Finite Abelian Groups III: The Fundamental Theorem

R. C. Daileda

Let A be a finite abelian group of order

$$n = p_1^{e_1} \cdots p_\ell^{e_\ell},$$

where the p_i are distinct primes and $e_i \geq 1$ for all i. According to Theorem 2 of Part I, we have

$$A = \bigoplus_{i=1}^{\ell} A[p_i^{e_i}], \tag{1}$$

where each $A[p_i^{e_i}]$ is a p_i-group of order $p_i^{e_i}$. According to Theorem 1 of Part II, for each i we have

$$A[p_i^{e_i}] = \bigoplus_{j=1}^{k_i} C(p_i^{r_{i,j}}), \tag{2}$$

where $C(m)$ denotes a cyclic subgroup of order m, and $r_{i,1} \geq r_{i,2} \geq \cdots \geq r_{i,k_i} \geq 1$.

Because the number of summands k_i in (2) can vary with i, we set

$$k = \max_i k_i,$$

and for any j satisfying $k_i < j \leq k$ we define $r_{i,j} = 0$. Then $C(p_i^{r_{i,j}}) = C(p_i^0) = \{0\}$ for any such i and j. Instead of (2) we can then write

$$A[p_i^{e_i}] = \bigoplus_{j=1}^{k} C(p_i^{r_{i,j}}),$$

since any summand beyond the k_i^{th} is simply the trivial group. Substituting these modified decompositions into (1) we obtain

$$\begin{aligned} A &= \bigoplus_{i=1}^{\ell} \bigoplus_{j=1}^{k} C(p_i^{r_{i,j}}) \\ &= \bigoplus_{j=1}^{k} \left(\bigoplus_{i=1}^{\ell} C(p_i^{r_{i,j}}) \right). \end{aligned} \tag{3}$$

Because the orders of the cyclic subgroups $C(p_i^{r_{i,j}})$ for $i = 1, 2, \ldots \ell$ are pairwise relatively prime, their direct sum is again cyclic, of order

$$d_j = \prod_{i=1}^{\ell} p_i^{r_{i,j}}. \tag{4}$$

So we have

$$A = \bigoplus_{j=1}^{k} C(d_j),$$

where

$$C(d_j) = \bigoplus_{i=1}^{\ell} C(p_i^{r_{i,j}})$$

for each j.

Now for any fixed i and all $j \leq k_i$ we have $r_{i,j-1} \geq r_{i,j}$. This continues to hold even if $j > k_i$ since we defined $r_{i,j} = 0$ in this case. Hence $p_i^{r_{i,j}} | p_i^{r_{i,j-1}}$ for all j. It follows from (4) that $d_j | d_{j-1}$ for all j. We have now arrived at our Fundamental Theorem.

Theorem 1 (Fundamental Theorem of Finite Abelian Groups)**.** *Let A be a finite abelian group. There exist unique integers $d_j \geq 2$ satisfying $d_k | d_{k-1} | \cdots | d_1$ so that A is the internal direct sum*

$$A = \bigoplus_{j=1}^{k} C(d_j)$$

of cyclic subgroups $C(d_j)$ of size d_j. The integers d_j are called the elementary divisors *of A.*

At this point we've proven every statement in the Fundamental Theorem aside from the uniqueness of the sequence of elementary divisors. We leave this to the interested and industrious reader.

Corollary 1. *Let A be a finite abelian group. There exist unique integers $d_j \geq 2$ satisfying $d_k | d_{k-1} | \cdots | d_1$ so that*

$$A \cong \prod_{j=1}^{k} \mathbb{Z}/d_j\mathbb{Z}.$$

Proof. The internal direct sum of the subgroups $C(d_j)$ in the Fundamental Theorem is isomorphic to their external product (by definition), and $C(d_j) \cong \mathbb{Z}/d_j\mathbb{Z}$ for all j. □

When we were dealing with classifying finite abelian p-groups of a given order p^e, we found that the exponents in the cyclic factors corresponded to the partitions of e. So by determining all of the partitions of e we could create a list of the isomorphism classes of finite abelian p-groups of order p^e.

The analogous problem, of classifying all the (general) finite abelian groups with a given order n, requires us to determine all sequences of elementary divisors $d_j \geq 2$ so that $d_k | d_{k-1} | \cdots | d_1$ and $n = d_1 d_2 \cdots d_k$. This can be done using partitions as in the case of p-groups, but the technique is somewhat more involved. The key idea is to realize that elementary divisors arose from the sizes of the cyclic summands in the decompositions of the prime power torsion subgroups, when we reversed the order of the double direct sum in (3).

