Motivation and Introduction

Main purpose of this course is to study Galois theory — a field that arose in trying to study roots of polynomials.

Consider $f(x) = ax^2 + bx + c$. If we want to find a general, closed-form expression for the roots of the function, we complete the square.

$$\text{roots} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

We found these roots by by the coefficients, $\mathbb{Q}$, addition, subtraction, multiplication, division, and square root (raising to the 1/2 power: see Math 310 notes, Page 104). Naturally, this leads us to ask whether we can do this for cubic polynomials with the same operations. Obviously, we have to change from 1/2 power to the 1/3 power, but Cardano showed that it was possible to solve a cubic and quartic equation using these traditional operations and radicals.

Évariste Galois invented his theory to prove there is no such closed formula by radicals for any polynomial of degree 5 or above.

For example, $x^5 - x + 1$ does not have roots given by radicals.

Example: A Solvable Polynomial

Consider the polynomial $f(x) = x^2 - 2$. We know that the roots of this polynomial are $\pm\sqrt{2}$. From this, we want to create a set $K(f)$ that satisfies the following rules:

- $\mathbb{Q} \subseteq K(f)$.
- $K(f)$ must contain the roots of f.
- $K(f)$ must be closed under the traditional operations: $+, -, \times, /$
- $K(f)$ must be the smallest field that satisfies the above three requirements.

Claim: $K(f) = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

- $\mathbb{Q} \subseteq K(f)$, because we can set $b = 0$.
- $\sqrt{2} = 0 + (1)(\sqrt{2})$, $-\sqrt{2} = 0 + (-1)(\sqrt{2})$
- Let $a + b\sqrt{2}$ and $c + d\sqrt{2}$ be elements of $K(f)$. Then,
  - $(a + b\sqrt{2}) \pm (c + d\sqrt{2}) = (a \pm c) + (b \pm d)\sqrt{2}$
  - $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$
  - Set $c + d\sqrt{2} \neq 0$

$$\begin{aligned}
\frac{a + b\sqrt{2}}{c + d\sqrt{2}} &= \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} \\
&= \frac{1}{c^2 - 2d^2}\left((ac - 2bd) + (bc - ad)\sqrt{2}\right) \\
&= \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}
\end{aligned}$$

- $K(f)$ is indeed the smallest set.
  - Note that $K(f)$ is a $\mathbb{Q}$-vector space, with basis $\{1, \sqrt{2}\}$. Therefore, $\dim_{\mathbb{Q}} K(f) = 2$. $K(f)$ is known as the "splitting field" of f.

We want to consider a bijective function $\varphi : K(f) \to K(f)$ with the following properties:

- $\varphi(r) = r$ for every $r \in \mathbb{Q}$
- $\varphi(x+y) = \varphi(x) + \varphi(y)$
- $\varphi(xy) = \varphi(x)\varphi(y)$

We denote the collection of all such φ as $\text{Aut}(K(f)/\mathbb{Q})$. This is a group under the operation $\circ$ (composition). Specifically, we have

$$\begin{aligned}\varphi(a+b\sqrt{2}) &= \varphi(a) + \varphi(b)\varphi(\sqrt{2})\\ &= a + b\varphi(\sqrt{2}).\end{aligned}$$

Notice

$$\begin{aligned}\left(\varphi(\sqrt{2})\right)^2 - 2 &= \varphi\left(\left(\sqrt{2}\right)^2 - 2\right)\\ &= \varphi(0)\\ &= 0.\end{aligned}$$

Therefore, $\varphi(\sqrt{2}) = \pm\sqrt{2}$. Therefore, we have that the elements of $\text{Aut}(K(f)/\mathbb{Q})$ as the following:

$$\begin{aligned}\varphi_0 &: a+b\sqrt{2} \mapsto a+b\sqrt{2}\\ \varphi_1 &: a+b\sqrt{2} \mapsto a-b\sqrt{2}\\ \varphi_1 \circ \varphi_1 &= \varphi_0\end{aligned}$$

Thus,

$$\begin{aligned}\text{Aut}(K(f)/\mathbb{Q}) &= \{\varphi_0, \varphi_1\}\\ &\cong \mathbb{Z}/2\mathbb{Z}\end{aligned}$$

Example: A Harder Polynomial

Let $f(x) = (x^2-2)(x^2-3)$. Our roots are $\{\pm\sqrt{2}, \pm\sqrt{3}\}$. We want to form $K(f)$ with the same properties. Let

$$\begin{aligned}K(f) &= \mathbb{Q}(\sqrt{2}, \sqrt{3})\\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a,b,c,d \in \mathbb{Q}\}.\end{aligned}$$

Just as with our previous example, $K(f)$ is a vector space over $\mathbb{Q}$, with basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$, so $\dim_{\mathbb{Q}} K(f) = 4$.

Now, we want $\text{Aut}(K(f)/\mathbb{Q})$. If $\varphi \in \text{Aut}(K(f)/\mathbb{Q})$, then

$$\begin{aligned}\varphi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{6})\\ &= a + b\varphi(\sqrt{2}) + c\varphi(\sqrt{3}) + d\varphi(\sqrt{2})\varphi(\sqrt{3}).\end{aligned}$$

Thus, we need to know $\varphi(\sqrt{2})$ and $\varphi(\sqrt{3})$. So,

$$\begin{aligned}f(\varphi(\sqrt{2})) &= \left(\left(\varphi(\sqrt{2})\right)^2 - 2\right)\left(\left(\varphi(\sqrt{2})\right)^2 - 3\right)\\ &= 0\end{aligned}$$

and the same is the case with $\varphi(\sqrt{3})$. So,

$$\begin{aligned}\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\}\\ \varphi(\sqrt{3}) &\in \{\pm\sqrt{2}, \pm\sqrt{3}\}.\end{aligned}$$

Suppose $\varphi(\sqrt{2}) = \sqrt{3}$. Then,

$$\begin{aligned}
\left(\left(\varphi(\sqrt{2})\right)^2\right) &= (\sqrt{3}^2 - 1)\\
&= 0\\
&= (\varphi(2) - 3)\\
&= -1. \perp
\end{aligned}$$

Thus,

$$\begin{aligned}
\varphi(\sqrt{2}) &\in \{\pm\sqrt{2}\}\\
\varphi(\sqrt{3}) &\in \{\pm\sqrt{3}\},
\end{aligned}$$

and we have the maps as:

$$\begin{aligned}
\varphi_0 &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}\\
\varphi_1 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}\\
\varphi_2 &: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}\\
\varphi_3 &: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}
\end{aligned}$$

Example: A Cubic Polynomial

Consider the function $f(x) = x^3 - 2$. The function has one real root, $r_1 = \sqrt[3]{2}$, and two complex roots. Let's examine $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$; r_2 and r_3 are not in $Q(\sqrt[3]{2})$. We could instead consider $\mathbb{Q}(\sqrt[3]{2}, r_1, r_2)$.

$$\begin{aligned}
x^3 - 2 &= (x - r_1)(x^2 + r_1 x + r_1^2)\\
r_2 &= \frac{-r_1 + \sqrt{r_1^2 - 4r_1^2}}{2}\\
&= r_1\frac{-1 + \sqrt{-3}}{2}\\
&= r_1\zeta_3\\
r_3 &= r_1\frac{-1 - \sqrt{-3}}{2}\\
&= r_1\zeta_3^2
\end{aligned}$$

However, including r_2 and r_3 is excessive — all we need is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Therefore, the basis of this vector space is $\{1, r_1, r_1^2, \zeta_3, \zeta_3 r_1, \zeta_3 r_1^2\}$ (note that $\zeta_3^2 = -1 - \zeta_3$). Therefore, $\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = 6$, and $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = K(f)$.Additionally, we have $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\varphi_0\}$, but $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$. For the full field extension, we need to find $\varphi(\sqrt[3]{2})$ and $\varphi(\zeta_3)$.

$$\begin{aligned}
\varphi(\sqrt[3]{2}) &\in \{r_1, \zeta_3 r_1, \zeta_3^2 r_1\}\\
\varphi(\zeta) &\in \{\zeta_3, \zeta_3^2\}\\
\varphi_0 &: r_1 \mapsto r_1, \zeta_3 \mapsto \zeta_3\\
\varphi_1 &: r_1 \mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3\\
\varphi_2 &: r_1 \mapsto r_1, \zeta_3 \mapsto \zeta_3^2\\
\varphi_3 &: r_1 \mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3\\
\varphi_4 &: r_1 \mapsto \zeta_3 r_1, \zeta_3 \mapsto \zeta_3^2\\
\varphi_5 &: r_1 \mapsto \zeta_3^2 r_1, \zeta_3 \mapsto \zeta_3^2
\end{aligned}$$

Therefore,

$$\begin{aligned}\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) &= 6 \\ &= \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{,}\sqrt[3]{2})\end{aligned}$$

Rings

Consider the integers under the normal operations, $(\mathbb{Z}, +, \cdot)$; this will serve as the motivation for rings in the future.

