CLASSIFICATION OF FINITE ABELIAN GROUPS

1. The main theorem

**Theorem 1.1.** Let $A$ be a finite abelian group. There is a sequence of prime numbers

$$p_1 \leq p_2 \leq \cdots \leq p_n$$

(not necessarily all distinct) and a sequence of positive integers

$$a_1 \leq a_2 \leq \cdots \leq a_n$$

such that $A$ is isomorphic to the direct product

$$A \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}.$$

In particular

$$|A| = \prod_{i=1}^{n} p_i^{a_i}.$$

**Example 1.2.** We can classify abelian groups of order $144 = 2^4 \times 3^2$. Here are the possibilities, with the partitions of the powers of 2 and 3 on the right:

- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3; \ (4, 2) = (1 + 1 + 1 + 1, 1 + 1)$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3; \ (4, 2) = (1 + 1 + 2, 1 + 1)$
- $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3; \ (4, 2) = (2 + 2, 1 + 1)$
- $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3; \ (4, 2) = (1 + 3, 1 + 1)$
- $\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3; \ (4, 2) = (4, 1 + 1)$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9; \ (4, 2) = (1 + 1 + 1 + 1, 2)$
- $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9; \ (4, 2) = (1 + 1 + 2, 2)$
- $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9; \ (4, 2) = (2 + 2, 2)$
- $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9; \ (4, 2) = (1 + 3, 2)$
- $\mathbb{Z}_{16} \times \mathbb{Z}_9$ cyclic, isomorphic to $\mathbb{Z}_{144}; \ (4, 2) = (4, 2)$.

There are 10 non-isomorphic abelian groups of order 144.

Theorem 1.1 can be broken down into two theorems.
Theorem 1.3. Let $A$ be a finite abelian group. Let $q_1, \ldots, q_r$ be the distinct primes dividing $|A|$, and say

$$|A| = \prod_j q_j^{b_j}.$$ 

Then there are subgroups $A_j \subseteq A$, $j = 1, \ldots, r$, with $|A_j| = q_j^{b_j}$, and an isomorphism

$$A \xrightarrow{\sim} A_1 \times A_2 \times \cdots \times A_r.$$ 

Let $p$ be a prime number. A finite group (abelian or not) is called a $p$-group if its order is a power of $p$.

Theorem 1.4 (Abelian $p$-groups). Let $p$ be a prime and let $A$ be a finite abelian group of order $p^N$ for some $N \geq 1$. Then there is a sequence of positive integers $c_1 \leq c_2 \leq \cdots \leq c_s$ and an isomorphism

$$A \xrightarrow{\sim} \mathbb{Z}_{p^{c_1}} \times \mathbb{Z}_{p^{c_2}} \times \cdots \times \mathbb{Z}_{p^{c_s}}.$$ 

Theorem 1.3 is essentially a series of applications of the Chinese Remainder Theorem, and is not very hard. It will be presented in class.

Theorem 1.4 is a more complicated induction argument that needs to be studied in order to be understood. It will be carried out in the next section.

2. The induction step (A very long lemma)

Let $p$ and $A$ be as in Theorem 1.4. We prove it by induction on the integer $N$, of course. If $N = 1$ then $|A| = p$. In that case we know that $A$ is a cyclic group isomorphic to $\mathbb{Z}_p$. So we assume the theorem is known for groups of order $p^k$ with $k < N$. The induction step is to show that it is then known when $|A| = p^N$.

Definition 2.1. Let $A$ be a finite $p$-group. The exponent of $A$ is the largest integer $m$ such that there is an element $a \in A$ of order exactly $p^m$. In other words $ap^n = e$ but $ap^{n-1} \neq e$.

Thus if $A$ is cyclic of order $p^N$, the exponent of $A$ is $N$: a generator has order $p^N$ but not $p^{N-1}$. We need the following facts about the exponent.

Fact 2.2. Let $A$ be a finite $p$-group, $H \subset A$ a normal subgroup. Suppose the exponent of $A$ is $m$. Then the exponent of $A/H$ is $\leq m$.

