Cyclic Groups

The integers \( \mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \) form an additive group. We shall determine its subgroups. In this context, we use the following fundamental fact of integer multiplication:

**FACT:** Let \( y, a \in \mathbb{Z} \). Then there exist integers \( n \in \mathbb{Z} \) and \( r \in \mathbb{Z} \), \( 0 \leq r < |a| \) such that

\[
y = n \cdot a + r.
\]

Let \( H \) be a subgroup of (\( \mathbb{Z}, + \)). Let \( a \) be the smallest positive element in \( H \). (Why is there such an element? Could not \( H \) only consist of negative numbers?) Show that \( H = (a) := \{ n \cdot a \mid n \in \mathbb{Z} \} \).

**Definition:** Let \( (G, \cdot) \) be a group. We say that \( G \) is cyclic if there exists an element \( a \in G \) such that every element of \( G \) can be written as \( a^n \) for some \( n \in \mathbb{Z} \). In this case, we call \( a \) a generator of \( G \).

Let \( (G, \cdot) \) be a group and \( a \in G \) an element of \( G \). Then \( f : (\mathbb{Z}, +) \rightarrow (G, \cdot), n \rightarrow f(n) := a^n \) is a homomorphism. (Why?)

The kernel of \( f \) is a subgroup of (\( \mathbb{Z}, + \)). If this subgroup is all of \( \mathbb{Z} \), then the subgroup \( < a > = \{ a^n \mid n \in \mathbb{Z} \} \) is isomorphic to \( \mathbb{Z} \). Otherwise, \( \ker f = (d) \). Prove that the elements \( e, a, a^2, \ldots, a^{d-1} \) are all distinct.

**Proposition:** If the number of elements in a group \( G \) is \( p \), a prime, then \( G \) is cyclic.

**Proposition:** If \( G \) is cyclic, then so is any subgroup and any homomorphically image of \( G \).

**Proposition:** Let \( G = < a > \) be a cyclic subgroup of order (=size) \( m \). An element \( b \in G \) is a generator of \( G \) if and only if \( b = a^i \) with \( i \) relatively prime to \( m \).