Def: (1) A ring is a triple $(R, +, \cdot)$ with $+$ and $\cdot$ binary operations such that

(i) $(R, +)$ is an abelian group.

(ii) $\cdot$ is associative: $a(bc) = (ab)c \quad \forall a, b, c \in R$.

(iii) The distributive laws hold: $a(b + c) = ab + ac \quad \forall a, b, c \in R$.

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

(2) A ring $(R, +, \cdot)$ is commutative if $ab = ba \quad \forall a, b \in R$.

(3) A ring $(R, +, \cdot)$ is a ring with identity if there exists $1 \in R$ such that

$$a1 = a = 1a \quad \forall a \in R.$$
(4) A ring with identity \((R, +, \cdot)\), where \(1 \neq 0\), is a division ring if every nonzero element of \(R\) has a multiplicative inverse: \(\forall a \in R \setminus \{0\}, \exists b \in R, ab = ba = 1\).

(5) A division ring \((R, +, \cdot)\) is a field if \(R\) is commutative.
Notation:  
- Additive identity $0 \in \mathbb{R}$
- Additive inverse $-r \in \mathbb{R}$
- Multiplicative identity $1 \in \mathbb{R}$
- Multiplicative inverse $r^{-1} \in \mathbb{R}$

Examples:

1. $\{0\}$ is a commutative ring with identity $1 = 0$. We call $\{0\}$ the zero ring.

2. $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity.
   - Additive identity: $0$
   - Multiplicative identity: $1$
   - Additive inverse: $-a$
   - Only $1$ and $-1$ have multiplicative inverses

3. Let $n \in \mathbb{Z}$, $n \geq 2$. Then $(n\mathbb{Z}, +, \cdot)$ is a commutative ring without identity.

4. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are fields.
3) Let \( n \in \mathbb{Q} \) be a number that is not a perfect square in \( \mathbb{Q} \), then
\[
\mathbb{Q}[\sqrt{n}] := \{ a + b\sqrt{n} \mid a, b \in \mathbb{Q} \}
\]
is a field called the \textit{quadratic field}.

\[
(a + b\sqrt{n})^{-1} = \frac{a - b\sqrt{n}}{a^2 - nb^2}
\]
where \( a \neq 0 \) or \( b \neq 0 \)

6) \((\mathbb{Z}/n, +, \cdot)\) is a \textit{commutative ring with identity}.

\begin{align*}
\text{Additive identity:} & \quad [0] \\
\text{Additive inverse:} & \quad [-a] \\
\text{Multiplicative identity:} & \quad [1] \\
\text{Multiplicative inverse:} & \quad [a] \text{ has a multiplicative inverse } \iff \gcd(a, n) = 1.
\end{align*}

7) \((\mathbb{Z}/p, +, \cdot)\) is a field. We denote it by \( \mathbb{F}_p \).
\( \mathbb{Z}/n \) is a field iff \( n \) is a prime.
9. The real Quaternions \( H = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \} \) is a division ring. See Example (5), RA7.

9. \( (M_{n \times n}(\mathbb{C}), +, \cdot) \) is a noncommutative ring with identity.

- Additive identity: Zero matrix \( O_{n \times n} \)
- Multiplicative identity: \( I_n \)
- Additive inverse: \( -A \)
- Some matrices are not invertible

10. If \( R \) and \( S \) are rings, then the direct product \( R \times S \) is a ring under componentwise addition and multiplication.

- \( R \times S \) is commutative \( \iff \) \( R \) and \( S \) are commutative
- \( R \times S \) has an identity \( \iff \) \( R \) and \( S \) have identities
Let $X \neq \emptyset$ be a set. Let $(A, +, \cdot)$ be a ring.

Define $\mathcal{F}(X, A) := \{ f : X \rightarrow A \mid f \text{ is a function} \}$. $\mathcal{F}(X, A)$ is a ring under addition and multiplication of function: Let $f, g \in \mathcal{F}(X, A)$ and $x \in X$

$(f + g)(x) := f(x) + g(x) \in A$ and $(fg)(x) := f(x) \cdot g(x) \in A$.

