# Math 103B

Modern Algebra: Rings and Fields

Winter 2022

Taught by Professor Brandon Alberts

# Table of Contents

# 1 Rings (Chapter 12)

Recall that a group is a set equipped with a binary operation. However, often times, a lot of sets are naturally endowed with *two* binary operations: addition *and* multiplication. In this case, we want to account for *both* of them at the same time instead of having two groups with the same sets but different operations. To that, we introduce the *ring*.

**Definition 1.1: Ring**

A ring $R$ is a set with two *binary operations* (meaning closed operations), addition (denoted by $a+b$) and multiplication (denoted by $ab$), such that for all $a, b, c \in R$:

1. **Commutative:** $a + b = b + a$
2. **Associative:** $(a + b) + c = a + (b + c)$
3. **Additive Identity:** There is an additive identity $0 \in R$ such that $a + 0 = 0 + a = a$ for all $a \in R$.
4. **Additive Inverse:** There is an element $-a \in R$ such that $a + (-a) = (-a) + a = 0$.
5. **Associative:** $a(bc) = (ab)c$.
6. **Distributive Property:** $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

We sometimes write this ring out as $(R, +, \cdot)$.

**Remarks:**

- A ring is an abelian group under addition, but also has an associative multiplication that is *left and right distributive* over addition.
- If $a$ and $b$ belong to a commutative ring $R$ and $a$ is nonzero, then we say that $a$ *divides* $b$ (or that $a$ is a factor of $b$) and write $a|b$ if there exists $c \in R$ such that $b = ac$. If $a$ does not divide $b$, we write $a \nmid b$.
- If we need to deal with something like:
$$\underbrace{a + a + \cdots + a}_{n \text{ times}}$$
Then, we will use $n \cdot a$ to mean this.

## 1.1 Basic Applications of the Ring

Here, we introduce several examples of rings.

### 1.1.1 Example 1: Integer Rings

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

The set of integers under ordinary addition and multiplication is a commutative ring with unity 1. The *units* of $\mathbb{Z}$ are 1 and -1.

### 1.1.2 Example 2: Integers Mod N

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$$

The set of integers modulo $n$ under addition and multiplication is also a commutative ring with unity 1. The set of *units* is $U(n)$. Here, we define $U(n)$ to be the set of integers less than $n$ and relatively prime to $n$ under multiplication modulo $n$.

This can also be written as $\mathbb{Z}_n$.

#### 1.1.3 Example 3: Polynomial Rings

The set $\mathbb{Z}[x]$ of all polynomials in the variable $x$ with integer coefficients under ordinary addition and multiplication is a commutative ring with unity $f(x) = 1$. Here, we define:

$$\mathbb{Z}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{Z}\}$$

So, for example, $x^2 + 4x + 5 \in \mathbb{Z}[x]$.

#### 1.1.4 Example 4: Matrix Rings

The set $M_2(\mathbb{Z})$ of $2 \times 2$ matrices with integer entries is a *noncommutative ring* with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

#### 1.1.5 Example 5: Even Integer Rings

The set $2\mathbb{Z}$ of even integers under ordinary addition and multiplication is a commutative ring without unity.

#### 1.1.6 Example 6: Direct Sum

If $R_1, R_2, \ldots, R_n$ are rings, then we can create a new ring:

$$R_1 \oplus R_2 \oplus \cdots \oplus R_3 = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R_i\}$$

From this, we can perform componentwise addition and multiplication; that is:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n)$$

### 1.2 More on Rings

**Definition 1.2: Commutative Ring**

A ring $R$ is **commutative** if $ab = ba$ for all $a, b \in R$.

**Remark:** In other words, multiplication in a ring does **not** have to be commutative. However, *if* it is commutative, we say that the ring is commutative.

**Definition 1.3: Unity**

A ring $R$ has **unity** if $1 \in R$ is a multiplicative identity:

$$1a = a1 = a$$

**Remark:** A ring *does not need to have* an identity under multiplication. If a ring does have a non-zero identity under multiplication, then we say that the identity is a *unity*.

**Definition 1.4: Unit**

An element $a \in R$ is called a **unit** if it has a multiplicative inverse. In other words, $a$ is a unit if there exists an $a^{-1} \in R$ such that:

$$a^{-1}a = aa^{-1} = 1$$

**Remarks:**

- A nonzero element of a commutative ring with unity need not have a multiplicative inverse. When it does, we say that it is a unit of the ring. In other words, $a$ is a unit if $a^{-1}$ exists.

- $U(R) = \{\text{Units in } R\}$
- $U(n) = \{\text{Units in } \mathbb{Z}/n\mathbb{Z}\}$

**Definition 1.5: Division**

For $a, b \in R$, we say that $a$ **divides** $b$ and write $a|b$ if $b = ac$ for some $c \in R$.

## 1.3 Properties of Rings

We begin by talking about a few important properties.

### 1.3.1 Basic Rules of Multiplication

**Theorem 1.1**

For all $a \in R$, we have:

$$a0 = 0a = 0$$

*Proof.* We know that:

$$0a = (0 + 0)a = 0a + 0a$$

Subtracting both sides by $0a$ gives:

$$0 = 0a + (0a - 0a) \implies 0 = 0a$$

By symmetry, we can do the same for $0a$. Therefore, we are done. □

**Theorem 1.2**

For all $a, b \in R$, we have:

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

*Proof.* First, we have:

$$a(-b) + ab = a(-b + b) = a0 = 0$$

Now, if we add $-(ab)$ to both sides, we have:

$$a(-b) + ab + -(ab) = -(ab) \implies a(-b) = -(ab)$$

By symmetry, $(-a)b = -(ab)$ as well. □

**Theorem 1.3**

For all $a, b \in R$, we have:

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

*Proof.* Note that:

$$\begin{aligned}(-a)0 = 0 \\ \iff (-a)(b+(-b)) = 0 \\ \iff (-a)b + -a(-b) = 0 \\ \iff -(ab) + -a(-b) = 0 \\ \iff ab + -(ab) + -a(-b) = ab \\ \iff -a(-b) = ab\end{aligned}$$

