<u>Thm</u> Sps G is a group and $a \in G$.

1. If a has infinite order, then $a^i = a^j \Leftrightarrow i = j$
2. If $|a| = n$, then
   a. $a^i = a^j \Leftrightarrow n \mid i - j$
   b. $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$

proof:

there is no value $q \neq 0$ s.t. $a^q = e$.

1. Sps $|a|$ is infinite.

proof by contradiction

"without loss of generality"

($\Leftarrow$) If $i = j$, then $a^i = a^j$.

($\Rightarrow$) OTOH, sps. $a^i = a^j$ and $i \neq j$. wlog, sps $i > j$.

mult both sides by a^{-j}.

Then $a^{i-j} = e$. But then $|a| \leq i - j$, contradicting the fact that $|a|$ is infinite. So $i = j$. ✓

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

a. $a^i = a^j \Leftrightarrow n \mid i-j$

2. Now sps. $|a| = n$.

a. ($\Rightarrow$) Sps $a^i = a^j$. Then $a^{i-j} = e$.

Write

$i-j = nq + r$, where $0 \le r < n$ (want: $n \mid i-j$ so NTS: $r = 0$.)

above

Then $e = a^{i-j} = a^{nq+r} = (\underbrace{a^n}_{e})^q a^r = a^r$. So, $e = a^r$.

Since $r < n$ and $|a| = n$, conclude $r = 0$. So $n \mid i-j$. ✓

smallest power s.t. $a^n = e$.

($\Leftarrow$) OTOH, sps $n \mid i-j$. Then $i-j = nk$ for some $k \in \mathbb{Z}$

So

$$a^i a^{-j} = a^{i-j} = a^{nk} = (\underbrace{a^n}_{e})^k = e.$$

Thus, multiplying both sides by a^j, we get $a^i = a^j$, as desired.