2. If $|a| = n$, then

b. $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

b. Recall: $\langle a \rangle = \{a^i \mid i \in \mathbb{Z}\}$

Let $S = \{e, a, a^2, \ldots, a^{n-1}\}$. ($e = a^0$)

(NTS: $S \subseteq \langle a \rangle$ and $\langle a \rangle \subseteq S$).

The fact that $S \subseteq \langle a \rangle$ is direct. ✓

OTOH, sps g is a generic element in $\langle a \rangle$.

Then $g = a^p$ for some $p \in \mathbb{Z}$.

Write $p = nq + r$ where $0 \leq r < n$.

Then

$g = a^p = a^{nq+r} = \underbrace{(a^n)}_{e}{}^q a^r = a^r$ So $a^p = a^r$ where $0 \leq r < n$

Since $0 \leq r < n$, $a^r \in S$ ($a^r = g$), So $\langle a \rangle \subseteq S$.

Therefore $\langle a \rangle = S$.

* Note similarity with modular arithmetic. *