DECOMPOSITION OF FINITE ABELIAN GROUPS

KEITH CONRAD

1. Introduction

Our goal is to prove the following decomposition theorem for finite abelian groups.

Theorem 1.1. *Each nontrivial finite abelian group A is a direct sum of cyclic subgroups of prime-power order: $A = C_1 \oplus \cdots \oplus C_r$, where C_i is cyclic and $|C_i|$ is a prime power.*[1]

Our strategy to prove Theorem 1.1 has the following steps:

- Define an analogue of primality and compositeness for finite abelian groups with respect to direct sums, called indecomposability and decomposability.
- Prove each nontrivial finite abelian group is a direct sum of indecomposable subgroups by copying the proof that integers greater than 1 have prime factorizations.
- Show the indecomposable finite abelian groups are cyclic of prime-power order.

The decomposition in Theorem 1.1 is both unique and not unique. For example,

$$(\mathbf{Z}/16\mathbf{Z})^\times = \{\pm 1 \bmod 16\} \times \langle 3 \bmod 16\rangle = \{1, 7 \bmod 16\} \times \langle 5 \bmod 16\rangle. \tag{1.1}$$

This shows an abelian group can be a direct product of cyclic subgroups of order 2 and 4 in more than one way, so in the most basic sense such a decomposition is not unique. On the other hand, the cyclic subgroups in one decomposition are isomorphic to those in the other. So if we consider the cyclic p-groups in a direct sum decomposition up to isomorphism (and account for multiplicity) then the decomposition is unique. That is analogous to uniqueness of prime factorization in $\mathbf{Z}^+$.

2. Decomposable and Indecomposable finite abelian groups

Here is an analogue for finite abelian groups of prime and composite numbers.

Definition 2.1. Let A be a nontrivial finite abelian group. Call A *indecomposable* if we can't write $A = B \oplus C$ for some nontrivial subgroups B and C. Call A *decomposable* if we can write $A = B \oplus C$ for two nontrivial subgroups B and C.

Example 2.2. A group of prime order is abelian (it's cyclic) and is indecomposable. For a group to be decomposable it at least must have nontrivial proper subgroups, and a group of prime order does not have such subgroups.

Example 2.3. A cyclic group of prime-power order is indecomposable. Let A be cyclic of order p^k where $k \geq 1$. If $A = B \oplus C$ where B and C are nontrivial subgroups of A then B and C have p-power order greater than 1 and thus B and C each contain a subgroup of order p (a subgroup of a cyclic group is cyclic and a cyclic group of order n has an element of order d for each d dividing n). That implies A has more than one subgroup of order p, but in a cyclic group there is at most one subgroup per size. Thus A is indecomposable.

Remark 2.4. The groups $\mathbf{Z}/(4)$ and $\mathbf{Z}/(2) \oplus \mathbf{Z}/(2)$ are *not* isomorphic since $\mathbf{Z}/(4)$ is indecomposable. Or since $\mathbf{Z}/(4)$ has an element of order 4 and $\mathbf{Z}/(2) \oplus \mathbf{Z}/(2)$ does not.

[1] We write abstract abelian groups here additively, so outside of examples we speak about direct sums rather than direct products.

Theorem 2.5. *A nontrivial finite abelian group is a direct sum of indecomposable subgroups.*

Proof. This argument will be the same as the standard proof of the existence of prime factorization in the positive integers. We argue by induction on the order n of the group.

For the base case $n = 2$, abelian groups of order 2 are indecomposable since 2 is prime (Example 2.2). Suppose $n > 2$ and each nontrivial abelian group of order less than n is a direct sum of indecomposable subgroups. Let A be abelian of order n.

Case 1: A is indecomposable. We are done, since A is a direct sum of itself (one term).

Case 2: A is decomposable. We have $A = B \oplus C$ for nontrivial subgroups B and C. Then $n = |B||C|$ with $|B|$ and $|C|$ being greater than 1, so they are less than n. By induction,

$$B = P_1 \oplus \cdots \oplus P_r, \quad C = Q_1 \oplus \cdots \oplus Q_s$$

for indecomposable P_i and Q_j. Then $A = P_1 \oplus \cdots \oplus P_r \oplus Q_1 \oplus \cdots \oplus Q_s$. □

3. Classification of indecomposable finite abelian groups

To give Theorem 2.5 more substance, we will describe the indecomposable finite abelian groups. In Example 2.3 we saw cyclic groups of prime-power order are indecomposable. It turns out every indecomposable finite abelian group is cyclic of prime-power order. We'll show the group has prime-power order by the next lemma, which decomposes a finite abelian group in terms of a decomposition of its order into relatively prime parts.