Definition of a Ring

Let R be a nonempty set with operations $(+, \cdot)$, with the following properties:

(1) $(R, +)$ is an abelian group:

- Closed: $r_1 + r_2 \in R,\ \forall r_1, r_2 \in R$
- Identity: $\exists 0_R,\ r + 0_R = 0_R + r = r$
- Associativity: $r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$
- Inverse: $\forall r \in R,\ \exists - r \in R, r + (-r) = 0_R$
- Commutativity: $r_1 + r_2 = r_2 + r_1$

(2) Closure under Multiplication: $r_1 \cdot r_2 \in R,\ \forall r_1, r_2 \in R$

(3) Associativity under Multiplication: $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$

(4) Distributivity: $r_1 \cdot (r_2 + r_3) = r_1 \cdot r_2 + r_2 \cdot r_3, (r_1 + r_2) \cdot r_3 = r_1 \cdot r_3 + r_2 \cdot r_3$

We say $(R, +, \cdot)$ is a ring if it satisfies all these properties.

If $\exists 1_R \in R$ such that $r \cdot 1_R = 1_R \cdot r = r$, then we say R is a ring with identity, and 1_R is the multiplicative identity. If multiplication is commutative, then R is known as a commutative ring.

Examples

(1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are commutative rings with identity value of 1.

(2) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative ring with identity $1_R = [1]_n$.

(3) $(\mathbb{R}[x], +, \cdot)$, where $\mathbb{R}[x] = \left\{\sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{R}\right\}$, is a commutative ring with identity.

(4) $(2\mathbb{Z}, +, \cdot)$ is a commutative ring *without* identity.

(5) $(\operatorname{Mat}_n(\mathbb{R}), +, \cdot)$, where $\operatorname{Mat}_n(\mathbb{R})$ refers to $n \times n$ matrices with real entries, is a *non*commutative ring with identity.

Division Rings and Fields

Let R be a ring with identity. We say R is a *division ring* if $\forall r \in R \setminus \{0_R\}$, $\exists r^{-1} \in R$ with $r \cdot r^{-1} = 1_R = r^{-1} \cdot r$. If R is also commutative, then R is a *field*.

Examples

(1) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, and $(\mathbb{C},+,\cdot)$ are all fields.

(2) Let p be prime, and set $F=\mathbb{Z}/p\mathbb{Z}$. Then, F is a field; we denote this $\mathbb{F}_p$.

(3) Define

$$\mathbb{H}=\{a+bi+cj+dk \mid a,b,c,d\in\mathbb{R}, i^2=j^2=k^2=-1, ij=k=-ji, jk=i=-kj, ki=j=-ik\}.$$

Then, $\mathbb{H}$ is a division ring, known as the Hamiltonian quaternions. Note that $\mathbb{C}\subset\mathbb{H}$.

Properties of Rings

Proposition 4.1: Let R be a ring.

(1) $0_R a = a0_r = 0\ \forall a\in R$
(2) $(-a)b=a(-b)=-(ab)\ \forall a,b\in R$
(3) $(-a)(-b)=ab\ \forall a,b\in R$
(4) If $\exists 1_R\in R$, then 1_R is unique, and $-a=(-1_R)a$.

Proof of (1): Let $a\in R$. Then,

$$\begin{aligned}
0_R a &= (0_R+0_R)a && \text{Additive Inverse}\\
0_R a &= 0_R a + 0_R a && \text{Distributivity}\\
0_R a + (-0_R a) &= 0_R a + 0_R a(-0_R a) &&\\
0_R &= 0_R a. && \text{Additive Inverse}
\end{aligned}$$

Proof of (2): Let $a,b\in R$. Note that $-(ab)$ is the unique inverse such that $ab+(-(ab))=0_R$ via group theory. We have

$$\begin{aligned}
ab+(-a)b &= (a+(-a))b && \text{Distributivity}\\
&= (0_R)b && \text{Additive Inverse}\\
&= 0_R. && \text{By Property (1)}
\end{aligned}$$

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

Zero Divisor and Units in Rings

Let $a\in R$, $a\neq 0_R$. If $\exists b\in R$ with $b\neq 0_R$ such that $ab=0_R=ba$, then we say a is a zero divisor.

If $1_R\in R$, we say $u\in R$ is a unit if $\exists v\in R$ (can be equal to u) with $uv=1_R=vu$. The collection of units in R is denoted $R^\times$.

Exercise: Show that $R^\times$ is a group under multiplication.

Examples

(1) Let $R=\mathbb{Z}/6\mathbb{Z}$. Note that $[2]_6[3]_6=[6]_6=[0]_6$, so both $[2]_6$ and $[3]_6$ are both zero divisors. Additionally, $[4]_6[3]_6=[6]_6=[0]_6$. Meanwhile, since $(\mathbb{Z}/6\mathbb{Z})^\times=\{[1]_6,[5]_6\}$, those are the two units of $\mathbb{Z}/6\mathbb{Z}$.

(2) $\mathbb{Z}$ has no zero divisors. $\mathbb{Z}^\times=\{\pm 1\}$.

(3) $\mathbb{Q}$ has no zero divisors. $\mathbb{Q}^\times=\mathbb{Q}\setminus\{0\}$.

(4) $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}, i^2=-1\}$ has no zero divisors (as $\mathbb{C}$ is a field). $\mathbb{Z}[i]^\times=\{\pm 1,\pm i\}$.

Subrings

Let $(R, +, \times)$. If $S \subseteq R$ is a nonempty subset, and $(S, +, \cdot)$ is a ring, then S is a subring of R. To see S is a subring, it is enough to show:

- $S \neq \emptyset$.
- S is closed under subtraction.
- S is closed under multiplication of elements in S.

Examples

(1)

$$\underbrace{\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}}_{\text{subrings}}$$

(2) $\mathbb{R} \subseteq \mathbb{R}[x]$ is a subring.

(3) $S = \{[0]_4, [2]_4\} \subseteq \mathbb{Z}/4\mathbb{Z}$ is a subring.

Integral Domains

Let R be a commutative ring with identity. We say R is an integral domain if R has no zero divisors.

Examples

(1) $\mathbb{Z}$, the integers, is an integral domain, that is not a field.

(2) All fields are integral domains.

(3) $\mathbb{Z}/6\mathbb{Z}$ is *not* an integral domain, as it has zero divisors.

(4) $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain if n is composite.

Integral domains are nice due to allowance of cancellations. For example, if $2m = 2n$ in $\mathbb{Z}$, then we find $2(m - n) = 0$, and since $\mathbb{Z}$ has no zero divisors, it must be the case that $m = n$.

However, in a ring that is not an integral domain, such as $\mathbb{Z}/6\mathbb{Z}$, we cannot use the same technique to find the solution to a similar equation. For example, $3 \cdot 2 = 0 = 3 \cdot 4$, but $2 \neq 4$.

Proposition: Equations in Integral Domains

Let R be an integral domain. If $a, b, c \in R$ with $a \neq 0_R$, and $ab = ac$, then $b = c$.

Proof:

$$\begin{aligned} ab &= ac \\ a(b - c) &= 0_R \end{aligned}$$

Since $a \neq 0$,

$$\begin{aligned} b - c &= 0_R \\ b &= c. \end{aligned}$$

Theorem: Finite Integral Domains and Fields

If R is an integral domain, and $\text{card}(R) < \infty$,then R is a field.

Proof: Let $a \in R$, $a \neq 0_R$. Note $ab \neq 0_R$ for all $b \in R$, $b \neq 0_R$.

Define $\varphi_a : R \setminus \{0_R\} \to R \setminus \{0_R\}$, $b \mapsto ab$. If $\varphi_a(b) = \varphi_a(c)$, then $ab = ac$, and by our previous result, $b = c$ — therefore, φ_a is injective.

