Consider a group $< G, \cdot >$ with an identity element e, $S^{'} = \{x \in G : x \neq x^{-1}\}$, and $S = \{x \in G : x = x^{-1}\}$. We take as fact that $G = S \cup S^{'}$. We denote the order of G to be $|G|$ and the set of whole numbers to be $\mathbb{W}$.

Statement 1. *$\exists n \in \mathbb{W}$ s.t. $|G| = n \Rightarrow \exists m \in \mathbb{W}$ s.t. $|S^{'}| = 2m$.*

Proof. Assume that the order of G is finite so that there is an $n_0 \in \mathbb{W}$ s.t. $|G| = n_0$. For sure, $|S^{'}| \neq n_0$ since $e \notin S^{'}$ and $S^{'} \subset G$, and is finite too. Let $m_0 \in \mathbb{W}$ be the order of $S^{'}$. It follows that $0 \leq m_0 < n_0$. Now partition $S^{'}$ into classes $S_i^{'} = \{x_i, x_i^{-1}\}$ of size 2. The partition of classes $S_i^{'}$ is finite. Since $S^{'} = \bigcup_i S_i^{'}$, it follows that the order of $S^{'}$ is even. □

Statement 2. *$\exists m_0 \in \mathbb{W}$ s.t. $|G| = 2 \cdot m_0 + 1 \Rightarrow |S| = 2 \cdot n_0 + 1$ for some $n_0 \in \mathbb{W}$.*

Proof. Since $|G| = |S| + |S^{'}|$ and $|S^{'}| = 2 \cdot r_0$ for an $r_0 \in \mathbb{W}$, $|S| = (2 \cdot m_0 + 1) - 2 \cdot r_0 = 2(m_0 - r_0) + 1$. Since $2 \cdot m_0 + 1 = |G| > |S^{'}| = 2 \cdot r_0$, $(m_0 - r_0) > -\frac{1}{2}$. But $m_0, r_0 \in \mathbb{W}$, so $m_0 - r_0 \in \mathbb{W}$ is a whole number greater than $-\frac{1}{2}$. Therefore, $|S|$ is an odd number. □

A similar proof yields the fact that if $|G|$ is even, then $|S|$ is even.

Statement 3. *$|G|$ is even implies that there is an $x \in G$ such that $x \in S - \{e\}$.*

Proof. Because $|G|$ is even, $|S|$ is even. Now since $|S|$ is even and $e \in S$, $|S|$ is at least 2. Therefore, there is an $x \in G$ such that $x^2 = e$ and $x \neq e$. □

Statement 4. *Consider G to be Abelian and finite. Then*

$$(\prod_{a \in G} a)^2 = e.$$

Proof. Since G is Abelian, we may pair an $a_i \in G$ in the first term $\prod_{a \in G} a$ with its unique inverse from the second term $\prod_{a \in G} a$. This pairing is done for each element of G. □

Statement 5. *Let G be an Abelian finite group. If $x \in S^{'}$ for all $x \in G - \{ e \}$, then $\prod_{a \in G} a = e$.*

Proof. For each $a \in G$, pair with its unequal inverse a^{-1}. □

The proof of Statement 6 follows similarly to the proof of Statement 5.

Statement 6. *Consider G to be a finite Abelian group. If $S = \{ x, e \}$ where $x \neq e$, then*

$$x = \prod_{a \in G} a.$$

We can establish that $H \subset G$ is a subgroup of G if we can show that

(1) $e \in H$ (Closed under identity)
(2) $\forall x, y \in H$, $x \cdot y \in H$ (Closed under the operation) and
(3) $\forall x \in H, x^{-1} \in H$ (Closed under inverses)

Statement 7. *Consider an Abelian group $< G, \cdot >$. Then S is a subgroup of G.*

Proof. $e \in S$ and so S is nonempty. Let $x_0, y_0 \in S$ so that $x_0 = x_0^{-1}$ and $y_0 = y_0^{-1}$. Since $(x_0 \cdot y_0)^{-1} = y_0^{-1} \cdot x_0^{-1} = y_0 \cdot x_0 = x_0 \cdot y_0$, $x_0 \cdot y_0 \in S$. Also, $x_0^{-1} = x_0 \in S$. Therefore S is a subgroup of G. □

Statement 8. *Consider an Abelian group G and let $n \in \mathbb{W}$. Then*

$$H = \{ \ x \in G : x^n = e \ \}$$

is a sugbroup of G.

The Abelian subgroup from Statement 8 is encountered in Complex Analysis.

