II. RING HOMOMORPHISMS.

In MATH 3360, we identified the maps we can use from a group $G$ to another group $G'$ and called them group homomorphisms. In this chapter we define ring homomorphisms. We show that how ring homomorphisms give rise to the special notion of a subring, called an ideal. The homomorphic image of a ring turns out to be isomorphic to a quotient ring.

Ring homomorphisms, ideals, and quotient rings are interrelated in exactly the same way that group homomorphisms, subgroup, and quotient groups were.

Definitions and basic properties.

Ex. Consider the two rings $\mathbb{Z}$ and $2\mathbb{Z}$ and the natural map $\phi(a) = 2a$, $\forall a \in \mathbb{Z}$. We know that $\phi$ is a group isomorphism under addition, since

$$\phi(x+y) = 2x+2y = \phi(x)+\phi(y), \forall x,y \in \mathbb{Z}.$$
But now look what happens under multiplication:

\[ 2 = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1) = 4. \]

In other words, this map does not respect multiplication in \( \mathbb{Z} \).

Exp 2. Consider the map, \( \phi : \mathbb{Z} \to \mathbb{Z}_3 \) defined by

\[ \phi(x) = x \pmod{3}, \ \forall x \in \mathbb{Z}. \]

We know from MATH 3B60 that

\[ \phi(x+y) = (x+y) \mod{3} = (x \mod{3}) + (y \mod{3}) = \phi(x) + \phi(y), \]

\[ \phi(x \cdot y) = (x \cdot y) \mod{3} = (x \mod{3}) \cdot (y \mod{3}) = \phi(x) \cdot \phi(y). \]

This is an example of a map that respects both operations.

**Definition.** A map, \( \phi : R \to R' \) from a ring \( R \) to a ring \( R' \) is called a **ring homomorphism** if for all \( a, b \in R \), we have

1. \( \phi(a+b) = \phi(a) + \phi(b) \)
2. \( \phi(a \cdot b) = \phi(a) \cdot \phi(b) \)
Remark.
On the left hand side, we use the two operations in $\mathbb{R}$, while on the right hand side we use the two operations in $\mathbb{R}'$.

Exp 3. Consider the map $\phi: \mathbb{Z}_4 \to \mathbb{Z}_6$, $\phi(x) = 3x$, $\forall x \in \mathbb{Z}_4$. Again, we obtain

$$
\phi(x+y) = 3(x+y) \mod 6 = (3x \mod 6) + (3y \mod 6) = \\
= \phi(x) + 6 \phi(y)
$$

$$
\phi(x \cdot y) = 3(x \cdot y) \mod 6 = 9(x \cdot y) \mod 6 = (3x \mod 6) \cdot (3y \mod 6) = \\
= \phi(x) \cdot 6 \phi(y), \quad \phi \text{ is a ring homomorphism.}
$$

In our calculation, we have used the fact that $3 \equiv 9 \mod 6$. The jump from $3$ to $9 \mod 6$ can be better seen in $3 \mod 6 = \phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot \phi(1) = \\
= 9 \mod 6$.

Exp 4. Let us determine all possible ring homomorphisms $\phi: \mathbb{Z} \to \mathbb{Z}$. This must be a group homomorphism under addition, and since $(\mathbb{Z}, +)$ is cyclic generated by $1$, the image $\phi(1)$ of $1$ determines $\phi$ completely.
Let \( \phi(x) = a \in \mathbb{Z} \). Then, we have
\[
\phi(x) = \phi(x+1) = \phi(1) - \phi(1) = a^2
\]
Hence \( a^2 = a \) in \( \mathbb{Z} \) and we obtain \( a = 0 \) or \( a = 1 \).
If \( \phi(x) = a = 0 \Rightarrow \phi(x) = 0, \forall x \in \mathbb{Z} \).
If \( \phi(x) = a = 1 \Rightarrow \phi(x) = x, \forall x \in \mathbb{Z} \).
These are the only two possible homomorphisms from \( \mathbb{Z} \) to \( \mathbb{Z} \).

**Exp. 5.** Let us find all ring homomorphisms \( \phi : \mathbb{Z}_6 \rightarrow \mathbb{Z}_{12} \).

Again, we use the fact that \( \mathbb{Z}_6 \) is a cyclic group under addition with \( 1 \) as its generator, \( \phi(1) = a \in \mathbb{Z}_{12} \) completely determines \( \phi \). Now, we know from MATH 3360 that if \( |a| \) is finite, then \( |\phi(a)| \) divides \( |a| \), so \( |\phi(1)| \) (the order of \( \phi(1) \)) divides the order of \( |1| = 6 \) of \( 1 \) in \( \mathbb{Z}_6 \). Hence, either we have
\[
|a| = 1 \text{ and } a = 0, \text{ or }
|a| = 2 \text{ and } a = 6 \text{ or }
|a| = 3 \text{ and } a = 4 \text{ or } 8 \text{ or }
|a| = 6 \text{ and } a = 2 \text{ or } 10.
\]
So far, we have used only condition (1) from the ring homomorphism. Let us use now condition (2) which implies

\[ a = \phi(1) = \phi(1+1) = \phi(1) \cdot \phi(1) = a^2. \]

In other words, among the elements of \( \mathbb{Z}_{12} \) we have found so far as candidates we need to pick those that satisfy \( a^2 = a \) (idempotents). The main question is what idempotents do we have in \( \mathbb{Z}_{12} \)?

\[ 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 6^2 = 0, \quad 8^2 = 16 \equiv 4, \quad 10^2 = 100 \equiv 4, \]

so the only possibilities we have are \( a = 0, \ a = 4 \). Thus either \( \phi(x) = 0 \) for all \( x \in \mathbb{Z}_6 \) or \( \phi(x) = 4x \) for all \( x \in \mathbb{Z}_6 \), and these are the only ring homomorphisms from \( \mathbb{Z}_6 \) to \( \mathbb{Z}_6 \).

Exp. Determine all ring homomorphisms from \( \mathbb{Z}_2 \) to \( \mathbb{Z}_6 \).

