

Solution to Problem 5.21.

Let $G = \langle x \rangle$, $|G| = n < \infty$.

Claim: $\langle x^r \rangle \subseteq \langle x^s \rangle$ iff $(s, n)|(r, n)$.

Proof:

1. "Only if direction":

$\langle x^r \rangle \subseteq \langle x^s \rangle \Rightarrow x^r \in \langle x^s \rangle$
 $\Rightarrow x^r = (x^s)^k$ for some $k \in \mathbb{Z}$.
 $\Rightarrow x^{r-sk} = e$
 $\Rightarrow \text{ord}(x)|(r - sk)$
 $\Rightarrow n|(r - sk)$
(b/c $G = \langle x \rangle$, $|G| = n \Rightarrow \text{ord}(x) = n$)
 $\Rightarrow r - sk = cn$ for some $c \in \mathbb{Z}$
 $\Rightarrow r = cn + sk$.
 $\Rightarrow (s, n)|r$
(b/c (s, n) divides both s and n)
 $\Rightarrow (s, n)|(r, n)$, as desired.

2. "If direction":

Let $g = (s, n)$.
 $\Rightarrow g|n$, and $g|g$
 $\Rightarrow g = (g, n)$
 $\Rightarrow (g, n) = (s, n)$
 $\Rightarrow \langle x^g \rangle = \langle x^s \rangle$ (by Theorem 5.5iii)
 $g|r$ (since $(s, n)|(r, n)$ and $(r, n)|r$)
 $\Rightarrow x^r = x^{kg}$ for some $k \in \mathbb{Z}$
 $\Rightarrow x^r \in \langle x^g \rangle = \langle x^s \rangle$
 $\Rightarrow \forall m \in \mathbb{Z}, (x^r)^m \in \langle x^s \rangle$
 $\Rightarrow \langle x^r \rangle \subseteq \langle x^s \rangle$, as desired.