We can show one binary structure is a group if it is isomorphic to another group. Because the required properties for groups are all structural properties.

1 Subgroups

Definition: subgroup

Let $(G, *)$ be a group. Let $H \subseteq G$. We call H a subgroup of G if H is a group under the same operation.

Note. Subspace in linear algebra is an example of subgroup.

Example.

- $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ under addition.
- U_{28} is a subgroup of U, where U is the unit circle under $\times$.
- $\mathbb{Z}_2$ is the integers mod 2 under $+_2$ is NOT a subgroup of $\mathbb{Z}$ because they don't have the same operation.
- $\{1, 2, 3, \ldots\}$ under addition is NOT a subgroup of the $\mathbb{Z}$ because there is no identity.
- $\{0, 1, 2, \ldots\}$ under $+$ is NOT a subgroup of $\mathbb{Z}$ because 1 doesn't have an inverse.

Theorem

Let $(G, *)$ be a group and let $H \subseteq G$. Then $H \leq G$ if

- $e \in H$
- if $x \in H$ then $x^{-1} \in H$
- if $x, y \in H$, then $x * y \in H$

Note. Associativity is implied because it's the same operation. The first condition ensures that $H \neq \emptyset$.

Corollary

Any group G has the following as subgroups:

- G itself
- $\{e\}$

Example. Find the subgroups of V_4. See iPad.

- 4 elements: $\{3, a, b, c\}$
- 1 element: $\{e\}$
- 2 elements: $\{e, a\}, \{e, b\}, \{e, c\}$
- 3 elements: nope

There are a total of 5 subgroups.

Note. In V_4, the smallest subgroup containing a is $\{e, a\}$. Likewise for other non-identity elements. The smallest subgroup for e is $\{e\}$.

Example. Find the subgroups of $\mathbb{Z}_4$. See iPad.

- 4 elements: $\{0, 1, 2, 3\}$
- 1 elements: 0
- 2 elements: only $\{0, 2\}$ works
- 3 elements: nope

There are only 3 subgroups.

Note. In $\mathbb{Z}_4$ the smallest subgroup containing 2 is $\{0, 2\}$, the smallest for 0 is $\{0\}$, the smallest for 1 or 3 is $\{0, 1, 2, 3\}$. This is a good thing.

A group with this property is called **cyclic**.

Definition: generator

The elements 1 (or 3) for $\mathbb{Z}_4$ is called a **generator** for $\mathbb{Z}_4$.

Definition: cyclic group

A group is **cyclic** if it has a generator.

Definition: generated subgroup

The **subgroup generated by** $x \in G$ is the smallest subgroup of G that contains x. We denote the subgroup generated by x by $\langle x \rangle$.

Example. In V_4, the following hold:

- $\langle a \rangle = \{e, a\}$
- $\langle b \rangle = \{e, b\}$

- $\langle c \rangle = \{e, c\}$
- $\langle e \rangle = \{e\}$

None of these is the whole group. This means V_4 is not cyclic, and has no generator.

Example. In $\mathbb{Z}_4$,

- $\langle 0 \rangle = \{0\}$
- $\langle 1 \rangle = \{0, 1, 2, 3\}$
- $\langle 2 \rangle = \{0, 2\}$
- $\langle 3 \rangle = \{0, 1, 2, 3\}$

$\mathbb{Z}_4$ is cyclic, it is generated by 1 or 3.