Order "Lifting" in Finite Abelian p-Groups

R. C. Daileda

One of the essential ingredients in the proof of the fundamental theorem of finite abelian groups is the classification of the finite abelian p-groups, (p being a prime number). The outline of the proof of the classification theorem is straightforward enough. Given a finite abelian p-group A, form a nontrivial quotient of A by a cyclic subgroup A_1. Then inductively decompose A/A_1 as a direct sum of cyclic p-groups. Finally, we form $A_1\times A/A_1$, which has the structure we want and whose size is $|A|$ and, and then argue that this is, in fact, isomorphic to A.

It's establishing the existence of an isomorphism $\psi : A_1\times A/A_1 \to A$ in the final step that's the most challenging task. However, this follows almost immediately from the Lemma stated below, which involves the ability to "lift" elements through the canonical map $\pi : A \to A/A_1$ while preserving their order. The Lemma is easy enough to state and prove "in a vacuum," and in most presentations its statement and proof are usually totally unmotivated. Given that it is the linchpin of the entire proof of the classification theorem, this is hardly an intellectually satisfying state of affairs. The goal of this note is rectify this situation. We will not only deduce the necessity of the Lemma, but will actually stumble across it's proof prior to its statement.

We now turn to a careful analysis of the data at hand. The inclusion $\iota : A_1 \hookrightarrow A$ and the canonical map $\pi : A \to A/A_1$ together yield a pair of homomorphisms of abelian groups,

$$A_1 \xrightarrow{\iota} A \xrightarrow{\pi} A/A_1,$$

with the property that $\operatorname{im}\iota = \ker\pi$. Such a pair is called *exact*. For convenience, denote the trivial group by 0. The pair $0 \to A_1 \xrightarrow{\iota} A$ is exact, since the inclusion is injective, as is the pair $A \xrightarrow{\pi} A/A_1 \to 0$, because the canonical map is surjective. Putting these together yields the sequence

$$0 \to A_1 \xrightarrow{\iota} A \xrightarrow{\pi} A/A_1 \to 0, \tag{1}$$

which is exact at each "link.". This is known as a *short exact sequence* of abelian groups.

A very similar short exact sequence can naturally be derived from $A_1 \times A/A_1$, namely

$$0 \to A_1 \xrightarrow{\iota_1} A_1 \times A/A_1 \xrightarrow{\pi_2} A/A_1 \to 0, \tag{2}$$

where $\iota_1(a) = (a, 0)$ and $\pi_2(a, \beta) = \beta$.[1] If we stack (1) and (2) we get a diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_1 & \xrightarrow{\iota_1} & A_1 \times A/A_1 & \xrightarrow{\pi_2} & A/A_1 & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \vdots\ \psi & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A_1 & \xrightarrow{\iota} & A & \xrightarrow{\pi} & A/A_1 & \longrightarrow & 0 \end{array} \tag{3}$$

[1] We've used the variable β only to indicate that elements of A/A_1 are cosets and not elements of A.

where the solid vertical arrows are identity functions. The dashed line represents the hypothetical isomorphism ψ between A and $A_1 \times A/A_1$.

With the goal of reverse engineering it, assume there is a homomorphism ψ so that the diagram (3) is *commutative*. The *short five lemma* then guarantees that it must be an isomorphism. If $\iota_2 : A/A_1 \to A_1 \times A/A_1$ is the map $\beta \mapsto (0, \beta)$, let $\sigma = \psi \circ \iota$. Notice that for any $\beta \in A/A_1$ we have

$$\pi(\sigma(\beta)) = \pi \circ \psi(0, \beta) = \pi_2(0, \beta) = \beta.$$

In other words, $\sigma : A/A_1 \to A$ is a homomorphism satisfying $\pi \circ \sigma = 1_{A/A_1}$. Such a map is called a *section* of π, and its existence is equivalent to the existence of ψ.

To see this, suppose $\sigma : A/A_1 \to A$ is a section of π and define $\psi : A_1 \times A/A_1 \to A$ by $(a, \beta) \mapsto a + \sigma(\beta)$. This is certainly a homomorphism and we have

$$\psi(\iota_1(a)) - \psi(a, 0) = a = \iota(a) \text{ for all } a \in A_1$$

as well as

$$\pi(\psi(a, \beta)) = \pi(a + \sigma(\beta)) = \pi(a) + \beta = \beta = \pi_2(a, \beta) \quad \text{for all } (a, \beta) \in A_1 \times A/A_1,$$

since $\ker \pi = A_1$. This means that (3) commutes and hence that ψ is an isomorphism.

The moral of all of this discussion is that if A is a finite abelian p-group, and we can find a nontrivial cyclic subgroup A_1 of A for which the canonical epimorphism $A \to A/A_1$ has a section, then $A \cong A_1 \times A/A_1$, and we can inductively argue that A has a decomposition as a direct sum of cyclic p-groups.