Since $R \setminus \{0_R\}$ is finite, and φ_a is injective, then φ_a is surjective. In particular, this means $\exists b \in R \setminus \{0_R\}$ with $\varphi_a(b) = 1_R$; therefore, $ab = 1_R$. Since R is commutative, $ba = 1_R$, so $b = a^{-1}$.

Examples of Abstract Rings

Ring of Integers in a Field

Let $d \in \mathbb{Z}$, d is square-free (there is no square that divides d). Set $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$. This is a field (can be verified as a subfield of $\mathbb{C}$).

We can define

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\} & d \equiv 2, 3 \mod 4 \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\left(\frac{1+\sqrt{d}}{2}\right) \mid a, b \in \mathbb{Z}\right\} & d \equiv 1 \mod 4 \end{cases}.$$

Then, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a subring of $\mathbb{Q}(\sqrt{d})$. This is known as the ring of integers of $\mathbb{Q}(\sqrt{d})$. This set behaves in $\mathbb{Q}(\sqrt{d})$ the same say that $\mathbb{Z}$ does inside $\mathbb{Q}$. The set $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is the collection of all roots in $\mathbb{Q}(\sqrt{d})$ of monic (coefficient of highest degree is 1) polynomials with coefficients in $\mathbb{Z}$.

For example, if $d = -1$, defining $\mathbb{Q}(i)$, then we can verify that $\mathbb{Z}[i]$ is a root of a monic polynomial with coefficients in $\mathbb{Z}$.

Ring of Matrices

Let R be a ring. Then,

$$\text{Mat}_n(R) = \{n \times n \text{ matrices with entries in } R\}$$

is a ring under matrix addition and multiplication.

Ring of Functions

Let $L^1(\mathbb{R})$ be all functions $f : \mathbb{R} \to \mathbb{R}$ such that

$$\int_{\mathbb{R}} |f(x)| dx$$

exists. The set $L^1(\mathbb{R})$ is a ring under pointwise addition and convolution, where convolution is defined as

$$(f * g)(x) = \int_{\mathbb{R}} f(x - y) g(y) dy.$$

This is a commutative ring without identity.

Group Ring

Let K be a field and G a group. Set $K[G]$ to be all formal linear combinations of the form

$$\alpha = \sum_{x \in G} a_x x,$$

with $a_x \in K$, $x \in G$, with $a_x = 0$ for all but finitely many x.

Given

$$\alpha = \sum_{x \in G} a_x x$$
$$\alpha = \sum_{y \in G} b_y y,$$

define

$$\begin{aligned} \alpha + \beta &= \sum_{x \in G} (a_x + b_x) x \\ \alpha\beta &= \sum_{x \in G} \sum_{y \in G} a_x b_y xy \\ &= \sum_{z \in G} \left(\sum_{xy = z} a_x b_y \right) z. \end{aligned}$$

This is a ring under these operations, known as the group ring. It is commutative if and only if G is abelian.

Polynomials under a Ring

Let R be a ring. Set

$$R[x] = \left\{ \sum_{i=1}^{n} a_i x^i \mid a_i \in R, n \in \mathbb{Z}_{\geq 0} \right\}$$

to be the all polynomials with coefficients in R. This is a ring under polynomial addition and multiplication. If R is commutative, then $R[x]$ is commutative.

Proposition: Polynomial Properties

Let R be an integral domain, with $p(x), q(x) \in R[x] \setminus \{0\}$. Then:

(1) $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$

(2) $R[x]^\times = R^\times$

(3) $R[x]$ is an integral domain.

Proof of (1): Let

$$p(x) = a_m x^m + \cdots + a_1 x + a_0$$
$$q(x) = b_n x^n + \cdots + b_1 x + b_0$$

with $a_m, b_n \neq 0$ — $\deg(p) = m$ and $\deg(q) = n$. Then,

$$p(x)q(x) = a_m b_n x^{m+n} + \text{lower degree terms},$$

and since $a_m b_n \neq 0$ as R is an integral domain with $a_m, b_n \neq 0$, $\deg(pq) = m + n$.

Ring Homomorphism

Let R and S be rings. A ring homomorphism between R and S is a map $\varphi : R \to S$ that satisfies the following properties for all $r_1, r_2 \in R$:

(1) $\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2)$

(2) $\varphi(r_1 \cdot_R r_2) = \varphi(r_1) \cdot_S \varphi(r_2)$

The kernel of a ring homomorphism φ is given by

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

A bijective ring homomorphism is called an isomorphism. If there exists such a bijection between R and S, we say R and S are isomorphic.

If φ is an isomorphism, we write

$$\varphi : R \xrightarrow{\simeq} S$$

Examples: Ring Homomorphisms

Not a Ring Homomorphism

Let $R = \mathbb{Z}$ and $S = 2\mathbb{Z}$. Define

$$\begin{aligned} \varphi : \mathbb{Z} &\to 2\mathbb{Z} \\ n &\mapsto 2n. \end{aligned}$$

Let $m, n \in \mathbb{Z}$. We have

$$\begin{aligned} \varphi(m+n) &= 2(m+n) \\ &= 2m + 2n \\ &= \varphi(m) + \varphi(n). \end{aligned}$$

However,

$$\begin{aligned} \varphi(mn) &= 2(mn) \\ \varphi(m)\varphi(n) &= 4(mn). \end{aligned}$$

Homomorphism between Integers and Integers Modulo n

Consider $R = \mathbb{Z}$ and $S = \mathbb{Z}/n\mathbb{Z}$. Define

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ a &\mapsto [a]_n. \end{aligned}$$

Let $a, b \in \mathbb{Z}$. We have

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

Additionally, we have

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

So, φ is a ring homomorphism. Note that

$$\begin{aligned}\ker(\varphi) &= \{a \in \mathbb{Z} \mid \varphi(a) = [0]_n\}\\ &= \{a \in \mathbb{Z} \mid [a]_n = [0]_n\}\\ &= \{a \in \mathbb{Z} \mid n|a\}\\ &= n\mathbb{Z}.\end{aligned}$$

Homomorphism Between the Polynomials and Reals

Let $S = \mathbb{R}[x]$ and $T = \mathbb{R}$. Define

$$\begin{aligned}\varphi_a : \mathbb{R}[x] &\to \mathbb{R}\\ f &\mapsto f(a)\end{aligned}$$

Let $f(x), g(x) = \mathbb{R}[x]$. Then,

$$\begin{aligned}\varphi_a(f(x) + \varphi(g)(x)) &= \varphi_a((a_0 + b_0) + \cdots + (a_m + b_m)x^m + b_{m+1}x^{m+1} + \cdots b_n x^n)\\ &= (a_0 + b_0) + \cdots + (a_m + b_m)a^m + b_{m+1}a^{m+1} + \cdots + b_n a^n\\ &= \varphi_a(f(x)) + \varphi_a(g(x)).\end{aligned}$$

Similarly, we can verify that $\varphi_a(f(x)g(x)) = \varphi_a(f(x))\varphi_a(g(x))$. So, φ_a is a ring homomorphism. Note that

$$\begin{aligned}\ker(\varphi_a) &= \{f(x) \in \mathbb{R}[x] \mid f(a) = 0\}\\ &= \{f(x) \in \mathbb{R}[x] \mid (x-a)|f(x)\}\\ &= (x-a)\mathbb{R}[x]\end{aligned}$$

Homomorphism between Matrices

Define

$$\begin{aligned}R &= \left\{\begin{bmatrix} a & b \\ 0 & d\end{bmatrix} \in \operatorname{Mat}_2(\mathbb{R})\right\}\\ S &= \mathbb{R},\end{aligned}$$

and

$$\begin{aligned}\varphi : R &\to S\\ \begin{bmatrix} a & b \\ 0 & d\end{bmatrix} &\mapsto a.\end{aligned}$$

Then,

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

and

$$\begin{aligned}\varphi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & d_1\end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & d_2\end{bmatrix}\right) &= \varphi\left(\begin{bmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ 0 & d_1d_2\end{bmatrix}\right)\\ &= a_1a_2\\ &= \varphi\left(\begin{bmatrix} a_1 & b_1 \\ 0 & d_1\end{bmatrix}\right)\varphi\left(\begin{bmatrix} a_2 & b_2 \\ 0 & d_2\end{bmatrix}\right).\end{aligned}$$

So φ is a ring homomorphism that is surjective but not injective. Note

$$\ker(\varphi) = \left\{ \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix} \mid b, d \in \mathbb{R} \right\}.$$

Proposition: Fundamental Theorem of Ring Homomorphisms

Let $\varphi : R \to S$ be a ring homomorphism.

