Chapter 3 Rings:

This chapter really begins "abstract algebra". The key point here is we have seen $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ share a lot of properties, but are also different in several regards. There are other objects that share lots of these properties as well. We define an abstract object called a ring and prove properties about rings. The point of doing this is then we show objects such as $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are rings. Once we know this, all the properties we prove about rings are automatically true for every example. In this way we don't have to prove the properties for each case separately.

3.1 Definitions and Examples:

We begin with the key definition of the chapter,

Def: Let R be a nonempty set with two operations denoted $+$ and $\cdot$ that satisfy the following properties:

1) If $a, b \in R$, then $a+b \in R$
2) $a+(b+c) = (a+b)+c$
3) $a+b = b+a$

4) There is an element $0_R \in R$ so that

$$0_R + a = a = a + 0_R \quad \text{for every } a \in R$$

5) For each $a \in R$ the equation $a + x = 0_R$ has a solution in R (ie, a has an additive inverse.)

6) if $a, b \in R$ then $ab \in R$ (Note we write ab for $a \cdot b$)

7) $a(bc) = (ab)c$

8) $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$.

In this case we call R a <u>ring</u>.

<u>Examples:</u> 1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ with usual addition and multiplication are rings.

2) Let $n \in \mathbb{Z}_{>1}$. The set $\mathbb{Z}/n\mathbb{Z}$ with addition and multiplication as defined in the previous chapter is a ring.

3) Let $Mat_2(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in R \right\}$ for R a ring.

We say $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ if $a = a'$, $b = b'$, $c = c'$, $d = d'$.

Define addition and multiplication by:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

We claim $Mat_2(R)$ is a ring. Since $R \neq \emptyset$, $Mat_2(R) \neq \emptyset$.

Now we check the properties one by one.

1) Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in Mat_2(R)$. Then since $a+a'$, $b+b'$,

$c+c'$, $d+d' \in R$ because R is closed under addition,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix} \in Mat_2(R).$$

2) Let $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} \in Mat_2(R)$.

Then

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \left(\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} + \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} \right) = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2+a_3 & b_2+b_3 \\ c_2+c_3 & d_2+d_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1+(a_2+a_3) & b_1+(b_2+b_3) \\ c_1+(c_2+c_3) & d_1+(d_2+d_3) \end{pmatrix}$$

$$= \begin{pmatrix} (a_1+a_2)+a_3 & (b_1+b_2)+b_3 \\ (c_1+c_2)+c_3 & (d_1+d_2)+d_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{pmatrix} + \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}$$ b/c R is a ring

$$= \left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right) + \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}.$$

3) $$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_2+a_1 & b_2+b_1 \\ c_2+c_1 & d_2+d_1 \end{pmatrix}$$ b/c R is a ring

$$= \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} + \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}.$$

4) Set $0_{Mat_2(R)} = \begin{pmatrix} 0_R & 0_R \\ 0_R & 0_R \end{pmatrix}$.

5) Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(R)$. Let $-a, -b, -c, -d \in R$ be the solutions to $a + x = 0_R$, $b + x = 0_R$, etc. Then $\begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ is a solution to $\begin{pmatrix} a & b \\ c & d \end{pmatrix} + X = \begin{pmatrix} 0_R & 0_R \\ 0_R & 0_R \end{pmatrix}$.

6) Let $\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in Mat_2(R)$. Then

Then $\begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix} \in Mat_2(R)$ b/c

R is a ring.

7)
$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \left(\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} \right) = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 a_3 + b_2 c_3 & a_2 b_3 + b_2 d_3 \\ c_2 a_3 + d_2 c_3 & c_2 b_3 + d_2 d_3 \end{pmatrix}$$

$$= \begin{pmatrix} a_1(a_2 a_3 + b_2 c_3) + b_1(c_2 a_3 + d_2 c_3) & a_1(a_2 b_3 + b_2 d_3) + b_1(c_2 b_3 + d_2 d_3) \\ c_1(a_2 a_3 + b_2 c_3) + d_1(c_2 a_3 + d_2 c_3) & c_1(a_2 b_3 + b_2 d_3) + d_1(c_2 b_3 + d_2 d_3) \end{pmatrix}$$

$$= \begin{pmatrix} (a_1 a_2)a_3 + (a_1 b_2)c_3 + (b_1 c_2)a_3 + (b_1 d_2)c_3 & (a_1 a_2)b_3 + (a_1 b_2)d_3 + (b_1 c_2)b_3 + (b_1 d_2)d_3 \\ (c_1 a_2)a_3 + (c_1 b_2)c_3 + (d_1 c_2)a_3 + (d_1 d_2)c_3 & (c_1 a_2)b_3 + (c_1 b_2)d_3 + (d_1 c_2)b_3 + (d_1 d_2)d_3 \end{pmatrix}$$

b/c R is a ring

$$= \left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right) \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}.$$

check this by multiplying out

5) This is checked by direct calculation and using that R is a ring. The details are omitted because my hand is cramping from writing.