Lemma 3.1. *If A is an abelian group and $|A| = mn$ where $(m, n) = 1$ then $A = A_m \oplus A_n$ for the subgroups $A_m = \{a \in A : ma = 0\}$ and $A_n = \{a \in A : na = 0\}$.*

Proof. The subsets A_m and A_n are subgroups because A is abelian, *e.g.*, if $ma = 0$ and $ma' = 0$ then $m(a + a') = ma + ma' = 0 + 0 = 0$. Using multiplicative notation for a moment, we have $(gh)^m = g^m h^m$ when $gh = hg$, but it might not be true if $gh \neq hg$.[2]

To show $A = A_m + A_n$, write $1 = mx + ny$ for $x, y \in \mathbf{Z}$ since $(m, n) = 1$. For all $a \in A$,

$$a = 1 \cdot a = (mx + ny)a = (mx)a + (ny)a.$$

We have $(ny)a \in A_m$ since $m((ny)a) = (mn)(ya) = |A|ya = 0$, and similarly $(mx)a \in A_n$. Thus $A = A_m + A_n$.

To show $A_m \cap A_n = \{0\}$, if $a \in A_m \cap A_n$ then $ma = 0$ and $na = 0$, so $a = (mx + ny)a = x(ma) + y(na) = 0 + 0 = 0$. Alternatively, the order of a divides m and n, so the order divides $(m, n) = 1$ and thus $a = 0$.

We have shown $A = A_m + A_n$ and $A_m \cap A_n = \{0\}$, so $A = A_m \oplus A_n$. □

Remark 3.2. Lemma 3.1 has a uniqueness aspect: $|A_m| = m$, $|A_n| = n$, and these are the unique subgroups of A with orders m and n. We will not need this.

Theorem 3.3. *An indecomposable finite abelian group has prime-power order.*

Proof. Let A be a nontrivial abelian group. We will prove the contrapositive of the theorem for A: if $|A|$ is not a prime power then A is decomposable.

Since $|A| > 1$ and $|A|$ is not a prime power, $|A|$ has more than one prime factor. Therefore the prime factorization of $|A|$ lets us write $|A| = mn$ where $(m, n) = 1$ and m and n are both greater than 1. For example, we can let m be the highest power of some prime dividing $|A|$ and let n be the complementary factor.

By Lemma 3.1, $A = A_m \oplus A_n$. The subgroups A_m and A_n are nontrivial by Cauchy's theorem: for a prime p dividing m, an element of A with order p lies in A_m, and a similar argument works for A_n. Note Cauchy's theorem can be proved in a direct way for abelian groups.[3] □

[2] In S_3, $\{g \in S_3 : g^2 = (1)\}$ is not a subgroup: it is $\{(1), (12), (13), (23)\}$.

[3] See https://kconrad.math.uconn.edu/blurbs/grouptheory/cauchypf.pdf.

To prove an indecomposable finite abelian p-group is cyclic, we'll use the following lemma.

Lemma 3.4. *A nontrivial finite abelian p-group with a unique subgroup of order p is cyclic.*

Proof. Let A be a finite abelian p-group with a unique subgroup of order p and let p^m be the largest order of the elements of A. Then $m \geq 1$ and each element of A has order p^j where $j \leq m$ (A is a p-group and p^m is the maximal order), so all elements of A have order dividing p^m: $p^m A = \{0\}$.

Let $a \in A$ have order p^m. Since $p^{m-1}a$ has order p, $\langle p^{m-1}a \rangle$ is a subgroup of order p, so it is the only one by assumption. To prove $A = \langle a \rangle$, we'll assume $A \neq \langle a \rangle$ and get a contradiction.

