We have learned a lot about groups. We now turn our attention to a different algebraic structure: rings. For now, think of a “ring” as an abelian group (under addition) that also has a multiplication.
Examples of Rings
Definitions
Proofs about rings
Subrings

Example
The standard example of a ring is $\mathbb{Z}$, the integers. Then $(\mathbb{Z}, +)$ certainly forms an abelian group, multiplication is closed and associative, and the distributive law holds (in both directions).

Example
Another example of a ring is $\mathbb{Z}_n$, the integers modulo $n$. Then $(\mathbb{Z}_n, +)$ certainly forms an abelian group, multiplication is closed and associative, and the distributive law holds (in both directions).

We will focus our attention on $\mathbb{Z}_3$ and $\mathbb{Z}_6$ for our examples.

Example
Let $\mathbb{Z}[x]$ be the set of all polynomials with integer coefficients, where
\[
\begin{align*}
(a_n x^n + \cdots + a_1 x + a_0) + (b_n x^n + \cdots + b_1 x + b_0) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 + (b_m + b_{m-1}) x^{m-1} + \cdots + (a_1 + b_1) x + (a_0 + b_0) \\
\text{Multiplication is the usual “FOIL”-type polynomial multiplication.} \\
0 &= 0 x + 0 \\
-(a_n x^n + \cdots + a_1 x + a_0) &= -a_n x^n - \cdots - a_1 x - a_0
\end{align*}
\]
for all $a_i, b_i \in \mathbb{Z}$ and $n, m \in \mathbb{Z}$ with $0 \leq m \leq n$.

Example
Let $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ for any integer $n$, where
\[
\begin{align*}
(na) + (nb) &= n(a + b) \\
(na)(nb) &= n(nab) \\
0 &= n(0) \\
-na &= -na
\end{align*}
\]
for all $a, b \in \mathbb{Z}$. We will use $2\mathbb{Z}$ (the even integers) as our “toy ring.”

Example
Let $M_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ where
\[
\begin{align*}
\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} &= \begin{bmatrix} a + e & b + f \\ c + g & d + h \end{bmatrix} \\
\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} &= \begin{bmatrix} ae + bg & af + bh \\ ce + dg & ef + dh \end{bmatrix} \\
0 &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\
-\begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}
\end{align*}
\]
for all $a, b, c, d \in \mathbb{Z}$.
Examples of Rings
Definitions
Proofs about rings
Subrings

Example
Let \( \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \) for any positive integer \( n \), where
\[
\begin{align*}
1. & \quad (a + bi) + (c + di) = (a + c) + (b + d)i \\
2. & \quad (a + bi)(c + di) = (ac - bd) + (ad + bc)i \\
3. & \quad 0 = 0 + 0i \\
4. & \quad -(a + bi) = -a - bi
\end{align*}
\]
for all \( a, b, c, d \in \mathbb{Z} \).

Example
Let \( \mathbb{Z}_n[i] = \{a + bi \mid a, b \in \mathbb{Z}_n\} \) for any positive integer \( n \), where
\[
\begin{align*}
1. & \quad (a + bi) + (c + di) = (a + c) + (b + d)i \\
2. & \quad (a + bi)(c + di) = (ac - bd) + (ad + bc)i \\
3. & \quad 0 = 0 + 0i \\
4. & \quad -(a + bi) = -a - bi
\end{align*}
\]
for all \( a, b, c, d \in \mathbb{Z}_n \). We will use \( \mathbb{Z}_3[i] \) as one of our “toy groups.”

Example
Let \( \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \) where
\[
\begin{align*}
1. & \quad (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \\
2. & \quad (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2} \\
3. & \quad 0 = 0 + 0\sqrt{2} \\
4. & \quad -(a + b\sqrt{2}) = -a - b\sqrt{2}
\end{align*}
\]
for all \( a, b, c, d \in \mathbb{Z} \).

Example
Let \( \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \) where
\[
\begin{align*}
1. & \quad (a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \\
2. & \quad (a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2} \\
3. & \quad 0 = 0 + 0\sqrt{2} \\
4. & \quad -(a + b\sqrt{2}) = -a - b\sqrt{2}
\end{align*}
\]
for all \( a, b, c, d \in \mathbb{Q} \).
Example
Let $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ where
\[ (a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a + c) + (b + d)\sqrt{-5} \]
\[ (a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (bc + ad)\sqrt{-5} \]
\[ 0 = 0 + 0\sqrt{-5} \]
\[ -(a + b\sqrt{-5}) = -a - b\sqrt{-5} \]
for all $a, b, c, d \in \mathbb{Z}$.

