Algebraic structures

*A group* is a set $G$ with a binary operation $\ast$ satisfying associativity, and the existence of an identity and inverses.
Algebraic structures

* A **group** is a set $G$ with a binary operation $\star$ satisfying associativity, and the existence of an identity and inverses.
* A **monoid** is a set $M$ with a binary operation $\star$ satisfying associativity and the existence of an identity. (e.g. $(\mathbb{Z}, \times)$)
Algebraic structures

* A **group** is a set $G$ with a binary operation $\star$ satisfying associativity, and the existence of an identity and inverses.

* A **monoid** is a set $M$ with a binary operation $\star$ satisfying associativity and the existence of an identity. (e.g. $(\mathbb{Z}, \times)$)

* A **semigroup** is a set $S$ with a binary operation $\star$ satisfying associativity (e.g. $(\mathbb{Z}_{>0}, +)$).
Algebraic structures

* A group is a set $G$ with a binary operation $\ast$ satisfying associativity, and the existence of an identity and inverses.
* A monoid is a set $M$ with a binary operation $\ast$ satisfying associativity and the existence of an identity. (e.g. $(\mathbb{Z}, \times)$)
* A semigroup is a set $S$ with a binary operation $\ast$ satisfying associativity (e.g. $(\mathbb{Z}_{>0}, +)$).
* A field is a set $F$ with two binary operations, $+$ and $\times$, such that $(F, +)$ and $(F - \{0\}, \times)$ are abelian groups, and the distributive property holds between $+$ and $\times$. (e.g. $\mathbb{R}$ or $\mathbb{Z}/p\mathbb{Z}$)
Algebraic structures

* A **group** is a set $G$ with a binary operation $\star$ satisfying associativity, and the existence of an identity and inverses.

* A **monoid** is a set $M$ with a binary operation $\star$ satisfying associativity and the existence of an identity. (e.g. $(\mathbb{Z}, \times)$)

* A **semigroup** is a set $S$ with a binary operation $\star$ satisfying associativity (e.g. $(\mathbb{Z}_{>0}, +)$).

* A **field** is a set $F$ with two binary operations, $+$ and $\times$, such that $(F, +)$ and $(F - \{0\}, \times)$ are abelian groups, and the distributive property holds between $+$ and $\times$. (e.g. $\mathbb{R}$ or $\mathbb{Z}/p\mathbb{Z}$)

* A **vector space** (over a field $F$) is a an abelian group $(V, +)$ that has a faithful action on it by $F$ that satisfies the distributive properties. (i.e. for $f \in F$, $u, v \in V$, $f \cdot (u + v) = f \cdot u + f \cdot v$). (e.g. $F = \mathbb{R}$, $V = \mathbb{R}^n$)
Algebraic structures

* A **group** is a set $G$ with a binary operation $\star$ satisfying associativity, and the existence of an identity and inverses.
* A **monoid** is a set $M$ with a binary operation $\star$ satisfying associativity and the existence of an identity. (e.g. $(\mathbb{Z}, \times)$)
* A **semigroup** is a set $S$ with a binary operation $\star$ satisfying associativity (e.g. $(\mathbb{Z}_{>0}, +)$).
* A **field** is a set $F$ with two binary operations, $+$ and $\times$, such that $(F, +)$ and $(F - \{0\}, \times)$ are abelian groups, and the distributive property holds between $+$ and $\times$. (e.g. $\mathbb{R}$ or $\mathbb{Z}/p\mathbb{Z}$)
* A **vector space** (over a field $F$) is a an abelian group $(V, +)$ that has a faithful action on it by $F$ that satisfies the distributive properties. (i.e. for $f \in F, u, v \in V, f \cdot (u + v) = f \cdot u + f \cdot v$). (e.g. $F = \mathbb{R}, V = \mathbb{R}^n$)
* A **ring** (with identity) is a set $R$ with two binary operations, $+$ and $\times$, such that $(R, +)$ is an abelian group, and $(R, \times)$ is a monoid, and the distributive property holds. (e.g. $\mathbb{Z}$ or $\mathbb{Z}[x]$)
Algebraic structures

* A **group** is a set $G$ with a binary operation $\ast$ satisfying associativity, and the existence of an identity and inverses.

* A **monoid** is a set $M$ with a binary operation $\ast$ satisfying associativity and the existence of an identity. (e.g. $(\mathbb{Z}, \times)$)

* A **semigroup** is a set $S$ with a binary operation $\ast$ satisfying associativity (e.g. $(\mathbb{Z}_{\geq 0}, +)$).

* A **field** is a set $F$ with two binary operations, $+$ and $\times$, such that $(F, +)$ and $(F - \{0\}, \times)$ are abelian groups, and the distributive property holds between $+$ and $\times$. (e.g. $\mathbb{R}$ or $\mathbb{Z}/p\mathbb{Z}$)

* A **vector space** (over a field $F$) is a an abelian group $(V, +)$ that has a faithful action on it by $F$ that satisfies the distributive properties. (i.e. for $f \in F, \ u, \ v \in V, f \cdot (u + v) = f \cdot u + f \cdot v$). (e.g. $F = \mathbb{R}, \ V = \mathbb{R}^n$)

* A **ring** (with identity) is a set $R$ with two binary operations, $+$ and $\times$, such that $(R, +)$ is an abelian group, and $(R, \times)$ is a monoid, and the distributive property holds. (e.g. $\mathbb{Z}$ or $\mathbb{Z}[x]$)

* An **algebra** (over a field $F$) is a ring $A$ such that $(A, +)$ forms a vector space over $F$ and the distributive properties hold. (e.g. $F = \mathbb{R}, \ A = \mathbb{R}[x]$)
Algebraic structures

* A **group** is a set $G$ with a binary operation $\ast$ satisfying associativity, and the existence of an identity and inverses.

