Classifying Finite Abelian Groups

A long time ago, we proved the following.

Proposition. *Any **finite cyclic** group of order n is isomorphic to $\mathbb{Z}_n$.*

It is time to prove a similar classification theorem for **finite abelian** groups!

Classification of Finite Abelian Groups

Theorem [Classification of Finite Abelian Groups]. *Every finite abelian group is isomorphic to a direct product of cyclic groups of the form*[1]

$$\mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}}$$

where the p_i are (not necessarily distinct) prime numbers.

Example. The following groups are the only possibilities with order $\mathbf{200} = \mathbf{8} \cdot \mathbf{25} = \mathbf{2^3} \cdot \mathbf{5^2}$

- $\mathbb{Z}_8 \times \mathbb{Z}_{25}$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$
- $\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
- $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

Note that these groups split into parts coming from the $\mathbf{8 = 2^3}$ factor and from the $\mathbf{25 = 5^2}$ factor.

Definition. A ***p*-group** is a group where every element has order equal to a power of a fixed prime.

We may incorporate the prime into the name (e.g. "5-group" to mean "p-group at the prime $p = 5$").

Example. The subgroups $\mathbb{Z}_8$ and $\mathbb{Z}_4 \times \mathbb{Z}_2$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ above are all p-groups at the prime $\boldsymbol{p = 2}$. The subgroups $\mathbb{Z}_{25}$ and $\mathbb{Z}_5 \times \mathbb{Z}_5$ above are both **5**-groups.

We can use this to identify groups, given a bit of information about their elements.

Proposition. *If $k < n$ then $\mathbb{Z}_{p^n}$ has exactly $p^k - p^{k-1}$ elements of order p^k.*

Proof. There are p^k elements with $x^{(p^k)} = e$, of which p^{k-1} have $x^{(p^{k-1})} = e$. □

Example. If a group of order 200 has only one element of order 2 and four of order 5, then it is $\mathbb{Z}_8 \times \mathbb{Z}_{25}$.

Proposition. $\underbrace{\mathbb{Z}_{p^n} \times \cdots \times \mathbb{Z}_{p^n}}_{k}$ *has exactly $(p^k - 1)$ elements of order p.*

Proof. The subgroup $H = \{x \in \mathbb{Z}_{p^n} \mid x^p = e\}$ has p elements. So $H \times \cdots \times H$ has p^k elements. Of these $(e, e, \ldots, e)$ has order 1 and all others have order p. □

Example. If a group of order 200 has at least two elements of order 2, at least one element of order 4, and at least five elements of order 5 then the group is $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$.

The classification theorem for finite abelian groups says that groups split into products of p-groups, and p-groups themselves split further into products of p^k-cycles.

The main clever idea we will use over and over is to choose a sneaky group homomorphism $\phi : G \to H$ so that applying the 1st Isomorphism Theorem yields $|G| = |\operatorname{Im}\phi| \cdot |\operatorname{Ker}\phi|$, splitting the order of $|G|$ into a "good" part and a "bad" part. We use the proposition below to identify products.

[1] Some people will write direct sum ⊕ instead of product ×... for groups these differ only in how they treat infinite collections. Probably ⊕ is more appropriate for abelian groups, but our textbook uses ×.

Proposition. *If G is an abelian group with $H, K < G$ such that $H \cap K = \{e\}$, then $HK \cong H \times K$.*

Proof. Suppose $H, K < G$ abelian with $H \cap K = \{e\}$. In this case the map $\phi : H \times K \to HK$ by $\phi(h,k) = hk$ is a homomorphism because $\phi(h_1,k_1)\,\phi(h_2,k_2) = h_1k_1\,h_2k_2 = h_1h_2\,k_1k_2 = \phi(h_1h_2,\,k_1k_2)$. Surjectivity is clear. For injectivity, note that if $hk = \phi(h,k) = e$, then $h = k^{-1} \in H \cap K = \{e\}$; so $h = k^{-1} = e$. □

The first step is the following weak version[2] of Cauchy's theorem (previously proved for cyclic groups). This proposition is useful because it allows us to convert between orders of elements and orders of groups.

Proposition. *A finite abelian group G contains an element of order p for each prime divisor of $|G|$.*

Proof by strong induction on $|G|$. If $|G| = 1, 2, 3$ then the statement is already known.

Suppose that the statement is true for all groups of order $k < |G|$. Pick a prime divisor p of $|G|$ and a nontrivial element $a \in G$. Since $|G|$ is finite, a has finite order $a^n = e$. If p divides n, then $a^{(n/p)}$ has order p and we are done.

