THE FUNDAMENTAL THEOREM FOR FINITE ABELIAN GROUPS: A BRIEF HISTORY AND PROOF.

ANTHONY PIRO

Abstract.

The purpose of this project was to investigate the origins and history of Finite Abelian Group Theory. We will also provide a proof to the Fundamental Theorem of Finite Abelian Groups. The beginnings of Finite Abelian Group Theory can be traced back to the 18th century and followed through to the early 20th century. In this work, we will discuss many well-known mathematicians, such as Lagrange and Gauss, and their connections to finite abelian group theory. This work will also provide an in-depth proof to the Fundamental Theorem of Finite Abelian Groups. This theorem is a structure theorem, which provides a structure that all finite abelian groups share. The proof to the Fundamental Theorem of Finite Abelian Groups relies on four main results. Throughout the proof, we will discuss the shared structure of finite abelian groups and develop a process to attain this structure.

1. Brief History of Group Theory

The development of finite abelian group theory occurred mostly over a hundred year period beginning in the late 18th century. During this time, mathematics saw a return of the axiomatic way of thinking, an increase in rigor across the field, and a greater degree of abstraction in mathematics. Many of the early properties of groups were discovered by happen stance as they were stumbled upon during studies of different mathematical disciplines. We will discuss several mathematicians and there contributions to finite abelian group theory. It is important to note that many of the following results were not presented in a group theoretic context, but these results relate directly to finite abelian groups theory.

One of the first mathematicians to work with group theoretic concepts was Joseph-Louise Lagrange (1736-1813). Some of Lagrange's most notable works were on the study of polynomials and their roots. In his article *"Reflexions sur la resolution algebrique des equations"* (1770), Lagrange discussed both theoretical questions, such as the nature and existence of roots and practical procedures for finding roots. Lagrange showed the usefulness of permutations of a polynomial's roots for solving the polynomial. In one result, Lagrange stated that if a polynomial of n variables has its variables permuted in $n!$ ways, the number of different polynomials that are obtained is always a factor of $n!$ [Kle86]. This result is the source of what is now referred to as Lagrange's Theorem, a very important result in group theory. Lagrange was the first person to connect the permutations of a polynomial's roots with a solution to an equation. Although Lagrange did not specifically work with permutations in a group theoretic sense, his ideas can be seen as some of the founding ideas of permutation groups and group theory.

Carl Fredrich Gauss' (1777-1855) results in Number Theory played an influential role in the development of finite abelian group theory. In Gauss' *"Disquisitiones Arithmeticae"* (1801), he presented a summary of the Number Theory results that preceded him and suggested new areas to study in the field. The theory of finite abelian groups may have been developed from the *"Disquisitiones Arithmeticae"*. Gauss writes in a Number Theory context, but establishes many important properties of abelian groups without using group terminology. In the *"Disquisitiones Arithmeticae"* Gauss works with the additive group of integers modulo n, the multiplicative group of integers modulo n relatively prime to n, the group of equivalence classes of binary quadratic forms, and the group of m^{th} roots of unity [DDP10]. Although he is working towards results in Number Theory, he treats the integers he works with as groups. Working with the non-zero integers modulo p Gauss proves the integers modulo p are all a power of a single element i.e. the group $\mathbb{Z}_p^*$ is cyclic. Further more, he also showed the number of generators of $\mathbb{Z}_p^*$ is equal to $\phi(p-1)$ and make references to the order of elements, indirectly [Kle07]. He uses these results to prove Fermat's little theorem. He also shows the converse of Lagrange's Theorem, by stating if there exists an integer x such that $x|(p-1)$ then there exists an element in $\mathbb{Z}_p^*$ that has an order of x [Kle86]. Although Gauss worked with different types of groups, he did not verify common group properties between the groups, nor did he fully grasp the concept of an abstract group. Still his results were pivotal in the development of finite abelian groups.

The work of Lagrange on permutations influenced other mathematicians such as Paolo Ruffini (1765-1822) and Niels Abel (1802-1829). Both Ruffini and Abel proved the unsolvability of the quintic independent from one another. Their results were directly influenced by Lagrange's work. In the process of proving this result, the two mathematicians developed a considerable amount of permutation group theory [Caj91].

