and $m$ is 1.

Conversely, if $gcd(r, m) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $rx + my = 1$.

It follows that $r^{-1} = \overline{x}$ is a multiplicative inverse of $r$. Here, $\overline{x} \in \mathbb{Z}_m$ is the remainder of the division of $x$ by $m$. □

**Corollary 8.16.** *For $p$ prime, every nonzero element of $\mathbb{Z}_p$ is a unit.*

**Example 8.17.** The only units of $\mathbb{Z}$ are $\pm 1$.

**Example 8.18.** Let $R$ be the ring of all real-valued functions on $\mathbb{R}$. Then, any function $f \in R$ satisfying $f(x) \neq 0, \forall x$, is a unit.

**Claim 8.19.** *The only units of $\mathbb{Q}[x]$ are nonzero constants.*

*Proof of Claim 8.19.* Given any $f \in \mathbb{Q}[x]$ such that $\deg f > 0$, for all nonzero $g \in \mathbb{Q}[x]$ we have

$$\deg fg \geq \deg f > 0 = \deg 1;$$

hence, $fg \neq 1$. If $g = 0$, then $fg = 0 \neq 1$. So, $f$ has no multiplicative inverse.

If $f$ is a nonzero constant, then $f^{-1} = \frac{1}{f}$ is a constant polynomial in $\mathbb{Q}[x]$, and $f \cdot \frac{1}{f} = \frac{1}{f} \cdot f = 1$. So, $f$ is a unit.

Finally, if $f = 0$, then $fg = 0 \neq 1$ for all $g \in \mathbb{Q}[x]$, so the zero polynomial has no multiplicative inverse. □

### 8.2.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**

## 8.3 Fields

**Definition 8.20.** A **field** is a commutative ring, with $1 \neq 0$, in which every nonzero element is a unit.

In other words, a nonzero commutative ring $F$ is a field if and only if every nonzero element $r \in F$ has a multiplicative inverse $r^{-1}$, i.e. $rr^{-1} = r^{-1}r = 1$.

Since every nonzero element of a field is a unit, a field is necessarily an integral domain, but an integral domain is not necessarily a field. For example $\mathbb{Z}$ is an integral domain which is not a field.

**Example 8.21.**

1. $\mathbb{Q}$, $\mathbb{R}$ are fields.
2. For $m \in \mathbb{N}$, it follows from a previous result that $\mathbb{Z}_m$ is a field if and only if $m$ is prime.

   **Notation** For $p$ prime, we often denote the field $\mathbb{Z}_p$ by $\mathbb{F}_p$.

**Claim 8.22.** *Equipped with the usual operations of addition and multiplications for real numbers, $F = \mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is a field.*

*Proof of Claim 8.22.* Observe that: $(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}$ lies in $F$, and $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2} \in F$. Hence, addition and multiplication for real numbers are well-defined operations on $F$. As operations on $\mathbb{R}$, they are commutative, associative, and satisfy distributativity; therefore, as $F$ is a subset of $\mathbb{R}$, they also satisfy these properties as operations on $F$.

It is clear that $0$ and $1$ are the additive and multiplicative identities of $F$. Given $a + b\sqrt{2} \in F$, where $a, b \in \mathbb{Q}$, it is clear that its additive inverse $-a - b\sqrt{2}$ also lies in $F$. Hence, $F$ is a commutative ring.

To show that $F$ is a field, for every nonzero $a + b\sqrt{2}$ in $F$, we need to find its multiplicative inverse. As an element of the field $\mathbb{R}$, the multiplicative inverse of $a + b\sqrt{2}$ is:

$$(a + b\sqrt{2})^{-1} = \frac{1}{a + b\sqrt{2}}.$$

It remains to show that this number lies in $F$. Observe that:

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2.$$

We claim that $a^2 - 2b^2 \neq 0$.

Suppose $a^2 - 2b^2 = 0$, then either (i) $a = b = 0$, or (ii) $b \neq 0$, $\sqrt{2} = |a/b|$.

Since we have assumed that $a + b\sqrt{2}$ is nonzero, case (i) cannot hold.

But case (ii) also cannot hold because $\sqrt{2}$ is known to be irrational. Hence $a^2 - 2b^2 \neq 0$, and:

$$\frac{1}{a+b\sqrt{2}} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2},$$

which lies in $F$. $\square$

**Claim 8.23.** *All finite integral domains are fields.*

*Proof of Claim 8.23.* Let $R$ be an integral domain with $n$ elements, where $n$ is finite. Write $R = \{a_1, a_2, \ldots, a_n\}$.

We want to show that for any nonzero element $a \neq 0$ in $R$, there exists $i$, $1 \leq i \leq n$, such that $a_i$ is the multiplicative inverse of $a$.

Consider the set $S = \{aa_1, aa_2, \ldots, aa_n\}$. Since $R$ is an integral domain, the cancellation law holds. In particular, since $a \neq 0$, we have $aa_i = aa_j$ if and only if $i = j$.

The set $S$ is therefore a subset of $R$ with $n$ distinct elements, which implies that $S = R$.