Otherwise p and n are relatively prime. Consider the projection $\phi : G \to G/\langle a\rangle$ (since G is abelian, all subgroups are normal; so we can make this quotient). By the first isomorphism theorem, $|G| = \big|\,G/\langle a\rangle\big| \cdot \big|\langle a\rangle\big|$. We know p divides $|G|$ but is relatively prime to $\big|\langle a\rangle\big| = n$; so p divides $\big|\,G/\langle a\rangle\big|$. But if p divides order of $G/\langle a\rangle$ and this order is less than $|G|$, then the induction hypothesis implies that $G/\langle a\rangle$ has an element $[b]$ of order p. The quotient maps is a homomorphism, so $\big|[b]\big| = p$ divides $|b| = m$. Then $b^{(m/p)}$ is our desired element of order p. □

Corollary. *A finite abelian group is a p-group if and only if its order is a power of a prime p.*

Using this, we can show that abelian groups split into products of p-groups.

Proposition. *Any abelian group with order $|G| = d\,p^n$ with p prime and d, p relatively prime, is a direct product $G \cong D \times P$ where $|D| = d$ and $|P| = p^n$.*

Proof. If G is abelian, then the map $\phi : G \to G$ by $\phi(g) = g^{(p^n)}$ is a homomorphism. Combining the 1st Isomorphism Theorem and the product formula we have

$$d\,p^n \;=\; |G| \;=\; |\operatorname{Im}\phi| \cdot |\operatorname{Ker}\phi| \;=\; |\operatorname{Im}\phi \cap \operatorname{Ker}\phi| \cdot |\operatorname{Im}\phi \cdot \operatorname{Ker}\phi|$$

By construction, $\operatorname{Ker}\phi$ is all elements of G whose order is a power of p. So the previous proposition implies that $|\operatorname{Ker}\phi| = p^n$ and $|\operatorname{Im}\phi| = d$. Thus $|\operatorname{Im}\phi \cap \operatorname{Ker}\phi| = 1$ because any $x \in \operatorname{Im}\phi \cap \operatorname{Ker}\phi$ must have order dividing both d and p^n which are relatively prime. Therefore $|G| = |\operatorname{Im}\phi \cdot \operatorname{Ker}\phi|$ which implies $G = \operatorname{Im}\phi \cdot \operatorname{Ker}\phi$.

Since G is abelian and $\operatorname{Im}\phi \cap \operatorname{Ker}\phi = \{e\}$, we have $\operatorname{Im}\phi \cdot \operatorname{Ker}\phi \cong \operatorname{Im}\phi \times \operatorname{Ker}\phi$. □

Corollary. *Finite abelian groups are isomorphic to products of p-groups.*

Proof. Use the previous proposition to split off primes, one at a time. □

It remains to show only that p-groups split into products of cyclic factors. We begin with an elementary, warm-up version. (We're not going to need this, but it is fun and easy.)

Definition. An abelian p-group is **elementary** if all nontrivial elements have order p.

Proposition. *Finite elementary abelian p-groups are isomorphic to direct products $P \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.*

[2] Cauchy's Theorem says that this is true for **all** finite groups, not just finite **abelian** groups.

Proof. Pick $x_1 \neq e$ in P. If P is an elementary p-group then x_1 has order p.

Let $H_1 = \langle x_1 \rangle$ and pick $x_2 \neq e$ in $P \setminus H_1$. Note that $\langle x_2 \rangle \cap H_1 = \{e\}$ because prime orders of x_1 and x_2 imply that any nontrivial elements are generators for their entire cyclic subgroups; so $\langle x_1 \rangle$ and $\langle x_2 \rangle$ are either equal or intersect only at $\{e\}$.

Let H_2 be the product subgroup $H_2 = \langle x_1 \rangle \cdot \langle x_2 \rangle$ and pick $x_3 \neq e$ in $P \setminus H_2$. Note that $\langle x_3 \rangle \cap H_2 = \{e\}$ because if $e \neq y \in \langle x_3 \rangle \cap H_2$, then $\langle y \rangle < \langle x_3 \rangle$ which implies $\langle y \rangle = \langle x_3 \rangle$ due to prime orders. But then $\langle y \rangle < H_2$ would imply $x_3 \in H_2$.

Let H_3 be the product subgroup $H_3 = \langle x_1 \rangle \cdot \langle x_2 \rangle \cdot \langle x_3 \rangle$ and continue until $H_k = P$.

Because all intersections were trivial, $P \;\cong\; \langle x_1 \rangle \times \cdots \times \langle x_k \rangle \;\cong\; \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$. □

The general proof (splitting cyclic factors out of general p-groups) is similar to this, but much messier!