Def: 1) We say a ring R is <u>commutative</u> if $ab = ba$ for all $a, b \in R$.

2) We say R is a ring with identity if there exists $1_R \in R$ so that $1_R r = r = r 1_R$ for all $r \in R$.

Examples: 1) All our rings so far have identity.

2) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}/n\mathbb{Z}$ are all commutative rings. $Mat_2(\mathbb{Z})$ is not commutative b/c $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$ and these are not equal.

In groups: Let $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ and $2\mathbb{Z}+1 = \{2n+1 : n \in \mathbb{Z}\}$. Are these rings? Do they have identities? Are they commutative?

Def: An integral domain is a commutative ring R with identity $1_R \neq 0_R$ so that if $a, b \in R$ with $ab = 0_R$, then $a = 0_R$ or $b = 0_R$.

Most familiar examples are integral domains such as $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$.

Example: Consider $R = \mathbb{Z}/n\mathbb{Z}$. If n is prime then R is an integral domain because we saw above that there are no zero divisors in R. If n is composite then R is not an integral domain because there are zero divisors. For example, in $\mathbb{Z}/4\mathbb{Z}$ we have $2 \cdot 2 = 0$ but $2 \neq 0$ in $\mathbb{Z}/4\mathbb{Z}$. (Note we will now drop the $[\cdot]_n$ from our notation as it should be clear from context at this point.

Def: A *field* is a commutative ring R with identity $1_R \neq 0_R$ that satisfies every nonzero element in R has a multiplicative inverse, i.e., if $a \in R$, $a \neq 0_R$, then there exists $b \in R$ so that $ab = 1_R$.

Examples: 1) $\mathbb{Q}$ and $\mathbb{R}$ are both fields

2) $\mathbb{Z}$ is not a field; 2 has no multiplicative inverse in $\mathbb{Z}$ for example.

3) $\mathbb{Z}/p\mathbb{Z}$ is a field for p prime, but $\mathbb{Z}/n\mathbb{Z}$ is not a field for n composite.

Theorem 3.1.1: Let R and S be rings. Define $R \times S$ by

$R \times S = \{(r,s) : r \in R, s \in S\}$. Define addition and multiplication on $R \times S$ by

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2).$$

Then $R \times S$ is a ring.

Proof: Exercise.

Example: 1) Recall that $\mathbb{Q}$ is a field. However, $\mathbb{Q} \times \mathbb{Q}$ is not a field.

In fact, it is not even an integral domain! For example,

$(0,1)\cdot(1,0) = (0,0) = 0_{\mathbb{Q}\times\mathbb{Q}}$.

2) Consider $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The elements in this ring are

$([a]_2, [b]_3)$; there are 6 elements. We will see later that

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is "essentially" the "same" ring as $\mathbb{Z}/6\mathbb{Z}$.

Def: Let R be a ring and $S \subseteq R$ a nonempty subset. If S is a ring under the same addition and multiplication as R we say S is a <u>subring</u> of R.

Examples: 1) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{Q}$ is a subring of $\mathbb{R}$.

2) $\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\} \subseteq \mathbb{C} = \{x+iy : x,y \in \mathbb{R}\}$ is a subring. It is called the ring of Gaussian integers.

3) $\mathrm{Mat}_n(\mathbb{Z})$ is a subring of $\mathrm{Mat}_n(\mathbb{Z}[i])$.

4) $\mathbb{Z}/n\mathbb{Z}$ is not a subring of $\mathbb{Z}$ because it is not a subset.

5) Let $S = \{[0]_4, [2]_4\} \subseteq \mathbb{Z}/4\mathbb{Z}$. Then S is a subring of $\mathbb{Z}/4\mathbb{Z}$, as you can check as an exercise. It is easiest to use the following theorem.

