# The Fundamendal Theorem of Abelian Groups

Alex Derhacobian

June 16, 2022

## 1 Introduction

This paper is an expository account of the proof of the Fundamental Theorem of Abelian Groups, which states that every finite abelian group is the direct product of cyclic groups. The proof that this paper explores consists of two proofs whose joint results will prove the Fundamental Theorem of Abelian Groups. First, we will prove that every finite abelian group can be expressed as the direct product of $p$-Sylow subgroups. Then we will prove that every $p$-Sylow subgroup can be expressed as the direct product of cyclic groups. By proving these two results, we will have demonstrated the Fundamental Theorem of Abelian Groups.

This result was originally proven by Leopold Kronecker in 1870 and serves great importance in classifying abelian groups. We can see an application in the construction of an isomorphism between $G$ and $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

## 2 Proof

**Theorem 2.1.** *Every finite abelian group is the direct product of cyclic groups*

*Proof.* Before beginning our proof, it is valuable to investigate some preliminary results that will aid us in proving this theorem. Notice that if we are able to demonstrate that Sylow subgroups can be expressed as the direct product of cyclic groups, then we are able to prove the above theorem by demonstrating that any finite abelian group $G$ is the direct product of its Sylow subgroups.

Therefore, we can proceed by proving that every finite abelian group is the direct product of these Sylow subgroups, then demonstrating that every Sylow subgroup

is the direct product of cyclic groups. When this is done, we will have successfully demonstrated that every finite abelian group is the direct product of cyclic groups.

**Lemma 2.2.** *If $G$ is a finite abelian group, then $G$ is isomorphic to the direct product of its Sylow subgroups.*

*Proof.* Let us decompose the order of $G$, denoted as $o(G)$ as the product of distinct primes $p_1, p_2, \dots p_n$. By Sylow's theorem, for every distinct prime $p$ where $p^\alpha \mid o(G)$, then there must exist a subgroup of order $p^\alpha$ in $G$. We know that the number of $p$-Sylow groups in $G$ equal $o(G)/o(N(P))$ where $P$ is any $p$-Sylow group of $G$. But since $G$ is abelian, it must follow that the normalizer of every $p$-Sylow group of $G$ is the entire group $G$. The normalizer of a subgroup $P$ is defined as $N(P) = \{g \in G \mid gP = Pg\}$. It should follow trivially that since $G$ is an abelian group that every element of $G$ commutes with any subgroup of $G$, so $o(N(P))$ for every $p$-Sylow subgroup $P$ of $G$ is equal to the order of the entire group $G$. Therefore, if the number of $p$-Sylow subgroups in a group $G$ is $o(G)/o(N(P))$ and $o(N(P)) = o(G)$, then there is one $p$-Sylow subgroup for every distinct prime divisor of $o(G)$.

Let us define a mapping $\phi$ such that

$$\prod_i P_i \xrightarrow{\phi} G$$

where $\phi(p_{\alpha_1}, p_{\alpha_2}, \dots, p_{\alpha_n}) = p_{\alpha_1} p_{\alpha_2} \dots p_{\alpha_n}$ and such that $p_{\alpha_i}$ is an element of the $p_i$-Sylow subgroup in $G$. It should be obvious that $\phi$ is a homomorphism. Now, we must prove that $\phi$ is an isomorphism. We know that $\phi$ is injective. Furthermore, we can conclude that $\prod P_i$ has the same number of elements as $G$. Therefore, since the direct product of the $p$-Sylow groups of $G$ have the same number of elements as $G$ and $\phi$ is injective, then $\phi$ must be an isomorphism from $G$ to the direct product of its Sylow subgroups. □

We have shown that a finite abelian group is the direct product of its Sylow subgroups. Now we will continue with our proof of the theorem by proving that Sylow subgroups are the direct products of cyclic groups. From this, it will follow that every finite abelian group is the direct product of cyclic groups.

