

§9 Subgroups

A group is a set with a binary operation on it which has some nice properties. Being a set, a group has subsets. Naturally, we are more interested in those subsets which reflect the algebraic structure of the group than in the other subsets. They help us understand the structure of the group. Foremost among them are the sets which are groups themselves. We give them a name.

9.1 Definition: Let G be a group. A nonempty subset H of G is called a *subgroup of G* if H itself is a group under the operation on G .

We write $H \leq G$ to express that H is a subgroup of G . Clearly, G is a subgroup of G , so $G \leq G$. If H is a subgroup of G and a proper subset of G , i.e., if $H \leq G$ and $H \subset G$, we call H a *proper subgroup of G* . In this case, we write $H < G$. The notations $H \not\leq G$ and $H \not< G$ mean that H is not a subgroup respectively not a proper subgroup of G .

Given a group G and a nonempty subset H of G , we must check the group axioms for H in order to determine whether H is a subgroup of G . We now discuss each one of these axioms. It turns out that we can do without some of them.

First of all, there must be a binary operation on H . The operation on H is the operation on G . More precisely, the operation on H is the restriction of the operation on G to H . Hence, for $a, b \in H$, the element ab is computed as the product of a and b in G . In order to have a binary operation on H , given by $(a, b) \rightarrow ab$ as in G , it is necessary and sufficient that $ab \in H$ for all $a, b \in H$. Hence H must be closed under the multiplication on G . Then and only then is there a binary operation on H that is the restriction of the multiplication on G .

In the second place, we must check associativity. For all $a, b, c \in H$, we must show $(ab)c = a(bc)$. But we know that $(ab)c = a(bc)$ for all $a, b, c \in G$.

Since $H \subseteq G$, we have all the more so $(ab)c = a(bc)$ for all $a, b, c \in H$. Indeed, if all the elements of G have a certain property, then all the elements of H will have the same property. Thus associativity holds in H automatically, so to speak. We do not have to check it.

In H , there must exist an identity, say $1_H \in H$ such that $a1_H = a$ for all $a \in H$. In particular, the identity 1_H of H has to be such that $1_H1_H = 1_H$. Since $1_H \in H \subseteq G$, Lemma 7.3(1) yields $1_H = 1_G =$ identity element of G . So the identity element of G is also the identity element of H , *provided it belongs to H* . Then we do not have to look for an identity element of H , we must only check that the identity element of G does belong to H . We write 1 for the identity element of H , since it is the identity element of G .

Finally, for each $a \in H$, there must exist an $x \in H$ such that $ax = 1$. Reading this equation in G , we see $x = a^{-1} =$ the inverse of a in G . We know that the inverse of a exists. Where? The inverse of a exists in G . We must also check $a^{-1} \in H$. Thus we do not have to look for an inverse of a . We must only check that the inverse a^{-1} of a , which we know to be in G , is in fact an element of H .

Summarizing this discussion, we see that a nonempty subset H of a group G is a subgroup of G if and only if

- (1) $ab \in H$ for all $a, b \in H$,
- (2) $1 \in H$,
- (3) $a^{-1} \in H$ for all $a \in H$.

Moreover, (2) follows from (1) and (3). Indeed, if $a \in H$ (remember that $H \neq \emptyset$), then $a^{-1} \in H$ by (3) and hence $aa^{-1} \in H$ by (1), which gives $1 \in H$. So (1),(2),(3) together is equivalent to (1),(3) together. We proved the following lemma.

9.2 Lemma (Subgroup criterion): *Let G be a group and let H be a nonempty subset of G . Then H is a subgroup of G if and only if*

(i) *for all $a, b \in H$, we have $ab \in H$ (H is closed under multiplication) and*

(ii) *for all $a \in H$, we have $a^{-1} \in H$ (H is closed under the forming of inverses). □*

So we can dispense with checking $1 \in H$ when we know $H \neq \emptyset$. On the other hand, when we do not know a priori that $H \neq \emptyset$, the easiest way to ascertain $H \neq \emptyset$ may be to check that $1 \in H$.

When our subset is finite, we can do even better.

9.3 Lemma: (1) *Let G be a group and let H be a nonempty finite subset of G . Then H is a subgroup of G if and only if H is closed under multiplication.*

(2) *Let G be a finite group and let H be a nonempty subset of G . Then H is a subgroup of G if and only if H is closed under multiplication.*

Proof: (1) We prove that 9.2(ii) follows from 9.2(i) when H is finite, so that 9.2(i) and 9.2(ii) are together equivalent to 9.2(i), which is the claim. So, for all $a \in H$, we must show that $a^{-1} \in H$ under the assumption that H is finite and closed under multiplication.

If $a \in H$ and H is closed under multiplication, we have $aa = a^2 \in H$, $a^2a = a^3 \in H$, ..., in general $a^n \in H$ for all $n \in \mathbb{N}$. The infinitely many elements $a, a^2, a^3, \dots, a^n, \dots$ of H cannot be all distinct, because H is a finite set. Thus $a^m = a^k$ for some $m, k \in \mathbb{N}$, $m \neq k$. Without loss of generality, let us assume $m > k$. Then

$$a^{m-k-1}a = a^{m-k} = a^m a^{-k} = a^m (a^k)^{-1} = a^m (a^m)^{-1} = 1,$$

so that $a^{-1} = a^{m-k-1} \in H$. So H is closed under the forming of inverses.