<u>Theorem 3.1.2:</u> Let R be a ring and S a nonempty subset of R. Then S is a subring of R if

1) S is closed under $+_R$ $\quad$ ($+_R$ = addition on R)
2) S is closed under mult. on R, i.e., $a, b \in S$ implies $a \cdot b \in S$.
3) $0_R \in S$
4) S is closed under additive inverses, i.e., the equation $a + x = 0_R$ has a solution in S for all $a \in S$.

<u>Proof:</u> Since S is a subset of R, all the elements of S are in R. Thus, the axioms (2), (3), (7), and (8) of being a ring hold for S as well. The rest hold by the properties required in the theorem. ∎

<u>Example:</u> Consider $S = \mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$.

We claim this is a subring. It is clearly nonempty.

Let $a+b\sqrt{3},\ c+d\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Then

$$(a+b\sqrt{3})+(c+d\sqrt{3}) = (a+c)+(b+d)\sqrt{3} \in \mathbb{Q}(\sqrt{3})$$

and

$$(a+b\sqrt{3})(c+d\sqrt{3}) = (ac+3bd)+(ad+bc)\sqrt{3} \in \mathbb{Q}(\sqrt{3}).$$

We have $0 = 0+0\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Finally, $-a-b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$

for all $a+b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Thus, $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$ is a subring.

Section 3.2: Basic Properties of Rings:

Recall that one of the axioms for a ring is the equation $a+x=0_R$ has at least one solution. Another way to think of this is every element has an additive inverse. We would like to know this is unique.

Theorem 3.2.1: Given $a \in R$, the equation $a+x=0_R$ has a unique solution.

Proof: Assume $b, c \in R$ are both solutions to $a+x=0_R$.

Then we have

$$\begin{aligned} b &= b+0_R \\ &= b+(a+c) \\ &= (b+a)+c \\ &= 0_R+c \\ &= c. \end{aligned}$$

Thus, $b=c$. ∎

Now that we know the solution of $a + x = 0_R$ is unique, we denote the element solving this by $-a$, ie, $-a$ is the unique element in R that satisfies $a + (-a) = 0_R$.

We set $a - b$ in R to be $a + (-b)$. This is how we define subtraction.

<u>Example:</u> Consider $2 \in \mathbb{Z}/5\mathbb{Z}$. We have $2 - 2 = 0$ in $\mathbb{Z}/5\mathbb{Z}$.

However, we have $-2 \equiv 3 \pmod 5$, so $-2 = 3$ in $\mathbb{Z}/5\mathbb{Z}$, ie.

$2 - 2 = 2 + 3 = 0$ in $\mathbb{Z}/5\mathbb{Z}$.

<u>Prop. 3.2.2:</u> Let $a, b, c \in R$ with $a + c = b + c$. Then $a = b$.

<u>Proof:</u> We have

$$(a + c) + (-c) = (b + c) + (-c)$$

$$\Leftrightarrow \quad a + (c - c) = b + (c - c)$$

$$\Leftrightarrow \quad a = b.$$

$\blacksquare$

<u>Prop. 3.2.3:</u> Let $a, b \in R$. Then we have

1) $a \cdot 0_R = 0_R = 0_R \cdot a$
2) $a(-b) = -ab = (-a)b$
3) $-(-a) = a$
4) $-(a+b) = (-a) + (-b)$

5) $-(a-b) = -a+b$

6) $(-a)(-b) = ab$

If R has an identity, then $(-1_R)a = -a$.

Proof: 1) We have

$$a\cdot 0_R + a\cdot 0_R = a(0_R+0_R)$$
$$= a\cdot 0_R$$
$$= a0_R + 0_R.$$

Subtract $a\cdot 0_R$ from both sides to obtain

$$a\cdot 0_R = 0_R.$$

2) Observe we have

$$ab + a(-b) = a(b-b)$$
$$= a0_R$$
$$= 0_R.$$

Thus, $a(-b)$ is a solution to $ab+x=0_R$. However, $-ab$ is the unique solution to this equation. Thus, $-ab = a(-b)$. The same arg. shows $-ab = (-a)b$.

3) Observe we have

$$-a + x = 0_R$$

has $-(-a)$ as its unique solution. However, $-a+a = 0_R$, so it must be that $-(-a) = a$.

4) Again, we use $-(a+b)$ is the unique solution to $(a+b)+x = 0_R$. However,

$$(a+b)+[(-a)+(-b)] = (a+(-a))+(b+(-b))$$
$$= 0_R + 0_R = 0_R.$$

Thus, $-(a+b) = (-a) + (-b)$.

