4-22-2015

Structure of Finitely Generated Abelian Groups

Turner J. Pepper
Lake Forest College, peppertj@lakeforest.edu

Structure of Finitely Generated Abelian Groups

Abstract
The fundamental theorem of finitely generated abelian groups describes precisely what its name suggests, a fundamental structure underlying finitely generated abelian groups. As such, it is an important result in group theory, but is considered too complex for the college-level Modern Algebra courses taught at Lake Forest College. I recall wanting a proof when I took the class, but one was not available at our current level, and so I have constructed a proof restricted almost exclusively to concepts encountered in Modern Algebra I. Furthermore, an application to the generation of finite fields and cryptography is presented, as a demonstration of the theorem's utility.

Document Type
Thesis

Distinguished Thesis
yes

Degree Name
Bachelor of Arts (BA)

Department or Program
Mathematics

First Advisor
David Yuen

Second Advisor
Enrique Treviño

Third Advisor
Michael Kash

Subject Categories
Algebra

LAKE FOREST COLLEGE

Senior Thesis

Structure of Finitely Generated Abelian Groups

by

T. J. Pepper

April 22, 2015

The report of the investigation undertaken as a
Senior Thesis, to carry one course of credit in
the Department of Mathematics

_____	_____
Michael T. Orr Krebs Provost and Dean of the Faculty	David Yuen, Chairperson
	_____
	Enrique Treviño
	_____
	Michael Kash

Abstract

The fundamental theorem of finitely generated abelian groups describes precisely what its name suggests, a fundamental structure underlying finitely generated abelian groups. As such, it is an important result in group theory, but is considered too complex for the college-level Modern Algebra courses taught at Lake Forest College. I recall wanting a proof when I took the class, but one was not available at our current level, and so I have constructed a proof restricted almost exclusively to concepts encountered in Modern Algebra I. Furthermore, an application to the generation of finite fields and cryptography is presented, as a demonstration of the theorem's utility.

1 Introduction

In today's society, we are raised to recognize the natural numbers and integers from an early age. In this time, we learn much about basic operations and interactions, such as multiplication or addition, and build a foundation of intuition in keeping with their practice. In broad terms, algebra is the abstraction of this intuition to more general forms. In fact, the abstraction is such that the integers remain an integral part of the resulting work. The primes, positive integers divisible by only themselves and 1, constitute one of the most well-known aspects of the positive integers, with their study stretching back at least as far as the time of Euclid. In accordance with the fundamental theorem of arithmetic, which states that all integers greater than one can be expressed uniquely as powers of primes and their products, primes form a foundation for the multiplication of integers (and even the rationals, with the inclusion of 0 and -1). However, they are also directly related to certain types of algebraic structures, which is what this thesis seeks to address.

The theorem itself, stating that a particular and very common structure can be treated as identical to groups of integers, is therefore an incredibly powerful tool that eases many proofs and manipulations. However, its proof is considered too advanced to be presented in the college level Modern Algebra courses in a reasonable amount of time. As this thesis demonstrates, the techniques certainly exist, but the in-class time required would have too high of a cost for the other material covered. The theorem is, consequently, used without proof for several key parts of the course material.

Although the textbook we used[1] does not include a proof of the theorem, many others[2,3] cover the theorem in at least one of its incarnations. However, the majority of these work in more advanced topics, which are typically modules or principal ideal domains. When I took the course, I recall wanting a proof that I could understand at my current level. In keeping with that desire, I have endeavored to create a proof of the Finitely Generated Abelian Groups Structure Theorem that is accessible at the college level.

As a matter of style, many lemmas and theorems in this proof include motivation sections to describe why they are necessary and how they will be used later in the proof, in order to provide a more consistent framework in which to understand the work.

2 Definitions

Specificity and precision of meaning are crucial in mathematics, and so the definitions needed for the foundation of this work are presented here, including the meanings of several shorthand symbols.

- $|$: divides. Example: $2 \mid 6$.

- $\forall$: for all. Example: $\forall\ n > 1$, n is either prime or composite.
- $\exists$: exists. Example: $\forall$ composite n, $\exists$ prime p such that $p|n$ and $p \neq n$.
- $\in$: in, element of. Example: $1 \in \{1,2,3,4,5\}$.
- $\Rightarrow$: implies. Example: n even $\Rightarrow$ n ends in 0, 2, 4, 6, or 8.
- $\mathbb{R}$: the set of real numbers.
- $A \times B$: Cartesian product of sets A and B. Example: $\mathbb{R} \times \mathbb{R}$, the x-y plane.
- $\mathbb{Z}$: the set of the integers.
- $\mathbb{Z}_n$: the set of the integers modulo n. Example: $\{0,1,2\}$ for $\mathbb{Z}_3$.
- A^n : $A \times A \times ... \times A$, n times. Example: $\mathbb{Z}^2$ for $\mathbb{Z} \times \mathbb{Z}$.
- $\simeq$: isomorphic. Example: The Klein-4 group $\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.
- $\langle x \rangle$: the orbit of x; that is, the set of all powers of x.
- $|S|$: The size of set S. Furthermore, this differentiates between different types of ∞, but the largest sets discussed here are countably infinite. Example: $|\{0, 1, 2\}| = 3$.
- $|a|$: The absolute value of a. Although this overloads the definition of $|...|$, it should be clear both from context and from the capitalization of set names whether the object being referred to is a number or a set. Example: $|-5| = 5$.

A function is a mapping f from set A to set B, where each input from A has exactly one output in B. The following are some important properties used throughout this thesis.

- 1-1 : a function $f : X \to Y$ is one to one if $\forall\ x, y \in X, f(x) = f(y) \Rightarrow x = y$.
- onto : a function $f : X \to Y$ is onto if $\forall\ y \in Y, \exists\ x \in X$ such that $f(x) = y$.
- bijection : a function $f : X \to Y$ is a bijection if it is both 1-1 and onto.

Some immediate results for the finite case and definitions for the infinite case:

- If there is a 1-1 function $f : X \to Y$, then $|X| \leq |Y|$.
- If there is an onto function $f : X \to Y$, then $|X| \geq |Y|$.
- If there is a bijection $f : X \to Y$, then $|X| = |Y|$.

3 Modern Algebra

Modern algebra, as it has been for the past few centuries, is abstract algebra. This includes, but is not limited to, the study of groups, rings, fields, and modules, as well as forms of these with relaxed constraints and axioms. It has been studied extensively for its applications to number theory, solutions to polynomial equations, and other branches of mathematics, in addition to being fascinating material in its own right.

3.1 Binary Operations

A binary operation on a set S is a function that maps two inputs from S back into S. Expressed $\langle S, * \rangle$, a more formal definition is a function $* : S \times S \to S$. The structures discussed herein are typically binary operations, but will require several more properties in order to be of use.

