11.3 The Classification Theorem of Finite Abelian Groups

Recall that we can list all abelian groups of order p^n. Well in fact, this can be extended easily to list all finite and finitely generated abelian groups!

Example 11.3.1. Here we list (up to isomorphism) all abelian groups of order $729 = 3^6$.

Shape	Decomposition of 3^6	Group	Remarks
(6)	3^6	C_{3^6}	$= C_{729}$
$(5,1)$	$3^5 \cdot 3^1$	$C_{3^5} \times C_3$	$\cong C_3 \times C_{3^5}$
$(4,2)$	$3^4 \cdot 3^2$	$C_{3^4} \times C_{3^2}$	$\cong C_{3^2} \times C_{3^4}$
$(4,1,1)$	$3^4 \cdot 3^1 \cdot 3^1$	$C_{3^4} \times C_3 \times C_3$	$\cong C_3 \times C_{3^4} \times C_3$ etc.
$(3,3)$	$3^3 \cdot 3^3$	$C_{3^3} \times C_{3^3}$	
$(3,2,1)$	$3^3 \cdot 3^2 \cdot 3^1$	$C_{3^3} \times C_{3^2} \times C_3$	$\cong C_{3^2} \times C_{3^3} \times C_3$ etc.
$(3,1,1,1)$	$3^3 \cdot 3 \cdot 3 \cdot 3$	$C_{3^3} \times C_3 \times C_3 \times C_3$	$\cong C_3 \times C_{3^3} \times C_3 \times C_3$ etc.
$(2,2,2)$	$3^2 \cdot 3^2 \cdot 3^2$	$C_{3^2} \times C_{3^2} \times C_{3^2}$	
$(2,2,1,1)$	$3^2 \cdot 3^2 \cdot 3 \cdot 3$	$C_{3^2} \times C_{3^2} \times C_3 \times C_3$	$\cong C_3 \times C_{3^2} \times C_{3^2} \times C_3$ etc.
$(2,1,1,1,1)$	$3^2 \cdot 3 \cdot 3 \cdot 3 \cdot 3$	$C_{3^2} \times C_3 \times C_3 \times C_3 \times C_3$	etc.
$(1,1,1,1,1,1)$	$3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3$	$C_3 \times C_3 \times C_3 \times C_3 \times C_3 \times C_3$	

Hence, up to isomorphism there are 11 abelian groups of order 729.

Theorem 11.3.2. (The Fundamental Theorem of finite abelian Groups) *If G is a nontrivial finite abelian group then G is isomorphic to a direct product of cyclic groups of prime power order,*

$$C_{p_1^{e_1}} \times \cdots \times C_{p_n^{e_n}},$$

where the primes p_i are not necessarily distinct, the e_i are natural numbers, and $p_1^{e_1} \cdots p_n^{e_n} = |G|$. Moreover, this decomposition is unique, up to reordering of the factors.

Warning! There are several different (equivalent) ways of stating this theorem! Some books will use $\oplus$ instead of $\times$. Other versions use Proposition 11.2.1 to write the factors in a different way (so they are no longer prime powers), for example writing $C_{5^4} \times C_{5^2} \times C_{3^2} \times C_3 \times C_2$ as $C_{5^4 \cdot 3^2 \cdot 2} \times C_{5^2 \cdot 3} = C_{11250} \times C_{75}$.

We also have the following for finitely generated abelian groups.

Theorem 11.3.3. (The Fundamental Theorem of Finitely Generated Abelian Groups) *If G is a nontrivial finitely generated abelian group then G is isomorphic to,*

$$\mathbb{Z}^{e_0} \times C_{p_1^{e_1}} \times \cdots \times C_{p_n^{e_n}},$$

where the primes p_i are not necessarily distinct and the e_i are natural numbers. Moreover, this decomposition is unique, up to reordering of the factors.

Definition 11.3.4. If G is a nontrivial finitely generated abelian group and $\mathbb{Z}^{e_0} \times C_{p_1^{e_1}} \times \cdots \times C_{p_n^{e_n}}$ is its factorisation, then the number e_0 is called *the rank of G*.

Example 11.3.5. Up to isomorphism, the abelian groups of order $12 = 2^2 \cdot 3$ are $C_{2^2} \times C_3$ and $C_2 \times C_2 \times C_3$.

[Advanced handout: You are NOT required to read this, it is here just in case you are interested] Proofs of the classification of finite and finitely generated abelian groups

In this section we prove Theorem 11.2.4 and give an outline of the proof of Theorem 0.1.2. These proofs involve material from the whole of the course, and they are rather intricate. This section does not form part of the course and is supplied here only for students who are particularly interested.

Theorem 11.2.4 follows easily from the following lemma.