Proof. Since $e^n = e$, $H \neq \emptyset$. Let $x_0, y_0 \in H$ so that $e = x_0^n \cdot y_0^n = (x_0 \cdot y_0)^n$. Hence $x_0 \cdot y_0 \in H$. Also, since $x_0 \in H$, $x_0^n = e$. So $e = e^{-1} = (x_0^n)^{-1} = (x_0^{-1})^n$. Thus $x_0^{-1} \in H$. Therefore H is a subgroup of G. $\square$

Statement 9. *Consider an Abelian group $< G, \cdot >$.*

$$H = \left\{ \ x \in G : x = y^2 \text{for some } y \in G \right\}$$

is a subgroup of G.

Proof. $e \in H$ since $e = e \cdot e$. So $e \in H \neq \emptyset$. Let $x_0, y_0 \in H$ so that there is an $m_0, n_0 \in G$ s.t. $x_0 = m_0^2$ and $y_0 = n_0^2$. So $x_0 \cdot y_0 = m_0^2 \cdot n_0^2 = (m_0 \cdot n_0)^2$. Thus $x_0 \cdot y_0 \in H$. Also, $e = x_0 \cdot x_0^{-1} = m_0^2 \cdot x_0^{-1}$ implies that $x_0^{-1} = (m_0^{-1})^2$. Hence $x_0^{-1} \in H$. Therefore H is a subgroup of G. $\square$

Statement 10. *Consider an Abelian group $< G, \cdot >$ and a subgroup H.*

$$K = \left\{ \ x \in G : x^2 \in H \ \right\}$$

is a subgroup of G.

Proof. K is nonempty since $e \in G$ and $e^2 \in H$. Let $x_0, y_0 \in K$ so that $x_0^2, y_0^2 \in H$. Because G is Abelian, $(x_0 \cdot y_0)^2 = x_0^2 \cdot y_0^2 \in H$. Thus $x_0 \cdot y_0 \in K$. Since $x_0^2 \in H$ and H is a subgroup of G, $(x_0^{-1})^2 = (x_0^2)^{-1} \in H$. Hence $x_0^{-1} \in K$. Therefore K is a subgroup of G. $\square$

Statement 11. *Consider an Abelian group $< G, \cdot >$ and a subgroup H. Then*

$$K = \{ \ x \in G : \text{ for some } n \in \mathbb{N}, \ x^n \in H \ \}$$

is a subgroup of G

Proof. K is nonempty since $e \in K$. Let $x_0, y_0 \in K$ so that there is an $m, n \in \mathbb{N}$ such that x_0^m, $y_0^n \in H$. So $(x_0 \cdot y_0)^{mn} = x_0^m \cdot y_0^n \in H$. Thus $x_0 \cdot y_0 \in K$. Since $x_0 \in K, x_0^n \in H$ for some $n \in \mathbb{N}$. So $(x_0^{-1})^n = (x_0^n)^{-1} \in H$. Hence $x_0^{-1} \in K$. Therefore K is a subgroup of G. $\square$

Statement 12. *Consider an Abelian group $< G, \cdot >$ and its 2 subgroups H and K. Then*

$$HK = \{ \ x \cdot y : x \in H \wedge y \in K \ \}$$

is a subgroup of G.

Proof. $e \in HK$ since $e \in H$ and $e \in K$ and $e \cdot e = e$. Let $p_0 \cdot m_0, \ r_0 \cdot t_0 \in HK$ where $p_0, r_0 \in H$, and so $p_0 \cdot r_0 \in H$. Also, $m_0 \cdot t_0 \in K$. Since G is Abelian, $(p_0 \cdot m_0) \cdot (r_0 \cdot t_0) = (p_0 \cdot r_0) \cdot (m_0 \cdot t_0) \in HK$.

Because $p_0 \cdot m_0 \in HK$, $p_0^{-1} \in H$ and $m_0^{-1} \in K$. Since G is Abelian, $(p_0 \cdot m_0)^{-1} = m_0^{-1} \cdot p_0^{-1} = p_0^{-1} m_0^{-1} \in HK$. Thus $(p_0 \cdot m_0)^{-1} \in HK$.