- Identity: A binary operation has an identity, denoted e, if $\exists\ e \in S$ such that $\forall\ x \in S$, $x * e = x = e * x$. A left identity is an element e_L such that $\forall\ x \in S$, $e_L * x = x$, and a right identity is the reverse. There can be multiple identities on a single side, but if there are both a left identity and a right identity, they must be the same element: $e_L = e_L * e_R = e_R$.
- Inverse: An element $x \in S$ has an inverse if there is an element $y \in S$ such that $x * y = y * x = e$. This y is then denoted x^{-1}.
- Associativity: The operation $*$ is associative if $\forall\ x, y, z \in S$, $(x * y) * z = x * (y * z)$. In essence, associativity is the property of being able to evaluate the operations in arbitrary order and achieve the same result. As an aside, although it is not proven here, associativity on a finite set implies the existence of an element x such that $x * x = x$.
- Commutativity: The operation $*$ is commutative if $\forall\ x, y \in S$, $x * y = y * x$. Binary operations do not need to exhibit this property, but it is hugely useful when present.

3.2 Groups

A group is set with a binary operation exhibiting the properties of identity, inverse, and associativity. The prototypical example of a group is addition over the integers:

1. $\langle \mathbb{Z}, + \rangle$ contains an identity: There is an identity element 0 such that $\forall\ x$ in $\mathbb{Z}$, $x + 0 = x$
2. $\langle \mathbb{Z}, + \rangle$ possesses inverses: For all $x \in \mathbb{Z}$, $x + (-x) = 0 = (-x) + x$, and so $-x$ is the inverse of x and is in $\mathbb{Z}$.
3. $\langle \mathbb{Z}, + \rangle$ is associative: Clearly, $\forall\ x, y, z$ in $\mathbb{Z}$, $(x + y) + z = x + (y + z)$.

In fact, groups are defined in a manner intended to extend and build upon our experience with normal operations on numbers. However, integer addition exhibits properties that are not required by the group axioms: $\langle \mathbb{Z}, + \rangle$ is also abelian and cyclic, defined below:

- Abelian: commutative. That is, for all x, y in the group G, $x * y = y * x$. Commutative groups are termed abelian groups after Niels Henrik Abel, who worked in group theory in the 19th century.
- Cyclic: A group G is cyclic if it possesses some generating element g, such that for all $x \in$ G, x is a power of g. A cycle $\langle g \rangle$ is the set produced by enumerating all powers of g: $\langle g \rangle = \{g^n, n \in \mathbb{Z}\}$.

Recalling that the identity element is denoted e, the order of an element x in a group G is defined as the smallest positive integer m for which $x^m = e$. If there is no such positive integer, then order$(x) = \infty$. Example: in $\mathbb{Z}_5$, order$(3) = 5$.

Unless otherwise stated, the operation on a group G will be expressed as $*$. Example: given $a, b \in G, a * b = c$. In cases where the use of the group operation can be easily seen from the context, it will be expressed, instead, as $ab = c$.

3.3 Subgroups

Given a group G, a set H is a subgroup of G if

- $H \subseteq G$.
- H satisfies the group axioms under the inherited operation $*$:
    1. H is closed under $*$. Example: {0,2,4} is closed under $+$ in $\mathbb{Z}_6$, but {0,2,3} is not: $2 + 3 = 5 \notin \{0,2,3\}$.
    2. H inherits the group identity e. For nonempty H, this in general follows from closure and inverses, as $x^{-1}x = e \in H$.
    3. H contains inverses of all of its elements.
    4. $*$ is associative over H. In general, this follows immediately from the fact that $H \subseteq G$, as $*$ is associative for all possible $x, y, z \in G \supseteq H$.

Given that nonempty $H \subseteq G$, it is only necessary to check for closure and inverses to determine that H is a subgroup of G, denoted $H \leq G$.

3.4 Homomorphisms

Given groups A and B, a homomorphism is a function $\phi : A \Rightarrow B$ such that $\forall\ x, y \in A$, $\phi(x *_A y) = \phi(x) *_B \phi(y)$. A and B are called isomorphic if there is a bijective homomorphism from A to B, which allows us to treat A and B as identical, for all typical intents and purposes. For example, $\langle \mathbb{R}, + \rangle \simeq \langle \mathbb{R}^+, * \rangle$ by $\phi(x) = e^x$.

1. Homomorphism: As is commonly known, $\forall\ x, y \in \mathbb{R}$, $\phi(x + y) = e^{x+y} = e^x * e^y = \phi(x) * \phi(y)$.

2. 1-1: Similarly, $\forall\ x, y \in \mathbb{R}$, $\phi(x) = \phi(y) \Leftrightarrow e^x = e^y \Leftrightarrow x = y$.

3. onto: Finally, $\forall\ y \in \mathbb{R}^+$, let $x = \ln(y)$. Then $x \in \mathbb{R}$ and $\phi(x) = y$.

Thus $\langle \mathbb{R}, + \rangle \simeq \langle \mathbb{R}^+, * \rangle$.

The following is a small, but crucial, lemma:

Lemma 3.1. *A group G is cyclic $\Leftrightarrow$*

- *$G \simeq \mathbb{Z}$, if $|G| = \infty$.*
- *$G \simeq \mathbb{Z}_n$, if $|G| = n$.*

Motivation. This lemma allows us to easily choose appropriate subgroups isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$.

Proof. G is cyclic $\Leftrightarrow G = \langle g \rangle$ for some $g \in G$. For finite G, $\phi : \mathbb{Z}_n \Rightarrow G$. For infinite G, $\phi : \mathbb{Z} \Rightarrow G$. Define $\phi(k) = g^k$. Then

1. $\forall\ x, y, \phi(x + y) = g^{(x+y)} = g^x * g^y = \phi(x) * \phi(y)$.

2. $\forall\ x, y, \phi(x) = \phi(y) \Leftrightarrow g^x = g^y \Leftrightarrow x = y$ (to within mod n, if G is finite).

3. $\forall\ y \in G, y = g^x$. Then $\phi(x) = g^x = y$.

This demonstrates the lemma. □

3.5 Normal Subgroups

A normal subgroup H of G is a subgroup with the additional property that, for all $n \in G$, $nHn^{-1} = H$. In abelian groups, all subgroups trivially have this property, because $nHn^{-1} = (nn^{-1})H = H$. However, the property of being normal is important for the following definition, which is not restricted to abelian groups.

3.6 Quotient Groups

Given a group G and a normal subgroup H, the associated quotient group on the right is G/H, read as "G mod H". The set G/H is a set of equivalence classes, defined by products of H and elements of G (so elements of $H = eH$ are equivalent to e in this set). Furthermore, elements of G/H are sets, with $Y \in G/H$ requiring $Y = gH$ for some g in G. In particular, $Y = yH$ for all y in Y.

Lemma 3.2. *Multiplication of elements X, Y of G/H can be performed by multiplication of elements $x \in X$ and $y \in Y$.*

Motivation. This imposes the group structure of G onto the structure of G/H, allowing us to pick useful representatives from cosets to manipulate in G.

Proof. Beginning with representation, $X = xH$, $\forall\ x \in X$: elements $a, b \in G$ are equivalent in G/H if $a = b * h$, for some $h \in H$. Then $x * H$ is precisely the set of elements of G equivalent to x.

Take $x \in X$, $y \in Y$. Then $X*Y = (xH)*(yH) = (xH)*(y*(y^{-1}Hy))$, by the definition of normal subgroups. Continuing, $X*Y = (xH)*(Hy) = x(H*H)y = x(Hy) = x(yH(y^{-1}y)) = (x*y)H$. $\square$

This allows us to treat operating in G/H as operating in G, with the additional caveat that we always have a product of H, and enables us to arbitrarily choose advantageous elements of $X \in G/H$ to treat as representatives of X.

