Structure of Finitely Generated Abelian Groups

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

Abstract

In this we state and prove a result which classifies all finitely generated abelian groups.

Theorem 1 (Structure of abelian groups)**.** *Every finitely generated abelian group can be written as a direct sum of cyclic groups of prime power order and infinite cyclic. The summands are determined up to isomorphism and order.*

Proof. Let A be a finite abelian group (written additively). Let the order n of G be written as $n = p_1^{m_1} \cdots p_k^{m_k}$ into powers of distinct primes. Let A_i be the set of elements $x \in A$ whose order is a power of p_i. Then it is easy to see that A_i is a subgroup of A.

We claim that $A = A_1 \oplus \cdots \oplus A_k$.

Let $q_i := p_1^{m_1} \cdots \widehat{p_i^{m_i}} \cdots p_k^{m_k}$. Then $q_1, \cdots, q_k$ have no common factors. Hence there exist integers t_i such that $t_1 q_1 + \cdots + t_k q_k = 1$. Given any $x \in A$, we write $x = x_1 \cdots + x_k$ where $x_i = t_i q_i x$. Note that $p_i^{m_i} x_i = t_i p_i^{m_i} q_i x = t_i n x = 0$ so that $x_i \in A_i$. Thus we have shown that $A = A_1 + \cdots + A_k$. This sum is direct since any element of $A_2 + \cdots + A_k$ has order relatively prime to p_i.

To complete the proof for the case of finite abelian groups, it is enough to show that any abelian group A of prime power oder, say p^k is a direct sum of cyclic groups and that the number of summands of a given order is uniquely determined.

If A is cyclic, there is nothing to prove. So, assume that A is not cyclic. Let B be a cyclic subgroup of maximal order p^r generated, say, by b. We claim that there exists an subgroup C of order p such that $B \cap C = \{0\}$.

Let $x \in A \setminus B$. Let the order of $x + B$ in A/B be p^s. Note that $s \geq 1$. Hence $p^s x \in B$ so that $p^s x = mb$ for some integer m. Now, we observe that

$$p^{r-s} mb = p^{r-s} p^s x = p^r c = 0, \text{ thanks to the maximality of } r.$$

Hence we conclude that p^r divides $p^{r-s}m$. It follows that p divides m, say, $m = pm'$. Consider $c := p^{s-1}x - m'b$. Clearly, c has order p. By the choice of x, we conclude that $c \notin B$. The subgroup C generated by c is as desired.

We now claim that there exists a subgroup D such that $A = B \oplus D$. We prove this by induction on $|A|$. Let C be the subgroup just found above. Consider the quotient group

$\overline{A} := A/C$. Then as $B \cap C = 0$, we conclude that the image $\overline{B}$ of B in $\overline{A}$ will have the same order as B and hence is cyclic of maximal order p^r. By induction , there exists a subgroup $\overline{D} \leq \overline{A}$ such that $\overline{A} = \overline{B} \oplus \overline{D}$. Let D be the inverse image of $\overline{D}$ under the quotient map $A \to \overline{A}$. It is obvious that $A = B + D$. We claim that the sum is direct. If $x \in B \cap D$, then $x + C \in (\overline{D} \cap \overline{B} = 0$, hence $x \in C$. Thus, $B \cap D \subset C$. Therefore, $B \cap D = (B \cap D) \cap C \subset B \cap C = 0$.

Now an induction on $|A|$ yields the desired decomposition. Also note that if the number of elements whose order divides p^i is n_i, then there are n_i/n_{i-1} summands of order p^i.

Now let us assume that A is a finitely generated group such that no nontrivial element is of finite order. Consider a set $\{a_1, \cdots, a_n\}$ of generators of least cardinality. Assume that there exists a relation $m_1a_1 + \cdots + m_na_n = 0$. We may assume that m_i's have no common factor other than 1. For, if $d > 1$ is their GCD, writing $m_i = n_id$, we see that $x := \sum_i n_ia_i$ is such that $d(\sum_i n_ia_i) = 0$. If $x \neq 0$, then x is an element of finite order, a contradiction to our assumption. So $x = 0$. This gives a relation among a_i's as we wanted, namely, $\sum_i n_ia_i = 0$ with no common factor of n_i's.

There exists an invertible matrix $C = (c_{ij})$ with integral entries of which $(m_1, \ldots, m_n)$ is the first row. (Why?)

Let $b_i := \sum_j c_{ij}a_j$. Then $\{b_i : 1 \leq i \leq n\}$ generates A. But then $b_1 = 0$ so that $\{b_j : 2 \leq j \leq n\}$ is a set of generators of A with $n - 1$ elements. This contradicts our assumption on the minimality of n. Thus we see that there is no nontrivial relation between the a_i's. Hence we have an isomorphism $\varphi\colon \mathbb{Z}^n \to A$ by setting $\varphi(m_1, \ldots, m_n) := m_1a_1 + \cdots + m_na_n$. That is, A is a direct sum of n copies of the infinite cyclic group $\mathbb{Z}$. The number n is uniquely determined by the relation $[A : 2A] = 2^n$.