Evariste Galois (1811-1832) also worked with permutations and is considered by many to be the founder of permutation group theory [Kle86]. Galois was the first to use the term group, and to him it was a collection of permutations closed under multiplication. He recognized that important parts of an algebraic equation were closely related to properties of a group that is uniquely related to the equation. Galois definition for the group of an equation was:

"Let an equation be given whose m roots are $a, b, c, ...$ There will always be a group of permutations of letters $a, b, c, ...$ which has the following properties:

1.) That every function of the roots, invariant under the substitution of that group, is rationally known, [i.e., is a rational function of the coefficients and any adjoined quantities].
2.) Conversely, that every function of the roots, which can be expressed rationally, is invariant under these substitutions" [Kle07].

In Galois description of this process, he invents the concept of a normal subgroup and uses the normal subgroup for many of his results. Galois work was published in 1846 although it was completed in 1830, as it took time for the mathematicians of the day to understand the material [DDP10]. Galois assisted in the advancement in finite abelian group theory

by leaving many new theorems related to group theory unproved. This in turn challenged mathematicians to prove his results and ultimately help to advance group theory.

Augustin-Louis Cauchy (1789-1857) was another major contributor to permutation groups. He was the first to consider permutation groups as their own subject of study rather than as just a useful tool to solve polynomial equations. In Cauchy's 1815 publication, he fails to give a name for sets of permutations closed under multiplication, but recognizes the importance of them. He does manage to give the name, *divisuer indicatif*, to the number of elements in one of these closed sets. In his 1844 publication, Cauchy defines a group of permutations as follows:

"Given one or more substitutions involving some or all of the elements $x, y, z...$ I call the products, of these substitutions, by themselves or by any other, in any order, derived substitutions. The given substitutions, together with the derived ones, form what I call a system of conjugate substitutions" [Kle86].

Cauchy also proves a very important theorem for finite abelian groups. If a prime p divides the order of a group, then there exists a subgroup of order p [Kle07]. This theorem was stated by Galois but given without proof. It should be noted that these results were presented in the context of permutation groups, not in the context of groups as they are used today.

The culmination of the development of permutation group theory was Marie Ennemond Camille Jordan's (1838-1922) *"Trait des substitutions et des equations algebraique"* (1870). The aim of this publication was to investigate the possible applications for permutations in all the fields of mathematics. In the *"Trait des substitutions et des equations algebraique"* Jordan synthesized the work of Cauchy and Galois. Jordan was able to introduce many fundamental concepts in group theory, such as isomorphisms and homomorphisms for substitution groups [Kle86]. Jordan's work was a building block for group theory and a major development for permutation group theory.

The major contributor to abelian groups was number theory although the major contributions remained implicit until the late 19^{th} century. While studying the units in an algebraic number field in 1846 Johann Peter Gustav Lejeune Dirichlet (1805-1859) was able to establish the group of these units is a direct product of a finite cyclic group and a free abelian group of finite rank [Kle07]. However, this result was presented in a strictly number theoretic sense, but in group terminology translates as stated above.

The first abstract definition of a group was given by Arthur Cayley (1821-1895) in his paper"*On the theory of groups, as depending on the symbolic equation* $\theta^n = 1$", published in 1854. Cayley's definition is as follows:

"A set of symbols $1, \alpha, \beta, ...$ all of them different, and such that the product of any two of them (no matter what order), or the product of any one of them into itself, belongs to that set, is said to be a *group*. These symbols are not in general convertible [commutative],but are

associative. It follows that if the the entire group is multiplied by any one of the symbols, either as a further or nearer factor, [i.e., on the left or on the right] the effect is simply to reproduce the group" [Kle86].

In his paper he gives examples of groups and investigates all groups of orders four and six, and he also determines there is only one group of a given prime order. Cayley's abstract view of mathematics was received well initially, it took another two or three decades before this abstract point of view was accepted.