3.7 Direct Products

Given groups A and B with operations $*_A$ and $*_B$, respectively, the direct product $A \times B$ is the set $\{(a, b)$ such that $a \in A, b \in B\}$, with the operation $*$ defined by $(a_1, b_1)*(a_2, b_2) = (a_1 *_A a_2, b_1 *_B b_2)$.

An important result of this definition is the property that, given groups A and B, their direct product is also a group. The A and B portions of the elements of $A \times B$ do not interact, so the operation preserves the original closure, associativity, and identities of the original groups for each component.

When A and B are subgroups of another group G and there is an isomorphism $\phi : A \times B \to G$ defined by $\phi((a, b)) = a * b$, then G is the internal direct product of A and B.
A useful lemma, not proven here, is that for normal subgroups A and B of G, G is the internal direct product of A and $B \Leftrightarrow$

1. $G = AB = \{a * b$, for $a \in A$ and $b \in B\}$
2. $A \cap B = \{e\}$

3.8 Sylow Theorems

The Sylow Theorems are a set of three theorems on the existence and properties of subgroups of particular sizes for any finite group. For any finite group G of size m, for any prime power p^k such that $m = p^k * n$ and p does not divide n (so p^{k+1} does not divide m), the following are true:

1. There exists a subgroup of G with size p^k (called a Sylow p-subgroup). This is the only one of the theorems that will be used here, and it will be used without proof, although the proof is much shorter and simpler than this work.

2. For any two p-subgroups H, K of G, $gHg^{-1} = K$ for some $g \in G$.

3. Let n_p be the number of Sylow p-subgroups of G. Then

   - $n_p \mid |G|/p^k$
   - $n_p = 1 \bmod p$
   - $n_p =$ the index of the normalizer of any Sylow p-subgroup H in G (not described here)

3.9 Finitely Generated

A finitely generated group is a group G that possesses a finite set of elements $\{g_1, ..., g_k\}$, referred to as generators, such that every element of G can be expressed as a product of powers of the generators and their inverses. Trivially, any finite group is finitely generated, as we can simply take the generating set to be the entire group. The quintessential example of an infinite finitely generated group is $\langle \mathbb{Z}, + \rangle$, which is generated by $\{1\}$. To demonstrate this, it is sufficient to note that all integers are multiples of 1 or -1, and so $\{1\}$ generates $\langle \mathbb{Z}, + \rangle$.

Lemma 3.3. *Any subgroup of $\mathbb{Z}^k$ is finitely generated.*

Motivation. There is a homomorphism from $\mathbb{Z}^k$ onto any finitely generated abelian group, and homomorphisms preserve properties of sets such as being subgroups and being finitely generated. In conjunction with lemma 3.4, this allows us to prove tha all subgroups of finitely generated abelian groups are themselves finitely generated. This will later allow us to prove that any finitely generated abelian group has a maximal cyclic subgroup, which is vital to the proof.

Proof. This shall be proven by induction on k. Clearly, any subgroup of $\mathbb{Z}$ is finitely generated, since $H \leq \mathbb{Z} \Rightarrow H = \{e\}$ or $H = n\mathbb{Z}$, for some $n \in \mathbb{Z}$. As both of these are finitely generated, all subgroups of $\mathbb{Z}$ are finitely generated.

For the induction, assume that subgroups of $\mathbb{Z}^{k-1}$ are finitely generated.
Given that, for x in $\mathbb{Z}^k$, $x = (x_1, x_2, ..., x_k)$, define $\phi : \mathbb{Z}^k \to \mathbb{Z}^{k-1}$ by $\phi(x) = (x_1, ..., x_{k-1})$. This is

clearly a homomorphism, because the k^{th} index does not interact with the first $k-1$ indices. For any subgroups H of $\mathbb{Z}^k$ such that $h_k = 0$ for all $h \in H$, ϕ is a bijection from H onto $\phi[H] \leq \mathbb{Z}^{k-1}$, and so H is isomorphic to $\phi[H]$. By the induction hypothesis, $\phi[H]$ is finitely generated, forcing H to be finitely generated by isomorphism.

This leaves H such that H contains elements with nonzero entries in the k^{th} index. The integers and $\mathbb{Z}^k$ are countably infinite, which, by definition, means that we can index their elements with the natural numbers. Consequently, we can order the elements of H to be $\{{}_1h, {}_2h, {}_3h, ...\}$ such that every $h \in H$ is assigned a finite index and ${}_1h_k$ (the k^{th} index of ${}_1h$) is nonzero.

Define the sequence $a_i = \gcd({}_1h_k, {}_2h_k, ..., {}_ih_k)$. The purpose of forcing ${}_1h_k$ to be nonzero is to ensure that a_i exists for all i. According to the definition of a_i, $a_{i+1}|a_i$, so $\{a_i\}$ is monotonically decreasing. Furthermore, $\{a_i\}$ is bounded above by $a_1 =_1 h_k$ and below by 1, and so $\{a_i\}$ converges to some a. Then $\exists\ n$ such that $|a_n - a| < 1$, which forces $a_n = a$ because of the restriction of a_i to the integers for all i. Furthermore, for every ${}_ih \in H$, $a_i|{}_ih_k$, and so this result divides the k^{th} index of every element of H.

By application of the Euclidean Algorithm, there exists an $x \in H$ such that $x_k = a$. Let $K = \{h \in H$ such that $h_k = 0\}$. Then K is a subgroup of H with only zero entries in the k^{th} index, and so is isomorphic to its image under the earlier homomorphism ϕ, forcing K to be finitely generated by the induction hypothesis. All that remains is to show that $H \simeq K \times \langle x \rangle$.

Take $h \in H$. Then $x_k = a|h_k$, by construction, and so $[h * x^{-h_k/a}]_k = 0$, causing it to be contained in K. Thus $H = K\langle x \rangle$. $K \cap \langle x \rangle = \{h \in K$ such that $h = x^n$, for some $n\}$. However, such an h exists in K if and only if $0 = [x^n]_k = n * x_k$, forcing $n = 0$. Consequently, $K \cap \langle x \rangle = \{e\}$.

Now we have that $H = K\langle x \rangle$ and $K \cap \langle x \rangle = \{e\}$, so $H \simeq K \times \langle x \rangle$. The union of a generating set for K and a generating set for $\langle x \rangle$ is therefore a generating set for H. However, both K and $\langle x \rangle$ have finite generating sets, and so H has a finite generating set, completing the induction for $\mathbb{Z}^k$. $\square$

Lemma 3.4. *Let $\phi : G \to G'$ be a homomorphism. If G is finitely generated, then its image $\phi[G]$ is finitely generated.*

Motivation. This is the counterpart to lemma 3.3, showing that homomorphisms preserve the property of being finitely generated.

Proof. We have a minimum generating set $\{g_1, ..., g_k\}$ for G. G is not necessarily abelian, however, and so we can only state that an element x of G can be expressed as $g_{n_1}^{\pm 1} * g_{n_2}^{\pm 1} * ... * g_{n_j}^{\pm 1}$, for $n_1, ..., n_j$ between 1 and k, rather than being able to use commutativity to consolidate powers of each g_i into $g_1^{n_1} * g_2^{n_2} * ... * g_k^{n_k}$.