5) We have $-(a-b)$ is the unique solution to

$$(a-b) + x = 0_R.$$

However,

$$(a-b) + [-a+b] = [a+(-a)] + [b-b]$$
$$= 0_R + 0_R = 0_R.$$

Thus, $-(a-b) = -a+b$.

6) We have

$$(-a)(-b) = -(-a)b \quad \text{by 2) w/ } a \text{ replaced by } -a.$$
$$= -(-ab) \quad \text{by 2)}$$
$$= ab \quad \text{by 3)}.$$

7) We have

$$(-1_R)a = -(1_R a) \quad \text{by 2)}$$
$$= -(a)$$
$$= -a.$$

$\boxtimes$

We can distribute and foil things out, but we must be careful because not all rings are commutative.

<u>Example:</u> Consider the ring $R = \mathrm{Mat}_2(\mathbb{Z})$. We have that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

Thus,

$$\left(\begin{pmatrix}1&1\\0&1\end{pmatrix}+\begin{pmatrix}0&1\\1&1\end{pmatrix}\right)^2 = \begin{pmatrix}1&1\\0&1\end{pmatrix}^2+\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&1\end{pmatrix}+\begin{pmatrix}0&1\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}+\begin{pmatrix}0&1\\1&1\end{pmatrix}^2$$

$$= \begin{pmatrix}1&2\\0&1\end{pmatrix}+\begin{pmatrix}1&2\\0&1\end{pmatrix}+\begin{pmatrix}0&1\\1&2\end{pmatrix}=\begin{pmatrix}2&5\\1&4\end{pmatrix}$$

and this is not the same as

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}^2+2\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&1\end{pmatrix}+\begin{pmatrix}0&1\\1&1\end{pmatrix}^2 = \begin{pmatrix}1&2\\0&1\end{pmatrix}+\begin{pmatrix}2&4\\0&2\end{pmatrix}+\begin{pmatrix}0&1\\1&2\end{pmatrix}$$

$$= \begin{pmatrix}3&7\\1&5\end{pmatrix}.$$

So in general we have

$$(a+b)^2 = a^2+ab+ba+b^2$$

but unless R is commutative we can't always reduce this to $a^2+2ab+b^2$.

We can also define units and zero divisors in rings the same as we did for $\mathbb{Z}/n\mathbb{Z}$.

Def: An element $a\in R$ (R a ring with identity) is a <u>unit</u> if there exists $b\in R$ so that $ab=1_R=ba$. We call b the <u>(multiplicative) inverse</u> of a. The collection of units is denoted $R^\times$.

<u>Examples:</u> 1) The only units in $\mathbb{Z}$ are ± 1.

2) The units of $(\mathbb{Z}/n\mathbb{Z})$ are those a so that $\gcd(a,n)=1$.

3) Let F be a field. Then $F^\times = F \setminus \{0\}$.

4) Let $R = \mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$. The units in this ring are ~~those~~ $\pm 1, \pm i$. We will see later how to prove this.

Prop. 3.2.3: Let $a \in R^\times$. Then the inverse of a is unique.

Proof: Suppose $b, c \in R$ so that $ab = 1_R = ba$ and $ac = 1_R = ca$.

Then we have
$$\begin{aligned} b &= b \cdot 1_R \\ &= b(ac) \\ &= (ba)c \\ &= 1_R c \\ &= c. \end{aligned}$$

Thus, $b = c$. ∎

Since the multiplicative inverse of a is unique we can denote it by a^{-1}.

Example: Let R be a ring with identity. Consider the ring $Mat_2(R)$. The group of units here contains all the matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ so that $ad-bc \in R^\times$. Observe

$$\begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

is the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where we write $\frac{1}{ad-bc}$ to denote $(ad-bc)^{-1}$ here.

Def: Let $a \in R$. We say a is a <u>zero divisor</u> if

1) $a \neq 0_R$
2) There is an element $b \in R \setminus \{0_R\}$ so that $ab = 0_R$ or $ba = 0_R$.

Example: 1) We saw before that if n is composite, then $\mathbb{Z}/n\mathbb{Z}$ contains zero divisors. Namely, any element $a \in \mathbb{Z}/n\mathbb{Z}$ so that $\gcd(a,n) > 1$ is a zero divisor.

2) There are no zero divisors in $\mathbb{Z}$.

