3-7-2018

Finitely Generated Abelian Groups

There is no (known) formula which gives the number of groups of order n for any $n > 0$. However, it's possible to classify the finite *abelian* groups of order n. This classification follows from the **structure theorem for finitely generated abelian groups**.

Definition. Let G be an abelian group. The **torsion subgroup** of G is

$$T = \{g \in G \mid ng = 0 \text{ for some } n \in \mathbb{Z}^+\}.$$

I'd better check that the definition makes sense!

Proposition. Let G be an abelian group. The torsion subgroup of G is a subgroup of G.

Proof. Let T be the torsion subgroup of G. $0 \in T$, so T is nonempty. Let $a, b \in T$. I must show $a - b \in T$. Find positive integers m, n, such that $ma = 0$ and $nb = 0$. Then

$$mn(a - b) = mna - mnb = 0 - 0 = 0.$$

Therefore, $a - b \in T$, and $T < G$. □

Definition. A group G is **torsion free** if the only element of finite order is the identity.

Definition. An abelian group G is **finitely generated** if there are elements $x_1, \ldots, x_n \in G$ such that every element $x \in G$ can be written as

$$x = a_1 x_1 + \cdots + a_n x_n, \qquad a_i \in \mathbb{Z}.$$

Note that this expression need not be unique.

Definition. A **free abelian group** is a direct sum of copies of $\mathbb{Z}$ (possibly infinitely many copies).

The number of copies (in the sense of cardinality) is the **rank** of the free abelian group. It's possible to prove that the rank of a free abelian group is well-defined.

Theorem. Let G be a finitely generated abelian group.

(a) $G = T \times F$, where T is the torsion subgroup and F is a free abelian group.

(b) The rank of F is uniquely determined by G.

(c) The torsion part T can be written as a direct sum of cyclic groups in the following ways. Each decomposition is unique (in the first case, up to the order of the factors):

$$T \approx \mathbb{Z}_{{p_1}^{r_1}} \times \mathbb{Z}_{{p_2}^{r_2}} \times \cdots \times \mathbb{Z}_{{p_n}^{r_n}}.$$

$$T \approx \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}, \qquad 1 \le d_1 \mid d_2 \mid \cdots \mid d_m.$$

In the first case, the p's are primes (not necessarily distinct), and $r_i > 0$ for all i. The first case is called a **primary decomposition** while the second case is called an **invariant factor decomposition**. □

The proof of this result is outside the scope of this course. But I should mention that it is related to the **Jordan canonical form** and **rational canonical form** that you may have seen in linear algebra. The structure theorem for finitely generated abelian groups and the results on canonical forms are special cases of a more general structure theorem: The *structure theorem for finitely generated modules over a principal ideal domain*.

structure theorem
for
finitely generated modules
over a PID

$\swarrow$ $\searrow$

structure theorem for finitely generated abelian groups	rational and Jordan canonical forms

Let's concentrate for now on the case of a *finite* abelian group. Since any factor of $\mathbb{Z}$ would make the group infinite, there can't be any $\mathbb{Z}$'s in the decomposition. The result then says that every finite abelian can be written as

$$\mathbb{Z}_{{p_1}^{r_1}} \times \mathbb{Z}_{{p_2}^{r_2}} \times \cdots \times \mathbb{Z}_{{p_n}^{r_n}}.$$

Here the p's are primes and the r's are positive integers (**primary decomposition**).

Alternatively, you can write the same group as

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}.$$

In this case, the d's are positive integers and $d_1 \mid \cdots \mid d_m$ (**invariant factor decomposition**).

Example. (**Listing all the primary and invariant factor decompositions**) Find the primary decompositions and corresponding invariant factor decompositions for all abelian groups of order 360.

First, factor 360 into a product of primes: $360 = 2^3 \cdot 3^2 \cdot 5$.

Next, write each prime power in all possible ways:

$$2^3 : \quad 2^3, 2 \cdot 2^2, 2 \cdot 2 \cdot 2$$

$$3^2 : \quad 3^2, 3 \cdot 3$$

$$5 : \quad 5$$

You get the primary decompositions by using one of the 2^4 factorizations, one of the 3^2 factorizations, and the lone 5. I'll list the possibilities below, together with the corresponding invariant factor decompositions.

Primary decomposition	**Invariant factor decomposition**
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{30}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{90}$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_6 \times \mathbb{Z}_{60}$
$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_{180}$
$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_3 \times \mathbb{Z}_{120}$
$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_{360}$

The two groups in each row are *isomorphic* — they're "the same" as groups.

Here's an example which shows how I got the invariant factor decompositions. Consider $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$. Write the numbers for each prime in a row, right-justified:

$$\begin{array}{ccc} 2 & 2 & 2 \\ & 3 & 3 \\ & & 5 \\ \hline 2 & 6 & 30 \end{array}$$

Multiply the numbers in each column. These give the numbers for the invariant factor decomposition. Note that 2 divides 6 and 6 divides 30. □

Example. (**Finding the primary and invariant factor decompositions for a specific group**) Find the primary decomposition and invariant factor decomposition for $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{18}$.

First, I take each of the factors apart into direct products of groups of prime power order.

$$\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{18} \approx \mathbb{Z}_4 \times (\mathbb{Z}_4 \times \mathbb{Z}_3) \times (\mathbb{Z}_2 \times \mathbb{Z}_9).$$

I'm using the fact that $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$ if and only if m and n are relatively prime. Thus, $\mathbb{Z}_{12} \approx \mathbb{Z}_4 \times \mathbb{Z}_3$ because 3 and 4 are relatively prime.

I can't replace $\mathbb{Z}_4$ with $\mathbb{Z}_2 \times \mathbb{Z}_2$ because 2 is not relatively prime to 2 (2 and 2 have the common factor 2!).

Thus, the primary decomposition is

$$\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9.$$

Next, I find the invariant factor decomposition:

$$\begin{array}{ccc} 2 & 4 & 4 \\ & 3 & 9 \\ \hline 2 & 12 & 36 \end{array}$$

So the invariant factor decomposition is

$$\mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{36}.$$

Note that 2 divides 12 and 12 divides 36. □

Example. (**Finding primary decompositions satisfying a condition on orders of elements**) Suppose G is an abelian group of order 24, and no element has order greater than 12. What are the possible primary decompositions for G?

Since $24 = 2^3 \cdot 3$, the primary decompositions for abelian groups of order 24 are

$$\mathbb{Z}_8 \times \mathbb{Z}_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Let $(a, b, c) \in \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$. Then

$$12(a, b, c) = (12a, 12b, 12c) = (0, 0, 0).$$

Therefore, no element of $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ has order greater than 12.

Let $(a, b, c, d) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Then

$$12(a, b, c, d) = (12a, 12b, 12c, 12d) = (0, 0, 0, 0).$$

Therefore, no element of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ has order greater than 12.

However, for $(1, 1) \in \mathbb{Z}_8 \times \mathbb{Z}_3$, I have

$$12(1, 1) = (4, 0) \neq (0, 0).$$

So $(1, 1)$ does not have order less than 12 — in fact, it has order 24.

Therefore, the possible primary decompositions for G are $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. □