The work of Cayley influenced mathematician Heinrich Martin Weber (1842-1913). In 1882 Weber presented the following definition for a finite group:

"A system G of arbitrary elements $\theta_1, \theta_2, ..., \theta_h$ is called a group of degree h if it satisfies the following conditions:

(1) By some rule which is designated as composition or multiplication, from any two elements of the same system one derives a new element of the same system. In symbols $\theta_r\theta_s = \theta_t$.
(2) It is always true that $(\theta_r\theta_s)\theta_t = \theta_r(\theta_s\theta_t) = \theta_r\theta_s\theta_t$.
(3) From $\theta\theta_r = \theta\theta_s$ or from $\theta_r\theta = \theta_s\theta$ it follows that $\theta_r = \theta_s$" [Kle07].

Another major contributor to finite abelian group theory, and the the main contributor to the Fundamental Theorem of Finite Abelian groups was Leopold Kronecker (1823-1891). His (1870) paper, "*Auseinandersetzung einiger Eigenshaften der Klassenzahl idealer complexer Zahlen*" implicitly introduces fundamental definitions and theorems for finite abelian groups. The paper's discussion is on algebraic number theory, but Kronecker takes a very abstract approach in his writing. He defined an arbitrary set of elements and defined an operation on them satisfying certain laws. His construction is listed below:

"Let $\theta', \theta'', \theta'''$, ... be finitely many elements such that with any two of them, we can associate a third by means of a definite procedure. Thus, if f denotes the procedure and θ', θ'' are two (possibly equal) elements, then there exists a θ''' equal to $f(\theta', \theta'')$. Furthermore $f(\theta', \theta'') = f(\theta'', \theta')$, $f(\theta', f(\theta'', \theta''')) = f(f(\theta', \theta''), \theta''')$, and if θ'' is different from θ''' then $f(\theta', \theta'')$ is different from $f(\theta', \theta''')$. Once this is assumed, we can replace the operation $f(\theta', \theta'')$ by multiplication $\theta' \cdot \theta''$ provided that instead of equality we employ equivalences. Thus using the usual equivalence symbol "$\sim$", we define the equivalence $\theta' \cdot \theta'' \sim \theta'''$ by means of the equation $f(\theta', \theta'') = \theta'''$" [Kle86].

Notice that we take these same properties as axioms of finite abelian group in today's time. Kronecker was attempting to work out the laws of combination magnitudes. In his attempts, he managed to implicitly define a finite abelian group. His definition was as follows:

(1) "If θ is any "element" of the set under discussion, then $\theta^k = 1$ for some positive integer k. If k is the smallest such then θ is said to "belong to k" [i.e., is of order k]. If θ belongs to k and $\theta^m = 1$, then k divides m.
(2) If an element θ belongs to k, then every divisor of k has an element belonging to it.
(3) If θ and θ' belong to k and k' respectively, and k and k' are relatively prime, then $\theta\theta'$ belongs to kk'.
(4) There exists a "fundamental system" of elements $\theta_1, \theta_2, \theta_3$,... such that the expression $\theta_1^{h_1}\theta_2^{h_2}\theta_3^{h_3} \cdot \cdot$ $(h_i = 1, 2, 3, ..., n_i)$ represents each element of the given set of elements just once. The numbers $n_1, n_2, n_3, ...$ to which, respectively, $\theta_1, \theta_2, \theta_3$, ... belong, are such that each is divisible by its successor; the product $n_1 n_2 n_3 \cdot \cdot$ is equal to the totality of elements of the set" [Kle86].

Although the above implicit definition is not directly applied to finite abelian groups, it can be interpreted as of The Fundamental Theorem of Finite Abelian Groups. Kronecker applied his results to number theoretic topics, but he acknowledged the benefits of the abstract method of thinking he used. His results would allow other mathematicians to formulate the field of abelian group theory.

Kronecker,s discoveries were formulated into explicit group theory results by Ferdinand Georg Frobenius (1849-1917) and L. Stickelberger in their paper, "*On Groups of Commuting Elements*" (1879) [Kle07]. Frobenius and Stickelberger not only developed Kronecker's work, they related the results to other mathematician's results such as Gauss' and Galois'. In this paper, Frobenius and Stickelberger provide a group theoretic proof of The Fundamental Theorem of Finite Abelian Groups, and formulate finite abelian group theory in line with views of modern mathematicians.

2. The Fundamental Theorem for Finite Abelian Groups

We will now discuss the Fundamental Theorem of Finite Abelian Groups. In this section we will provide several concepts necessary to the proof of this theorem.