3) Consider R a ring with identity. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(R)$ with $ad - bc = 0$. Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a zero divisor because

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

In particular, if $F = R$ is a field then we have $R^\times = R \setminus \{0\}$, so we have

$$\mathrm{Mat}_2(F)^\times = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0 \right\}$$

and if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has $ad - bc = 0$ it is a zero divisor.

Theorem 3.2.4: Let F be a field. Then F is an integral domain.

Proof: Since F is necessarily a commutative ring with identity, we only need to show F has no zero divisors. Suppose $a \in F$ is a zero divisor, i.e., there exists a nonzero $b \in F$ so that $ab = 0_F$ or $ba = 0_F$. (Since F is commutative these are equivalent.) Then $a \neq 0_R$, so $a^{-1} \in F$. Thus,

$$ab = 0_F \iff a^{-1}(ab) = a^{-1}0_F$$

$$\iff (a^{-1}a)b = 0_F$$

ie,

$$b = 0_F.$$

Thus, it must be that a is not a zero divisor and F is an integral domain. ☒

Example: Every field is an integral domain, but not every integral domain is a field. For example, $\mathbb{Z}$ is an integral domain that is not a field.

Theorem 3.2.5: Let R be an integral domain with finitely many elements. Then R is a field.

Proof: Let $R = \{0_R, a_1, \dots, a_n\}$. Consider a_j, and the products $a_j a_i$ for $i = 1, \dots, n$. Note if $i \neq k$, then $a_j a_i \neq a_j a_k$. (If $a_j a_i = a_j a_k$, then $a_j a_i - a_j a_k = 0_R$ ie, $a_j(a_i - a_k) = 0_R$, so $a_i = a_k$.) Thus, the elements $a_j a_i$ are n distinct elements of R and are all nonzero because R has no zero divisors. Thus,

$$\{a_j a_i : 1 \leq i \leq n\} = \{a_1, \dots, a_n\}.$$

So for some i_0, $a_j a_{i_0} = 1_R$, ie, $a_{i_0} = a_j^{-1}$. ☒

Section 3.3 Homomorphisms and Isomorphisms:

One way of studying an object is to study functions from the object or into an object. For instance, in set theory we consider sets to be equivalent if they have the same number of elements, i.e., there is a bijection between the sets. In our case we want not just any functions between our rings, but ones that preserve the structure of the rings.

Example: Consider $R = \mathbb{Z}/2\mathbb{Z}$ and $S = \{[0]_4, [2]_4\} \subseteq \mathbb{Z}/4\mathbb{Z}$.

If we write out addition and multiplication tables for these we have:

$\mathbb{Z}/2\mathbb{Z}$

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

S

$+$	$[0]_4$	$[2]_4$
$[0]_4$	$[0]_4$	$[2]_4$
$[2]_4$	$[2]_4$	$[0]_4$

$\cdot$	$[0]_4$	$[2]_4$
$[0]_4$	$[0]_4$	$[0]_4$
$[2]_4$	$[0]_4$	$[0]_4$.

Thus, even though these have the same number of elements they are "different" because their multiplication doesn't match up. Namely, S does not have a multiplicative identity.

Example: Consider the rings $R = \mathbb{Z}/3\mathbb{Z}$ and $S = \{[0]_6, [2]_6, [4]_6\} \subseteq \mathbb{Z}/6\mathbb{Z}$.

Writing out addition and multiplication tables here we have

R |

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

S |

$+$	$[0]_6$	$[2]_6$	$[4]_6$
$[0]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[2]_6$	$[2]_6$	$[4]_6$	$[0]_6$
$[4]_6$	$[4]_6$	$[0]_6$	$[2]_6$

$\cdot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$.

$\cdot$	$[0]_6$	$[2]_6$	$[4]_6$
$[0]_6$	$[0]_6$	$[0]_6$	$[0]_6$
$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$.

Note that R is a field with 3 elements. Looking at the table for S we see this is a ring with $[4]_6$ as the identity (multiplicative.)

Note we can rewrite these table as

$+$	0	1	X
0	0	1	X
1	1	X	0
X	X	0	1

$\cdot$	0	1	X
0	0	0	0
1	0	1	X
X	0	X	1

Where we can have $\{0,1,x\} = \{[0]_3, [1]_3, [2]_3\}$

or $\{0,1,x\} = \{[0]_6, [4]_6, [2]_6\}$. Thus, these are really in some sense the same ring where the elements have different names.

We now formalize this.