(1) The image of φ, $\varphi(R) = \{s \in S \mid s = \varphi(r) \text{ for some } r \in R\}$, is a subring of S.

(2) The kernel, $\ker(\varphi)$, is a subring of R.

Additionally, for any $r \in R$, and $a \in \ker(\varphi)$, $ar \in \ker(\varphi)$ and $ra \in \ker(\varphi)$.

Proof of (2): To show $\ker(\varphi)$ is a subring, we must show that $\ker(\varphi)$ is non-empty, closed under subtraction, and closed under multiplication.

First, since $\varphi(0_R) = 0_S$ (verify this), $\ker(\varphi)$ is non-empty.

Let $a, b \in \ker(\varphi)$. We have

$$\begin{aligned} \varphi(a-b) &= \varphi(a + (-b)) \\ &= \varphi(a) + \varphi(-b) \\ &= \varphi(a) - \varphi(b) && \text{check } \varphi(-b) = -\varphi(b) \\ &= 0_S - 0_S \\ &= 0_S. \end{aligned}$$

Thus, $a - b \in \ker(\varphi)$, and $\ker(\varphi)$ is closed under subtraction.

To show $\ker(\varphi)$ is closed under multiplication, we will prove the general case. Let $a \in \ker(\varphi)$ and $r \in R$. We have

$$\begin{aligned} \varphi(ra) &= \varphi(r)\varphi(a) \\ &= \varphi(r)0_S \\ &= 0_S. \end{aligned}$$

Similarly, $\varphi(ar) = 0_S$. So, $ar, ra \in \ker(\varphi)$.

The stronger condition that we found for $\ker(\varphi)$ (closed under multiplication of all elements of the ring, not merely those from the subring) forms what we call an ideal.

Quotient Rings

Defining an Equivalence Relation on a Ring

Set $K = \ker(\varphi)$. We will define a relation on R, $\sim$, where $r_1 \sim r_2$ if $r_1 - r_2 \in K$. We want to see if $\sim$ is an equivalence relation:

- Reflexive: $r \sim r$ since $r - r = 0_R \in K$.
- Symmetric: $r_1 \sim r_2$ implies $r_1 - r_2 = k$ for some $k \in K$. Since k is a subring, $-k \in K$, so $r_2 - r_1 \in K$.

- Transitive: suppose $r_1 \sim r_2$ and $r_2 \sim r_3$. This means there are elements $k_1, k_2 \in K$ with $r_1 - r_2 = k_1$ and $r_2 - r_3 = k_2$. Since K is a subring, $(r_1 - r_2) + (r_2 - r_3) = r_1 - r_3 = k_1 + k_2 \in K$. Thus, $r_1 \sim r_3$.

Since $\sim$ is reflexive, symmetric, and transitive, $\sim$ is an equivalence relation on R.

Since $\sim$ is an equivalence relation on R, we will want to examine equivalence classes of R under $\sim$. Specifically, for $r \in R$, we have

$$\begin{aligned}
[r]_K &= \{\tilde{r} \in R \mid r - \tilde{r} \in K\} \\
&= \{\tilde{r} \in R \mid r - \tilde{r} = k \text{ for some } k \in K\} \\
&= \{r + k \mid k \in K\} \\
&= r + K.
\end{aligned}$$

We will define the set

$$R/K = \{r + K \mid r \in R\}$$

to be the set of all equivalence classes.

Example: Let $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto [a]_n$. Then, $\ker(\varphi) = n\mathbb{Z}$. Then, $R/K = \mathbb{Z}/n\mathbb{Z}$.

Let $r_1 + K, r_2 + K \in R/K$. The new question is whether or not we can define addition and multiplication on R/K. Suppose that the following are the definition of multiplication and addition on R/K.

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

Suppose $r_1 + K = \tilde{r}_1 + K$ and $r_2 + K = \tilde{r}_2 + K$. This means there are $k_1, k_2 \in K$ with $r_1 - \tilde{r}_1 = k_1$, $r_2 - \tilde{r}_2 = k_2$, or that $r_1 = \tilde{r}_1 + k_1$, $r_2 = \tilde{r}_2 + k_2$.

To see if the map is well-defined, we have

$$\begin{aligned}
(r_1 + K) + (r_2 + K) &= (r_1 + r_2) + K \\
&= (\tilde{r}_1 + k_1 + \tilde{r}_2 + k_2) + K \\
&= (\tilde{r}_1 + k_1) + K + (\tilde{r}_2 + k_2) + K \\
&= (\tilde{r}_1 + K) + (\tilde{r}_2 + K)
\end{aligned}$$

since $\tilde{r}_1 + k_1 - \tilde{r}_1 = k \in K$.

Thus, our addition is well-defined.

Examining multiplication, we see that

$$\begin{aligned}
(r_1 + K)(r_2 + K) &= r_1 r_2 + K \\
&= (\tilde{r}_1 + k_1)(\tilde{r}_2 + k_2) + K \\
&= \tilde{r}_1\tilde{r}_2 + \underbrace{k_1\tilde{r}_2 + \tilde{r}_1 k_2 + k_1 k_2}_{\in K \text{ since } K = \ker(\varphi)} + K \\
&= \tilde{r}_1\tilde{r}_2 + K.
\end{aligned}$$

Therefore, our multiplication is well-defined.

We can show that R/K is a ring (verify for yourself).

Note: This construction would not have worked if K was merely a subring, as multiplication would not be well-defined.

Ideals

Let $I \subseteq R$ be a subring.

(1) If $ra \in I$ for every $r \in R$, we say I is a left-ideal of R.

(2) If $ar \in I$ for every $r \in R$, then we say I is a right-ideal of R.

(3) If I is a left-ideal and a right-ideal of R, then we say I is an ideal of R.

If $I \subseteq R$ is an ideal, we define $r_1 \sim_I r_2$ if $r_1 - r_2 \in I$, and $R/I = \{r + I \mid r \in I\}$. Addition and multiplication in R/I are defined as

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

Examples of Ideals

(1) $n\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal; if $nk \in n\mathbb{Z}$, and $m \in \mathbb{Z}$, then $m(nk) = n(mk) \in n\mathbb{Z}$.

(2) Let $R = \mathbb{Z}[x]$. Set $\langle x^2 \rangle = \{f(x)x^2 \mid f(x) \in \mathbb{Z}[x]\}$. This is an ideal.

(3) Let R be a ring. If $r \in R$, we define $\langle r \rangle = \{ar \mid a \in R\}$.

(4) Set $I = \{(2n, 0) \mid n \in \mathbb{Z}\}$ in $\mathbb{Z} \times \mathbb{Z}$. Let $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Then, $(a, b)(2n, 0) = (2an, 0) \in I$, meaning I is an ideal.

(5) Define $R = \left\{\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in \operatorname{Mat}_2(\mathbb{R})\right\}$. Consider $I = \left\{\begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \mid a, b \in \mathbb{R}\right\}$. Then,

$$\begin{aligned}\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} s & 0 \\ 0 & t \end{bmatrix} &= \begin{bmatrix} as & bt \\ 0 & dt \end{bmatrix}\\ \begin{bmatrix} s & 0 \\ 0 & t \end{bmatrix}\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} &= \begin{bmatrix} sa & sb \\ 0 & td \end{bmatrix}.\end{aligned}$$

Therefore, I is a subring but not an ideal.

(6) Let $R = \mathbb{Z}[x]$. Consider $I = \langle 2, x \rangle = \{2f(x) + g(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}$. Then,

$$\begin{aligned}(2f_1(x) + xg(x))(2f_2(x) + xg_2(x)) &= 2\left(f_1(x)(2f_2(x) + xg_2(x))\right) + x(g_1(x)(2f_2(x) + xg_2(x)))\\ h(x)\left(2f(x) + xg(x)\right) &= 2(f(x)h(x)) + x(g(x)h(x)),\end{aligned}$$

meaning I is an ideal.

Examples of Quotient Rings

(1) Let $R = \mathbb{Z}$, $I = n\mathbb{Z}$. Then, $R/I = \mathbb{Z}/n\mathbb{Z}$.