The definition of a ring

Definition
A ring $R$ is a set with two binary operations: addition (denoted by $a + b$) and multiplication (denoted by $ab$) such that for all $a, b, c \in R$:
\[ \text{There is an additive identity 0 such that } a + 0 = a = 0 + a. \]
\[ \text{There is an element } -a \text{ such that } a + (-a) = 0 = (-a) + a. \]
\[ a + (b + c) = (a + b) + c. \]
\[ a + b \in R. \]
\[ a + b = b + a \]
\[ ab \in R \]
\[ a(bc) = (ab)c \]
\[ a(b + c) = ab + ac \text{ and } (b + c)a = ba + ca. \]
The ring definition, simplified

In short, a ring $R$ is a set with addition and multiplication such that:

1. $(R, +)$ is an abelian group.
2. Multiplication is associative and closed.
3. There is a left and right distributive law.

Note that the definition of a ring does not allow us to assume the following:

1. Every ring has a multiplicative identity.
2. Every element of every ring has a multiplicative inverse.
3. Every ring has commutative multiplication.

Basically, we cannot assume that $R$ is a group under multiplication. However, some rings have some of these properties. We give them special names when this happens.

1. If $R$ has a multiplicative identity, we call it a unity and denote it by 1. We then say “$R$ is a ring with unity.”
2. If an element $a \in R$ has a multiplicative inverse, we denote it by $a^{-1}$ and call $a$ a unit. (Note that $a^{-1}$ is also a unit).
3. If a ring $R$ has commutative multiplication, we say that $R$ is a commutative ring.

Some definitions

**Definition (Short-hand for repeated addition)**

Let $R$ be a ring, $a \in R$, and $n \in \mathbb{Z}$. Then

$$n \cdot a = na = a + a + \cdots + a.$$  

**Definition (Short-hand for adding inverses)**

Let $R$ be a ring, $a, b \in R$. Then $a - b$ denotes $a + (-b)$.

**Definition**

Let $R$ be a ring with unity such that $a \in R$. We say $a$ is a unit if there is an element $b \in R$ such that $ab = 1 = ba$.

**Definition**

Let $R$ be a ring with $a, b \in R$. We say $a$ divides $b$ if there is an element $c \in R$ such that $ac = b$.

Note that the definition of a ring does not allow us to assume the following:

- Every ring has a multiplicative identity.
- Every element of every ring has a multiplicative inverse.
- Every ring has commutative multiplication.

Examples of Rings

**Example**

The only units in $\mathbb{Z}$ are 1 and $-1$.

**Example**

Some units from $\mathbb{Z}[\sqrt{2}]$ are $1$, $-1$, $3 + 2\sqrt{2}$, and $3 - 2\sqrt{2}$ (note that $1 \cdot 1 = 1$, $-1 \cdot -1 = 1$, $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$).

**Example**

In $\mathbb{Z}$, 3 divides 15 since $3 \cdot 5 = 15$.

**Example**

In $M_2(\mathbb{Z})$, $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ divides $\begin{bmatrix} 2 & -2 \\ -2 & 2 \end{bmatrix}$, since

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 2 & -2 \\ -2 & 2 \end{bmatrix} = \begin{bmatrix} 2 & -2 \\ 2 & -2 \end{bmatrix}.$$
More definitions

Definition
Let $R$ be a ring with $0 \neq a \in R$. If there exists a nonzero $b \in R$ such that $ab = 0$, then we say that $a$ is a zero-divisor.

Definition
Suppose that $R$ is a ring such that it is commutative, it has a unity, and there are no zero-divisors. Then we say that $R$ is an integral domain.

Example
Find the roots of $f(x) = x^2 - 3x + 2$ (in $\mathbb{R}$, which is also a ring).

\[ x^2 - 3x + 2 = (x - 1)(x - 2) \]

So either $x - 1 = 0$ or $x - 2 = 0$ BECAUSE WE KNOW THERE ARE NO ZERO-DIVISORS IN $\mathbb{R}$! Note that $\mathbb{R}$ is an integral domain, since 1 is the unity and the multiplication is commutative, and we use this fact whenever we set factors equal to zero to find roots of polynomials.

Example (Non-example)
Consider one of our toy rings, $\mathbb{Z}_6$. Then $2(3) = 0$, so 2 is a zero-divisor (and so is 3).

So the function $f(x) = x^2 - 3x + 2$ has four roots in $\mathbb{Z}_6$: 1, 2, 4, 5. We would not find them all by factoring and setting equal to zero.

Definition
Suppose that $R$ is a ring such that it is commutative, it has a unity, and every non-zero element is a unit. Then we say that $R$ is a field.

Definition
The characteristic of a ring $R$ (denoted $\text{char}(R)$) is the least positive integer $n$ such that $na = 0$ for all $a \in R$. If not such $n$ exists, we define $\text{char}(R) = 0$ and say that it has characteristic zero.
Examples of Rings
Definitions
Proofs about rings
Subrings

Example
The real numbers \( \mathbb{R} \) and the rationals \( \mathbb{Q} \) are fields, but the integers \( \mathbb{Z} \) is not a field (for instance, 2 does not have a multiplicative inverse, so it is not a unit). However, \( \mathbb{Z} \) is an integral domain.