Take any y in $\phi[G]$. Then there is an x in G such that $\phi(x) = y$, but x can be rewritten as $g_{n_1} * ... * g_{n_j}$.

According to the definition of a homomorphism, $\phi(x) = \phi(g_{n_1} * ... * g_{n_j}) = \phi(g_{n_1}) * ... * \phi(g_{n_j})$, and so every element of $\phi[G]$ can be expressed in terms of $\{\phi(g_1), ..., \phi(g_k)\}$, demonstrating that $\phi[G]$ is finitely generated. □

Theorem 3.5. *Any subgroup of a finitely generated abelian group is finitely generated.*

Motivation. This theorem is the consolidation of lemmas 3.3 and 3.4, and is used in lemma 4.11 to demonstrate the existence of a maximal cyclic subgroup.

Proof. Let G be a finitely generated abelian group, generated by a minimal generating set $\{g_1, ..., g_k\}$. Define $\phi : \mathbb{Z}^k \to G$ by $\phi((n_1, ..., n_k)) = g_1^{n_1} * ... * g_k^{n_k}$. ϕ is clearly both a homomorphism and onto, so any subgroup H of G has an inverse image $\phi^{-1}[H]$ in $\mathbb{Z}^k$, where $\phi^{-1}[H]$ is the set of elements x of $\mathbb{Z}^k$ for which ϕx is in H. Then $\phi^{-1}[H]$ is a subgroup of $\mathbb{Z}^k$, and so is finitely generated, by lemma 3.3. By lemma 3.4, $\phi[\phi^{-1}[H]] = H$ is finitely generated for any subgroup H of G. □

4 Finitely Generated Abelian Groups

The Finitely Generated Abelian Group Structure Theorem describes the limitations and qualities of finitely generated abelian groups. In particular, for any finitely generated abelian group G, $G \simeq \mathbb{Z}^n \times \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$, with $1 < n_k | n_{k-1} | ... | n_1$ and $n \geq 0$.

The overall proof is split into three steps.

Theorem 4.1. *G has prime power size $p^N \Rightarrow G \simeq \mathbb{Z}_{p^{n_1}} \times ... \times \mathbb{Z}_{p^{n_k}}$, with $n_1 \geq n_2 \geq ... \geq n_k \geq 1$.*

Theorem 4.2. *G finite and abelian $\Rightarrow$ G is the direct product of its Sylow subgroups.*

Theorem 4.3. *G finitely generated and abelian $\Rightarrow G \simeq \mathbb{Z}^m \times \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$, with $1 \leq n_k | n_{k-1} | ... | n_1$.*

These proofs all follow the same general style of proof by construction, but with different nuances.

4.1 Step 1

G has prime power size $p^N \Rightarrow G \simeq \mathbb{Z}_{p^{n_1}} \times ... \times \mathbb{Z}_{p^{n_k}}$, with $n_1 \geq n_2 \geq ... \geq n_k \geq 1$.

Let G be abelian and have size p^N, for some prime p.

Lemma 4.4. *If $y \in K$ such that order(y) is maximum among the elements in K, with $|K|$ a prime power, then $[\forall\ x \in K,\ x^n = y \Rightarrow y^m = x$ for some $m]$*

Motivation. Although it is not immediately clear from the statement of the lemma, this is actually a powerful tool that will enable us to preserve the underlying structure of a group G while acting in a quotient group G/H, by requiring exponentiation into H to be onto the identity only.

Proof. Pick an x such that $x^n = y$, for some $0 < n < \text{order}(x)$.

y has maximum order in K, which has size p^N, and so $\text{order}(x)|\text{order}(y) \forall\ x \in K$.

Yet, $y^{\text{order}(x)} = x^{n*\text{order}(x)} = e \Rightarrow \text{order}(y)|\text{order}(x)$. Therefore $\text{order}(x) = \text{order}(y)$.

However, we can show that $y = x^n \Rightarrow \text{order}(y) = \text{order}(x)/\gcd(n, \text{order}(x))$:

By definition, $e = y^{\text{order}(y)} = (x^n)^{\text{order}(y)} = x^{n*\text{order}(y)} \Rightarrow \text{order}(x)|n*\text{order}(y) \Rightarrow \text{order}(x)/\gcd(n, \text{order}(x))|\text{order}(y)$.

However, $y^{\text{order}(x)/\gcd(n,\text{order}(x))} = x^{n*\text{order}(x)/\gcd(n,\text{order}(x))} = x^{\text{lcm}(n,\text{order}(x))} = (x^{\text{order}(x)})^k$, for some k, and so $y^{\text{order}(x)/\gcd(n,\text{order}(x))} = e^k = e \Rightarrow \text{order}(y)|\text{order}(x)/\gcd(n, \text{order}(x))$.

Therefore $\text{order}(y) = \text{order}(x)/\gcd(n, \text{order}(x)), \forall\ y \in \langle x \rangle$.

However, $\text{order}(y)$ is maximal for elements of K, and so $\text{order}(y)|\text{order}(x) \Rightarrow \text{order}(y) = \text{order}(x)$.

$\text{order}(y) = \text{order}(x) \Rightarrow \gcd(n, \text{order}(x)) = 1 \Rightarrow y$ is a generator of $\langle x \rangle \Rightarrow x = y^m$, some m. □

Lemma 4.5. *There are distinct cyclic subgroups $S_1, ..., S_k$ of G such that $G = S_1S_2...S_k \simeq S_1 \times ... \times S_k$*

Motivation. The purpose of this lemma is to produce the cyclic structures underlying the group G, completing Theorem 4.1.

Proof. This shall be proven by creating S_i and performing induction on $G/S_1S_2...S_i$ until we have $G = S_1...S_k$, for some k.

Base Case: S_1

Take s_1 of maximum order in G.

Define $S_1 = \langle s_1 \rangle$. $|S_1| = p^{n_1}$, and clearly $S_1 \simeq \mathbb{Z}_{p^{n_1}}$.

Induction on $G/S_1...S_i$

The goal of this induction is to produce $S_1, S_2, ..., S_i$ such that $S_1S_2...S_i \simeq S_1 \times ... \times S_k$

Given $S_1, S_2, ..., S_{i-1}$, take Y of maximum order in $G/S_1S_2...S_{i-1}$.

Clearly $\text{order}(Y) \leq \text{order}(s_{i-1})$.

Take $s_i \in Y$ such that $\text{order}(s_i) = \text{order}(Y)$. Define $S_i = \langle s_i \rangle$.

By lemma, $Y = s_i * S_1S_2...S_{i-1}$ of maximum order in $G/S_1S_2...S_{i-1} \Rightarrow \forall\ X \in G/S_1S_2...S_{i-1}, X^n = Y \Rightarrow Y^m = X$ for some m.

For any $n \in \mathbb{Z}$, $\forall\ x \in Y$, $x^n \in S_1S_2...S_{i-1} \Leftrightarrow \text{order}(Y)|n$. But $\text{order}(Y) = \text{order}(s_i)$, and $s_i \in Y \Rightarrow s_i^n = e \Leftrightarrow \text{order}(Y) = \text{order}(s)|n \Leftrightarrow s^n = e$.