We will proceed by proving this theorem for abelian groups of order $p^n$, where $p$ is prime. This will suffice since if we are able to demonstrate that all such groups are the direct product of cyclic groups, then it will hold for all the $p$-Sylow subgroups of $G$, since they are all abelian groups of order $p^n$. So consider some arbitrary

abelian group $G$ of order $p^n$. Since we want to prove that all $p$-Sylow groups are the direct products of cyclic groups, our objective is to find elements $a_1, a_2 \ldots, a_k$ in $G$ such that for every element $x$ in $G$, $x$ can be uniquely represented as the product $x = a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_k^{\alpha_k}$. You can think of the cyclic groups being generated by $a_1, a_2, \ldots, a_k$ and $a_i^{\alpha_i}$ be some element of the cyclic group $(a_i)$ for some $i$. Since the order of any subgroup must divide the order of the total group, we can assert that each of these cyclic groups must have order $p^k$ for some $k \leq n$. More precisely, if any element $x$ could be expressed as a direct product of the generating elements $a_1, a_2, \ldots, a_k$ of cyclic subgroups with orders $p^{n_1}, p^{n_2}, \ldots, p^{n_k}$, respectively, and if $n_1 \geq n_2 \geq, \ldots, n_k$, then $p^{n_1}$ is the maximal degree of any element in $G$. Although this seems like a useless result, it will interest us because it will help find $a_1, a_2 \ldots, a_k$ for which a direct product can express any element of $G$.

One more helpful observation is worth noting before continuing with our proof. Considering our discovery about the orders of factors of the direct product, we should find a certain procedure that will help us in finding the values of $a_1, a_2, \ldots, a_k$. Let $a_1$ be an element of highest order $p^{n_1}$ and we will define $A_1 = (a_1)$ as the cyclic group of $a_1$. The quotient group $G/A_1$ will produce all right cosets of $A_1$ with elements of $G$. Since we know that $A_1 = (a_1)$ and $a_1$ is an element of maximal order in $G$, then $a_2$ maps into an element of highest order in $G/A_1$. Upon finding an appriate $a_2$ such that $A_2 = (a_2)$, we can perform a parallel process for $a_3$, which would map into an element of maximal order in $G/A_1A_2$. We continue this process for all such desired $a_1, a_2, \ldots, a_k$. Now that we have a basic understanding of the general mechanics we will use in this proof, we will begin the construction of all such $A_2, A_3, \ldots, A_k$. Additionally, it is also important to recognize that all such subgroups $A_1, A_2, \ldots, A_k$ are distinct, meaning for any such $A_i, A_j$, $i \neq j$, $A_i \cap A_j = (e)$. Although this might not seem important now, it will be crucial later on in this proof.

Now, we can begin our construction of the cyclic subgroups. Let us consider $a_1$ in $G$, where $a_1$ has the highest possible order, $p^{n_1}$, and $A_1 = (a_1)$. As we demonstrated above in the rough sketch of this method, we will choose some element we will denote as $b_2$ in $G$ such that the image $\bar{b_2}$ in $G/A_1$ is of maximal order $p^{n_2}$. But notice that not any choice of $b_2$ in $G$ will produce a cyclic group $A_2$ from which we can build a direct product. Recall that if $G$ is the direct product of $N_1, N_2, \ldots, N_k$, then $N_i \cap N_j = (e)$ for all $i \neq j$. Therefore, it must be true that for the $b_2$ that we chose that $A_1 \cap (b_2) = (e)$. In other words, since the image of $b_2$ in $G/A_1$ has order $p^{n_2}$, it would mean that for the element $b_2A_1 \in G/A_1$, $b_2^{p^{n_2}}A_1 = A_1$. By our mechanism of choosing $b_2$, we know that $b_2^{p^{n_2}}$ is the first power of $b_2$ to fall into $A_1$.

