Subgroups of Cyclic Groups

In this handout, I'll write out a proof of the following theorem, which is Theorem 5.2 in Saracino's book:

Theorem. Let G be a **cyclic** group, and let $H \subseteq G$ be a subset. Then H is also cyclic.

Proof. By hypothesis, there is some $a \in G$ such that $G = \langle a \rangle$.

[That is, G has a generator, which we're choosing to call a. We need to find a generator for H.]

Note that H, being a subgroup, contains the identity element e of G. We consider two cases.

Case 1. $H = \{e\}$, i.e., the only element in H is the identity. Then $H = \langle e \rangle$, and we are done.

Case 2. $H \supsetneq \{e\}$. [That is, H contains at least one non-identity element.]
Let $S = \{n \geq 1 \,|\, a^n \in H\}$, which is some set of positive integers.

Claim 1: $S \neq \varnothing$.

Proof of Claim 1. By our assumption in this case, there is some $h \in H$ with $h \neq e$. Then $h \in G = \langle a \rangle$, and hence there is some $m \in \mathbb{Z}$ such that $h = a^m$.
If $m = 0$, then $h = a^0 = e$, a contradiction, so $m \neq 0$.
If $m \geq 1$, then $m \in S$, since $m \geq 1$ and $a^m = h \in H$.
Finally, if $m \leq -1$, then $-m \in S$, since $-m \geq 1$, and $a^{-m} = h^{-1} \in H$.
Either way, we get $S \neq \varnothing$, as desired. QED Claim 1

Thus, S is a nonempty set of positive integers.
By the **Well-Ordering Principle**, then, S has a smallest element $k \in S$. That is, $\exists k \in S$ such that for all $n \in S$ we have $k \leq n$.

[For more on the Well-Ordering Principle, see page 4 of Saracino. Also see Optional Video 11, "Another $mx + ny$ Proof," which states and discusses the Well-Ordering Principle.]

Let $b = a^k$, which is an element of H, since $k \in S$.
[Recall the definition of S; since $k \in S$, we have $k \geq 1$ and $a^k \in H$.]

Claim 2: $H = \langle b \rangle$.

Proof of Claim 2.
($\subseteq$): Given $h \in H$, we have $h \in G = \langle a \rangle$, and hence $\exists m \in \mathbb{Z}$ such that $h = a^m$.
By the Division Algorithm, $\exists q, r \in \mathbb{Z}$ such that $m = qk + r$ and $0 \leq r \leq k - 1$.
[Recall that $k \in S$, so $k \geq 1$, which is required to use the Division Algorithm.]
So $h = a^m = a^{qk+r} = (a^k)^q a^r = b^q a^r$.
Therefore, $a^r = b^{-q} h$, which is an element of H, since $b, h \in H$ and H is a subgroup.

If we had $r \geq 1$, then since we also have $a^r \in H$, we would have $r \in S$, by definition of S. But on the other hand, k is the smallest element of S, and we have $r < k$. This is a contradiction.
Therefore, $r \not\geq 1$. That is, $r = 0$.
Hence, $h = b^q a^0 = b^q \in \langle b \rangle$. QED ($\subseteq$)

($\supseteq$): Given $x \in \langle b \rangle$, we have $x = b^n$ for some $n \in \mathbb{Z}$.
Since $b \in H$ and H is a subgroup, it follows that $x \in H$. QED ($\supseteq$)

QED Claim 2

QED Theorem