0.1 Classification of finite abelian groups

Of all the groups, the finite abelian groups are relatively nice behaved, because they're abelian. What is even nicer behaved are the finite cyclic groups. Since they're so nicely behaved, it would be nice if we could understand everything about them. The theorem we present in this chapter will go a long way to dealing with this.

To motivate the theorem, recall that the fundamental theorem of arithmetic tells us that every number can be factorized uniquely as a product of primes, i.e. $n = p_1^{k_1} \cdots p_m^{k_m}$, where the p_i's are distinct primes. It turns out that we can do something similar for groups. We first state the theorem; the proof is difficult. Before embarking on this proof, please check out **??**.

Theorem 0.1 (Classification of finite abelian groups)**.** Every finite abelian group is a unique product of cyclic groups of prime power order.

Now let's see what this means. Let G be a finite abelian group of order n. Then, Theorem 0.1 says that

$$G \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

However, note that *the p_i's may not be distinct primes.* However, this "factorization" is unique, meaning that if

$$G \cong \mathbb{Z}_{q_1^{l_1}} \times \cdots \times \mathbb{Z}_{q_n^{l_n}},$$

where q_i's are primes, then $n = m$, and $\{ p_1, \ldots, p_n \} = \{ q_1, \ldots, q_m \}$, and if $p_j = q_i$ then their powers are the same too.

This theorem is extremely powerful. It is extremely easy to determine *all* Abelian groups of a certain order. In contrast, classifying non abelian groups is extremely difficult. We additionally obtain a partial converse to Lagrange's theorem as a corollary.

Corollary 0.2 (Subgroups of finite abelian groups)**.** Let G be a finite abelian group and m divide the order of G. Then G has a subgroup of order m.

Proof. See Exercise 0.8. □

We will now prove the theorem. This proof comes from [Gal20, Ch 11]. We first "factorize" the group G using primes. We will encounter the following lemma but stated more generally; it is essentially Sylow's First Theorem.

Lemma 0.3 (Sylow's First Theorem for Abelian groups)**.** *Let G be a finite abelian group of order $p^n m$ where p does not divide m. Then, $G = H \times K$[1], where $H = \{ x \in G : x^{p^n} = e \}$ and $K = \{ x \in G : x^m = e \}$. Additionally, $|H| = p^n$.*

Proof. Obviously H and K are subgroups. Let us show that $H \cap K = \{ e \}$ and $HK = G$. The fact that $H \cap K = \{ e \}$ is trivial. By Bezout's lemma, let s, t be integers such that $1 = sm + tp^n$. For any $x \in G$, we have

$$x = x^{sm+tp^n} = x^{sm} x^{tp^n}.$$

Then observe that $(x^{sm})^{p^n} = x^{smp^n} = e$ so $x^{sm} \in H$. A similar idea holds to show $x^{tp^n} \in K$. This shows $G = HK$. To prove the order statement, notice that

$$p^n m = |HK| = \frac{|H||K|}{|H \cap K|},$$

by **??**, so that $|H||K| = p^n m$. Now, by Cauchy's Theorem (for finite abelian groups) (**??**) and **??**, if p divides $|K|$ then there would be an element of order p in K, call it k. But then $k^m = e$ and p does not divide m so that is not possible. Thus p does not divide $|K|$. So p divides $|H|$, thus $|H| = p^n$. □

We apply the lemma in the following form.

[1] This is an internal direct product. See **??** for the definition of an internal direct product.

Corollary 0.4. Suppose G is an abelian group where $|G| = p_1^{k_1} \cdots p_n^{k_n}$. Define $G(p_i) = \left\{ x \in G : x^{p_i^{n_i}} = e \right\}$. Then, $G = G(p_1) \times \cdots \times G(p_n)$, and $|G(p_i)| = p_i^{k_i}$.

Proof. Induction. □

Next, we show that if an abelian group G has prime power order, we can "factorize" it with one of the factors being cyclic.