* A **monoid** is a set $M$ with a binary operation $\ast$ satisfying associativity and the existence of an identity. (e.g. $(\mathbb{Z}, \times)$)

* A **semigroup** is a set $S$ with a binary operation $\ast$ satisfying associativity (e.g. $(\mathbb{Z}_{>0}, +)$).

* A **field** is a set $F$ with two binary operations, $+$ and $\times$, such that $(F, +)$ and $(F - \{0\}, \times)$ are abelian groups, and the distributive property holds between $+$ and $\times$. (e.g. $\mathbb{R}$ or $\mathbb{Z}/p\mathbb{Z}$)

* A **vector space** (over a field $F$) is a an abelian group $(V, +)$ that has a faithful action on it by $F$ that satisfies the distributive properties. (i.e. for $f \in F$, $u, v \in V$, $f \cdot (u + v) = f \cdot u + f \cdot v$). (e.g. $F = \mathbb{R}$, $V = \mathbb{R}^n$)

* A **ring** (with identity) is a set $R$ with two binary operations, $+$ and $\times$, such that $(R, +)$ is an abelian group, and $(R, \times)$ is a monoid, and the distributive property holds. (e.g. $\mathbb{Z}$ or $\mathbb{Z}[x]$)

* An **algebra** (over a field $F$) is a ring $A$ such that $(A, +)$ forms a vector space over $F$ and the distributive properties hold. (e.g. $F = \mathbb{R}$, $A = \mathbb{R}[x]$)

* A **module** (over a ring $R$) is an abelian group $(M, +)$ with an action from $R$ that satisfies the distributive properties. (e.g. $R = \mathbb{Z}$ acts on $M = \mathbb{Z}/n\mathbb{Z}$ by multiplication)
Algebraic structures

* A group is a set $G$ with a binary operation $\star$ satisfying associativity, and the existence of an identity and inverses.

* A monoid is a set $M$ with a binary operation $\star$ satisfying associativity and the existence of an identity. (e.g. $(\mathbb{Z}, \times)$)

* A semigroup is a set $S$ with a binary operation $\star$ satisfying associativity (e.g. $(\mathbb{Z}_{>0}, +)$).

* A field is a set $F$ with two binary operations, $+$ and $\times$, such that $(F, +)$ and $(F - \{0\}, \times)$ are abelian groups, and the distributive property holds between $+$ and $\times$. (e.g. $\mathbb{R}$ or $\mathbb{Z}/p\mathbb{Z}$)

* A vector space (over a field $F$) is a an abelian group $(V, +)$ that has a faithful action on it by $F$ that satisfies the distributive properties. (i.e. for $f \in F, u, v \in V, f \cdot (u + v) = f \cdot u + f \cdot v$). (e.g. $F = \mathbb{R}, V = \mathbb{R}^n$)

* A ring (with identity) is a set $R$ with two binary operations, $+$ and $\times$, such that $(R, +)$ is an abelian group, and $(R, \times)$ is a monoid, and the distributive property holds. (e.g. $\mathbb{Z}$ or $\mathbb{Z}[x]$)

* An algebra (over a field $F$) is a ring $A$ such that $(A, +)$ forms a vector space over $F$ and the distributive properties hold. (e.g. $F = \mathbb{R}, A = \mathbb{R}[x]$)

* A module (over a ring $R$) is an abelian group $(M, +)$ with an action from $R$ that satisfies the distributive properties. (e.g. $R = \mathbb{Z}$ acts on $M = \mathbb{Z}/n\mathbb{Z}$ by multiplication) ...and many many others.
Relating different algebraic structures:

one binary operation

A **semigroup** is a set $S$ with a binary operation $\star$ satisfying associativity.

A **monoid** is a semigroup $(M, \star)$ that has an identity element.

A **group** is a monoid $(G, \star)$ that has an inverse for every element.

\[
\{ \text{groups} \} \subset \{ \text{monoids} \} \subset \{ \text{semigroups} \}
\]
Relating different algebraic structures: two binary operations

A ring (with identity) is a set $R$ with two binary operations, $+$ and $\times$, such that $(R, +)$ is an abelian group, and $(R, \times)$ is a monoid, and the distributive property holds.

A field is a ring $R$ where $(R - \{0\}, \times)$ is an abelian group.

An algebra (over a field $F$) is a ring $A$ such that $(A, +)$ forms a vector space over $F$ and the distributive properties hold.

\[
\{ \text{fields} \} \subset \{ \text{rings w/ 1} \} \subset \{ \text{groups} \}
\]

\[
\{ \text{algebras} \} \subset \{ \text{rings w/ 1} \} \subset \{ \text{groups} \}
\]
Relating different algebraic structures: actions

A vector space (over a field $F$) is a an abelian group $(V, +)$ that has a faithful action on it by $F$ that satisfies the distributive properties.