S ol. Since \( \mathbb{Z}_2 \) is generated from 1 by addition and subtraction, if a ring homomorphism \( f: \mathbb{Z} \rightarrow \mathbb{Z}_6 \) then for any \( a \in \mathbb{Z} \), we have \( f(a) = a \cdot m \), where \( m = f(1) \). Then \( f \) is linear, so \( f(a)+f(b) = am+bm \). 

\[ -5 - \]
\[(a+b) \cdot m = f(a+b), \text{ for any } a, b \in \mathbb{Z}.\]

So \(f\) is a ring homomorphism if and only if for any \(a, b \in \mathbb{Z},\)

\[0 = f(ab) - f(a)f(b) = abm - (am)(bm) = ab(m-m^2).\]

In particular, taking \(a = b = 1\), we need \(0 = m - m^2 \pmod{6}\). Working \(\pmod{6}\), we have

\[0-0^2 = 0-0 = 0, \quad 1-1^2 = 1-1 = 0, \quad 2-2^2 = 2-4 = -2 = 4 \neq 0,\]
\[3-3^2 = 3-9 = -6 = 0, \quad 4-4^2 = 4-16 = 0, \quad 5-5^2 = 5-25 = 2.\]

The possible values of \(m\) are 0, 1, 3 and 4. So the homomorphisms are:

- \(f(a) = 0 \pmod{6}, \forall a \in \mathbb{Z}\)
- \(f(a) = a \pmod{6}, \forall a \in \mathbb{Z}\)
- \(f(a) = 3a \pmod{6}, \forall a \in \mathbb{Z}\)
- \(f(a) = 4a \pmod{6}, \forall a \in \mathbb{Z}\)

**Definition.** Let \(\phi: \mathbb{R} \rightarrow \mathbb{R}'\) be a ring homomorphism. Then the **kernel** of \(\phi\) is the set \(\text{ker}\phi = \{\}\).
Proposition.
Let \( \phi : R \rightarrow R' \) be a ring homomorphism. Then:

1. \( \phi(0) = 0 \)
2. \( \phi(-a) = -\phi(a) \), \( \forall a \in R \)
3. \( \phi(na) = n\phi(a) \), \( \forall a \in R, \forall n \in \mathbb{Z} \)
4. \( \phi \) is one to one if and only if \( \text{Ker} \phi = \{0\} \).

Proposition.
Let \( \phi : R \rightarrow R' \) be a ring homomorphism. Then:

1. \( \phi(a^n) = \phi(a)^n \), \( \forall a \in R, \forall n \geq 0 \)
2. If \( A \) is a subring of \( R \), then
   \[ \phi(A) = \{ \phi(a) \in R' \mid a \in A \} \] is a subring of \( R' \).
3. If \( R \) is a ring with unity \( 1 \), then \( \phi(1) \) is unity in \( \phi(R) \), and \( \phi(1)^2 = \phi(1) \).
4. If \( R \) is a ring with unity \( 1 \), and \( a \in U(R) \) is a unit in \( R \), then \( \phi(a^n) = \phi(a)^n \) in \( \phi(R) \) for all \( n \in \mathbb{Z} \).
5. If \( B \) is a subring of \( R' \), then \( \phi^{-1}(B) = \{ x \in R \mid \phi(x) \in B \} \).
is a subring of $R$, and \( \ker \phi \subseteq \phi^{-1}(B) \).

(6) \( \ker \phi \) is a subring of $R$.

(7) If $R$ is a commutative ring, then \( \phi(R) \) is a commutative ring.

Proof. (1) For $n = 1$ we have \( \phi(a^1) = \phi(a) = \phi(a)^1 \). If $k > 0$ and \( \phi(a^k) = \phi(a)^k \), then \( \phi(a^{k+1}) = \phi(a^k \cdot a) = \phi(a^k) \cdot \phi(a) = \phi(a)^k \cdot \phi(a) = \phi(a)^{k+1} \) and (1) is proved by induction.

(2) If $A$ is a subring of $R$, then \( \phi(A) \) is a subgroup of $R'$ under addition. For any $x, y \in \phi(A)$, we have $x = \phi(a)$ and $y = \phi(b)$ for some $a, b \in A$. Note that since $A$ is a subring of $R$ we have $ab \in A$. Then $xy = \phi(a) \phi(b) = \phi(ab) \in \phi(A)$, and therefore by the subring test \( \phi(A) \) is subring of $R$.

(3) Let $x \in \phi(R)$. Then $x = \phi(a)$ for some $a \in R$. Hence $x \cdot \phi(1) = \phi(a) \cdot \phi(1) = \phi(a \cdot 1) = \phi(a) = x$. Similarly, we can show $\phi(1) \cdot x = x$, and therefore $\phi(1)$ is unity in $\phi(R)$, and $\phi(1) \cdot \phi(1) = \phi(1)$.

(4) Let $a \in U(R)$. For $n > 0$, (4) follows from (1). For $n = 0$, \( \phi(a^0) = \phi(1) \) is unity in $\phi(R)$ by (3), and hence $\phi(1) = \phi(a^0)$, and (4) follows. For $n = -1$, we have $\phi(a) \cdot \phi(a^{-1}) = \phi(a \cdot a^{-1}) = \phi(1)$, which is unity in $\phi(R)$ by (3), and similarly we can show $\phi(a^{-1}) \cdot \phi(a) = \phi(1)$, and hence $\phi(a^{-1}) = \phi(a^{-1})$, the inverse of $\phi(a)$ in $\phi(R)$. For any $n \leq 0$, let $n = -s$, where $s > 0$. Then, using (1) and the case
\( n = -1 \) of (4) we have
\[
\phi(a^n) = \phi(a^{-1}) = \phi((a^{-1})^n) = \phi(a)^n = 1.
\]

(5) If \( B \) is a subring of \( R' \), then \( \phi^{-1}(B) \) is a subring
under addition. For any \( a, b \in \phi^{-1}(B) \), we have
\[
\phi(ab) = \phi(a) \cdot \phi(b) \in B,
\]
since \( B \) is a subring of \( R' \). Therefore, by the subring test, \( \phi^{-1}(B) \) is a
subring of \( R' \). Furthermore, since \( 0 \in B \), \( \ker \phi = \phi^{-1}(0) \leq \phi^{-1}(B) \).

(6) Let \( B = \{0\} \subseteq R' \) be the trivial subring. Then, by
(5),
\[
\ker \phi = \phi^{-1}(0) \text{ is a subring of } R.
\]

(7) Given \( x, y \in \phi(R) \) we have \( x = \phi(a) \) and \( y = \phi(b) \),
for some \( a, b \in R \). If \( R \) is commutative, then
\[
x y = \phi(a) \cdot \phi(b) = \phi(ab) = \phi(ba) = \phi(b) \cdot \phi(a) = y x,
\]
and \( \phi(R) \) is commutative. \( \square \)
Definition.
A ring homomorphism $\phi: R \to R'$ that is one-to-one and onto is called a ring isomorphism.
Two rings $R$ and $R'$ are isomorphic, written $R \cong R'$, if there exists a ring isomorphism $\phi: R \to R'$.

