The Definition of Subgroup

09/14/06 Radford

There are three logically equivalent ways of describing the same structure listed in the proposition below. The first may be viewed as conceptual and the third as practical.

Proposition 1 *Let G be a group and let H be a subset of G. Then the following are logically equivalent:*

(a) *For $a, b \in H$ the product $ab \in H$ and the restriction of the binary operation $H \times H \longrightarrow H$ for G to H endows H with a group structure.*

(b) *$e \in H$, $ab \in H$ for all $a, b \in H$, and $a^{-1} \in H$ for all $a \in H$.*

(c) *$H \neq \emptyset$ and $ab^{-1} \in H$ for all $a, b \in H$.*

Proof: To show that any of the statements implies any of the others, we need only show that (a) implies (b), (b) implies (c), and (c) implies (a).

Suppose that (a) holds. Then products in H are computed as products in G. Let $e' \in H$ be the neutral element of H. Then e' satisfies the equation $x^2 = x$ in G. Since the neutral element e of G is the only solution to this equation, $e' = e$. Therefore $e \in H$. By assumption $ab \in H$ for all $a, b \in H$. Let $a \in H$. Since H is a group there exists an $a' \in H$ which satisfies $a'a = e' = aa'$. Since $e = e'$ by definition a' is an inverse in G for a. By uniqueness of inverses $a' = a^{-1}$. Therefore $a^{-1} \in H$ and (b) follows.

Suppose that (b) holds. Then $H \neq \emptyset$ since $e \in H$. That $ab^{-1} \in H$ for all $a, b \in H$ follows directly by assumption. Therefore (b) implies (c).

Suppose that (c) holds. Since $H \neq \emptyset$ there is an element in H. Choose one and call it a. With $b = a$ we have $e = aa^{-1} = ab^{-1} \in H$. Let $a \in H$. Since $e \in H$ it now follows that $a^{-1} = ea^{-1} \in H$. Now suppose that $a, b \in H$. Since $b^{-1} \in H$ the product $ab = a(b^{-1})^{-1} \in H$. We have established (a). Our proof is complete. $\square$

Any one of the statements (a), (b), and (c) can be taken to be the the definition of subgroup since they are all logically equivalent.