To see how this works, write out the prime factorization of n as usual:

$$n = p_1^{e_1} \cdots p_k^{e_\ell}.$$

For each i, find the set $\mathcal{P}_i$ of all partitions $(r_{i,1}, r_{i,2}, \ldots, r_{i,k_i})$ of the exponent e_i. The possible sequences of elementary divisors correspond to the tuples $(\pi_i) \in \mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_\ell$. Given such a tuple (π_i), let k denote the maximum length of any of the π_i. Add zeros as necessary to the end of each π_i so that all of the resulting modified partitions have common length k. We then have $\pi_i = (r_{i,1}, r_{i,2}, \ldots, r_{i,k})$ for all i. Finally, set

$$d_j = \prod_{i=1}^{\ell} p_i^{r_{i,j}}$$

for $j = 1, 2, \ldots, k$. The resulting sequence $d_1, d_2, \ldots, d_k$ yields the elementary divisors corresponding to the tuple (π_i) of partitions of the exponents e_i. By running through every tuple in $\mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_\ell$ one obtains all of the possible elementary divisors for the isomorphism classes of finite abelian groups of order n.

Example 1. Let's classify the finite abelian groups of order $n = 756 = 2^2\, 3^3\, 7$. The exponents of the prime factors are $e_1 = 2$, $e_2 = 3$ and $e_3 = 1$. The partitions of 2 are $\mathcal{P}_1 = \{(1,1), (2)\}$, the partitions of 3 are $\mathcal{P}_2 = \{(1,1,1), (2,1), (3)\}$, and the partitions of 1 are $\mathcal{P}_3 = \{(1)\}$. Rather than lengthen these on a case by case basis, we simply note that the largest length is 3, and add zeros to the shorter partitions to give them length 3, also. This yields the modified partitions

$$\mathcal{P}_1 = \{(1,1,0), (2,0,0)\},$$
$$\mathcal{P}_2 = \{(1,1,1), (2,1,0), (3,0,0)\},$$
$$\mathcal{P}_3 = \{(1,0,0)\}.$$

We now choose one partition from each of $\mathcal{P}_1$, $\mathcal{P}_2$ and $\mathcal{P}_3$ in every possible way to construct the elementary divisors. This yields:

$$(1,1,0), (1,1,1), (1,0,0) \rightsquigarrow d_1 = 2^1\, 3^1\, 7^1 = 42,\ d_2 = 2^1\, 3^1\, 7^0 = 6,\ d_3 = 2^0\, 3^1\, 7^0 = 3,$$
$$(2,0,0), (1,1,1), (1,0,0) \rightsquigarrow d_1 = 2^2\, 3^1\, 7^1 = 84,\ d_2 = 2^0\, 3^1\, 7^0 = 3,\ d_3 = 2^0\, 3^1\, 7^0 = 3,$$
$$(1,1,0), (2,1,0), (1,0,0) \rightsquigarrow d_1 = 2^1\, 3^2\, 7^1 = 126,\ d_2 = 2^1\, 3^1\, 7^0 = 6,\ d_3 = 2^0\, 3^0\, 7^0 = 1,$$
$$(2,0,0), (2,1,0), (1,0,0) \rightsquigarrow d_1 = 2^2\, 3^2\, 7^1 = 252,\ d_2 = 2^0\, 3^1\, 7^0 = 3,\ d_3 = 2^0\, 3^0\, 7^0 = 1,$$
$$(1,1,0), (3,0,0), (1,0,0) \rightsquigarrow d_1 = 2^1\, 3^3\, 7^1 = 378,\ d_2 = 2^1\, 3^0\, 7^0 = 2,\ d_3 = 2^0\, 3^0\, 7^0 = 1,$$
$$(2,0,0), (3,0,0), (1,0,0) \rightsquigarrow d_1 = 2^2\, 3^3\, 7^1 = 756,\ d_2 = 2^0\, 3^0\, 7^0 = 1,\ d_3 = 2^0\, 3^0\, 7^0 = 1,$$