Proposition.
Let $R$ and $R'$ be isomorphic rings. Then
(1) $R$ is a commutative ring with unity iff $R'$ is a commutative ring with unity.
(2) $R$ is an integral domain iff $R'$ is an integral domain.
(3) $R$ is a field if and only if $R'$ is a field.

Example.
For $a, b \in R$, let $A(a, b) \in M(2, R)$ be defined by
\[ A(a, b) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}. \]
Let $R = \{ A(a, b) | a, b \in R \} \subseteq M(2, R)$. We want to show that $R \cong C$.

Selection. Let $\phi: R \to C$ be defined by $\phi(A(a, b)) = a + bi$.
We show (firstly) that $\phi$ is a ring homomorphism. etc.
For addition, we have
\[ \phi\left(\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} + \begin{bmatrix} a' \\ b' \\ c' \\ d' \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a+c \\ b+d \end{bmatrix}\right) = (a+c) + (b+d) \cdot i \]
\[ = (a+b \cdot i) + (c+d \cdot i) = \phi\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) + \phi\left(\begin{bmatrix} c \\ d \end{bmatrix}\right). \]

For multiplication, we have
\[ \phi\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix}\right) = \phi\left(\begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix}\right) = \phi\left(\begin{bmatrix} ac-bd \\ ad+bc \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a \\ -b \end{bmatrix}\right) \cdot \phi\left(\begin{bmatrix} c \\ d \end{bmatrix}\right). \]
\[ = (ac-bd) + (ad+bc) \cdot i = (a+b \cdot i)(c+d \cdot i) = \phi\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) \cdot \phi\left(\begin{bmatrix} c \\ d \end{bmatrix}\right). \]

Now, \( \phi \) is one-to-one since \( \phi\left(\begin{bmatrix} a \\ b \end{bmatrix}\right) = \begin{bmatrix} a \\ b \end{bmatrix} \cdot i = 0 \) iff \( a = b = 0 \), and \( \ker \phi = \{\begin{bmatrix} a \\ 0 \end{bmatrix} | a = 0\} \) is trivial.

Also, \( \phi \) is obviously onto. \( \square \)

**Example.**
We show that the equation \( 2x^3 - 5x^2 + 7x - 8 = 0 \) has no solutions in \( \mathbb{Z} \).

Let \( \phi : \mathbb{Z} \to \mathbb{Z}_3 \) be the natural homomorphism \( \phi(x) = x \mod 3 \). Suppose that there is an integer \( a \in \mathbb{Z} \) such that \( 2a^3 - 5a^2 + 7a - 8 = 0 \).
Then
\[ 0 = \phi(0) = \phi(2a^3 - 5a^2 + 7a - 8) = 2\phi(a)^3 - 5\phi(a)^2 + 7\phi(a) - 8. \]

Since \(-5 \equiv 7 \equiv -8 \equiv 1 \pmod{3}\) in \(\mathbb{Z}_3\), we have
\[ 2\phi(a)^3 - 5\phi(a)^2 + 7\phi(a) - 8 = 2\phi(a)^3 + \phi(a)^2 + \phi(a) + 1, \]
and thus \(2b^3 + b^2 + b + 1 = 0\), where \(b = \phi(a)\) in \(\mathbb{Z}_3\).

But, one can easily check that no element \(b \in \{0, 1, 2\}\) in \(\mathbb{Z}_3\) is a solution to this equation.

Therefore, there is no integer \(a \in \mathbb{Z}\) solution to the original equation. \(\square\)

Example.
Show that the rings \(\mathbb{Z}_2\) and \(3\mathbb{Z}\) are not isomorphic.

Solution.
Assume the contrary and let \(\phi: \mathbb{Z}_2 \rightarrow 3\mathbb{Z}\) be an isomorphism. Let's examine \(\phi(2)\). Note that for some \(k \in \mathbb{Z}\), \(\phi(2) = 3k\). Since \(\phi\) is a homomorphism,
\[ \phi(4) = \phi(2+2) = \phi(2) + \phi(2) = 3k + 3k = 6k. \]
But \(\phi\) is a ring homomorphism \(\phi(4) = \phi(2 \cdot 2) = \phi(2)^2 = (3k)^2 = 9k^2 \neq 6k\).
This implies that $6k = 9k^2 \Rightarrow k = 0$ or $k = \frac{2}{3}$.
For $k = 0 \Rightarrow \phi(x) = 0$ is not one-to-one and not onto. Also, $k = \frac{2}{3} \notin \mathbb{Z}$, and thus $\phi$ cannot be an isomorphism. \[ \square \]

**Example.**

Show that $\mathbb{C}$ and $\mathbb{R}$ are not isomorphic.

**Solution.**

Assume that there exists a ring homomorphism $\phi : \mathbb{R} \rightarrow \mathbb{R}$. Here, we shall look at $\phi(-1)$.
Let us recall that the ring homomorphisms map the unity in $\mathbb{C}$ to the unity in $\mathbb{R}$. In this case, we have

$$1 = \phi(1) = \phi((-1)(-1)) = \phi(-1) \cdot \phi(-1).$$

Note that, we must have $\phi(-1) \in \mathbb{R}$ and $\phi(-1)^2 = 1$, so $\phi(-1) = 1$, but our map won't be one-to-one since we must have $\phi(1) = 1$. Therefore, the only choice is $\phi(-1) = -1$. Now, since $i^2 = -1$, we have

$$-1 = \phi(-1) = \phi(i^2) = \phi(i \cdot i) = \phi(i) \cdot \phi(i) = \phi(i^2).$$

But $\phi(i) \in \mathbb{R}$, which is a contradiction. So, there is no such isomorphism from $\mathbb{C}$ to $\mathbb{R}$. \[ \square \]
Example.

Show that \( \mathbb{Q}(\sqrt{2}) \) is not isomorphic to \( \mathbb{Q}(\sqrt{5}) \) as rings.

Solution.