An algebra (over a field $F$) is a ring $A$ such that $(A, +)$ forms a vector space over $F$ and the distributive properties hold.

A module (over a ring $R$) is an abelian group $(M, +)$ with an action from $R$ that satisfies the distributive properties.

\[
\{ \text{algebras} \} \subset \{ \text{vector spaces} \} \subset \{ \text{modules} \} \subset \{ \text{groups} \}
\]
A ring $R$ is a set together with two binary operations $+$ and $\times$ such that

(a) $(R, +)$ is an abelian group,
(b) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$,  
   (i.e. $(R, \times)$ is a semigroup)
(c) the distributive laws hold for $R$

$$(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c).$$
PART II: RING THEORY

A ring $R$ is a set together with two binary operations $+$ and $\times$ such that

(a) $(R, +)$ is an abelian group,
(b) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$,
    (i.e. $(R, \times)$ is a semigroup)
(c) the distributive laws hold for $R$

$$(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c).$$

The ring $R$ is said to have an identity (R is a ring with identity) if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \quad \text{for all} \ a \in R.$$  
    (i.e. $(R, \times)$ is a monoid)
A ring $R$ is a set together with two binary operations $+$ and $\times$ such that

(a) $(R, +)$ is an abelian group,
(b) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$,  
(i.e. $(R, \times)$ is a semigroup)
(c) the *distributive laws* hold for $R$

$$(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c).$$

The ring $R$ is said to have an identity ($R$ is a ring with identity) if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \quad \text{for all} \ a \in R.$$  
(i.e. $(R, \times)$ is a monoid)

A ring $R$ is a division ring if $(R - \{0\}, \times)$ is a group.  
(i.e. $R$ has 1 and multiplicative inverses)
A ring \( R \) is a set together with two binary operations \(+\) and \(\times\) such that

(a) \((R, +)\) is an abelian group,

(b) \(\times\) is associative: \((a \times b) \times c = a \times (b \times c)\),

\(\text{(i.e. } (R, \times) \text{ is a semigroup)}\)

(c) the **distributive laws** hold for \( R \)

\[(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c).\]

The ring \( R \) is said to have an **identity** (\( R \) is a **ring with identity**) if there is an element \(1 \in R\) with

\[1 \times a = a \times 1 = a \quad \text{for all } a \in R.\]

\(\text{(i.e. } (R, \times) \text{ is a monoid)}\)

A ring \( R \) is a **division ring** if \((R - \{0\}, \times)\) is a group.

\(\text{(i.e. } R \text{ has 1 and multiplicative inverses)}\)

A ring \( R \) is **commutative** if \((R, \times)\) is commutative.
PART II: RING THEORY

A ring \( R \) is a set together with two binary operations \( + \) and \( \times \) such that

(a) \((R,+)\) is an abelian group,
(b) \(\times\) is associative: \((a \times b) \times c = a \times (b \times c)\),

(c) the distributive laws hold for \( R \)

\[
(a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c). \]

The ring \( R \) is said to have an identity (\( R \) is a ring with identity) if there is an element \( 1 \in R \) with

\[
1 \times a = a \times 1 = a \quad \text{for all} \ a \in R. \]

A ring \( R \) is a division ring if \((R - \{0\}, \times)\) is a group.

A ring \( R \) is commutative if \((R, \times)\) is commutative.

A commutative division ring is a field.
A ring $R$ is a set together with two binary operations $+$ and $\times$ such that

(a) $(R, +)$ is an abelian group,
(b) $\times$ is associative: $(a \times b) \times c = a \times (b \times c)$,  
   (i.e. $(R, \times)$ is a semigroup)
(c) the distributive laws hold for $R$

$$ (a + b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b + c) = (a \times b) + (a \times c). $$

The ring $R$ is said to have an identity ($R$ is a ring with identity) if there is an element $1 \in R$ with

$$ 1 \times a = a \times 1 = a \quad \text{for all} \quad a \in R. $$

(i.e. $(R, \times)$ is a monoid)

A ring $R$ is a division ring if $(R - \{0\}, \times)$ is a group.  
(i.e. $R$ has 1 and multiplicative inverses)

A ring $R$ is commutative if $(R, \times)$ is commutative.

A commutative division ring is a field.

We usually write $ab$ instead of $a \times b$.  

Some favorite examples

1. Since $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields, they are also rings, rings with 1, commutative rings, and division rings.
Some favorite examples

1. Since \( \mathbb{Z}/p\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) are all fields, they are also rings, rings with 1, commutative rings, and division rings.

2. \( \mathbb{Z} \) and \( \mathbb{Z}/n\mathbb{Z} \) are commutative rings with 1, but not a division rings.
Some favorite examples

1. Since $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields, they are also rings, rings with 1, commutative rings, and division rings.

2. $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are commutative rings with 1, but not a division rings.

3. $M_n(F) = \{n \times n \text{ matrices with entries in the field } F\}$ is a ring with 1. It is not commutative, nor is it a division ring.
Some favorite examples

1. Since $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields, they are also rings, rings with 1, commutative rings, and division rings.

2. $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are commutative rings with 1, but not a division rings.

3. $M_n(F) = \{n \times n$ matrices with entries in the field $F\}$ is a ring with 1. It is not commutative, nor is it a division ring. In fact, $M_n(R)$ is a ring for $R$ a ring as well.
Some favorite examples

1. Since \( \mathbb{Z}/p\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \) and \( \mathbb{C} \) are all fields, they are also rings, rings with 1, commutative rings, and division rings.