$\Rightarrow S_i \cap S_1S_2...S_{i-1} = e$. This directly produces the result that $|S_1...S_i| = |S_1...S_{i-1}| * |S_i|$, but only non-trivial S_i are produced and so this must eventually fill G. Furthermore, $|S_i| \mid |G|$, so $|S_i| = p^{n_i}$. In conjunction with the fact that S_i is cyclic, $S_i \simeq \mathbb{Z}_{p^{n_i}}$.

Continue until $G = S_1S_2...S_i$.

It remains to be shown that G is the internal direct product of $S_1, ..., S_k$.

Now we have sets $S_1, ..., S_k$ such that

- $G = S_1S_2...S_k$
- Each $S_i = \langle s_i \rangle$ for some $s_i \in G$, and so is isomorphic to $\mathbb{Z}_{p^{n_i}}$.
- $\forall\ i \leq k$, $S_1S_2...S_{i-1} \cap S_i = \{e\}$.
- $\forall\ i \leq k$, $|(S_1S_2...S_{i-1})(S_i)| = |S_1S_2...S_{i-1}| * |S_i)||\{e\}| = |S_1S_2...S_{i-1}| * |S_i|$.

Then $\forall\ i \leq k$, $S_1S_2...S_i \simeq S_1S_2...S_{i-1} \times S_i$, and so $S_1S_2...S_i \simeq S_1 \times S_2 \times ... \times S_i$. Since $G = S_1S_2...S_k$, $G \simeq S_1 \times S_2 \times ... \times S_k \simeq \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times ... \times \mathbb{Z}_{p^{n_k}}$. By reordering of indices, $n_1 \leq n_2 \leq ... \leq n_k$, and so $p^{n_1}|p^{n_2}|...|p^{n_k}$. □

4.2 Step 2

G finite and abelian $\Rightarrow$ G is the direct product of its Sylow subgroups.

Let G be finite and abelian. Let S be any p-Sylow subgroup of G for any prime p that divides $|G|$. To prove this theorem, it is sufficient to show that there is a subgroup H of G such that $G \simeq H \times S$.

Lemma 4.6. *We can pick a unique representative element y from each coset Y in G/S such that order(y) is not a multiple of p.*

Motivation. The purpose of this lemma is to produce a set of elements that will turn out to be the subgroup H for which $G \simeq H \times S$.

Proof. More formally, $\forall\ Y \in G/S, \exists$ unique $y \in Y$ such that order(y) in G = order(Y) in G/S.

Take $Y \in G/S$ (so p does not divide order(Y)).

Fix $x \in Y$. Let $s = x^{\text{order}(Y)}$ (so $s \in S$).

For any n, $x^n \in S \Leftrightarrow \text{order}(Y)|n \Leftrightarrow n = j * \text{order}(Y)$ (some $j \in \mathbb{Z}$) $\Leftrightarrow x^n = x^{\text{order}(Y)*j} = s^j$.

However, $s^j = e \Leftrightarrow \text{order}(s)|j$, but $\gcd(\text{order}(s), \text{order}(Y)) = 1$. Thus $\text{lcm}(\text{order}(s), \text{order}(Y))|n$, but $\text{lcm}(\text{order}(s), \text{order}(Y)) = \text{order}(s) * \text{order}(Y)/\gcd(\text{order}(s), \text{order}(Y)) = \text{order}(s) * \text{order}(Y)/1 = \text{order}(s) * \text{order}(Y)$. Clearly, $x^{\text{order}(s)*\text{order}(Y)}$ works, so $n = \text{order}(s) * \text{order}(Y)$.

Take $x_1, x_2 \in Y$. Define $s_1 = x_1^{\text{order}(Y)}, s_2 = x_2^{\text{order}(Y)}$. Clearly, $s_1, s_2 \in S$.

However, $x_1, x_2 \in Y \Rightarrow \exists\ s \in S$ such that $x_2 = s * x_1$.

Then $s_2 = x_2^{\text{order}(Y)} = s^{\text{order}(Y)} * x_1^{\text{order}(Y)} = s^{\text{order}(Y)} * s_1$.

If $(s_1 = s_2)$, then $e = s^{\text{order}(Y)} \Rightarrow \text{order}(s)|\text{order}(Y)$, but $s \in S \Rightarrow \text{order}(s)||S|$.

Consequently, $\text{order}(s)|\gcd(\text{order}(Y), |S|) \Rightarrow \text{order}(s)|1 \Rightarrow s = e \Rightarrow x_2 = x_1$.

So raising elements to the power of order(Y) is a 1-1 function between sets of the same finite size, making this function a bijection. As a result, $\exists\ y \in Y$ such that $s = y^{\text{order}(Y)} = e$, and then

order(y) = order$(Y) *$ order(s) = order(Y).

Consequently, $\exists\ y \in Y$ such that order(y) = order(Y).

□

This proves the lemma that such a y uniquely exists for each Y. Furthermore, it demonstrates that each Y contains exactly one element y such that p does not divide order(y), and that this y is the only element in Y with order(y) = order(Y), proving

Corollary 4.7. *For any $Y \in G/S$, $\forall\ y \in Y$, order(y) = order$(Y) \Leftrightarrow$ p does not divide order(y).*

Lemma 4.8. *For an appropriate subgroup H of G, $G \simeq H \times S$.*

Motiviation. Taking the set H we produced in lemma 4.6, now the purpose is to show that H is the desired subgroup, finishing Theorem 4.2.

Proof. Define $H = \{y \in G$ such that $y \in Y$ and order(y) = order(Y) for some $Y \in G/S\}$.

Take $a, b \in H$.

Then order$(a * b)|$order$(a) *$ order(b)

By the definition of H, p divides neither order(a) nor order(b), and so p does not divide order$(a) *$ order(b). Consequently, p does not divide order$(a * b) \Rightarrow a * b \in H$.

H is closed and finite, so $H \leq G$. According to corollary 4.7, $y \in H \Leftrightarrow p$ does not divide order(y).

Then $H \cap S = \{e\}$, and $|H| = |G/S| = |G|/|S|$.

To establish that $|HS| = |G|$,

$|HS| = |H| * |S|/|H \cap S| = |G|/|S| * |S|/|\{e\}| = |G|$. Since G is a finite set, equal size implies set equality, and so $HS = G$. $HS = G$ and $H \cap S = \{e\}$, so G is a direct product of S and H and $G \simeq H \times S$. □

Proof of Theorem 4.2. The same argument can be applied to H and its Sylow subgroups, proving Theorem 4.2. □

The conjunction of Theorems 4.1 and 4.2 gives us the finite case of the Structure Theorem. Starting with a finitely generated abelian group G, application of Theorem 4.2 gives us that G is isomorphic to its Sylow subgroups. However, by definition, Sylow subgroups have prime power size, and so we can apply Theorem 4.1 independently to each of the Sylow subgroups, giving the result that $G \simeq \mathbb{Z}_{p_1^{n_{1,1}}} \times \mathbb{Z}_{p_1^{n_{1,2}}} \times ... \times \mathbb{Z}_{p_1^{n_{1,j_1}}} \times \mathbb{Z}_{p_2^{n_{2,1}}} \times ... \times \mathbb{Z}_{p_k^{n_{1,j_k}}}$, where the indices are unique up to reordering. With the additional restriction that each of the indices must divide the preceding index, so $G \simeq \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$, the n_i turn out to be uniquely determined.