(2) Let $R = \mathbb{R}[x]$, $I = \langle x^2 \rangle$ as defined earlier. Then,

$$\begin{aligned}R/I &= \mathbb{R}[x]/\langle x^2 \rangle\\ &= f(x) + \langle x^2 \rangle.\end{aligned}$$

Other examples include

$$\begin{aligned}
f(x) &= a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]\\
f(x) + \langle x^2\rangle &= a_1 x + a_0 + \langle x^2\rangle \in \mathbb{R}[x]/\langle x^2\rangle\\
\mathbb{R}[x]/\langle x^2\rangle &= \{a + bx + \langle x^2\rangle \mid a, b \in \mathbb{R}\}.\\
(a + bx + \langle x^2\rangle)(c + dx\langle x^2\rangle) &= ac + adx + bcx + bdx^2 + \langle x^2\rangle\\
&= (ac) + (ad + bc)x + \langle x^2\rangle\\
(x + \langle x^2\rangle)^2 &= x^2 + \langle x^2\rangle\\
&= \langle x^2\rangle.
\end{aligned}$$

(3) Let $R = \mathbb{Z}\times\mathbb{Z}$, $I = \{(2n, 0) \mid n \in \mathbb{Z}\}$. Then,

$$\begin{aligned}
R/I &= \{(a, b) + I \mid a, b \in \mathbb{Z}\}.\\
(a, b) + I &= ([a]_2, b) + I && \text{where } [a]_2 \text{ is } a \text{ modulo } 2.
\end{aligned}$$

We would expect that $\varphi : \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z} \to R/I$, $([a]_2, b) \to (a, b) + I$ is an isomorphism (verify for yourself).

Isomorphisms to Quotient Rings

Let $R = \mathbb{Z}[x]$, $I = \langle 2, x\rangle$, $J = \langle 2\rangle = \{2f(x) \mid f(x) \in \mathbb{Z}[x]\}$.

$$\begin{aligned}
R/J &= \{f(x) + \langle 2\rangle \mid f(x) \in \mathbb{Z}[x]\}\\
f(x) + \langle 2\rangle &= g(x) + \langle 2\rangle
\end{aligned}$$

if $2|(f(x) - g(x))$, meaning all coefficients of $f(x) - g(x)$ are divisible by 2. Therefore,

$$\begin{aligned}
f(x) + \langle 2\rangle &= 5 + 4x + 7x^2 - 5x^3\langle 2\rangle\\
&= (1 + (2)(2)) + 2(2x) + x^2 + 2(3x^2) - x^3 - 2(2x^3) + \langle 2\rangle\\
&= 1 + x^2 - x^3 + \langle 2\rangle\\
&= 1 + x^2 - 2(x^3) + x^3 + \langle 2\rangle\\
&= 1 + x^2 + x^3 + \langle 2\rangle.\\
(1 + x + x^2 + \langle 2\rangle) + (x + \langle 2\rangle) &= 1 + 2x + x^2 + \langle 2\rangle\\
&= 1 + x^2 + \langle 2\rangle.
\end{aligned}$$

Therefore, we can consider

$$\begin{aligned}
\mathbb{Z}[x]/\langle 2\rangle &= \mathbb{Z}[x]/2\mathbb{Z}[x]\\
&\cong \mathbb{Z}/2\mathbb{Z}.
\end{aligned}$$

$$\begin{aligned}
R/I &= \mathbb{Z}[x]/\langle 2, x\rangle\\
f(x) + \langle 2, x\rangle &= a_n x^n + \cdots + a_1 x + a_0 + \langle 2, x\rangle\\
&= a_0 + \langle 2, x\rangle\\
&= \begin{cases} 0 & 2|a_0\\ 1 & 2 \nmid a_0\end{cases},
\end{aligned}$$

So, we can consider

$$\mathbb{Z}[x]/\langle 2, x\rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

Isomorphism Example: Complex Numbers to Matrices

Consider the set

$$R = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathrm{Mat}_2(\mathbb{R}) \right\}.$$

We can verify that R is a ring.

Define

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

We can verify that φ is a bijective map.

Let $a + bi, c + di \in \mathbb{C}$. Then,

$$\begin{aligned} \varphi((a+bi) + (c+di)) &= \varphi((a+c) + (b+d)i) \\ &= \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \varphi(a+bi) + \varphi(c+di), \end{aligned}$$

and

$$\begin{aligned} \varphi((a+bi)(c+di)) &= \varphi((ac-bd) + (ad+bc)i) \\ &= \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} \\ \varphi(a+bi)\varphi(c+di) &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix}. \end{aligned}$$

Therefore, $\mathbb{C} \cong R$.

First Isomorphism Theorem

Let $\varphi : R \to S$ be a homomorphism. We have $R/\ker\varphi \cong \varphi(R)$.

Proof of the First Isomorphism Theorem

We want to show that $R/\ker(\varphi) \cong \varphi(R)$. Without loss of generality, assume φ is surjective. Let $K = \ker(\varphi)$.

We define $\Phi : R/K \to S$, $r + K \mapsto \varphi(r)$. We must show that Φ is a well-defined map. Let $r_1 + K = r_2 + K$ (meaning $r_1 - r_2 \in K$). This means $r_1 = r_2 + k$ for some $k \in K$. Applying Φ, we have

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

Let $r_1 + K,\ r_2 + K \in R/K$. Observe

$$\begin{aligned}\Phi((r_1 + K) + (r_2 + K)) &= \Phi((r_1 + r_2) + K)\\ &= \varphi(r_1 + r_2)\\ &= \varphi(r_1) + \varphi(r_2)\\ &= \Phi(r_1 + K) + \Phi(r_2 + K),\end{aligned}$$

and

$$\begin{aligned}\Phi((r_1 + K)(r_2 + K)) &= \Phi(r_1 r_2 + K)\\ &= \varphi(r_1 r_2)\\ &= \varphi(r_1)\varphi(r_2)\\ &= \Phi(r_1 + K)\Phi(r_2 + K),\end{aligned}$$

meaning Φ is a homomorphism.

Let $s \in S$. Since φ is surjective, there exists $r \in R$ with $\varphi(r) = s$. So, $\Phi(r + K) = \varphi(r) = s$. Thus, Φ is surjective.

Let $r + K \in \ker(\Phi)$. Then,

$$\begin{aligned}\Phi(r + k) &= 0_S\\ &= \varphi(r),\end{aligned}$$

meaning $r \in \ker(\varphi) = K$. So, $r + K = 0_R + K = 0_{R/K}$. Thus, Φ is injective.

Using the First Isomorphism Theorem: Example 1

Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}/2\mathbb{Z}$, $a_0 + a_1 x + \cdots + a_n x^n \mapsto [a_0]_2$.

To apply the first isomorphism theorem, we must check that this is a ring homomorphism. Let

$$\begin{aligned}f &= a_0 + a_1 x + \cdots + a_m x^m\\ g &= b_0 + b_1 x + \cdots + b_m x^m\end{aligned}$$

be elements in $\mathbb{Z}[x]$. Note that

$$\begin{aligned}\varphi(f + g) &= \varphi((a_0 + b_0) + \cdots)\\ &= [a_0 + b_0]_2\\ &= [a_0]_2 + [b_0]_2\\ &= \varphi(f) + \varphi(g)\end{aligned}$$

and

$$\begin{aligned}\varphi(fg) &= \varphi((a_0 b_0) + \cdots)\\ &= [a_0 b_0]_2\\ &= [a_0]_2 + [b_0]_2\\ &= \varphi(f)\varphi(g).\end{aligned}$$

So φ is a homomorphism. Note that $\varphi(0) = [0]_2$ and $\varphi(1) = [1]_2$. The first isomorphism theorem gives that $\mathbb{Z}[x]/\ker\varphi \cong \mathbb{Z}/2\mathbb{Z}$.

We claim that $\ker\varphi = \langle 2, x\rangle$.

If $2f(x) + xg(x) \in \langle 2, x\rangle$, and we write $f(x) = a_0 + a_1x + \cdots + a_nx^n$, then

$$\begin{aligned}\varphi(2f(x) + g(x)) &= \varphi(2)\varphi(f(x)) + \varphi(x)\varphi(g(x))\\ &= [0]_2[a_0]_2 + [0]_2\varphi(g(x))\\ &= [0]_2,\end{aligned}$$

so $\langle 2, x\rangle \subseteq \ker\varphi$.

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \ker(\varphi)$, meaning

$$\begin{aligned}[0]_2 &= \varphi(f(x))\\ &= [a_0]_2.\end{aligned}$$

Therefore, $a_0 = 2k$. So,

$$\begin{aligned}f(x) &= 2kx(a_1 + a_2x + \cdots + a_nx^{n-1})\\ &\in \langle 2, x\rangle.\end{aligned}$$

Thus, $\ker(\varphi) \subseteq \langle 2, x\rangle$, meaning $\ker(\varphi) = \langle 2, x\rangle$.