2. \( \mathbb{Z} \) and \( \mathbb{Z}/n\mathbb{Z} \) are commutative rings with 1, but not a division rings.

3. \( M_n(F) = \{n \times n \text{ matrices with entries in the field } F\} \) is a ring with 1. It is not commutative, nor is it a division ring. In fact, \( M_n(R) \) is a ring for \( R \) a ring as well.

4. If \( R \) is a commutative ring, then so are polynomials: \( R[x] = \{r_0 + r_1x + \cdots + r_nx^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0}\} \), power series: \( R[[x]] = \{r_0 + r_1x + \cdots \mid r_i \in R\} \), Laurent polynomials: \( R[x, x^{-1}] = \{r_mx^m + r_{m+1}x^{m+1} + \cdots + r_nx^n \mid r_i \in R, m \leq n \in \mathbb{Z}\} \), Laurent series: \( R((x)) = \{r_mx^m + r_{m+1}x^{m+1} + \cdots \mid r_i \in R, m \in \mathbb{Z}\} \).
Some favorite examples

1. Since $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields, they have also rings, rings with 1, commutative rings, and division rings.

2. $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are commutative rings with 1, but not a division ring.

3. $M_n(F) = \{n \times n$ matrices with entries in the field $F\}$ is a ring with 1. It is not commutative, nor is it a division ring. In fact, $M_n(R)$ is a ring for $R$ a ring as well.

4. If $R$ is a commutative ring, then so are polynomials:

$$R[x] = \{r_0 + r_1 x + \cdots + r_n x^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0}\},$$

power series:

$$R[[x]] = \{r_0 + r_1 x + \cdots \mid r_i \in R\},$$

Laurent polynomials:

$$R[x, x^{-1}] = \{r_m x^m + r_{m+1} x^{m+1} + \cdots + r_n x^n \mid r_i \in R, m \leq n \in \mathbb{Z}\},$$

Laurent series:

$$R((x)) = \{r_m x^m + r_{m+1} x^{m+1} + \cdots \mid r_i \in R, m \in \mathbb{Z}\}.$$

Tip: For every new definition or theorem, ask yourself what it means for

$$\mathbb{R}, \mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, M_2(\mathbb{R}), \mathbb{R}[x], \mathbb{Z}[x], \text{ and } \mathbb{Z}/6\mathbb{Z}[x].$$
Some favorite examples

3. For a field $F$, $M_n(F) = \{n \times n$ matrices with entries in $F\}$.

4. For a commutative ring $R$,
   $$R[x] = \{r_0 + r_1 x + \cdots + r_n x^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0}\}.$$
Some favorite examples

3. For a field $F$, $M_n(F) = \{n \times n \text{ matrices with entries in } F\}$.

4. For a commutative ring $R$,
   \[ R[x] = \{r_0 + r_1 x + \cdots + r_n x^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0}\}. \]

Note that $M_n(F)$ and $R[x]$ are both rings whose elements are functions. In both examples, the binary operation $+$ is function addition:

\[(M_1 + M_2)(v) = M_1(v) + M_2(v) \text{ and } (f + g)(x) = f(x) + g(x).\]
Some favorite examples

3. For a field $F$, $M_n(F) = \{n \times n \text{ matrices with entries in } F\}$.

4. For a commutative ring $R$,
   
   $$R[x] = \{r_0 + r_1 x + \cdots + r_n x^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0}\}.$$

Note that $M_n(F)$ and $R[x]$ are both rings whose elements are functions. In both examples, the binary operation $+$ is function addition:

- $(M_1 + M_2)(v) = M_1(v) + M_2(v)$ and $(f + g)(x) = f(x) + g(x)$.

(Ok because the images of the functions are additive groups.)
Some favorite examples

3. For a field $F$, $M_n(F) = \{n \times n$ matrices with entries in $F\}$.

4. For a commutative ring $R$, 
   \[ R[x] = \{r_0 + r_1 x + \cdots + r_n x^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0}\}. \]

Note that $M_n(F)$ and $R[x]$ are both rings whose elements are functions. In both examples, the binary operation $+$ is function addition:

\[ (M_1 + M_2)(v) = M_1(v) + M_2(v) \] and \[ (f + g)(x) = f(x) + g(x). \]
(Ok because the images of the functions are additive groups.)

However, the binary operation playing the role of $\times$ is fundamentally different between the two examples!
Some favorite examples

3. For a field $F$, $M_n(F) = \{n \times n$ matrices with entries in $F\}$.

4. For a commutative ring $R$,
   $$R[x] = \{r_0 + r_1 x + \cdots + r_n x^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0}\}.$$ 

Note that $M_n(F)$ and $R[x]$ are both rings whose elements are functions. 

In both examples, the binary operation $+$ is function addition:

$$(M_1 + M_2)(v) = M_1(v) + M_2(v) \text{ and } (f + g)(x) = f(x) + g(x).$$

(Ok because the images of the functions are additive groups.)

However, the binary operation playing the role of $\times$ is fundamentally different between the two examples!