From this and the fact that $b_2^{p^{n_2}} A_1 = A_1$, it follows that $b_2^{p^{n_2}} \in A_1$, where $A_1$ is the identity element of $G/A_1$.

Since $b_2^{p^{n_2}} \in A_1$, $b_2^{p^{n_2}} = a_1^i$, where $a_1^i$ is some power of $a_1$ in the cyclic group $A_1 = (a_1)$. In this equation, we can raise each side to the power of $p^{n_1-n_2}$, which would result in $(a_1^i)^{p^{n_1-n_2}} = (b_2^{p^{n_2}})^{p^{n_1-n_2}} = b_2^{p^{n_1}} = e$. This also means that $(a_1^i)^{p^{n_1-n_2}} = e$. In other words, the order of $a_1$ is some divisor of $ip^{n_1-n_2}$. We know that since $(a_1)$ has order $p^{n_1}$, so it must be true that $p^{n_1} \mid ip^{n_1-n_2}$, or equivalently, $p^{n_2} \mid i$. This means that we can express $i$ in terms of $jp^{n_2}$ for some $j$. But we must remember that we assumed that $b_2^{p^{n_2}} = a_1^i$, so it must follow that $b_2^{p^{n_2}} = a_1^i = a_1^{jp^{n-2}}$. Now, we must find a value in $G$ with order $p^{n_2}$ as we originally desired. If we denote this element $a_2$, it must be true that $a_2^{p^{n_2}} = e$. If we set $a_2$ to $a_1^{-j} b_2$, then it follows that $a_2^{p^{n_2}} = (a_1^{-j} b_2)^{p^{n_2}} = (a_1^{-j})^{p^{n_2}} b_2^{p^{n_2}}$. Recall that from the above expression $b_2^{p^{n_2}} = a_1^i = a_1^{jp^{n_2}}$, it follows that $b_2^{p^{n_2}} = a_1^{jp^{n_2}}$, so it must be true that $(a_1^{-j})^{p^{n_2}} = b_2^{-p^{n_2}}$. Therefore, it follows that $a_2^{p^{n_2}} = (a_1^{-j})^{p^{n_2}} b_2^{p^{n_2}} = b_2^{-p^{n_2}} b_2^{p^{n_2}} = e$. This $a_2$ is the element of interest for our generation of $A_2$. For $A_1A_2$ to be a direct product, $A_1 \cap A_2 = (e)$. Using our construction of $a_2$, we will be able to prove this true. Suppose for the sake of contradiction that $A_1 \cap A_2 \neq (e)$, or rather that there exists some $t < p^{n_2}$ such that $a_2^t \in A_1$. Since we claimed that $a_2 = a_1^{-j} b_2$, an equivalent assumption for our contradiction is that $(a_1^{-j} b_2)^t \in A_1$. This would require that $b_2^t \in A_1$. But by our choice of $b_2$, this forces $p^{n_2} \mid t$ and since $a_2 p^{n_2} = e$, it must follow that $a_2^t = e$. Therefore, we have shown that $A_1 \cap A_2 = (e)$.

We have successfully found elements $a_1$ and $a_2$ in $G$ with orders $p^{n_1}$ and $p^{n_2}$, respectively, so that they form cyclic groups $A_1$ and $A_2$ such that $A_1 \cap A_2$. We must continue this process until we find a collection of cyclic groups $A_1, A_2, \ldots, A_k$ which form a direct product that can produce any element in $G$. Let us continue with this same process for one more step to find an $a_3$ that satisfies the above conditions.

