ALGEBRAIC STRUCTURES

DEFINITION. A **binary operation** on a set A is a function f that maps each and every ordered pair (a,b) A A to an element of A. That is f : A A A.

Notation: Denote binary operations by * and denote the element assigned to the ordered pair (a,b) by a*b. In other words, f (a,b) = a*b.

DEFINITION. A set A is said to be **closed** under the operation * if it has the following property: *if a and b are elements of the set A, then a*b A*

Remark: If A = {a_1, a_2, … , a_n} is a finite set, *we can define a binary operation on A* by means of a table, as follows:

*	a_1	a_2	…	a_j	…	a_n
a_1	a_1*a_1	a_1*a_2	…	a_1*a_j	…	a_1*a_n
a_2	a_2*a_1	a_2*a_2	…	a_2*a_j	…	a_2*a_n
:	:	:		:		:
a_i	a_i*a_1	a_i*a_2	…	a_i*a_j	…	a_i*a_n
:	:	:		:		:
a_n	a_n*a_1	a_n*a_2	…	a_n*a_j	…	a_n*a_n

Properties of Binary Operations

- A binary operation on a set A is said to be **commutative** if a*b = b*a for all elements a and b in A.
- A binary operation on a set A is said to be **associative** if (a*b)*c = (a*b)*c for all elements a and b in A.

GROUPOIDS, SEMIGROUPS and GROUPS

DEFINITION. A **groupoid**, denoted by (G,*), is a nonempty set G *together* with a binary operation * defined on G.

DEFINITION. A **semigroup** denoted by (S,*) is a nonempty set S *together* with an *associative* binary operation * defined on S.

Remark: a*b is also known as the *product of a and b*.

DEFINITION. The semigroup (S,*) is said to be **commutative semigroup** if * is also a commutative operation.

DEFINITION. Let (S,*) be a semigroup and let T be a subset of S. If T is closed under the operation *, then (T,*) is called a **subsemigroup** of (S,*).

DEFINITION. An element e in a semigroup (S,*) is called an **identity element** if e*a = a*e = a for all elements a in S.

THEOREM. If a semigroup (S,*) has an identity element, that *identity element is unique*.

DEFINITION. A **monoid** is a semigroup (M,*) that *has an identity element*.

DEFINITION. Let (M,*) be a monoid with identity element e, and let T be a nonempty subset of M. If
a) T is closed under the operation *, and
b) the identity element e of M is also in T,
then (T,*) is called a **submonoid** of (M,*).

DEFINITION. An element a' in a monoid (M,*) with identity element e is called the **inverse of a** if a*a' = a'*a = e for every element a in M.

THEOREM. If a monoid (M,*) has an inverse element, that *inverse element is unique* for every element a.

DEFINITION. A **group** is a monoid (G,*) with identity element e, which *also has an inverse element* a' for each element a in S.

DEFINITION. A group (G,*) is said to be an **abelian group** if * is *also commutative*.

DEFINITION. If G is a finite group, then the **order of G**, denoted by |G| is *the number of elements in G*.

DEFINITION. Let (H,*) be a subset of group (G,*) such that
a) the identity element e in G is also in H;
b) if for every element a in H there exists an inverse a' also in H; and
c) H is closed under the binary operation *.
then (H,*) is called a **subgroup** of (G,*).

CYCLIC GROUPS

DEFINITION. Suppose (S,*) is a semigroup and let a S. For n Z^+, the powers of *a* can be defined recursively as follows:
a) $\mathbf{a^1 = a}$
b) $\mathbf{a^n = a^{n-1}*a}$ for n ³ 2
Moreover if (S,*) is a monoid with identity element e, a^0 = e.

THEOREM. Let (G,*) be a group and let a G. Then H = { a^n | n Z } is a subgroup of (G,*) and is the smallest subgroup of G which contains a.

DEFINITION. H = {a^n| n Z} is the **cyclic subgroup** of G generated by a, denoted by <a>.

DEFINITION. An element *a* of a group G **generates G** and is a **generator for G** if <a> = G itself. A group (G,*) is **cyclic** if there is some element a in G which generates G.