GROUPS

BURTON ROSENBERG

Definition 1 (Albert)**.** *A Group is a non-empty set G along with an operation $\cdot$ satisfying,*

(1) *closure: for all $g, h \in G$, then $g \cdot h$ is in G;*
(2) *associativity: for all $f, g, h \in G$, $f \cdot (g \cdot h) = (f \cdot g) \cdot h$;*
(3) *solutions to equations: for any $a, b \in G$ there exist $x, y \in G$ such that $a \cdot x = b$ and $y \cdot a = b$.*

This definition is found in A. Adrian Albert's MODERN HIGHER ALGEBRA. There are other ways to define a group. Although all definitions are equivalent, this is my favorite definition. However, it is not the most common definition. More common is to define a group by existence of inverses and an identity element. Inverses and identity elements are nice, but the reason one wants a group is so that one can solve equations. This definition makes this clear and moves forward minimally from that simple requirement.

Because this definition is less common, I am providing this note which gives a proof of the equivalence of this definition and the more common definition.

We first show the necessary existence in a group of an identity element, which is both a "'left-hand" and a "right-hand" identity, which we will call e, which for all $g \in G$ gives $eg = ge = g$.

Since we can solve equations, we can solve $e_l g = g e_r = g$ for a certain $g \in G$. For some other $g' \in G$, write $g' = gc = dg$, again since we can solve equations. Then,

$$e_l g' = e_l(gc) = (e_l g)c = gc = g'$$

and

$$g' e_r = (dg)e_r = d(ge_r) = dg = g'$$

so for all $g \in G$ we have $e_l g = g$ and $ge_r = g$. Putting e_r in for g in the first equation gives $e_l e_r = e_r$; putting e_l in for g in the second equation gives $e_l e_r = e_l$, so $e_l = e_r$. Calling the common element e, we have $eg = ge = g$ for all $g \in G$.

We now explore the uniqueness of this element. Given any solution to the left identity equation $e_l g = g$, solve $e = gx$, and write,

$$e_l = e_l e = e_l g x = g x = e.$$

Likewise, the right identity equation $ge_r = g$ implies $e_r = e$. Hence e is the only solution to $gx = xg = g$ for all and any $g \in G$.

Date: Last update 2 February 2009 / Created 23 January 2009.

Concerning inverses, we next show that left and right inverses are the same. That is, for every $g, e \in G$ there is a g' such that $gg' = e$, and for that g', a g'' such that $g'g'' = e$. Then,

$$gg' = e = g'g'' = (g'e)g'' = (g'(gg'))g'' = g'(g(g'g'')) = g'(ge) = g'g.$$

Consider a second solution, $gg'' = e$. Then,

$$g' = g'e = g'(gg'') = (g'g)g'' = (gg')g'' = eg'' = g''.$$

So the solution to $gx = e$ is unique, and is the same as the solution to $xg = e$, for all $g \in G$. This solution is the inverse of g, denoted g^{-1}. From this it follows $(g^{-1})^{-1} = g$, since they both g and $(g^{-1})^{-1}$ solve $g^{-1}x = e$.

Finally, considering a general equation $ax = b$, for any $a, b \in G$, it follows that $b^{-1}ax = e$, so x is unique, as it is the inverse of $b^{-1}a$. Since $x = a^{-1}b$ works, then this must be the unique solution. Likewise, the unique solution of $xa = b$ is $x = ba^{-1}$.

This gives the following theorem.

Theorem 1. *For a group G,*

1. *There exists a unique identity element e such that for any $g \in G$, $ge = eg = g$.*
2. *For any $g, e' \in G$ if either $ge' = g$ or $e'g = g$ then $e' = e$.*
3. *For every $g \in G$ there is a unique $g^{-1} \in G$ such that, $gg^{-1} = g^{-1}g = e$.*
4. *With the above notation, $(g^{-1})^{-1} = g$.*
5. *The solution $ax = b$ is unique, and is $x = a^{-1}b$. The solution to $xa = b$ is unique, and is $x = ba^{-1}$.*

For comparison, here is Serge Lang's definition for a group (see Algebra):

Definition 2 (Lang)**.** *A group is a non-empty set G along with an operation $\cdot$ satisfying,*

1. *closure;*
2. *associativity;*
3. *identity element: there exists an element $e \in G$ such that for all $x \in G$, $ex = xe = x$;*
4. *inverses: for every $g \in G$ exists an $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = e$.*

These axioms can in fact be weakened so that only a one-sided identity and inverse is demanded, since it follows that such an identity or inverse would be two sided (and unique).

Like I said, rather than focus on special elements, I like to think of equation solving as the heart of a group. Just as we started from equation solving and derived the existence (and uniqueness) of an identity and inverse, so can one start from the existence of (even one-sided) identity and inverse elements and derive the equation solving axioms. So the two foundations describe the same concept.