Concepts of Algebra

Algebraic structures

Definition

Let $(A, *)$ be an algebraic system. Then
$*$ is *commutative* on A if $\forall x, y \in A, x * y = y * x$.
$*$ is *associative* on A if $\forall x, y, z \in A, (x * y) * z = x * (y * z)$.
An element $e \in A$ is an *identity element* for $*$ if $\forall x \in A$,
$x * e = e * x = x$.
If A has an identity element e and if $a, b \in A$, then b is an *inverse* of a if $a * b = b * a = e$. Thus, a would also be an inverse of b.


UCDAVIS
AGGIES

Theorem (6.1.1)

Let $(A, *)$ be an algebraic structure.

a) *$(A, *)$ has at most one identity element.*

b) *Suppose $*$ is associative with identity e. If $a \in A$ has an inverse, then a has only one inverse.*

Theorem (6.1.2)

For every natural number m,

a) $(\mathbb{Z}_m, +_m)$ *is an algebraic system that is associative and commutative with identity element* 0. *Every element has an inverse.*

b) $(\mathbb{Z}_m, \cdot_m)$ *is an algebraic system that is associative and commutative. If* $m > 1$, *the system has identity element* 1 .

Definition

Let a be a nonzero element of $(\mathbb{Z}_m, \cdot)$.

- If $ab = 0$ for some $b \neq 0$, then we say a (and also b) is a *divisor of zero*.
- If a has a multiplicative inverse in $\mathbb{Z}_m$, then a is called a *unit* in $\mathbb{Z}_m$. The set of all units in $\mathbb{Z}_m$ is denoted $\mathbb{U}_m$.

Theorem (6.1.3)

Let $m, a \in \mathbb{N}$ with $a < m$. Then

a) *a is a unit in $(\mathbb{Z}_m, \cdot)$ iff a and m are relatively prime.*

b) *a is a divisor of zero in $(\mathbb{Z}_m, \cdot)$ iff a and m are not relatively prime.*


UCDAVIS
AGGIES

Theorem (6.1.4)

$\forall m \in \mathbb{N}$ *with* $m > 1$, $(\mathbb{U}_m, \cdot)$ *is an algebraic system, has identity element* 1, *is associative, and is commutative. Furthermore, every element in* $\mathbb{U}_m$ *has a multiplicative inverse.*


UCDAVIS
AGGIES

Groups

Definition

$(G, \circ)$ is a group iff $(G, \circ)$ is an algebraic system such that

i) the operation $\circ$ is associative on G.

ii) there is an identity element $e \in G$ for $\circ$.

iii) $\forall x \in G$, $\exists x^{-1} \in G$.

If G is a finite set, the *order* of G is $\bar{\bar{G}}$. When G is infinite, the group has *infinite order*.

Theorem (6.2.1)

Let $m \in \mathbb{N}$. Then

a) $(\mathbb{Z}_m, +)$ *is a group of order m with identity* 0.

b) *If $m > 1$,* $(\mathbb{U}_m, \cdot)$ *is a group of with identity* 1.

Definition

A group G is *abelian* if the group operation is commutative.

Theorem (6.2.2)

Let A be a nonempty set. The set of all permutations on A with the operation of function composition is a group, called the group of permutations of A.

Definition

Let $n \in \mathbb{N}$. The group of all permutations of $\mathbb{N}_n$ is called the *symmetric group on n symbols* and is designated by S_n.


UCDAVIS
AGGIES

Theorem (6.2.3)

Let G be a group with identity e. For all a, b, and c in G,

a) $(a^{-1})^{-1} = a$.

b) $(ab)^{-1} = b^{-1}a^{-1}$.

c) *If* $ac = bc$, *then* $a = b$

d) *If* $ca = cb$, *then* $a = b$

Theorem (6.2.4)

Let G be a finite group with identity e. For every $a \in G$,

a) *The function $\lambda_a : G \to G$, where $\lambda_a(x) = ax$ for each $x \in G$, is a permutation of G.*

b) *The function $\rho_a : G \to G$, where $\rho_a(x) = xa$ for each $x \in G$, is a permutation of G.*

Subgroups

Definition

Let $(G, \circ)$ be a group and $H \subseteq G$. Then $(H, \circ)$ is a *subgroup* of G iff $(H, \circ)$ is a group.

Theorem (6.3.1)

Let H be a subgroup of G. Then

a) *The identity of H is the identity e of G.*

b) *If $x \in H$, the inverse of x in H is its inverse in G.*

Theorem (6.3.2)

Let G be a group. A subset H of G is a group iff $H \neq \varnothing$ and for all $a, b \in H$, $ab^{-1} \in H$.


UCDAVIS
AGGIES

Theorem (6.3.3)

Let G is a group and $a \in G$. Then $\{a^n : n \in \mathbb{Z}\}$ is an abelian subgroup of G.

Definition

Let G be a group and $a \in G$. Then $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ is called the *cyclic subgroup generated by a*. The *order of the element a* is the order of (number of elements in) the group $\langle a \rangle$. If $\langle a \rangle$ is an infinite set, we say a has *infinite order*.


UCDAVIS
AGGIES