In $M_n(F)$, “multiplication” is function composition:

matrix multiplication is the same as linear function composition, 

i.e. $(M_1 M_2)(v) = M_1(M_2(v))$. 
Some favorite examples

3. For a field $F$, $M_n(F) = \{n \times n \text{ matrices with entries in } F\}$.

4. For a commutative ring $R$,
   
   $R[x] = \{r_0 + r_1 x + \cdots + r_n x^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0}\}$.

Note that $M_n(F)$ and $R[x]$ are both rings whose elements are functions. In both examples, the binary operation $+$ is function addition:

$(M_1 + M_2)(v) = M_1(v) + M_2(v)$ and $(f + g)(x) = f(x) + g(x)$.

(Ok because the images of the functions are additive groups.)

However, the binary operation playing the role of $\times$ is fundamentally different between the two examples!

In $M_n(F)$, “multiplication” is function composition:

matrix multiplication is the same as linear function composition, i.e. $(M_1M_2)(v) = M_1(M_2(v))$.

But in $R[x]$, “multiplication” is function multiplication:

the image of the product is the product of the images, i.e. $(fg)(x) = f(x)g(x)$.
Some favorite examples

3. For a field $F$, $M_n(F) = \{n \times n$ matrices with entries in $F\}$.

4. For a commutative ring $R$,
   
   $R[x] = \{r_0 + r_1 x + \cdots + r_n x^n \mid r_i \in R, n \in \mathbb{Z}_{\geq 0}\}$.

Note that $M_n(F)$ and $R[x]$ are both rings whose elements are functions. In both examples, the binary operation $+$ is function addition:

$(M_1 + M_2)(v) = M_1(v) + M_2(v)$ and $(f + g)(x) = f(x) + g(x)$.

(Ok because the images of the functions are additive groups.)

However, the binary operation playing the role of $\times$ is fundamentally different between the two examples!

In $M_n(F)$, “multiplication” is function composition:

matrix multiplication is the same as linear function composition, i.e. $(M_1 M_2)(v) = M_1(M_2(v))$.

But in $R[x]$, “multiplication” is function multiplication:

the image of the product is the product of the images, i.e. $(fg)(x) = f(x)g(x)$.

(Can’t do this unless the image of the functions is a ring!)
Rings of functions

In general, let $A$ be a ring, and let $X$ be a set. Then the set of functions $R = \{ f : X \rightarrow A \}$ is a ring under the binary operations

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x).$$
Rings of functions

In general, let $A$ be a ring, and let $X$ be a set. Then the set of functions $R = \{ f : X \to A \}$ is a ring under the binary operations

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (f g)(x) = f(x)g(x). \quad (*)$$

If $A$ has 1, then so does $R$, given by $1_R : x \mapsto 1.$
Rings of functions

In general, let $A$ be a ring, and let $X$ be a set. Then the set of functions $R = \{ f : X \to A \}$ is a ring under the binary operations

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x).$$

(*)

If $A$ has 1, then so does $R$, given by $1_R : x \mapsto 1$.
If $A$ is commutative, then so is $R$. 

A subring of the $A$ is a subgroup of $R$ that is closed under multiplication.

Think: what are some subrings of our favorite examples?

Subring criterion: $S \subseteq R$ is a subring iff $S \neq \emptyset$, and $S$ is closed under subtraction and multiplication.
Rings of functions

In general, let $A$ be a ring, and let $X$ be a set. Then the set of functions $R = \{ f : X \to A \}$ is a ring under the binary operations

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x). \quad (*)$$

If $A$ has 1, then so does $R$, given by $1_R : x \mapsto 1$.
If $A$ is commutative, then so is $R$.
However, the only those functions for which $f(x) \neq 0 \ \forall x \in X$ are multiplicatively invertible, so $R$ is never a division ring.
Rings of functions

In general, let \( A \) be a ring, and let \( X \) be a set. Then the set of functions \( R = \{ f : X \to A \} \) is a ring under the binary operations

\[
(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x). \quad (\ast)
\]

If \( A \) has 1, then so does \( R \), given by \( 1_R : x \mapsto 1 \).

If \( A \) is commutative, then so is \( R \).

However, the only those functions for which \( f(x) \neq 0 \ \forall x \in X \) are multiplicatively invertible, so \( R \) is never a division ring.

Putting restrictions on the kinds of functions in your set can sometimes also produce rings (e.g. polynomial functions).
Rings of functions

In general, let $A$ be a ring, and let $X$ be a set. Then the set of functions $R = \{ f : X \rightarrow A \}$ is a ring under the binary operations

\[(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x). \quad (*)\]

Putting restrictions on the kinds of functions in your set can sometimes also produce rings (e.g. polynomial functions).

Example: Which of the following form rings under the binomial operations given in $(*)$? Why or why not?

(a) \{ differentiable functions $\mathbb{R} \rightarrow \mathbb{R}$ \} \hspace{1cm} (\text{$f'(x)$ is defined $\forall x \in \mathbb{R}$})
(b) \{ even functions $\mathbb{R} \rightarrow \mathbb{R}$ \} \hspace{1cm} (\text{$f(-x) = f(x) \ \forall x \in \mathbb{R}$})
(c) \{ odd functions $\mathbb{R} \rightarrow \mathbb{R}$ \} \hspace{1cm} (\text{$f(-x) = -f(x) \ \forall x \in \mathbb{R}$})
(d) \{ strictly positive functions $\mathbb{R} \rightarrow \mathbb{R}$ \} \hspace{1cm} (\text{$f(x) > 0 \ \forall x \in \mathbb{R}$})
(e) \{ non-zero functions $\mathbb{R} \rightarrow \mathbb{R}$ \} \hspace{1cm} (\text{$f(x) \neq 0 \ \forall x \in \mathbb{R}$})

A subring of a ring $R$ is a subgroup of $R$ that is closed under multiplication.