Therefore HK is a subgroup of G. $\square$

Statement 13. *Let G be a group.*

$$H, K \text{ are subgroups of } G \Rightarrow H \cap K \text{ is a subgroup of } G.$$

Proof. Since H and K are subgroups of G, $e \in H \cap K$. Let $x_0, y_0 \in H \cap K$ so that $x_0, y_0 \in H,\ K$. Hence $x_0 \cdot y_0 \in H,\ K$. So $x_0 \cdot y_0 \in H \cap K$. Since $x_0^{-1} \in H,\ K$, so $x_0^{-1} \in H \cap K$. Therefore, if H and K are subgroups of G, then $H \cap K$ is a subgroup of G. □

The center of a group G refers to a set $\{\ a \in G : (\forall x \in G)(a \cdot x = x \cdot a)\ \}$.

Statement 14. *Consider the group* $< G, \cdot >$ *and its center* C*. Then* C *is a subgroup of* G*.*

Proof. First, the identity e is in C since by definition it commutes with all elements of the group G. Let $m, n \in C$ and $x \in G$ so that $x \cdot m = m \cdot x$ and $x \cdot n = n \cdot x$. From properties of a group, $x \cdot (m \cdot n) = (x \cdot m) \cdot n = (m \cdot x) \cdot n = m \cdot (x \cdot n) = m \cdot (n \cdot x) = (m \cdot n) \cdot x$. Thus $m \cdot n \in C$. Since $m \in C$, $m \cdot x = x \cdot m$. Now $m^{-1} \cdot m \cdot x = m^{-1} \cdot x \cdot m \Rightarrow x \cdot m^{-1} = m^{-1} \cdot x$. Thus $m^{-1} \in C$. Therefore C is a subgroup of G. □

Statement 15. *For a group* G*, we have that the set*

$$S = \left\{\ a \in G : \forall x \in G, (x \cdot a)^2 = (a \cdot x)^2\ \right\}$$

is a subgroup of G*.*

Proof. Note that $e \in S$ so that $S \neq \emptyset$. Let $a, b \in S$ and $x \in G$. We then have that because $b \cdot x \in G$, $(a \cdot (b \cdot x))^2 = ((b \cdot x) \cdot a)^2$. Now because $x \cdot a \in G$, $((b \cdot x) \cdot a)^2 = (b \cdot (x \cdot a))^2 = ((x \cdot a) \cdot b)^2 = (x \cdot (a \cdot b))^2$. We have shown that $((a \cdot b) \cdot x)^2 = (x \cdot (a \cdot b))^2$, i.e. that $a \cdot b \in S$. Now to show closure under inverse. We have that $(x \cdot a^{-1})^2 = ((a \cdot x^{-1})^{-1})^2 = ((a \cdot x^{-1})^2)^{-1} = ((x^{-1} \cdot a)^2)^{-1} = ((x^{-1} \cdot a)^{-1})^2 = (a^{-1} \cdot x)^2$ and thus $a^{-1} \in S$. Therefore S is a subgroup of G. □

Statement 16. *Consider* $< G, \cdot >$ *where* G *is finite and* $\emptyset \neq H \subset G$*.*

$$(\forall a, b \in H)\ (a \cdot b \in H) \Rightarrow H \text{ is a subgroup of } G$$

Proof. Let $a \in H$ and $n \in \mathbb{W}$ be the order of a so that a^n is the identity e of G. An inductive argument establishes that $a^k \in H$ for all non-negative integers k. It then follows that $e = a^n \in H$. All that remains to be shown is closure under inverses. We have that $e = a^n = a \cdot a^{n-1}$. It then follows that $a^{-1} = a^{n-1} \in H$. This completes the proof that H is a subgroup of G. □

We define what it means to say that an element of a group is a period of a function f.

Definition 1. *Let* G *be a group and* $f : G \to G$*. Then* $a \in G$ *is a period of* f *is to say that*

$$\forall x \in G,\ f(ax) = f(x)$$

Statement 17. *The set* $M = \{\ a \in G :\ a \text{ is a period of } f\ \}$ *is a subgroup of* G*.*

Proof. Let $a, b \in M$, $x \in G$, and $y = a^{-1} \cdot x$. So $f(a^{-1} \cdot x) = f(y) = f(a \cdot y) = f(a \cdot a^{-1} \cdot x) = f(x)$. So $f(a^{-1} \cdot x) = f(x)$ which is to say that $a^{-1} \in M$. Also, since $b, x \in G$, $b \cdot x \in G$. Thus, $f(a \cdot b \cdot x) = f(a \cdot (b \cdot x)) = f(b \cdot x) = f(x)$. Hence $a \cdot b \in M$. Therefore, M is a subgroup of G. □