<u>Def:</u> Let R and S be rings. We say a function $\varphi: R \to S$ is a <u>(ring) homomorphism</u> if for all $a, b \in R$ we have

1) $\varphi(a +_R b) = \varphi(a) +_S \varphi(b)$

2) $\varphi(ab) = \varphi(a)\varphi(b)$. $\quad$ ($a \cdot b$ in R, $\varphi(a)\cdot\varphi(b)$ in S)

We say φ is an <u>isomorphism</u> if φ is a homomorphism and φ is also bijective. We say R and S are <u>isomorphic</u> and write $R \cong S$ if there is an isomorphism from R to S.

<u>Example:</u> Consider the previous example with $R = \mathbb{Z}/3\mathbb{Z}$ and $S = \{[0]_6, [2]_6, [4]_6\} \subseteq \mathbb{Z}/6\mathbb{Z}$. Define

$$\varphi: R \to S$$

by setting

$$\varphi([0]_3) = [0]_6$$

$$\varphi([1]_3) = [4]_6$$

$$\varphi([2]_3) = [2]_6.$$

It is clearly bijective and one can check it satisfies the properties of being a homomorphism from the table. Thus, φ is an isomorphism, i.e. $\mathbb{Z}/3\mathbb{Z} \cong \{[0]_6, [2]_6, [4]_6\}$.

<u>Example:</u> Let $m, n \in \mathbb{Z}_{\geq 2}$ and assume $m \mid n$. We can define a homomorphism $\varphi: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ by setting $\varphi([a]_n) = [a]_m$. The first thing we need to show is this is well-defined; namely, if $[a]_n = [b]_n$ then $\varphi([a]_n) = \varphi([b]_n)$. If $[a]_n = [b]_n$, then $n \mid (a-b)$. Since $m \mid n$, we have $m \mid (a-b)$. Thus,

$$\varphi([a]_n) = [a]_m = [b]_m = \varphi([b]_n),$$

and so φ is well defined. We now check it is a homomorphism. Let $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$. Then

$$\begin{aligned}
\varphi([a]_n + [b]_n) &= \varphi([a+b]_n) \\
&= [a+b]_m \\
&= [a]_m + [b]_m \\
&= \varphi([a]_n) + \varphi([b]_n).
\end{aligned}$$

and

$$\begin{aligned}
\varphi([a]_n \cdot [b]_n) &= \varphi([ab]_n) \\
&= [ab]_m \\
&= [a]_m \cdot [b]_m
\end{aligned}$$

$= \varphi([a]_m)\,\varphi([b])_m.$

<u>Example:</u> Consider the map $\varphi: \mathbb{R} \to \mathbb{R}$ given by $x \mapsto x^2$.

This is not a homomorphism. Observe

$$\varphi(1+2) = (1+2)^2 = 9$$

but $\varphi(1) + \varphi(2) = 1^2 + 2^2 = 5.$

<u>Example:</u> Let $R = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Define

$\varphi: R \to R$ by $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$. Then we have

φ is clearly a bijection (check this!) and

$$\varphi((a+b\sqrt{2}) + (c+d\sqrt{2})) = \varphi((a+c) + (b+d)\sqrt{2})$$

$$= (a+c) - (b+d)\sqrt{2}$$

$$= (a - b\sqrt{2}) + (c - d\sqrt{2})$$

$$= \varphi((a+b\sqrt{2})) + \varphi(c+d\sqrt{2}).$$

and

$$\varphi((a+b\sqrt{2})(c+d\sqrt{2})) = \varphi((ac+2bd) + (ad+bc)\sqrt{2})$$

$$= (ac+2bd) - (ad+bc)\sqrt{2}$$

$$\varphi(a+b\sqrt{2})\varphi(c+d\sqrt{2}) = (a-b\sqrt{2})(c-d\sqrt{2})$$

$$= (ac+2bd) - (ad+bc)\sqrt{2}.$$

Thus, φ is an isomorphism.

__Example:__ Consider the polynomial ring $\mathbb{Z}[x] = \{ p_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n : a_i \in \mathbb{Z},\ n \in \mathbb{Z}_{\geq 0} \}$.

let $\alpha \in \mathbb{Z}$. Define $\varphi_\alpha : \mathbb{Z}[x] \to \mathbb{Z}$ by $\varphi_\alpha(f) = f(\alpha)$.