So, we are done. □

**Theorem 1.4**

For all $a, b, c \in R$, we have:

$$a(b-c) = ab - ac \text{ and } (b-c)a = ba - ca$$

*Proof.*

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

By symmetry, we can apply the other side as well. So, we are done. □

### 1.3.2 Rules of Multiplication with Unity Element

**Theorem 1.5**

For all $a \in R$ where $R$ has a unity element 1, we have:

$$(-1)a = -a$$

*Proof.* Applying the theorem that we proved:

$$(-1)a = -(1a) = -a$$

So, we are done. □

Alternatively:

*Proof.* Since $(\mathbb{R}, +)$ is an abelian group, it suffices to prove that $(-1)a + a = 0$.

$$(-1)a + a = (-1)a + 1a = (-1+1)a = 0a = 0$$

So, we are done. □

**Theorem 1.6**

$$(-1)(-1) = 1$$

*Proof.* Applying the theorem that we proved:

$$(-1)(-1) = 1(1) = 1$$

So, we are done. □

### 1.3.3 Uniqueness of Unity and Inverses

**Theorem 1.7**

If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is also unique.

*Proof.* We will prove both parts individually. Suppose $R$ is a ring.

1. Suppose $e$ and $e'$ are unity elements in a ring $R$. Then, we know that:
   - $e = ee'$ since $e'$ is a unity.
   - $e' = ee'$ since $e$ is a unity.

   Therefore:
   $$e = ee' = e'$$
   Which means that the unity must be unique.
2. Suppose $a \in R$ and further suppose that $x$ and $y$ are both multiplicative inverses of $a$. Then:
   $$x = x1 = x(ay) = (xa)y = 1y = y$$
   Therefore, $x = y$ and the two inverses are equal.

Therefore, we are done. □

**Important Note 1.1**

Rings are not groups under multiplication. $R - \{0\}$ is not a group under multiplication. Rings may not have multiplicative cancellations.

To show that this is the case, consider the question: Which elements $a \in R$ satisfy $a^2 = a$?

- If $R$ has unity, then $a = 1$.
- $a = 0$ is always a solution.

Now, consider $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$. Then, $a^2 = a$ for $a = 0, 1, 3, 4$. The only units in this ring are 1 and 5.

# 2 Subrings (Chapter 12)

Recall that, with groups, we have objects called *subgroups*. The same thing applies here: with rings, we have objects called *subrings*.

**Definition 2.1: Subring**

A nonempty subset $S$ of a ring $R$ is a **subring** of $R$ if $S$ itself is a ring with the operations of $R$.

**Remark:** If $R$ is commutative, then $S$ is commutative.

## 2.1 Examples of Subrings

Below are some examples of subrings.

### 2.1.1 Example 1: Simple Subrings

The trivial subring $\{0\}$ is a subring of any ring $R$. This is because:

$$0(0) \in R \qquad 0 - 0 \in R$$

Any ring $R$ is a subring of itself. This is because for any $a, b \in R$, we know that $a - b = a + (-b) \in R$ and $ab \in R$.

### 2.1.2 Example 2: Integers

For any positive integer $n$, the set below is a subring of the integers $\mathbb{Z}$:

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$$

Take any $a, b \in \mathbb{Z}$. Then, suppose we have $an$ and $bn$. We know that:

$$an - bn = (a - b)n \in \mathbb{Z}$$

$$an(bn) = anbn$$

Since $anb \in \mathbb{Z}$, it follows that $(anb)n \in n\mathbb{Z}$.

### 2.1.3 Example 3: Rational Numbers

The ring $\mathbb{Q}$ is a subring of $\mathbb{R}$.

### 2.1.4 Example 4: Gaussian Integers

Consider the Gaussian integers:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

This is a subring of $\mathbb{C}$. Note that $i^2 = -1$ so:

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = ac + adi + bci - bd = (ac - bd) + (ad + bc)i$$

### 2.1.5 Example 5: Integers with Square Root 2

Consider the following set:

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

This is a subring of $\mathbb{R}$. This is because:

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

Note that we can apply the same work used in the previous example.

### 2.1.6 Example 6: Diagonal Matrices

The set of diagonal matrices is a subring of $M_2(\mathbb{Z})$.

$$\left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \mid a, d \in \mathbb{Z} \right\}$$

## 2.2 Subring Test

**Theorem 2.1: Subring Test**

A nonempty subset $S$ of a ring $R$ is a subring if $S$ is closed under subtraction and multiplication; that is, if $a - b \in S$ and $ab \in S$ whenever $a, b \in S$.

*Proof.* If $S$ is a subring, then it is a ring and so $S$ must be closed under subtraction and multiplication.

Suppose $S$ is closed under subtraction and multiplication. Then, we know the following properties (inherited from $R$):

- $a + b = b + a$
- $(a + b) + c = a + (b + c)$
- $a(bc) = (ab)c$
- $a(b + c) = ab + ac$
- $(a + b)c = ac + bc$

We need to check if $S$ has 0. Since $S$ is not empty, pick some $a \in S$. Then, it follows that:

$$a - a = 0 \in S$$

So, the additive identity exists. Now, if $a \in S$, then $-a = 0 - a \in S$, so additive inverses exist.

Finally, we need to show that addition is closed. We know that subtraction is closed, so if $a, b \in S$, then $-b \in S$ and $a + b = a - (-b) \in S$. □

# 3 Integral Domains (Chapter 13)

Recall that rings do not have multiplicative cancellation. That is, $ab = ac$ does not imply that $b = c$. However, there are exceptions to this rule.

## 3.1 Zero-Divisors

First, we briefly talk about zero-divisors.

**Definition 3.1: Zero-Divisors**

A **zero-divisor** is a nonzero element $a$ of a commutative ring $R$ such that there is a nonzero element $b \in R$ with $ab = 0$.

For example, $2 \in \mathbb{Z}/4\mathbb{Z}$ is a zero divisor. That is:

$$2 \cdot 2 \equiv 0 \pmod 4$$

Another example is $M_2(\mathbb{R})$. Take $A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$. Then:

$$A \cdot B = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

## 3.2 Integral Domains

Now, we talk about integral domains.

**Definition 3.2: Integral Domain**

An **integral domain** is a commutative ring with unity and no zero-divisors.