Set-theoretically, every surjective function has a "section," because it has a right inverse. But a section of a surjective homomorphism $f : A \to B$ is not only a right inverse, but also itself an (injective) homomorphism. Arranging this is not as simple as it sounds: simply choosing an arbitrary preimage for each element of B is not likely to yield a subgroup of A. For example, consider the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. The subgroup $Z = Z(Q) = \{\pm 1\}$ is normal and the quotient Q/Z has order 4, so is abelian. But there is no abelian subgroup of Q of order 4 of the form $\{1, \epsilon_1 i, \epsilon_2 j, \epsilon_3 k\}$ with all $\epsilon_i \in Z$. So the canonical map $\pi : Q \to Q/Z$ has no section.

Before thinking any further about sectioning π specifically, let's work a bit more generally. Let $f : A \to B$ be a surjective homomorphism of groups. Suppose $g : B \to A$ is a section of f. What distinguishes an arbitrary right inverse of f from a section of f? A right inverse simply chooses, for each $b \in B$, an element in $f^{-1}(\{b\})$. So let's compare arbitrary preimages with the preimages provided by g. Let $b \in B$ and let $a_1 \in A$ be any preimage of b. Set $a_2 = g(b)$, a particular preimage of b. Both a_1 and a_2 solve the equation $f(x) = b$, i.e. are *lifts* of b to A. However, because g is an injective homomorphism, $|a_2| = |b|$, whereas the most we can say about a_1 is that $|b|$ *divides* $|a_1|$. So a section of $f : A \to B$ must lift each element of B to A while simultaneously preserving order.

In and of itself, this more restrictive condition on a set-theoretic right inverse of $f : A \to B$ by no means guarantees it will be a section f. But it gives us a place to start. For suppose B is cyclic, generated by b, and that we can find *at least one* preimage $a \in A$ of b so that $|a| = |b|$. Then the map $g : B = \langle b \rangle \to \langle a \rangle$ defined by $nb \mapsto na$ is a well-defined isomorphism (n is not

necessarily unique, but a and b have the same order), and $f(g(nb)) = f(na) = nf(a) = nb$. Composing g with the inclusion of $\langle a \rangle$ into A, we obtain a section of f. This proves that when the codomain is cyclic, the existence of a section is *equivalent* to the existence of an order preserving right inverse (the former may be constructed from the latter).

And this is still true under the weaker hypothesis that B is a direct sum of cyclic groups. For suppose that $B = \oplus_{i \in I} B_i$,[2] that $B_i = \langle b_i \rangle$ for each i, and that we have $a_i \in f^{-1}(\{b_i\})$ so that $|a_i| = |b_i|$. Given $b \in B$, there is a unique expression $b = \sum_{i \in I} \beta_i$ with $\beta_i \in B_i$ for all i. Write $\beta_i = n_i b_i$ with $n_i \in \mathbb{Z}$ for each i, and define $g(b) = \sum_{i \in I} n_i a_i$. Although the β_i are unique, the integers n_i need not be, so we must check to see that g is well-defined. If we also have $\beta_i = m_i b_i$ for every i, then $|b_i| = |a_i|$ divides $m_i - n_i$, and so $\sum_{i \in I} n_i a_i = \sum_{i \in I} m_i a_i$. Therefore $g(b)$ is indeed well-defined. It is easy to see that it is a homomorphism, and hence

$$f(g(b)) = f\left(\sum_{i \in I} n_i a_i\right) = \sum_{i \in I} n_i f(a_i) = b,$$

for any $b \in B$. That is, g is a section of f.

It's important to notice that the real technical subtlety in the preceding two paragraphs is whether or not the maps we have constructed are well-defined. Once that question is settled, the fact that we've built a section is more or less automatic. To illustrate this point, suppose $B = \langle b \rangle$ and we choose an *arbitrary* preimage a of b in A. We might still attempt to define $g : \langle b \rangle \to \langle a \rangle$ by the same formula, namely $g(nb) = na$. If $nb = mb$, then $|b|$ divides $n - m$, but $na = ma$ if an only if $|a|$ divides $n - m$. Unless $|b| = |a|$ we cannot guarantee that the former condition implies the latter, meaning that g may not actually define a function.

Returning to the case in which A is a finite abelian p-group, $A_1 < A$ is a nontrivial cyclic subgroup, and our homomorphism is the canonical map $\pi : A \to A/A_1$, we now see that we will be able to inductively prove that A is a direct sum of cyclic (sub)groups if we can show that π has an order-preserving right inverse. To that end, let $\beta \in A/A_1$ with $|\beta| = p^s$. If $\pi(b) = \beta$, then $|\beta| = p^s$ divides $|b|$. It suffices to show we can always choose b so that $p^s b = 0$.