$0(x) = 0_A$ \hspace{1cm} $1(x) = 1_A$ (if $A$ has an identity).

$\mathcal{F}(X, A)$ is commutative $\iff$ $A$ is commutative

$\mathcal{F}(X, A)$ has an identity $\iff$ $A$ has an identity

If $A$ is a division ring, then $\mathcal{F}(X, A)$ is not a division ring necessarily.

See Example 4 of Zero divisors/Units.
Proposition 1: Let $R$ be a ring. Then

1. $0a = a0 = 0$, $\forall a \in R$

2. $(-a)b = a(-b) = -(ab)$, $\forall a, b \in R$

3. $(-a)(-b) = ab$, $\forall a, b \in R$

4. If $R$ has an identity $1$, then the identity is unique and $-a = (-1)a$.

Proof: Exercise.
Let \((R, +, \cdot)\) be a ring.

1. A nonzero element \(a \in R\) is called a zero divisor if there is a nonzero element \(b \in R\) s.t. either \(ab = 0\) or \(ba = 0\).

2. Let \(R\) have an identity \(1 \neq 0\). A nonzero element \(a \in R\) is called a unit if there is \(b \in R\) s.t. \(ab = 1 = ba\).

The set of units in \(R\) is denoted \(R^x\) and it is a group called the group of units of \(R\). Prove \((R^x, \cdot)\) is a group.

\[\text{A zero divisor cannot be a unit.}\]

\[\text{A noncommutative ring can have } ab = 0 \text{ and } ba \neq 0.\]
1. A field $F$ is a commutative ring with identity $1 \neq 0$ in which every nonzero element is a unit, i.e. $F^\times = F \setminus \{0\}$.  

$\mathbb{F}_p$, $p$ prime, $\mathbb{Q}$, $\mathbb{Q}[\sqrt{m}]$, $\mathbb{R}$, $\mathbb{C}$

2. $\mathbb{Z}$

**Units:** $\mathbb{Z}^\times = \{ \pm 1 \}$

**Zero divisors:** None

3. $\mathbb{Z}/n$, $n \geq 2$

In Exam 1 you proved that $[a] \in \mathbb{Z}/n$ is either a unit or a zero divisor.

**Units:** $\left( \mathbb{Z}/n \right)^\times = \left\{ [a] \mid \gcd(a, n) = 1 \right\}$

**Zero divisors:** $(\mathbb{Z}/n) \setminus \left( \left( \mathbb{Z}/n \right)^\times \cup \{ [0] \} \right)$
4. Let $R$ denote $\mathcal{F}([0,1], \mathbb{R})$.

**Units:**

$R^\times = \left\{ f \in R \mid f(x) \neq 0 \text{ for all } x \in [0,1] \right\}$

If $f \in R$, then $f^{-1} := \frac{1}{f}$ where $\left(\frac{1}{f}\right)(x) = \frac{1}{f(x)}$ for all $x \in [0,1]$.

**Zero divisors:**

$R \setminus (R^\times \cup \{0\})$

If $f \in R$, $f \notin R^\times$ and $f \neq 0$, then $fg = 0$ where

$$g(x) := \begin{cases} 0, & \text{if } f(x) \neq 0 \\ 1, & \text{if } f(x) = 0 \end{cases}$$

is not the zero function.
Def: A commutative ring with identity \( 1 \neq 0 \) is called an integral domain if it has no zero divisors.

Explicitly \( \forall a, b, c \in R \quad (ab = 0 \Rightarrow a = 0 \text{ or } b = 0) \)

\( (a \neq 0 \text{ and } b \neq 0 \Rightarrow ab \neq 0) \)

Ex: \( \mathbb{Z} \) - Division rings - Fields

Proposition 2: (1) Let \( a, b, c \in R \) with \( a \) not a zero divisor.

