Algebraic Structures:
Finite abelian groups.*

Finite abelian groups are products of cyclic groups

The simplest abelian groups are the cyclic groups. Not all groups are cyclic though. For example, the group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is not cyclic; its order is 4, but its every element satisfies $2x = 0$.

It turns out that the group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is about as complicated as *finite* abelian can ever be. Specifically, we shall show that every finite group is isomorphic to a product of cyclic groups. The finiteness assumption is crucial: there are infinite groups that are not isomorphic to a product of cyclic groups. The most familiar example is $\mathbb{Q}$. We can see that it is not a product of cyclic groups because $\mathbb{Q}$ is *divisible*, which means that for every $x \in \mathbb{Q}$ and every positive integer n there is y such that $ny = x$. On the other hand, a product of indivisible groups is easily seen to be indivisible, and cyclic groups are indivisible.

Theorem 1. *Every finite abelian group is isomorphic to a product of cyclic groups.*

The proof consists of two steps. The first step is the reduction to the case of p-groups.

Lemma 2. *Suppose G is a finite abelian group, and $P_1, P_2, \ldots, P_k$ are its Sylow subgroups (for various primes) Then $G \cong P_1 \times \cdots \times P_k$.*

Proof. Since G is abelian, its subgroups are normal, and so there is just one Sylow p-subgroup for each prime p. Let $|G| = p_1^{t_1} \cdots p_k^{t_k}$ be the prime factorization of $|G|$. Without loss of generality, P_i is a Sylow p_i-subgroup of G, i.e., $|G_i| = p_i^{t_i}$.

We claim that, for each i, the set $G_i \stackrel{\text{def}}{=} P_1 P_2 \ldots P_i$ is a subgroup of G and $G_i \cong P_1 \times \cdots \times P_i$. The proof is by induction. Since the case $i = 1$ is trivial, assume that $i > 1$. Since the orders of G_{i-1} and P_i are coprime (by the induction hypothesis), it follows that $G_{i-1} \cap P_i = 1$. Since P_i is normal in G, the set $G_{i-1}P_i$ is actually a subgroup of G. Furthermore, since both P_i an G_{i-1} are normal in G, we in fact have $G_i = G_{i-1}P_i \cong G_i \times P_i$, completing the induction step. □

The second step, which is more difficult, is to show that abelian p-groups are isomorphic to a product of cyclic groups. This relies on the following lemma.

Lemma 3. *Suppose G is a finite abelian p-group and $a \in G$ is the element of the largest order in G. Then there is a subgroup H of G such that $\langle a \rangle \cap H = 0$ and $\langle a \rangle + H = G$.*

Proof. Let the order of a be $|a| = p^n$. The assumption on a implies that

$$p^n x = 0 \text{ for every } x \in G. \tag{1}$$

Let H be a largest subgroup of G satisfying $\langle a \rangle \cap H = 0$. We want to show that $\langle a \rangle + H = G$.

Assume on the contrary that some $x_0 \in G$ satisfies $x_0 \neq \langle a \rangle + H$. Consider the sequence $x_0, px_0, \ldots, p^n x_0$. Since the first element of the sequence is not in $\langle a \rangle + H$, and the last element is in $\langle a \rangle + H$, there must exist some x in this sequence such that

$$x \notin \langle a \rangle + H, \tag{2}$$
$$px \in \langle a \rangle + H. \tag{3}$$

The condition (3) means that

$$px = ta + h \qquad \text{for some } t \in \mathbb{Z} \text{ and } h \in H.$$

Combining this with (1) we obtain $0 = p^n x = p^{n-1}(ta + h) = (p^{n-1}t)a + p^{n-1}h$. This implies that the element $(p^{n-1}t)a = -p^{n-1}h$ is both in $\langle a \rangle$ and in H. Since $\langle a \rangle \cap H = 0$, it follows that $(p^{n-1}t)a = 0$. Because $|a| = p^n$, we may infer that $p \mid t$.

Say $t = pm$ for some $m \in \mathbb{Z}$. Let

$$y \overset{\text{def}}{=} x - ma.$$

Observe that $y \notin H$ and $py = h \in H$.

Let $H' \overset{\text{def}}{=} H + \langle y \rangle$; because $y \notin H$, this group is strictly larger than H. We claim that $H' \cap \langle a \rangle = 0$, which would contradict the choice of H. Suppose that the claim is false, and there is some non-zero element that is of the form $sa = h_0 + ry$ for some $h_0 \in H$ and $r \in \mathbb{Z}$. Note that $p \nmid r_0$, for otherwise the element $sa = h_0 + ry$ would belong to both $\langle a \rangle$ and H. Therefore, by the Euclidean algorithm, there exists $r' \in \mathbb{Z}$ such that $rr' \equiv 1 \pmod{p}$, say $rr' = 1 + pu$. Because $(s + rm)a = h_0 + rx$, it follows that $r'(s + rm)a = r'h_0 + x + pux$ contradicting that assumption that $x = r'(s + rm)a - r'h_0 - u(px)$ is not an element of $\langle a \rangle + H$. $\qquad \square$

These lemma quickly imply Theorem 1. Indeed, by Lemma 2 it suffices to prove Theorem 1 only for the case when the finite group G is a p-group. This case follows from Lemma 3 by induction on the order of G; we just need to apply the induction hypothesis to the subgroup H from that lemma.