Recall: $(\mathbb{Z}/4\mathbb{Z}, +)$ is a group.

Note: $(\mathbb{Z}/4\mathbb{Z}, \cdot) \rightarrow [2]_4 \cdot [2]_4 = [4]_4 = [0]_4$

$\rightarrow$ cannot have a number be its own inverse.

$$\left.\begin{array}{r} [a]_n \cdot [x]_n = [0]_n \\ \text{and } [a]_n \cdot [b]_n = [1]_n \end{array}\right\} \quad [b]_n \cdot [a]_n \cdot [x]_n = [b]_n [0]_n = [0]_n.$$

contradiction

but $[b]_n [a]_n [x]_n = [1]_n [x]_n = [x]_n$

$\Rightarrow \{[1]_n, [3]_n\}$ is a group under multiplication.

Example: Let $GL_n(\mathbb{R}) = \{ g \in Mat_n(\mathbb{R}) : \det(g) \neq 0 \}$.
This is a group under matrix multiplication.

- $g, h \in GL_n(\mathbb{R})$, $g \cdot h \in GL_n(\mathbb{R})$ b/c $\det(gh) = \det(g)\det(h) \neq 0$.
- 1_n (id matrix) is the identity element.
- Associative. Do painful calculations or something with invertible linear transformations and check with maps.
- $\det(g) \neq 0$ means g has inverse.

Example: $GL_2(\mathbb{Z}/4\mathbb{Z}) \overset{?}{=} \{ g \in Mat_2(\mathbb{Z}/4\mathbb{Z}) : \det(g) \neq [0]_4 \}$.

Let $g = \begin{pmatrix} [2]_4 & [0]_4 \\ [0]_4 & [2]_4 \end{pmatrix}$, $g \cdot g = \begin{pmatrix} [0]_4 & [0]_4 \\ [0]_4 & [0]_4 \end{pmatrix}$. Thus not closed.

So $GL_2(\mathbb{Z}/4\mathbb{Z}) = \{ g \in Mat_2(\mathbb{Z}/4\mathbb{Z}) : \det(g) \text{ has inverse in } \mathbb{Z}/4\mathbb{Z} \}$.

Note for $GL_2(\mathbb{Z})$, $\det(g)$ must be $-1, 1$ to be invertible.
e.g. $\det(g) = 2$ is invertible in $\mathbb{Q}$.

Example: Let $X = \{1, 2, 3\}$
Let $S_3 = \{ f : X \rightarrow X : f \text{ is bijective} \}$.

	1	1	3 choices for 1
f:	2	2	2 choices for 2
	3	3	1 choice for 3

$\rightarrow$ 3! total elements.

So $\#S_3 = 6$.
This is a group under composition of functions.

$$\mathrm{id}: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)$$

$$\sigma_1: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$$

$$\sigma_2: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$$

$$\sigma_3: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$$

$$\sigma_4: \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$$

$$\sigma_5: \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

We say S_3 is the symmetric group on 3 letters.

Example: Let $X = \{1, 2, \dots, n\}$
Let $S_n = \{f: X \to X : f \text{ is bijective}\}$.
$\#S_n = n!$

This is still a group under composition of function.
(non-abelian finite group)

Fact: Every finite group injects into S_n for some n.

Example: Consider the regular n-gon.
Set r_n = rotation by $\frac{2\pi}{n}$ clockwise.
So $r_n^2 = r_n \circ r_n$ = rotation by $2\left(\frac{2\pi}{n}\right)$ clockwise.
r_n^{n-1} = rotation by $(n-1)\left(\frac{2\pi}{n}\right)$ clockwise.
r_n^n = rotation by $n\left(\frac{2\pi}{n}\right)$ = no rotation.

So $\mathrm{id}, r_n, r_n^2, \dots, r_n^{n-1}$ are distinct rigid motions.
Set $C_n = \{\mathrm{id}, r_n, r_n^2, \dots, r_n^{n-1}\}$. This is an abelian group of order n.
This is referred to the cyclic group of order n.

Example: If we also allow a flip over axis σ, then
$D_n = \{ id, r_n, r_n^2, \dots, r_n^{n-1}, \sigma, \sigma r_n, \sigma r_n^2, \dots, \sigma r_n^{n-1} \}$.

Example: The addition table for $(\mathbb{Z}/4\mathbb{Z}, +)$ is:

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Example: Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{ ([a]_2, [b]_2) : [a]_2, [b]_2 \in \mathbb{Z}/2\mathbb{Z} \}$
with addition $([a]_2, [b]_2) + ([c]_2, [d]_2) = ([a+c]_2, [b+d]_2)$.
The addition table is:

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

We call G the Klein 4-group.