Lemma 11.3.6. *Let p be a prime and let G be a finite abelian group of order p^n. If $a \in G$ has maximal order, then $G \cong \langle a \rangle \times K$ for some $K \leq G$.*

Proof. Now $o(a) = p^m$ for some $m \leq n$. We proceed by induction. If $n = 1$ then G is cyclic and the lemma holds. Now suppose $n \in \mathbb{N}$ and the lemma holds for all finite abelian group of order p^k with $k < n$.
If G is cyclic then there is nothing to prove, so assume this is not the case. Since $G \neq \langle a \rangle$, we can find $b \in G$ such that b has minimal order in $G \setminus \langle a \rangle$. This means of course that if $g \in G$ and $o(g) < o(b)$ then $g \in \langle a \rangle$.

Claim 1: For all $g \in G$ we have $g^{p^m} = e$. Proof. Now $o(g) \big| p^n$, so $o(g) = p^i$ with $i \leq m$ (since $o(a)$ is maximal and equal to p^m). Therefore,

$$g^{p^m} = g^{p^i \cdot p^{m-i}} = \left(g^{p^i}\right)^{p^{m-i}} = e^{p^{m-i}} = e.$$

Claim 2: $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$ and $o(b) = p$. Proof. Now $o(b^p) < o(b)$ so by minimality of $o(b)$ we have $b^p \in \langle a \rangle$. In particular, $b^p = a^i$ for some i. By Claim 1,

$$e = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}} = a^{i \cdot p^{m-1}}.$$

Since $o(a) = p^m$ we know $p^m \big| i \cdot p^{m-1}$ and therefore $i = pj$ for some $j \in \mathbb{N}$. Define $c := a^{-j} b$ and note that $c \notin \langle a \rangle$ (since if it were, then $b \in \langle a \rangle$ which is absurd). Moreover, $c^p = a^{-jp} b^p = a^{-i} b^p = b^{-p} b^p = e$. To summarise:

$$o(c) = p \quad \text{and} \quad c \notin \langle a \rangle.$$

By Lagrange's Theorem, we know that $o(b)$ is a power of p. Hence, by the minimality of $o(b)$, we must have that $o(b) = o(c) = p$.
Now $o(b) = p$, so $\langle b \rangle$ is cyclic of prime order. In particular, any nontrivial element of $\langle b \rangle$ generates $\langle b \rangle$. Therefore $\langle a \rangle \cap \langle b \rangle$ must equal $\langle e \rangle$ or $\langle b \rangle$. Since $b \notin \langle a \rangle$, the latter is impossible. Hence $\langle a \rangle \cap \langle b \rangle = \langle e \rangle$.

Claim 3: In $\overline{G} := G/\langle b \rangle$, the element $\overline{a} := a\langle b \rangle$ has order p^m, and this order is maximal in $\overline{G}$. Proof. Since every element in G has order at most p^m, the same is true of $\overline{G}$. Hence, we need only show that $o(\overline{a}) = p^m$.
Let us assume, for a contradiction, that $o(\overline{a}) < p^m$. Then $\overline{a}^{p^{m-1}} = \overline{e}$. Hence

$$(a\langle b \rangle)^{p^{m-1}} = a^{p^{m-1}} \langle b \rangle = \overline{a}^{p^{m-1}} = \overline{e} = \langle b \rangle.$$

Thus, $a^{p^{m-1}} \in \langle b \rangle \cap \langle a \rangle$, and this is trivial by Claim 2. Hence $a^{p^{m-1}} = e$, which is absurd.

Claim 4: $\overline{G} = \langle \overline{a} \rangle \times \overline{K}$ for some $\overline{K} \leq \overline{G}$. Proof. This follows from the induction hypothesis, because $|\overline{G}| = |G|/|\langle b \rangle| = p^{n-1}$.

Claim 5: G is the internal direct product $G = \langle a \rangle K$. Proof. Now $\overline{K}$ corresponds to a subgroup K with $\langle b \rangle \leq K \leq G$ and $\overline{K} = K/\langle b \rangle$. Since $|\langle b \rangle| = p$, we have $|\overline{K}| = |K|/p$.
If $g \in \langle a \rangle \cap K$, then $\overline{g} \in \langle \overline{a} \rangle \cap \overline{K}$. However, by Claim 4 we know that $\langle \overline{a} \rangle \cap \overline{K} = \langle \overline{e} \rangle$. Therefore $\langle a \rangle \cap K \subseteq \langle b \rangle$. However, by Claim 2 this then implies that $\langle a \rangle \cap K = \langle e \rangle$. Since G is abelian, we therefore have that:

$$\langle a \rangle \trianglelefteq G \quad \text{and} \quad K \trianglelefteq G \quad \text{and} \quad \langle a \rangle \cap K = \langle e \rangle.$$

It remains simply to check that $\langle a \rangle K = G$, which we can show by proving that $|\langle a \rangle K| = |G|$. Now $|\langle a \rangle K| = |\langle a \rangle| \cdot |K| = |\langle a \rangle|(p|\overline{K}|) = p^m p|\overline{K}|$. By Claim 3 the latter equals $|\langle \overline{a} \rangle| p|\overline{K}| = p|\langle \overline{a} \rangle \overline{K}|$. By Claim 4 the latter equals $p|\overline{G}| = p^n = |G|$.

