Until now: The set of integers $\mathbb{Z}$ is a group under addition.

New perspective: $\mathbb{Z}$ has *two* operations, addition and multiplication. The same can be said about the following sets:

- $\mathbb{R}$ = the set of real numbers
- $\mathbb{Z}_{12} = \{0, 1, 2, 3, \ldots, 10, 11\}$

Observation: There are *properties* of addition and multiplication that are common to $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Z}_{12}$. For example, $a + b = b + a$ in all three sets.

Discuss in your group: Name other properties of addition and multiplication that are common to $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{Z}_{12}$.

Properties of $+$ and $\cdot$ in $\mathbb{Z}$ (and $\mathbb{R}$ and $\mathbb{Z}_{12}$)

1. $\mathbb{Z}$ is closed under addition.
2. $(a+b)+c = a+(b+c)$ for all a, b, $c \in \mathbb{Z}$.
3. There exists $0 \in \mathbb{Z}$ such that $0+a = a$ and $a+0 = a$ for all $a \in \mathbb{Z}$.
4. For $a \in \mathbb{Z}$, there exists $-a \in \mathbb{Z}$ s.t. $a+(-a) = 0$ and $(-a)+a = 0$.
5. $a+b = b+a$ for all a, $b \in \mathbb{Z}$.
6. $\mathbb{Z}$ is closed under multiplication.
7. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all a, b, $c \in \mathbb{Z}$.
8. There exists $1 \in \mathbb{Z}$ such that $1 \cdot a = a$ and $a \cdot 1 = a$ for all $a \in \mathbb{Z}$.
9. $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ and $(b+c) \cdot a = (b \cdot a) + (c \cdot a)$ for all a, b, $c \in \mathbb{Z}$.

Definition: A set R is called a ring if it has two operations (denoted $+$ and $\cdot$) satisfying properties 1 through 9.

- R is a commutative group under addition (properties $1-5$).
- R is *never* a multiplicative group, since the element $0 \in R$ does *not* have a multiplicative inverse.
- R need *not* be commutative under multiplication. (More on this later.)
- Use 0 and 1 to denote the additive and multiplicative identities.

$3 \in \mathbb{Z}$ $-3 \in \mathbb{Z}$ $3^{-1} \notin \mathbb{Z}$

- Given an element $a \in R$, use $-a$ (always exists) and a^{-1} (sometimes exists) to denote its additive and multiplicative inverses.

Examples: In the ring $\mathbb{Z}_{10}$...

- $3 \cdot 7 = 1 \implies$ 3 and 7 are *units*. $3^{-1} = 7$, $7^{-1} = 3$.
- $5 \cdot 2 = 0 \implies$ 5 and 2 are *zero divisors*.

Definitions. Let R be a ring.

- An element $u \in R$ is a unit if it has a *multiplicative* inverse in R (denoted u^{-1}).
- A *nonzero* element $a \in R$ is a zero divisor if there exists a nonzero $b \in R$ such that $a \cdot b = 0$.

Remark. In any ring...

- 1 is a unit, because $1 \cdot 1 = 1$.
- 0 is neither a unit nor a zero divisor.

Unit, zero divisor, neither, or both? (Classify nonzero elements)

Nonzero elts of…	$\mathbb{Z}_{12}$	$\mathbb{Z}_7$	$\mathbb{Z}$	$\mathbb{R}$
units	$U_{12} = \{1, 5, 7, 11\}$	$U_7 = \{1, 2, 3, 4, 5, 6\}$	$1, -1$	$\mathbb{R}^*$ (all nonzero elts)
ZDs	2, 3, 4, 6, 8, 9, 10	none	none	none
neither	none (0)	none (0)	All integers except $1, -1$ (0)	none (0)
both	none	none	none	none

Theorem. A ring element $\alpha \in R$ cannot be both a unit and a zero divisor.

Proof. For contradiction, assume α is both a unit and a zero divisor.

Thus, there exists $\alpha^{-1} \in R$ such that $\alpha^{-1} \cdot \alpha = 1$.

Also, there exists $\beta \in R$, $\beta \neq 0$, such that $\alpha \cdot \beta = 0$.

Multiply both sides of $\alpha \cdot \beta = 0$ on the left by α^{-1} to get:

$$\begin{aligned} \alpha^{-1} \cdot (\alpha \cdot \beta) = \alpha^{-1} \cdot 0 &\implies (\alpha^{-1} \cdot \alpha) \cdot \beta = \alpha^{-1} \cdot 0 \\ &\implies 1 \cdot \beta = 0 \quad \text{(Reading: Why } \alpha^{-1} \cdot 0 = 0.\text{)} \\ &\implies \beta = 0, \end{aligned}$$

which contradicts $\beta \neq 0$. Thus, such an element α does not exist.

Next time...

- In a finite ring, a nonzero α can't be neither (like $2 \in \mathbb{Z}$), i.e., it must be either a unit or a zero divisor.
- $\mathbb{Z}_7$ and $\mathbb{R}$ are *almost* multiplicative groups.

Nonzero elts of...	$\mathbb{Z}_{12}$	$\mathbb{Z}_7$	$\mathbb{Z}$	$\mathbb{R}$
units	$U_{12} = \{1, 5, 7, 11\}$	$U_7 = \{1, 2, 3, 4, 5, 6\}$	$1, -1$	$\mathbb{R}^*$ (all nonzero elts)
ZDs	2, 3, 4, 6, 8, 9, 10	none	none	none
neither	✓none (0)	✓none (0)	All integers except $1, -1$ (0)	none (0)