(2) This follows from (1), since any subset of a finite set is finite. □

9.4 Examples: (a) For any group G , the subsets $\{1\}$ and G are subgroups of G . Here $\{1\}$ is called the *trivial subgroup of G* .

(b) If $K \leq H$ and $H \leq G$, then K is clearly a subgroup of G .

(c) Let $4\mathbb{Z} = \{4z \in \mathbb{Z} : z \in \mathbb{Z}\} = \{u \in \mathbb{Z} : 4|u\} \subseteq \mathbb{Z}$. Now \mathbb{Z} is a group under addition (Example 7.1(a)), and $4\mathbb{Z}$ is closed under addition and under the forming of inverses by Lemma 5.2(5) and Lemma 5.2(1):

(i) if $x, y \in 4\mathbb{Z}$, then $4|x$ and $4|y$, then $4|x + y$, so $x + y \in 4\mathbb{Z}$,

(ii) if $x \in 4\mathbb{Z}$, then $4|x$, then $4|-x$, so $-x \in 4\mathbb{Z}$.

Hence $4\mathbb{Z} \leq \mathbb{Z}$.

(d) The additive group \mathbb{Z} is a subgroup of the additive group \mathbb{Q} . Also, we have $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, where the group operation is ordinary addition.

(e) Under multiplication, $\mathbb{Q}^+ := \{x \in \mathbb{Q} : x > 0\}$ is a subgroup of $\mathbb{Q} \setminus \{0\}$, since

(i) the product of two positive rational numbers is a positive rational number, and

(ii) the reciprocal, that is, the multiplicative inverse $\frac{1}{a}$ of any

positive rational number a is a positive rational number.

($\mathbb{Q} \setminus \{0\}$ is a group under multiplication by §7, Ex.1(b).) Also, $\mathbb{Q}^+ \leq \mathbb{R}^+$ (see Example 7.1(b)) and $\mathbb{Q} \setminus \{0\} \leq \mathbb{R} \setminus \{0\}$. We have in fact $\mathbb{Q}^+ = (\mathbb{Q} \setminus \{0\}) \cap \mathbb{R}^+$.

(f) If H_1 and H_2 are subgroups of G , then $H_1 \cap H_2$ is a subgroup of G . Indeed, $H_1 \cap H_2 \neq \emptyset$ since $1 \in H_1$ and $1 \in H_2$. Also

(i) $a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1$ and $a, b \in H_2 \Rightarrow ab \in H_1$ and $ab \in H_2 \Rightarrow ab \in H_1 \cap H_2$

(ii) $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2 \Rightarrow a^{-1} \in H_1$ and $a^{-1} \in H_2 \Rightarrow a^{-1} \in H_1 \cap H_2$.

Thus $H_1 \cap H_2 \leq G$. More generally, if H_i are subgroups of G , where i runs through an index set I , then $\bigcap_{i \in I} H_i \leq G$. Indeed, $\bigcap_{i \in I} H_i \neq \emptyset$ since $1 \in H_i$ for all $i \in I$ and

(i) $a, b \in \bigcap_{i \in I} H_i \Rightarrow a, b \in H_i$ for all $i \in I \Rightarrow ab \in H_i$ for all $i \in I \Rightarrow ab \in \bigcap_{i \in I} H_i$

(ii) $a \in \bigcap_{i \in I} H_i \Rightarrow a \in H_i$ for all $i \in I \Rightarrow a^{-1} \in H_i$ for all $i \in I \Rightarrow a^{-1} \in \bigcap_{i \in I} H_i$

(g) Let $S_{[0,1]}$ be the set of all one-to-one mappings from $[0,1]$ onto $[0,1]$, which is a group under the composition of mappings (Example 7.1(d)). Consider

$$T = \{\alpha \in S_{[0,1]} : 0\alpha = 0\}.$$

Then T is a subgroup of $S_{[0,1]}$, for T is not empty (why?) and

(i) $\alpha, \beta \in T \Rightarrow 0\alpha = 0$ and $0\beta = 0 \Rightarrow 0(\alpha\beta) = (0\alpha)\beta = 0\beta = 0 \Rightarrow \alpha\beta \in T$,

(ii) $\alpha \in T \Rightarrow 0\alpha = 0 \Rightarrow 0\alpha\alpha^{-1} = 0\alpha^{-1} \Rightarrow 0I = 0\alpha^{-1} \Rightarrow 0 = 0\alpha^{-1} \Rightarrow \alpha^{-1} \in T$.

