Finite Abelian Groups II: Finite Abelian p-Groups

R. C. Daileda

Our goal now is to decompose any finite abelian p-group (p a prime) as an internal direct sum of cyclic subgroups. First we nee two lemmas.

Lemma 1. *Let A be an additive abelian group and suppose $a \in A$ has order p^r where p is prime and $r \geq 0$. Then for any $k \in \mathbb{N}_0$:*

$$|p^k a| = \begin{cases} p^{r-k} & \text{if } k \leq r, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. We have

$$|p^k a| = \frac{|a|}{\gcd(p^k, |a|)} = \frac{p^r}{\gcd(p^k, p^r)} = \frac{p^r}{p^{\min\{k,r\}}} = p^{r-\min\{k,r\}}.$$

$\square$

Now let A be a finite abelian p-group. Choose $a_1 \in A$ whose order p^{r_1} is as large as possible. Let $A_1 = \langle a_1 \rangle$. Then A/A_1 is a finite abelian p-group and we have the canonical epimorphism $\pi : A \to A/A_1$. Given $b \in A$, because π is a homomorphism, we know that $|\pi(b)|$ in A/A_1 must divide $|b|$ in A. In order for our argument below to work, we need to know that, in fact, $|b| = |\pi(b)|$. But in general there's nothing to prevent $|b|$ from being strictly larger than $|\pi(b)|$. Fortunately, $\pi(a) = \pi(b)$ for any $a \in b + A_1$, so it might be possible to "adjust" b by an element of A_1 to get $a \in A$ with $|a| = |\pi(a)|$ and $\pi(a) = \pi(b)$. The next lemma shows that this is indeed always possible.

Lemma 2. *Let A be a finite abelian p-group, and suppose $a_1 \in A$ has maximum possible order p^{r_1}. Set $A_1 = \langle a_1 \rangle$ and let $\pi : A \to A/A_1$ denote the canonical epimorphism. For any $b \in A$, there exists $a \in A$ so that $\pi(a) = \pi(b)$ and $|a| = |\pi(b)|$.*

Proof. Let $c \in \pi(b) = b + A_1$ so that $\pi(c) = \pi(b)$. Then

$$p^r = |\pi(b)| = |\pi(c)| \quad \text{divides} \quad |c| = p^s,$$

which implies that $r \leq s$. Furthermore, since $|\pi(c)| = p^r$ in A/A_1, we have

$$A_1 = p^r \pi(c) = \pi(p^r c) \quad \Rightarrow \quad p^r c \in A_1 \quad \Rightarrow \quad p^r c = n a_1$$

for some $n \in \mathbb{N}$. Write $n = p^k t$ with $k \geq 0$ and $p \nmid t$. Then

$$|t a_1| = \frac{|a_1|}{\gcd(t, |a_1|)} = \frac{p^{r_1}}{\gcd(t, p^{r_1})} = p^{r_1}.$$

This means we can compute $p^r c = na_1 = p^k(ta_1)$ in two ways using Lemma 1. On the one hand

$$|p^r c| = p^{s-\min\{r,s\}} = p^{s-r} \quad \text{since} \quad r \leq s.$$

On the other hand

$$|p^k(ta_1)| = p^{r_1-\min\{k,r_1\}}.$$

Since both elements have the same order we conclude that

$$s - r = r_1 - \min\{k, r_1\}. \tag{1}$$

If $k > r_1$, (1) becomes $s-r = 0$ or $r = s$. That is, $|c| = p^s = p^r$. Since $\pi(c) = \pi(b)$, we can take $a = c$ to prove the lemma. If $k \leq r_1$, (1) becomes $s - r = r_1 - k$ or $k - r = r_1 - s \geq 0$, since p^{r_1} is the largest possible order of elements in A, and $|c| = p^s$. Therefore $k \geq r$ and we have

$$p^r c = p^k(ta_1) = p^r(p^{k-r}ta_1) = p^r a_1',$$

where $a_1' = p^{k-r}ta_1 \in A_1$, since $p^{k-r} \in \mathbb{N}$. We then have

$$p^r(c - a_1') = 0.$$

This shows that $|c - a_1'|$ divides p^r. But we also know that $|\pi(c - a_1')| = |\pi(c)| = |\pi(b)| = p^r$, which shows that $|c - a_1'|$ is divisible by p^r. We conclude that $a = c - a_1'$ has order p^r and satisfies $\pi(a) = \pi(c) = \pi(b)$, as needed. □

Example 1. Assume p is an odd prime and consider the finite abelian p-group $A = (\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z})$. The element $(1,1)$ has order p^2, which is as large as possible, since $A = A[p^2]$. So, in the notation of Lemma 2, we have $a_1 = (1,1)$ and $A_1 = \langle (1,1) \rangle$. Since $|A/A_1| = p^3/p^2 = p$, every nontrivial element of A/A_1 has order p.

