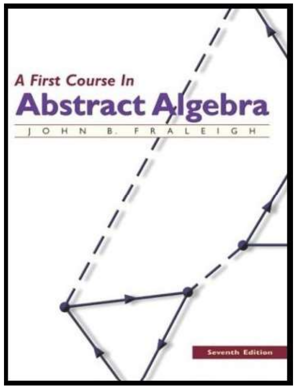
Introduction to Modern Algebra

Part I. Groups and Subgroups
I.5. Subgroups



Theorem 5.14.

Theorem. 5.14. A subset H of a group G is a subgroup of G if and only if

(1) H is closed under the binary operation of G,

(2) the identity element e of G is in H,

(3) for all $a \in H$ we have $a' = a^1 \in H$.

Proof. If H is a subgroup of G, then (1) holds since H is a group. Also, the equation $ax = a$ has an unique solution in both G and H (Theorem 4.10) since both are groups. This unique solution in G is e and so e is also the unique solution in H. Hence $e \in H$ and (2) follows. Similarly, the equation $ax = e$ has an unique in both G and H and so $a' = a^{-1} \in H$ for all $a \in H$ and (3) holds.

Theorem 5.14. (continued)

Theorem 5.14. A subset H of a group G is a subgroup of G if and only if

(1) H is closed under the binary operation of G,

(2) the identity element e of G is in H,

(3) for all $a \in H$ we have $a' = a^1 \in H$.

Proof (continued). Now suppose $H \subset G$ and $(1), (2), (3)$ hold. Then (2) $\Longrightarrow$ there is an identity in H and G_2 holds for H. Similarly (3) $\Longrightarrow$ for each $a \in H$, there is an inverse of a in H and G_3 holds for H. Since the binary operation is associative in G_1 then it is associative in H ((1) is needed here to guarantee that all of the results of the binary operation are in H in the equation $a * (b * c) = (a * b) * c$ for $a, b, c \in H$). It is said that H "inherits" the associativity of $*$ from G. □

Theorem 5.17.

Theorem 5.17. Let G be a multiplicative group and let $a \in G$. Then $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G and is the "smallest" subgroup of G that contains a (that is, every subgroup of G which contains 'a' contains all the elements of H).

Proof. Let $x, y \in H$. Then $x = a^r$ and $y = a^s$ for some $r, s \in \mathbb{Z}$. So $xy = a^r a^s = a^{r+s} \in H$ and (1) of Theorem 5.14 holds. By definition, $a^0 = e$ and (2) of Theorem 5.14 holds. For any $a^r \in H$, we have $a^{-r} \in H$ and since $a^r a^{-r} = a0 = e$, then $(a^r)' = (a^r)^{-1} \in H$ and (3) of Theorem 5.14 holds.

So H is a subgroup of G by Theorem 5.14. Now, let K be a subgroup of G containing a. Then, by the definition of group $e, a^{-1} \in K$. Since K is closed under the binary operation, then (by mathematical induction) all positive powers of a and all positive powers of a^{-1} are in K. That is, $H \subset K$. Therefore H is the "smallest" subgroup of G containing a. □