We have for $f, g \in \mathbb{Z}[x]$:

$$\begin{aligned} \varphi_\alpha(f+g) &= (f+g)(\alpha) \\ &= f(\alpha) + g(\alpha) \\ &= \varphi_\alpha(f) + \varphi_\alpha(g) \end{aligned}$$

and

$$\begin{aligned} \varphi_\alpha(fg) &= (fg)(\alpha) \\ &= f(\alpha) g(\alpha) \\ &= \varphi_\alpha(f) \varphi_\alpha(g). \end{aligned}$$

Thus, φ_α is a homomorphism. Note since $\mathbb{Z} \subseteq \mathbb{Z}[x]$, we have $\varphi_\alpha(\beta) = \beta$ for any $\beta \in \mathbb{Z}$. Thus φ_α is surjective.

__Example:__ Consider $R = \{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{R}) \}$. This is a field as you can check as an exercise. In fact, we have $R \cong \mathbb{C}$. To see this, define

$$\begin{aligned} \varphi : R &\to \mathbb{C} \\ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} &\mapsto a + bi. \end{aligned}$$

$$\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}+\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix}\right)$$

$$= (a+c) + (b+d)i$$

$$= (a+bi) + (c+di)$$

$$= \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right),$$

$$\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix}\right)$$

$$= (ac-bd) + (ad+bc)i$$

$$= (a+bi)(c+di)$$

$$= \varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right)\varphi\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right).$$

This shows φ is a homomorphism. It remains to show bijectivity. Suppose $\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} c & d \\ -d & c \end{pmatrix}\right)$. Then

$$a+bi = c+di,$$

which gives $a=c$ and $b=d$. Thus, $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, so φ is injective. Let $a+bi \in \mathbb{C}$. Then $\varphi\left(\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right) = a+bi$ so φ is surjective. Thus, $R \cong \mathbb{C}$ as claimed.

<u>Def</u>: Let $\varphi: R \to S$ be a ring homomorphism. We define $\text{im}(\varphi) = \{s \in S : \varphi(r) = s \text{ for some } r \in R\}$. This is the <u>image of φ</u>.

We actually have $\text{im}(\varphi)$ is a subring of S. Before we prove this we need some basic facts.

<u>Theorem ~~3.3.1~~ 3.3.1</u>: Let $\varphi: R \to S$ be a homomorphism of rings. We have

1) $\varphi(0_R) = 0_S$
2) $\varphi(-r) = -\varphi(r)$ for all $r \in R$
3) $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2)$ for all $r_1, r_2 \in R$.

If R is a ring with identity and φ is surjective, then

4) S is a ring with identity and $1_S = \varphi(1_R)$.
5) If $u \in R^\times$, then $\varphi(u) \in S^\times$ and $\varphi(u)^{-1} = \varphi(u^{-1})$.

<u>Proof:</u> 1) We have

$$\varphi(0_R) = \varphi(0_R + 0_R) = \varphi(0_R) + \varphi(0_R).$$

Subtracting $\varphi(0_R)$ from both sides we get $\varphi(0_R) = 0_S$.

2) We have

$$\varphi(r-r) = \varphi(0_R) = 0_S$$

and

$$\varphi(r-r) = \varphi(r + (-r)) = \varphi(r) + \varphi(-r).$$

Since the additive inverse of $\varphi(r)$ is unique and

$$\varphi(r) + \varphi(-r) = 0_S,$$

we have $\varphi(-r) = -\varphi(r)$.

3) Observe

$$\begin{aligned}\varphi(r_1 - r_2) &= \varphi(r_1 + (-r_2)) \\ &= \varphi(r_1) + \varphi(-r_2) \\ &= \varphi(r_1) - \varphi(r_2).\end{aligned}$$

Now assume R is a ring with identity 1_R.

4) Let $s \in S$. Since φ is surjective we have $r \in R$ s.t. $\varphi(r) = s$.

Then

$$\begin{aligned}\varphi(1_R)\cdot s &= \varphi(1_R)\,\varphi(r) \\ &= \varphi(1_R\, r) \\ &= \varphi(r) \\ &= s\end{aligned}$$

and similarly

$$s \cdot \varphi(1_R) = s.$$

Thus $\varphi(1_R)$ is the identity element of S, i.e., S is a ring with identity and $1_S = \varphi(1_R)$.

5) Let $u \in R^\times$, i.e., there exist $u^{-1} \in R^\times$ s.t. $u \cdot u^{-1} = 1_R = u^{-1} u$.

