Very Basic Definitions and Results Concerning Binary Operations

09/15/06 Radford

Here we split hairs to see what axioms are used in some basic proofs. This is a very good exercise in abstract algebra.

Let S be a non-empty set with binary operation $S{\times}S \longrightarrow S$ described by $(a,b) \mapsto ab$. Then $e \in S$ is a *left identity element for* S if $ex = x$ for all $x \in S$ and $e' \in S$ is a *right identity element for* S if $xe' = x$ for all $x \in S$. An identity element for S is an element which is both a left and right identity element for S.

Suppose further that S is a monoid with identity element e and let $a, b, c \in S$. Then b is a *left inverse for* a if $ba = e$ and c is a *right inverse for* a if $ac = e$.

Lemma 1 *Let S be a non-empty set with a binary operation.*

(a) *Let $e, e' \in S$. If e is a left identity element for S and e' is a right identity element for S then $e = e'$. In particular S has* at most *one identity element.*

Suppose further that S is a monoid with identity element e and let $a, b, c \in S$. Then:

(b) *If b is a left inverse for a and c is a right inverse for a then $b = c$. In particular a has* at most *one inverse.*

(c) *Suppose that a has a left inverse and $ab = ac$. Then $b = c$.*

(d) *Suppose that a has a right inverse and $ba = ca$. Then $b = c$.*

(e) *Suppose that a has a left inverse or a right inverse and $a^2 = a$. Then $a = e$.*

PROOF: To show part (a) suppose that e (respectively e') is a left (respectively right) identity element. Since $ex = x$ for all $x \in S$ it follows that $ee' = e'$. Likewise, since $xe' = x$ for all $x \in S$, it follows that $ee' = e$. Therefore $e' = ee' = e$ and part (a) follows.

Now suppose S is a monoid with identity element e and $a, b, c \in S$. If $ba = e$ and $ac = e$ then

$$b = be = b(ac) = (ba)c = ec = c.$$

We have established part (b). To show part (c), suppose that a has left inverse d and $ab = ac$. Then

$$b = eb = (da)b = d(ab) = d(ac) = (da)c = ec = c$$

and part (c) follows. Part (d) follows in a similar manner.

Finally, part (e) follows from parts (c) and (d). For suppose that $a^2 = a$. Then $aa = ae$ and $aa = ea$. $\square$

Part (d) of the preceding lemma follows from part (c) applied to S^{op} which we describe below. By means of S^{op} multiplication on the right is switched to multiplication on the left.

Suppose that S is a non-empty set with a binary relation. Then we define its "opposite" binary operation by

$$a \cdot^{op} b = ba$$

for all $a, b \in S$ and denote S with its opposite binary relation by S^{op}. Let $a, b, c, e \in S$. The calculations

$$a \cdot^{op} (b \cdot^{op} c) = a \cdot^{op} (cb) = (cb)a$$

and

$$(a \cdot^{op} b) \cdot^{op} c = (ba) \cdot^{op} c = c(ba)$$

show that S^{op} is associative if and only if S is associative. The calculations

$$a \cdot^{op} e = ea$$

and

$$e \cdot^{op} a = ae$$

show that e is an identity element for S^{op} if and only if e is an identity element for S. In particular S^{op} is a monoid with identity element e if and only if S is a monoid with identity element e.

Suppose that S is a group. Then it is easy to see that S^{op} is a group. If $a, b \in S$ then b is an inverse of a in S^{op} if and only if b is an inverse of a in S; thus a^{-1} is unambiguous.

Now back to part (d) follows by part (c). Suppose that a has a right inverse d in S and $ba = ca$. Then d is a left inverse for a in S^{op} and $a \cdot^{op} b = a \cdot^{op} c$. Assume part (c) holds for *all* monoids, in particular for S^{op}. Then $b = c$.

A group is a non-empty set with an associative binary operation in which certain equations can always be solved.

Proposition 1 *Suppose that S is a non-empty set with associative binary operation. Then the following are equivalent:*

(a) *S is a group.*

(b) *For all $a, b \in S$ there are $x, y \in S$ such that $ax = b$ and $ya = b$.*

When either (a) or (b) is satisfied then $ax = b$ and $ya = b$ have unique solutions.

Proof: We first show that part (a) implies part (b) and when part (a) is satisfied the uniqueness claim holds.

Suppose that S is a group and let $a, b, c \in S$. If $ac = b$ then multiplying both sides of the equation on left by a^{-1} yields

$$a^{-1}b = a^{-1}(ac) = (a^{-1}a)c = ec = c.$$

Thus the equation $ax = b$ has *at most one* solution in S. Since

$$a(a^{-1}b) = (a^{-1}a)b = eb = b$$

the equation $ax = b$ has *at least one* solution in S. Therefore $ax = b$ has a unique solution in S. Replacing S by the group S^{op} we conclude that $a \cdot^{op} y = b$, or equivalently $ya = b$, has a unique solution which is $y = a \cdot^{op} b = ba^{-1}$.

To complete the proof we show that part (b) implies part (a). Suppose that part (b) holds. Note that S^{op} is associative and part (b) holds for S^{op}

also. Since S is not empty there exists an element $a \in S$. By assumption there is an element $e_a \in S$ such that $ae_a = a$. Let $b \in S$. Then $ya = b$ for some $y \in S$ by assumption. By associativity

$$be_a = (ya)e_a = y(ae_a) = ya = b.$$

Therefore e_a is a right identity element for S. Replacing S by S^{op} we conclude that S^{op} has a right identity element f_a. Now f_a is a left identity element for S. By part (a) of Lemma 1 it follows that $e_a = f_a$ and is thus $e = e_a$ is an identity element for S.

Now let a be any element of S. By assumption there are $c, b \in S$ such that $ac = e$ and $ba = e$. Thus $b = c$ by part (b) of Lemma 1. We have shown that a has an inverse in S. $\square$

The axioms for a group can ostensibly be weakened.

Proposition 2 *Let S be a set with associative binary operation. Suppose that S has a left identity element e and that every element $a \in S$ has a left inverse a', meaning $a'a = e$. Then S is a group.*

PROOF: (Sketch). Let e be a left identity element of S. Then the equation $x^2 = x$ has exactly one solution in S, namely $x = e$. Let $a \in S$ and suppose that $a' \in S$ is a left inverse for a. Then aa' satisfies the equation $x^2 = x$ which means $aa' = e$. Thus $a'a = e = aa'$. The calculation $ae = a(a'a) = (aa')a = ea = a$ shows that e is a right identity element for S as well and therefore is an identity element for S. $\square$