

### Proof of the Subgroup Theorem

**Definition.** Let  $(G, *)$  be a group, and let  $H \subseteq G$  be a subset of the set  $G$ . If  $(H, *)$  itself is a group, then we say  $H$  is a **subgroup** of  $G$ .

---

In this handout, I'll write out a proof of the following theorem, which is essentially Theorem 5.1 in Saracino's book. I'll also state and prove some slight variants. Here's the theorem:

**Theorem.** Let  $G$  be a group, and let  $H \subseteq G$  be a subset. The following are equivalent:

- A.  $H$  is a subgroup of  $G$  [as defined above]
- B.  $H$  satisfies all of the following properties:
  - 0.  $e \in H$
  - 1. For all  $h_1, h_2 \in H$ , we have  $h_1 h_2 \in H$ .
  - 2. For all  $h \in H$ , we have  $h^{-1} \in H$

---

**Notes:**

i. In the original definition of subgroup above, I really should have said  $(H, *_H)$  is a group, where  $*_H$  is the function with domain  $H \times H$  (rather than domain  $G \times G$ , which is the domain of  $*$ ) given by the rule  $h_1 *_H h_2 = h_1 * h_2$ . That is, technically  $*$  and  $*_H$  have different domains, so they are technically different functions, even if they are given by the same formula.

That said, in the proof below, for any two elements  $x, y$  of either  $G$  or  $H$ , we will simply write  $xy$  for  $x * y$ , as there is no danger of a double meaning. (In particular, if  $x, y \in H$ , then  $x *_H y = x * y$  by definition of  $*_H$ , so  $x *_H y$  and  $x * y$  are both simply equal to  $xy$ .)

ii. Condition 1 in part (B) of the theorem above is often stated as “ $H$  is closed under  $*$ ”

iii. Condition 2 in part (B) of the theorem above is often stated as “ $H$  is closed under inverses”

iv. In the proof below, as usual, any [comments in square brackets] are not actually part of the proof, but simply my side commentary.

---

**Proof of Theorem.** (A  $\Rightarrow$  B): Since  $(H, *_H)$  is a group, there is an element  $e_H \in H$  that is the identity for the binary operation  $*_H$  on  $H$ .

We claim that  $e_H = e$ , i.e., that the identity of  $H$  is the same as the identity of  $G$ .

[Warning: We don't know that yet! At first blush, it's conceivable that different rules apply to  $G$  and  $H$ , and so maybe somehow these two groups have different identity elements! So we actually have something to prove in this claim.]

In particular, then,  $e_H e_H = e_H$ , since  $e_H$  is the identity in the group  $H$ .

We wrote down the above equality thinking in terms of working inside the group  $H$ , but of course it is also true viewing it as an equality inside the larger group  $G$ . Recall from an earlier result from class that for any  $x, g \in G$ , if  $gx = g$ , then  $x = e$ . Thus, with  $g = x = e_H \in G$  in the above equation, it follows that  $e_H = e$ .

In particular,  $e = e_H \in H$ , proving statement (0) of B.

For statement (1): Given  $h_1, h_2 \in H$ , then because  $*_H$  is a binary operation on  $H$  (since  $(H, *_H)$  is a group), it follows by definition of binary operation that  $h_1 h_2 \in H$ , proving statement (1) of B.

For statement (2): Given  $h \in H$ , let  $\tilde{h} \in H$  be the inverse of  $h$  in  $H$ .

[Again, similar to what happened with  $e$  versus  $e_H$ , it's conceivable that the inverse  $\tilde{h}$  in  $H$  is different from the inverse  $h^{-1}$  in the bigger group  $G$ .]

So  $h\tilde{h} = e_H = e$ , where the second equality is by the claim earlier in this proof. Viewing this equation as an equation involving elements of  $G$  rather than  $H$ , then by another proposition from class (which is also Theorem 3.5 in the book), we have  $\tilde{h} = h^{-1}$ .

In particular,  $h^{-1} = \tilde{h} \in H$ , proving statement (2) of B.

QED ( $A \Rightarrow B$ )

( $B \Rightarrow A$ ): We check the four conditions for  $(H, *_H)$  to be a group:

**Binary Operation:** Given  $h_1, h_2 \in H$ , we have  $h_1h_2 \in H$  by statement (1) of B, as desired.

**Associative:** Given  $a, b, c \in H$ , then  $a, b, c \in G$ , so  $(ab)c = a(bc)$ , as desired.

**Identity:** By statement (0) of B, we have  $e \in H$ . We claim that this element of  $H$  works as the identity of  $H$ . Indeed, for any  $h \in H$ , we have  $he = eh = h$ , as desired.

**Inverses:** Given  $h \in H$ , by statement (2) of B we have  $h^{-1} \in H$ . We claim that this element of  $H$  is the inverse of  $h$  in  $H$ . Indeed, we have  $h^{-1}h = hh^{-1} = e$ , as desired. **QED Theorem**

**Variant #1:** In the Theorem, we can replace statement (0) of B [that  $e \in H$ ] by the statement:

0'.  $H$  is nonempty

(This is still in combination with statements (1) and (2), of course.)

**Variant #2:** In both the Theorem and in Variant #1, we can replace the two statements (1) and (2) of B by the single statement:

1'. For all  $h_1, h_2 \in H$ , we have  $h_1h_2^{-1} \in H$ .

(This is still in combination with either statement (0) or statement (0'), of course.)

**Proof of Variant #1.** Clearly statement (0) implies statement (0').

Conversely, given all three of statements (0'), (1), and (2), we have that there exists some  $h \in H$ , since  $H \neq \emptyset$  by (0').

Therefore, by statement (2), we have  $h^{-1} \in H$ .

Therefore, by statement (1), since  $h, h^{-1} \in H$ , we have  $e = hh^{-1} \in H$ , proving statement (0) as desired. **QED Variant #1**

**Proof of Variant #2.** Assuming statements (1) and (2), we will show (1'). Given any  $h_1, h_2 \in H$ , we have  $h_2^{-1} \in H$  by statement (2).

Therefore, by statement (1), we have  $h_1h_2^{-1} \in H$ , as desired.

Conversely, given both statements (0) and (1'), given any  $h \in H$ , we have  $e \in H$  by statement (0), and hence by statement (1'), we have  $h^{-1} = eh^{-1} \in H$ , proving statement (2).

To prove statement (1), given  $h_1, h_2 \in H$ , since we now know that statement (2) holds, we have  $h_2^{-1} \in H$ . Therefore, by statement (1') applied to  $h_1$  and  $h_2^{-1}$ , we have  $h_1h_2 = h_1(h_2^{-1})^{-1} \in H$ , as desired.

Finally, we also need to show, assuming statements (0') and (1'), that statement (0) holds. [And therefore statements (0) and (1') hold, so by what we just showed, statements (1) and (2) must hold as well.]

To see this, by statement (0'), there exists some  $h \in H$ . Therefore, by statement (1'), we have  $e = hh^{-1} \in H$ , proving statement (0). **QED Variant #2**