(h) Let $U = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \subseteq \mathbb{Z}_8$ and consider the multiplication in \mathbb{Z}_8 . We see

$$\begin{array}{cccc} \bar{1} \bar{1} = \bar{1} & \bar{1} \bar{3} = \bar{3} & \bar{1} \bar{5} = \bar{5} & \bar{1} \bar{7} = \bar{7} \\ \bar{3} \bar{1} = \bar{3} & \bar{3} \bar{3} = \bar{1} & \bar{3} \bar{5} = \bar{7} & \bar{3} \bar{7} = \bar{5} \\ \bar{5} \bar{1} = \bar{5} & \bar{5} \bar{3} = \bar{7} & \bar{5} \bar{5} = \bar{1} & \bar{5} \bar{7} = \bar{3} \\ \bar{7} \bar{1} = \bar{7} & \bar{7} \bar{3} = \bar{5} & \bar{7} \bar{5} = \bar{3} & \bar{7} \bar{7} = \bar{1} \end{array}$$

so U is closed under multiplication. Since \mathbb{Z}_8 is a finite set, U is a subgroup of \mathbb{Z}_8 by Lemma 9.3. Right? No, this is wrong. This would be correct if \mathbb{Z}_8 were a group under multiplication, which it is not (for instance, $\bar{0}$ has no inverse by Lemma 6.4(12)). \mathbb{Z}_8 is a group under addition, but this is something else. When we want to use Lemma 9.2 or Lemma 9.3, we must make sure that the larger set is a group.

Nevertheless, U is a group under multiplication:

- (i) U is closed under multiplication by the calculations above.
- (ii) Multiplication on U is associative since it is in fact associative on \mathbb{Z}_8 (Lemma 6.4(7)).
- (iii) $\bar{1} \in U$ and $\bar{a} \bar{1} = \bar{a}$ for all $\bar{a} \in U$. This follows from our calculations or from Lemma 6.4(8). So $\bar{1}$ is an identity element of U .
- (iv) Each element of U has an inverse in U . This follows from the equations $\bar{1} \bar{1} = \bar{1}$, $\bar{3} \bar{3} = \bar{1}$, $\bar{5} \bar{5} = \bar{1}$, $\bar{7} \bar{7} = \bar{1}$ and from $\bar{1}, \bar{3}, \bar{5}, \bar{7} \in U$.

So U is a group. Let us find its subgroups. Now we can use Lemma 9.3. This lemma shows that $\{\bar{1}, \bar{3}\}, \{\bar{1}, \bar{5}\}, \{\bar{1}, \bar{7}\}$ are subgroups of U since they are closed under multiplication. The reader will easily see that these are the only nontrivial proper subgroups of U . Hence the subgroups of U have orders 1, 2, 4, which are all divisors of the order $|U| = 4$ of U .

(i) $E := \{1, -1, i, -i\} \subseteq \mathbb{C} \setminus \{0\}$ is a subgroup of the group $\mathbb{C} \setminus \{0\}$ of nonzero complex numbers under multiplication by Lemma 9.3 as it is closed under multiplication. The same lemma shows that $\{1, -1\}$ is a subgroup of E . Also, E has no other nontrivial proper subgroup, for any subgroup of E that contains i or $-i$ must contain i^2, i^3, i^4 or $(-i)^2, (-i)^3, (-i)^4$ and thus must be E itself. So E has exactly three subgroups, one of order 1, one of order 2, one of order 4. Here, too, the orders of the subgroups are divisors of the order $|E| = 4$ of the group E .

(j) Lemma 9.3 may be false if the subset is not finite. For example, \mathbb{Z} is a group under addition, \mathbb{N} is a subset of \mathbb{Z} and \mathbb{N} is closed with respect to addition. Still, \mathbb{N} is not a subgroup of \mathbb{Z} since there is no additive identity in \mathbb{N} ($0 \notin \mathbb{N}$).

Exercises

1. Let G be a group and let H be a nonempty subset of G . Show that H is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.

2. Show that $n\mathbb{Z} := \{nz \in \mathbb{Z} : z \in \mathbb{Z}\} = \{u \in \mathbb{Z} : n|u\} \subseteq \mathbb{Z}$ is a subgroup of \mathbb{Z} (under addition), where n is any natural number.

3. Let $M = \{\alpha \in S_{[0,1]} : 0\alpha = 0 \text{ or } 1\alpha = 1\}$. Is M a subgroup of $S_{[0,1]}$ under multiplication?

4. Let $L = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\} \subseteq \mathbb{Z}_9$. Show that L is a group under multiplication. Find all subgroups of L . Do the orders of the subgroups divide the order $|L| = 6$ of the group L ?

5. Let G be a group and let $H \leq G$, $K \leq G$. Show that $H \cup K$ is not a subgroup of G unless $H \cup K = H$ or $H \cup K = K$. (The union of two subgroups is (generally) not a subgroup.)

6. Give an example of a group G and subgroups H, K, L of G such that $H \cup K \cup L \leq G$. (The union of three subgroups can be a subgroup.)

7. Let G be a group and let a be a fixed element of G . Determine whether the subsets

$$C = \{x \in G : ax = xa\} \quad \text{and} \quad D = \{x \in G : ax = xa \text{ or } ax = xa^{-1}\}$$

of G are subgroups of G .

8. In Example 9.4(h), why cannot we use Lemma 6.4(9) to prove that the axiom (iv) holds?