Finally, let A be any finitely generated abelian group. Let T be the torsion subgroup consisting of elements of finite order. Then A/T is a finitely generated abelian with no nontrivial elements of finite order and hence is isomorphic to $\mathbb{Z}^n$. Let $a_1, \ldots, a_n$ be any elements A whose images is a set of free generators of A/T. Let B be the subgroup generated these elements. Then $A = B \oplus T$. By the first part, T is a direct sum of cyclic groups of prime power order while by the second part B is a direct sum of infinite cyclic groups. This completes the proof of the theorem. □

Corollary 2. *Every finite abelian group can be written as a direct sum of cyclic groups:* $A = B_1 \oplus \cdots \oplus B_r$ *where* $|B_i|$ *divides* $|B_{i+1}|$.

Proof. We saw in the last theorem that A is a direct sum of cyclic groups of prime power orders, for distinct primes. It is easy to see that the direct sum of cyclic groups of prime power orders p^r and q^s where p and q are distinct primes is again a cyclic group. Collecting cyclic groups of prime power order of the highest power together and then next highest and so on, we get the decomposition as in the corollary. □

Remark 3. The proofs above are from *Basic Algebra* by P.M. Cohn.

Theorem 4 (Fundamental Theorem of F.G. Abelian Groups)**.** *Let A be a finitely generated abelian group. Then A can be written as a direct sum of finite number of cyclic groups*

$$A = C_1 \oplus \cdots \oplus C_k,$$

such that either all C_j's are all infinite or for some $j \leq k$, C_1, $C_2, \ldots, C_j$ are of order $m_1, \ldots, m_j$ respectively with $m_1 | m_2 \cdots | m_j$ and $C_{j+1}, \ldots, C_k$ are infinite.

Proof. Let k be the smallest number such that A is generated by a set of k elements. We prove the result by induction on k. If $k = 1$, then A is cyclic and the result is true in this case. So, we assume that $k \geq 2$ and that the result is true for any abelian group generated by a set of r elements with $1 \leq r \leq k-1$.

We first consider the case when A admits a set of k generators $\{a_1, \ldots, a_k\}$ which have no relation, that is, if $m_1 a_1 + \cdots + m_k a_k = 0$, then each $m_i = 0$. This implies that each $x \in A$ can be written as $x = \sum_i x_i a_i$ for unique integers x_i. Then the map $\varphi \colon \mathbb{Z}^k \to A$ as follows: $\varphi(m_1, \ldots, m_k) := m_1 a_1 + \cdots + m_k a_k$ is an isomorphism. In particular, $A = C_1 \oplus \cdots \oplus C_k$ where C_i is the infinite cyclic group generated by a_i.

Let us now assume that A does not have the property (in the first line of the last paragraph) stated above. That is, given any set $\{a_1, \ldots, a_k\}$ of generators of A, there exist integers x_i, not all of them zero, such that $\sum_i x_i a_i = 0$. If such a relation holds, then $-\sum_i x_i a_i = 0$, so we may assume that at least one of the x_i's is positive.

Consider now the set S of all generators with k elements. Let S denote the set of all $(x_1, \ldots, x_k) \in \mathbb{Z}^k$ such that (i) $x_i > 0$ for some i and (ii) there exists a generating set $\{a_1, \ldots, a_k\}$ with $x_1 a_1 + \cdots + x_k a_k = 0$. Let m be the least positive integer that occurs as a component in any k-tuple in S. By permuting the set of generators, we may assume $m = m_1$, the first coordinate. That is, there exists a generating set $\{a_1, \ldots, a_k\}$ such that $m_1 a_1 + \cdots + m_k a_k = 0$. If $\{b_1, \ldots, b_k\}$ is any generating set and if $\sum_i y_i b_i = 0$, then $m_1 \leq y_i$ for any i with $y_i > 0$.

Claim 1: With the assumption as above, we have m_1 divides each of m_i .

For, let us write $m_i = q_i m_1 + r_i$, with $0 \leq r_i < m_1$. Consider $b_1 := a_1 + q_2 a_2 + \cdots + q_k a_k$. We claim that $\{b_1, a_2, \ldots, a_k\}$ is a generating set. For, $a_1 = b_1 - q_2 a_2 - \cdots - q_k a_k$ so that a_1 lies in the subgroup generated by $\{a_2, \ldots, a_k\}$. Hence the set $\{b_1, a_2, \ldots, a_k\}$ generates A. Also, we have $m_1 b_1 + r_2 a_2 + \cdots + r_k a_k = 0$. By the 'minimality' assumption on m_1, it follows that $r_2 = \cdots = r_k = 0$. Hence the claim that m_1 divides m_j is established.

