9.5: Roots of Unity

**Theorem:** Let $F$ be a finite field.

Then $F^\times = F - \{0\}$ is a cyclic group.

**Proof:** Let $n = |F|$, so $n-1 = |F^\times|$.

Then every $x \in F^\times$ satisfies $x^{n-1} = 1$ by Lagrange's Theorem.

The order of any $x \in F^\times$ is a divisor of $n-1$.

By the Fundamental Theorem of Finite Abelian Groups

$F^\times \cong C_{m_1} \times C_{m_2} \times \cdots \times C_{m_t}$

where $m_{i+1} | m_i$ for $1 \leq i \leq t-1$.

Then $n-1 = |F^\times| = m_1 m_2 \cdots m_t$.

Also, every element $x$ satisfies $x^{m_t} = 1$.

Thus, $x^{m_t} = 1$ has $n-1$ solutions in $F$,

which is a contradiction unless $m_t \geq n-1$.

Then $m_t = n-1$ and all other $m_i$'s are 1.

That means $F^\times$ is cyclic. \[[Q.E.D.\]
Other Proof:

Let \( \psi(d) = \# x \text{ of order } d, \text{ for } d \mid n-1 \).

If \( x \) has order \( d \), then \( \frac{1}{d} x, x^2, \ldots, x^{d-1} \)
are \( d \) distinct solutions of \( y^d = 1 \) in \( F \).

Hence, they are all the solutions.

\( x \) has order \( d \) iff \( (j, d) = 1 \).

Thus, either \( \psi(d) = 0 \) or \( \psi(d) = \varphi(d) \).

But \( n-1 = \sum_{d \mid n-1} \psi(d) \leq \sum_{d \mid n-1} \varphi(d) = n-1 \).

This fails if any \( \psi(d) = 0 \).

So \( \psi(d) = \varphi(d) \) for all \( d \mid n-1 \).

Hence, there are \( \varphi(n-1) \) primitive roots
or generators of \( F^\times \).