Proof. Let $\pi : A \to A/H$ be the reduction map. Every element $x \in A/H$ is of the form $\pi(a)$ for some element $a \in A$. We know that $a^{p^r} = e$ for some $r \leq m$. It follows that

$$x^{p^r} = (\pi(a))^{p^r} = \pi(a^{p^r}) = \pi(e) = e.$$ 

So $x^{p^m} = e$ for all $x \in A/H$, which implies that the exponent of $A/H$ is at most $m$. \qed
Fact 2.3. Let $A$ be a finite $p$-group, $H \subset A$ a normal subgroup, $a \in A$. Suppose
\[ \langle a \rangle \cap H = \{ e \}, \]
where $\langle a \rangle \subset A$ is the cyclic subgroup generated by $a$. Suppose $a$ is of order $p^m$. Let $\pi : A \to A/H$ be the reduction map and let $\bar{a} = \pi(a) \in A/H$. Then $\bar{a}$ is of order $p^m$ in $A/H$.

Proof. In any case $\bar{a}^{p^m} = e$ for the reason already seen in the proof of Fact 2.2. Suppose $\bar{a}$ is of order less than $p^m$, say $\bar{a}^s = e$ for some $1 \leq s < p^m$. That means that $\pi(a^s) = e$, or $a^s \in \ker \pi$, which implies that $a^s \in H$. Thus $a^s \in \langle a \rangle \cap H = \{ e \}$, which implies that $a^s = e$, and this contradicts the assumption that $a$ is of order $p^m$. \[\Box\]

Here is the main step in the proof.

Lemma 2.4. Let $A$ be a finite abelian $p$-group of order $p^N$ and exponent $m$, so that the cyclic group $\langle a \rangle$ has order $p^m$. Let $a \in A$ be an element of order $p^m$. Then there is a subgroup $B \subseteq A$ such that $B \cap \langle a \rangle = \{ e \}$, and the inclusion of $B$ and $\langle a \rangle$ as subgroups of $A$ defines an isomorphism
\[ B \times \langle a \rangle \xrightarrow{\sim} A. \]

Proof. This is an induction on $N$. If $N = 1$ then $A$ is cyclic and we are done. Suppose we know the statement for $1 \leq k < N$. We have already chosen $a$ of maximal exponent. Now we choose $h \in A$ of smallest order such that $h \not\in \langle a \rangle$. (We will soon see that $h$ is of order $p$.) If no such $h$ exists, then every $h \in A$ belongs to $\langle a \rangle$ and so $A = \langle a \rangle$ is cyclic, and we can take $B = \{ e \}$.

So we assume such an $h$ exists. Let $u = h^p$. If $u = e$ then $h$ has order $p$. If not, then $h$ has order $p^r$ for some $r > 1$, by Lagrange’s theorem, because $A$ is a $p$-group. And then $u^{p^{r-1}} = h^{p^{r-1}} = h^{p^r} = e$, so $u$ has smaller order than $h$, which by definition implies that $u \in \langle a \rangle$, say $u = a^s$, for some integer $s \in \{1, 2, \ldots, p^m - 1 \}$. Thus $h^p = a^s$, so
\[ (a^s)^{p^{m-1}} = (h^p)^{p^{m-1}} = h^{p^m} = e \]
since $m$ is the exponent of $A$. It follows that $a^s$ has order strictly less than $p^m$, so $a^s$ is not a generator of the cyclic group $\langle a \rangle$. Thus $s$ is divisible by $p$, say $s = pc$. Then
\[ h^p = (a^c)^p \Rightarrow (a^{-c}h)^p = e. \]
Let $h' = a^{-c}h$. If $h' \in \langle a \rangle$ then so is $a^c h' = h$, but $h$ was chosen not in $\langle a \rangle$, contradiction. So $h' \in A$ is an element of order $p$ that is not in $\langle a \rangle$. Since $h$ has the smallest order of elements not in $\langle a \rangle$, it follows that $h$ has order $p$ after all.

Let $H = \langle h \rangle$. We see $H = | \langle h \rangle | = p$, and $\langle a \rangle \cap H = \{ e \}$, since $h \notin \langle a \rangle$. Consider the composite homomorphism
\[ \langle a \rangle \hookrightarrow A \to A/H. \]
We call this composite $\phi$, and write $\bar{a} = \phi(a)$. Since $\langle a \rangle \cap H = \{e\}$, it follows from Fact 2.3 that $\bar{a} = \phi(a)$ has order $p^m$.