The quotient group $A/\langle a \rangle$ (this makes sense since A is abelian) is *nontrivial*, abelian, and of p-power order. By Cauchy's theorem, $A/\langle a \rangle$ has an element of order p, say $\overline{b}$. That means $b \notin \langle a \rangle$ and $pb \in \langle a \rangle$. So we can write

$$pb = ja$$

for some $j \in \mathbf{Z}$. Since $p^m b = 0$ (all elements of A have order dividing p^m) and $m \geq 1$,

$$0 = p^m b = p^{m-1}(pb) = p^{m-1}(ja) = (p^{m-1}j)a.$$

Since a has order p^m, $p^m \mid p^{m-1}j$, so $p \mid j$. Thus $j = pn$ for some $n \in \mathbf{Z}$, so $pb = (pn)a$. Rewrite that as $p(b - na) = 0$. The only subgroup of order p is in $\langle a \rangle$, so $b \in na + \langle a \rangle \subset \langle a \rangle$. This contradicts $b \notin \langle a \rangle$, so $A = \langle a \rangle$. □

Remark 3.5. Lemma 3.4 is true without assuming A is abelian when $p > 2$,[4] but the quaternion group Q_8 has a unique subgroup of order 2 and is not cyclic.

Theorem 3.6. *For each finite abelian p-group A, let a be an element of A with maximal order. Then $A = \langle a \rangle \oplus B$ for a subgroup B of A.*

Proof. We use induction on $|A|$. The cases $|A| = 1$ and $|A| = p$ are easy. Suppose $|A| > p$ and the theorem is true for all finite abelian p-groups of smaller order.

If A is cyclic then $A = \langle a \rangle = \langle a \rangle \oplus \{0\}$ since a has maximal order in A (each element of maximal order in a finite cyclic group generates the group). Now we may assume A is not cyclic. By Lemma 3.4, A has more than one subgroup of order p. In $\langle a \rangle$ there is only one subgroup of order p, so some $b \in A$ has order p and is not in $\langle a \rangle$. Thus $\langle a \rangle \cap \langle b \rangle = \{0\}$.

We will use the quotient group $A/\langle b \rangle$. Let p^m be the order of a, so $m \geq 1$. We'll show in $A/\langle b \rangle$ that $\overline{a}$ also has order p^m. From $p^m a = 0$ in A we get $p^m \overline{a} = \overline{0}$ in $A/\langle b \rangle$. If $p^{m-1}\overline{a} = \overline{0}$ then $p^{m-1}a \in \langle a \rangle \cap \langle b \rangle = \{0\}$, but $p^{m-1}a \neq 0$. So $p^{m-1}\overline{a} \neq \overline{0}$, which means $\overline{a}$ has order p^m.

As in the proof of Lemma 3.4, all elements of A have order dividing p^m, so $p^m A = \{0\}$. Therefore $p^m(A/\langle b \rangle) = \{\overline{0}\}$. Since $\overline{a}$ has order p^m, it has maximal order among the elements of $A/\langle b \rangle$. Since $1 < |A/\langle b \rangle| < |A|$, by induction $\langle \overline{a} \rangle$ is a direct summand of $A/\langle b \rangle$:

$$A/\langle b \rangle = \langle \overline{a} \rangle \oplus B/\langle b \rangle \tag{3.1}$$

where B is a subgroup of A containing $\langle b \rangle$ (all subgroups of $A/\langle b \rangle$ have the form $B/\langle b \rangle$ where $\langle b \rangle \subset B \subset A$). By (3.1), each element of A is congruent mod $\langle b \rangle$ to a multiple of a plus an element of B, so

$$A = \langle a \rangle + B + \langle b \rangle = \langle a \rangle + B,$$

where the last equation follows from $\langle b \rangle \subset B$. Since $\langle \overline{a} \rangle \cap (B/\langle b \rangle) = \{\overline{0}\}$ we get $\langle a \rangle \cap B \subset \langle b \rangle$, so $\langle a \rangle \cap B \subset \langle a \rangle \cap \langle b \rangle = \{0\}$. Thus $A = \langle a \rangle + B$ can be refined to $A = \langle a \rangle \oplus B$. □

[4] See Corollary 4.10 in https://kconrad.math.uconn.edu/blurbs/grouptheory/genquat.pdf.