By the first isomorphism theorem, $\mathbb{Z}[x]/\langle 2, x\rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Using the First Isomorphism Theorem: Example 2

We want to find the ring that is isomorphic to $(\mathbb{Z}\times\mathbb{Z})/(2\mathbb{Z}\times 5\mathbb{Z})$. We define

$$\begin{aligned}\varphi : \mathbb{Z}\times\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}\\ (m, n) &\mapsto ([m]_2, [n]_5).\end{aligned}$$

We will start by showing homomorphism as follows:

$$\begin{aligned}\varphi((m_1, n_1) + (m_2, n_2)) &= \varphi((m_1 + m_2, n_1 + n_2))\\ &= ([m_1 + m_2]_2, [n_1 + n_2]_5)\\ &= ([m_1]_2 + [m_2]_2, [n_1]_5 + [n_2]_5)\\ &= ([m_1]_2, [n_1]_5) + ([m_2]_2, [n_2]_5)\\ &= \varphi((m_1, n_1)) + \varphi((m_2, n_2)),\end{aligned}$$

and similarly for multiplication

$$\begin{aligned}\varphi((m_1, n_1)(m_2, n_2)) &= \varphi((m_1m_2, n_1n_2))\\ &= ([m_1m_2]_2, [n_1n_2]_5)\\ &\vdots\\ &= \varphi((m_1, n_1))\varphi((m_2, n_2))\end{aligned}$$

Let $([a]_2, [b]_5) \in \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$. Then, $\varphi((a, b)) = ([a]_2, [b]_5)$. Thus, φ is surjective.

Finally, we have $(m, n) \in \ker(\varphi)$ if and only if $[m]_2 = [0]_2$ and $[n]_5 = [0]_5$, meaning $m \in 2\mathbb{Z}$ and $n \in 5\mathbb{Z}$. Therefore, $\ker(\varphi) = 2\mathbb{Z}\times 5\mathbb{Z}$.

Using the First Isomorphism Theorem: Example 3

Consider the map $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $n \mapsto ([n]_2, [n]_5)$. Note

$$\begin{aligned}\varphi(m+n) &= ([m+n]_2, [m+n]_5)\\ &= ([m]_2 + [n]_2, [m]_5 + [n]_5)\\ &= ([m]_2, [m]_5) + ([n]_2, [n]_5)\\ &= \varphi(m) + \varphi(n),\end{aligned}$$

and

$$\varphi(mn) = \varphi(m)\varphi(n).$$

We want to find if this map is surjective. Let $([a]_2, [b]_5) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. We are trying to find $n \in \mathbb{Z}$ such that $[n]_2 = [a]_2$ and $[n]_5 = [b]_5$, or $n \equiv a$ modulo 2 and $n \equiv b$ modulo 5.

$$\begin{aligned}n - a &\equiv 2k \text{ for some } k \in \mathbb{Z}\\ n &\equiv a + 2k\\ a + 2k &\equiv b \text{ modulo } 5\\ 2k &= b - a \text{ modulo } 5\\ k &= 3(b-a) \text{ modulo } 5\\ n &= a + 2(3(b-a))\\ &= a + 6(b-a).\end{aligned}$$

So $\varphi(a + 6(b-a)) = ([a]_2, [b]_5)$. Thus, φ is surjective.

Finally, we desire $\ker(\varphi)$. Observe that

$$\begin{aligned}\ker(\varphi) &= \{n \in \mathbb{Z} \mid [n]_2 = [0]_2, [n]_5 = [0]_5\}\\ &= \{n \in \mathbb{Z} \mid 2|n, 5|n\}\\ &= \{n \in \mathbb{Z} \mid 10|n\}\\ &= 10\mathbb{Z}.\end{aligned}$$

Thus, the first isomorphism theorem gives $\mathbb{Z}/10\mathbb{Z} \equiv \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Proposition: Ring Homomorphisms and Ideals

Let R be a ring and $I \subseteq R$ be an ideal. The map

$$\begin{aligned}\varphi : R &\to R/I\\ r &\mapsto r + I\end{aligned}$$

is a surjective ring homomorphism with $\ker(\varphi) = I$. The proof is left as an exercise to the reader.

Using the First Isomorphism Theorem: Example 3

Let A be a ring and X be any non-empty set. Let R be the set of functions from X to A.

We have R is a ring.

$$\begin{aligned}(f+g)(x) &= f(x) +_A g(x)\\ (fg)(x) &= f(x) \cdot_A g(x).\end{aligned}$$

Fix $x_0 \in X$. We define $E_{x_0} : R \to A$ by

$$E_{x_0}(f) = f(x_0).$$

We have

$$\begin{aligned} E_{x_0}(f+g) &= (f+g)(x_0) \\ &= f(x_0) + g(x_0) \\ &= E_{x_0}(f) + E_{x_0}(g) \end{aligned}$$

and

$$\begin{aligned} E(x_0)(fg) &= (fg)(x_0) \\ &= f(x_0)g(x_0) \\ &= E_{x_0}(f)E_{x_0}(g). \end{aligned}$$

Therefore, E_{x_0} is a homomorphism. Additionally, E_{x_0} is surjective, since we can find $f_a : X \to A$, $x \mapsto a$, meaning $E_{x_0}(f_a) = f_a(x_0) = a$.

If $f \in \ker(E_{x_0})$, then $E_{x_0}(f) = 0_A$. However, $E_{x_0}(f) = f(x_0)$. Then,

$$\begin{aligned} \ker(\varphi) &= \{f : X \to A \mid f(x_0) = 0_A\} \\ &= \mathcal{M}_{x_0}. \end{aligned}$$

By the first isomorphism theorem, we can see that $R/\mathcal{M}_{x_0} \cong A$.

Other Isomorphism Theorems

Let R be a ring.

Diamond Isomorphism Theorem: Let A be a subring of R and I an ideal of R. Define $A + I = \{a + i \mid a \in A, i \in I\}$. This is an ideal of R. We also have that $A \cap I$ is an ideal in A, and $(A + I)/I \equiv A/A \cap I$.

$$\begin{tikzcd} & A+I & \\ I \arrow[ur, "\simeq"] & & A \arrow[ul] \\ & A \cap I \arrow[ul] \arrow[ur, "\simeq"'] & \end{tikzcd}$$

Third Isomorphism Theorem: Let I, J be ideals of R with $I \subseteq J$. Then, J/I is an ideal of R/I with $(R/I)/(J/I) \cong R/J$.

Lattice Isomorphism Theorem: Let $I \subseteq R$ be an ideal. The correspondence $A \leftrightarrow A/I$ is an inclusion-preserving bijection between the subrings A of R that contain I and the subrings of R/I. Moreover, A is an ideal if and only if A/I is an ideal.

Using the Third Isomorphism Theorem

Let $R = \mathbb{Z}$, $I = 12\mathbb{Z}$, and $J = 4\mathbb{Z}$. By the third isomorphism theorem, $J/I = 4\mathbb{Z}/12\mathbb{Z}$ is an ideal of $R/I = \mathbb{Z}/12\mathbb{Z}$, and

$$\begin{aligned} (R/I)/(J/I) &= (\mathbb{Z}/12\mathbb{Z})/(4\mathbb{Z}/12\mathbb{Z}) \\ &\cong \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

Applying the Isomorphism Theorems

Consider the rings $3\mathbb{Z}$ and $12\mathbb{Z}$. We have that $12\mathbb{Z} \subseteq 3\mathbb{Z}$ as an ideal. Therefore, we can form the quotient ring $3\mathbb{Z}/12\mathbb{Z}$. We might ask how it's related to other $\mathbb{Z}/n\mathbb{Z}$, or to $\mathbb{Z}/12\mathbb{Z}$.