Example
\( \text{char}(\mathbb{Z}) = 0 \), \( \text{char}(\mathbb{Z}_3) = 3 \), and \( \text{char}(\mathbb{Z}_6) = 6 \).

In your teams, fill in the following table:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathbb{Z} )</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>0</td>
</tr>
<tr>
<td>( \mathbb{Z}_3 )</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>3</td>
</tr>
<tr>
<td>( \mathbb{Z}_6 )</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>6</td>
</tr>
<tr>
<td>( \mathbb{Z}[x] )</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>0</td>
</tr>
<tr>
<td>( \mathbb{Z} \oplus \mathbb{Z} )</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>0</td>
</tr>
<tr>
<td>( \mathbb{M}_2(\mathbb{Z}) )</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>0</td>
</tr>
<tr>
<td>( \mathbb{Z}[i] )</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>0</td>
</tr>
<tr>
<td>( \mathbb{Z}_3[i] )</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>3</td>
</tr>
<tr>
<td>( \mathbb{Z}[\sqrt{2}] )</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>0</td>
</tr>
<tr>
<td>( \mathbb{Q}[\sqrt{2}] )</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>0</td>
</tr>
<tr>
<td>( \mathbb{Z}[\sqrt{-5}] )</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>0</td>
</tr>
</tbody>
</table>

Even more definitions

Definition
Let \( D \) be an integral domain. An element \( a \in D \) is called an \textit{irreducible} if \( a \) is not a unit and whenever \( b, c \in D \) with \( a = bc \), then either \( b \) is a unit or \( c \) is a unit.

Note that this is the idea we usually think of as “prime,” which is confusing because . . .

Definition
Let \( D \) be an integral domain. An element \( a \in D \) is called a \textit{prime} if \( a \) is not a unit and whenever \( b, c \in D \) with \( a \mid bc \), then either \( a \mid b \) or \( a \mid c \).

In the integers, the terms \textit{prime} and \textit{irreducible} are equivalent.

Definition
An integral domain \( D \) is called a \textit{unique factorization domain} (usually referred to as a \textit{UFD}) if
- every nonzero, nonunit \( a \in D \) can be written as \( a = p_1 \cdots p_n \) for some irreducibles \( p_i \), and
- if \( p_1 \cdots p_n = a = q_1 \cdots q_m \), then \( n = m \) and \( q_1 \cdots q_m = (u_1 \cdot p_1) \cdots (u_n \cdot p_n) \) for some units \( u_i \in D \).
Example
You know from elementary school that \( \mathbb{Z} \) is a UFD.

Example (Non-example)
The ring \( \mathbb{Z}[\sqrt{-5}] \) is not a UFD. Observe that 6 = 2 \cdot 3 and 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}). It is routine to show that 2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5} are irreducible, but we will not do that now.

Theorem
Let \( R \) be any ring, and \( a \in R \). Then \( a0 = 0 = 0a \).

Proof.
We can use the distributive law to get:
\[
\begin{align*}
a0 &= a(0 + 0) \\
0 &= a0 + a0 \\
(a0) + (-a0) &= (a0 + a0) + (-a0) \\
o &= a0 + (a0 + (-a0)) \\
o &= a0
\end{align*}
\]
Similarly, \( 0a = 0 \).

Theorem (A negative times a negative is a positive)
Let \( R \) be any ring, and \( a, b \in R \). Then \((-a)(-b) = ab\).

Proof.
We will show that \((-ab) + a(-b) = 0\), thereby proving that \(a(-b) = -(ab)\). Proving that \((-a)b = -(ab)\) would be similar, but will not be done here. Again, by the distributive property:
\[
\begin{align*}
(ab) + a(-b) &= a(b + (-b)) \\
&= a(0) \\
&= 0
\end{align*}
\]
Theorem
Let $R$ be any ring, and $a, b \in R$. Then $-(-a) = a$, $-(a + b) = -a - b$, and $-(a - b) = -a + b$.

Proof.
These facts following directly from the fact that $(R, +)$ is an abelian group. We just use the facts that we already proved about groups.

Theorem
Let $R$ be any ring with unity. Then its unity is unique.

Proof.
Let $1$ and $1'$ be unities for $R$. Then $1' = 11' = 1$.

Theorem
Let $R$ be any ring with unity and $a \in R$ be a unit. Then $a^{-1}$ is unique.

Proof.
Let $b, c \in R$ both be multiplicative inverses for $a$. Then $ab = 1 = ac$, so $ab = ac$. Then $(ba)b = (ba)c$, $1b = 1c$, and $b = c$.