Theorem 2.1. The Fundamental Theorem for Finite Abelian Groups

Let G be an abelian group of order $n \geq 1$ and let the unique factorization of n into distinct prime powers be :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \text{ with } \alpha_i \geq 1.$$

Then

(1) $G \cong A_1 \times A_2 \times \cdots \times A_k$, *where* $|A_i| = p_i^{\alpha_i}$
(2) *for each* $A \in \{A_1, A_2, ..., A_k\}$ *with* $|A| = p^{\alpha}$,

$$A \cong \mathbb{Z}_{p^{\beta_1}} \times \mathbb{Z}_{p^{\beta_2}} \times \cdots \times \mathbb{Z}_{p^{\beta_t}}$$

with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ *and* $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$ *(where* t *and* $\beta_1, ..., \beta_t$ *depend on* i*)*

(3) *the decomposition in* (1) *and* (2) *is unique i.e. if* $G \cong B_1 \times B_2 \times \cdots \times B_m$ *with* $|B_i| = p_i^{\alpha_i}$ *for all* i*, then* $B_i \cong A_i$ *and* B_i *and* A_i *have the same invariant factors.*

Notice the above theorem outlines a process for decomposing a group G into a direct product of cyclic groups. The proof of this theorem relies on four results, which are discussed below.

Proposition 2.2. The Recognition Theorem for Direct Products

Suppose G *is a group with subgroups* H *and* K *such that:*

(1) H *and* K *are normal in* G*, and*
(2) $H \cap K = 1$.

Then $HK \cong H \times K$.

In order to represent G as a direct product of cyclic groups, we need to be able to split the group into several pieces. The Recognition Theorem for Direct Products provides us with the necessary criteria for splitting. We will now begin the process of decomposition of a group G. The following Theorem is the first step of this decomposition.

Theorem 2.3. The Primary Decomposition Theorem for Finite Abelian Groups

Let G *be an abelian group of order* $n \geq 1$ *and let the unique factorization of* n *into distinct prime powers be :*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then

$$G \cong A_1 \times A_2 \times \cdots \times A_k$$

where $|A_i| = p_i^{\alpha_i}$.

The Primary Decomposition Theorem uses the Fundamental Theorem of Arithmetic to represent the order of a group as a product of primes. The group can then be represented as a direct product of Abelian p-groups, each with prime power order.

Lemma 2.4. *Let* E *be an elementary abelian* p*-group. That is, for all* $x \in E$*, we have* $x^p = 1$*. For all* $x \in E$*, there exists* $M \subseteq E$ *such that* $E = M \times \langle x \rangle$.

Proof.

Let E be an elementary abelian p-group. Let $x \in E$. For the trivial case, if $x = 1$, let $M = E$. Otherwise let M be a subgroup of E of maximal order, subject to the condition that $x \notin M$. Suppose, for purposes of contradiction, that $[E : M] \neq p$. Let $\bar{E} = E/M$. Note that $\bar{E}$ is elementary abelian as for all $xM \in \bar{E}$ we see that:

$$\begin{aligned}(xM)^p &= x^pM \\ &= (1)M \\ &= M.\end{aligned}$$

Since $[E : M] \neq p$, there exists a $\bar{y} \in \bar{E} - \langle \bar{x} \rangle$. Note that $\langle \bar{y} \rangle$ is elementary abelian as for all $y^jM \in \langle \bar{y} \rangle$:

$$\begin{aligned}(y^jM)^p &= y^{jp}M \\ &= (1)M \\ &= M.\end{aligned}$$

Therefore $|yM| = p$. Suppose $\bar{x} \in \langle \bar{y} \rangle$. Therefore $xM = (yM)^j$, with $j \in \mathbb{N}$, and $j < p$. Recall the following result:

Let $a, n \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then there exist $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$.