In particular, we have $m_1 b_1 = 0$. We also infer that m_1 is the order of the element b_1. For if m is the order of b_1, then $m b_1 + 0 a_2 + \cdots + 0 a_k = 0$ shows that $m_1 \leq m$. Hence the subgroup C_1 generated by b_1 is cyclic of order m_1.

Let A_1 be the subgroup generated by $\{a_2, \ldots, a_k\}$. Clearly, $A = C_1 + A_1$. We claim that the sum is direct. Suppose a nonzero $b \in C_1 \cap A_1$. Then b is of the form $x_1 b_1$ for some $0 < x_1 < m_1$. There exist integers $x_2, \ldots, x_k$ such that $x_1 b_1 = x_2 a_2 + \cdots + x_k a_k$. This leads us to conclude that the relation $x_1 b_1 - x_2 a_2 + \cdots + x_k a_k = 0$ holds among the set of generators $\{b_1, a_2, \ldots, a_k\}$. This contradicts our minimality assumption on m_1. This contradiction proves our claim that $A = C_1 \oplus A_1$.

The group A_1 is finitely generated by the minimal set $\{a_2, \ldots, a_k\}$. Hence, by induction hypothesis, we can write

$$A_1 = C_2 \oplus \cdots \oplus C_k,$$

where C_i are cyclic, all of which are either infinite cyclic or there exists $2 \leq j \leq k$ such that for each $2 \leq i \leq j$, the group C_i is cyclic of order m_i with $m_2|m_3|\cdots|m_j$ and C_i is infinite cyclic for $i > j$.

Let b_i be a generator of C_i for $2 \leq i \leq k$. Let b_2 be of finite order m_2. Then $m_1 b_1 + m_2 b_2 + 0b_3 + \cdots + 0b_k = 0$. The argument of Claim 1 shows that m_1 divides m_2. This completes the proof of the theorem. □

If A is finite, then all the cyclic groups C_i, $1 \leq i \leq k$ are finite. The next theorem says that their orders m_i are uniquely determined by the requirement $m_1|m_2|\cdots|m_k$.

Theorem 5. *Let A be a finite abelian group of order n. Then there exist a unique set of positive integers $m_1|m_2\cdots|m_k$ such that there exist subgroups C_i of A with $|C_i| = m_i$ for $1 \leq i \leq k$ with $A = C_1 \oplus \cdots \oplus C_k$. Consequently, we have*

$$A \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}.$$

Proof. We need only prove the uniqueness of the integers $M - 1, \ldots, m_k$. To this end, let

$$A = C_1 \oplus \cdots \oplus C_k = D_1 \oplus \cdots \oplus D_l,$$

where C_i, D_j are cyclic subgroups of A with
$|C_i| = m_i$, $m_1|m_2\cdots|m_k$ and $|D_j| = n_j$, $n_1|n_2\cdots|n_l$. Assume that $k \leq l$.

Now D_l has an element of order n_l. But the order of any element in $A = \oplus_i C_i$ is at most m_k. Hence $n_l \leq m_k$. By symmetry, $m_k \leq n_l$ so that $m_k = n_l$.

Now consider $m_{k-1}A := \{m_{k-1}a : a \in A\}$. Using the two decompositions of A, we get

$$\begin{aligned} m_{k-1}A &= (m_{k-1}C_1) \oplus \cdots \oplus (m_{k-1}C_k) \\ &= (m_{k-1}D_1) \oplus \cdots \oplus (m_{k-1}D_l). \end{aligned}$$

By hypothesis, m_i divided m_{k-1} for $1 \leq i \leq k-1$. Hence $m_{k-1}C_i = 0$ for $1 \leq i \leq k-1$. We therefore see that $|m_{k-1}A| = |m_{k-1}C_k| = |m_{k-1}D_l|$. It follows that $|m_{k-1}D_j| = 1$ for $1 \leq j \leq l-1$. In particular, for $j = l-1$, we see that n_{l-1} divides m_{k-1}. By symmetry again, we see that m_{k-1} divides n_{l-1} so that $m_{k-1} = n_{l-1}$. Proceeding this way, we see that $m_{k-r} = n_{l-r}$ for $0 \leq r \leq k$. Since $n = m_k \cdots m_1 = n_l \cdots n_{l-k+1} \cdots n_1 = m_k \cdots m_1 n_{l-k} \cdots n_1$ we deduce that $l = k$ and $m_i = n_i$ for $1 \leq i \leq k$. □