Then

$$\begin{aligned} a^{n+s} &= a^{n+s'+ur} \\ &= a^{s'}a^{n+ur} \text{ in } S^1 \\ &= a^{s'}a^{n+r}a^{(u-1)r} \\ &= a^{s'}a^{n}a^{(u-1)r} \\ &= a^{s'}a^{n+(u-1)r} \\ &\vdots \\ &= a^{s'}a^{n} \\ &= a^{n+s'}. \end{aligned}$$

Similarly, $a^{n+t} = a^{n+t'}$. Therefore

$$a^{n+s} = a^{n+t} \Leftrightarrow a^{n+s'} = a^{n+t'} \Leftrightarrow s' = t' \Leftrightarrow s \equiv t(\bmod r).$$

Notice that

$$a^{n+ur} = a^n$$

for all u.
We have shown

$$\{a, a^2, \ldots, a^n, a^{n+1}, \ldots, a^{n+r-1}\} = \langle a \rangle$$

and

$$|\langle a \rangle| = n + r - 1.$$

Clearly

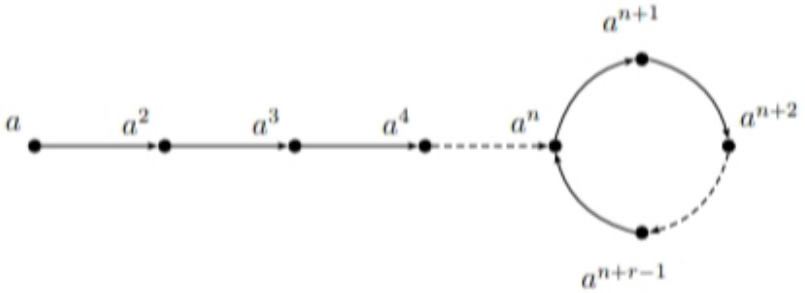
$$\{a^n, a^{n+1}, \ldots, a^{n+r-1}\}$$

is a subsemigroup. In fact

$$a^{n+s}a^{n+t} = a^{n+u}$$

where $u \equiv s + n + t \pmod r$ and $0 \leq u \leq r - 1$. This is case (ii).

We can express this pictorially:



□

Lemma 2.16 (The Idempotent Power Lemma). *If $\langle a \rangle$ is finite, then it contains an idempotent.*