If \( ab = ac \), then \( a = 0 \) or \( b = c \).

(2) If \( R \) is an integral domain, then for all \( a, b, c \in R \)

\( ab = ac \) implies \( a = 0 \) or \( b = c \).

Proof: Exercise.
Corollary 3: Any finite integral domain is a field.

Proof: Let \( R \) be a finite ID.

We need \( \Rightarrow \)  
- \( R \) has identity \( \checkmark \)  
- \( R \) is commutative \( \checkmark \)  
- \( 1 \neq 0 \)  
- \( \forall a \in R \setminus \{0\}, \exists b \in R, \ ab = 1 \)

Let \( a \in R \setminus \{0\} \). Define a map \( \lambda_a : R \to R \) by \( \lambda_a(r) = ar \) for all \( r \in R \).

WTS: \( \lambda_a \) is surjective.

Observe that \( \lambda_a \) is injective. Let \( r, s \in R \) s.t. \( \lambda_a(r) = \lambda_a(s) \), i.e. \( ar = as \).

By Prop 2(b), \( a = 0 \) or \( r = s \). Since \( a \neq 0 \), then \( r = s \).

Now, \( \lambda_a : R \to R \) is injective and \( R \) is finite. This implies \( \lambda_a \) must be surjective.

Thus, \( 1 \in R \) is so that \( \exists b \in R \) s.t. \( ab = \lambda_a(b) = 1 \).
Definition: Let \((R, +, \cdot)\) be a ring. A subset \(S \subseteq R\) is called a subring of \(R\) if:

1. \(0 \in S\)
2. \(S\) is closed under addition.
3. \(S\) is closed under additive inverses.
4. \(S\) is closed under multiplication.

A subring of the ring \(R\) is a subgroup of \(R\) that is closed under multiplication.

Examples:

1. \(\mathbb{Z}: S = \{\text{even integers}\}\) \(O = \{\text{odd integers}\}\)

\(S\) is a subring
\(O\) is not a subring because \(0 \notin O\).
2. \( \mathbb{Z} \) is a subring of \( \mathbb{Q} \) is a subring of \( \mathbb{R} \) is a subring of \( \mathbb{C} \).
3. \( n\mathbb{Z} \) is a subring of \( \mathbb{Z} \) for \( n \in \mathbb{Z} \).
4. \( \{ f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ is continuous} \} \) is a subring of \( \mathcal{F}(\mathbb{R}, \mathbb{R}) \).
5. Let \( S := \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z} \} \) (integral quaternions) is a subring of the real quaternions \( \mathbb{H} \).
6. Let \( M \in \mathbb{Z} \) be a number that is not a perfect square in \( \mathbb{Z} \).
    \( \mathbb{Z}[\sqrt{M}] := \{ a + b\sqrt{M} \mid a, b \in \mathbb{Z} \} \) is a subring of \( \mathbb{Q}[\sqrt{M}] \).

\[ \text{commutative with an identity} \]
Let $F$ be a field and $S$ a subring of $F$.

- $S$ is not a field necessarily. See previous example: $\mathbb{Z}[\sqrt{M}]$ is not a division ring.

- If $1_F \in S$, then $S$ is an ID. Prove it!

Subring Tests

**Theorem 4:** Let $(R, +, \cdot)$ be a ring and $S \subseteq R$.

$S$ is a subring $\iff$

1. $S \neq \emptyset$
2. $a - b \in S \ \forall a, b \in S$
3. $ab \in S \ \forall a, b \in S$

**Proof:** Exercise
Theorem 5: Let \((R, +, \cdot)\) be a finite ring and \(S \subseteq R\).

\(S\) is a subring \(\iff\)

1. \(S \neq \emptyset\)

2. \(a + b \in S\) \(\forall a, b \in S\)

3. \(ab \in S\) \(\forall a, b \in S\)

Proof: Exercise