Note that $3\mathbb{Z}/12\mathbb{Z}$ starts with elements in $3\mathbb{Z}$ and examines elements in $12\mathbb{Z}$. We might ask whether or not $3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$. However,

$$\begin{aligned} 3\mathbb{Z}/12\mathbb{Z} &= \{a + 12\mathbb{Z} \mid a \in 3\mathbb{Z}\} \\ &= \{3b + 12\mathbb{Z} \mid b \in \mathbb{Z}\}. \end{aligned}$$

We can define

$$\begin{aligned} \varphi : 3\mathbb{Z} &\to \mathbb{Z}/4\mathbb{Z} \\ 0 + 12\mathbb{Z} &\mapsto [0]_4, \\ 3 + 12\mathbb{Z} &\mapsto [3]_4, \\ 6 + 12\mathbb{Z} &\mapsto [2]_4, \\ 9 + 12\mathbb{Z} &\mapsto [1]_4. \end{aligned}$$

which we look at by aiming for $12\mathbb{Z}$ to be the kernel of φ. Then, by the first isomorphism theorem, $3\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z}$.

If we want to examine $3\mathbb{Z}/12\mathbb{Z}$ in relation to $\mathbb{Z}/12\mathbb{Z}$, we see that $3\mathbb{Z}/12\mathbb{Z} \cong \langle [3]_{12} \rangle \subseteq \mathbb{Z}/12\mathbb{Z}$.

Generated Ideals

Let $I, J \subseteq R$ be ideals. We define

(1) the sum, $I + J = \{i + j \mid i \in I, j \in J\}$,

(2) the product, IJ, the collection of finite sums of elements of the form xy, where $x \in I$ and $y \in J$, and

(3) The nth power of I, denoted I^n, which is the collection of finite sums of elements of the form $x_1, \dots, x_n \in I$.

Exercises:

(1) $I + J$ is the smallest ideal containing I and J.

(2) $IJ \subseteq I \cap J$.

Let R be a ring with $1_R \neq 0_R$. Let $A \subseteq R$.

(1) Let $\langle A \rangle$ be the smallest ideal that contains A. It is called the ideal *generated* by A.

(2) We set $RA = \{r_1 a_1 + \cdots + r_n a_n \mid r_i \in R, a_i \in A\}$ for any $n \in \mathbb{Z}_{\geq 0}$. Additionally, AR is analogous to RA. We set $RAR = \{r_1 a_1 \tilde{r}_1 + \cdots + r_n a_n \tilde{r}_n \mid r_i, \tilde{r}_i \in R, a_i \in A\}$.

(3) If A is a single element a, we write $\langle a \rangle$ to denote the ideal generated by A and refer to this as a principal ideal. If A is finite, then we say $\langle A \rangle$ is a finitely generated ideal.

For example, if $R = \mathbb{Z}[x_1, x_2, \dots]$, then $I = \langle x_1, x_2, \dots \rangle$ is not finitely generated.

Note: If R is commutative, then $\langle a \rangle = Ra$ and if R is not commutative, $\langle a \rangle = RaR$. For R commutative, we say that for $b \in \langle a \rangle$, $b = ra$ for some $r \in R$. We say a divides b — if a divides b, then $\langle b \rangle \subseteq \langle a \rangle$.

Principal Ideal: Example 1

Every ideal in $\mathbb{Z}$ is a principal ideal.

Let $I \subseteq \mathbb{Z}$ be a nonzero ideal (the zero ideal is generated by 0). Let $m \in I, m \neq 0$. Since I is an ideal, if $m \in I$, so too is $-m \in I$. Therefore, we know there is a positive integer in I.

By the well-ordering principle, let $n \in I$ be the smallest positive integer in I. Let $a \in I$, $a \neq 0$. Write $a = nq + r$ for $q, r \in \mathbb{Z}$, and $0 \leq r < n$. Then, we have $r = a - nq$. Since $a \in I$ and $n \in I$, $r \in I$. Therefore, $r = 0$, and $n|a$. Thus, $I = n\mathbb{Z}$.

Principal Ideal: Example 2

Let $R = \mathbb{Z}[x]$. Consider $I = \langle 2, x\rangle$. We claim that I is not a principal ideal.

Suppose toward contradiction that $\langle 2, x\rangle = \langle f(x)\rangle$ for some $f(x) \in \mathbb{Z}[x]$. Therefore, $2 = f(x)g(x)$ for some $g(x) \in \mathbb{Z}[x]$. Since degrees add, $\deg(2) = \deg(f) + \deg(g)$, or $0 = f(x)g(x)$. Therefore, $f(x), g(x) \in \mathbb{Z}$. Therefore, we must have that $f(x) \in \{\pm 1, \pm 2\}$.

So, we have elements of $\langle 2, x\rangle$ of the form $2s(x) + xt(x)$. So we have constant term divisible by 2, meaning $f(x) \neq \pm 1$, so $f(x) = \pm 2$.

Then, $x = 2h(x)$ for some $h(x) \in \mathbb{Z}[x]$. However, we have that $h(x)$ has integer coefficients. Therefore, $\langle 2, x\rangle \neq \langle f(x)\rangle$ for any $f(x) \in \mathbb{Z}[x]$.

Proposition: Ideals in Unital Rings

Let I be an ideal of R.

(1) $I = R$ if and only if I contains a unit.

(2) If R is commutative, then R is a field if and only if the only ideals in R are $\langle 0_R\rangle$ and R.

Proof of (1): Suppose $I = R$. Then, $1_R \in I$, and 1_R is a unit.

Suppose I contains a unit, u. Then, we have $u^{-1} \in R$. Since I is an ideal, we have $uu^{-1} \in I$, and $uu^{-1} = 1_R$. Letting $r \in R$, using the fact that I is an ideal, $(r)(1_R) = r \in I$. Thus, $I = R$.

Proof of (2): Suppose R is a field. Let I be any nonzero ideal. Every nonzero element in I is a unit, meaning $I = R$.

Suppose $\langle 0_R\rangle$ and R are the only ideals in R. Let $r \in R$, $r \neq 0_R$. Since $r \neq 0$, $\langle r\rangle = R$. Thus, $1_R \in \langle r\rangle$. Thus, $1_R = sr$ for some $s \in R$, implying every nonzero element of R has an inverse.

Corollary: Field Homomorphisms

Let F be a field, and $\varphi : F \to R$ be a homomorphism. Then, φ is either the zero map ($\varphi(f) = 0_R$) or φ is injective.

Proof: Since $\ker(\varphi)$ is an ideal in F by the first isomorphism theorem, then $\ker(\varphi) = \langle 0_F\rangle$ or $\ker(\varphi) = R$. If $\ker(\varphi) = \langle 0_F\rangle$, then φ is injective, and if $\ker(\varphi) = F$, then φ is the zero map.

Maximal Ideals

(1) An ideal $\mathcal{M} \subseteq R$ is a maximal ideal if $\mathcal{M} \neq R$ and the only ideals containing $\mathcal{M}$ are $\mathcal{M}$ and R. The collection of maximal ideals is denoted m-spec(R) or maxspec(R).

(2) An ideal $\mathfrak{p} \subseteq R$ with $\mathfrak{p} \neq R$ is a prime ideal if whenever $ab \in \mathfrak{p}$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. We denote the collection of prime ideals Spec(R).

For example, $\text{Spec}(\mathbb{Z}) = \{0\mathbb{Z}, p\mathbb{Z}\}$ for p prime, and $\text{maxspec}(\mathbb{Z}) = \{p\mathbb{Z}\}$.

Aside: Let R be commutative. The set Spec(R) is a topological space. Let $A \subseteq R$ be any subset. Closed sets look like

$$\begin{aligned} V(A) &= \{\mathcal{P} \in \text{Spec}(R) \mid A \subset \mathcal{P}\} \\ &= V(I) \\ &= \langle A \rangle \end{aligned}$$

For example, if $R = \mathbb{R}[x, y]$, if $f(x, y) = y - x^2$, then $V(f) = \{(a, b) \in \mathbb{R}^2 \mid f(a, b) = 0\}$. The topology on Spec$(R)$ is called the Zariski topology.

Let $\varphi : R \to S$ be a ring homomorphism. If $\mathcal{P} \in \text{Spec}(S)$, then $\varphi^{-1}(\mathcal{P})$ is a prime ideal in R. We get a map $\varphi^*(\text{Spec}(S)) \to \text{Spec}(R)$ given by $\mathcal{P} \to \varphi^{-1}(\mathcal{P})$.

We get a contravariant functor that takes $R \mapsto \text{Spec}(R)$, mapping from the category of rings to the category of topological spaces.

Proposition: Existence of Maximal Ideals

Let R be a ring. Every proper ideal is contained in a maximal ideal.

Let I be a proper ideal. Let $\mathcal{S}$ be the collection of all proper ideals that contain I. We know that $\mathcal{S}$ is non-empty as $I \in \mathcal{S}$. Then, $\mathcal{S}$ has a partial ordering under inclusion.