**Remarks:**

- Recall that a ring $R$ has **unity** if $1 \in R$ is a multiplicative identity; that is, $1a = a1 = a$.
- Essentially, in an integral domain, a product is 0 only when one of the factors is 0. That is, $ab = 0$ only when $a = 0$ or $b = 0$.

## 3.3 Examples of Integral Domains

Here are some examples of integral domains.

### 3.3.1 Example 1: The Integers

The ring of integers is an integral domain.

### 3.3.2 Example 2: Gaussian Integers

The ring of Gaussian integers $Z[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ is an integral domain.

### 3.3.3 Example 3: Ring of Polynomials

The ring $\mathbb{Z}[x]$ of polynomials with integer coefficients is an integral domain.

### 3.3.4 Example 4: Square Root 2

The ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain.

#### 3.3.5 Example 5: Modulo Prime Integers

The ring $\mathbb{Z}/p\mathbb{Z}$ of integers modulo $a$ prime $p$ is an integral domain. This is because:

$$ab \equiv 0 \pmod{p} \iff p|ab \implies p|a \text{ or } p|b \implies a \equiv 0 \pmod{p} \text{ or } b \equiv 0 \pmod{p}$$

#### 3.3.6 Non-Example 1: Modulo Integers

The ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo $n$ is not an integral domain when $n$ is not prime. If we write $n = ab$, then $1 < a$ and $b < n$ implies that $ab \equiv 0 \pmod{b}$. We saw an example of this in the zero-divisors section; that is, $\mathbb{Z}/4\mathbb{Z}$ is not an integral domain because we had $2 \cdot 2 \equiv 0 \pmod{n}$

#### 3.3.7 Non-Example 2: Matrices

The ring $M_2(\mathbb{Z})$ of $2 \times 2$ matrices over the integers is not an integral domain.

#### 3.3.8 Non-Example 3: Direct Product

$\mathbb{Z} \oplus \mathbb{Z}$ is not an integral domain. The reason why is because, for:

$$\mathbb{Z} \oplus \mathbb{Z} = \{(x, y) \mid x, y \in \mathbb{Z}\}$$

Take $(0, 1) \in \mathbb{Z} \oplus \mathbb{Z}$ and $(1, 0) \in \mathbb{Z} \oplus \mathbb{Z}$. Then:

$$(0, 1) \cdot (1, 0) = (0, 0)$$

### 3.4 Properties of Integral Domains

**Theorem 3.1: Cancellation**

Let $a$, $b$, and $c$ belong to an integral domain. If $ab = ac$, then:

$$a = 0 \text{ or } b = c$$

*Proof.* From $ab = ac$, we know that $ab - ac = 0$. Then, we know that $a(b - c) = 0$. There are two cases to consider:

- If $a \neq 0$, it follows that $b - c = 0$.
- Otherwise, $a = 0$ and it's trivial.

So, we are done. □

### 3.5 Fields

**Definition 3.3: Field**

A **field** is a commutative ring with unity in which every nonzero element is a unit (i.e. every nonzero element has a multiplicative inverse).

**Remarks:**

- To verify that every field is an integral domain, observe that if $a$ and $b$ belong to a field with $a \neq 0$ and $ab = 0$, we can multiply both sides of the last expression by $a^{-1}$ to obtain $b = 0$.
- In other words, you can never have an $x$ such that $0x = 1$.

### 3.5.1 Properties of Fields

**Theorem 3.2**

A finite integral domain is a field.

*Proof.* Let $R$ be a finite integral domain and suppose $a \in R \setminus \{0\}$. Consider the set:

$$\{a, a^2, a^3, a^4, \dots\} \subseteq R$$

Because $R$ is finite, there must be some overlap, i.e. there exists two integers $j < i$ such that $a^j = a^i$. This implies that $a^j = a^{i-j}a^j$. Since we have an integral domain, we can perform multiplicative cancellation; so:

$$1 = a^{i-j} \text{ for } i - j \geq 1$$

Then, $i - j - 1 \geq 0$ with $(a)(a^{i-j-1}) = a^{i-j} = 1$. So, $a^{-1} = a^{i-j-1}$ is a multiplicative inverse of $a$. □

**Corollary 3.1**

For every prime $p$, $\mathbb{Z}/p\mathbb{Z}$, the ring of integers modulo $p$ is a field.

**Remark:** This is often denoted $\mathbb{F}_p$ in this context.

### 3.5.2 Examples of Fields

Here are some examples and non-examples of fields.

1. Infinite Sets: $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{Q}$ are all fields.
2. Matrices: $M_2(\mathbb{R})$ is not a field because not all matrcies have an inverse.
3. (Non-Example) Polynomials: $\mathbb{R}[x]$ is not a field. This is because not all functions have a *polynomial* inverse. For example, the inverse of $x+3$ is $\frac{1}{x+3}$, which isn't a polynomial. However, $\mathbb{R}[x]$ is an integral domain.
4. Field w/ 9 Elements: $\mathbb{F}_3[i] = \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$. Recall that $i^2 = -1 \equiv 2 \pmod 3$.
5. Field w/ 4 Elements: $\{0, 1, a, b\}$.

| $+$ | $0$ | $1$ | $a$ | $b$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $a$ | $b$ |
| $1$ | $1$ | $0$ | $b$ | $a$ |
| $a$ | $a$ | $b$ | $0$ | $1$ |
| $b$ | $b$ | $a$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $a$ | $b$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $a$ | $b$ |
| $a$ | $0$ | $a$ | $b$ | $1$ |
| $b$ | $0$ | $b$ | $1$ | $a$ |

6. Rational Numbers: $\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ is a field. First, to show that it's a field, we need to show that every nonzero element has multiplicative inverses. Suppose $a + b\sqrt{5} \neq 0$. Then:

$$a + b\sqrt{5} \neq 0 \iff b\sqrt{5} \neq a \iff (a, b) \neq (0, 0)$$

In other words, $a, b$ are not both zero. Note that since $\sqrt{5}$ is irrational, $\sqrt{5} \neq \frac{a}{b}$. So, $\frac{1}{a+b\sqrt{5}} \in \mathbb{R}$ by $a + b\sqrt{5}$ is not zero and $\mathbb{R}$ is a field. With this in mind, we have:

$$\begin{aligned}\frac{1}{a+b\sqrt{5}} &= \frac{1}{a+b\sqrt{5}} \cdot \frac{a-b\sqrt{5}}{a-b\sqrt{5}} \\ &= \frac{a-b\sqrt{5}}{a^2 - ab\sqrt{5} + ab\sqrt{5} - 5b^2} \\ &= \frac{a-b\sqrt{5}}{a^2-5b^2} \\ &= \frac{a}{a^2-5b^2} + \frac{-b}{a^2-5b^2}\sqrt{5} \in \mathbb{Q}[\sqrt{5}]\end{aligned}$$

