

Group theory

Peter Rowlett

Recall that we defined (G, \circ) as a set G and a binary operation on that set, \circ . Remember that the definition of a binary operation tells us that (G, \circ) has **closure**.

- **Closure:** $\forall a, b \in G \ (a \circ b \in G)$.

1 Group

If (G, \circ) satisfies the following, then it is called a *group*.

- **Associativity:** $\forall a, b, c \in G \ (a \circ (b \circ c) = (a \circ b) \circ c)$.
- **Identity:** $\exists e \in G \ \forall a \in G \ (e \circ a = a \circ e = a)$.
- **Inverse:** $\forall a \in G \ \exists b \in G \ (a \circ b = b \circ a = e)$

2 Abelian group

If (G, \circ) is a group that also satisfies commutativity, it is called an *Abelian group*.

- **Commutativity:** $\forall a, b \in G \ (a \circ b = b \circ a)$.

3 Algebraic structures that are not groups

- If (G, \circ) satisfies closure but none of the other properties, it is called a *magma*, or sometimes a *groupoid*.
- If (G, \circ) satisfies closure and associativity only, it is a *semi-group*.
- If (G, \circ) satisfies closure, associativity, and has an identity, it is a *monoid*.

4 Order of an element and generators

For a group with identity e , the *order* of an element a is the smallest positive integer power of a such that $a^n = e$.

A *generator* is an element g such that every element of the group can be expressed as some power of g .

A group with a generator is called a *cyclic group*.

If g is a generator for a group G , and $g^n = e$, then we write $G = \langle g \rangle$ and can draw a general group table.

| | e | g | g^2 | g^3 | \dots | g^{n-2} | g^{n-1} |
|-----------|-----------|-----------|----------|----------|----------|-----------|-----------|
| e | e | g | g^2 | g^3 | \dots | g^{n-2} | g^{n-1} |
| g | g | g^2 | g^3 | g^4 | \dots | g^{n-1} | e |
| g^2 | g^2 | g^3 | g^4 | g^5 | \dots | e | g |
| g^3 | g^3 | g^4 | g^5 | g^6 | \dots | g | g^2 |
| \vdots | \vdots | \vdots | \vdots | \vdots | \ddots | \vdots | \vdots |
| g^{n-2} | g^{n-2} | g^{n-1} | e | g | \dots | g^{n-4} | g^{n-3} |
| g^{n-1} | g^{n-1} | e | g | g^2 | \dots | g^{n-3} | g^{n-2} |

5 Subgroups

A *subgroup* of a group (G, \circ) is some $H \subseteq G$ such that (H, \circ) forms a group in its own right.