Finite Abelian Groups I:
Direct Sum Torsion Decompositions

R. C. Daileda

The Classification of Finite Cyclic groups tells us that for each $n \in \mathbb{N}$, there is (up to isomorphism) exactly one cyclic group of order n, namely $\mathbb{Z}/n\mathbb{Z}$. It is also possible to completely characterize the finite abelian groups as those that are (internal) direct sums of certain cyclic subgroups. Somewhat more precisely, every (additive) finite abelian group A is the internal direct sum

$$A = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle \cong (\mathbb{Z}/n_1\mathbb{Z}) \oplus \cdots (\mathbb{Z}/n_r\mathbb{Z}),$$

for certain $a_i \in A$ with $|a_i| = n_i$. Under appropriate hypotheses on the orders n_i, this decomposition is unique to A, and gives a complete description of the group-theoretic structure of A. The precise version of these statements is known as the Fundamental Theorem of Finite Abelian groups, which we will state and prove later.

So how can we determine the cyclic summands of a finite abelian group A given that we know so little about it? In the decomposition above, notice that since $n_i = |a_i| = |\langle a_i \rangle|$, so that $n_i a = 0$ for all $a \in \langle a_i \rangle$, by Lagrange's Theorem. Recall that for any $n \in \mathbb{N}$, the *n-torsion subgroup* of A is

$$A[n] := \{a \in A \,|\, na = 0\},$$

which consists of those elements of A whose order divides n. So in the case above we have $\langle a_i \rangle \leq A[n_i]$, with $n_i || A|$. This suggests that the torsion subgroups of A, which are defined independent of any direct sum decomposition of A, are the place to start looking for the cyclic summands of A.

Given an abelian group A (which need not be finite) and an integer $n \geq 1$, multiplicative factorizations of n very naturally give rise to direct sum decompositions of $A[n]$. We begin by noting that if $n = dm$ with $d, m \in \mathbb{N}$ then:

- $A[d] \leq A[n]$;
- for all $a \in A[n]$, $ma \in A[d]$.

The proofs of these statements are easy exercises, and we can freely interchange m and d in both, since $dm = md$. We can now prove:

Theorem 1. *Let A be an abelian group and let $n \in \mathbb{N}$. If $n = dm$ for some $m, d \in \mathbb{N}$ with $\gcd(d, m) = 1$, then $A[n]$ is the internal direct sum*

$$A[n] = A[d] \oplus A[m].$$

Proof. Use Bézout's Lemma to write $1 = rd + sm$ for some $r, s \in \mathbb{Z}$. Then for any $a \in A[n]$ we have

$$a = 1a = (rd + sm)a = (rd)a + (sm)a = r(da) + s(ma) \in A[m] + A[d],$$

by the second remark above. Thus $A[n] \leq A[m] + A[d]$. The first remark tells us that $A[m]$ and $A[d]$ are subgroups of $A[n]$, so that $A[m] + A[d] \leq A[n]$, too. Therefore $A[n] = A[m] + A[d]$.

To prove that the sum is direct we must show $A[m] \cap A[d]$ is trivial. To that end, let $a \in A[m] \cap A[d]$. Then $|a|$ divides both m and d. But $\gcd(m, d) = 1$, so this implies that $|a| = 1$ and hence $a = 0$. This completes the proof. □

Corollary 1. *Let A be an abelian group and let $n \geq 2$ be an integer. Write*

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

where the p_i are distinct primes and $e_i \geq 1$ for all i. Then $A[n]$ is the internal direct sum

$$A[n] = A[p_1^{e_1}] \oplus \cdots \oplus A[p_r^{e_r}] = \bigoplus_{i=1}^{r} A[p_i^{e_i}].$$

Proof. Since $p_j^{e_j}$ and $p_{j+1}^{e^{j+1}} \cdots p_r^{e^r}$ are relatively prime for $j = 1, \ldots, r-1$, Theorem 1 tells us that we have internal direct sums

$$\begin{aligned} A[n] &= A[p_1^{e_1}] \oplus A[p_2^{e_2} \cdots p_r^{e_r}] \\ &= A[p_1^{e_1}] \oplus A[p_2^{e_2}] \oplus A[p_3^{e_3} \cdots p_r^{e_r}] \\ &\vdots \\ &= A[p_1^{e_1}] \oplus A[p_2^{e_2}] \oplus \cdots \oplus A[p_r^{e_r}]. \end{aligned}$$

□

Let p be a prime. Because a prime power p^e has no nontrivial factorizations with relatively prime factors, the decomposition of Corollary 1 clearly can be carried no further. So we turn to an analysis of the p^e-torsion subgroups $A[p^e]$ of an abelian group A. Because every member of $A[p^e]$ has order dividing p^e, and the only divisors of p^e are of the form p^j, we conclude that the order of every element of $A[p^e]$ is a power of p.

A group with the property that every one of its elements has order equal to a power of p is called a *p-group*. A p-group (abelian or not) can certainly have infinite order. Take the direct sum (or product) of an infinite number of copies of $\mathbb{Z}/p\mathbb{Z}$, for instance (the product is actually an *uncountable* p-group). But the order of a *finite* p-group must always be a power of p. For general groups this is an easy consequence of *Cauchy's theorem*, which we won't get into here. But for finite *abelian* p-groups, however, all we need is strong induction.