Claim 6: $G \cong \langle a \rangle \times K$. Proof. This follows immediately from Theorem 11.1.3 and Claim 5. □

Proof of Theorem 11.2.4. We proceed by induction on n. If $n = 1$ then G is cyclic of order p and there is nothing to prove. Suppose the theorem is true for all groups of order p^k, for all $k < n$.
If G is cyclic then there is nothing to prove, so suppose this is not the case. Let $a \in G$ have maximal order. Then by Lemma 0.1.6 we can write $G \cong \langle a \rangle \times K$, where $K \leq G$. Now $p^n = |\langle a \rangle \times K| = |\langle a \rangle| \cdot |K|$. Hence $|K| = p^r$ and $|\langle a \rangle| = p^s$ for some r, s with $r + s = n$. Note that, since $\langle a \rangle$ is cyclic, we have, $\langle a \rangle \cong C_{p^s}$.
Since $|K| = p^r < p^n$, we can apply the induction hypothesis to deduce that there are natural numbers $e_2, \ldots, e_t$ such that,

$$K \cong C_{p^{e_2}} \times \cdots \times C_{p^{e_t}},$$

where $p^{e_2} \cdots p^{e_t} = p^r$, and this factorisation of K is unique up to reordering of the factors. Setting $e_1 := s$ we therefore have,

$$G \cong \langle a \rangle \times K \cong C_{p^{e_1}} \times C_{p^{e_2}} \times \cdots \times C_{p^{e_t}},$$

where $p^{e_1} \cdot (p^{e_2} \cdots p^{e_t}) = p^s p^r = p^n$.
Finally, we must show the factorisation is unique. By Proposition 11.1.1, the order of the factors doesn't matter, so we can without loss of generality assume that $p^{e_2} \geq \cdots \geq p^{e_t}$. Since the order of a was chosen to be maximal, we also have $p^{e_1} \geq p^{e_2}$. If we are given another factorisation $G \cong C_{q^{f_1}} \times C_{q^{f_2}} \times \cdots \times C_{q^{f_r}}$ with q prime and $q^{f_1} \geq \cdots \geq q^{f_r}$ then the largest order of any element in G is clearly q^{f_1}. Since a has maximal order in G, it follows that $o(a) = q^{f_1}$ and therefore $p^{e_1} = q^{f_1}$. Hence,

$$K \cong G/\langle a \rangle \cong G/C_{p^{e_1}} \cong G/C_{q^{f_1}} \cong C_{q^{f_2}} \times \cdots \times C_{q^{f_r}}.$$

By the induction hypothesis, the factorisation of K as $C_{p^{e_2}} \times \cdots \times C_{p^{e_t}}$ is unique. □

Outline of proof of Theorem 0.1.2. (The proof of Theorem 0.1.3 is similar) Let G be a nontrivial finite abelian group.

- Let $p_1, p_2, \ldots, p_r$ be the distinct prime divisors of $|G|$, and let P_i be the Sylow p_i-subgroup of G for $1 \leq i \leq r$.
- Because G is abelian, every subgroup is normal. Therefore $P_i \trianglelefteq G$ for all i.
- For $s \leq r$ let $\Pi_s = P_1 P_2 \cdots P_s$. Because each $P_i \trianglelefteq G$, we have that Π_s is a group, and therefore a subgroup of G. Moreover, for all $g \in G$ we have $g^{-1}(\Pi_s)g$ is equal to $g^{-1}P_1 g g^{-1} P_2 g g^{-1} \cdots g g^{-1} P_s g = \Pi_s$. Hence $\Pi_s \trianglelefteq G$.
- Let $s \leq r$. Now $|P_s|$ is a power of p_s, so by Lagrange every element in P_s has order a power of p_s. On the other hand, every element in Π_{s-1} has order a product of powers of $p_1, \ldots, p_{s-1}$. Hence $\Pi_{s-1} \cap P_s = \langle e \rangle$.
- We have shown that $\Pi_{s-1} \cap P_s = \langle e \rangle$ and both Π_{s-1} and P_s are normal in G and therefore also normal in Π_s. Hence Π_s is the internal direct product of Π_{s-1} and P_s.
- Hence (using an induction argument) one can show that:

$$\Pi_r \cong \Pi_{r-1} \times P_r \cong \Pi_{r-2} \times P_{r-1} \times P_r \cong \cdots \cong P_1 \times \cdots \times P_r.$$

- Since $|G| = p_1 \cdots p_r = |P_1 \times \cdots \times P_r|$ we see that $\Pi_r = G$. Hence G is isomorphic to the direct product $P_1 \times \cdots \times P_r$.
- Each group P_i is a finite abelian group whose order is $p_i^{n_i}$, and so we can apply Theorem 11.2.4 to P_i to uniquely decompose it into a direct product of cyclic groups, like so:

$$P_i = C_{p_i^{e_{i,1}}} \times C_{p_i^{e_{i,2}}} \times \cdots \times C_{p_i^{e_{i,t_i}}}$$

- The result then follows immediately.

□