Definition 6.1

A group G is cyclic if there is an element $a \in G$ such that

$$G = \{a^n \mid n \in \mathbb{Z}\}$$

or, in other notation, $G = \langle a \rangle$. In such case we say that a is a *generator* of G.

Example. The following groups are cyclic:

- $\mathbb{Z}$
- $\mathbb{Z}_n$ for any $n \geq 1$

Note. If G is any group and $a \in G$ then $\langle a \rangle$ is a cyclic subgroup of G.

Theorem 6.2

Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$, and let H be a subgroup of G. If H contains only the trivial element $e = a^0$ then H is cyclic since $H = \langle e \rangle$. Otherwise there are some elements $a^n \in H$ with $n > 0$. Let $m > 0$ be the smallest integer such that $a^m \in H$. We will show that $H = \langle a^m \rangle$.

Since $a^m \in H$, thus $(a^m)^k \in H$ for all $k \in \mathbb{Z}$, so $\langle a^m \rangle \subseteq H$.

Conversely, let $a^n \in H$ for some n. Then $n = qm + r$ for some $0 \leq r < m$. This gives

$$a^n = a^{qm+r} = a^{qm} \cdot a^r$$

We have seen already that $a^{-qm} \in H$, so $a^{-qm} \cdot a^n \in H$. However we have

$$a^{-qm} \cdot a^n = a^{-qm} \cdot a^{qm} \cdot a^r = a^r$$

which means that $a^r \in H$. Since $r < m$, this means that $r = 0$. Therefore $a^n = a^{qm} \in \langle a^m \rangle$. This means that $H \subseteq \langle a^m \rangle$. $\square$

Theorem 6.3

If G is a finite cyclic group and $H \subseteq G$ is a subgroup then $|H|$ divides $|G|$.

Proof. Let $G = \langle a \rangle$ and let $|G| = |a| = n$. By Theorem 6.2 we have $H = \langle a^m \rangle$ for some m. Then $|H| = |a^m|$ and by Theorem 4.5 $|a^m| = \frac{n}{\gcd(n,m)}$. Therefore $|H|$ divides $|G|$. $\square$

Theorem 6.4

If G is a finite cyclic group and $d > 0$ is an integer that divides $|G|$ then there exists exactly one subgroup $H \subseteq G$ such that $|H| = d$.

Proof. Let $G = \langle a \rangle$ and let $|G| = |a| = n$. Since d divides n we have $n = dm$ for some $m > 0$. We will first show that a subgroup H of order d exists. Take $H = \langle a^m \rangle$. Then

$$|H| = |a^m| = \frac{n}{\gcd(n,m)} = \frac{n}{m} = d$$

Next, $H' \subseteq G$ be some other subgroup of G such that $|H'| = d$. We have $H' = \langle a^k \rangle$ for some $0 < k \leq n$ such that $\gcd(k,n) = m$. Then $m = pk + qn$ for some $p, q \in \mathbb{Z}$. Which gives

$$a^m = a^{pk} \cdot a^{qn} = \left(a^k\right)^p \in H'$$

This gives $H \subseteq H'$. Since both groups H and H' consist of d elements, this means that $H = H'$.

$\square$

Theorem 6.5

Let $G = \langle a \rangle$ be a cyclic group of order n. An element a^k is a generator of G (i.e. $\langle a^k \rangle = G$) if and only if $\gcd(n,k) = 1$.

Proof. The group $\langle a^k \rangle$ consists of $\frac{n}{\gcd(n,k)}$ elements. We have $\langle a^k \rangle = G$ if and only if $\frac{n}{\gcd(n,k)} = n$ i.e. $\gcd(k,n) = 1$. $\square$