## 3.6 Characteristic of a Ring

Consider the ring $\mathbb{Z}_3[i]$, with the elements:

$$\{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$$

For any element $x$ in this ring, we have:

$$3x = x + x + x = 0$$

To better see this process, consider the following examples of elements in the ring:

- $2i + 2i + 2i = 6i = 0i = 0$
- $(1 + 2i) + (1 + 2i) + (1 + 2i) = 3 + 6i = 0$
- And so on.

Similarly, in the ring $\{0, 3, 6, 9\} \subset \mathbb{Z}_{12}$, we have, for all $x$:

$$4x = x + x + x + x = 0$$

We can formalize this into a definition.

**Definition 3.4: Characteristic of a Ring**

The **characteristic** of a ring $R$ is the least positive integer $n$ such that $nx = 0$ for all $x \in R$. If no such integer exists, we say that $R$ has characteristic 0. The characteristic of $R$ is denoted by $\operatorname{char} R$.

So, for example, the ring of integers $\mathbb{Z}$ has characteristic 0 and $\mathbb{Z}_n$ has characteristic $n$. Also, consider $\mathbb{Z}_3 = \{0, 1, 2\}$. Then, we know that:

$$3x = x + x + x = 0 \qquad \forall x$$

So the characteristic of $\mathbb{Z}_3$ is $\boxed{3}$. Now, consider $\mathbb{Z}_6$. We know that:

$$6x = x + x + x + x + x + x = 0 \qquad \forall x$$

So, its characteristic is $\boxed{6}$. As a final example, $\{0\}$ has characteristic $\boxed{1}$.

### 3.6.1 Characteristic of a Ring with Unity

Occasionally, we might have more complicated rings where the above theorem may be hard to apply.

**Theorem 3.3: Characteristic of a Ring with Unity**

Let $R$ be a ring with unity 1. If 1 has infinite order under addition, then the characteristic of $R$ is 0. If 1 has order $n$ under addition, then the characteristic of $R$ is $n$.

**Remark:** Here, suppose $(\mathbb{R}, +)$ is a group. Then, we say that $x \in \mathbb{R}$ has an additive order $n$ if $nx = 0$ and $n$ is the smallest positive number with this property.

*Proof.* Suppose 1 has infinite order. Then, there is no positive integer $n$ such that $n \cdot 1 = 0$, so $R$ must have characteristic 0. Now, let's suppose that 1 does have additive order $n$. Then, we know that $n \cdot 1 = 0$ and $n$ is the least positive integer with this property. So, for any $x \in R$, we have:

$$\begin{aligned} n \cdot x &= \overbrace{x + x + \cdots + x}^{n \text{ times}} \\ &= \overbrace{1x + 1x + \cdots + 1x}^{n \text{ times}} \\ &= (\overbrace{1 + 1 + \cdots + 1}^{n \text{ times}})x \\ &= (n \cdot 1)x = 0x = 0 \end{aligned}$$

So, $R$ has characteristic $n$. □

For example, take $R = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

1. Does this ring have unity? Each member of this direct product ring has 1, so the unity would be $(1, 1, 1) \in R$.
2. What is the characteristic of $R$? The characteristic order of $R$ is the additive order of $(1, 1, 1) \in R$. Well, we have that:
$$n(1, 1, 1) = (n1, n1, n1)$$
Consider the first element in the pair. When is $n1 \equiv 0 \pmod 6$? This is when $6|n$, or:
$$n \in \{6, 12, 18, 24, \dots\}$$
For the third element in the pair, we need to know when $n1 \equiv 0 \pmod{10}$. This is when $10|n$, or:
$$n \in \{10, 20, 30, \dots\}$$
Here, it's clear that the answer is $\operatorname{lcm}(6, 4, 10) = 60$.

**Theorem 3.4: Characteristic of an Integral Domain**

The characteristic of an integral domain is 0 or prime.

*Proof.* It suffices to consider the additive order of 1. Suppose towards a contradiction that 1 has composite order $n$ and $1 < s$ and $t < n$ such that $n = st$. Then, we know that:

$$0 = n1 = (st)1 = s(t1) = (s1)(t1)$$

But, $1 < s$ and $t < n$, so by minimality of $n$ being the order of 1, it must be that $s1, t1 \neq 0$ and are thus zero-divisors. But, this is a contradiction. □

## 3.7 Summary of Rings

| Ring | Characteristic | Integral Domain? |
|---|---|---|
| $\mathbb{Z}$ | 0 | Yes |
| $M_2(\mathbb{Z})$ | 0 | No |
| $\mathbb{Z} \oplus \mathbb{Z}$ | 0 | No |
| $\mathbb{F}_p$ $(\mathbb{Z}/p\mathbb{Z})$ | $p$ | Yes |
| $\mathbb{F}_p \oplus \mathbb{F}_p$ | $p$ | No |
| $\mathbb{F}_p[x]$ | $p$ | Yes |
| $\mathbb{Z}/n\mathbb{Z}[i]$ | $n$ | No $n$ not prime.<br>Maybe $n$ prime. |

# 4 Ideals & Quotient Rings (Chapter 14)

Recall that if $H$ is a *normal* subgroup of $G$, then there exists a quotient group $G/H$ defined by:

$$G/H = \{gH \mid g \in G\}$$

Where the operation of the quotient group is:

$$(g_1H)(g_2H) = (g_1g_2)H$$

We can use this same notion in *rings*. In our case, the normal subgroup of groups is the same as *ideals* in rings.

