Chapter 6

July 29, 2020

Concepts of Algebra

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*.

Cyclic groups

Definition

Let G be a group. If there is an element $a \in G$ such that $\langle a \rangle = G$, then we say G is a *cyclic group*. Any element a of G such that $\langle a \rangle = G$ is called a *generator for* G.

Operation Preserving Maps

Definition

Let $(A, \circ)$ and $(B, *)$ be algebraic systems and f be *a* function from A to B. Then f is *operation preserving (OP)* iff for all x, $y \in A$,

$$f(x \circ y) = f(x) * f(y)$$

.

UCDAVIS
AGGIES

Theorem (6.4.1)

Let $f : (A, \circ) \to (B, *)$ *be an OP map.*

a) $(Rng(f), *)$ *is an algebraic system.*

b) *If* f *is onto* B *and* $\circ$ *is associative on* A*, then* $*$ *is associative on* B*.*

c) *If* f *is onto* B *and* $\circ$ *commutative on* A*, then* $*$ *is commutative on* B*.*

d) *If* f *is onto* B *and* e *is the identity for* A*, then* $f(e)$ *is the identity for* B*.*

e) *If* x *has an inverse in* A*, then* $f(x)$ *has an inverse in* B *and* $(f(x))^{-1} = f(x^{-1})$*.*

UCDAVIS
AGGIES

Group Homomorphisms

Definition

Let $(G, \circ)$ and $(H, *)$ be groups. An *OP* mapping $h : (G, \circ) \to (H, *)$ is called a *homomorphism* from $(G, \circ)$ to $(H, *)$. The range of h is called the *homomorphic image* of $(G, \circ)$ under h.

Theorem (6.4.2)

1. *The homomorphic image of a group is a group.*
2. *The homomorphic image of an abelian group is an abelian group.*

Isomorphic Groups

Definition

Let $(G, \circ)$ and $(K, *)$ be groups. *A* homomorphism $h : (G, \circ) \to (K, *)$ that is one-to-one and onto H is called an isomorphism. If K is called an *isomorphism*, we say $(G, \circ)$ and $(K, *)$ are *isomorphic*.

THE END