Think: what are some subrings of our favorite examples?

Subring criterion: $S \subseteq R$ is a subring iff $S$ is closed under subtraction and multiplication.
Rings of functions

In general, let $A$ be a ring, and let $X$ be a set. Then the set of functions $R = \{ f : X \to A \}$ is a ring under the binary operations

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (f g)(x) = f(x) g(x). \quad (\ast)$$

Putting restrictions on the kinds of functions in your set can sometimes also produce rings (e.g. polynomial functions).

Example: Which of the following form rings under the binomial operations given in $(\ast)$? Why or why not?

(a) $\{ \text{differentiable functions } \mathbb{R} \to \mathbb{R} \}$ \hspace{2cm} ($f'(x)$ is defined $\forall x \in \mathbb{R}$)

(b) $\{ \text{even functions } \mathbb{R} \to \mathbb{R} \}$ \hspace{2cm} ($f(-x) = f(x) \forall x \in \mathbb{R}$)

(c) $\{ \text{odd functions } \mathbb{R} \to \mathbb{R} \}$ \hspace{2cm} ($f(-x) = -f(x) \forall x \in \mathbb{R}$)

(d) $\{ \text{strictly positive functions } \mathbb{R} \to \mathbb{R} \}$ \hspace{2cm} ($f(x) > 0 \forall x \in \mathbb{R}$)

(e) $\{ \text{non-zero functions } \mathbb{R} \to \mathbb{R} \}$ \hspace{2cm} ($f(x) \neq 0 \forall x \in \mathbb{R}$)

A subring of the ring $R$ is a subgroup of $R$ that is closed under multiplication.
Rings of functions

In general, let $A$ be a ring, and let $X$ be a set. Then the set of functions $R = \{ f : X \to A \}$ is a ring under the binary operations

\[(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x). \quad (*)\]

Putting restrictions on the kinds of functions in your set can sometimes also produce rings (e.g. polynomial functions).

**Example:** Which of the following form rings under the binomial operations given in $(*)$? Why or why not?

(a) \{ differentiable functions $\mathbb{R} \to \mathbb{R}$ \} \quad (f'(x) \text{ is defined } \forall x \in \mathbb{R})

(b) \{ even functions $\mathbb{R} \to \mathbb{R}$ \} \quad (f(-x) = f(x) \forall x \in \mathbb{R})

(c) \{ odd functions $\mathbb{R} \to \mathbb{R}$ \} \quad (f(-x) = -f(x) \forall x \in \mathbb{R})

(d) \{ strictly positive functions $\mathbb{R} \to \mathbb{R}$ \} \quad (f(x) > 0 \forall x \in \mathbb{R})

(e) \{ non-zero functions $\mathbb{R} \to \mathbb{R}$ \} \quad (f(x) \neq 0 \forall x \in \mathbb{R})

A **subring** of the a $R$ is a subgroup of $R$ that is closed under multiplication. **Think:** what are some subrings of our fav examples?
**Rings of functions**

In general, let $A$ be a ring, and let $X$ be a set. Then the set of functions $R = \{ f : X \to A \}$ is a ring under the binary operations

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x). \quad (*)$$

Putting restrictions on the kinds of functions in your set can sometimes also produce rings (e.g. polynomial functions).

**Example**: Which of the following form rings under the binomial operations given in $(*)$? Why or why not?

(a) $\{ \text{differentiable functions } \mathbb{R} \to \mathbb{R} \}$  \hspace{1cm} ($f'(x)$ is defined $\forall x \in \mathbb{R}$)

(b) $\{ \text{even functions } \mathbb{R} \to \mathbb{R} \}$  \hspace{1cm} ($f(-x) = f(x) \forall x \in \mathbb{R}$)

(c) $\{ \text{odd functions } \mathbb{R} \to \mathbb{R} \}$  \hspace{1cm} ($f(-x) = -f(x) \forall x \in \mathbb{R}$)

(d) $\{ \text{strictly positive functions } \mathbb{R} \to \mathbb{R} \}$  \hspace{1cm} ($f(x) > 0 \forall x \in \mathbb{R}$)

(e) $\{ \text{non-zero functions } \mathbb{R} \to \mathbb{R} \}$  \hspace{1cm} ($f(x) \neq 0 \forall x \in \mathbb{R}$)

A **subring** of the a $R$ is a subgroup of $R$ that is closed under multiplication. **Think**: what are some subrings of our fav examples?

Subring criterion:
Rings of functions

In general, let $A$ be a ring, and let $X$ be a set. Then the set of functions $R = \{ f : X \rightarrow A \}$ is a ring under the binary operations

$$ (f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x). \quad (*) $$

Putting restrictions on the kinds of functions in your set can sometimes also produce rings (e.g. polynomial functions).

