1. **Introduction:** Rings are closer to familiar structures like $\mathbb{R}$ in that they get addition (therefore subtraction) and multiplication, but they don't necessarily get division. More generally certain standard assumptions break down. For example in $\mathbb{R}$ we know that if $ab = 0$ then $a = 0$ or $b = 0$ but this isn't necessarily the case in a general ring. What we'll do in this chapter is focus on certain types of ring in which behavior is a little more familiar.

2. **Integral Domains:**

   (a) **Definition:** If R is a commutative ring then $a \in R$ is a *zero-divisor* if there is some $b \in \mathbb{R}$ with $ab = 0$.

   Example: In $\mathbb{Z}_{10}$ the integer 5 is a zero-divisor because $(5)(2) = 0$ whereas 3 is not a zero-divisor because there is no $b \in \mathbb{Z}_{10}$ with $3b = 0$.

   Note: When defining a zero-divisor we requite R to be commutative to avoid issues that arise if $ab = 0$ but $ba \neq 0$. This can happen in rings, for example in $M_2\mathbb{R}$:

   $$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ but } \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

   This complicates the definition as to whether we should consider a and b to be zero-divisors.

   (b) **Definition:** A commutative ring with a unity is an *integral domain* if it has no zero-divisors.

   In other words a commutative ring with unity is an integral domain if, whenever $ab = 0$, we must have $a = 0$ or $b = 0$.

   Example: The following are all integral domains: $\mathbb{Z}$, $\mathbb{Z}_p$ when p is a prime, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}[x]$, $\mathbb{Z}[\sqrt{2}]$

   Example: The following are all not integral domains:

   - $\mathbb{Z}_n$ when n is not a prime, for example in $\mathbb{Z}_6$ we have $(2)(3) = 0$.
   - $\mathbb{Z} \oplus \mathbb{Z}$, for example $(1, 0)(0, 1) = (0, 0)$.
   - $M_2\mathbb{Z}$ because it's not commutative to begin with.

   Note: Integral domains are assumed to have unity for historical reasons. It's possible to consider rings which have no zero divisors but have no unity (like $2\mathbb{Z}$) but these are not considered integral domains.

   (c) **Theorem (Cancellation):** If R is an integral domain and $a, b, c \in R$ with $a \neq 0$ and $ab = ac$ then $b = c$.

   Note: In groups we can do this because of inverses but here this is not the reason!

   Proof: If $ab = ac$ then $ab - ac = 0$ and so $a(b - c) = 0$. Since $a \neq 0$ we have $b - c = 0$ and so $b = c$. $\mathcal{QED}$

3. **Fields**

   (a) **Definition:** A commutative ring with unity is a *field* if every nonzero element is a unit.

   Note: Recall a unit is an element with a multiplicative inverse so this is basically saying that each nonzero element has a multiplicative inverse. In this case we have to have a unity to even begin the discussion about whether elements are units.

Example: The following are all fields: $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_3[i] = \{a + bi \mid a, b \in \mathbb{Z}_3$ (not obvious)

Example: The following are all not fields: $\mathbb{Z}$, $\mathbb{R}[x]$

Note: As we'll see, fields are a subset of integral domains (which we know are a subset of rings).

(b) **Theorem:** Every field is an integral domain.

Proof: Suppose R is a field and $a, b \in R$ with $ab = 0$. We claim $a = 0$ or $b = 0$. If $a = 0$ we are done. if not then we can multiply both sides by a^{-1} and get $b = 0$. $\mathcal{QED}$

(c) **Note:** The reverse is not true, we can have an integral domain which is not a field, for example $\mathbb{Z}$.

However we do have the following:

(d) **Theorem:** Every finite integral domain is a field.

Proof: Let R be a finite integral domain with unity 1 and let $a \in R$. We claim a is a unit. If $a = 1$ then we are done. If $a \neq 1$ then examine $a^1, a^2, a^3, \ldots$. Since R is finite two of these must be equal, say $a^i = a^j$ for $i > j$. By cancellation then we have $a^{i-j} = 0$ and so $a\left(a^{i-j-1}\right) = 1$ and we have found the multiplicative inverse of a. $\mathcal{QED}$

Example: If p is a prime then $\mathbb{Z}_p$ is a finite integral domain and hence is a field.