Statement 18. *Consider the group* G *generated by* $a, b \in G$*.*

$$a \cdot b = b \cdot a \Rightarrow G \text{ is Abelian}$$

Proof. Let $x_1, x_2 \in G$. Since a and b generate G, x_1 and x_2 can be expressed as factors of a and b. Let m_i and n_i be the exponents of a and b for x_i, where $i \in \{1, 2\}$. We then have that $x_1 = a^{m_1} \cdot b^{n_1}$ and $x_2 = a^{m_2} \cdot b^{n_2}$. Thus $x_1 \cdot x_2 = (a^{m_1} \cdot b^{n_1})(a^{m_2} \cdot b^{n_2})$. Because a and b commute, $x_1 \cdot x_2 = (a^{m_1} \cdot b^{n_1}) \cdot (a^{m_2} \cdot b^{n_2}) = (a^{m_1} \cdot a^{m_2}) \cdot (b^{n_1} \cdot b^{n_2}) = (a^{m_2} \cdot a^{m_1}) \cdot (b^{n_2} \cdot b^{n_1}) = (a^{m_2} \cdot b^{n_2}) \cdot (a^{m_1} \cdot b^{n_1}) = x_2 \cdot x_1$. □

Statement 19. *Let $< G, \cdot >$ be a group and H be a subgroup of G. Then*

$$K = \left\{ x \in G : a \in H \iff x \cdot a \cdot x^{-1} \in H \right\}$$

is a subgroup of G.

We have that K is the set of all elements from the group G whose conjugation of $x \in G$ with an element $a \in G$ will stay in the subgroup H if and only if $a \in H$. The set K preserves the structure of H under conjugation. This set K is named the normalizer of G. Other ways of expressing K are as

$$\left\{ x \in G : xHx^{-1} = H \right\} \text{ and } \{ x \in G : xH = Hx \}.$$

Proof. Let $y, z \in K$. To show that $y \cdot z \in K$, we will first prove that $a \in H$ implies $(y \cdot z) \cdot a \cdot (y \cdot z)^{-1} \in H$. So assume $a \in H$. Since $z \in K$ and $a \in H$, $z \cdot a \cdot z^{-1} \in H$. Also, since $y \in K$ and $z \cdot a \cdot z^{-1} \in H$, $(y \cdot z) \cdot a \cdot (y \cdot z)^{-1} = y \cdot (z \cdot a \cdot z^{-1}) \cdot y^{-1} \in H$. Now we will prove that $(y \cdot z) \cdot a(y \cdot z)^{-1} \in H$ implies $a \in H$. Because $y \cdot z \cdot a \cdot (y \cdot z)^{-1} \in H$, $y \cdot (z \cdot a \cdot z^{-1}) \cdot y^{-1} \in H$, which implies that $z \cdot a \cdot z^{-1} \in H$ since $y \in K$. And since $z \in K$ and $z \cdot a \cdot z^{-1} \in H$, it must be that $a \in H$. Hence we have shown that $(y \cdot z) \cdot a \cdot (y \cdot z)^{-1} \in H \iff a \in H$.

It remains to show that $y^{-1} \in K$. To show this, we will first prove that $a \in H$ implies $y^{-1} \cdot a \cdot y \in H$. Assume $a \in H$ so that $y \cdot y^{-1} \cdot a \cdot y \cdot y^{-1} = a \in H$. Because $y \in K$ and $y \cdot y^{-1} \cdot a \cdot y \cdot y^{-1} \in H$, $y^{-1} \cdot a \cdot y \in H$. Now we will prove in the other direction that $y^{-1} \cdot a \cdot y \in H$ implies $a \in H$. Since $y \in K$ and $y^{-1} \cdot a \cdot y \in H$, $a = (y \cdot y^{-1}) \cdot a \cdot (y \cdot y^{-1}) = y \cdot (y^{-1} \cdot a \cdot y) \cdot y^{-1} \in H$. Hence, we have established closure under inverses.

Therefore, K is a a subgroup of G. □

Statement 20. *H is a subgroup of K.*

Proof. It suffices to show that $H \subset K$ since all properties of a subgroup hold for H. Let $x \in H$. We will first prove that $a \in H$ implies $x \cdot a \cdot x^{-1} \in H$. Since H is a subgroup and $x, a \in H$, $x \cdot a \cdot x^{-1} \in H$. Now it remains to show that $x \cdot a \cdot x^{-1} \in H$ implies that $a \in H$. Since $x, x \cdot a \cdot x^{-1} \in H$, $a = x^{-1}(x \cdot a \cdot x^{-1}) \cdot x \in H$. Thus $x \in H$ implies $x \in K$. Therefore, H is a subgroup of K. □