Proposition. *If $x \in P$ is a maximal order element in an abelian p-group, then $P \cong \langle x \rangle \times K$, where $K < P$.*

The most difficult part of this proof involves showing existence of a nontrivial element $y \in P$ with $\langle x \rangle \cap \langle y \rangle = \{e\}$ (assuming $P \neq \langle x \rangle$). We give a proof assuming this *technical step* has been completed.

Proof after finding y. If $|P| = p$ then $P \cong \langle x \rangle$ and we are done. Proceed by strong induction. Suppose that the statement holds for all p-groups with order $< |P|$.

If $P = \langle x \rangle$ then we are done. Otherwise we will use $y \in P$ with $\langle x \rangle \cap \langle y \rangle = \{e\}$ (constructed later). Consider the quotient $q : P \to P/\langle y \rangle$. The quotient is also a p-group; and $[x] \in P/\langle y \rangle$ has the same order as x, because $\langle x \rangle$ intersects $\operatorname{Ker} q = \langle y \rangle$ trivially.

By the induction hypotheses, $P/\langle y \rangle$ splits as $P/\langle y \rangle = \big\langle [x] \big\rangle \times \overline{K}$ where $\overline{K} < P/\langle y \rangle$. From the Correspondence Theorem, the pullback $K = q^{-1}\overline{K}$ is a subgroup $\langle y \rangle < K < P$.

To show $\langle x \rangle \cap K = \{e\}$, note that $\langle x \rangle \cap \operatorname{Ker} q = \{e\}$ and $\langle [x] \rangle \cap \overline{K} = \{e\}$. So $(\langle x \rangle \cap K)/\{e\} \cong \{e\}$.

To show $\langle x \rangle \cdot K = P$, count orders, applying the 1st Isomorphism Theorem and the Product Formula.

$$\big|\langle x \rangle \cdot K\big| \;=\; \big|\langle x \rangle\big| \cdot \big|K\big| \;=\; \Big|\big\langle [x] \big\rangle\Big| \cdot \big|\overline{K}\big| \cdot \big|\langle y \rangle\big| \;=\; \Big|\big\langle [x] \big\rangle \cdot \overline{K}\Big| \cdot \big|\langle y \rangle\big| \;=\; \big|P/\langle y \rangle\big| \cdot \big|\langle y \rangle\big| \;=\; \big|P\big|.$$ □

Corollary. *Finite abelian p-groups are isomorphic to products of cyclic groups $\mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \mathbb{Z}_{p^{n_r}}$ (where the n_i are not necessarily distinct).*

Proof. Use the previous proposition to split off cyclic generators, one at a time. □

It remains to complete the *technical step* of finding y.

Lemma [Technical step]. *If $x \in P$ is a* ***maximal order*** *element in an abelian p-group with $P \neq \langle x \rangle$, then there is $y \in P$ with $\langle x \rangle \cap \langle y \rangle = \{e\}$.*

Proof. It is enough to find $y \notin \langle x \rangle$ of order p. Then any nontrivial element in $\langle x \rangle \cap \langle y \rangle$ would generate all of $\langle y \rangle$, forcing $y \in \langle x \rangle$. Since we choose $y \notin \langle x \rangle$ the intersection must be trivial.

Choose nontrivial $y \notin \langle x \rangle$ of **minimum order** and consider $\langle x \rangle \cap \langle y \rangle$. Because P is a p-group, all elements have order equal to a power of p. If y has order p then we are done. If not, then $y^p \in \langle x \rangle$; because otherwise y^p would have lower order than y with $y^p \notin \langle x \rangle$, contradicting the choice of y.

In this case $y^p = x^m$ for some power m. We will show that p must divide m and use $x^{(m/p)}$ to make a nontrivial element $z = x^{(m/p)}y^{-1}$ of order p. Since $z \notin \langle x \rangle$ our choice of y means it must be order p as well.

To show that p divides m, we will investigate the order of x^m. If x has maximal order p^n then all elements have order $\leq p^n$; in particular

$$e \;=\; y^{p^n} \;=\; (y^p)^{p^{n-1}} \;=\; (x^m)^{p^{n-1}} \;=\; x^{(m\,p^{n-1})}$$

Since x has order p^n, this means p divides m, which completes the proof. □

Following are some sections with other ideas that I messed about with while trying to develop a better proof for the final part of the structure theorem. In the end, I couldn't beat the textbook's proof. Though I could at least give a better explanation for it.