Basic Properties of Groups

Theorem: Let G be any group.
1) The identity element is unique.
2) Inverses are unique.
3) Let $a, b, c \in G$ with $ab = ac$. Then $b = c$.
4) Let $a, b \in G$. One can always solve the equation $ax = b$ for some $x \in G$.

proof: (1) Let e_1, e_2 be identity elements of G.
So $e_1 = e_1 e_2$. But also $e_2 = e_1 e_2$
So $e_1 = e_2$.

(2) Let g_1, g_2 be inverses of g.

So
$$\begin{aligned} g_1 &= e g_1 \\ &= (g_2 g) g_1 \\ &= (g_1 g) g_2 \\ &= e g_2 \\ &= g_2. \end{aligned}$$

(3) Since $a \in G$, $\exists!\, a^{-1}$ s.t. $aa^{-1} = e$.

So
$$\begin{aligned} ab = ac &\iff a^{-1}(ab) = a^{-1}(ac) \\ &\iff (a^{-1}a)b = (a^{-1}a)c \\ &\iff eb = ec \\ &\iff b = c. \end{aligned}$$

(4) Set $x = a^{-1}b \in G$.

Then $a(a^{-1}b) = (aa^{-1})b = eb = b$. $\square$

We saw earlier $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication.

$(\mathbb{Z}/4\mathbb{Z})^* = \{[1]_4, [3]_4\}$ is a group under multiplication.

Note $2|4$, so that seems to be a problem...
in reference to $[2]_4$ not being in $(\mathbb{Z}/4\mathbb{Z})$.

What about $\mathbb{Z}/8\mathbb{Z}$ and $[8]_{10}$?

$[8]_{10} \cdot [5]_{10} = [40]_{10} = [0]_{10} \longleftarrow$ BAD!
We want our elements to have no common divisors with n.

Set $(\mathbb{Z}/n\mathbb{Z})^* = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}$.

careful! this is a representative of $[a]_n$...
Test well-definedness.

If $[b]_n = [a]_n$, then $a = b + nk$ for some $k \in \mathbb{Z}$.
If $d = \gcd(b,n)$, then $d \mid b + nk$. So $d \mid \gcd(a,n) = 1$.
Thus $d = 1$.

Is $(\mathbb{Z}/n\mathbb{Z})^*$ a group?

Well-definedness: Define $[a]_n[b]_n = [ab]_n$.

Let $[a]_n = [c]_n$ and $[b] = [d]_n$.
So $a = c + ns$ and $b = d + nt$.
Then
$$
\begin{aligned}
[a]_n[b]_n &= [ab]_n \\
&= [(c+ns)(d+nt)]_n \\
&= [cd + n(s+t+nst)]_n \\
&= [cd]_n \\
&= [c]_n[d]_n.
\end{aligned}
$$

Identity: Let $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^*$. Note

$$[1]_n[a]_n = [1 \cdot a] = [a]_n.$$
and $[1 \cdot a]_n = [a \cdot 1]_n = [a]_n[1]_n$.

Thus $[1]_n$ is the identity.

Associativity: Let $[a]_n, [b]_n, [c]_n \in (\mathbb{Z}/n\mathbb{Z})^*$
we have
$$
\begin{aligned}
([a]_n[b]_n)[c_n] &= [ab]_n[c]_n \\
&= [(ab)c]_n \\
&= [a(bc)]_n \\
&= [a]_n[bc]_n \\
&= [a]_n([b]_n[c]_n).
\end{aligned}
$$

Thus $\mathbb{Z}/n\mathbb{Z}$ is associative.

Inverse: Let $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^*$. Since $\gcd(a,n) = 1$, $\exists s,t \in \mathbb{Z}$ s.t. $as + nt = 1$.

Moreover, $\gcd(s,n) = 1$ b/c if $e|s$ and $e|n$, then $e|(as+nt) = 1$. Observe

$$[as+nt]_n = [1]_n$$
$$\downarrow$$
$$[a]_n[s]_n + [n]_n[t]_n = [a]_n[s]_n.$$

So $[a]_n[s]_n = [1]_n$. Thus $[s]_n = [a]_n^{-1}$.

Thing: Let $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^*$. To see $[ab]_n \in (\mathbb{Z}/n\mathbb{Z})^*$,
WTS $\gcd(ab,n)=1$.

If $\gcd(ab,n) \neq 1$, then there is a prime p s.t.
$p \mid \gcd(ab,n)$. So $p \mid n$ and $p \mid ab$. Since p is prime,
$p \mid ab$ implies $p \mid a$ and $p \mid b$.
Thus $p \mid \gcd(a,n)$ or $p \mid \gcd(b,n)$. $\#$ Thus $\gcd(ab,n)=1$.