Journal of Natural Sciences,
Life and Applied Sciences
Issue (3) 1 - October 2017
ISSN: 2518-5780

المجلة العربية للعلوم و نشر الأبحاث
Arab Journal of Sciences & Research Publishing
AJSRP

A Study on Finite Abelian Groups: Sylow's Theorems Based

Amaira Moaitiq Mohammed Al-Johani
Tabuk University || Tabuk || Kingdom of Saudi Arabia

Abstract: In abstract algebra, an algebraic structure is a set with one or more finitary operations defined on it that satisfies a list of axioms. Algebraic structures include groups, rings, fields, and lattices, etc. A group is an algebraic structure $(G, *)$, which satisfies associative, identity and inverse laws. An Abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on the order in which they are written. That is, these are the groups that obey the axiom of commutatively. The concept of an Abelian group is one of the first concepts encountered in abstract algebra, from which many other basic concepts, such as rings, commutative rings, modules and vector spaces are developed. This study sheds the light on the structure of the finite abelian groups, basis theorem, Sylow's theorem and factoring finite abelian groups. In addition, it discusses some properties related to these groups. The researcher followed the exploratory and comparative approaches to achieve the study objective. The study has shown that the theory of Abelian groups is generally simpler than that of their non-abelian counter parts, and finite Abelian groups are very well understood.

Keywords: algebra, Finite, Abelian, Groups

1. Introduction

An algebraic structure is a set with one or more finitary operations defined on it that satisfies a list of axioms. Examples of algebraic structures include groups, rings, fields, and lattices. Addition and multiplication on numbers are the prototypical example of an operation that combines two elements of a set to produce a third. These operations obey several algebraic laws [1].

An abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on the order in which they are written. That is, these are the groups that obey the axiom of commutatively. Abelian groups generalize the arithmetic of addition of integers. The concept of an abelian group is one of the first concepts encountered in undergraduate abstract algebra, from which many other basic concepts, such as modules and vector spaces are developed. The theory of abelian groups is generally simpler than that of their non-abelian counterparts, and finite abelian groups are very well understood [2]

Importance of Study

The study is important for researchers and students specialized in Algebra. It provides them with set-theoretical backgrounds of abelian groups through exploring their fundamental types and main properties.

To achieve the study objective, the researcher followed the exploratory and comparative approaches to achieve the study objective.

1.1 Algebraic Structures: Basic Definitions and Results

1.1.1 Definition of set S [3]

A *set* S is a collection of well-defined objects, and those objects are called the *elements*(or *members*) of S.

1.1.2 Definition of finite set [4]

A *finite set* is a set whose elements are enumerable and it can be described by listing its elements inside{ }.

We also say that they belong to that set (we denote this by ∈)

1.1.3 Definition of infinite set [4]

An *infinite set* is a set whose elements are none numerable.

1.1.4 Definition of union [5]

The *union* of two sets M and Nis the set of all elements each of which belongs to at least one of the two sets. The union of two sets is symbolized by $M \cup N$.

1.1.5 Definition of intersection [5]

The *intersection* of two sets M and Nis the set of elements each of which belongs to both sets. The *intersection* of two sets is symbolized by $M \cap N$.

1.1.6 Definition of p [1]

A natural number p is prime if $p \geq 2$ and there is no factorization $p = ab$, where $a < p$ and $b < p$ are natural numbers.

1.1.7 Theorem (Mathematical Induction) [7]

Let $P(x)$ be a property (possibly with parameters). Assume that

(i) $P(0)$ holds.

(ii) For all $n \epsilon N, P(n)$ implies $P(n+1)$.

Then P holds for all-natural numbers n .

1.1.8 Theorem (Division Algorithm) [1]

Given integers a and b with $a \neq 0, b \neq 0$ there exist unique integers q and r with

$b = qa + r$ and $0 \leq r < |a|$.

1.1.9 Definition [1]

If a and b are integers, then a is a divisor of b if there is an integer d with $b = ad$. We also say that a divides b or that b is a multiple of a, and we denote this by $a|b$.