## 4.1 Ideals

**Definition 4.1: Ideal**

A subring $A$ of a ring $R$ is called a (two-sided) **ideal** of $R$ if for every element $r \in R$ and every $a \in A$ then:

$$ra \in A \text{ and } ar \in A$$

That is, $rA = \{ra \mid a \in A\} \subseteq A$ and $Ar \subseteq A$.

**Definition 4.2: Proper Ideal**

An ideal $A$ is called **proper** if $A \subset R$.

### 4.1.1 Ideal Test

**Theorem 4.1: Ideal Test**

A nonempty subset $A \subseteq R$ is an ideal if and only if:

1. $a, b \in A \implies a - b \in A$.
2. $a \in A, r \in R \implies ra, ar \in R$.

*Proof.* This is similar to the subring test. □

### 4.1.2 Principal Ideal

If $R$ is a commutative ring with unity, then the principal ideal generated by $a \in R$ is:

$$\langle a \rangle = (a) = \{ra \mid r \in R\}$$

*Proof.* Pick two elements $ra, sa \in \langle a \rangle$. Then, $ra - sa = (r - s)a \in \langle a \rangle$. Likewise, if $r \in R$, then $sa \in \langle a \rangle$ so:

$$(sa)r = r(sa) = (rs)a \in \langle a \rangle$$

So, we are done. □

### 4.1.3 Basic Examples of Ideals

We now go over some basic examples of ideals.

1. Even Integers: $2\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal. Suppose that there is some integer $r \in \mathbb{Z}$ and $a \in 2\mathbb{Z}$. Then, $a = 2k$ for some $k \in \mathbb{Z}$ so that $ra = r \cdot 2k = 2(rk) \in 2\mathbb{Z}$. Note that this also extends to any $n\mathbb{Z}$; that is, $n\mathbb{Z}$ is an ideal.
2. Trivial Subring: $\{0\} \subseteq R$ is a trivial ideal because $r\{0\} = \{0\}r = \{0\}$.
3. Integers/Rationals: $\mathbb{Z} \subseteq \mathbb{Q}$ is *not* an ideal. Take $r = \frac{1}{2} \in \mathbb{Q}$ and $a = 1 \in \mathbb{Z}$. Then
$$ra = \frac{1}{2}(1) = \frac{1}{2} \notin \mathbb{Z}$$
4. Integers: Consider $R = \mathbb{Z}$ with $\langle n \rangle = n\mathbb{Z}$. This is a principal ideal.
5. Polynomials: If $R = \mathbb{R}[x]$, then
$$\begin{aligned}\langle x \rangle &= \{f(x)x \mid f(x) \in \mathbb{R}[x]\} \\ &= \{\text{Polynomials divisible by } x\} \\ &= \{f(x) \in \mathbb{R}[x] \mid f(0) = 0\}\end{aligned}$$
6. Ring of Unity: The ideal generated by $a_1, a_2, \ldots, a_n \in R$, where $R$ is a commutative ring of unity, is:
$$\langle a_1, a_2, \ldots, a_n \rangle = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R\}$$
7. Two Elements: Consider $\langle 2, x \rangle \subseteq \mathbb{Z}[x]$. This is defined by
$$\{f(x) \in \mathbb{Z}[x] \mid f(0) \text{ is even.}\}$$

## 4.2 Quotient Ring

Now, we talk about quotient rings, which are very similar to quotient groups.

**Definition 4.3: Quotient Ring**

Let $I \subseteq R$ be an ideal of $R$. Then, the **quotient ring** (or factor ring) is the set of *cosets*
$$R/I = \{r + I \mid r \in R\}$$
with the operations
$$\begin{aligned}(r + I) + (s + I) &= (r + s) + I \\ (r + I)(s + I) &= (rs) + I\end{aligned}$$

**Proposition.** *$R/I$ is a ring.*

*Proof.*
- For addition, we know that $(R, +)$ is an abelian group. This implies that $(I, +)$ is a normal subgroup of $(R, +)$, so $(R/I, +)$ is a group.
- For multiplication, suppose $r + I = r' + I$ and $s + I = s' + I$, i.e.
$$r = r' + a \text{ and } s = s' + b \text{ for some } a, b \in I$$
Then, $(rs) = (r' + a)(s' + b) = r's' + r'b + as' + ab$. Note that $r'b, as', ab$ all belong to the ideal. So $r's' + r'b + as' + ab \in r's' + I$.

And, we are done. □

### 4.2.1 Examples of Quotient Rings

Now, we go over some examples of quotient rings.

1. Integer Ring Modulo 5: Consider $\mathbb{Z}/5\mathbb{Z} = \{0+5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\}$. We know that $5\mathbb{Z} \subseteq \mathbb{Z}$ is an ideal.

2. Polynomial Ideal: Consider $\mathbb{R}[x]/\langle x^2+1\rangle$. This ring is "isomorphic" to $\mathbb{C}$. By identifying $x+\langle x^2+1\rangle \in \mathbb{R}[x]/\langle x^2+1\rangle$ as $i \in \mathbb{C}$, then

$$(x + \langle x^2+1\rangle)^2 = x^2 + \langle x^2+1\rangle = x^2 + -(x^2+1) + \langle x^2+1\rangle = -1 + \langle x^2+1\rangle$$

We can also see this through polynomial long division. There is a unique way to write $f(x) = g(x)q(x)+r(x)$ with $\deg r(x) < \deg g(x)$. From this, we can tell that

$$f(x) + \langle x^2+1\rangle = (x^2+1)q(x) + (a+bx) + \langle x^2+1\rangle = (a+bx) + \langle x^2+1\rangle$$

3. Gaussian Integers: Take $\mathbb{Z}[i]/\langle 2-i\rangle$. We claim that this is "isomorphic" to $\mathbb{Z}/5\mathbb{Z}$. It turns out:

$$\mathbb{Z}[i]/\langle 2-i\rangle = \{0 + \langle 2-i\rangle, 1 + \langle 2-i\rangle, 2 + \langle 2-i\rangle, 3 + \langle 2-i\rangle, 4 + \langle 2-i\rangle\}$$

Consider that $2 + \langle 2-i\rangle = i + \langle 2-i\rangle$ because $2-i \in \langle 2-i\rangle$. Then:

$$\begin{aligned} 2^2 + \langle 2-i\rangle &= i^2 + \langle 2-i\rangle \\ \implies 4 + \langle 2-i\rangle &= -1 + \langle 2-i\rangle \\ \implies 5 &\in \langle 2-i\rangle \end{aligned}$$

