THE UNIQUENESS ASPECT OF THE FUNDAMENTAL THEOREM OF FINITE ABELIAN GROUPS

DAVID B. SUROWSKI
Department of Mathematics, Kansas State University, Manhattan, KS 66506-2602, USA

We shall use additive notation for abelian groups. The following is well-known to every graduate student of mathematics:

**Fundamental Theorem of Finite Abelian Groups.** Let \( A \) be a finite abelian group. Then there exist cyclic subgroups \( Z_1, Z_2, \ldots, Z_r \) of orders \( m_1, m_2, \ldots, m_r > 1 \), respectively, satisfying \( m_2 | m_1, m_3 | m_2, \ldots, m_r | m_{r-1} \) such that

\[
A = Z_1 \oplus Z_2 \oplus \cdots \oplus Z_r.
\]

Furthermore, the integers \( r \) and \( m_1, \ldots, m_r \) are uniquely determined.

Note that the above theorem involves two parts: an existence part and a uniqueness part. While there are many short papers that provide novel proofs of the existence aspect, the uniqueness aspect has been largely neglected. Indeed, an alarming number of textbook treatments of the "Fundamental Theorem" do not even mention uniqueness as part of the theorem. Those treatments that do address uniqueness all, in varying degrees, obtain the uniqueness along the lines of the argument as given in Mac Lane and Birkoff's standard text [2], or by an analysis of the \( i \)-rowed minors of the "relations" matrix defining \( A \). (Compare [1; Theorem 3.9]; this amounts to a proof of the uniqueness, up to associates of the "Smith Canonical Form" of the relations matrix defining \( A \).) There may be some who, on the grounds of "purity," might object to arguments akin to those in [2], as they invoke the uniqueness of dimension of a vector space. While this is hardly a serious objection, our argument below is quite independent of even this simple result.

Thus, assume that we have decompositions of the finite abelian group \( A \) into direct sums of cyclic groups:

\[
Z_1 \oplus Z_2 \oplus \cdots \oplus Z_r = A = Z'_1 \oplus Z'_2 \oplus \cdots \oplus Z'_s,
\]

where \( |Z_i| = m_i, \ |Z'_j| = m'_j, i = 1, \ldots, r, \ j = 1, \ldots, s \), and that the above divisibility conditions on the orders \( m_j, m'_j \) hold. Note first of all, that if we set \( m = \exp(A) = \text{least positive integer } m \text{ such that } ma = 0 \text{ for all } a \in A \), then
exists an automorphism \( \phi \) such that \( \phi(Z) = Z' \), for then it would follow that \( B \cong B' \), and the desired uniqueness would follow by induction.

We hasten to concede a small logical glitch in the above induction. Indeed, we have started with a fixed abelian group \( A \) with two direct sum decompositions; after application of the above isomorphism we obtain two isomorphic, but not identical groups, viz., \( B \) and \( B' \). However, this is not a serious problem and the student should have no difficulty in enunciating an induction hypothesis sufficiently general to be applicable here.

What is really going on is summarized in the following:

**Theorem.** The group \( \text{Aut}(A) \) of automorphisms of \( A \) acts transitively on the cyclic subgroups of order \( m = \exp(A) \) of \( A \).

In other words, given any two cyclic subgroups \( C, C' \leq A \), both of order \( m \), then there exists an automorphism \( \psi : A \to A \) with \( \psi(C) = C' \). In fact, we'll prove a slightly stronger result, namely that \( \text{Aut}(A) \) actually acts transitively on the elements of order \( m \) in \( A \).

To prove this result, it suffices to prove that if \( p \) is a prime and if \( p^k \) is the highest power of \( p \) that divides \( m \), then \( \text{Aut}(A) \) acts transitively on the elements of order \( p^k \) in \( A \). It therefore suffices to consider the case in which the exponent \( m \) is itself a prime power: \( m = p^k \).

Thus we have a decomposition \( A = Z_1 \oplus Z_2 \oplus \cdots \oplus Z_r \), where \( Z_i \) is cyclic of order \( p^{k_i} \), and where \( k_1 = k \geq k_2 \cdots \geq k_r \).

The following two lemmas are very easy, but fundamental.

**Lemma 1.** Let \( B = B_1 \oplus B_2 \) be a finite abelian group and let \( \mu_1 : B_1 \to B, \ \mu_2 : B_2 \to B \) be injective homomorphisms. If \( \mu_1(B_1) \cap \mu_2(B_2) = 0 \), then the mapping \( \mu : B \to B \) defined by \( \mu(b_1 + b_2) = \mu_1(b_1) + \mu_2(b_2) \), \( b_1 \in B_1, \ b_2 \in B_2 \) is an automorphism of \( B \).

**Lemma 2.** Let \( A = Z_1 \oplus Z_2 \oplus \cdots \oplus Z_r \) be as above, and assume that \( Z_i = \langle z_i \rangle \) is cyclic of order \( p^{k_i} \), \( i = 1, \ldots, r \). Assume that \( k = k_1 = k_2 = \cdots = k_l < k, \ k_{l+1} \leq k \).

If
\[
a = \sum_{i=1}^{r} \alpha_i z_i \in A,
\]
then \( a \) has order \( p^k \) if and only if \( p \nmid \alpha_j \), for some \( j, 1 \leq j \leq l \).

**Proof.** Simply note that because \( Z_1 \oplus Z_2 \oplus \cdots \oplus Z_r \) is a direct sum, we conclude that the order of \( \sum_{i=1}^{r} \alpha_i z_i \) is equal to the least common multiple of the individual orders \( o(\alpha_i z_i) \), \( i = 1, \ldots, r \). Since \( p \nmid \alpha_j \), we see that \( o(\alpha_j z_j) = o(z_j) = p^k \).

Thus, let \( a \in A \) be an arbitrary element of order \( p^k \). We shall show that there exists an automorphism \( \phi : A \to A \) such that \( \phi(z_1) = a \). If we write
\[
a = \sum_{i=1}^{r} \alpha_i z_i,
\]
we may assume that \( p \nmid \alpha_1 \). Indeed, if \( p \nmid \alpha_j \), then an automorphism of \( A \) that interchanges \( Z_1 \) and \( Z_j \) will reduce us to this situation. Next, according to Lemma 1, write \( A = Z_1 \oplus B_2 \), where \( B_2 = Z_2 + \cdots + Z_r \) and define injections \( \mu_1 : Z_1 \to A, \mu_2 : B_2 \to A \) by setting \( \mu_1(z_1) = a, \mu_2 = 1_{B_2} \). Therefore the map \( \mu : A \to A \), given by \( \mu(w_1 + b_2) = \mu_1(w_1) + \mu_2(b_2) \) defines an automorphism of \( A \) which carries \( z_1 \) to \( a \).

References


E-mail address: dbski@math.ksu.edu