Uniqueness of Decompositions of Finite Abelian Groups as Direct Sums of p-Groups

R. C. Daileda

Let A be a finite (additive) abelian group. We have seen that any such group can be decomposed as a direct sum of p-groups whose orders are relatively prime.[1] The goal of this short note is to prove that this can be accomplished in (essentially) only one way. To simplify notation, given a prime p we let

$$A(p) = \bigcup_{j=1}^{\infty} A_{p^j}.$$

Then $A(p) < A$ (exercise) and it consists of all elements in A whose orders are powers of p. The uniqueness of p-group decompositions for abelian groups is an immediate consequence of the following fact.

Lemma 1. *Let A be a finite abelian group and let p be a prime number. If $A = A_1 \oplus B$ where A_1 is a p-group and $p \nmid |B|$, then p divides $|A|$ and $A_1 = A(p)$.*

Proof. Since p divides $|A_1|$, which divides $|A_1 \oplus B| = |A_1| \cdot |B|$, the first conclusion holds. Let $a \in A(p)$. Then $p^j a = 0$ for some $j \geq 0$. Write $a = a_1 + b$ with $a_1 \in A_1$ and $b \in B$. Then

$$0 = p^j a = p^j a_1 + p^j b.$$

Because the sum of A_1 and B is direct, this means that $p^j b = 0$. If $b \neq 0$, this means that its order must be divisible by p. But $|b|$ divides $|B|$, and $p \nmid |B|$, so $b \neq 0$ is impossible. Hence $a = a_1 \in A_1$. That is, $A(p) \subset A_1$.

On the other hand, since $|A_1|$ is a power of p, the orders of its elements are also powers of p. This means that $A_1 \subset A(p)$. Combined with the inclusion above, we now have $A_1 = A(p)$. □

Theorem 1. *Let A be a finite abelian group and let $p_1, \ldots, p_k$ be distinct primes. Suppose that*

$$A = A_1 \oplus \cdots \oplus A_k,$$

where each A_i is a p_i-group. Then p_i divides $|A|$, $A_i = A(p_i)$ for all i, and k is the number of distinct prime factors of $|A|$.

Proof. The first assertion follows from the lemma, upon taking $B = A_1 \oplus \cdots \oplus \widehat{A_i} \oplus \cdots \oplus A_k$ for each i. Since $|A| = |A_1| \times \cdots \times |A_k| = p_1^{r_1} \cdots p_k^{r_k}$, and each $r_i \geq 1$ by the definition of a p-group, the fundamental theorem of arithmetic implies that k is, indeed, the number of distinct prime factors of $|A|$. □

[1] To avoid the inclusion of trivial summands, we require all p-groups to be nontrivial.

The theorem tells us that no matter how we write A as a direct sum of p-groups, the summands will correspond to the prime factors of $|A|$, and for each prime p dividing $|A|$ the corresponding summand will in fact be $A(p)$. So, up to the order of the summands, the p-group decomposition of A is unique. In class, we produced the decomposition

$$A = A_{p_1^{r_1}} \oplus \cdots \oplus A_{p_k^{r_k}},$$

where $|A| = p_1^{r_1} \cdots p_k^{r_k}$ and the p_i are distinct. According to the theorem, we must therefore have $A(p_i) = A_{p_i^{r_i}}$ for all i. This isn't hard to prove directly, but the definition of $A(p)$ is somewhat easier to work with, since it doesn't require keeping track of a specific exponent.