Thus, $a+bi+\langle 2-i\rangle = a+2b+\langle 2-i\rangle = r+\langle 2-i\rangle$ for $0 \le r < 5$ such that $a+2b = 5q+r$. Now, how do we know that these cosets are distinct? It suffices to show that $1+\langle 2-i\rangle$ has additive order 5. So:

$$5(1 + \langle 2-i\rangle) = 5 + \langle 2-i\rangle = 0 + \langle 2-i\rangle$$

Where the last step is due to $5 \in \langle 2-i\rangle$. This tells us that the additive order of $1+\langle 2-i\rangle$ divides 5. This implies that the order is either 1 or 5. If the order is 5, we are done since this implies that there are 5 distinct cosets. Otherwise, suppose towards a contradiction that $1 + \langle 2-i\rangle \in \mathbb{Z}[i]/\langle 2-i\rangle$ has additive order 1. In this case:

$$\begin{aligned} 1(1 + \langle 2-i\rangle) &= 0 + \langle 2-i\rangle \\ \implies 1 &\in \langle 2-i\rangle = \{(2-i)r \mid r \in \mathbb{Z}[i]\} \\ \implies 1 &= (2-i)(a+bi) \text{ for some } a, b \in \mathbb{Z} \\ \implies 1 &= 2a + 2bi - ai + b \\ \implies 1 + 0i &= (2a+b) + (2b-a)i \\ \implies &\begin{cases} 1 = 2a+b \\ 0 = 2b-a \end{cases} \\ \implies a &= \frac{1}{5} \text{ and } \frac{2}{5} \end{aligned}$$

However, $a, b \in \mathbb{Z}$ so we have a contradiction and so $1 + \langle 2-i\rangle$ must have additive order 5.

## 4.3 Prime and Maximal Ideals

**Definition 4.4: Prime Ideals**

A **prime ideal** $A$ of a commutative ring $R$ is a proper ideal of $R$ such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$.

Consider the following examples:

- Consider $R = \mathbb{Z}$. The ideals of $\mathbb{Z}$ are $\{0\}$ and $n\mathbb{Z}$ for $n = 1, 2, \ldots$. We know that $2\mathbb{Z}$ is prime. So, if $nm \in 2\mathbb{Z}$, then $nm = 2k$, which is even. This implies that one of $n$ or $m$ is even, so $n \in 2\mathbb{Z}$ or $m \in 2\mathbb{Z}$.

  This is true in general. If $p$ is prime, then $p\mathbb{Z}$ is a prime ideal. Recall that if $p|ab$, then $p|a$ or $p|b$ by Euclid's Lemma.

- Consider $6\mathbb{Z}$, which is not prime. We want to show that this is not a prime ideal. To do this, we want to find an $n, m \in \mathbb{Z}$ such that $nm \in 6\mathbb{Z}$ but $n, m \notin 6\mathbb{Z}$. An obvious example is $n = 2$ and $m = 3$.

  In general, if $n = st$ is composite, then $st \in n\mathbb{Z}$ but $s, t \notin n\mathbb{Z}$.

- Consider $R = \{0\}$. This is a prime ideal. Suppose $n, m \in \mathbb{Z}$ with $nm \in R$. Then, $nm = 0$ means that one of $n$ or $m$ is 0, which implies that $n \in R$ or $m \in R$.

**Fact:** $\{0\} \subseteq R$ is a prime ideal if and only if $R$ is an integral domain.

**Definition 4.5: Maximal Ideals**

A **maximal ideal** of a commutative ring $R$ is a proper ideal of $R$ such that, when $B$ is an ideal of $R$ and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

Put it another way, a maximal ideal $I$ of a commutative ring $R$ is a proper ideal which is not contained in any other proper ideals, i.e. if $I \subseteq A \subseteq R$ for some ideal $A$, then $A = I$ or $A = R$.

### 4.3.1 Properties of Prime & Maximal Ideals

**Theorem 4.2**

Let $R$ be a commutative ring with unity and $I \subseteq R$ an ideal. Then, $R/I$ is an integral domain if and only if $I$ is prime.

*Proof.* Supose $R/I$ is an integral domain. Suppose then that $a, b \in R$ with $ab \in I$. Then, $ab + I = 0 + I$. This further implies that $(a + I)(b + I) = 0 + I$. This implies that $a + I = 0 + I$ *or* $b + I = 0 + I$ by integral domain definition. By the definition of a coset, $a \in I$ or $b \in I$. Thus, $I$ is prime.

Suppose now that $I$ is prime. Suppose $a, b \in R$ with $(a + I)(b + I) = 0 + I$ with $ab + I = 0 + I$. This implies that $ab \in I$, which further means that $a \in I$ or $b \in I$ by prime. Thus, $a + I = 0 + I$ or $b + I = 0 + I$. Thus, $R/I$ is an integral domain. □

**Theorem 4.3**

Let $R$ be a commutative ring with unity and $I \subseteq R$ an ideal. Then, $R/I$ is a field if and only if $I$ is maximal.

*Proof.* Suppose $R/I$ is a field. We want to show that if $I \subseteq A \subseteq R$, then $A = I$ or $A = R$.[a] Suppose $A \subseteq R$ is an ideal satisfying $I \subseteq A$ and $A \neq I$. The fact that $A \neq I$ implies that we can choose some $b \in A \setminus I$. This implies that $b + I \neq 0 + I$ and so $b + I \in R/I$ is a unit. This implies that there exists some $c + I \in R/I$ with $(b + I)(c + I) = 1 + I$, which further implies that $bc + I = 1 + I$. Thus, .... We know that $1 - bc \in A$, but $b \in A \setminus I \subseteq A$ so $bc \in A$ and thus $1 = (1 - bc) + bc \in A$. So, $R = R \cdot 1 \subseteq A$ so that $A = R$. Thus, $I$ is maximal.

