Discuss in your group:

- Classify each nonzero element of $\mathbb{Z}_{12}$ as a unit, a zero divisor, neither, or both.
- Do the same in $\mathbb{Z}$.

	$\mathbb{Z}_{12}$	$\mathbb{Z}$
units	$U_{12} = \{1, 5, 7, 11\}$	$1, -1$
ZDs	$2, 3, 4, 6, 8, 9, 10$	none!
neither	none (0)	All integers except ± 1 (0)
both	none	none

Recall: "Both" isn't possible (proved last time).

Definition. A commutative ring is called an integral domain if it does *not* contain any zero divisors.

- $\mathbb{Z}$ is an integral domain.
- $\mathbb{Z}_{12}$ is *not* an integral domain.

	$\mathbb{Z}_{12}$	$\mathbb{Z}$
units	$U_{12} = \{1, 5, 7, 11\}$	$1, -1$
ZDs	2, 3, 4, 6, 8, 9, 10	none!
neither	none (0)	All integers except ± 1 (0)
both	none	none

Cancellation (in an integral domain)

$3 \cdot b = 3 \cdot c \qquad b \neq c$

- In $\mathbb{Z}$: $3b = 3c \implies b = c$.
- In $\mathbb{Z}_{12}$: $3 \cdot 10 = 3 \cdot 6$, but $10 \neq 6$.

Theorem: Let a, b, c be elements of an integral domain with $a \neq 0$.
If $ab = ac$, then $b = c$.

Proof: Assume $ab = ac$. Thus, $ab - ac = 0 \implies a \cdot (b - c) = 0$.

Since we're in an integral domain, $a = 0$ or $b - c = 0$. (Zero product property.)

But $a \neq 0$, which implies $b - c = 0$. Thus, $b = c$.

Proof fails in $\mathbb{Z}_{12}$

$$3 \cdot 10 = 3 \cdot 6 \implies 3 \cdot 10 - 3 \cdot 6 = 0$$
$$\implies 3 \cdot (10 - 6) = 0 \quad \text{(i.e., } 3 \cdot 4 = 0 \text{ in } \mathbb{Z}_{12}\text{)}$$
$$\implies 3 = 0 \text{ or } 10 - 6 = 0 \quad \text{(false!)}$$

Elizabeth: $\mathbb{Z}_7$ and $\mathbb{R}$ are *almost* multiplicative groups.
(Because every nonzero element has a multiplicative inverse.)

Definition. A commutative ring is called a field if every nonzero element is a unit.

Key: In a field, we can always "divide" (i.e., multiply by a^{-1}), except when $a = 0$.

Theorem: If R is a field, then R is an integral domain.

Proof outline: Assume R is a field.

- Let $\alpha \in R$, $\alpha \neq 0$.
- Since R is a field, α is a unit.
- Then α is *not* a zero divisor, since α can't be both.

Thus, R is an integral domain.

Some Food for Thought

Consider the equation $x^2 - 6x + 8 = 0$.

Factoring gives: $(x-2)(x-4) = 0 \implies x - 2 = 0 \text{ or } x - 4 = 0$

14 14

$$\implies \boxed{x = 2 \text{ or } x = 4}$$

But if we're in $\mathbb{Z}_{15}$:

- $x = 7$ is possible, because $(7-2)(7-4) = 0$. $\longleftarrow 5 \cdot 3 = 0$
- $x = 14$ is possible, because $(14-2)(14-4) = 0$. $\longleftarrow 12 \cdot 10 = 0$

Conclusion: Funny things happen when we're *not* in an integral domain!

Solve $x^2 - 6x + 8 = 0$ in $\mathbb{Z}_{15}$ using the *quadratic formula*.

Recall: When $ax^2 + bx + c = 0$, we have $\boxed{x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}.}$

$$x = \frac{-(-6) \pm \sqrt{(-6)^2 - 4 \cdot 1 \cdot 8}}{2 \cdot 1}$$

$$= \frac{6 \pm \sqrt{4}}{2} = \frac{6 \pm \sqrt{49}}{2} = \frac{6 \pm 7}{2} = \frac{6 \pm 22}{2}$$

$$= 14 \text{ or } -8$$

$$= 14 \text{ or } 7$$

$$\frac{6 \pm 2}{2} = 4 \text{ or } 2$$