Now it follows from Fact 2.2 that $A/H$ has exponent at most $m$. But $\bar{a} \in A/H$ has order exactly $p^m$, so $A/H$ has exponent $m$. On the other hand $|A/H|$ has order $|A|/|H| = p^N/p < |A|$. By induction on $N$, it follows that there is a subgroup $B' \subset A/H$ such that $B' \cap \langle \bar{a} \rangle = \{e\}$ and

$$B' \times \langle \bar{a} \rangle \xrightarrow{\sim} A/H.$$ 

In particular

$$|A/H| = |A|/p = |B'| \cdot |\langle \bar{a} \rangle|; \quad |A| = p \cdot |B'| \cdot |\langle \bar{a} \rangle| = p \cdot |B'| \cdot p^m.$$ 

We know that there is a unique subgroup $\tilde{B}' \subset A$ containing $H$ such that $\tilde{B}'/H = B'$, and thus

$$|\tilde{B}'| = p \cdot |B'|.$$ 

We claim that

$$\langle a \rangle \cap \tilde{B}' = \{e\}.$$ 

This implies that the homomorphism

$$\phi': \langle a \rangle \times \tilde{B}' \to A$$

has trivial kernel. Thus

$$p^N = |A| \geq |\langle a \rangle \times \tilde{B}'| = |\langle a \rangle| \cdot |\tilde{B}'| = p^m \cdot |\tilde{B}'| = p^m \cdot p \cdot |B'| = |A|.$$ 

Thus $\phi'$ is the isomorphism we are seeking.

It remains to prove $\langle a \rangle \cap \tilde{B}' = \{e\}$. But if $b \in \langle a \rangle \cap \tilde{B}'$ then the coset $bH \in A/H$ belongs to

$$\langle aH \rangle \cap \tilde{B}'/H = \langle \bar{a} \rangle \cap B' = e_{A/H}.$$ 

In other words, $b \in H$, but $b \in \langle a \rangle$, hence $b = e$. 

$\square$

3. Completion of the proof of Theorem 1.4

Now let $A$ be any abelian $p$ group. We have seen that $A$ is isomorphic to a product

$$A \xrightarrow{\sim} \langle a \rangle \times B,$$

where $B$ is a subgroup of $A$. We can write this

$$A \xrightarrow{\sim} B \times \mathbb{Z}_{p^m}.$$ 

Now $|B| < |A|$, so by induction $B$ is isomorphic to a product

$$B \xrightarrow{\sim} \mathbb{Z}_{p^{c_1}} \times \mathbb{Z}_{p^{c_2}} \times \cdots \times \mathbb{Z}_{p^{c_{s-1}}}$$

where $c_1 \leq c_2 \cdots \leq c_{s-1}$. Since $m$ is the exponent of $A$, we know that $c_{s-1} \leq m$. Thus setting $c_s = m$, we have

$$A \xrightarrow{\sim} \mathbb{Z}_{p^{c_1}} \times \mathbb{Z}_{p^{c_2}} \times \cdots \times \mathbb{Z}_{p^{c_{s}}}$$

and this completes the proof.
To summarize the induction proof: Theorem 1.4 is obvious when the group $A$ has order $p$. So we assume it is true for abelian groups of order $p^k$ for $k < N$. We introduce the notion of exponent of a finite $p$-group and choose an element $a \in A$ of maximal order. We then show that there is a subgroup $H \subset A$ of order $p$ such that $H \cap \langle a \rangle$ contains just the identity. It follows that the image $\bar{a} \in A/H$ of $a$ is of maximal order, and since $|A/H| < |A|$, the induction step implies that the theorem holds for $A/H$. Thus $A/H \sim \langle a \rangle \times B'$ for some $B'$, and a short argument then allows us to conclude that $A \sim \langle a \rangle \times B$, where $B = \bar{B}'$ is the subgroup of $A$ corresponding to the subgroup $B'$ of $A/H$.

This completes the proof of the Lemma, and then a second application of the induction step, this time to $B$, completes the proof of Theorem 1.4.