**Example:** Which of the following form rings under the binomial operations given in $(*)$? Why or why not?

(a) $\{ \text{differentiable functions } \mathbb{R} \rightarrow \mathbb{R} \}$ \quad ($f'(x)$ is defined $\forall x \in \mathbb{R}$)

(b) $\{ \text{even functions } \mathbb{R} \rightarrow \mathbb{R} \}$ \quad ($f(-x) = f(x) \ \forall x \in \mathbb{R}$)

(c) $\{ \text{odd functions } \mathbb{R} \rightarrow \mathbb{R} \}$ \quad ($f(-x) = -f(x) \ \forall x \in \mathbb{R}$)

(d) $\{ \text{strictly positive functions } \mathbb{R} \rightarrow \mathbb{R} \}$ \quad ($f(x) > 0 \ \forall x \in \mathbb{R}$)

(e) $\{ \text{non-zero functions } \mathbb{R} \rightarrow \mathbb{R} \}$ \quad ($f(x) \neq 0 \ \forall x \in \mathbb{R}$)

A subring of the a $R$ is a subgroup of $R$ that is closed under multiplication. **Think:** what are some subrings of our fav examples?

**Subring criterion:** $S \subseteq R$ is a subring iff $S \neq \emptyset$, and $S$ is closed under subtraction and multiplication.
Mixing the two binary operations

As usual, we denote

0 is the additive identity,  
1 is the multiplicative identity (if it exists),  
\(-a\) is the additive inverse to \(a\), and  
\(a^{-1}\) is the multiplicative inverse to \(a\) (if it exists).
Mixing the two binary operations

As usual, we denote

- $0$ is the additive identity,
- $1$ is the multiplicative identity (if it exists),
- $-a$ is the additive inverse to $a$, and
- $a^{-1}$ is the multiplicative inverse to $a$ (if it exists).

Proposition

Let $R$ be a ring.

1. $0a = a0 = 0$ for all $a \in R$.
2. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.
3. $(-a)(-b) = ab$ for all $a, b \in R$.
4. If $R$ has an identity $1$, the identity is unique and $-a = (-1)a$. 
Definition
Let $R$ be a ring.

1. A nonzero element $a \in R$ is called a zero divisor if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$. 

Think: what are some zero divisors of our fav examples?

2. Assume $R$ has identity $1 \neq 0$. An element $u \in R$ is called a unit in $R$ if there is some $v \in R$ such that $uv = vu = 1$.

The set of units $R^\times$ is a group (under $\cdot$) called group of units of $R$.

Think: what are the groups of units in our fav examples?

3. A commutative ring with identity $1 \neq 0$ is called an integral domain if it has no zero divisors.

Think: which our fav examples are integral domains?
Definition

Let $R$ be a ring.

1. A nonzero element $a \in R$ is called a zero divisor if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.

Think: what are some zero divisors of our fav examples?

2. Assume $R$ has identity $1 \neq 0$. An element $u \in R$ is called a unit in $R$ if there is some $v \in R$ such that $uv = vu = 1$.

The set of units $R^\times$ is a group (under $\cdot$) called group of units of $R$.

Think: what are the groups of units in our fav examples?

3. A commutative ring with identity $1 \neq 0$ is called an integral domain if it has no zero divisors.

Think: which our fav examples are integral domains?
Definition
Let $R$ be a ring.

1. A nonzero element $a \in R$ is called a zero divisor if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.
   
   Think: what are some zero divisors of our fav examples?

2. Assume $R$ has identity $1 \neq 0$. An element $u \in R$ is called a unit in $R$ if there is some $v \in R$ such that $uv = vu = 1$. 


Definition
Let $R$ be a ring.

1. A nonzero element $a \in R$ is called a zero divisor if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.
   
   Think: what are some zero divisors of our fav examples?

2. Assume $R$ has identity $1 \neq 0$. An element $u \in R$ is called a unit in $R$ if there is some $v \in R$ such that $uv = vu = 1$.
   
   The set of units $R^\times$ is a group (under $\times$) called group of units of $R$. 

Definition
Let $R$ be a ring.

1. A nonzero element $a \in R$ is called a **zero divisor** if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.
   
   **Think:** what are some zero divisors of our fav examples?

2. Assume $R$ has identity $1 \neq 0$. An element $u \in R$ is called a **unit** in $R$ if there is some $v \in R$ such that $uv = vu = 1$.
   The set of units $R^\times$ is a group (under $\times$) called **group of units** of $R$.
   
   **Think:** what are the groups of units in our fav examples?
Definition
Let $R$ be a ring.

1. A nonzero element $a \in R$ is called a zero divisor if there is a nonzero element $b \in R$ such that $ab = 0$ or $ba = 0$.
   
   Think: what are some zero divisors of our fav examples?

2. Assume $R$ has identity $1 \neq 0$. An element $u \in R$ is called a unit in $R$ if there is some $v \in R$ such that $uv = vu = 1$.
   The set of units $R^\times$ is a group (under $\times$) called group of units of $R$.
   
   Think: what are the groups of units in our fav examples?

3. A commutative ring with identity $1 \neq 0$ is called an integral domain if it has no zero divisors.
Definition
Let \( R \) be a ring.

1. A nonzero element \( a \in R \) is called a zero divisor if there is a nonzero element \( b \in R \) such that \( ab = 0 \) or \( ba = 0 \).
   
   Think: what are some zero divisors of our fav examples?

2. Assume \( R \) has identity \( 1 \neq 0 \). An element \( u \in R \) is called a unit in \( R \) if there is some \( v \in R \) such that \( uv = vu = 1 \).
   