Example 3.7. In $(\mathbf{Z}/(16))^\times$, the maximal order of the elements is 4. Two elements of order 4 are 3 and 5: $\langle 3\rangle = \{1,3,9,11\}$ and $\langle 5\rangle = \{1,5,9,13\}$. The elements of order 2 in $(\mathbf{Z}/(16))^\times$ are 7, 9, and 15. Since $\langle 7\rangle$ and $\langle 15\rangle = \langle -1\rangle$ intersect $\langle 3\rangle$ and $\langle 5\rangle$ trivially,

$$(\mathbf{Z}/(16))^\times = \langle 3\rangle \times \langle 7\rangle = \langle 3\rangle \times \langle -1\rangle \cong \mathbf{Z}/(4) \times \mathbf{Z}/(2)$$

and

$$(\mathbf{Z}/(16))^\times = \langle 5\rangle \times \langle 7\rangle = \langle 5\rangle \times \langle -1\rangle \cong \mathbf{Z}/(4) \times \mathbf{Z}/(2).$$

This shows for $a = 3$ and $a = 5$ that B in Theorem 3.6 need not be unique. A simpler example of that is $\mathbf{Z}/(p) \oplus \mathbf{Z}/(p)$ for prime p and $a = \binom{0}{1}$: the group is $\langle \binom{0}{1}\rangle \oplus \langle \binom{1}{b}\rangle$ for each $b \in \mathbf{Z}/(p)$, so p subgroups $\langle \binom{1}{b}\rangle$ (the lines $y = bx$) are complementary to $\langle \binom{0}{1}\rangle$ (the y-axis).

Corollary 3.8. *An indecomposable finite abelian p-group is cyclic.*

Proof. Let A be an indecomposable finite abelian p-group and $a \in A$ be an element of maximal order, so $a \neq 0$. By Theorem 3.6, $A = \langle a\rangle \oplus B$ for a subgroup B of A. Since A is indecomposable and $\langle a\rangle$ is nontrivial, $B = \{0\}$. Thus $A = \langle a\rangle$, which is cyclic. □

Now we put everything together to prove Theorem 1.1. The hard work was already done.

Proof. A nontrivial finite abelian group A is a direct sum of indecomposable subgroups by Theorem 2.5. The indecomposable finite abelian groups are the nontrivial cyclic p-groups (for varying p) by Example 2.3, Theorem 3.3, and Corollary 3.8, so A is a direct sum of cyclic p-groups. □

The splitting in Theorem 3.6 using a cyclic subgroup of maximal order in a finite abelian p-group works in all finite abelian groups A: for a maximal cyclic subgroup C, $A = C \oplus B$ for a subgroup B. This is proved in Section 5 of `https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf` and that leads to a proof that each finite abelian group is a direct sum of cyclic subgroups without relying on the case of finite abelian p-groups.

Example 3.9. In the group $(\mathbf{Z}/(100))^\times$, of order 40, the maximal order of its elements is 20. One element of order 20 is 3, and $(\mathbf{Z}/(100))^\times = \langle 3\rangle \times \langle -1\rangle$, which is a direct product of cyclic groups of order 20 and 2.

4. Comparing two indecomposable decompositions

Let A be a direct sum of nontrivial cyclic subgroups of prime-power order in two ways:

$$A = C_1 \oplus \cdots \oplus C_r = C_1' \oplus \cdots \oplus C_s'. \tag{4.1}$$

We want to show $r = s$ and, after relabeling, $C_i \cong C_i'$ for $i = 1, \ldots, r$.[5] This kind of relation between two direct sum decompositions of A is what we mean when we say A has a "unique" decomposition into indecomposable subgroups up to isomorphism. How is this proved?

First there is a useful reduction step. For a prime p, the subset of elements of A with p-power order form a subgroup of A (since A is abelian). In the direct sum of C_i's in (4.1), an element has p-power order if and only if it has component 0 in C_i whenever $|C_i|$ is *not* a power of p. That is, the elements of p-power order in A are the direct sum of subgroups C_i of p-power order. Therefore the equality between two direct sum decompositions in (4.1) implies, for each prime p, the equality (not merely isomorphism, but actual equality) of the direct sums of cyclic p-subgroups in both decompositions. So proving the uniqueness in (4.1) is reduced to the case that A has prime-power order.

[5] It is *not* true that we can literally have $C_i = C_i'$ (equality), as shown with the subgroups of order 2 in decompositions of $(\mathbf{Z}/(16))^\times$ in (1.1).

Theorem 4.1. *For a prime p, when a nontrivial finite abelian p-group is written in two ways as a direct sum of nontrivial cyclic subgroups, the number of direct summands of each p-power order is the same for both direct sums.*

Proof. Let A be a nontrivial finite abelian p-grpoup. If $A \cong \mathbf{Z}/(p^{e_1}) \oplus \mathbf{Z}/(p^{e_2}) \oplus \cdots \oplus \mathbf{Z}/(p^{e_r})$ for $e_i \in \mathbf{Z}^+$, we want to show $e_1, e_2, \ldots, e_r$ are determined by the group structure of A. The key idea is to look at the successive quotient groups

$$A/pA, \quad pA/p^2A, \quad p^2A/p^3A, \quad \ldots$$

and get information using these. We'll explain this by means of an example.