Firstly, let us remark that one cannot just choose a homomorphism and show that it is not an isomorphism. Basically, we are asked to show that no homomorphism from \( \mathbb{Q}(\sqrt{2}) \) to \( \mathbb{Q}(\sqrt{5}) \) can be an isomorphism. Suppose that \( \phi: \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{5}) \) is a homomorphism. If \( \phi \) is onto then we know that \( \phi(1) = 1 \) and consequently \( \phi(n) = n \) for all \( n \in \mathbb{Z} \), and moreover, \( \phi(a) = a \) for all \( a \in \mathbb{Q} \). Therefore, if \( a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \) then

\[
\phi(a + b\sqrt{2}) = \phi(a) + \phi(b\sqrt{2}) = \phi(a) + \phi(b) \phi(\sqrt{2}) = a + b \phi(\sqrt{2}).
\]

The main question is what is \( \phi(\sqrt{2}) \)?

If \( \phi(\sqrt{2}) = c + d\sqrt{5} \) then what are the possible values for \( c \) and \( d \)? Here, we shall use a tactic which is similar to that for showing that no isomorphism exists from \( \mathbb{Z} \) to \( \mathbb{Z} \).

Observe that \( \phi(2) = 2 \), and since \( 2 \in \mathbb{Z} \) and \( 2 = (\sqrt{2})^2 \) we have \( \phi(\sqrt{2}) = \phi((\sqrt{2})^2) = \phi(\sqrt{2})^2 = (c + d\sqrt{5})^2 \). Thus, we have
\[ 2 = c^2 + 5d^2 + 2cd\sqrt{5}. \]

This implies \( cd = 0 \). So, either \( c = 0 \) or \( d = 0 \). If \( c = 0 \), we have \( 2 = 5d^2 \) which gives us \( d = \sqrt{\frac{2}{5}} \in \mathbb{Q} \), false. If \( d = 0 \), we have \( 2 = c^2 \) which implies \( c = \sqrt{2} \notin \mathbb{Q} \).

In conclusion, there is no isomorphism from \( \mathbb{Q}(\sqrt{2}) \) to \( \mathbb{Q}(\sqrt{5}) \). \( \square \)

Example.

Let \( R \) be a commutative ring of prime characteristic \( p > 0 \). Show that the Frobenius map, defined by \( x \mapsto x^p \) is a ring homomorphism from \( R \) to \( R \).

Solution.

We need to show that this map respects addition and multiplication. Let us recall the binomial theorem,

\[(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p.\]

On the other hand, all these binomial coefficients are divisible by \( p \) since \( \binom{p}{k} = \frac{p!}{k!(p-k)!} \).

This implies that \( (x+y)^p = x^p + y^p \) and therefore the Frobenius map \( x \mapsto x^p \) satisfies \( \phi(x+y) = \phi(x) + \phi(y) \), \( \forall x, y \in R \).

For multiplication, we have:
\[(xy)^2 = xy \cdot xy \quad \therefore xy = x^p y^q \quad \text{since } R \text{ is commutative.}\]

Therefore, \(\phi(xy) = \phi(x) \cdot \phi(y)\), \(\forall x, y \in R\) and thus \(x \mapsto x^p\) is a ring homomorphism. \(\square\)

**Example.**

Show that \(x^3 - 8x^2 + 5x + 3 = 0\) has no solutions in \(\mathbb{Z}\).

**Solution.**

Suppose the contrary, that there exists \(x \in \mathbb{Z}\) such that \(x^3 - 8x^2 + 5x + 3 = 0\).

Consider the ring homomorphism \(\phi : \mathbb{Z} \to \mathbb{Z}_5\), \(\phi(x) = x \mod 5\). Then, we have

\[0 = \phi(0) = \phi(x^3 - 8x^2 + 5x + 3) = \phi(x^3) - 8\phi(x^2) + 5\phi(x) + 3\]

\[= \phi(x)^3 - 8\phi(x)^2 + 5\phi(x) + 3 = b^3 - 8b^2 + 3 = b^3 + 2\cdot b^2 + 3\]

where \(b = \phi(x)\) in \(\mathbb{Z}_5\). We only need to check that our equation does not have solutions in \(\mathbb{Z}_5\). We have

- \(b = 0 \Rightarrow 0^3 + 2 \cdot 0^2 + 3 = 3 \neq 0\)
- \(b = 1 \Rightarrow 1^3 + 2 \cdot 1^2 + 3 = 6 \neq 0\)
- \(b = 2 \Rightarrow 2^3 + 2 \cdot 2^2 + 3 = 4 \neq 0\)
- \(b = 3 \Rightarrow 3^3 + 2 \cdot 3^2 + 3 = 3 \neq 0\)
- \(b = 4 \Rightarrow -1^3 + 2 \cdot (-1)^2 + 3 = 4 \neq 0\). Since \(\mathbb{Z}_5 = \{0, 1, 2, \ldots, 4\}\), this yields a contradiction that \(x^3 + 2x^2 + 3 = 0\) in \(\mathbb{Z}_5\). \(\square\)
Example.

Prove that there is no ring homomorphism from \( \mathbb{Q}[\sqrt{3}] \) to \( \mathbb{Q}[\sqrt{7}] \). In particular, they are not isomorphic.

Solution.

Suppose that \( \phi: \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{7}] \) is a homomorphism. Then, we must have,

\[
\phi(3) = \phi(1+1+1) = \phi(1) + \phi(1) + \phi(1) = 1 + 1 + 1 = 3.
\]
On the other hand, \( \phi(3) = a + b\sqrt{7} \), for some \( a, b \in \mathbb{Q} \). Then

\[
3 = \phi(3) = \phi(\sqrt{3} \cdot \sqrt{3}) = \phi(13).
\]
\[
\phi(13) = \phi(13)^2 = (a + b\sqrt{7})^2 = (a^2 + 7b^2) + (2ab\sqrt{7}).
\]
This gives us the following

\[
\begin{cases}
  a^2 + 7b^2 = 3 \\
  2ab = 0.
\end{cases}
\]

The second equality implies that either \( a = 0 \) or \( b = 0 \). If \( a = 0 \), then \( b^2 = \frac{3}{7} \), which gives us \( b = \pm \frac{\sqrt{3}}{7} \in \mathbb{Q} \), impossible. If \( b = 0 \), then \( a^2 = 3 \) or \( a = \pm \sqrt{3} \in \mathbb{Q} \), false! Therefore, \( \phi: \mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{7}] \) does not exist!

Example.

Let \( R = \left\{ \begin{bmatrix} r & s \\ 2s & r \end{bmatrix} \right\} / r, s \in \mathbb{Q} \right\} \). Prove that \( R \) is a commutative ring and show that \( \mathbb{Q}[\sqrt{3}] \cong R \).

