

Groups.

If we look at the properties of the set of integers \mathbb{Z} we find that it satisfies the following:

The integers are a set with an operation $+$ defined on them which satisfies:

- (1) For every pair $a, b \in \mathbb{Z}$ $a + b \in \mathbb{Z}$. That is the integers are closed under $+$.
- (2) For all $a, b, c \in \mathbb{Z}$ we have $a + (b + c) = (a + b) + c$. That is $+$ is associative.
- (3) There is an element $0 \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$ $a + 0 = 0 + a = a$.
- (4) For every $a \in \mathbb{Z}$ there is an element $b \in \mathbb{Z}$ such that $a + b = b + a = 0$.
- (5) For all $a, b \in \mathbb{Z}$ $a + b = b + a$. That is $+$ is commutative or abelian.

Instead of using the Peano axioms to define the integers we could instead use the properties above as a set of axioms and ask. What properties do sets have which satisfies these axioms? A set which satisfies the first four axioms is called a group. If it also satisfies the fifth axiom it is called a commutative (or abelian) group. Here then is the definition of a group:

Definition. A set G with an operation \circ defined on it is a group if:

- (1) G is closed under \circ . That is: For every pair $a, b \in G$

$$a \circ b \in G.$$

- (2) \circ is associative. That is: For all $a, b, c \in G$ we have

$$a \circ (b \circ c) = (a \circ b) \circ c$$

- (3) G contains an identity element for \circ . That is: There is an element $e \in G$ such that for all $a \in G$

$$a \circ e = e \circ a = a$$

- (4) Every element in G has an inverse for \circ in G . That is: For every $a \in G$ there is an element $b \in G$ such that

$$a \circ b = b \circ a = e$$

This completes the set of axioms for G to be a group under \circ .

If in addition:

- (5) \circ is commutative. That is: For all $a, b \in G$

$$a \circ b = b \circ a$$

we say that G is an Abelian group.