Suppose that $I$ is maximal. We want to show that any $b + I \neq 0 + I$ is a unit in $R/I$. Choose some $b + I \in R/I$ with $b + I \neq 0 + I$, i.e. choose some $b \in R \setminus I$. Consider $B = \{rb + a \mid r \in R, a \in I\}$. Thus,

$B = R$ by $I \subseteq B \subseteq R$ and $b \neq I$ $(b \in B, b \in I)$.[b] From there, $1 \in B$ which means that $1 = rb + a$ for some $r \in R$ and $a \in I$, which finally implies that $1 + I = (r + I)(b + I)$. □

[a] We can prove the fact that $I \subseteq A \subseteq R$ and $A \neq I$ *implies that* $A = R$.
[b] Exercise: Show that $B$ is an ideal with contains $I$

**Corollary 4.1**

All maximal ideals are prime ideals.

*Proof.* Suppose $I \subseteq R$ is maximal.

$$\begin{aligned} & R/I \text{ is a field.} \\ \implies\ & R/I \text{ is an integral domain.} \\ \implies\ & R/I \text{ is prime.} \end{aligned}$$

So, we are done. □

**Remark:** The converse is not true. Consider $\langle x \rangle \subseteq \mathbb{Z}[x]$. This is not maximal by $\langle x \rangle \subset \langle 2, x \rangle \subset \mathbb{Z}[x]$.

$$\mathbb{Z}[x]/\langle x \rangle \longleftrightarrow \mathbb{Z}$$

$$f(x) + \langle x \rangle \longleftrightarrow f(0)$$

$$f(x) + \langle x \rangle = h(x) + \langle x \rangle \iff f(x) - h(x) = g(x)x \text{ for some } g(x) \iff f(0) - h(0) = 0$$

Thus, this ideal $\langle x \rangle$ is prime.

# 5 Ring Homomorphisms

Ring homomorphism is very similar in nature to group homomorphisms. Here, a ring homomorphism preserves the ring operations.

**Definition 5.1: Ring Homomorphism**

A **ring homomorphism** $\varphi$ from a ring $R$ to a ring $S$ is a mapping from $R$ to $S$ that preserves the ring operation. That is, for all $a, b \in R$:

$$\varphi(a+b) = \varphi(a) + \varphi(b) \qquad \varphi(ab) = \varphi(a)\varphi(b)$$

**Remark:** As is the case for groups, the operations on the left of the equal signs are those of $R$, while the operations on the right side are those of $S$.

Along with ring homomorphisms, there is also ring isomorphisms.

**Definition 5.2: Ring Isomorphism**

A **ring isomorphism** is a ring homomorphism that is both one-to-one and onto (i.e. bijective).

## 5.1 Properties of Ring Homomorphisms

**Theorem 5.1**

Let $\varphi$ be a ring homomorphism from a ring $R$ to a ring $S$, and let $A$ be a subring of $R$ and let $B$ be an ideal of $S$.

1. For any $r \in R$ and any positive integer $n$, $\varphi(nr) = n\varphi(r)$ and $\varphi(r^n) = (\varphi(r))^n$.
2. $\varphi(A) = \{\varphi(a) \mid a \in A\}$ is a subring of $S$.
3. If $A$ is an ideal and $\varphi$ is onto $S$, then $\varphi(A)$ is an ideal.
4. $\varphi^{-1}(B) = \{r \in R \mid \varphi(r) \in B\}$ is an ideal of $R$.
5. If $R$ is commutative, then $\varphi(R)$ is commutative.
6. If $R$ has a unity 1, $S \neq \{0\}$, and $\varphi$ is onto, then $\varphi(1)$ is the unity of $S$.
7. $\varphi$ is an isomorphism if and only if $\varphi$ is onto and $\ker(\varphi) = \{r \in R \mid \varphi(r) = 0\} = \{0\}$.
8. If $\varphi$ is an isomorphism from $R$ onto $S$, then $\varphi^{-1}$ is an isomorphism from $S$ onto $R$.

# 6 Ring Homomorphisms

**Theorem 6.1**

Let $\varphi : R \mapsto S$ be a ring homomorphism. Then, $\ker\varphi = \{r \in R \mid \varphi(r) = 0\}$ is an ideal of $R$.

*Proof.* If $a, b \in \ker\varphi$, then $\varphi(a-b) = \varphi(a) - \varphi(b) = 0 - 0 = 0$, which implies that $a - b \in \ker\varphi$. Now, if we check $a \in \ker\varphi$ and $r \in R$, then $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$. Therefore, $ra \in \ker\varphi$. Thus, $\ker\varphi$ is an ideal by the ideal test. □

## 6.1 Examples of Ring Homomorphism

Here are some examples of ring homomorphisms.

### 6.1.1 Example 1: Integers and Modulo

Consider the mapping:

$$k \mapsto k \pmod{n}$$

This is a ring homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}_n$, and is called the natural homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$.

### 6.1.2 Example 2: Complex Numbers

Consider the mapping:

$$a + bi \mapsto a - bi$$

This is a ring homomorphism from the complex numbers onto the complex numbers.

### 6.1.3 Example 3: Functions

Consider the ring of all polynomials with real coefficients $\mathbb{R}[x]$. Consider the mapping:

$$f(x) \mapsto f(1)$$

This is a ring homomorphism from $\mathbb{R}[x]$ onto $\mathbb{R}$.

## 6.2 First Isomorphism Theorem

**Theorem 6.2: First Isomorphism Theorem**

Let $\varphi : R \mapsto S$ be a ring homomorphism. Then, the map

$$\overline{\varphi} = R/\ker\varphi \mapsto \varphi(R)$$

defined by the mapping

$$r + \ker\varphi \mapsto \varphi(r)$$

is an isomorphism.

*Proof.* We already know that $\overline{\varphi} : R/\ker\varphi \mapsto \varphi(R)$ is an isomorphism of additive groups; in particular,

$$(R/\ker\varphi, +) \mapsto (\varphi(R), +)$$

by the First Isomorphism Theorem for groups. Thus, it suffices to check that:

$$\overline{\varphi}(xy) = \overline{\varphi}(x)\overline{\varphi}(y)$$

So, it suffices to check:

$$\begin{aligned}\overline{\varphi}((r+\ker\varphi)(s+\ker\varphi)) &= \overline{\varphi}(rs+\ker\varphi)\\ &= \varphi(rs)\\ &= \varphi(r)\varphi(s)\\ &= \overline{\varphi}(r+\ker\varphi)\overline{\varphi}(s+\ker\varphi)\end{aligned}$$

And so we are done. □

**Remark:** If $I \subseteq R$ is an ideal, then $I = \ker q$ where $q : R \mapsto R/I$, defined by the mapping $r \mapsto r + I$, is the quotient homomorphism.