-16-
Selection.

To show that \( R \) is commutative, we need to see that \( AB = BA \), for all \( A, B \in R \). Let

\[
A = \begin{bmatrix} r & s \\ 2s & r \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} m & n \\ 2n & m \end{bmatrix}.
\]

We have

\[
AB = \begin{bmatrix} r & s \\ 2s & r \end{bmatrix} \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} = \begin{bmatrix} rm + 2ns & rn + bm \\ 2sm + 2rn & 2sn + rm \end{bmatrix}.
\]

Also,

\[
BA = \begin{bmatrix} m & n \\ 2n & m \end{bmatrix} \begin{bmatrix} r & s \\ 2s & r \end{bmatrix} = \begin{bmatrix} mr + 2ns & ms + nr \\ 2rn + 2ms & 2ns + mr \end{bmatrix}.
\]

Clearly, \( AB = BA \), and thus \( R \) is commutative.

Now, define the map \( \phi: R[\sqrt{2}] \to R \) defined by

\[
\phi(a + b\sqrt{2}) = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix}.
\]

Firstly, let us show that

\[
\phi(a + b\sqrt{2}) + \phi(c + d\sqrt{2}) = \phi((a + b\sqrt{2}) + (c + d\sqrt{2})),
\]

for \( a, b, c, d \in R \).

This is equivalent with

\[
\begin{bmatrix} a & b \\ 2b & a \end{bmatrix} + \begin{bmatrix} c & d \\ 2d & c \end{bmatrix} = \phi((a + c) + (b + d)\sqrt{2}),
\]

which is obvious.

For multiplication, we have
\[
\phi((a+b\sqrt{2})(c+d\sqrt{2})) = \phi(ac+2bd+(ad+bc)\sqrt{2}) = \\
= \begin{bmatrix}
ac+2bd & ad+bc \\
2(ad+bc) & ac+2bd
\end{bmatrix} = \\
= \begin{bmatrix}
a & b \\
2b & a
\end{bmatrix} \begin{bmatrix}
c & d \\
2d & c
\end{bmatrix} = \\
= \phi(a+b\sqrt{2}) \cdot \phi(c+d\sqrt{2}).
\]

The map is one-to-one: if \( \phi(a+b\sqrt{2}) = \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} = \\
= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \), then we must have \( a=b=0 \), and \( a+b\sqrt{2}=0 \) so \( \ker \phi = \{0\} \) and thus \( \phi \) is one-to-one. Also, \( \phi \) is onto since an arbitrary element of \( R \) is equal to \( \begin{bmatrix} a & b \\ 2b & a \end{bmatrix} \), and this equals \( \phi(a+b\sqrt{2}) \).

Therefore, \( \phi \) is an isomorphism! \( \square \)

Ideals.

In the case of a group homomorphism \( \phi: G \to G' \), the kernel, \( \ker \phi \) is a subgroup of \( G \) with the property that left coset is a right coset. We call any such subgroup a normal subgroup. We then saw that they give rise to quotient groups. Similarly, for the case of a ring homomorphism
\( \phi : R \to R', \text{ Ker}\, \phi \text{ is a subring of } R. \) In fact, Ker\, \phi is a subring of \( R \) with an extra property that will give rise to quotient rings.

**Example.**

Let \( K = \text{Ker}\, \phi, \) \( \phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \) homomorphism given by \( \phi(x) = x \mod 2. \) In this case \( K = 2\mathbb{Z} \leq \mathbb{Z}. \) Note that for any \( n \in \mathbb{Z} \) and any \( k = 2x \in K, \) we have \( \phi(nk) = \phi(2nx) = \phi(n)\phi(2x) = 0, \) and similarly, \( \phi(kn) = \phi(2xn) = \phi(2x)\phi(n) = 0. \) In other words, for any \( n \in \mathbb{Z} \) and \( k \in K \) we have \( nk \in K \) and \( kn \in K. \) We show that this property holds for the kernel of any ring homomorphism.

**Proposition.**

Let \( \phi : R \to R' \) be a ring homomorphism, and let \( K = \text{Ker}\, \phi. \) Then

1. \( K \) is a subring of \( R \)
2. For all \( r \in R \) and for all \( k \in K, \) we have \( rkeK \) and \( kereK. \)

**Definition.** Let \( R \) be a ring and \( I \) is a subset of \( R. \) Then \( I \) is called an ideal in \( R \) if
(1) \( I \) is a subring of \( R \), and
(2) For all \( r \in R \) and for all \( x \in I \), we have \( rxeI \) and \( xreI \).

\textbf{Corollary.}

Let \( \phi: R \to R' \) be a ring homomorphism with \( K = \ker \phi \). Then \( K \) is an \textbf{ideal of} \( R \).

\textbf{Ex.}

Find all the ideals of \( \mathbb{Z} \).

If \( I \) is an ideal in \( \mathbb{Z} \), then \( I \) is a subring of \( \mathbb{Z} \). Hence \( I = n\mathbb{Z} \), for some \( n \geq 1 \). So, let \( I = n\mathbb{Z} \) and let \( a \in \mathbb{Z} \) and \( b \in I \). Then \( b = nk \), for some \( k \in \mathbb{Z} \), and \( ab = a(nk) = n(ak) = n(ak) \in n\mathbb{Z} = I \), so \( I \) is an ideal. Thus, all the ideals in \( \mathbb{Z} \) are precisely \( n\mathbb{Z} \), for any \( n \geq 1 \).

\textbf{Ex.}

\( \mathbb{Z} \) is a subring of \( \mathbb{Q} \) but it is \textbf{not} an ideal in \( \mathbb{Q} \), since for instance, \( \frac{1}{2} \in \mathbb{Q} \), \( 5 \in \mathbb{Z} \), but \( 5 \cdot \frac{1}{2} \not\in \mathbb{Z} \).

\textbf{Ex.}

In any ring \( R \), \( \{0\} \) is an ideal in \( R \), called the \textbf{trivial ideal}.
and R itself is an ideal of R, called the improper ideal.

Exp. Let R be a commutative ring and let a ∈ R. Define the principal ideal generated by a, and denote <a> as follows

\[
<a> = \{ ra \mid r \in R \}.
\]

In other words, <a> consists of all multiples of a by any element r ∈ R. Note that <a> is an ideal because

1. Given x, y ∈ <a>, we have x = ra, y = sa, for some r, s ∈ R, and

\[
x - y = ra - sa = (r - s)a \in <a>.
\]

\[
xy = (ra)(sa) = (ras)a \in <a>.
\]

2. For any r ∈ R, and x = sa ∈ <a>, we have

\[
r \cdot x = r(sa) = (rs)a \in <a> \quad \text{and} \quad x \cdot r = (sa)r = (rs)a \in <a>.
\]

So, both conditions in the definition of ideal are satisfied.