Suppose

$$A \cong \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p^3\mathbf{Z} \oplus \mathbf{Z}/p^4\mathbf{Z} \oplus \mathbf{Z}/p^4\mathbf{Z}. \tag{4.2}$$

Then

$$\begin{aligned} pA &\cong \{0\} \oplus \{0\} \oplus p\mathbf{Z}/p^3\mathbf{Z} \oplus p\mathbf{Z}/p^4\mathbf{Z} \oplus p\mathbf{Z}/p^4\mathbf{Z}, \\ p^2A &\cong \{0\} \oplus \{0\} \oplus p^2\mathbf{Z}/p^3\mathbf{Z} \oplus p^2\mathbf{Z}/p^4\mathbf{Z} \oplus p^2\mathbf{Z}/p^4\mathbf{Z}, \\ p^3A &\cong \{0\} \oplus \{0\} \oplus \{0\} \oplus p^3\mathbf{Z}/p^4\mathbf{Z} \oplus p^3\mathbf{Z}/p^4\mathbf{Z}, \\ p^4A &= 0. \end{aligned}$$

The direct sums on the right side are all compatible, *e.g.*, the fourth direct summand each time is a subgroup of the first $\mathbf{Z}/p^4\mathbf{Z}$ in the direct sum decomposition of A. To compute the successive quotients $p^iA/p^{i+1}A$ up to isomorphism, note $(p^i\mathbf{Z}/p^j\mathbf{Z})/(p^{i+1}\mathbf{Z}/p^j\mathbf{Z})$ is cyclic of order p when $j \geq i+1$, so

$$\begin{aligned} A/pA &\cong (\mathbf{Z}/p\mathbf{Z})^5, \\ pA/p^2A &\cong (\mathbf{Z}/p\mathbf{Z})^3, \\ p^2A/p^3A &\cong (\mathbf{Z}/p\mathbf{Z})^3, \\ p^3A/p^4A &\cong (\mathbf{Z}/p\mathbf{Z})^2, \\ p^4A/p^5A &= 0. \end{aligned}$$

Each $p^iA/p^{i+1}A$ is isomorphic to a direct sum of some number of copies of $\mathbf{Z}/p\mathbf{Z}$, so all that really matters is its size: set $|p^iA/p^{i+1}A| = p^{d_i}$, so $(d_0, d_1, d_2, d_3, d_4) = (5, 3, 3, 2, 0)$ in (4.2).

A cyclic direct summand of order p^e contributes to $p^iA/p^{i+1}A$ until $i \geq e$. It is the differences $d_{i-1} - d_i$ for $i \geq 1$, rather than the individual d_i's, that provide the most directly relevant information: the number of cyclic direct summands of order p^i is $d_{i-1} - d_i$. In (4.2), for instance,

- $d_0 - d_1 = 5 - 3 = 2$ and there are 2 summands in (4.2) that are cyclic of order p,
- $d_1 - d_2 = 0$ and there are 0 summands in (4.2) that are cyclic of order p^2,
- $d_2 - d_3 = 3 - 2 = 1$ and there is 1 summand in (4.2) that is cyclic of order p^3,
- $d_3 - d_4 = 2 - 0 = 2$ and there are 2 summands in (4.2) that are cyclic of order p^4.

We can access this information using the individual d_i's too: d_0 is the number of nonzero cyclic summands (note $d_0 = 5$ in (4.2)) and in general d_i is the number of cyclic summands of *order at least* p^{i+1}. The largest i such that $d_i \neq 0$ tells us the largest summand in A has order p^{i+1}. For (4.2), $d_3 \neq 0$ and $d_i = 0$ for $i \geq 4$.