Therefore since p is prime $\gcd(j, p) = 1$ and there exists $k \in \mathbb{Z}$ with $1 < k < p$ such that $kj \equiv 1 \pmod{p}$. Now we can obtain:

$$\begin{aligned}(xM)^k &= ((yM)^j)^k \\ &= (yM)^{jk} \\ &= (yM)^1 \\ &= yM.\end{aligned}$$

Since we chose $\bar{y} \in \bar{E} - \langle \bar{x} \rangle$, from above we also have $\bar{x} \notin \langle \bar{y} \rangle$.
To show $\langle \bar{y} \rangle$ is a subgroup of E, let $Z = \{z \in E | zM \in \langle \bar{y} \rangle\}$. Then for each $z \in E$,

$$\begin{aligned}(zM)^p &= z^pM \\ &= (1)M \\ &= M.\end{aligned}$$

Thus M is an element of $\langle \bar{y} \rangle$. Let $z_1, z_2 \in Z$, then $z_1 = y^kM$ and $z_2 = y^jM$ for some $k, j \in \mathbb{Z}$. Observe the following:

$$\begin{aligned}(z_1M)(z_2M) &= y^kMy^jM \\ &= y^ky^jMM \text{ (as } E \text{ is abelian.)} \\ &= y^ky^jM \text{ (as } MM = M.) \\ &= y^{k+j}M \\ &= y^lM.\end{aligned}$$

As $\bar{y}$ is cyclic $y^l M \in \langle \bar{y} \rangle$. Therefore $\bar{y}$ is closed under the group operation. Since $|\langle \bar{y} \rangle| = p$ for every $y^j M \in \langle \bar{y} \rangle$, there exists $y^k M \in \langle \bar{y} \rangle$ with $k = p - j$ such that $y^j M y^k M = y^{k+j} M = y^p M = M$. Therefore $\langle \bar{y} \rangle$ contains inverses and is a subgroup of E. As Z contains M, Z contains $\langle y \rangle$, and Z does not contain $\langle x \rangle$ since we chose $\bar{y} \in \bar{E} - \langle \bar{x} \rangle$, we have a subgroup of E larger than M contradicting the maximality of M. Thus $[E : M] = p$. Since M was chosen such that $\langle x \rangle \notin M$ then $\langle x \rangle \cap M = 1$ and $E = M\langle x \rangle$. By the recognition theorem of direct products $E = M \times \langle x \rangle$.

□

We will now work on the abelian p-groups. Our goal is to show these abelian p-groups are a direct product of cyclic groups. The above Lemma provides a strategy for splitting off cyclic pieces.

Lemma 2.5. *If A is an abelian p-group then A is the direct product of cyclic groups.*

Proof.

Let A be an abelian p-group, i.e. for every $x \in A$ we obtain $x^{p^\alpha} = 1$ for some prime p and some $\alpha \geq 1$. Define a mapping $\phi : A \to A$ such that $\phi(x) = x^p$. Note as A is abelian, ϕ is a homomorphism as for every $x, y \in A$:

$$\begin{aligned} \phi(xy) &= (xy)^p \\ &= x^p y^p \\ &= \phi(x)\phi(y) \end{aligned}$$

Denote the kernel of ϕ by K. By definition $K = \{x \in A | x^p = 1\}$. Note that if $x_i \in A$ then $|x_i| = p^{\alpha_i}$. Therefore for each $x_i \in A$ the elements that map to the identity are $\{x_i^{p^{\alpha-1}}, x_i^{2p^{\alpha-1}}, x_i^{3p^{\alpha-1}}, ..., x_i^{(p-1)p^{\alpha-1}}, x_i^{(p)p^{\alpha-1}}\}$. Thus we obtain $K = \langle x_i^{p^{\alpha_i - 1}} \rangle$.

Denote the image of ϕ by H. Note that if $x_i \in A$ then $x_i^p \in H$. Therefore since $\langle x_i \rangle = \{x_i, x_i^2, x_i^3, ..., x_i^{p^\alpha - 2}, x_i^{p^\alpha - 1}\}$, we obtain:

$\langle x_i \rangle^p = \{x_i^p, x_i^{2p}, x_i^{3p}, ..., x_i^{p^{\alpha-1}}, x_i^{p^{\alpha-1}+p}, x_i^{p^{\alpha-1}+2p}, ..., x_i^{p^\alpha - 2p}, x_i^{p^\alpha - p}\} \in H$.

Observe H is a subgroup of A consisting of p^{th} powers.