In particular, $1 = aa_i$ for some $i$. This $a_i$ is the multiplicative inverse of $a$. $\square$

### 8.3.1 Field of Fractions

An integral domain fails to be a field precisely when there is a nonzero element with no multiplicative inverse. The ring $\mathbb{Z}$ is such an example, for $2 \in \mathbb{Z}$ has no multiplicative inverse.

But any nonzero $n \in \mathbb{Z}$ has a multiplicative inverse $\frac{1}{n}$ in $\mathbb{Q}$, which is a field.

So, a question one could ask is, can we "enlarge" a given integral domain to a field, by formally adding multiplicative inverses to the ring?

#### An Equivalence Relation

Given an integral domain $R$ (commutative, with $1 \neq 0$). We consider the set: $R \times R_{\neq 0} := \{(a,b) : a, b \in R, b \neq 0\}$. We define a relation $\equiv$ on $R \times R_{\neq 0}$ as follows:

$$(a,b) \equiv (c,d) \text{ if } ad = bc.$$

**Lemma 8.24.** *The relation $\equiv$ is an equivalence relation.*

*In other words, the relation $\equiv$ is:*

1. **Reflexive:** $(a,b) \equiv (a,b)$ *for all* $(a,b) \in R \times R_{\neq 0}$
2. **Symmetric:** *If* $(a,b) \equiv (c,d)$, *then* $(c,d) \equiv (a,b)$.

3. **Transitive:** *If* $(a,b) \equiv (c,d)$ *and* $(c,d) \equiv (e,f)$*, then* $(a,b) \equiv (e,f)$.

*Proof of Lemma 8.24.* **Exercise.** $\square$

Due to the properties (reflexive, symmetric, transitive), of an equivalence relation, the equivalent classes form a **partition** of $S$. Namely, equivalent classes of non-equivalent elements are disjoint:

$$[s] \cap [t] = \varnothing$$

if $s \not\sim t$; and the union of all equivalent classes is equal to $S$:

$$\bigcup_{s \in S} [s] = S.$$

**Definition 8.25.** Given an equivalence relation $\sim$ on a set $S$, the **quotient set** $S/\sim$ is the set of all equivalence classes of $S$, with respect to $\sim$.

We now return to our specific situation of $R \times R_{\neq 0}$, with $\equiv$ defined as above. We define addition $+$ and multiplication $\cdot$ on $R \times R_{\neq 0}$ as follows:

$$(a,b) + (c,d) := (ad + bc, bd)$$
$$(a,b) \cdot (c,d) := (ac, bd)$$

**Claim 8.26.** *Suppose* $(a,b) \equiv (a',b')$ *and* $(c,d) \equiv (c',d')$*, then:*

1. $(a,b) + (c,d) \equiv (a',b') + (c',d')$.

2. $(a,b) \cdot (c,d) \equiv (a',b') \cdot (c',d')$.

*Proof of Claim 8.26.* By definition, $(a,b) + (c,d) = (ad + bc, bd)$, and $(a',b') + (c',d') = (a'd' + b'c', b'd')$. Since by assumption $ab' = a'b$ and $cd' = c'd$,
we have:

$$(ad + bc)b'd' = adb'd' + bcb'd' = a'bdd' + c'dbb' = (a'd' + b'c')bd;$$

hence, $(a,b) + (c,d) \equiv (a',b') + (c',d')$.

For multiplication, by definition we have $(a,b) \cdot (c,d) = (ac, bd)$ and $(a',b') \cdot (c',d') = (a'c', b'd')$.

Since

$$acb'd' = ab'cd' = a'bc'd = a'c'bd,$$

we have $(a,b) \cdot (c,d) \equiv (a',b') \cdot (c',d')$. $\square$

Let:

$$\mathrm{Frac}(R) := (R \times R_{\neq 0})/\equiv,$$

and define $+$ and $\cdot$ on $\mathrm{Frac}(R)$ as follows:

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$$
$$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$$

**Corollary 8.27.** *$+$ and $\cdot$ thus defined are well-defined binary operations on $\mathrm{Frac}(R)$.*

*In other words, we get the same output in $\mathrm{Frac}(R)$ regardless of the choice of representatives of the equivalence classes.*

**Claim 8.28.** *The set $\mathrm{Frac}(R)$, equipped with $+$ and $\cdot$ defined as above, forms a field, with additive identity $0 = [(0,1)]$ and multiplicative identity $1 = [(1,1)]$. The multiplicative inverse of a nonzero element $[(a,b)] \in \mathrm{Frac}(R)$ is $[(b,a)]$.*

*Proof of Claim 8.28.* **Exercise.** □

**Definition 8.29.** $\mathrm{Frac}(R)$ is called the **Fraction Field** of $R$.

**Note.** $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$, if we identify $a/b \in \mathbb{Q}$, $a, b \in \mathbb{Z}$, with $[(a,b)] \in \mathrm{Frac}(\mathbb{Z})$.

### 8.3.2 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**
5. **WeBWorK**
6. **WeBWorK**
7. **WeBWorK**
8. **WeBWorK**
9. **WeBWorK**
10. **WeBWorK**