Example. Every ideal in \( \mathbb{Z} \) is a principal ideal.
At this point, we know that any ideal $I$ in $\mathbb{Z}$ is of the form $I = n\mathbb{Z}$, for some $n \geq 1$. Thus $I = \langle n \rangle$, the principal ideal generated by $n$.

**Example.**

Let us find all the ideals of $\mathbb{Q}$. Let $I \neq \{0\}$ be a nontrivial ideal in $\mathbb{Q}$. So there exists an element $a \in I$, $a \neq 0$. Since $a \in \mathbb{Q}^*$, and $\mathbb{Q}$ is a field, $a$ is unit. In other words, there exists a multiplicative inverse $a^{-1} \in \mathbb{Q}$ with $a^{-1}a = 1$. But since $a^{-1} \in \mathbb{Q}$, $a \in I$, and $I$ is an ideal, we have

$$1 = a^{-1}a \in I.$$ 

Now, let us use again the fact that $I$ is an ideal, and let us take any rational number $b \in \mathbb{Q}$. Then, since $1 \in I$, and $I$ is an ideal, we have

$$b = b \cdot 1 \in I$$

and this implies $I = \mathbb{Q}$. Therefore, $\{0\}$ and $\mathbb{Q}$ are the only ideals in $\mathbb{Q}$.

This is a striking conclusion! If we look at the proof, we see that the key ingredient was the fact that $a \neq 0$ implied that $a$ is a unit or, in other words, the fact that $\mathbb{Q}$ is a field.

We have the following...
Proposition.
Let \( R \) be a commutative ring with unity. Then \( R \) is a field iff \( \{0\} \) and \( R \) are the only ideals of \( R \).

Proof.

\[ \Rightarrow \] if \( R \) is a field and \( \{0\} \) is an ideal in \( R \), then there exists \( a \in I, a \neq 0 \). Since \( R \) is a field, every nonzero element is a unit, and therefore \( 1 = a^{-1} a \in I \), since \( I \) is an ideal. Hence for all \( r \in R \), we have \( r = r \cdot 1 \in I \), and \( I = R \).

\[ \Leftarrow \] \( R \) is a commutative ring with unity, so to show that \( R \) is a field we only need to show that all the nonzero elements in \( R \) are units. Let \( a \in R, a \neq 0 \). Consider \( I = \langle a \rangle \), the principal ideal generated by \( a \). \( I = \{0\} \) since \( a \in I, a \neq 0 \). If \( \{0\} \) and \( R \) are the only ideals then we must have \( I = R \). \( R \) is ring with unity, hence \( 1 \in I \). Thus, for instance, the only ideals in \( \mathbb{Q}, \mathbb{R}, \mathbb{C} \), and \( \mathbb{Z}_p \), where \( p \) is a prime, are the trivial and the improper ideals.

Example.
Let us consider the ideal \( I = 5 \mathbb{Z} \) in \( R = \mathbb{Z} \). We know that \( (\mathbb{Z}, +) \) is an abelian group and the subgroup \( (5\mathbb{Z}, +) \) is a normal subgroup.
Hence, we have
\[ \mathbb{Z}/5\mathbb{Z} = \{ 5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z} \} \]
is a group under the commutative operation of addition of cosets:
\[ (a+5\mathbb{Z}) + (b+5\mathbb{Z}) = (a+b) + 5\mathbb{Z}. \]
Now, let us try to define a multiplication operation on \( \mathbb{Z}/5\mathbb{Z} \). The natural way would be
\[ (a+5\mathbb{Z}) \cdot (b+5\mathbb{Z}) = a \cdot b + 5\mathbb{Z}. \]
Let's see if this is well-defined!
If \( x + 5\mathbb{Z} = a + 5\mathbb{Z} \) and \( y + 5\mathbb{Z} = b + 5\mathbb{Z} \), then
\( x = a + 5k \) and \( y = b + 5j \), and so \( x = a + 5k \),
and \( y = b + 5j \), for some \( k, j \in \mathbb{Z} \). Thus,
\[ xy = (a+5k)(b+5j) = ab + 5k(b+5j). \]
Since \( 5k(b+5j) \) and \( a(5j) \) and \( (5k)(5j) \) are elements of \( 5\mathbb{Z} \), we have \( xy = ab + 5z \), where \( z \) is an element of \( 5\mathbb{Z} \), and the operation is well defined.
Note that, we have used the fact that \( 5\mathbb{Z} \) is an ideal in \( \mathbb{Z} \), and we concluded that \( b(5k) \) and \( a(5j) \) are elements of \( 5\mathbb{Z} \).
A ring $R$ is a group under addition and an ideal $I$ in $R$ is a subring of $R$, therefore a subgroup of $R$ under addition. Since $R$ is an Abelian group under addition, $I$ is a normal subgroup of $R$ under addition. Thus $R/I$ is an Abelian group under the addition of cosets. In the case of groups, we know that a subgroup being a normal subgroup is equivalent to the group operator on cosets being well-defined. The next result is similar.

**Lemma.**

Let $I$ be a subring of a ring $R$. Then $I$ is an ideal in $R$ iff multiplication

$$(a+I)(b+I) = (ab+I)$$

is a well-defined operation on the cosets of $I$ in $R$.

**Proof.**

Assume that $I$ is an ideal in $R$, and suppose that $a_1 + I = a_2 + I$ and $b_1 + I = b_2 + I$. This implies that $a_1 = a_2 + k$ and $b_1 = b_2 + j$ for some $k, j \in I$. Then

$$a_1b_1 = a_2b_2 + a_2j + b_1k + kj.$$  

Since $I$ is a subring of $R$, and therefore closed under multiplication as well as addition, $kj \in I$. Since $I$ is an ideal, $a_2j + I$ and $b_2k + I$, and so $a_2j + b_2k + I$. Therefore, $a_1b_1 + I = a_2b_2 + I$ and $a_1b_1 + I = a_2b_2 + I$. Thus, the multiplication on the set of cosets of $I$ is well defined.
Assume that the indicated operation is well-defined. We need to show that for all \( r \in R \), and \( x \in I \), we have \( rx \in I \) and \( x+I \in I \). So, let \( r \in R \) and \( x \in I \). Since \( x \in I \), we have \( x+I = 0+I = I \). Hence

\[
rx + I = (r+I)(x+I) = (a+I)(0+I) = 0+I = I.
\]

This implies that \( rx \in I \). Using a similar argument, we have \( x \in I \).