The element $b = (1,2)$ does not belong to A_1, since $(1,2) = k(1,1) = (k,k)$ would imply $k \equiv 1 \pmod{p}$ and $k \equiv 2 \pmod{p^2}$, which is impossible. So $b + A_1$ has order p in A/A_1. However, $(1,2)$ does not have order p in A since $p(1,2) = (p, 2p) = (0, 2p) \neq (0,0)$. Following the proof of Lemma 1 we write $pb = p(1,2) = (0,2p) = (2p,2p) = 2p(1,1) = 2pa_1$, so that $p(b - 2a_1) = 0$. So $a = b - 2a_1$ has order p in A and $a \equiv b \pmod{A_1}$.

Theorem 1. *Let p be a prime and let A be a finite abelian p-group. Then there is a sequence of positive integers $r_1 \geq r_2 \geq \cdots \geq r_k$ so that A is the internal direct sum*

$$A = C(p^{r_1}) \oplus C(p^{r_2}) \oplus \cdots \oplus C(p^{r_k}),$$

where each $C(p^{r_i})$ is a cyclic subgroup of A of order p^{r_i}.

Proof. We induct on $|A|$. When $|A| = 1$, A has *no* nontrivial cyclic subgroups. We may therefore take the sequence $\{r_i\}$ to be empty, since any direct sum indexed by the empty set is understood to be the trivial group. So assume $|A| > 1$ and that we have proven the theorem for all finite abelian p-groups of order strictly less than $|A|$. As in Lemma 2, choose $a_1 \in A$ with $|a_1| = p^{r_1}$ as large as possible, and set $A_1 = \langle a_1 \rangle$. Since $|A/A_1|$ is a finite abelian p-group whose order is less than $|A|$, the inductive hypothesis implies that A/A_1 is an internal direct sum

$$A/A_1 = C(p^{r_2}) \oplus C(p^{r_3}) \oplus \cdots \oplus C(p_k^{r_k}), \tag{2}$$

where each $C(p^{r_i})$ is a cyclic subgroup of A/A_1 with order p^{r_i}. For each i write

$$C(p^{r_i}) = \langle b_i + A_1 \rangle.$$

Then $b_i + A_1$ has order p^{r_i} and we can use Lemma 2 to find $a_i \in A$ so that $a_i + A_1 = b_i + A_1$ and $|a_i| = p^{r_i}$. In particular, $C(p^{r_i}) = \langle a_i + A_1 \rangle$ for all i.

We claim that the sum

$$A_1 \oplus \langle a_2 \rangle \oplus \langle a_3 \rangle \oplus \cdots \oplus \langle a_k \rangle \tag{3}$$

is direct. To see why, suppose that

$$n_1 a_1 + n_2 a_2 + \cdots + n_k a_k = 0$$

in A. Apply the canonical epimorphism $\pi : A \to A/A_1$ to obtain

$$\begin{aligned} 0 &= n_1 \pi(a_1) + n_2 \pi(a_2) + \cdots + n_k \pi(a_k) \\ &= n_2(a_2 + A_1) + \cdots + n_k(a_k + A_1). \end{aligned}$$

Because each $C(p^{r_i}) = \langle a_i + A_1 \rangle$, and the sum of the $C(p^{r_i})$ is direct, it must be the case that $n_i(a_i + A_1) = A_1$ for all i. Since $|a_i + A_1| = p^{r_i}$, it follows that p^{r_i} divides n_i for all i. But we also have $|a_i| = p^{r_i}$, so this implies $n_i a_i = 0$ in A. Therefore, the equality

$$n_1 a_1 + n_2 a_2 + \cdots + n_k a_k = 0$$

implies that $n_i a_i = 0$ for all $2 \leq i \leq k$, and therefore $n_1 a_1 = 0$ as well. This proves the sum (3) is direct.

The final step is to show that A is actually equal to the direct sum. This can be accomplished with a quick counting argument. First of all

$$|\langle a_i \rangle| = |a_i| = p^{r_i} = |C(p^{r_i})|$$

So by (2) and Lagrange's theorem

$$\frac{|A|}{|A_1|} = |A/A_1| = \prod_{i=2}^{k} |C(p_i^{r_i})| = \prod_{i=2}^{k} |\langle a_i \rangle|.$$

Therefore

$$|A| = |A_1| \prod_{i=2}^{k} |\langle a_i \rangle| = |A_1 \oplus \langle a_2 \rangle \oplus \langle a_3 \rangle \oplus \cdots \oplus \langle a_k \rangle|.$$

Since the sum on the right is a subgroup of A, this implies that the two groups coincide. □

Given a finite abelian p-group A, the tuple $(r_1, r_2, \ldots, r_k)$ of exponents occurring in the direct sum decomposition of Theorem 1 will be called the *type* of A. Our final goal is to show that the type of a finite abelian p-group is unique. That is, if A also has type $(s_1, s_2, \ldots, s_\ell)$, then

$$(r_1, r_2, \ldots, r_k) = (s_1, s_2, \ldots, s_\ell).$$

Equivalently, $k = \ell$ and $r_i = s_i$ for all i.