Since elementary divisors of an abelian group must be at least 2, we discard any $d_j = 1$ (if we included them, they would contribute the trivial group $\mathbb{Z}/1\mathbb{Z} = \{0\}$ to the direct sum decomposition, which wouldn't change the overall group anyway). So our final list of elementary divisors for an abelian group of order 756 is:

$$3|6|42,\ 3|3|84,\ 6|126,\ 3|252,\ 2|378,\ 756.$$

And the corresponding list of representative abelian groups is finally

$$(\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/6\mathbb{Z}) \oplus (\mathbb{Z}/42\mathbb{Z}),\ (\mathbb{Z}/3\mathbb{Z})^2 \oplus (\mathbb{Z}/84\mathbb{Z}),\ (\mathbb{Z}/6\mathbb{Z}) \oplus (\mathbb{Z}/126\mathbb{Z}),$$
$$(\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/252\mathbb{Z}),\ (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/378\mathbb{Z}),\ \mathbb{Z}/756\mathbb{Z}.$$

Before proceeding to the next example, we make a quick observation. If $d_k|d_{k-1}|\cdots|d_1$ are the elementary divisors of an abelian group A, so that

$$A \cong (\mathbb{Z}/d_k\mathbb{Z}) \oplus (\mathbb{Z}/d_{k-1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_1\mathbb{Z}),$$

then d_1 (the largest elementary divisor) is an (in fact the smallest) *exponent* for A. That is, $d_1 a = 0$ for all $a \in A$. To see why, let $(m_k, m_{k-1}, \ldots, m_1)$ belong to the direct sum. Then

$$d_1(m_k, m_{k-1}, \ldots, m_1) = (d_1 m_k, d_1 m_{k-1}, \ldots, d_1 m_1).$$

But every element of $\mathbb{Z}/d_j\mathbb{Z}$ has order dividing d_j (the size of the group), and $d_j|d_1$ for all j. So

$$(d_1 m_k, d_1 m_{k-1}, \ldots, d_1 m_1) = (0, 0, \ldots, 0),$$

as claimed. A nice application of this fact is the following.

Example 2. Let G be a finite subgroup of $\mathbb{C}^\times$. Use the Fundamental Theorem to write

$$G \cong (\mathbb{Z}/d_k\mathbb{Z}) \oplus (\mathbb{Z}/d_{k-1}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/d_1\mathbb{Z}),$$

with $d_k|d_{k-1}|\cdots|d_1$ (keep in mind that the group G is written multiplicatively). According to the discussion above, $z^{d_1} = 1$ for all $z \in G$. This shows that every member of G is a root of the polynomial $X^{d_1} - 1$. This means that $X^{d_1} - 1$ has at least $|G| = d_1 d_2 \cdots d_k$ roots in $\mathbb{C}$. But it is well known that the number of complex roots of a polynomial $f(X)$ with complex coefficients cannot exceed its degree $\deg f$, which is simply the largest power of X occurring in $f(X)$. In particular, $X^{d_1} - 1$ has at most d_1 complex roots. Since the members of G have yielded $d_1 d_2 \cdots d_k$ roots, we must therefore have

$$d_1 d_2 \cdots d_k \leq d_1.$$

If $k > 1$ this is impossible, since each $d_j \geq 2$. So we must have $k = 1$. That is, d_1 is the only elementary divisor of G, so that

$$G \cong \mathbb{Z}/d_1\mathbb{Z},$$

which shows that G *must be cyclic*. So we have proven:

Theorem 2. *Every finite subgroup of the multiplicative group $\mathbb{C}^\times$ must be cyclic.*

Going a little bit further, suppose G is a finite subgroup of $\mathbb{C}^\times$ of order n. Then G is cyclic, say $G = \langle\zeta\rangle$. And every $z \in G$ satisfies $z^n = 1$, or $z^n - 1 = 0$, since $n = |G|$. So the members of G are precisely the roots of the polynomial $X^n - 1$. That is

$$G = \langle\zeta\rangle = \boldsymbol{\mu}_n = \{z \in \mathbb{C} \,|\, z^n - 1 = 0\},$$

the group of *nth roots of unity*, which we encountered previously in the homework. The generator ζ (which is not unique) is called a *primitive* nth root of unity. This provides a classification of *every* finite subgroup of $\mathbb{C}^\times$.

Theorem 3. *For each $n \in \mathbb{N}$, the group $\boldsymbol{\mu}_n$ of nth roots of unity is cyclic, and it is the unique subgroup of $\mathbb{C}^\times$ of order n.*