Theorem 1 Let $G$ be an infinite cyclic group.

1. $G$ is isomorphic to $\mathbb{Z}$, and in fact there are two such isomorphisms.

2. Every subgroup of $G$ is cyclic. Furthermore, for every positive integer $n$, $n\mathbb{Z}$ is the unique subgroup of $\mathbb{Z}$ of index $n$.

3. If $n_1$ and $n_2$ are positive integers, then $\langle n_1 \rangle + \langle n_2 \rangle = \langle \gcd(n_1,n_2) \rangle$ and $\langle n_1 \rangle \cap \langle n_2 \rangle = \langle \lcm(n_1,n_2) \rangle$.

Proof: We omit the proof of (1). Using it, we reduce (2) to the case when $G = \mathbb{Z}$. Let $H$ be a subgroup of $\mathbb{Z}$. If $H = \{0\}$ there is nothing to prove. Otherwise $H \cap \mathbb{Z}^+$ is nonempty and has a smallest element $n$. Then if $m \in H$, we can write $m = nq + r$ with $q \in \mathbb{Z}$ and $0 \leq r < n$. Since $n,m \in H$, it follows that $r \in H$, and hence $r = 0$. Thus $H = \langle n \rangle$. It is clear that $\langle n \rangle$ has index $n$, since each coset has a unique representative $i$ with $0 \leq i < n$. On the other hand, if $H$ is any subgroup of index $n$, then as we have seen it is cyclic, say generated by $n' > 0$. But then the index of $H$ is $n'$, so in fact $n' = n$.

For (3), we use the fact that the subgroup $H := \langle n_1 \rangle + \langle n_2 \rangle$ is cyclic. Let $n$ be its positive generator. Since $n_1$ and $n_2$ belong to $H$, $n$ divides $n_1$ and $n_2$. On the other hand, since $n \in H$, it follows that there exist integers $x$ and $y$ such that $n = xn_1 + yn_2$. Then any common divisor of $n_1$ and $n_2$ is also a divisor of $n$ so $n$ is the greatest common divisor. We omit the proof for intersections.

Theorem 2 Let $G$ be a cyclic group of order $n$.

1. Every subgroup of $G$ is cyclic.
2. For every divisor \( d \) of \( n \), \( G \) has a unique subgroup \( H_d \) of order \( d \), and \( H_d = \{ g \in G : g^d = e \} \).

3. For every \( d \in \mathbb{Z} \), \( H_d = H_{d'} \), where \( d' := \gcd(d, n) \).

4. \( G \) has \( \phi(n) \) generators, where \( \phi(n) \) is the cardinality of the set of \( i \) with \( 1 \leq i < n \) which are relatively prime to \( n \).

5. \( \text{Aut}(G) \) has order \( \phi(n) \).

**Proof:** A choice of a generator for \( G \) determines a surjective homomorphism \( \pi : \mathbb{Z} \to G \). Let \( K \) be its kernel, so that \( G \cong \mathbb{Z}/K \). Then the index of \( K \) is the order of \( G \), which must be \( n \). If \( H \) is a subgroup of \( G \), then \( \pi^{-1}(H) \) is a subgroup of \( \mathbb{Z} \) containing \( K \), and in particular is cyclic. It follows that \( H \) is cyclic. In fact \( \pi^{-1} \) defines an index-preserving bijection between the subgroups of \( G \) and the subgroups of \( \mathbb{Z} \) containing \( K \). It follows that \( G \) has a unique subgroup of index \( m \) for every \( m \) dividing \( n \), and hence also a unique subgroup of order \( d \) for every \( d \) dividing \( n \). In particular, for such a \( d \), let \( H_d := \{ g \in G : g^d = e \} \). Then \( H_d \) is a subgroup of \( G \) (since \( G \) is commutative), and in particular is cyclic, hence generated by an element of maximal order and hence has at most \( d \) elements. On the other hand, it contains \( \pi(n/d) \), which is an element of \( \text{of order } d \), and, it follows that \( H_d \) is the unique subgroup of order \( d \). Now let \( G \) be any group of order \( n \) and let \( d \) and \( d' \) be as in (3). Write \( d = d'c \) and \( n = d'm \). Let us note that \( g^{d'} = e \) iff \( g^d = e \). Indeed, if \( g^{d'} = e \), then also \( g^d = g^{d'c} = e \). Moreover, there exist integers \( x, y \) such that \( d' = xd + ym \). Then \( g^d = g^{x'd}g^{ym} = d^x \) so if \( g^d = e \), it follows also that \( g^{d'} = e \). This proves (3). In particular, the homomorphism \( \phi_d : g \mapsto g^d \) is bijective iff it is injective iff \( \gcd(n, d) = 1 \). Furthermore, \( \phi_d \) is bijective iff it is an isomorphism iff it takes generators to generators, so if \( g \) is a generator, \( g^d \) is another generator iff \( \gcd(d, n) = 1 \). This shows that the number of generators is \( \phi(d) \), as well as the number of automorphisms, since every automorphism is of this form. \( \square \)