Thus \( I \) is an ideal in \( R \). 

**Theorem.**

Let \( I \) be an ideal in a ring \( R \). Then \( R/I \) is a ring under the operations defined by

1. \((a+I)(b+I) = (a+b)+I\)
2. \((a+I)(b+I) = ab+I\), for all \( a+I, b+I \in R/I \).

**Definition.**

Let \( I \) be an ideal in a ring \( R \). Then \( R/I \) with the operation on cosets specified in the above theorem is called the quotient ring of \( R \) by \( I \).

**Proposition.**

Let \( I \) be an ideal in a commutative ring \( R \) with unity \( 1 \). Then \( R/I \) is a commutative ring with unity \( 1+I \).
Theorem. (First Isomorphism Theorem for rings)
Let \( \phi : R \to R' \) be a ring homomorphism with \( K = \ker \phi \). Then
\[
\frac{R}{K} \cong \phi(R).
\]

Proof.
Since \( \phi : R \to R' \) is a group homomorphism under addition, by the isomorphism theorems for groups tells us that the map \( X : \frac{R}{K} \to \phi(R) \) defined by \( X(a+K) = \phi(a) \) is a group isomorphism. Now, to show that it is actually a ring isomorphism. Now, to show that we only need that it is a ring homomorphism or, in other words, that it respects multiplication. Let \( a+K \) and \( b+K \) be elements of \( \frac{R}{K} \). Then, we have
\[
X[(a+K)(b+K)] = X(ab+K) = \phi(ab) = \phi(a) \cdot \phi(b) = X(a+K) X(b+K), \text{ since } \phi \text{ is a ring homomorphism,}
\]
and we are done. \( \Box \)

Theorem. Given a ring \( R \) and an ideal \( K \) in \( R \), there exists an onto ring homomorphism \( \phi : R \to \frac{R}{K} \) with \( \ker \phi = K \).

Proof.
We know that the map $\phi: R \to R/k$ defined by $\phi(a) = a + k$ is a group homomorphism under addition, with $\text{Ker} \phi = k$. We need to check that it respects multiplication. So, let $a, b \in R$. Then

$$\phi(a, b) = ab + k = (a + k)(b + k) = \phi(a) \cdot \phi(b),$$

and thus $\phi$ is a ring homomorphism. Also, $\phi$ is onto. $\square$

**Proposition.**

Let $\phi: R \to R'$ be a ring homomorphism. Then

1. If $I$ is an ideal in $R$, then $\phi(I)$ is an ideal in $\phi(R)$.
2. If $J$ is an ideal in $R'$, then $\phi^{-1}(J)$ is an ideal in $R$ with $\text{Ker} \phi \subseteq \phi^{-1}(J)$.

**Proposition.**

Let $K$ be an ideal in a ring $R$. Then

1. Given an ideal $I$ in $R$, with $K \subseteq I$, then $I^* = I/k = \{a + k' \mid a \in I, k' \in K\}$ is an ideal in $R/k$.
2. Given an ideal $J^*$ in $R/k$, then there exists an ideal $J$ in $R$, with $K \subseteq J$ such that $J^* = J/k = \{a + k' \mid a \in J, k' \in K\}$. 

-28-
(3) Given ideals $I$ and $J$ in $R$, both containing $K$, then $I \subseteq J$ if and only if $I/K \subseteq J/K$.

Now, we study two special types of ideals and the corresponding quotient rings.

**Example.**

In $\mathbb{Z}$ consider the two ideals $5\mathbb{Z}$ and $6\mathbb{Z}$. Clearly, by Euclid's lemma, if $b$ and $c$ are integers such that $bc \in 5\mathbb{Z}$, then either $5|b$, in which case $b \in 5\mathbb{Z}$, or else $5|c$, in which case $c \in 5\mathbb{Z}$. On the other hand, we can have integers $x$ and $y$ such that $x \notin 6\mathbb{Z}$, and $y \notin 6\mathbb{Z}$, but $xy \in 6\mathbb{Z}$; for example $x = 4$ and $y = 9$.

Now, notice that using the ring homomorphism $\phi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\phi(x) = x \mod n$. Using the isomorphism theorem, we have

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/(2)\mathbb{Z} = \mathbb{Z}/(3)\mathbb{Z}.$$  

Hence, $\mathbb{Z}/5\mathbb{Z}$ is an integral domain, while $\mathbb{Z}/6\mathbb{Z}$ is a ring with zero divisors.

Let us also point out more difference between the two ideals $5\mathbb{Z}$ and $6\mathbb{Z}$. First, note $6\mathbb{Z} = 3\mathbb{Z} = \mathbb{Z}$, where $6\mathbb{Z} = 3\mathbb{Z}$ and $3\mathbb{Z} \neq \mathbb{Z}$. Now, suppose that
$J$ is an ideal with $5 \mathbb{Z} \leq J \leq \mathbb{Z}$. Then, there is an integer $n \in \mathbb{Z}$ such that $J = n\mathbb{Z}$. Since $5\mathbb{Z} \leq J = n\mathbb{Z}$, we have $5 \in n\mathbb{Z}$ and $5 = nk$, for some $k \in \mathbb{Z}$. But then either $n=5$ and $k=1$, in which case $5\mathbb{Z} = J$, or else $n=1$ and $k=n$, in which case $J = \mathbb{Z}$.

**Definition.**

A nontrivial proper ideal $I \subset R$ in a commutative ring $R$ is called a **prime ideal** if $ab \in I$ implies $a \in I$ or $b \in I$ in $R$.

**Definition.**

A nontrivial proper ideal $I \subset R$ in a ring $R$ is called a **maximal ideal** if the only ideals $J$ in $R$ such that $I \leq J \leq R$ are $J = I$ and $J = R$.

Thus, in the previous example, $5\mathbb{Z}$ is both a prime and a maximal ideal, while $6\mathbb{Z}$ is neither.