Although it was not stated as a corollary, a result of Theorem 4.2 is that $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ if and only if m and n are relatively prime. This allows us to combine relatively primes indices completely

at will, and so we can group the largest power of each prime, the second largest power of each prime, and so on, down through the smallest power of each prime, in order to achieve indices $n_1, ..., n_k$ such that $n_k|n_{k-1}|...|n_1$, which turns out to uniquely determine the n_i.

For illustration, consider the example of $G = \mathbb{Z}_{36=4*9} \times \mathbb{Z}_{15=3*5} \times \mathbb{Z}_{12=4*3}$. Although G is clearly defined in terms of $\mathbb{Z}_n$, we would not know its underlying structure prior to the application of Theorems 4.1 and 4.2. Beginning with the usage of Theorem 4.2, we have the intermediate result that $G \simeq {}_2G \times_3 G \times_5 G$, where ${}_pG$ is the p-Sylow subgroup of G. By applying Theorem 4.1 to each ${}_pG$, we get ${}_2G \simeq \mathbb{Z}_4 \times \mathbb{Z}_4$, ${}_3G \simeq \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3$, and ${}_5G \simeq \mathbb{Z}_5$. By substituting these results into the result of Theorem 4.2 and rearranging the $\mathbb{Z}_n$ so that we have grouped the largest power of each prime, the second largest power of each prime, and so on, we get the result that $G \simeq [\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5] \times [\mathbb{Z}_4 \times \mathbb{Z}_3] \times [\mathbb{Z}_3] \simeq \mathbb{Z}_{180} \times \mathbb{Z}_{12} \times \mathbb{Z}_3$. This result is the desired unique n_i such that $(n_3 = 3)|(n_2 = 12)|(n_1 = 180)$.

4.3 Step 3

G finitely generated and abelian $\Rightarrow G \simeq \mathbb{Z}^m \times \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$, with $1 \leq n_k|n_{k-1}|...|n_1$.

Let G be abelian and finitely generated.

If G is finite, then we are done, as the finite case has already been completed.

Subgroup of Elements of Finite Order

Define $H = \{x \in G \text{ such that } \text{order}(x) < \infty\}$.

Lemma 4.9. *H is a subgroup of G.*

Motivation. Once we have that H is a subgroup of G, we can work in the quotient group G/H, enabling us to construct cyclic subgroups whose structure matches the result described in Theorem 4.3.

Proof. To check that $H \leq G$, we need to show that H is closed and contains inverses.

1. H is closed: Take $x, y \in H$. Then $(x*y)^{\text{order}(x)*\text{order}(y)} = (x^{\text{order}(x)})^{\text{order}(y)} * (y^{\text{order}(y)})^{\text{order}(x)} = e^{\text{order}(y)} * e^{\text{order}(x)} = e$, so $x * y \in H$.

2. H contains inverses: Take $x \in H$. Then $x^{\text{order}(x)-1} \in H$, but $x^{\text{order}(x)-1} * x = x^{\text{order}(x)} = e$, so $x^{\text{order}(x)-1} = x^{-1} \in H$.

□

Thus $H \leq G$, and so H is finitely generated, by Theorem 3.5. Since the generators of H must be in H, they are also of finite order, and so H is a finite set. Consequently, we can apply the finite case of the theorem to H in order to show that $H \simeq \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_k}$, with $1 < n_k|...|n_1$.

Lemma 4.10. *Abelian G has an element of infinite order $\Rightarrow$ [G has a non-identity element of finite order $\Leftrightarrow$ G has two distinct elements of infinite order whose orbits have a nontrivial intersection, with at least one of the orbits being maximal among cyclic subgroups of G].*

Motivation. Later on, we will be constructing several groups with no non-indentity elements of finite order, and the result about the intersection of orbits plays a pivotal role in producing contradictions in some of those cases, when one of the sides is easier to check than the other.

Proof. The two directions of the proof shall be addressed separately.

$\Rightarrow$: G has a element of finite order $s \neq e$.

Let x be any element of infinite order whose orbit is maximal among cyclic subgroups of G.

Then $s \notin \langle x \rangle \Rightarrow y = s * x \notin \langle x \rangle \Rightarrow \langle y \rangle \neq \langle x \rangle$,

Then $y^{\text{order}(s)} = (s * x)^{\text{order}(s)} = x^{\text{order}(s)} \in \langle y \rangle \cap \langle x \rangle$.

$\Leftarrow$: G has two distinct elements of infinite order, x and y, whose orbits have a nontrivial intersection. $\langle y \rangle$ is maximal among cyclic subgroups of G.

In particular, $x^a = y^b$ for some a, b, a minimal for positive such powers of x. The intersection of $\langle x \rangle$ and $\langle y \rangle$ is nontrivial, so both $|a|$ and $|b|$ are greater than 1.

Case 1: $g = \gcd(a, b) > 1$

a is minimal, so $x^{a/g} \notin \langle y \rangle \Rightarrow x^{-a/g} * y^{b/g} \neq e$, and $(x^{-a/g} * y^{b/g})^g = x^{-a} * y^b = y^{b-b} = y^0 = e$.

Therefore $x^{-a/g} * y^{b/g}$ is a non-identity element of finite order.

For example, take $x = (1, 0)$ and $y = (1, 1)$ in $\mathbb{Z}x\mathbb{Z}_3$. The orbit of x is clearly maximal, and so the theorem applies, with $(1, 0)^3 = (3, 0) = (3, 3) = (1, 1)^3$. Let $g = \gcd(3, 3) = 3$. Following the proof, $(1, 0)^{3/g=1} = (1, 0) \neq (0, 0) = e$, but $[(-1, 0)^{3/g=1} * (1, 1)^{3/g=1}]^g = [(-1, 0) * (1, 1)]^3 = (0, 1)^3 = (0, 3) = (0, 0) = e$, giving us a non-identity element of finite order.

Case 2: $\gcd(a, b) = 1$

Then $\exists\ c, d \in \mathbb{Z}$ such that $a * c + b * d = 1$.

By substitution, $(x^d * y^c)^a = x^{a*d} * y^{a*c} = y^{b*d+a*c}$, but $(x^d * y^c)^a = y^1 = y, |a| > 1$, contradicting the premise that $\langle y \rangle$ is maximal among cyclic subgroups.

This contradiction demonstrates the impossibility of the second case, finishing the lemma. $\square$

Lemma 4.11. *If K is a finitely generated abelian group, then K has a maximal cyclic subgroup.*

Motivation. As will shortly be shown in the counterexample of $\mathbb{Q}$, this is not, in general, true of groups. However, taking maximal cyclic subgroups is important to the proof by construction used here, much as it was in the case of groups of prime power size in Theorem 4.2.

Proof. This not true, in general, if K is not required to be finitely generated. For example, take $K = \mathbb{Q}$. $\mathbb{Q}$ is clearly abelian, but not finitely generated, as any finite set of rationals other than $\{0\}$ has some least common denominator d. Then $1/(2d)$ cannot be produced, as it would increase the least common denominator to $2d$, and so $\mathbb{Q}$ is not finitely generated. In order to show that $\mathbb{Q}$ has no maximal cyclic subgroups, it is necessary to show that any cyclic subgroup is a proper subset of a larger cyclic subgroup. Let $\langle a \rangle$ be any cyclic subgroup in $\mathbb{Q}$. If $a = 0$, then $\langle a \rangle$ is trivially not maximal, so $a \neq 0$. Pick any integer $n > 1$. Then $n * (a/n) = a$, and so a is a power of a/n, forcing $\langle a/n \rangle \supset \langle a \rangle$ and demonstrating that $\langle a \rangle$ is not maximal. Thus $\mathbb{Q}$ has no maximal cyclic subgroups.