Since $K = \{x_i^{p^{\alpha-1}}, x_i^{2p^{\alpha-1}}, x_i^{3p^{\alpha-1}}, ..., x_i^{(p-1)p^{\alpha-1}}, x_i^{(p)p^{\alpha-1}}\}$, we obtain $|K| = p$. Thus for each $x \in K$ we have $x^p = 1$. Therefore K is elementary abelian.

Consider A/H. Note for each $x_i \in A$ we have $x_i^p \in H$, therefore if $x_i H \in A/H$ then $x_i^p H = x_i^p H = h_i H = H$. Thus A/H is elementary abelian. Observe $|A : H| = |K|$.

We will now proceed with induction on H. Let $h_1 \in H$ be an element of maximal order.

Let H_1 be a subgroup of H of maximal order subject to the condition that $\langle h_1\rangle \cap H_1 = 1$. Suppose that $\langle h_1\rangle H_1 \neq H$. Choose $\langle h_2\rangle \subset H$ such that $h_2 \notin \langle h_1\rangle$. Suppose $h_2^k \in \langle h_1\rangle$ then $h_2^k = h_1^j$. Since $\langle h_2\rangle$ is cyclic then there exists $l \in \mathbb{Z}$ such that $kl = 1$. Observe:

$$\begin{aligned}(h_2^k)^l = (h_1^j)^l &\implies h_2^{kl} = h_1^{jl} \\ &\implies h_2 = h_1^l\end{aligned}$$

Since $\langle h_1\rangle$ is cyclic $h_1^l \in \langle h_1\rangle$. Since we chose h_2 such that $h_2 \notin \langle h_1\rangle$ then $\langle h_2\rangle \cap \langle h_1\rangle$. Continuing this process we can obtain a subgroup H_1 of H such that $\langle h_1\rangle H_1 = H$. Since H_1 was chosen such that $\langle h_1\rangle \cap H_1 = 1$, the recognition theorem of direct products tells us that $H = \langle h_1\rangle \times H_1$. With induction in mind, if we continue this process on H_1, we can obtain:

$$H = \langle h_1\rangle \times \langle h_2\rangle \times \langle h_3\rangle \times \cdots \times \langle h_r\rangle \quad \text{with } r \geq 1.$$

Note that for $i = 1, 2, 3, ..., r$, the cyclic group $\langle h_i\rangle$ has order of p^α with $\alpha \geq 1$. Since $\langle h_i\rangle$ is cyclic and $\langle h_i\rangle$ has order p^{α_i}, then $\langle h_i\rangle \cong \mathbb{Z}_{p^{\alpha_i}}$. Therefore,

$$\begin{aligned}H &= \langle h_1\rangle \times \langle h_2\rangle \times \langle h_3\rangle \times \cdots \times \langle h_r\rangle \\ &\cong \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \mathbb{Z}_{p^{\alpha_3}} \times \cdots \times \mathbb{Z}_{p^{\alpha_r}}.\end{aligned}$$

By definition of ϕ, there exist elements $a_i \in A$ such that $a_i^p \in h_i$ for $1 \leq i \leq r$. Let $A_0 = \langle g_1, g_2, g_3, ..., g_r\rangle$. Since $\langle h_1\rangle \cap \langle h_2\rangle \cap \langle h_3\rangle \cap \cdots \cap \langle h_r\rangle = 1$ and for each $\langle g_i\rangle \in A_0$ we have $\langle g_i\rangle^p = \langle h_i\rangle$ then $\langle g_1\rangle \cap \langle g_2\rangle \cap \langle g_3\rangle \cap ... \cap \langle g_r\rangle = 1$. Thus by the recognition theorem of direct products,

$$A_0 = \langle g_1\rangle \times \langle g_2\rangle \times \langle g_3\rangle \times \cdots \times \langle g_r\rangle.$$

Consider A_0/H. By properties of quotients $A_0/H = \langle g_1\rangle H \times \langle g_2\rangle H \times \langle g_3\rangle H \times ... \times \langle g_r\rangle H$.