For any group \( G \), let \( m_G(d) \) be the number of elements of \( G \) of (exact) order \( d \). Then

\[ |G| = \sum_d m_G(d). \]

**Corollary 1** If \( n \) is a positive integer,

\[ n = \sum_{d \mid n} \phi(m). \]
Proof: Let $G$ be any cyclic group of order $n$. Then $m_G(d)$ is zero if $d$ does not divide $n$ and otherwise is the number of generators of the group $H_d$ defined above. Since $H_d$ is cyclic of order $d$, $H_d$ has $\phi(d)$ generators. Thus $m_G(d) = \phi(d)$, and the corollary follows from the formula above.

**Theorem 3** Let $G$ be a finite group. Then the following conditions are equivalent:

1. $G$ is cyclic.
2. For each $d \in \mathbb{Z}^+$, the number of $g \in G$ such that $g^d = e$ is less than or equal to $d$.
3. For each $d \in \mathbb{Z}^+$, $G$ has at most one subgroup of order $d$.
4. For each $d \in \mathbb{Z}^+$, $G$ has at most $\phi(d)$ elements of order $d$.

*Note:* In statements (2)–(4), one may restrict to those $d$ which divide $n$.

Proof: The implication of (2) by (1) follows from Theorem 2.

Suppose that (2) holds and $d \in \mathbb{Z}^+$. Let $H$ be a subgroup of $G$ of order $d$. Then $g^d = e$ for every $g \in H$. According to (2), there are at most $d$ such elements. But then $H = \{g \in G : g^d = e\}$, and hence $H$ is unique.

Suppose (3) holds. If there are no elements of order $d$, then there is nothing to check. If $g$ is an element of order $d$, then $\langle g \rangle$ is a subgroup of order $d$, and by (3), it is the unique such subgroup. Hence if $g'$ is any element of order $d$, $g' \in \langle g \rangle$. Since $\langle g \rangle$ contains exactly $\phi(d)$ elements of order $d$, we see that $G$ has exactly $\phi(d)$ elements of order $d$.

Suppose that (4) holds. For each divisor $d$ of the order of $G$, let $m(d)$ denote the number of elements of $G$ of order $d$. If $G$ is a group of order $n$ and satisfies (3) we find that

$$n = \sum_{d \mid n} m(d) \leq \sum_{d \mid n} \phi(d) = n$$

Since each $0 \leq m(d) \leq \phi(d)$ for each $d$, we see that the equality $\sum_{d \mid n} m(d) = \sum_{d \mid n} \phi(d)$ implies that each $m(d) = \phi(d)$ for every $d$. In particular $m(n) = \phi(n) \neq 0$. This means that $G$ has at least one element of order $n$, and hence is cyclic.

**Corollary 2** Every finite subgroup of a field is cyclic.

Proof: We use the fact that a polynomial of degree $d$ has at most $d$ roots to conclude that any such group has at most $d$ elements of order $d$. 

---

3