Theorem (Cancellation in integral domains)
Let $D$ be an integral domain with $a, b, c \in D$ and $a \neq 0$. Then if $ab = ac$, then $b = c$.

Proof.
Suppose $ab = ac$. Then $ab - ac = 0$, and $a(b - c) = 0$. Since there are no zero-divisors, we conclude that $b - c = 0$. So $b = c$.

Example
Note that the assumption that $D$ is an integral domain is very important. If $D = \mathbb{Z}_6$ (not an integral domain), then $2(3) = 0 = 2(0)$, but $3 \neq 0$. 
Theorem
If \( D \) is a finite integral domain, then \( D \) is a field.

Proof.
We must show that every non-zero element of \( D \) has an inverse. So let \( 0 \neq a \in D \). If \( a = 1 \), then \( aa = 11 = 1 \), so \( a^{-1} = 1 = a \).
So assume \( a \neq 1 \). Then consider \( \{a, a^2, a^3, \ldots, a^{n+1}\} \) where \( n \) is the number of elements in \( D \). By the Pigeonhole Principle, there exists \( i, j \) with \( i > j \) such that \( a^i = a^j \). Then \( a^{i-j} = 1 \) by cancellation. So \( aa^{i-j-1} = 1 \), and \( a^{-1} = a^{i-j-1} \).

Theorem
Let \( p \) be a prime number. Then \( \mathbb{Z}_p \) is a field.

Proof.
By the previous theorem, it is sufficient to show that \( \mathbb{Z}_p \) has no zero divisors. Let \( a, b \in \mathbb{Z}_p \) such that \( ab = 0 \). By considering \( a \) and \( b \) to be elements of \( \mathbb{Z} \), we see that \( ab = np \) for some integer \( n \). Since \( p \) divides the right side, it also divides the left side \( ab \). But then \( p \mid a \) or \( p \mid b \). Therefore, either \( a = 0 \) or \( b = 0 \) in \( \mathbb{Z}_p \).

Theorem
Let \( R \) be a ring with unity. If \( 1 \) has finite order \( n \), then the characteristic of \( R \) is \( n \). If \( 1 \) has infinite order, then the characteristic of \( R \) is 0.

Proof.
If \( 1 \) has infinite order, then \( m(1) \neq 0 \) for any integer \( m \). Therefore, \( R \) has characteristic 0.
So suppose \( 1 \) has order \( n \), and let \( a \in R \). Consider \( na \).

\[
na = a + a + \cdots + a \\
= a(1 + 1 + \cdots + 1) \\
= a(n1) \\
= a(0)
\]

Theorem
If \( D \) is an integral domain, then the characteristic of \( D \) is either prime or zero.

Proof.
If the order of \( 1 \) is infinite, then \( D \) has characteristic 0 by the previous theorem. So suppose the order of \( 1 \) is \( n \). Further suppose that \( n = lm \) for integers \( l, m \). Then \( 0 = n(1) = (lm)(1) = (l(1))(m(1)) \).
Since \( D \) is an integral domain, either \( l(1) = 0 \) or \( m(1) = 0 \). Without loss of generality, assume \( m(1) = 0 \). Since \( n \) is the order of \( 1 \), we conclude that \( m = n \) and \( l = 1 \).
Since this is true for any \( l, m \in \mathbb{Z} \), we conclude that \( n \) is prime.
**Definition**
A subset $S$ of a ring $R$ is called a subring if $S$ is a ring under the operations of $R$.

**Example**
The ring $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

**Example**
The ring $\mathbb{Z}$ is a subring of $\mathbb{Z}[i]$.

**Theorem**
A nonempty subset $S$ of a ring $R$ is a subring if $a - b$ and $ab$ are in $S$ for all $a, b \in S$.

**Proof.**
Since $a - b \in S$ for all $a, b \in S$, $(S, +)$ is a subgroup of the group $(R, +)$ by the $ab^{-1}$ theorem from group theory. So $S$ fulfills the first five axioms for rings from the previous slide. It remains to show $ab \in S$, $a(bc) = (ab)c$, $a(b + c) = ab + ac$, and $(b + c)a = ba + ca$ for all $a, b, c \in S$.

But $ab \in S$ by assumption, and the other axioms hold for all elements $a, b, c \in R$, so they certainly hold for all elements of $S$. 

**Example**
The set $\{0, 3\}$ is a subring of $\mathbb{Z}_6$ and $3$ is the unity!

**Example**
The set $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ with $a, b \in \mathbb{Z}$ is a subring of $M_2(\mathbb{Z})$.

**Example**
Let $R$ be any ring. Then $R$ and $\{0\}$ are subrings of $R$. 

Bret Benesh  Rings and Integral Domains (Chapters 12 and 13)