**Definition:** A non-empty set $G$ equipped with a binary operation $* : G \times G \to G$ is a **group** if...

- **Associativity:** $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
- **Identity:** There exists $e \in G$ such that $a * e = a = e * a$ for all $a \in G$.
- **Inverses:** For each $a \in G$ there exists $b \in G$ such that $a * b = e = b * a$.

If in addition, we have...

- **Commutativity:** $a * b = b * a$ for all $a, b \in G$.

then $G$ is called an **Abelian group** or sometimes a **commutative group**.

## Some groups we already know...

- $\mathbb{Z}$ (integers) with $+$ (addition) is an infinite Abelian group.
- $\mathbb{E}$ (even integers) with $+$ is also an infinite Abelian group. However, odd integers are not closed under addition so they do not form a group.
- Some related (infinite) Abelian groups are $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers), and $\mathbb{C}$ (complex numbers) each with the operation $+$ (addition).
- $\mathbb{Z}$ with $\times$ (multiplication) is not a group since most elements do not have inverses. However, $U(\mathbb{Z}) = \{\pm 1\}$ (the "units" of $\mathbb{Z}$) is an Abelian group under multiplication.
- In the same way, 0 does not have a multiplicative inverse (ever), but once we remove 0, the following sets become (infinite Abelian) groups under multiplication: $\mathbb{Q}^\times$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$ (non-zero rational, real, and complex numbers respectively).
- Let $n \in \mathbb{Z}_{>0}$. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ (integers mod $n$) with the operation $+$ (mod $n$) form a finite Abelian group.
- Let $n \in \mathbb{Z}_{>0}$. $U(n) = U(\mathbb{Z}_n) = \{k \in \mathbb{Z}_n \,|\, (k, n) = 1\}$ (units of $\mathbb{Z}_n$) with the operation $\times$ (multiplication mod $n$) is a finite Abelian group. As before, $\mathbb{Z}_n$ itself is not a group under multiplication since in general many elements lack inverses.
- $\mathbb{R}^n$ ($n$-tuples), $\mathbb{R}^{m \times n}$ ($m \times n$ matrices), $\mathbb{R}[x]$ (polynomials with real coefficients) or other vector spaces under vector addition are Abelian groups.

## "New" groups...

- $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathbb{R}^{n \times n} \,|\, \det(A) \neq 0\}$ (invertible $n \times n$ matrices) with matrix multiplication is a non-Abelian (if $n > 1$) group. [GL = General Linear]
- $\mathrm{GL}_n(\mathbb{Z}) = \{A \in \mathbb{Z}^{n \times n} \,|\, \det(A) = \pm 1\}$ ($n \times n$ matrices with integer entries and determinant equal to $\pm 1$) with matrix multiplication is a non-Abelian (if $n > 1$) group.
- $\mathrm{GL}_n(\mathbb{Z}_m) = \{A \in (\mathbb{Z}_m)^{n \times n} \,|\, \det(A) \in U(\mathbb{Z}_m)\}$ ($n \times n$ matrices with entries in $\mathbb{Z}_m$ and determinant equal to a unit of $\mathbb{Z}_m$) with matrix multiplication is a finite group (and is non-Abelian for $m$ and $n$ large enough).
- $\mathrm{SL}_n(BLAH) = \{A \in \mathrm{GL}_n(BLAH) \,|\, \det(A) = 1\}$ is a group (usually non-Abelian) under matrix multiplication. [SL = Special Linear]
- Fix some integer $n \geq 3$ and let $X$ be some regular $n$-gon. $D_n = \{f : \mathbb{R}^2 \to \mathbb{R}^2 \,|\, f \text{ an isometry and } f(X) = X\}$ with the operation of function composition is a non-Abelian group. For example: $D_3$ is symmetries of an equilateral triangle and $D_4$ is symmetries of a square. *Note:* Isometry = distance and angle preserving bijection (think reflection/rotation).
- Fix some set $X$, $S(X) = \{f : X \to X \,|\, f \text{ bijective}\}$ is a non-Abelian (if $|X| > 2$) group under function composition. $S(X)$ is the *group of permuations of* $X$ or *symmetric group on* $X$. If $X = \{1, 2, \ldots, n\}$, we write $S_n$ instead of $S(X)$.