It is left to the reader to show this approach to recovering the number of cyclic summands in (4.2) from the group structure of A works in the general case. □

If A is a finite abelian p-group of order p^n then $A \cong \mathbf{Z}/(p^{n_1}) \oplus \mathbf{Z}/(p^{n_2}) \oplus \cdots \oplus \mathbf{Z}/(p^{n_k})$ with $n_1 + \cdots + n_k = n$, and A is determined up to isomorphism by the exponents $n_1, \ldots, n_k$

(ignoring their order). Therefore the number of abelian groups of order p^n, up to isomorphism, equals the number of ways of writing n as a sum of positive integers (ignoring their order). For example, the different ways of writing 2, 3, and 4 as a sum of positive integers (in increasing order) is

$$2 = 1+1, \quad 3 = 1+2 = 1+1+1, \quad 4 = 1+3 = 2+2 = 1+1+2 = 1+1+1+1,$$

so the abelian groups of order p^2, p^3, and p^4 are

- $\mathbf{Z}/(p^2)$ and $(\mathbf{Z}/(p))^2$,
- $\mathbf{Z}/(p^3)$, $\mathbf{Z}/(p) \oplus \mathbf{Z}/(p^2)$, and $(\mathbf{Z}/(p))^3$,
- $\mathbf{Z}/(p^4)$, $\mathbf{Z}/(p) \oplus \mathbf{Z}/(p^3)$, $(\mathbf{Z}/(p^2))^2$, $(\mathbf{Z}/(p))^2 \oplus \mathbf{Z}/(p^2)$, and $(\mathbf{Z}/(p))^4$.

It's natural to ask how much of this carries over to nonabelian finite groups. We can define decomposable and indecomposable finite groups using direct product decompositions (require the subgroups to be normal!). Theorem 2.5 extends easily to all nontrivial finite groups. But in contrast to the abelian case, where indecomposable groups can be described in a second way (they are the nontrivial cyclic p-groups), there isn't a good description of general indecomposable finite groups besides their definition. Simple groups are indecomposable (they have no nontrivial normal subgroups), but many non-simple groups are also indecomposable.[6] For example, S_n is indecomposable for $n \geq 2$ but it is not simple when $n \geq 3$: the only nontrivial normal subgroup of S_n is A_n, so we can't write $S_n = A_n \times H$ for a subgroup H (necessarily normal of order 2).

There is a uniqueness for indecomposable decompositions of a finite group G: if

$$G = H_1 \times \cdots \times H_r = K_1 \times \cdots \times K_s$$

where H_i and K_j are indecomposable subgroups of G, then $r = s$ and, after relabeling, $H_i \cong K_i$ for $i = 1, \ldots, r$. This is a special case of the Krull–Remak–Schmidt theorem. While the decomposition of finite abelian groups into a direct product of cyclic subgroups is very useful in applications of such groups, the decomposition of finite nonabelian groups into a direct product of indecomposable (normal) subgroups is not that useful in practice.

Appendix A. Fitting's Lemma

In this appendix we provide another approach to Theorem 3.3. It is based on the next result, called Fitting's lemma after Hans Fitting (not because the result is "fitting" to be used in mathematics).

Lemma A.1 (Fitting)**.** *Let A be a finite abelian group and $f\colon A \to A$ be a homomorphism. For sufficiently large k, $A = \operatorname{im}(f^k) \oplus \ker(f^k)$.*

This result, which is surprising when you first meet it, shows that each *homomorphism* of an abelian group A to itself leads to a *direct sum decomposition* of A if you iterate the homomorphism enough times. This is best appreciated by seeing how it looks in some examples.

- Consider $A = \mathbf{Z}/(12)$ (the additive group mod 12, not units mod 12 under multiplication!) and $f(a) = 2a$. We have $\operatorname{im}(f) = \{0, 2, 4, 6, 8, 10\} = \langle 2 \rangle$ and $\ker(f) = \{0, 6\} = \langle 6 \rangle$. These subgroups intersect nontrivially (the kernel is inside the image). Since $f^2(a) = 4a$, we have $\operatorname{im}(f^2) = \{0, 4, 8\} = \langle 4 \rangle$ and $\ker(f^2) = \{0, 3, 6, 9\} = \langle 3 \rangle$. Compared to the image and kernel of f, the image of f^2 is smaller and the kernel of f^2 is larger, and their intersection is trivial. We have a direct sum decomposition
$$A = \langle 4 \rangle \oplus \langle 3 \rangle = \operatorname{im}(f^2) \oplus \ker(f^2).$$

[6] We already saw this for abelian groups: $\mathbf{Z}/(p^k)$ is indecomposable for $k \geq 1$ but simple only for $k = 1$.