Lemma 1. *Let p be a prime number. The order of a finite abelian p-group is a power of p.*

Proof. Let A be a finite abelian p-group. We (strongly) induct on the order of A. If $|A| = 1$, the conclusion is immediate. Now suppose $|A| > 1$ and assume that we have proven every

finite abelian p-group of order strictly less than $|A|$ has order equal to a power of p. Choose $0 \neq a \in A$ (why is this possible?) and let $A' = \langle a \rangle$. Because A is a p-group, we know that $|A'| = |a|$ is a power of p. Since A/A' is a finite abelian p-group and $|A/A'| = |A|/|A'| < |A|$ (because $|A'| = |a| > 1$), the inductive hypothesis implies that $|A/A'|$ is also a power of p. Therefore $|A| = |A/A'| \cdot |A'|$ is a power of p as well. This completes the inductive step and completes the proof. □

Corollary 2. *If A is a finite abelian group, p is a prime and $e \geq 0$, then the order of $A[p^e]$ is a power of p.*

If A is a finite abelian group of order n, then $A = A[n]$, by Lagrange's theorem. Thus:

Theorem 2. *Let A be a finite abelian group of order $n = p_1^{e_1} \cdots p_r^{e_r}$, where the p_i are distinct primes and each $e_i \geq 1$. Then A is the internal direct sum*

$$A = A[p_1^{e_1}] \oplus \cdots A[p_r^{e^r}],$$

and $|A[p_i^{e_i}]| = p_i^{e_i}$ for all i.

Proof. Since $A = A[n]$, the direct sum decomposition follows from Corollary 1. Corollary 2 tells us that $|A[p_i^{e_i}]| = p_i^{f_i}$ for some $f_i \geq 0$. From the direct sum we then have

$$p_1^{e_1} \cdots p_r^{e_r} = n = |A| = |A[p_1^{e_1}]| \cdot |A[p_2^{e_2}]| \cdots |A[p_r^{e_r}]| = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}.$$

We now appeal to the Fundamental Theorem of Arithmetic to conclude that $e_i = f_i$ for all i, and we're finished. □

It's interesting to note that our proof that $|A[p_i^{e_i}]| = p_i^{e_i}$ is completely indirect. We only arrived at this conclusion because Corollary 2 and the Fundamental Theorem of Arithmetic ensured there were no other options. We didn't actually *count* anything!

Another interesting observation is that the conclusions of Theorem 2 remain valid if we weaken the hypothesis on the exponents in the prime factorization of n to $e_i \geq 0$, since

$$A[1] = \{0\}.$$

So, for instance, if we instead wrote the prime factorization of n in the more abstract form

$$n = \prod_p p^{e_p}, \quad e_p \in \mathbb{N}_0,$$

then we'd still have the internal direct sum

$$A = \bigoplus_p A[p^{e_p}]$$

with $|A[p^{e_p}]| = p^{e_p}$ for all p.

On the other hand, if we replace the order n of A by any multiple $n' = kn$, the direct sum decomposition of Theorem 2 is still valid since

$$A[p_i^{e_i+f_i}] = A[p_i^{e_i}]$$

for any $f_i \geq 0$, and $A[q^f] = \{0\}$ for any prime q not dividing n, by Lagrange's theorem. The formula for the orders of the p-power torsion subgroups of A may no longer hold in this case, however.

Along these same lines, we can also express the direct sum decomposition of Theorem 2 in a way that makes no reference to the exponents e_i at all. Because

$$A[p] \leq A[p^2] \leq A[p^3] \leq \cdots$$

and the union of an ascending chain of subgroups is always a subgroup (exercise), we can define the *p-power torsion subgroup* of A to be

$$A(p) = \bigcup_{e=1}^{\infty} A[p^e]. \tag{1}$$

$A(p)$ consists of all elements of A whose order is *any* power of p. In the notation of Theorem 2 we clearly have $A(p_i) = A[p_i^{e_i}]$ for every p_i dividing the order of A, so that the internal direct sum decomposition becomes

$$A = A(p_1) \oplus A(p_2) \oplus \cdots A(p_r).$$

This p-power torsion notation is somewhat simpler, but the notation $A(p)$ alone doesn't include enough information to immediately tell us the size of this subgroup. But this actually has an aesthetic advantage. Since we have already seen that $A(q) = \{0\}$ for q not dividing $|A|$, we can now rewrite (1) as

$$A = \bigoplus_{p} A(p), \tag{2}$$

which makes no reference to the exponents occurring in the prime factorization of A. Theorem 2 then tells us that

$$|A(p)| = p^e$$

for every prime p, where p^e is the largest power of p dividing $n = |A|$.

The "exponent free" internal direct sum decomposition (2) actually holds for any *torison* abelian group A (one in which every element has finite order, although $|A|$ itself need not be finite). The proof requires a modification of the argument used in Corollary 1 and is left as an exercise for the reader.