Once again we induct on $|A|$. When $|A| = 1$ the only possible type is the empty tuple $()$, which is clearly unique. Now suppose $|A| > 1$ and that we have proven the type of any smaller abelian p-group is unique. Write

$$(r_1, r_2, \ldots, r_k) = (r_1, r_2, \ldots, r_{k-\mu}, \underbrace{1, 1, \ldots, 1}_{\mu \text{ ones}}),$$

$$(s_1, s_2, \ldots, s_\ell) = (s_1, s_2, \ldots, s_{\ell-\nu}, \underbrace{1, 1, \ldots, 1}_{\nu \text{ ones}}),$$

where $r_{k-\mu} \geq 2$, $s_{\ell-\nu} \geq 2$, and we allow $\mu = 0$ or $\nu = 0$ if necessary. Then pA is a finite abelian p-group of types

$$(r_1 - 1, r_2 - 1, \ldots, r_{k-\mu} - 1),$$

$$(s_1 - 1, s_2 - 1, \ldots, s_{\ell-\nu} - 1),$$

since $pC(p^r)$ is a cyclic group of order p^{r-1} (why?). Because $|pA| < |A|$ (why?), the inductive hypothesis implies that

$$(r_1 - 1, r_2 - 1, \ldots, r_{k-\mu} - 1) = (s_1 - 1, s_2 - 1, \ldots, s_{\ell-\nu} - 1),$$

so that $k - \mu = \ell - \nu = m$ and $r_i - 1 = s_i - 1$ for $i \leq m$. We then have $r_i = s_i$ for $i \leq m$ and the order of A is therefore

$$p^{r_1 + r_2 + \cdots + r_m + \mu} = p^{s_1 + s_2 + \cdots + s_m + \nu}.$$

Because $r_i = s_i$ for all $i \leq m$, it follows that $\mu = \nu$, and hence $k = \ell$, since $k - \mu = \ell - \nu$. And since $r_i = s_i = 1$ for $i \leq k$, and $k = \ell$, we finally have

$$(r_1, r_2, \ldots, r_k) = (s_1, s_2, \ldots, s_\ell),$$

as needed. This proves that the type of A is unique, which completes the inductive step and finishes our proof. To summarize:

Theorem 2. *Let A be a finite abelian p-group. The exponents $r_1 \geq r_2 \geq \cdots \geq r_k$ of Theorem 1 are unique.*

Because every cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, as an immediate corollary to Theorems 1 and 2 we obtain

Corollary 1. *Let A be a finite abelian p-group. Then there is a unique sequence of positive integers $r_1 \geq r_2 \geq \cdots \geq r_k$ so that*

$$A \cong (\mathbb{Z}/p^{r_1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{r_2}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{r_k}\mathbb{Z}).$$

Notice that if A is an abelian p-group of order p^e, and we decompose A as in Corollary 1, then

$$p^e = |A| = |(\mathbb{Z}/p^{r_1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{r_2}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{r_k}\mathbb{Z})| = p^{r_1} p^{r_2} \cdots p^{r_k} = p^{r_1 + r_2 + \cdots + r_k}.$$

That is,
$$e = r_1 + r_2 + \cdots + r_k \quad \text{with} \quad r_1 \geq r_2 \geq \cdots \geq r_k \geq 1,$$
which is called a *partition* of e. It follows that:

Corollary 2. *The isomorphism classes of abelian p-groups of order p^e correspond to the integer partitions of e.*

Example 2. Let's classify the finite abelian p-groups of order p^5, up to isomorphism. According to Corollary 2, the isomorphismclasses correspond to partitions of $e = 5$. These are
$$(1,1,1,1,1), (2,1,1,1), (2,2,1), (3,1,1), (3,2), (4,1), (5).$$
and the corresponding groups representing each class are
$$\begin{aligned}
&(\mathbb{Z}/p\mathbb{Z})^5, \;\; (\mathbb{Z}/p^2\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z})^3, \;\; (\mathbb{Z}/p^2\mathbb{Z})^2 \oplus (\mathbb{Z}/p\mathbb{Z}), \\
&(\mathbb{Z}/p^3\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z})^2, \;\; (\mathbb{Z}/p^3\mathbb{Z}) \oplus (\mathbb{Z}/p^2\mathbb{Z}), \\
&(\mathbb{Z}/p^4\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z}), \;\; \mathbb{Z}/p^5\mathbb{Z}.
\end{aligned}$$
It is important to note that no two groups in this list can be isomorphic.