Example:

- $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is a group under addition.
- Let $H = \{0, 2, 4, 6\}$ be a subset of $\mathbb{Z}_8$.

Discuss in your group:

Verify that H is also a group, with the same operation as $\mathbb{Z}_8$.

Note: You may assume that addition in $\mathbb{Z}_8$ is associative.

mod 8

+	0	2	4	6
0	0	2	4	6
2	2	4	6	0
4	4	6	0	2
6	6	0	2	4

Verification:

✓ (1) H is closed under addition.

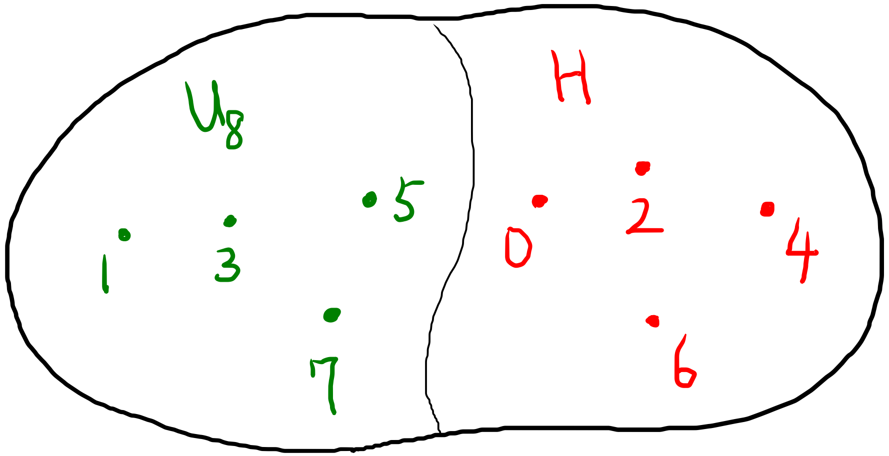
✓ (3) H contains the *additive* identity 0.

✓ (4) If $a \in H$, then $-a \in H$.

Example: $H = \{0, 2, 4, 6\}$ is a subgroup of $\mathbb{Z}_8$ (under $+$).

Definition: Let G be a group. A subset $H \subseteq G$ is called a subgroup of G if H is also a group using the operation of G.

Non-Example: $U_8 = \{1, 3, 5, 7\}$ is *not* a subgroup of $\mathbb{Z}_8$. Although $U_8 \subseteq \mathbb{Z}_8$, their operations ($*$ and $+$) are different.



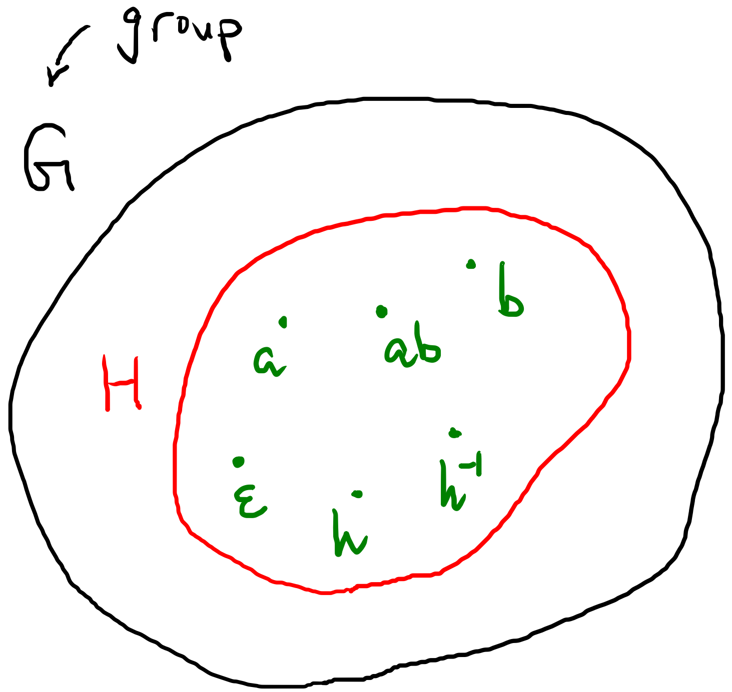
$\mathbb{Z}_8$ (additive group)

Proof know-how: Suppose we're given a group G and a subset $H \subseteq G$.

Example:

- Group $G = G(\mathbb{Z}_{10}) = \{\alpha \in M(\mathbb{Z}_{10}) \mid \alpha \text{ has a multiplicative inverse}\}$.
- Subset $H = S(\mathbb{Z}_{10}) = \{\alpha \in M(\mathbb{Z}_{10}) \mid \det \alpha = 1\}$.

To show that H is a subgroup of G, we must show...



1. If $a, b \in H$, then $ab \in H$.
2. No need to check (or even mention) associativity, since H inherits the associative operation from G.
3. $\varepsilon \in H$, where ε is the identity element of G.
4. If $h \in H$, then $h^{-1} \in H$.

Theorem: Consider the group $G(\mathbb{Z}_{10})$ and its subset

$$S(\mathbb{Z}_{10}) = \{\alpha \in M(\mathbb{Z}_{10}) \mid \det \alpha = 1\}.$$

Then $S(\mathbb{Z}_{10})$ is a subgroup of $G(\mathbb{Z}_{10})$.

Rough draft:

1. Closure: If $\alpha, \beta \in S$, then $\alpha\beta \in S$. ✓

$$\alpha, \beta \in S \implies \left.\begin{matrix} \det \alpha = 1 \\ \det \beta = 1 \end{matrix}\right\} \implies \det(\alpha\beta) = \underbrace{\det \alpha}_{1} \cdot \underbrace{\det \beta}_{1} = 1.$$

3. Identity: $\varepsilon = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \in S$. ✓

$$\det \varepsilon = 1 \cdot 1 - 0 \cdot 0 = 1.$$

4. Inverses: If $\alpha \in S$, then $\alpha^{-1} \in S$. ✓

Know: $\det \alpha = 1$

$$\det(\alpha^{-1}) = (\det \alpha)^{-1} = 1^{-1} = 1.$$

Theorem: $S(\mathbb{Z}_{10})$ is a subgroup of $G(\mathbb{Z}_{10})$.

Proof: Let $\alpha, \beta \in S$. Then $\det \alpha = 1$, $\det \beta = 1$.

Thus $\det(\alpha\beta) = \det \alpha \cdot \det \beta = 1 \cdot 1 = 1$. Hence $\alpha\beta \in S$,

so that S is closed.

We have $\det \varepsilon = \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1 \cdot 1 - 0 \cdot 0 = 1$. Thus, $\varepsilon \in S$.

Recall that $\alpha \in S$. Then

$$\det(\alpha^{-1}) = (\det \alpha)^{-1} = 1^{-1} = 1.$$ Thus, $\alpha^{-1} \in S$.

Therefore S is a subgroup of $G(\mathbb{Z}_{10})$.

Subgroups of $\mathbb{Z}_8$:

Subgroup	# of elements
• $\{0\}$	1
• $\{0, 4\}$	2
• $\{0, 2, 4, 6\}$	4
• $\mathbb{Z}_8$	8

More on this later!