Let K be a finitely generated abelian group. By way of contradiction, assume that K has no maximal cyclic subgroups. Then for every cyclic subgroup $\langle s_i \rangle$, $\exists$ an $\langle s_{i+1} \rangle \subset K$ such that $\langle s_i \rangle \subset \langle s_{i+1} \rangle$. Define $H \leq K = \langle s_1, s_2, ... \rangle$.

To demonstrate that H is a subgroup of K, it is sufficient to observe that any pair of elements x, y of H are elements of an $\langle s_i \rangle$ for some i, and so their product and inverses are also in $\langle s_i \rangle$, and therefore in H.

Then H is finitely generated, by Theorem 3.5, and so has a minimum size generating set $\{g_1, ..., g_k\}$. Clearly, each $g_i \in H$, and so for each g_i there is some n_i such that $g_i \in \langle s_{n_i} \rangle$. Take $n = max(n_1, ..., n_k)$. For all g_i, $g_i \in \langle s_n \rangle$, and so $H \subseteq \langle s_n \rangle$, but $\langle s_n \rangle \subset \langle s_{n+1} \rangle \subseteq H$, a contradiction. □

It remains to be shown that there is a subgroup K of G such that $G \simeq K \times H$ and K is finitely generated. Induction will be used to construct such a subgroup.

Lemma 4.12. *Any quotient group of a finitely generated G is also finitely generated.*

Motivation. This demonstrates that the many lemmas and theorems so far proved for finitely generated groups also apply to the quotient groups used in the induction.

Proof. Take $H \leq G$.

G finitely generated $\Rightarrow$ $\exists$ a minimum size generating set $\{g_1, ..., g_k\}$.

Beginning with the definition of finitely generated, $\langle g_1, ..., g_k \rangle = G \Rightarrow \langle g_1, ..., g_k \rangle * H = G \Rightarrow \langle g_1 * H, ..., g_k * H \rangle = G/H$. □

Lemma 4.13. *Let K be a finitely generated abelian group with $X \leq K$ such that K/X is comprised of only e and elements of infinite order. Then $\langle S \rangle$ maximal among cyclic subgroups of K/X (so $S = s * X$) $\Rightarrow$ $K/X\langle s \rangle$ has no non-identity elements of finite order.*

Motivation. This lemma provides conditions under which we can continue to meet the assumption in the induction that there are no non-identity elements of finite order present in the quotient group G/H.

Proof. By way of contradiction, assume $\exists\ H \in K/X\langle s\rangle$ such that $0 < \text{order}(H) < \infty$. Fix $h \in H$.
The premise for K/X clearly requires that $(h * X)^n \neq X \forall\ n \neq 0$, and so $h^n \notin X \forall\ n \neq 0$.
However, $(h * X)^{\text{order}(H)} = (s * X)^b$ for some b. By lemma 4.10, K/X must contain a non-identity element of finite order, violating the premise.
Consequently, $K/X\langle s\rangle$ has no non-identity elements of finite order. □

Lemma 4.14. *For the base case of the induction, the quotient group G/H meets the criteria for lemma 4.13.*

Motivation. Induction must begin somewhere, and it needs to be proven that this is an appropriate starting point.

Proof. If there is an element Y of G/H such that $\text{order}(Y) < \infty$, then for any $y \in Y$, $Y^{\text{order}(Y)} = (yH)^{\text{order}(Y)} = y^{\text{order}(Y)}H = H$, and so $(y^{\text{order}(Y)})^{-1} \in H$, as H contains e and so something in H must be the inverse of $y^{\text{order}(Y)}$. Consequently, $y^{\text{order}(Y)}$ is an element of finite order, and so y also has finite order, meaning that $y \in H$ and $Y = yH = H$. □

Lemma 4.15. *Using induction, we can construct distinct cyclic subgroups $S_1, S_2, ..., S_i$ such that $S_1S_2...S_iH \simeq S_1 \times S_2 \times ... \times S_i \times H$ and $G/S_1...S_iH$ has no non-identity elements of finite order.*

Motivation. Although it requires another lemma to prove it, the cyclic subgroups produced by this induction represent the underlying structure of $\mathbb{Z}^k$ referred to in the statement of Theorem 4.3.

Proof. By lemma 4.11, we know that a maximal $\langle Y\rangle$ exists in $G/S_1S_2...S_{i-1}H$. Take any such Y.
Take s_i such that $Y = s_i * S_1S_2...S_{i-1}H$ (so any element of Y), and define $S_i = \langle s_i\rangle$.
Take $s_i^n \in S_1S_2...S_{i-1}H \cap S_i$.
If $s_i^n \in S_1S_2...S_{i-1}H$, then $Y^n = S_1S_2...S_{i-1}H \Rightarrow n = 0$ or $\text{order}(Y) < \infty$, contradicting lemma 4.10. Therefore we may conclude that $n = 0 \Rightarrow s_i^n = e$, and so $S_1S_2...S_{i-1}H \cap S_i = \{e\}$.
As a result of the fact that $S_1...S_{i-1}H \cap S_i = \{e\}$, $S_1...S_iH \simeq S_1...S_{i-1}H \times S_i$, which is crucial to the conclusion of the theorem.
$\langle Y\rangle$ is maximal among cyclic subgroups of $G/S_1...S_{i-1}H$, so $G/S_1...S_{i-1}S_iH$ continues to meet the precondition of having no elements of finite order, by lemma 4.13. This is true of each such step, and so the induction continues properly. Furthermore, the induction eventually terminates, as shown by the following lemma. □

Lemma 4.16. *There are only finitely many S_j.*

Motivation. For the similar portion of Theorem 4.1, we had a finite starting size that decreased with each iteration, and so it was trivial that the induction had to terminated eventually. Now that

we have a group of infinite size, this is no longer the case, and it must be proven that the induction does terminate.

Proof. Let k be the size of a minimal generating set $\{g_1, ..., g_k\}$ for G. By way of contradiction, assume that there are more than k distinct S_j; in particular, there are at least $k+1$ S_j.

Each s_i is in G, and so can be rewritten as $s_i = \prod_{j=1}^{k} g_j^{n_{ij}}$. Then by linear algebra, there is a non-trivial combination of $\{s_1, ..., s_{k+1}\}$ such that $e = s_1^{n_1} * ... * s_{k+1}^{n_{k+1}}$. In particular, there is a $j \leq k+1$ such that $s_j^{n_j} = s_1^{-n_1} * ... * s_{j-1}^{-n_{j-1}} = x$ for some x in $S_1...S_{j-1}$. We can achieve this by taking j to be the maximum index with a nonzero power n_j.