Generating Sets and Rank

We liked to understand cyclic groups by talking about their generators. Finite abelian groups are built from multiple cyclic groups, so they require multiple "generators".

Definition. The subgroup $\langle S\rangle < G$ **generated by** subset $S \subset G$ is the smallest subgroup containing S.
A subset **generates a group** if $\langle S\rangle = G$.
If G is generated by a finite subset S, then G is **finitely generated** (or finite rank).[3]

Proposition. $\langle S\rangle = \bigcap\limits_{\substack{\text{subgroups } H\\ \text{with } S\subset H}} H$

Proposition. $\langle S\rangle = \big\{\textit{finite products in } G \textit{ using elements of } S \textit{ and their inverses}\big\}$

This extends the notion (and notation) of cyclic group generators. For example in $\mathbb{Z}$, we have $\langle 2\rangle = 2\mathbb{Z}$ in both senses.

Example. All groups are generated by themselves $\langle G\rangle = G$.

That example was silly, because the whole point of generating sets is to find SMALL sets of generators.

Definition. The **rank** of a group, $\operatorname{rank}(G)$, is the minimal number of elements required to generate it.

Example. In $\mathbb{Z}$, we have $\langle 2,3\rangle = \mathbb{Z} = \langle 1\rangle$, and $\langle 4,6\rangle = 2\mathbb{Z} = \langle 2\rangle$.
In general, $\langle m,n\rangle = \big\langle \gcd(m,n)\big\rangle$ in $\mathbb{Z}$. Cyclic groups like $\mathbb{Z}$ and its subgroups are all rank 1 (by definition).

Example. The group $\mathbb{Z}_2\times\mathbb{Z}_2$ is generated by $(1,0)$ and $(0,1)$. The rank of $\mathbb{Z}_2\times\mathbb{Z}_2$ is 2.
In general, if $G = \langle S\rangle$ and $H = \langle T\rangle$ then $G\times H = \big\langle (S\times e)\ \cup\ (e\times T)\big\rangle$.

Example. Sometimes we can do better than this! The group $\mathbb{Z}_2\times\mathbb{Z}_3$ is generated by $(1,0)$ and $(0,1)$.
But we previously showed this group is cyclic and is in fact generated by the degree 6 element $(1,1)$.

Remark. It is **not** true that if $H < G$, then $\operatorname{rank}(H) \le \operatorname{rank}(G)$! For example, S_6 has rank 2 (generated by $(1\ 2)$ and $(1\ 2\ 3\ 4\ 5\ 6)$. But its subgroup $\big\langle (1\ 2),\ (3\ 4),\ (5\ 6)\big\rangle$ is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ of rank 3.

We will **not** prove the following statement from combinatorial group theory.

Theorem [Schreier's ineq.]. *If $H < G$ has index $[G:H] = n$ then $\big(\operatorname{rank}(H)-1\big) \le n\big(\operatorname{rank}(G)-1\big)$.*

But we can easily prove some statements about how rank interacts with homomorphisms.

Proposition. *If $\phi : G \to H$ is a homomorphism, then*

$$\operatorname{rank}\big(\operatorname{Im}\phi\big) \ \le\ \operatorname{rank}\big(G\big) \ \le\ \operatorname{rank}\big(\operatorname{Im}\phi\big) \ +\ \operatorname{rank}\big(\operatorname{Ker}\phi\big).$$

Corollary. *If $N \lhd G$ then* $\operatorname{rank}\big(G/N\big) \ \le\ \operatorname{rank}\big(G\big) \ \le\ \operatorname{rank}\big(G/N\big) \ +\ \operatorname{rank}\big(N\big)$.

Remark (On notions of finiteness)**.** We now have multiple senses in which a group could be "finite".

[3] The additive group $\mathbb{Z}$ is inifinite, but finitely generated since $\mathbb{Z} = \langle 1\rangle$.
The additive groups $\mathbb{Q}$ and $\mathbb{R}$ are both infinite rank.

- A group could have finitely many elements $|G| = n$.
- A group could be finitely generated $G = \langle S \rangle$ where $|S| = n$.
- A group could have elements of bounded order $|g| \leq n$ for some n. This is called "finite exponent."

Torsion Filtration

We leverage our understanding of elementary groups by building general p-groups using elementary parts. "Filter" p-groups into "layers" by orders of elements; where the "difference between" layers is elementary.

Definition. Given a p-group G, define the $\boldsymbol{p^k}$**-torsion** subgroup to be $\Omega_k(G) = \{g \in G \mid g^{(p^k)} = e\}$.

