Math 403 Chapter 11: The Fundamental Theorem of Finite Abelian Groups

---

1. **Introduction:** The Fundamental Theorem of Finite Abelian Groups basically categorizes all finite Abelian groups.

2. **Theorem:** Every finite Abelian group is an external direct product $\oplus$ of cyclic groups of the form $\mathbb{Z}_{p^\alpha}$ for prime p. Moreover any two such groups are isomorphic in the sense that $\mathbb{Z}_a \oplus \mathbb{Z}_b \approx \mathbb{Z}_{ab}$ whenver $\gcd(a, b) = 1$.

   Proof: Omit. $\mathcal{QED}$

3. **Impliementation:** To see how this allows us to list all distinct (up to isomorphism) finite Abelian groups of order n:

   (a) **Step 1:** Let's first start with order $n = p^\alpha$. If we partition α into various nonincreasing sums:

   $$\alpha = \beta_1 + \beta_2 + ... + \beta_k \text{ with } \beta_1 \geq \beta_2 \geq ... \geq \beta_k$$

   Then each partition yields a distinct Abelian group:

   $$\mathbb{Z}_{p^{\beta_1}} \oplus \mathbb{Z}_{p^{\beta_2}} \oplus ... \oplus \mathbb{Z}_{p^{\beta_k}}$$

   Example: To find all distinct finite Abelian groups of order $16 = 2^4$ we first list all partitions of 4:

   $$\begin{array}{l} 4 \\ 3+1 \\ 2+2 \\ 2+1+1 \\ 1+1+1+1 \end{array}$$

   This then yields distinct groups:

   $$\begin{array}{ll} \mathbb{Z}_{2^4} & = \mathbb{Z}_{16} \\ \mathbb{Z}_{2^3} \oplus \mathbb{Z}_{2^1} & = \mathbb{Z}_8 \oplus \mathbb{Z}_2 \\ \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} & = \mathbb{Z}_4 \oplus \mathbb{Z}_4 \\ \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} & = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\ \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} \oplus \mathbb{Z}_{2^1} & = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \end{array}$$

   (b) **Step 2:** For n which are not simply of order $n = p^\alpha$ we find the prime factorization of n:

   $$n = p_1^{\alpha_1} ... p_k^{\alpha_k}$$

   and then apply the above consequence to each $p_i^{\alpha^i}$ and then create all possible combinations of each.

   Example: To find all distinct finite Abelian groups of order $72 = 2^3 \cdot 3^2$ we first list those for 2^3 using partitions $3 = 3 = 2 + 1 = 1 + 1$:

   $$\begin{array}{l} \mathbb{Z}_8 \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \end{array}$$

   and then for 3^2 using partitions $2 = 2 = 1 + 1$:

$\mathbb{Z}_9$
$\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Then we create all possible combinations:

$$\begin{aligned}
&\mathbb{Z}_8 \oplus \mathbb{Z}_9\\
&\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3\\
&\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9\\
&\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3\\
&\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9\\
&\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3
\end{aligned}$$

(c) **Example:** Consider $U(13) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ with multiplication mod 13. Since $U(13)$ is Abelian and $|U(13)| = 12$ we must have either $U(13) \approx \mathbb{Z}_4 \oplus \mathbb{Z}_3$ or $U(13) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$. To figure out which we could try a variety of things. One option: The elements in $\mathbb{Z}_4 \oplus \mathbb{Z}_3$ can have order 1,2,3,4,6,12 and the elements in $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$ can have order 1,2,3,6,12. Thus if $U(13)$ has an element of order 4 then it must be isomorphic to $\mathbb{Z}_4 \oplus \mathbb{Z}_3$. In fact in $U(13)$ we have $|5| = 4$ and so $U(13) \approx \mathbb{Z}_4 \oplus \mathbb{Z}_3$. Interestingly since $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_{12}$ this also tells us that $U(13) \approx \mathbb{Z}_{12}$ which means it's cyclic.

(d) **Note:** There is no known closed formula for the number of partitions of a given α. In other words if we assign $p(\alpha)$ to be the number of ways to partition α then we have $p(1) = 1$ (because $1 = 1$), $p(2) = 2$ (because $2 = 2 = 1 + 1$), $p(3) = 3$ (because $3 = 3 = 2{+}1 = 1{+}1{+}1$), $p(4) = 5$ (because $4 = 4 = 3{+}1 = 2{+}2 = 2{+}1{+}1 = 1{+}1{+}1{+}1$), $p(5) = 7$ (because $5 = 5 = 4{+}1 = 3{+}2 = 3{+}1{+}1 = 2{+}2{+}1 = 2{+}1{+}1{+}1 = 1{+}1{+}1{+}1{+}1$), $p(6) = 11$ (because ...), $p(7) = 13$ (because ...), etc. but no known closed formula exists for $p(\alpha)$ in general. There are a variety of non-closed ways to calculate it, however.

4. **Corollary:** If G is a finite Abelian group and if $m \mid n = |G|$ then G has a subgroup of order m.

Proof: The proof is (interestingly) by strong induction on $n = |G|$. If $|G| = 1$ the result is obvious so assume the result is true for Abelian groups of order less than n and assume $m \mid n$. If $m = 1$ the result is also trivial so assume $m > 1$. Suppose p is a prime with $p \mid m$. Then $p \mid n$ and then since $G \approx Z_{p^\alpha} + G'$ for some G' and by properties of cyclic groups we know there is some $K \leq Z_{p^\alpha}$ with $|K| = p$. Put $K = K \oplus \{0\}$ Then G/K is an Abelian group of order n/p. Since $m \mid n$ we know $(m/p) \mid (n/p)$ and hence by induction G/K has a subgroup of order m/p which has the form H/K with $H \leq G$ (*). Then since $|H/K| = m/p$ and $|H/K| = |H|/|K| = |H|/p$ we have $|H| = p(m/p) = m$. $\mathcal{QED}$

(*) The fact that a subgroup of G/N must have the form H/N where $H \leq G$ is not obvious but not difficult to prove.

Example: An Abelian group of order 100 must have subgroups of orders 1,2,4,5,10,20,50 and 100.