Consider some element $b_3$ in $G$ such that $b_3$ maps into $G/(A_1A_2)$. We will denote the order of the image of $b_3$ in $G/(A_1A_2)$ as $p^{n_3}$, and since $b_3$ has an image in $G/(A_1A_2)$ of order $p^{n_3}$, we can claim that $n_1 \geq n_2 \geq n_3$. We can make this conclusion based on our selection of $p^{n_2}$ above, which indicates that $b_3^{p^{n_2}} \in A_1$. Consequently, $b_3^{p^{n_2}}$ must also exist in $A_1A_2$ as a result. If we claim that $b_3^{p^{n_3}} \in A_1A_2$, then it certainly must be true that $b_3^{p^{n_3}} = a_1^i a_2^j$ for some $i$ and $j$. It must follow that $p^{n_3} \mid i$ and $p^{n_3} \mid j$. We can derive this from the fact that since $b_3^{p^{n_2}} \in A_1$, we can rewrite this element as a product of powers of $a_1$ and $a_2$ such that $(a_1^i a_2^j)^{p^{n_2-n_3}} = (b_3^{p^{n_3}})^{p^{n_2-n_3}} = b_3^{p^{n_2}} \in A_1$. From this, we can conclude that $a_2^{i_2 p^{n_1-n_2}} \in A_1$, which would mean that $p^{n_2} \mid i_2 p^{n_2-n_3}$, or

equivalently that $p^{n_3} \mid i_2$. Similarly, in the case where $p^{n_3} \mid i$, we can demonstrate this through the fact that $b_3^{p^{n_1}} = e$. Since we know this fact, we can rewrite it as a direct product of of elements of $A_1$ and $A_2$ such that $(a_1^i a_2^j)^{p^{n_1-n_3}} = b_3^{p^{n_1}} = e$. Therefore, $a_1^{i_1(p^{n_1-n_3})} \in A_1 \cap A_2 = (e)$, so we can conclude that $a_1^{i_1(p^{n_1-n_3})} = e$. From this, we can conclude that $p^{n_3} \mid i_1$. Let us denote $i_1, j_1, i_2, j_2$ such that $i_1 = j_1 p^{n_3}$ and $i_2 = j_2 p^{n_2}$. For notational convenience, we will discard the previous $a_1^i a_2^j$ and consider some $b_3$ expressed as the direct product $a_1^{j_1} a_2^{j_2}$. It follows that $b_3^{p^{n_3}} = a_1^{j_1 p^{n_3}} a_2^{j_2 p^{n_3}}$. Let us consider some element $a_3 = a_1 - j_1 a_2^{-j_2} b_3$. We will form a cyclic subgroup as we did above with $a_2$ such that $A_3 = (a_3)$. To preserve the theorem we are trying to prove, note that $a_3$ has order $p^{n_3}$. We claim that $A_1 \cap (A_2 A_3) = (e)$. Let us consider the alternative case where $a_3^t \in A_1 A_2$. In this case, it would follow that $(a_1^{-j_1} a_2^{-j_2} b_3)^t \in A_1 A_2$, which would mean that $b_3^t \in A_1 A_2$. But from the fact that $p^{n_3} \mid t$ and since $a_3^{p^{n_3}} = e$, we would have that $a_3^t = e$. Therefore, we can conclude that $A_3 \cap (A_1 A_2) = (e)$.

We can continue with this method to produce cyclic groups $A_1 = (a_1), A_2 = (a_2), \ldots, A_k = (a_k)$, each of order $p^{n_1}, p^{n_2}, \ldots, p^{n_k}$, respectively where $n_1 \geq n_2, \ldots, n_k$ such that $A_i \cap A_j = (e)$ for every $i \neq j$ and $G = A_1 A_2 \ldots A_k$. In other words, this demonstrates that we can express every $x$ in $G$ as the unique product of $a_1^{\alpha_1}, a_2^{\alpha_2}, \ldots, a_k^{\alpha_k}$ where $a_i^{\alpha_i} \in (a_i) = A_i$.

Therefore, $G$, which we assumed to be a finite abelian group of order $p^n$, is the direct product of cyclic subgroups $A_1, A_2, \ldots, A_k$, and since we demonstrated that all finite abelian groups are a direct product of $p$-Sylow subgroups, we can conclude that all finite abelian groups are direct products of cyclic groups. Therefore, the theorem is proved. $\square$