Lemma 0.5. *Suppose G is an Abelian group of order p^n. Let $a \in G$ be an element of maximum order. Then, $G = \langle a \rangle \times K$ for some subgroup K of G.*

Proof. We induct on n. If $n = 1$, it is trivial. Assume the lemma is true for all abelian groups of order p^k where $k < n$. Let a be an element of maximum order, say $|a| = p^m$. This means that $x^{p^m} = e$ for all $x \in G$. Assume $m < n$, else it is trivial. Let b be an element of minimum order such that $b \notin \langle a \rangle$. We claim that $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Firstly, b^p has order $|b|/p$. Since b is of minimum order with $b \notin \langle a \rangle$, we know that b^p having a smaller order will satisfy $b^p \in \langle a \rangle$, so let $b^p = a^i$. Now, since $e = (b^p)^m = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}}$, we know that a^i does not generate $\langle a \rangle$, so that $\gcd(i, p^m) \neq 1$ (by **??**). Thus p divides i, so let $i = pj$. Then $b^p = a^{pj}$. Let us consider the element $c = a^{-j}b$ (for reasons that will become clear shortly). Note that $c \notin \langle a \rangle$. Also, $c^p = a^{-jp}b^p = a^{-i}b^p = b^{-p}b^p = e$. This shows c has order p, and $c \notin \langle a \rangle$. Since b is an element of minimum order such that $b \notin \langle a \rangle$, we know b has order p. We have now shown the claim, since if $g \in \langle a \rangle \cap \langle b \rangle$, but $g \neq e$, then g generates $\langle b \rangle$, but then $b \in \langle a \rangle$, a contradiction.

We still need to show $\langle a \rangle \langle b \rangle = G$. To do so, we study a factor group and use induction. Let $\overline{G} = G/\langle b \rangle$. Let $\overline{x}$ denote the coset $x\langle b \rangle \in \overline{G}$. It's not hard to see that $|\overline{a}| = |a|$. If not, we have $\overline{a}^{p^{m-1}} = \overline{e}$. This shows that $a^{p^{m-1}} \in \langle b \rangle$, but then we would have $\langle a \rangle \cap \langle b \rangle$ having nontrivial intersection, since $a^{p^{m-1}} \neq e$. As such, $\overline{a}$ is an element of maximum order in $\overline{G}$. By induction, this tells us that $\overline{G} = \langle \overline{a} \rangle \times \overline{K}$ where $\overline{K} \leq \overline{G}$. Letting $\pi : G \to \overline{G}$ be the homomorphism defined by $\pi(g) = g\langle b \rangle$, we see that $K := \pi^{-1}\left[\overline{K}\right]$ is a subgroup of G. Now, we claim that $\langle a \rangle \cap K = \{e\}$. If $x \in \langle a \rangle \cap K$, then $\overline{x} \in \langle \overline{a} \rangle \cap \overline{K} = \{\overline{e}\} = \{e\langle b \rangle\}$. In particular we have $\overline{x} = \langle b \rangle$, but this means $x \in \langle b \rangle$, and since $x \in \langle a \rangle$, it must be that $x = e$. Now consider the order of K, and notice that $|G| = |\langle a \rangle| \cdot |K|$, so it must be that $G = \langle a \rangle K$. □

The above lemma implies the following:

Lemma 0.6. *Let G be an abelian group of prime power order. Then, it is an (internal) direct product of cyclic groups.*

Proof. Use Lemma 0.5 and induction on order of G. □

We now need to deal with uniqueness.

Lemma 0.7. *Let G be a finite abelian group with order p^n. If $G = H_1 \times \cdots \times H_m$, and $G = K_1 \times \cdots \times H_n$, where all H_i, K_j are nontrivial cyclic subgroups such that $|H_1| \geq \cdots \geq |H_i| \geq |H_{i+1}| \geq \cdots$, $|K_1| \geq \cdots \geq |K_j| \geq |K_{j+1}| \geq \cdots$, then $n = m$, and $|H_i| = |K_i|$ for all i.*

Proof. We start by induction on order of G. □

We end off this chapter with some closing remarks. Firstly, the group $\langle a \rangle$ in Lemma 0.5 would be a Sylow p-subgroup of G.

Secondly, this theorem can be derived as a corollary of a more general theorem, the classfiication of finitely generated abelian groups. This theorem can be derived as a corollary of a even more general theorem, the classification of finitely generated modules over a principal ideal domain. We will take up these theorems in the future, but for now these facts are just interesting to note.

0.1.1 Exercises and Problems

Exercise 0.8 (Subgroups of finite abelian groups)**.** Prove Corollary 0.2. A sketch is given in the next paragraph.

Let G be a finite abelian group of order n. We perform induction on n. When $n = 1$ or $m = 1$ it is trivial. Suppose the theorem is true for all abelian groups of order less than n. Let p be a prime dividing m, so that G has a subgroup of order p, say K (by Cauchy's Theorem). Then G/K has order n/p, and by the inductive hypothesis there is some subgroup of G/K of the form H/K that has order m/p.