Corollary: Let H be a subgroup of the group G with identity e. Then $e \in H$.

proof: H as a subgroup must have an identity, say $f \in H$. But then $f^2 = f$ and this not only in H but of course also in G. Then according to the lemma we find $f = e$.

Proposition: A subset H of a group G is a subgroup, if and only if the following hold

(a) $H \neq \emptyset$

(b) $a, b \in H$ implies $a \cdot b \in H$

(c) If $a \in H$ then $a^{-1} \in H$

This can even be shortened to the two criteria

(a') $H \neq \emptyset$

(b') $a, b \in H$ implies $ab^{-1} \in H$.

Proof: Assume first that H is a subgroup of G. Then $H \neq \emptyset$, so we have (a), and due to the fact that H is closed under the operation on G, we clearly have (b). For (c) we argue as follows. Let $x \in H$ be given, then by the group axioms for H there exists $y \in H$ such that $x \cdot y = e = y \cdot x$. Now there is also $x^{-1} \in G$ that satisfies $x x^{-1} = x^{-1} x = e$. By the uniqueness of the inverse, we follow that $y = x^{-1}$, and hence $x^{-1} \in H$.

Now assume $H \subseteq G$ with properties (a), (b), and (c). By (a) we have $H \neq \emptyset$ and by (b) we see that H is closed under the operation on G. The associative law holds for elements in H because it holds for elements in G. Combining (b) and (c) we find that for arbitrary $a \in H$ there holds $e = a \cdot a^{-1} \in H$, so we have an identity. Then finally a simple application of (c) shows that inverses exist in H. Altogether we have shown that H forms a group with respect to the restricted operation. $\square$

We will now show that
(a), (b), (c) $\Leftrightarrow$ (a'), (b'), where for the part of "$\Rightarrow$" there is not much to do. Assume therefore, we have $H \subseteq G$ that satisfies (a') and (b'). Then we clearly have (a). Now apply (b') to see that for arbitrary x there holds $x \cdot x^{-1} = e \in H$, and applying the same to the elents $a = e$ and $b = x$, we find that $x^{-1} = e \cdot x^{-1} \in H$, which shows (c). Combining (c) with (b') we finally find for ~~$a, b \in H$ that~~ $a, b \in H$ that using (c) we get $b^{-1} \in H$ and then applying (b') we obtain $a \cdot (b^{-1})^{-1} \in H$, which is the claim of (b). □

proposition: Let G be a group.
Then $Z(G) := \{g \in G \mid gx = xg \text{ for all } x \in G\}$
is a subgroup of G.

proof. Use the above criteria (a), (b), (c) or (a'), (b').

proposition: The intersection of any non-empty set of subgroups of a group again forms a subgroup.

Proof. Let $\mathcal{H}$ be a nonempty set of subgroups of G. As $e \in H$ for all $H \in \mathcal{H}$, we find $e \in \bigcap \{H \mid H \in \mathcal{H}\}$, so this intersection is non-empty. If $a, b \in \bigcap \{H \mid H \in \mathcal{H}\}$, then $a, b \in H$ for all $H \in \mathcal{H}$. But then $ab^{-1} \in H$ for all $H \in \mathcal{H}$. Consequently we find $ab^{-1} \in \bigcap \{H \mid H \in \mathcal{H}\}$. This completes the proof of the two criteria (a') and (b').

Def. For a group G and a subset $T \subseteq G$ define

$$\langle T \rangle := \bigcap \{H \leq G \mid T \subseteq H\},$$

the intersection of all subgroups that contain T.
It is the smallest subgroup of G that contains T. If $T = \{g\}$, a singleton, then write $\langle g \rangle$ instead of $\langle \{g\} \rangle$.

Proposition. Let G be a group and $g \in G$ some element. Then

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\} = \langle g^{-1} \rangle.$$

proof: Let $K := \{g^k \mid k \in \mathbb{Z}\}$.

Then it is easy to see that K is a subgroup of G. As $g \in K$, we infer $\langle g \rangle \subseteq K$ because $\langle g \rangle$ was anyway the smallest subgroup containing g.

Now keep in mind, that every subgroup, that contains g, must also contain g^k for every $k \in \mathbb{Z}$. This shows that K must be contained in every subgroup of G that contains g. Hence $K \subseteq \langle g \rangle$, q.

Def. Let G be a group and let $g \in G$ some element. If there exists a non zero integer k such that $g^k = e$, then we say g is of finite order. If no such k exists, then g is said to be of infinite order.

If $g \in G$ is of finite order, then $m := \min\{k \in \mathbb{N} \mid g^k = e\}$ is called the order of g. We write $|g| = m$ or sometimes also $o(g) = m$.

proposition. Let G be a group and let $g \in G$ be some element.

(a) If $|g| = m$, then $\langle g \rangle = \{ g^k \mid 0 \leq k \leq m-1 \}$

(b) If g is of infinite order, then the mapping $\mathbb{Z} \longrightarrow \langle g \rangle$, $n \mapsto g^n$ is a bijection.

proof. In any case, the mapping $\mathbb{Z} \to \langle g \rangle$, $n \mapsto g^n$ is surjective. Assume g is of infinite order and this mapping is <u>not</u> injective. Then there exist $k, n \in \mathbb{Z}$ such that $g^k = g^n$. This however implies $g^{k-n} = e$, i.e $g^m = e$ for $m = k-n \in \mathbb{Z}$ which contradicts the infinite order. Hence, in this case the above mapping must be injective, and so bijective.

If $|g| < \infty$, then let $m = |g|$. It is easy to see that $K := \{ g^k \mid 0 \leq k \leq m-1 \}$ forms a subgroup of G that satisfies $g \in K$. (Use quotient and reminder), so $\langle g \rangle \subseteq K$. On the other hand $K \subseteq \{ g^k \mid k \in \mathbb{Z} \} = \langle g \rangle$ and so, we have equality!

Remark : If G is finite, then every element of G must be of finite order