Returning to the induction hypothesis, at each step we have a quotient group $G/S_1...S_iH$ with exactly one element of finite order, the identity. Then $G/S_1...S_{j-1}H$ has an element $s_jS_1...S_{j-1}H$ such that $(s_jS_1...S_{j-1}H)^{n_j} = s_j^{n_j}S_1...S_{j-1}H = xS_1...S_{j-1}H$, which equals $S_1...S_{j-1}H$ because x is in $S_1...S_{j-1} \subseteq S_1...S_{j-1}H$. Consequently, $s_jS_1...S_{j-1}H$ is an element of finite order in $G/S_1...S_{j-1}H$, and so $s_jS_1...S_{j-1}H$ must be the identity, $S_1...S_{j-1}H$. However, s_j was specifically chosen so that $\langle s_jS_1...S_{j-1}H\rangle$ is maximal among cyclic subgroups of $G/S_1...S_{j-1}H$, which is true for the identity if and only if $G/S_1...S_{j-1}H \simeq \{e\}$. That is, we would have selected s_j if and only if $S_1...S_{j-1}H = G$, by which point the induction would have already terminated, precluding the presence of s_j and creating a contradiction.

So there are at most k distinct S_j; that is, finitely many. Furthermore, since the induction continues as long as $G/S_1S_2...S_iH \not\simeq e$, $G/S_1S_2...S_iH \simeq e$, and so $G = S_1...S_iH$ for some i. □

Post-Induction

Proof. Let k be the maximum index attained in the induction (so there are k distinct S_j).
Since $S_1S_2...S_kH = G$ and $S_1S_2...S_k \cap H = \{e\}$, $G \simeq S_1S_2...S_k \times H$.
By construction, $S_1...S_kH \simeq S_1 \times ... \times S_k \times H$, and $S_j = \langle s_j\rangle \simeq \mathbb{Z}$.
By the application of Theorems 4.1 and 4.2, $H \simeq \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_j}$, with $1 < n_k$ and $n_j|n_{j-1}|...|n_1$ for some $n_1, ..., n_j$.
Thus $G = S_1...S_kH \simeq \mathbb{Z}^k \times \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_j}$, with $1 < n_j$ and $n_j|n_{j-1}|...|n_1$ for some $n_1, ..., n_j$, proving the general case of the Finitely Generated Abelian Groups Structure Theorem. □

5 Application

5.1 Public Key Encryption

Much of today's information exchange is based around the premise that the information is intelligible only to its intended parties, although this is impossible to guarantee fully. It is somewhat

understandable that a large amount of time and effort is put into making this exchange as secure as possible. Public key encryption algorithms were first suggested during the 70s, and one of the earliest methods was the Diffie-Hellman Key Exchange.

5.2 Diffie-Hellman Key Exchange

The underlying premise of this method of encryption is the difficulty of finding discrete logarithms, which are the integer exponents of generating elements found in $x = g_1^{n_1} * ... * g_k^{n_k}$. There is not presently a proof that solving for the discrete log of an element is difficult, but so far this problem has proved resistant enough for this premise to become relied upon by many such algorithms.

The Diffie-Hellman Key Exchange is especially reliant upon this supposition, as all of the information in the exchange is publicly available except for the exponents. Parties agree upon a set, typically based on integer multiplication, and a generator, prior to exchanging keys. Then each involved party chooses a private number to serve as the exponent, raises the generator to that power, and provides the result to the other members conducting the encryption. Upon receiving the new number, it is then exponentiated using the receiving party's own private number, resulting in a shared key by use of the fact that $g^{a*b} = g^{b*a}$.

More explicitly, parties A and B will agree upon a generator n and a prime modulus p, then choose private exponents a and b. A will provide B with $n^a \bmod p$ and receive $n^b \bmod p$, then exponentiate that with a. The result is $(n^b)^a \bmod p = n^{b*a} \bmod p = n^{a*b} \bmod p = (n^a)^b \bmod p$, so A and B end up with the same integer key.

In order to maximize the difficulty of attacks on the encryption, n should generate as many elements as possible, which is why it is preferable for n to generate all of the positive integers mod$p$. For that to happen, $\mathbb{Z}_p^\times$, the group of elements of $\mathbb{Z}_p$ with multiplicative inverses mod$p$, must be a cyclic group, with no duplicates among the powers $n^1, n^2, ..., n^{p-1} = 1$.

5.3 $\mathbb{Z}_p^\times$ is Cyclic

Theorem 5.1. *$\mathbb{Z}_p^\times$ is Cyclic*

Motivation. Multiplication and exponentiation are easy in $\mathbb{Z}_n^\times$, but if that group is cyclic, then attacks to break the encryption have the maximum possible search space for potential keys, maximizing the difficulty of decryption without prior knowledge.

Proof. By way of Fermat's Little Theorem, for prime p, $x^p = x \bmod p$.
By Theorem 4.2, $\mathbb{Z}_p^\times \simeq \mathbb{Z}_{p_1^{n_1}} \times ... \times \mathbb{Z}_{p_k^{n_k}}$, while still retaining the property that $x^p = x \forall\ x \in \mathbb{Z}_p^\times$.
Let $m = \text{lcm}(p_1^{n_1}, ..., p_k^{n_k})$, which divides $p - 1 = |\mathbb{Z}_p^\times|$. Then $p_i^{n_i} | m | p - 1$ for all i, and so $x^m = x, \forall$

$x \in \mathbb{Z}_p^\times$. Shifting terms around, we get $x^m - x = 0, \forall\ x \in \mathbb{Z}_p^\times$. Then $m \geq p-1$ and $m|p-1 \Rightarrow m = p-1$. This happens if and only if each of the p_i are distinct, which happens if and only if $\mathbb{Z}_p^\times$ is cyclic. $\square$

5.4 Extension to Finite Fields

Multiplication in the integers mod$n$ is only the most accessible group usable for the Diffie-Hellman Key Exchange. In fact, any finite field will work. A field is a set with two operations, addition and multiplication, with distinct identities 0 and 1. Addition is a group across all elements of the field, whereas multiplication is a group across all non-zero elements of the field and distributes over addition. Using this definition, $\mathbb{Z}_p$ is immediately a field, and the result that $\mathbb{Z}_p^\times$ is cyclic is a specific case of the fact that the multiplicative group of any finite field is cyclic. The elements do not even need to be numbers, although it is natural to retain them as such, given their origin and the necessity of converting them to machine-processable data.

The proof of Theorem 5.1 can be adapted to the multiplicative groups of other fields. However, all that is truly necessary is an abelian group with a hard discrete log problem. For example, it is easy to solve $k^a = k * a \bmod n$, making addition $\mathbb{Z}_n$ a poor choice for Diffie-Hellman. A better way to pick groups for Diffie-Hellman is to use elliptic curves over large finite fields, which is used today for some secure connections, or picking large subgroups of the multiplicative group of the field $\mathbb{Z}_p$.

The ability to choose generators for these groups enables us to rapidly exponentiate with the maximum number of options to examine when attempting to break the encryption, providing rapid encryption and decryption and slow codebreaking, an understandably desirable trait in cryptography.

References

1. J. B. Fraleigh, *A First Course in Abstract Algebra*, 7th edition, Addison Wesley, 2003.

2. I. N. Herstein, *Topics in Algebra*, 2nd edition, John Wiley & Sons, 1975.

3. P. Garret, Website: http://www.math.umn.edu/ garrett/m/algebra/, last modified 2013.