- Consider $A = \mathbf{Z}/(12)$ and $f(a) = 6a$. Then $\mathrm{im}(f) = \{0, 6\} = \langle 6\rangle$ and $\ker(f) = \{0, 2, 4, 6, 8\} = \langle 2\rangle$, while $f^2(a) = 36a = 0$ so $\mathrm{im}(f^2) = \{0\}$ and $\ker(f^2) = A$. Thus $A = \mathrm{im}(f^2) \oplus \ker(f^2)$.
- The decomposition in Lemma 3.1 fits Fitting's lemma: when $|A| = mn$ with $(m, n) = 1$, $A = A_m \oplus A_n$ and $A_m = \mathrm{im}(f)$ while $A_n = \ker(f)$ where $f(a) = na$.

Proof. Iterates of f are homomorphisms $A \to A$. Since $f^{k+1}(a) = f^k(f(a))$, $\mathrm{im}(f^{k+1}) \subset \mathrm{im}(f^k)$ and $f^k(a) = 0 \Rightarrow f^{k+1}(a) = f(f^k(a)) = f(0) = 0$, so $\ker(f^k) \subset \ker(f^{k+1})$. That means

$$\mathrm{im}(f) \supset \mathrm{im}(f^2) \supset \mathrm{im}(f^3) \supset \cdots, \qquad \ker(f) \subset \ker(f^2) \subset \ker(f^3) \subset \cdots,$$

and since A is finite these containments have to stabilize: for some $k \geq 1$, $\mathrm{im}(f^k) = \mathrm{im}(f^\ell)$ and $\ker(f^k) = \ker(f^\ell)$ for all $\ell > k$. We'll show for such k that $A = \mathrm{im}(f^k) \oplus \ker(f^k)$.

Step 1: $A = \mathrm{im}(f^k) + \ker(f^k)$.

For $a \in A$, $f^k(a) = f^{2k}(a')$ for some a' since $\mathrm{im}(f^k) = \mathrm{im}(f^{2k})$. Thus $f^k(a) = f^k(f^k(a'))$, so $f^k(a - f^k(a')) = 0$. Set $b = a - f^k(a')$, so $b \in \ker(f^k)$. The equation $a = f^k(a') + b$ shows $A = \mathrm{im}(f^k) + \ker(f^k)$.

Step 2: $\mathrm{im}(f^k) \cap \ker(f^k) = \{0\}$.

Suppose $a = f^k(c)$ for some $c \in A$ and $f^k(a) = 0$. Then $0 = f^k(a) = f^k(f^k(c)) = f^{2k}(c)$, so $c \in \ker(f^{2k}) = \ker(f^k)$, which implies $a = f^k(c) = 0$. □

Remark A.2. A seemingly weaker notion of stabilization for images and kernels is $\mathrm{im}(f^k) = \mathrm{im}(f^{k+1})$ and $\ker(f^k) = \ker(f^{k+1})$ for some $k \geq 1$, not equality from the kth point onwards. This actually implies stabilization for all higher iterates of f: if $\mathrm{im}(f^k) = \mathrm{im}(f^{k+1})$ for some k then $\mathrm{im}(f^k) = \mathrm{im}(f^\ell)$ for all $\ell > k$, and similarly for the kernels. Therefore $A = \mathrm{im}(f^k) \oplus \ker(f^k)$ when f^k and f^{k+1} have the same image and kernel. This is a more practical condition to check in order to apply Fitting's lemma.

Theorem A.3. *An indecomposable finite abelian group has prime-power order.*

Proof. Let A be an indecomposable finite abelian group. Since $|A| > 1$, $|A|$ has a prime factor, say p. Let $f\colon A \to A$ by $f(a) = pa$. then $f^k(a) = p^k a$ for each $k \geq 1$. By Cauchy's theorem, A has an element of order p, so $\ker(f) \neq \{0\}$.

By Fitting's lemma, $A = \mathrm{im}(f^k) \oplus \ker(f^k)$ for some $k \geq 1$. Since A is indecomposable, $\mathrm{im}(f^k)$ or $\ker(f^k)$ is $\{0\}$. Since $\ker(f) \subset \ker(f^k)$ and $\ker(f) \neq \{0\}$, $\ker(f^k)$ is not $\{0\}$. Therefore $\mathrm{im}(f^k) = \{0\}$, so $p^k A = \{0\}$: all elements of A are killed by multiplication by p^k, so the order of each element of A is a power of p. Thus A has p-power order. □