   The set of units \( R^\times \) is a group (under \( \times \)) called group of units of \( R \).
   
   Think: what are the groups of units in our fav examples?

3. A commutative ring with identity \( 1 \neq 0 \) is called an integral domain if it has no zero divisors.
   
   Think: which our fav examples are integral domains?
Proposition

Let $R$ be a ring and $a, b, c \in R$ such that $a$ is not a zero divisor. If $ab = ac$, then $a = 0$ or $b = c$. ("zero divisors are bad for cancellation")
If particular, if $R$ is an integral domain and $ab = ac$, then $a = 0$ or $b = c$. ("cancellation always works in integral domains")
Proposition

Let $R$ be a ring and $a, b, c \in R$ such that $a$ is not a zero divisor.
If $ab = ac$, then $a = 0$ or $b = c$. (“zero divisors are bad for cancellation”)
If particular, if $R$ is an integral domain and $ab = ac$,
then $a = 0$ or $b = c$. (“cancellation always works in integral domains”)

Corollary

Any finite integral domain is a field.
More on polynomial rings

Definition
Let $R$ be a commutative ring with identity. The formal sum

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $n \geq 0$ and each $a_i \in R$ is called a polynomial in $x$ with coefficients $a_i$ in $R$. 
More on polynomial rings

Definition
Let $R$ be a commutative ring with identity. The formal sum

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

with $n \geq 0$ and each $a_i \in R$ is called a polynomial in $x$ with coefficients $a_i$ in $R$.

If $a_n \neq 0$, the polynomial is of degree $n$, $a_n x^n$ is the leading term and $a_n$ is the leading coefficient. The polynomial is monic if $a_n = 1$. 
More on polynomial rings

Definition
Let $R$ be a commutative ring with identity. The formal sum

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $n \geq 0$ and each $a_i \in R$ is called a polynomial in $x$ with coefficients $a_i$ in $R$.
If $a_n \neq 0$, the polynomial is of degree $n$, $a_n x^n$ is the leading term and $a_n$ is the leading coefficient. The polynomial is monic if $a_n = 1$.
The set of all such polynomials is the ring of polynomials in the $x$ with coefficients in $R$, denoted $R[x]$. The ring $R$ appears in $R[x]$ as the constant polynomials.
More on polynomial rings

If \( R \) is not an integral domain, then neither is \( R[x] \).
More on polynomial rings

If $R$ is not an integral domain, then neither is $R[x]$.

If $S \leq R$ is a subring, then $S[x] \leq R[x]$ is a subring.
More on polynomial rings

If $R$ is not an integral domain, then neither is $R[x]$.

If $S \leq R$ is a subring, then $S[x] \leq R[x]$ is a subring.

Proposition

Let $R$ be an integral domain and let $p(x), q(x) \in R[x] - \{0\}$. Then

1. $\text{degree } p(x)q(x) = \text{degree } p(x) + \text{degree } q(x)$,
2. the units of $R[x]$ are the units of $R$,
3. $R[x]$ is an integral domain.
Rational functions

Let $R$ be an integral domain.
The field of fractions of $R[x]$ is

$$\{p(x)/q(x) \mid p(x), q(x) \in R[x], q(x) \neq 0\}.$$
Rational functions

Let $R$ be an integral domain.

The field of fractions of $R[x]$ is

$$\{p(x)/q(x) \mid p(x), q(x) \in R[x], q(x) \neq 0\}.$$ 

The field of fractions over a field $F$ is written $F(x)$. 
Rational functions

Let $R$ be an integral domain.
The field of fractions of $R[x]$ is

$$\{p(x)/q(x) \mid p(x), q(x) \in R[x], q(x) \neq 0\}.$$  

The field of fractions over a field $F$ is written $F(x)$.
The ring of fractions of $\mathbb{Z}[x]$ is $\mathbb{Q}(x)$ (which is $\subset \mathbb{Q}((x))$).
Rational functions

Let $R$ be an integral domain.
The field of fractions of $R[x]$ is

$$\{p(x)/q(x) \mid p(x), q(x) \in R[x], q(x) \neq 0\}.$$  

The field of fractions over a field $F$ is written $F(x)$.
The ring of fractions of $\mathbb{Z}[x]$ is $\mathbb{Q}(x)$ (which is $\subset \mathbb{Q}((x))$).
The ring of formal power series over $R$ is

$$R[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n \mid a_n \in R \right\}.$$  

(“Formal” means we need not deal with convergence.)
Rational functions

Let $R$ be an integral domain.
The field of fractions of $R[x]$ is

$$\{p(x)/q(x) \mid p(x), q(x) \in R[x], q(x) \neq 0\}.$$ 

The field of fractions over a field $F$ is written $F(x)$.
The ring of fractions of $\mathbb{Z}[x]$ is $\mathbb{Q}(x)$ (which is $\subset \mathbb{Q}((x))$).
The ring of formal power series over $R$ is

$$R[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n \mid a_n \in R \right\}.$$ 

("Formal" means we need not deal with convergence.)

If $F$ is a field, the ring of fractions over $F[[x]]$ is the set of (formal) Laurent series

$$F((x)) = \left\{ \sum_{n \geq N} a_n x^n \mid a_n \in F, N \in \mathbb{Z} \right\}.$$