Let $\mathcal{C}$ be a chain of ideals (that is, totally ordered subset) in $\mathcal{S}$, and

$$J = \bigcup_{A \in \mathcal{C}} A.$$

Since $\mathcal{C} \neq \emptyset$, there is at least one A in the union with $0_R \in A$. So, $J \neq \emptyset$. Let $a, b \in J$. There exists A with $a \in A$ and b with $b \in B$. Since $\mathcal{C}$ is a chain, either $A \subseteq B$ or $B \subseteq A$. So, a and b are both in either A or B. Thus, $a - b$ and ab are in either A or B. Thus, $a - b$ and ab are elements in J, meaning J is an ideal.

If $J = R$, then $1_R \in J$, meaning 1_R is an element of some $A \in \mathcal{C}$. Since $A \in \mathcal{S}$ is a proper ideal, this would be a contradiction.

Therefore, J is an upper bound for $\mathcal{C}$. Since every chain in $\mathcal{S}$ has an upper bound in $\mathcal{S}$, then, by Zorn's Lemma, there is a maximal element in $\mathcal{S}$.

Proposition: Maximal Ideals, Quotient Rings, and Fields

An ideal $\mathcal{M} \subseteq R$ of a commutative ring with identity is maximal if and only if $R/\mathcal{M}$ is a field.

Suppose $\mathcal{M}$ is maximal. Let $x + \mathcal{M} \neq 0 + \mathcal{M}$. We want to show that $x + \mathcal{M}$ has an inverse.

Consider $\langle x, \mathcal{M}\rangle$, the ideal generated by x and $\mathcal{M}$. We have $\mathcal{M} \subset \langle x, \mathcal{M}\rangle$, as $x \notin \mathcal{M}$. Therefore, $\langle x, \mathcal{M}\rangle = R$ by the definition of a maximal ideal. Therefore, $1_R \in \langle x, \mathcal{M}\rangle$, meaning $1_R = xu + mv$ for some $u, v \in R$, $m \in \mathcal{M}$. Note

$$\begin{aligned}(x+\mathcal{M})(u+\mathcal{M}) &= xu + \mathcal{M}\\ &= (1_R - mv) + \mathcal{M}\\ &= 1_R + \mathcal{M},\end{aligned}$$

meaning $x + \mathcal{M}$ has an inverse, meaning $R/\mathcal{M}$ is a field.

Suppose $R/\mathcal{M}$ is a field. Assume we have $\mathcal{M} \subset I \subset R$ for some ideal I. From the third isomorphism theorem, we have $I/\mathcal{M}$ is an ideal of $R/\mathcal{M}$. Specifically, by our construction, $I/\mathcal{M}$ is a proper nonzero ideal of $R/\mathcal{M}$, but since $R/\mathcal{M}$ is a field, no such proper nonzero ideal exists, meaning no such I exists.

Examples: Maximal Ideals

(1) Let $R = \mathbb{Z}$. Given $m \in \mathbb{Z}$, we know $m\mathbb{Z}$ is a maximal ideal if and only if m is prime. If $p|m$ and $p \neq m$, then $m\mathbb{Z} \subseteq p\mathbb{Z}$. Additionally, if p is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field. Additionally, $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain if m is composite.

(2) Let $R = F[x]$ for F a field. Let $\alpha \in F$ and consider $\mathcal{M}_\alpha = \langle x - \alpha\rangle$. We claim that $F[x]/\mathcal{M}_\alpha \cong \mathcal{F}$, meaning $\mathcal{M}$ is a maximal ideal.

Let $\varphi : F[x] \to F$, $x \mapsto \alpha, f(x) \mapsto f(\alpha)$. Let $f(x), g(x) \in F[x]$. Then,

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

and

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

Let $\beta \in F$. Then,

$$\begin{aligned}\varphi(\beta + (x-\alpha)) &= \beta + (\alpha - \alpha)\\ &= \beta.\end{aligned}$$

Thus, φ is surjective. Finally, we have $f(x) \in \ker(\varphi)$ if and only if $f(\alpha) = 0$. However, $f(\alpha) = 0$ if and only if $(x - \alpha)|f(x)$. Therefore, $\ker(\varphi) = \langle x - \alpha\rangle$.

(3) Let $R = \mathbb{Z}[x]$. Let $\mathcal{M} = \langle 2, x\rangle$. We saw that $\mathbb{Z}[x]/\langle 2, x\rangle \cong \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Therefore, we know that $\mathcal{M}$ is a maximal ideal by the above categorization.

(4) Let $R = \mathbb{F}_2[x]$. Consider the ideal $\mathcal{M} = \langle x^2 + x + 1\rangle$.

$$\begin{aligned}R/\mathcal{M} &= \left\{f(x) + \langle x^2+x+1\rangle \mid f(x) \in \mathbb{F}_2[x]\right\}\\ f(x) &= \left\{(x^2+x+1)q(x) + r(x) \mid q(x), r(x) \in \mathbb{F}_2[x],\ r(x) = 0 \text{ or } \deg r(x) < 2\right\}.\end{aligned}$$

So,

$$f(x) + \mathcal{M} = r(x) + \mathcal{M},$$

meaning

$$R\mathcal{M} = \{0+\mathcal{M}, 1+\mathcal{M}, x+\mathcal{M}, 1+x+\mathcal{M}\}.$$

This is a field.

$+$	$0+\mathcal{M}$	$1+\mathcal{M}$	$x+\mathcal{M}$	$x+1+\mathcal{M}$
$0+\mathcal{M}$	0	1	x	$x+1$
$1+\mathcal{M}$	1	0	$1+x$	x
$x+\mathcal{M}$	x	$1+x$	0	1
$x+1+\mathcal{M}$	$1+x$	x	1	0

$\times$	$0+\mathcal{M}$	$1+\mathcal{M}$	$x+\mathcal{M}$	$x+1+\mathcal{M}$
$0+\mathcal{M}$	0	0	0	0
$1+\mathcal{M}$	0	1	x	$x+1$
$x+\mathcal{M}$	0	x	$1+x$	1
$x+1+\mathcal{M}$	0	$1+x$	x	1

Specifically, this is a field of order 4. Note that $\mathbb{F}_2 \hookrightarrow R/\mathcal{M}$. We say $R/\mathcal{M} \cong \mathbb{F}_4$.

Note: For every p prime and every $n \in \mathbb{Z}$ positive, there is exactly one field of order p^n up to isomorphism.

(5) Let $R = \mathbb{Z}[i]$. Set $\mathcal{M} = \langle 3 \rangle$. This is a maximal ideal, and $|\mathbb{Z}[i]/\langle 3\rangle| = 9$.

Proposition: Prime Ideals, Quotient Rings, and Integral Domains

Let R be a commutative ring with identity. An ideal $\mathfrak{p} \subseteq R$ is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain.

Let $\mathfrak{p} \subseteq R$ be a prime ideal. Let $x, y \in R$ with $(x+\mathfrak{p})(y+\mathfrak{p}) = 0+\mathfrak{p}$. We have

$$xy + \mathfrak{p} = 0 + \mathfrak{p}$$

meaning

$$xy \in \mathfrak{p},$$

so, since $\mathfrak{p}$ is prime,

$$x \in \mathfrak{p}$$

or

$$y \in \mathfrak{p}$$

so $x + \mathfrak{p} = 0 + \mathfrak{p}$ or $y + \mathfrak{p} = 0\mathfrak{p}$.

In the reverse direction, assume $R/\mathfrak{p}$ is an integral domain. Let $xy \in \mathfrak{p}$. Then,

$$\begin{aligned}(x+\mathfrak{p})(y+\mathfrak{p}) &= xy + \mathfrak{p}\\ &= 0 + \mathfrak{p},\end{aligned}$$

implying that $x+\mathfrak{p}$ or $y+\mathfrak{p}$ is equal to $0+\mathfrak{p}$, or $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

Examples: Prime Ideals

(1) If $R = \mathbb{Z}[x]$, then $\mathfrak{p} = \langle x \rangle$ is a prime ideal that is not a maximal ideal, as $\mathbb{Z}[x]/\langle x \rangle \cong \mathbb{Z}$.

Corollary: Maximal Ideals and Prime Ideals

Let R be a commutative ring with identity. Then, $\operatorname{maxspec}(R) \subseteq \operatorname{Spec}(R)$.