**Theorem**

Suppose $S \subseteq R$. $S \leq R$ is a subring if

(i) $0_R \in S$ or check $S \neq \emptyset$ if we use it in junction with the negation axiom.

(ii) Closed under $+$.

(iii) Closed under $-$ or negation: if $a, b \in S$ then $a - b \in S$. Or if $a \in S$ then $-a \in S$.

(iv) Closed under $\times$: if $a, b \in S$ then $a \times b \in S$.

*Note.* The first three proves that $S$ is a subgroup.

**Example** (integral domain)**.** $\mathbb{Z}$ is an integral domain (but not a field). Having inverses doesn't mean an element is not a zero divisor.

In a group, recall the cancellation laws: $ab = ac \Rightarrow b = c, ba = ca \Rightarrow b = c$.

In $\mathbb{Z}$, if $3x = 3y$, then $x = y$. If $ab = ac$, then $a = 0$ or $b = c$.

**Proof**

Suppose $ab = ac$. Then

$$\begin{aligned} ab - ac &= 0 \\ a(b - c) &= 0 \\ a = 0 &\text{ or } b - c = 0 \text{ since no zero divisors} \\ a = 0 &\text{ or } b = c \end{aligned}$$

$\square$

**Theorem**

If $R$ is an integral domain and $ab = ac$, then $a = 0$ or $b = c$. The other direction follows from commutativity.

**Example** (bad)**.** $\mathbb{Z}_{12}$ is not an integral domain. It is commutative, has identity 1, but has zero divisors like $3 \times 4 = 0$. In general, any composite (non-prime) order of $\mathbb{Z}_n$ is not an integral domain.

Consider $x^2 - 5x + 6 = 0$ in $\mathbb{Z}_{12}$. 2,3,6,11 are all solutions.

$$(6 - 2)(6 - 3) = 4 \times 3 = 0.$$

So what are the zero divisors of $\mathbb{Z}_{12}$?

It's 2,3,4,6,8,9,10. It happens that the non-zero divisors 1,5,7,11 are units. Their inverses are themselves. They form a group isomorphic to $V_4$.

**Proposition**

In $\mathbb{Z}_n$, any nonzero element is either a zero divisor or a unit.

*Note.* In $\mathbb{Z}$, this is not true. Units are $\{\pm 1\}$ but there is no zero divisors.

**Proof**

If $a$ is a zero divisor then $ab = 0$ for $a \neq 0, b \neq 0$. If $a$ is a unit, then there exists $c \in R : ac = ca = 1$.

$$\begin{aligned} ab &= 0 \\ (ca)b &= c0 \\ 1b &= 0 \\ b &= 0 \end{aligned}$$

which is a contradiction. □

**Theorem**

Any field is an integral domain.

**Proof**

(i) $F$ is commutative by definition of field.

(ii) $F$ has identity by definition of division ring.

(iii) $F$ has no zero divisors. Suppose $ab = 0, a \neq 0, b \neq 0$. Then $a$ is a unit and cannot be a zero divisor. Division ring forces all nonzero elements units.

□

Is every integral domain a field? No. $\mathbb{Z}$.

**Theorem**

Every finite integral domain is a field.

**Example** (zero divisors in $\mathbb{Z}_{12}$)**.** Immediately we can say 2,3,4,6 are zero divisors because they are factors of 12.

All multiples of these are zero divisors too. 8,9,10 are such multiples.

Therefore, as long as $\gcd(a, n) \neq 1$, $a$ is a zero divisor.

*Note.* In $\mathbb{Z}$, the gcd of $a$ and $b$ is of the form $ra + sb$ where $r, s \in \mathbb{Z}$.

So 5 is coprime to 12 means $\gcd(5, 12) = 1 \Rightarrow 5r + 12s = 1$ in integers. Let $r = 5, s = -2$ so it works.