The fundamental theorem of finitely generated abelian groups

Alex Fu

2023-01-05

Theorem 1 (Fundamental theorem of finitely generated abelian groups)**.**

Every finitely generated abelian group $(A, +)$ is the direct sum of cyclic groups:

$$A \simeq \mathbb{Z}^n \oplus \bigoplus_{k=1}^{m} \mathbb{Z}/(p_k^{r_k}\mathbb{Z}),$$

where n is the *rank* or *Betti number* of A, and $p_1^{r_1}, \ldots, p_m^{r_m}$ are (not necessarily distinct) prime powers. A is finite iff $n = 0$, and A is free abelian (of rank n) iff $m = 0$. The set of prime powers is uniquely determined by A up to isomorphism when they are put into the canonical form of *elementary divisors* or *invariant factors*.

Abelian groups are already a particularly well-behaved class of groups, and Theorem 1 characterizes an even nicer class of abelian groups: finitely generated $A = \langle g_1, \ldots, g_n \rangle$, in which every element $g \in A$ can be expressed as a finite linear combination $\sum_{i=1}^{n} a_n g_n$ of the generators. Here, we will briefly explore a few preliminary results used in building up to a proof of Theorem 1, or equivalently reducing it to simpler cases.

A simple corollary of the above is the fundamental theorem of *finite abelian groups*, which states that every finite abelian group is the direct sum of its p-primary subgroups, or p-subgroups.

Proposition 1 (p-groups)**.**

p-primary groups are abelian p-groups. G is a p-group if every element of G has order p^m for some $m \in \mathbb{N}$. A group is a p-group iff it has order p^n for some $n \in \mathbb{N}$.

The "finite abelian" part of A in Theorem 1 is also known as the *torsion* or *periodic subgroup* of A, in which every element has finite order (or period). The "free abelian" part $\mathbb{Z}^n$ is the *torsion-free* subgroup $A/\operatorname{tor}(A)$, in which every non-identity element has infinite order. With $A = \mathbb{Z}^n \oplus \operatorname{tor}(A)$, we can reduce to the case of finite abelian groups without much trouble.

From here, Proposition 1 reduces the case of finite abelian groups to p-primary groups. How precise can we make this decomposition? Let us first recall a result in a similar vein for finite cyclic groups:

Proposition 2 (Chinese Remainder Theorem)**.**

If m and n are coprime, then $\mathbb{Z}/(mn\mathbb{Z}) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proposition 3 (Primary decomposition)**.**

Let G be an abelian group of order mn for coprime m and n, i.e. $\gcd(m, n) = 1$. Then there exist subgroups $A, B \leq G$ such that $|A| = m$, $|B| = n$, and $A \oplus B = G$.

Inducting on the number of distinct prime factors, we have that if G is an abelian group of order n, where n has prime factorization $\prod_{i=1}^{k} p_i^{r_i}$, then $G \simeq A_1 \times \cdots \times A_k$, where $|A_i| = p_i^{r_i}$ for $i = 1, \ldots, k$.

Note that the direct sum and direct product coincide for abelian groups. The direct product may in fact be clearer in the finite case, in which the prime factorization of the order can give information about the factorization of the group itself, *factorization* in the sense of "breaking into a product." Now, it suffices to address p-primary groups, abelian groups of prime power order.

Proposition 4 (Elementary divisor decomposition)**.**

Let A be an abelian group of order p^n. Then $A \simeq \mathbb{Z}/(p^{n_1}\mathbb{Z}) \times \cdots \times \mathbb{Z}/(p^{n_\ell}\mathbb{Z})$, where $n_1 + \cdots + n_\ell = n$ and $n_1 \leq \cdots \leq n_\ell$ without loss of generality. This decomposition is also unique.

Continuing from Proposition 3, if we perform the above for each of $A_1, \ldots, A_k$, then the resulting set of prime powers (with multiplicity) $\{\{p_i^{n_1}, \ldots, p_i^{n_{\ell(i)}}\}\}_{i=1}^{k}$ are the unique **elementary divisors** of G.

For example, the elementary divisors of $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are $\{2^1, 2^1, 7^1\}$. And this is it: we have simplified a finitely generated abelian group down to cyclic groups of prime power order. Alternatively, the following decomposition is equally as "canonical" as the one in Proposition 3 and Proposition 4:

Proposition 5 (Invariant factor decomposition)**.**

Let G be abelian of order n. Then there exist $d_1, \ldots, d_k > 1$ unique, such that $\prod_{i=1}^{k} d_i = n$, each d_i divides d_{i+1}, and d_k contains all prime factors of n. Then $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$, and $d_1, \ldots, d_k$ are the unique **invariant factors** of G.

For example, $(\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ (whose elementary divisors are apparent) has invariant factors $2, 6, 210$, and we can check that it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/210\mathbb{Z}$ by the Chinese Remainder Theorem.

Lastly, while $\mathbb{Z}/(p^n\mathbb{Z}) \not\simeq (\mathbb{Z}/p\mathbb{Z})^n$ for $n > 1$, let us highlight a result for the (quite literally) simplest case possible:

Proposition 6 ($\mathbb{Z}/p\mathbb{Z}$)**.**

Every group of prime order p is cyclic. Every simple abelian group is cyclic of prime order.

This has been an incomplete whirlwind tour of the fundamental theorem of finitely generated abelian groups; we nonetheless invite you to continue exploring many of the wonderful details and intricacies left to be seen.

■