Fix a particular preimage b_0 of β. Since $\ker \pi = A_1$, every other preimage is of the form $b = b_0 - a$ with $a \in A_1$. We have $p^s b = 0$ if and only if $p^s b_0 = p^s a$. So it suffices to show that if $p^s b_0 \in A_1$, then $p^s b_0 \in p^s A_1$. So, how do we choose A_1 so that

$$p^s A \cap A_1 \subset p^s A_1?$$

If $|A_1| = p^r$ and $s \leq r$, then the fact that A_1 is cyclic means $p^s A_1$ is the p^{r-s}-torsion subgroup of A_1. So $p^s A \cap A_1 \subset p^s A_1$ if and only if $p^{r-s}(p^s A \cap A_1) = p^r A \cap p^{r-s} A_1 = 0$. Since we have no control over s, the easiest way to make this happen is to simply choose r so large that $p^r A = 0$. This puts two restrictions on r: p^r needs to be an exponent for A and also needs to be the order of A_1, a cyclic subgroup of A.

So our entire discussion has boiled down to the following conclusion. We can inductively prove that a finite abelian p-group A is a direct sum of cyclic subgroups provided A has an element of order p^r (to generate A_1), and *no element of higher order* (lest p^r fail to be

[2]We need not assume that I is finite, but if it happens to be infinite we need to add the caveat that in any sum over I only finitely many summands are nonzero.

an exponent for A). This is easy to achieve. Simply let a be an element in A with largest possible order and set $A_1 = \langle a \rangle$. Although the proof that this accomplishes what we need is laid out above, we give the condensed (and unmotivated) version usually presented in textbooks.

Lemma. *Let A be a finite abelian p-group, $a \in A$ with maximum order, $A_1 = \langle a \rangle$, and $\pi : A \to A/A_1$ the canonical epimorphism. For any $\beta \in A/A_1$, there exists $b \in A$ so that $\beta = \pi(b)$ and $|b| = |\beta|$.*

Proof. Choose any $b' \in A$ so that $\pi(b') = \beta$. Since $|\beta| = p^s$ must divide $|b|$, and $|a| = p^r$ is an exponent for A, we must have $s \leq r$. Because the canonical map is a homomorphism,

$$0 = p^s\beta = \overline{p^s b'} \;\; \Rightarrow \;\; p^s b' \in \langle a \rangle.$$

Now $p^{r-s} \in \mathbb{N}$ and

$$p^{r-s}(p^s b') = p^r b' = 0 \;\; \Rightarrow \;\; p^s b' \in (\langle a \rangle)_{p^{r-s}}.$$

But $\langle a \rangle$ is a cyclic group of order p^r, so the p^{r-s}-torsion subgroup is precisely $\langle p^s a \rangle$ (exercise). This means that there is an $n \in \mathbb{Z}$ so that

$$p^s b' = n(p^s a) = p^s a',$$

where $a' = na \in \langle a \rangle$. Let $b = b' - a'$. Then $\pi(b) = \pi(b' - a') = \pi(b') = \beta$ and $p^s b = 0$. This means $|b|$ divides p^s and is divisible by $|\pi(b)| = |\beta| = p^s$, so that $|b| = p^s$, as needed.

□

Assembling everything above, the inductive proof that a finite abelian p-group A is the direct sum of cyclic subgroups is now almost immediate. We induct on n, where $|A| = p^n$. When $n = 1$, there is nothing to prove. Suppose that $|A| = p^n$ and we have proven the result for all finite abelian p-groups of smaller order. Let $a \in A$ have maximum order p^r and set $A_1 = \langle a \rangle$. By the Lemma, the canonical surjection $\pi : A \to A/A_1$ has an order-preserving right inverse. By our inductive hypothesis, A/A_1 is a direct sum of cyclic subgroups. As we have seen, these conditions together ensure the existence of a section $\sigma : A/A_1 \to A$ of π, and therefore there is an isomorphism $\psi : A_1 \times A/A_1 \to A$. This shows that A is a sum of cyclic subgroups, and completes the induction.

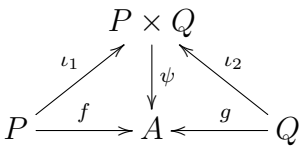
Remartk 1. There's one more, sightly more advanced, approach that can be taken here. Given the direct product/sum $P \times Q$ of any two abelian groups P and Q, we have a pair of homomorphisms

$$P \xrightarrow{\iota_1} P \times Q \xleftarrow{\iota_2} Q,$$

where $\iota_1(p) = (p, 0)$ and $iota_2(q) = (0, q)$. The *universal property of direct sums* states that given any similar arrangements of homomorphisms

$$P \xrightarrow{f} A \xleftarrow{g} Q,$$

there is a unique homomorphism $\psi :: P \times Q \to A$ so that



commutes.

In our context, this means that if we can section π (which still remains the crucial issue!), we get the homomorphism ψ "for free." Of course, there's still work remaining to show this is an isomorphism, but it gives us a new way to think about the problem.

Remark 2. The direct sum and direct product of a finite number of abelian groups are the same object. If we treat $P \times Q$ as a product, we get the same types of diagrams as above, but with the "arrows" reversed. Using the universality of products, one can show along the same lines that if its's possible to section the inclusion $\iota : A_1 \to A$, one can achieve the same effect. But this seems much more difficult to do.