Groups

Kevin James

Definition

Definition

A binary operation on a nonempty set A is a mapping f form $A \times A$ to A. That is $f \subseteq A \times A \times A$ and f has the property that for each $(a, b) \in A \times A$, there is precisely one $c \in A$ such that $(a, b, c) \in f$.

Notation

If f is a binary operation on A and if $(a, b, c) \in f$ then we have already seen the notation $f(a, b) = c$. For binary operations, it is customary to write instead

$$a \; f \; b = c,$$

or perhaps

$$a * b = c.$$

Example

Some binary operations on $\mathbb{Z}$ are

1. $x * y = x + y$
2. $x * y = x - y$
3. $x * y = xy$
4. $x * y = x + 2y + 3$
5. $x * y = 1 + xy$

Commutativity and Associativity

Definition

Suppose that $*$ is a binary operation of a nonempty set A.

- $*$ is *commutative* if $a * b = b * a$ for all $a, b \in A$.
- $*$ is *associative* if $(a * b) * c = a * (b * c)$.

Example

1. Multiplication and addition give operators on $\mathbb{Z}$ which are both commutative and associative.
2. Subtraction is an operation on $\mathbb{Z}$ which is neither commutative nor associative.
3. The binary operation on $\mathbb{Z}$ given by $x * y = 1 + xy$ is commutative but not associative. For example $(1 * 2) * 3 = 3 * 3 = 10$ while $1 * (2 * 3) = 1 * (7) = 8$.

Closure

Definition

Suppose that $*$ is a binary operation on a nonempty set A and that $B \subseteq A$. If it is true that $a * b \in B$ for all $a, b \in B$, then we say that B is closed under $*$.

Example

Consider addition on $\mathbb{Z}$. The set of even integers is closed under addition.

Proof.

Suppose that $a, b \in \mathbb{Z}$ are even.
Then there are $x, y \in \mathbb{Z}$ such that $a = 2x$ and $b = 2y$.
Thus $a + b = 2x + 2y = 2(x + y)$ which is even.
Since a and b were arbitrary even integers, it follows that the set of even integers is closed under addition. $\square$

Identity Element

Definition

Let $*$ be a binary operation on a nonempty set A. An element e is called an identity element with respect to $*$ if

$$e * x = x = x * e$$

for all $x \in A$.

Example

1. 1 is an identity element for multiplication on the integers.
2. 0 is an identity element for addition on the integers.
3. If $*$ is defined on $\mathbb{Z}$ by $x * y = x + y + 1$ Then $\underline{-1}$ is the identity.
4. The operation $*$ defined on $\mathbb{Z}$ by $x * y = 1 + xy$ has no identity element.

Right, Left and Two-Sided Inverses

Definition

Suppose that $*$ is a binary operation on a nonempty set A and that e is an identity element with respect to $*$. Suppose that $a \in A$.

- If there exists $b \in A$ such that $a * b = e$ then b is called a *right inverse* of a with respect to $*$.
- If there exists $b \in A$ such that $b * a = e$ then b is called a *left inverse* of a with respect to $*$.
- If $b \in A$ is both a right and left inverse of a with respect to $*$ then we simply say that b is an *inverse* of a and we say that a is *invertible*.

Example

1. Consider the operation of addition on the integers. For any integer a, the inverse of a with respect to addition is $-a$.
2. Consider the operation of multiplication on $\mathbb{Z}$. The invertible elements are $\underline{1\ }$ and $\underline{\ -1\ }$.

Fact

Suppose that $*$ is a binary operation on a nonempty set A. If there is an identity element with respect to $*$ then it is unique. In the case that there is an identity element and that $*$ is associative then for each $a \in A$ if there is an inverse of a then it is unique.

Definition

A group is a nonempty set G along with a binary operation $*$ which satisfies the following axioms.

Associativity If $a, b, c \in G$ then $(a * b) * c = a * (b * c)$.

Identity Element There is an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.

Inverses For each $a \in G$ there is an element $b \in G$ called the inverse of a which satisfies $a * b = b * a = e$.

A group is called Abelian if it also satisfies the following axiom

Commutativity For all $a, b \in G$, $a * b = b * a$.

Definition

- A group is said to have finite order if it has a finite number of elements. In this case, the number of elements of G is denoted $|G|$ and is called the order of G.
- A group with infinitely many elements is said to be of infinite order.

Example

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are Abelian groups under addition.
2. $\mathbb{Z}/n\mathbb{Z}$ is an Abelian group under addition.
3. $\mathbb{Q} - \{0\}$ is an Abelian group under multiplication.

Theorem

- *Every vector space V is an Abelian group under its addition.*
- *Every ring is an abelian group under the ring addition.*
- *If R is a ring with identity, then the set R^* of units of R is a group under multiplication.*
- *The nonzero elements of a field form an abelian group under multiplication.*

Theorem

Let $(G, *)$ and $(H, \circ)$ be groups. Then $G \times H$ is a group with operation defined by $(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$. If G and H are abelian then so is $G \times H$. If G and H are finite then so is $G \times H$ and $|G \times H| = |G||H|$.

Proposition

Suppose that G is a group.

1. *The identity element is unique.*
2. *Given $a \in G$, the inverse of a is unique.*
3. $(a^{-1})^{-1} = a$.
4. $(ab)^{-1} = b^{-1}a^{-1}$.
5. $a_1 * a_2 * \cdots * a_k$ *is well defined for all k. (Induct on the associative law for G.)*

Note

Since the group law is a well-defined function, we have

1. $u = v \Rightarrow au = av$.
2. $u = v \Rightarrow ub = vb$.

Proposition

Suppose that $a, b \in G$. Then the equations $ax = b$ and $ya = b$ have unique solutions in G. As a consequence, we have the cancellation laws.

1. $au = av \Rightarrow u = v$.
2. $ub = vb \Rightarrow u = v$.

Definition

Suppose that G is a group and that $a \in G$. If the elements $e = a^0, a, a^2, \ldots$ are all distinct, then we say that a has infinite order and write $|a| = \infty$. Otherwise, we define the order of a written $|a|$ to be the smallest positive integer k such that $a^k = e$.

Example

1. In $(\mathbb{Z}, +)$, $|1| = \infty$.
2. In $((\mathbb{Q} - \{0\}), *)$, $|-1| = 2$.
3. In $\mathbb{Z}/n\mathbb{Z}$, all elements have finite order.