These filter G into an ascending series of subgroups called the $\boldsymbol{p}$**-torsion series** (or "Omega series")

$$\Omega_1(G) \;<\; \Omega_2(G) \;<\; \cdots \;<\; \Omega_k(G) \;<\; \cdots \;<\; G$$

Remark. For abelian p-groups this is "dual" to the $\boldsymbol{p}$**-power series** for G (a descending series of subgroups)

$$G \quad > \quad G^p \quad > \quad G^{p^2} \quad > \cdots > \quad G^{p^k} \quad > \cdots$$

The p^k-power homomorphism for abelian groups $\phi_k(g) = g^{(p^k)}$ has $\operatorname{Ker}\phi_k = \Omega_k(G)$ and $\operatorname{Im}\phi_k = G^{p^k}$; so the 1st Isomorphism Theorem says $G/\Omega_k(G) \;\cong\; G^{p^k}$. This further implies that $\left[G : G^{p^k}\right] = \left|\Omega_k(G)\right|$.

The p-torsion filtration isolates the elements that *die quickly* under p-powers. Each step upwards adds new elements that require one more power of p to vanish. So $\Omega_1(G)$ are the "fragile" elements that vanish after a single p, $\Omega_2(G)$ contains some slightly more substantial elements, etc. By construction, $\Omega_1(G)$ is the largest elementary subgroup of G, and successive quotients $\Omega_k(G)/\Omega_{k-1}(G)$ are all elementary.[4]

Quotienting by p-torsion groups drops orders of elements!

Lemma [Order drop]. *If G is a abelian and $g \in G$ has order p^n, then $[g] \in G/\Omega_k(G)$ has order p^{n-k} (assuming $k \leq n$).*

Proof. Note that if $k \leq n$ then by the 1st Isomorphism Theorem, $G/\Omega_k(G) \cong G^{p^k}$. Thus $[g] \in G/\Omega_k(G)$ corresponds to $g^{(p^k)} \in G^{p^k}$ which has $\left(g^{(p^k)}\right)^{(p^{n-k})} = g^{(p^n)} = e$. □

The power map traverses the p-torsion series in the reverse direction!

Lemma [Power reverse]. *If G is an abelian p-group, then $\phi_1 : \Omega_{k+1}(G) \to \Omega_k(G)$ by $\phi_1(g) = g^p$ is a homomorphism with $\operatorname{Ker}\phi_1 = \Omega_1(G)$ and $\operatorname{Im}\phi_1 = \Omega_k(G) \cap G^p$.*

Proof. Note that $x \in \Omega_{k+1}(G)$ if and only if $x^{(p^{k+1})} = e$. Then $\phi_1(x) = x^p$ satisfies $(x^p)^{(p^k)} = x^{(p^{k+1})} = e$; so $\phi_1(x) = x^p \in \Omega_k(G)$. Thus ϕ_1 has the indicated target and is a homomorphism because G is abelian.

For the kernel, note that $x \in \operatorname{Ker}\phi_1$ if and only if $x^p = e$ So $\operatorname{Ker}\phi_1 = \Omega_1(G) < \Omega_{k+1}(G)$.

For the image, note that $\operatorname{Im}\phi_1 = \left(\Omega_{k+1}(G)\right)^p$. Thus $\operatorname{Im}\phi_1 \subset \Omega_k(G) \cap G^p$ immediately. In the other direction, if $y \in \Omega_k(G) \cap G^p$, then $y^{(p^k)} = e$ and also $y = x^p$ for some $x \in G$. Thus $x^{(p^{k+1})} = \left(x^{(p^k)}\right)^p = e$; so $x \in \Omega_{k+1}(G)$ and $y \in \left(\Omega_{k+1}(G)\right)^p$. □

[4] In many areas of mathematics, we consider similar "filtrations" or "towers" of objects. We think of them analogous to power series in calculus, which approximate functions by adding increasingly higher power terms. Successive quotients Ω_k/Ω_{k-1} are like the homogeneous terms $\frac{f^{(n)}(a)}{n!}\,(x-a)^n$ added at each step of the power series computation.

Interesting Additional Lemmas

The (unused) lemmas below might be good homework problems (for an earlier section).

Lemma [Orders pull back]. *If $N \lhd G$ and ${}^{G}\!/_{N}$ has an element of order n, then G also has an element of order n.*

Proof. Suppose $[g] \in {}^{G}\!/_{N}$ has order n. If g has order k in G, then $g^k = e$; so in particular $[g]^k = [g^k] = [e]$. Since $\big\langle [g] \big\rangle$ is cyclic, this implies k is a multiple of n □