## 6.3 Examples

1. Consider the homomorphism $\varphi : \mathbb{Z}[x] \mapsto \mathbb{Z}$ defined by the mapping $f(x) \mapsto f(0)$. $\varphi$ is a surjective[1] homomorphism. By the First Isomorphism Theorem:

$$\mathbb{Z}[x]/\ker\varphi \cong \mathbb{Z}$$

Here, we define $\ker\varphi = \{a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{Z}\}$ because $f(0)$ is a constant term. However, we can factor $x$ out to get:

$$\ker\varphi = \{x(a_1 + a_2x^1 + \cdots + a_nx^{n-1}) \mid a_i \in \mathbb{Z}\} = \langle x\rangle$$

And so it follows that:

$$\boxed{\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}}$$

2. Consider the homomorphism $\varphi : \mathbb{R}[x] \mapsto \mathbb{C}$ defined by the mapping $f(x) \mapsto f(i)$. $\varphi$ is surjective because $f(a+bx) = a+bi$ for any $a, b \in \mathbb{R}$. We also know that $x^2+1 \in \ker\varphi$ by $i^2+1=0$. This implies that:

$$\langle x^2+1\rangle \subseteq \ker\varphi \subset \mathbb{R}[x]$$

**Fact:** $\langle x^2+1\rangle$ is maximal, which implies that $\langle x^2+1\rangle = \ker\varphi$.

> *Proof.* (Of fact.) We prove that $\mathbb{R}[x]/I$ for $I = \langle x^2+1\rangle$ is a field for any $a+bx+I$ with $a, b$ not both zero, then $(a+b+I)^{-1} = \frac{a-bx}{a^2+b^2} + I$. □

Therefore, $\boxed{\mathbb{R}[x]/\langle x^2+1\rangle \cong \mathbb{C}}$ by the First Isomorphism Theorem.

## 6.4 Rings with Unity

**Proposition.** *If $R$ has unity, then $\varphi : \mathbb{Z} \mapsto \mathbb{R}$ defined by*

$$\varphi(n) = n \cdot 1 = \begin{cases} \underbrace{1 + \cdots + 1}_{n \text{ times}} & n > 0 \\ 0 & n = 0 \\ \underbrace{-1 - 1 - \cdots - 1}_{-n \text{ times}} & n < 0 \end{cases}$$

*is a homomorphism.*

> *Proof.* Left as an exercise. □

**Proposition.** *If $R$ is a ring with unity, then:*

*(a) If* $\operatorname{char} R = n > 0$*, then $R$ contains a subring isomorphic to $\mathbb{Z}/n\mathbb{Z}$.*

*(b) If* $\operatorname{char} R = 0$*, then $R$ contains a subring isomorphic to $\mathbb{Z}$.*

> *Proof.* Let $\varphi : \mathbb{Z} \mapsto \mathbb{R}$ with $\varphi(n) = n \cdot 1$. Then, $\operatorname{char} R$ is the additive order of 1. This implies that if $\operatorname{char} R = n > 0$, then $\ker\varphi = n\mathbb{Z}$ so $\mathbb{Z}/n\mathbb{Z} \cong \varphi(\mathbb{Z}) \subseteq R$ by the First Isomorphism Theorem. Likewise, if $\operatorname{char} R = 0$, then $\ker\varphi = \{0\}$ and it follows that $\mathbb{Z} \cong \varphi(\mathbb{Z}) \subseteq R$ by the First Isomorphism Theorem. □

[1] If $a \in \mathbb{Z}$, then $(x+a) \xrightarrow{\varphi} 0 + a = a$

## 6.5 Fields

**Definition 6.1: Prime Subfield**

The subfield of a field isomorphic to $\mathbb{F}_p$ or $\mathbb{Q}$ is called the **prime subfield**.

**Theorem 6.3**

- If $F$ is a field of characteristic $p$, then $F$ contains a subfield isomorphic to $\mathbb{F}_p$.
- If $F$ is a field of characteristic 0, then $F$ contains a subfield isomorphic to $\mathbb{Q}$.

*Proof.* We prove both parts.

- By the previous proposition, $\operatorname{char} F = p$ implies that the subring is isomorphic to $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.
- $\operatorname{char} F = 0$ implies that the subring is isomorphic to $\mathbb{Z}$, given by

$$\varphi : \mathbb{Z} \mapsto F$$

which sends $n \mapsto n \cdot 1$. Consider the set

$$T = \{ab^{-1} \mid a, b \in \varphi(\mathbb{Z}), b \neq 0\} \subseteq F$$

We claim that $T$ is a subring isomorphic to $\mathbb{Q}$.

*Proof.* Define $\overline{\varphi} : \mathbb{Q} \mapsto F$ by $\overline{\varphi}(a/b) = \varphi(a)\varphi(b)^{-1}$.

- Well-Defined: This is well-defined since $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$, which then implies that $\varphi(a)\varphi(d) = \varphi(b)\varphi(c)$ for $\varphi : \mathbb{Z} \mapsto F$. This implies that $\varphi(a)\varphi(b)^{-1} = \varphi(c)\varphi(d)^{-1}$, which again implies that $\overline{\varphi}(a/b) = \overline{\varphi}(c/d)$.
- Homomorphism: Addition is left as an exercise. For multiplication, see lecture.

So, we are done. □

And so on (need to come back). □

**Remark:** If $F$ is a field and $I \subseteq F$ is an ideal, then $I = \{0\}$ or $I = F$.

*Proof.* $F/\{0\} \cong F$ is a field. Thus, $\{0\}$ is a maximal ideal of $F$. This implies that, for all ideals $I$ with $\{0\} \subseteq I \subseteq F$, $I = \{0\}$ or $I = F$. The fact that all ideals satisfy $\{0\} \subseteq I \subseteq F$ concludes the proof. □