Semigroups

Luis Alonso-Ovalle

11/10/2003

Contents

1 *Subgroups* 1

2 *Semigroups and monoids* 2

1 *Subgroups*

Groups. A *group* **G** is an algebra consisting of a set G and a single binary operation $\circ$ satisfying the following axioms:

1. $\circ$ is completely defined and G is closed under $\circ$.
2. $\circ$ is associative.
3. G contains an identity element.
4. Each element in G has an inverse element.

Subgroups. We define a subgroup G' as a subalgebra of G which is itself a group.

Examples:

1. The group of even integers with addition is a proper subgroup of the group of all integers with addition.
2. The group of all rotations of the square $\langle\{I, R, R', R''\}, \circ\rangle$, where $\circ$ is the composition of the operations is a subgroup of the group of all symmetries of the square.

Some non-subgroups:

1. The system $\langle\{I, R, R'\}, \circ\rangle$ is *not* a subgroup (and not even a subalgebra) of the original group. Why? (Hint: $\circ$ closure).
2. The set of all non-negative integers with addition is a subalgebra of the group of all integers with addition, because the non-negative integers are closed under addition. But it is not a subgroup because it is not itself a group: it is associative and has a zero, but ... does any member (except for 0) have an inverse?

Order. The order of any group $\mathbf{G}$ is the number of members in the set G.

The order of any subgroup exactly divides the order of the parental group. E.g.: only subgroups of order 1, 2, and 4 are possible for a 4-member group. (The theorem does not guarantee that every subset having the proper number of members will give rise to a subgroup.)

If a group is finite, all its non-empty subalgebras are also subgroups.

(1) THEOREM 10.3. *The intersection* $\mathbf{G}'\cap\mathbf{G}''$ *of two subgroups* $\mathbf{G}', \mathbf{G}''$ *of a group* $\mathbf{G}$ *is itself a subgroup of* $\mathbf{G}$.

PROOF:

- If a, b are in $\mathbf{G}' \cap \mathbf{G}''$, they must both be in both $\mathbf{G}'$ and $\mathbf{G}''$. $\mathbf{G}'$ and $\mathbf{G}''$ are both groups, so $a \circ b$ is in both, hence $a \circ b$ is in $\mathbf{G}' \cap \mathbf{G}''$.
- If a is in $\mathbf{G}' \cap \mathbf{G}''$, it is both in $\mathbf{G}'$ and $\mathbf{G}''$.$\mathbf{G}'$ and $\mathbf{G}''$ are groups, so a^{-1} is in both, hence $\mathbf{G}'$ and $\mathbf{G}''$ must contain a^{-1}.
- Since $\mathbf{G}'$ and $\mathbf{G}''$ are groups, they both contain e; hence $\mathbf{G}' \cap \mathbf{G}''$ must contain e.

2 *Semigroups and monoids*

A *semigroup* is an algebra which consists of a set and a binary associative operation. There need not be an identity element nor inverses for all elements.

A *monoid* is defined as a semigroup which has an identity element. There need not be inverses for all elements. (An *Abelian monoid* is a monoid with a commutative operation.)

Any group is a subgroup of itself and a semigroup and a monoid as well. Every monoid is a semigroup, but not vice versa.

Some examples:

1. The set of all non-negative integers with addition is an Abelian monoid.

2. The set of all positive integers (excluding zero) with addition is a semigroup, but not a monoid.

3. Since both ordinary addition and ordinary multiplication are associative, it can be deduced that addition and multiplication modulo n are also associative. Therefore any system with addition or multiplication (either ordinary, or modulo some n) is a semigroup if it is closed and is a monoid if it also contains the appropriate identity element 0 or 1. So,

   - The set of all positive even integers with ordinary multiplication is a semigroup, but not a monoid. (Why? Hint: think about 1.)
   - The set of all positive odd integers with ordinary multiplication is a monoid. Let's see why.
   - The set {0,1,2,3,4} with multiplication modulo 5 is a monoid.
   - The set of all multiples of 10 which are greater than 100 with ordinaty addition is a semigroup, but not a monoid.

   None of the above examples are groups, because one of more elements lack inverses. Where multiplication (modulo n) is involved, no system which contains 0 can be a group (since 0 has no multiplicative inverse).

Submonoids. $\mathbf{M}$ is a submonoid of the monoid $\mathbf{M}'$ iff $\mathbf{M}$ is a monoid and its identity element is the same as in $\mathbf{M}'$. The stipulation that the identity elements must be the same is not necessary for subgroups, since there it is an automatic consequence. It is possible to find elements of a monoid that themselves form monoids but with different identity elements.