We have

$$\varphi(u)\varphi(u^{-1}) = \varphi(uu^{-1}) = \varphi(1_R)$$
$$= 1_S.$$

and

$$\varphi(u^{-1})\varphi(u) = \varphi(1_R) = 1_S.$$

Thus, $\varphi(u^{-1})$ is the inverse of $\varphi(u)$, i.e., $\varphi(u^{-1}) = \varphi(u)^{-1}$. $\blacksquare$

<u>Cor. 3.3.2:</u> Let $\varphi: R \to S$ be a homom. of rings. Then $\operatorname{im}(\varphi)$ is a subring of S.

<u>Proof:</u> We have $\operatorname{im}(\varphi) \neq \emptyset$ because $0_S = \varphi(0_R) \in \operatorname{Im}(\varphi)$.

Let $\varphi(r_1), \varphi(r_2) \in \operatorname{Im}(\varphi)$. Then

$$\varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2) \in \operatorname{Im}(\varphi)$$

and

$$\varphi(r_1) - \varphi(r_2) = \varphi(r_1 - r_2) \in \operatorname{Im}(\varphi).$$

Thus, $\operatorname{im}(\varphi)$ is a subring of S. $\blacksquare$

<u>Def:</u> Let $\varphi: R \to S$ be a homom. The <u>kernel of φ</u>, denoted $\ker\varphi$, is defined by

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

<u>Cor. 3.3.3:</u> The kernel of φ is a subring of R.

Proof: We have $0_R \in \ker\varphi$ because $\varphi(0_R) = 0_S$.

Let $r_1, r_2 \in \ker\varphi$. Then

$$\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2) = 0_S \cdot 0_S = 0_S$$

and

$$\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2) = 0_S - 0_S = 0_S.$$

Thus, $\ker\varphi$ is a subring of R. ∎

We can now look back at our examples to calculate the kernels and homomorphisms. Before, we note one more useful result.

Prop. 3.3.4: Let $\varphi: R \to S$ be a homom.

1) We have φ is surj iff $\mathrm{im}(\varphi) = S$.

2) We have φ is inj. iff $\ker\varphi = \{0_R\}$.

Proof: 1) If $\mathrm{Im}(\varphi) = S$, clearly φ is surjective and vice versa.

2) Suppose φ is inj. Let $r \in \ker\varphi$. Then we have

$$\varphi(r) = 0_S = \varphi(0_R).$$

Since φ is inj., then $r = 0_R$. Thus, $\ker\varphi = \{0_R\}$.

Now if $\ker\varphi = \{0_R\}$, we have the following. Let $\varphi(r_1) = \varphi(r_2)$. Then $\varphi(r_1 - r_2) = 0_S$, so $r_1 - r_2 \in \ker\varphi$, i.e. $r_1 - r_2 = 0_R$. Thus, $r_1 = r_2$. ∎

Example: Consider the map $\varphi: \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ via $[a]_{10} \longmapsto [a]_5$. This map is surjective as given $[b]_5 \in \mathbb{Z}/5\mathbb{Z}$ we have $\varphi([b]_{10}) = [b]_5$. We have $[a]_{10} \in \ker\varphi$ iff $[a]_5 = [0]_5$, i.e. if $a \equiv 0 \pmod 5$. Thus, $\ker\varphi = \{[0]_{10}, [5]_{10}\}$.

Example: Define $\varphi: \mathbb{Z}[x] \to \mathbb{Z}$ by $a_0 + a_1 x + \cdots + a_n x^n \mapsto a_0$. This is a homom as you can check. This is surjective as given $m \in \mathbb{Z}$, $m \in \mathbb{Z}[x]$ so $\varphi(m) = m$. If $f \in \ker\varphi$, then f must be of the form $0 + a_1 x + \cdots + a_n x^n$. Thus, $\ker\varphi = x\mathbb{Z}[x] = \{f \in \mathbb{Z}[x] : x \mid f(x)\}$.

Example: Consider the rings $R = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{R})\}$, $S = \mathbb{R} \times \mathbb{R}$.

One can check these are both rings. Define

$$\varphi: R \to S$$
$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a, 0).$$

This is a homomorphism as

$$\varphi\left(\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 0 & d_1 + d_2 \end{pmatrix}\right)$$

$$= (a_1 + a_2, 0)$$

$$= \varphi\left(\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}\right)$$

and

$$\varphi\left(\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix}\right)$$

$$= (a_1 a_2, 0)$$

$$= \varphi\left(\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}\right)\varphi\left(\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}\right).$$

The image of φ is $\mathbb{R} \times \{0\} = \{(a,0) : a \in \mathbb{R}\}$. The kernel is $\left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{R}) \right\}$.