Note that for each $\langle g_i\rangle \subset A_0$, $\langle g_i^p\rangle \subset H$. Therefore $\langle g_i\rangle^p H = \langle g_i^p\rangle H = H$. Thus A_0/H is elementary abelian of rank r. For each $h_i \in H$ we obtain $h_i \cap K = \langle h_i^{p^{\alpha_i - 1}}\rangle$. Note $|h_i^{p^{\alpha_i - 1}}| = p$, therefore $H \cap K = \langle h_1^{p^{\alpha_1 - 1}}\rangle \times \langle h_2^{p^{\alpha_2 - 1}}\rangle \times \langle h_3^{p^{\alpha_3 - 1}}\rangle \times ... \times \langle h_r^{p^{\alpha_r - 1}}\rangle$.

If K is contained in H, then $|K| = |K \cap H| = p^r = |A_0 : H| = |A : H|$. Therefore $A_0 = A$ and the theorem is proved. Assume therefore that K is not a subgroup of H. We will use the bar notation again to denote the passage to the quotient group A/H. Let $x \in K - H$. As $x \in K$ the order of x is p. Observe $x \notin H$ then $|\bar{x}| = p$. Since $A/H = \bar{A}$ is elementary abelian we can use our initial result on elementary abelian p-groups to pick a subgroup $\bar{M}$ of $\bar{A}$ such that $\bar{A} = \bar{M} \times \langle \bar{x}\rangle$. If M is the complete pre-image in A of $\bar{M}$, and since x has order p and $\langle x\rangle \cap M = 1$, by the recognition theorem of direct products $A = \langle x\rangle \times M$. Proceeding with induction on M, we obtain A is the direct product of cyclic groups.

□

The uniqueness of the decomposition of a finite abelian group can be proved by the p^{th} power map as well. From the results above, the Fundamental Theorem of Finite abelian groups is proved [DF04].

Example 2.6. The following is a simple example of the use of the Fundamental Theorem of Finite Abelian Groups. Let G be an abelian group of order 162. Using the Fundamental Theorem of Arithmetic we observe $162 = 2 \cdot 3^4$. From Fundamental Theorem of Finite Abelian Groups G is isomorphic to one of the following groups:

(1) $G \cong \mathbb{Z}_{162}$.
(2) $G \cong \mathbb{Z}_{54} \times \mathbb{Z}_3$.
(3) $G \cong \mathbb{Z}_{18} \times \mathbb{Z}_9$.
(4) $G \cong \mathbb{Z}_{18} \times \mathbb{Z}_3 \times \mathbb{Z}_3$.
(5) $G \cong \mathbb{Z}_6 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

3. The Fundamental Theorem of Finitely Generated Abelian Groups

The Fundamental Theorem of Finite Abelian Groups directly applies to a more general theorem, which accounts for infinite cases as well as finite cases.

Definition 3.1.

(1) A group G is finitely generated if there is a finite subset A of G such that $G = \langle A \rangle$.
(2) For each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of r copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the free abelian group of rank r.

Theorem 3.2. *The Fundamental Theorem of Finitely Generated Abelian Groups*
Let G be a finitely generated abelian group. Then,

(1)
$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s},$$
for some integers $r, n_1, n_2, ..., n_s$ satisfying the following conditions:
- *$r \geq 0$ and $n_j \geq 2$ for all j, and*
- *$n_{i+1} | n_i$ for $1 \leq i \leq s-1$.*

(2) *The expression in (1) is unique: if $G \cong \mathbb{Z}^t \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_u}$, where t and $m_1, m_2, \ldots, m_u$ satisfy the two conditions in (1), then $t = r$, $u = s$, and $m_i = n_i$ for all i.*

References

[Caj91] Florian Cajori. *A history of mathematics*, volume 303. American Mathematical Soc., 1991.

[DDP10] Amy Dahan-Dalmedico and Jeanne Peiffer. *History of Mathematics: Highways and Byways*. 2010.

[DF04] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[Kle86] Israel Kleiner. The evolution of group theory: A brief survey. *Mathematics Magazine*, 59(4):195–215, 1986.

[Kle07] Israel Kleiner. *A history of abstract algebra*. Springer Science & Business Media, 2007.

Georgia College & State University, Department of Mathematics, Milledgeville, GA 31061, United States, steven.piro@bobcats.gcsu.edu