Definition 9.1

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 $n \geq 1$
- If G is any group and $a \in G$ then $\langle a \rangle$ is a cyclic subgroup of G.

Theorem 9.2

If G is a finite group then G is cyclic if and only if there is an element $a \in G$ such that $|a| = |G|$.

Proof. If G is cyclic then $G = \langle a \rangle$ for some $a \in G$ and then $|G| = |\langle a \rangle| = |a|$. Conversely, if there is $a \in G$ such that $|a| = |G|$, then $\langle a \rangle \subseteq G$ and $|\langle a \rangle| = |G|$, which gives $\langle a \rangle = G$. □

Theorem 9.3

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 $r < m$, we get that $r = 0$. Therefore $a^n = a^{qm} \in \langle a^m \rangle$. This implies that $H \subseteq \langle a^m \rangle$. $\square$

Theorem 9.4

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 9.3 we have $H = \langle a^m \rangle$ for some m. Then $|H| = |a^m|$ and by Theorem 6.5 $|a^m| = \frac{n}{\gcd(n,m)}$. Therefore $|H|$ divides $|G|$. $\square$

Theorem 9.5

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 $\gcd(n, k) = m$. Then $m = pk + qn$ for some $p, q \in \mathbb{Z}$. This gives

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

and so $H = \langle a^m \rangle \subseteq H'$. Since both groups H and H' consist of d elements, it follows that $H = H'$.

$\square$

Theorem 9.6

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. $\gcd(k, n) = 1$. $\square$

Exercise. In the group $\mathbb{Z}_{15}$ find all elements a such that a generates $\mathbb{Z}_{15}$

Theorem 9.7

Let $G_1 = \langle a_1 \rangle$ and $G_2 = \langle a_2 \rangle$ be finite cyclic groups. The group $G_1 \times G_2$ is cyclic if and only if $\gcd(|G_1|, |G_2|) = 1$.

Proof. Assume that $\gcd(|G_1|, |G_2|) = 1$. Consider the element $(a_1, a_2) \in G_1 \times G_2$. By Theorem 8.3 we have:

$$|(a_1, a_2)| = \operatorname{lcm}(|a_1|, |a_2|) = \operatorname{lcm}(|G_1|, |G_2|) = \frac{|G_1| \cdot |G_2|}{\gcd(|G_1|, |G_2|)} = |G_1| \cdot |G_2| = |G_1 \times G_2|$$

This shows that $G_1 \times G_2 = \langle (a_1, a_2) \rangle$.

Conversely, assume that $|G_1| = n_1$, $|G_2| = n_2$ and that $\gcd(n_1, n_2) = d > 1$. Let $(b_1, b_2) \in G_1 \times G_2$ be an arbitrary element. Then

$$(b_1, b_2)^{n_1 n_2 / d} = (b_1^{n_1 \cdot (n_2/d)}, b_2^{n_2 \cdot (n_1/d)}) = (e, e)$$

This means that $|(b_1, b_2)|$ divides $n_1 n_2 / d$, and so $|(b_1, b_2)| < n_1 n_2 = |G_1 \times G_2|$. $\square$

Example. The group $\mathbb{Z}_2 \times \mathbb{Z}_3$ is a cyclic group generated by the element $(1, 1)$. On the other hand the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

Using induction, Theorem 9.7 can be generalized as follows:

Theorem 9.8

For $i = 1, \dots, n$ let $G_i = \langle a_i \rangle$ be a cyclic group. The group $G_1 \times G_2 \times \dots \times G_n$ is cyclic if and only if $\gcd(|G_i|, |G_j|) = 1$ for all $i \neq j$.