**Example.**

In $\mathbb{Z}$, an ideal $I$ is a prime ideal if and only if $I = p\mathbb{Z}$, where $p$ is a prime. For, on the one hand, if $p$ is a prime and $ab \in p\mathbb{Z}$, then either $a \in p\mathbb{Z}$ or $b \in p\mathbb{Z}$ and $p\mathbb{Z}$ is a prime ideal.
But on the other hand, if \( \mathbb{I} = n\mathbb{Z} \), where \( n > 1 \) is not a prime, then \( n = uv \) for some positive integers \( u, v \leq n \). Hence \( u \in \mathbb{Z} \), while \( u \not\in n\mathbb{Z} \) and \( V \not\in n\mathbb{Z} \) is not a prime ideal.

**Example.**

In \( \mathbb{Z} \) an ideal \( \mathbb{I} \) is a maximal ideal if and only if \( \mathbb{I} \) is a prime ideal. For, on the one hand, if \( \mathbb{I} = p\mathbb{Z} \) is a prime ideal and \( p\mathbb{Z} \subset \mathbb{I} \), then \( p = r \cdot k \), for some \( k \in \mathbb{Z} \). But then either \( r = p \) and \( k = 1 \), in which case \( \mathbb{I} = p\mathbb{Z} = \mathbb{I} \), or else \( r = 1 \) and \( k = p \), in which case \( \mathbb{I} = 1 \mathbb{Z} = \mathbb{Z} \).

This shows that \( \mathbb{I} = p\mathbb{Z} \) is a maximal ideal. On the other hand, if \( \mathbb{I} = n\mathbb{Z} \), \( n > 1 \), is not a prime ideal, then \( n \) is not a prime and \( n = uv \), for some \( u, v \) with \( 1 < u < n \) and \( 1 < v < n \). But then \( \mathbb{I} = n\mathbb{Z} \subset u\mathbb{Z} \subset \mathbb{Z} \), where \( n\mathbb{Z} \not\subset u\mathbb{Z} \), since \( u \not\in n\mathbb{Z} \), and \( u\mathbb{Z} \not\subset \mathbb{Z} \) since \( 1 \leq u \), and \( \mathbb{I} = n\mathbb{Z} \) is not a maximal ideal.

**Example.**

With this example, we want to point out that prime ideals and maximal ideals do not always coincide. In the ring \( \mathbb{R} = \mathbb{Z} \times \mathbb{Z} \) consider \( \mathbb{I} = \mathbb{Z} \times \{(0)_{\mathbb{Z}}\} \subset \mathbb{R} \).
One can show that $I$ is an ideal in $R$. Let $x = (a_1, b_1)$ and $y = (a_2, b_2)$ be two elements of $R$ such that $xy \in I$. Then $(a_1 a_2, b_1 b_2) = (a_1, b_1)(a_2, b_2) = xy \in I$ implies $b_1 b_2 = 0$. Since $\mathbb{Z}$ has no zero divisors, either $b_1 = 0$ and $x \in I$ or $b_2 = 0$ and $y \in I$. Therefore, $I$ is a prime ideal. But $I$ is not a maximal ideal in $R$ since we have

$$I = \mathbb{Z} \times \{0\} \subseteq \mathbb{Z} \times \mathbb{Z} < \mathbb{Z} \times \mathbb{Z} = R,$$

where $\mathbb{Z} \times \{0\} \neq \mathbb{Z} \times \mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z} \neq \mathbb{Z} \times \mathbb{Z}$, and $\mathbb{Z} \times \mathbb{Z}$ is an ideal in $R$.

The importance of the notions of prime ideal and maximal ideal becomes apparent with the next theorem.

**Theorem.** Let $R$ be a commutative ring with unity, and let $I$ be an ideal in $R$. Then

1. $I$ is a prime ideal in $R$ if and only if $R/I$ is an integral domain.
2. $I$ is a maximal ideal in $R$ if and only if $R/I$ is a field.

**Proof.** (1) $R/I$ will therefore be an integral domain if and only if it has no zero divisors. This
condition is equivalent to the condition that

\[(a+I)(b+I) = I \iff a+I = I \text{ or } b+I = I.\]

Thus \(R/I\) is an integral domain if and only if \(ab+I = I\) implies that \(a+I = I\) or \(b+I = I\) or, in other words, if and only if \(ab = I\) implies that \(a = I\) or \(b = I\), which is to say that \(I\) is a prime ideal in \(R\).

(2) By a previous proposition we know that \(R/I\) will be a field if and only if its only ideals are \(0/I\) and \(R/I\). Suppose \(R/I\) is a field and consider any ideal \(J\) in \(R\) such that \(I \subseteq J \subseteq R\). This implies that \(0/I \subseteq J/I \subseteq R/I\) and \(J/I\) is an ideal in \(R/I\). Thus either \(J/I = 0/I\), in which case \(J = I\), or \(J/I = R/I\), in which case \(J = R\). Thus \(I\) is maximal ideal in \(R\). Conversely, suppose that \(I\) is a maximal ideal in \(R\) and consider any ideal \(J^*\) in \(R/I\). Again, by a previous proposition, \(J^* = J/I\) for some ideal \(J\) in \(R\) such that \(I \subseteq J \subseteq R\). Since \(I\) is a maximal ideal, either \(J = I\), in which case \(J^* = 0/I\), or \(J = R\), in which case \(J^* = R/I\). Thus \(R/I\) is a field. \(\square\)
Corollary.

In a commutative ring $R$ with unity, every maximal ideal is a prime ideal.

Proof: If $I$ is a maximal ideal in $R$, then $R/I$ is a field. Every field is an integral domain, so $R/I$ is an integral domain, and $I$ is a prime ideal. \(\Box\)

Example.

Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be the ring homomorphism defined by $\phi((a,b)) = b$. Then $\ker \phi = \mathbb{Z} \times \{0\}$, and by the isomorphism theorem, we have

$$(\mathbb{Z} \times \mathbb{Z}) / (\mathbb{Z} \times \{0\}) \cong \mathbb{Z},$$

which is an integral domain, but not a field. This agrees with the conclusion in the previous example that $\mathbb{Z} \times \{0\}$ is a prime ideal but not a maximal ideal.

Example.

Let $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_3$ be the ring homomorphism defined by $\phi((a,b)) = b \mod 3$. Then $\ker \phi = \mathbb{Z} \times \{0\}$ and $$(\mathbb{Z} \times \mathbb{Z}) / (\mathbb{Z} \times \{0\}) \cong \mathbb{Z}_3,$$

which is a field. Thus $\mathbb{Z} \times \mathbb{Z}_3$ is a maximal ideal in $\mathbb{Z} \times \mathbb{Z}$.\(\text{-}\)