1.1.10 Definition [24]

Let a and b be nonzero integers. A common divisor of a and $b$is an integer that divides both a and b. We define $gcd(a, b)$, or the greatest common divisor of a and b, to be the largest positive common divisor of a and b. (Note that 1 is always a common divisor of any two integers).

1.1.11 Theorem (Euclid's Lemma) [1]

If p is a prime and $p|ab$, then $p|a$ or $p|b$. More generally, if a prime *p* divides a product $a_1 a_2 \cdots a_n$, then it must divide at least one of the factors a_n.

1.1.12 Definition [14]

If X and Y are sets, then their *Cartesian product* $X \times Y$ is the set of all ordered pairs (x, y), where $x \in X$ and $y \in Y$.

1.1.13 Example [14]

The plane is $R \times R$.

1.1.14 Definition [16, 6]

Let X and Y be (not necessarily distinct) sets. *A function* f from X to Y, denoted by

$f: X \to Y$,

Is a subset $f \subseteq X \times Y$ such that, for each $a \in X$, there is a unique $b \in Y$ with $(a, b) \in f$.

For each $a \in X$, the unique element $b \in Y$ for which $(a, b) \in f$ is called *the value of* f at a, and b is denoted by $f(a)$.Thus, f consists of all those points in $X \times Y$ of the form $(a, f(a))$.When $f : R \to R$, then f is *the graph of* $f(x)$.

Here we say X is the *domain* of f, and Y is the *target* (or *codomain*) of f, and define the *image* (or *range*) of f, denoted by $im\ f$, to be the subset of Y consisting of all the values of f.

a well-defined function is therefore one whose formula produces exactly one value in its codomain for every input from its domain.

1.1.15 Definition [1]

A function $f : X \to Y$ is *a surjection* (or is *onto*) if

$$im\ f = Y.$$

Thus, f is surjective if, for each $y \in Y$, there is some $x \in X$ with $y = f(x)$.Surjections are often called *epimorphosis.*

1.1.16 Definition [1]

A function $f: X \to Y$ is *an injection* (or is *one-to-one)* if, whenever a and a^r are distinct elements of X, then $f(a) \neq f(a^r)$.

Equivalently f is injective if, for every pair $a, a^r \in X$, we have

$f(a) = f(a^r)$ implies $a = a^r$.

Injections are often called *monomorphisms*.

1.1.17 Definition [1]

A function $f: X \to Y$ is *a bijection* if it is both an injection and a surjection.

1.1.18 Definition [2]

A *group* is anon empty set G on which there is defined a binary operation

$(a, b) \to ab$ Satisfying the following properties:

Closure: If a and b belong to G, then ab is also in G;

Associativity: $a(bc) = (ab)c$ for all $a, b, c \in G$;

Identity: There is an element 1 in G such that $a1 = 1a = a$ for all a in G

Inverse: If a is in G there is an element a^{-1} in G such that $aa^{-1} = a^{-1}a = 1$.

1.1.19 Definition [7]

A set G together with a binary operation $(a, b) \mapsto a.b: G \times G \longrightarrow G$ is called a *magma*. When the binary operation is associative, $(G, .)$ is called a *semi group*.

1.1.20 Definition [18]

A *finite group* is a group with a finite number of elements

1.1.21 Definition [2]

A group G is an *abelian group* if the binary operation is commutative, i.e.,

$$ab = ba$$

for all a, b in G.

1.1.22 Lemma [1]

Let $(G,*)$ be a group

(i) The cancellation law should : If either

$x * a = x * b$ or $a * x = b * x$,

Then $a = b$.

(ii) The element e is the unique element in G with

$$e * x = x = x * e$$

For all $x \in G$.

(iii) Each $x \in G$ has a unique inverse: There is only one element $xr \in G$ with

$$x * xr = e = x\,r * x$$

(Henceforth, this element will be denoted by x^{-1}).

(iv) $(x^{-1})^{-1} = x$ For all $x \in G$.

1.1.23 Proposition [1]

The notation$an$is the natural way to denote $a * a *\cdots* a$ (n-times).

However, if the operation is $+$, then it is more natural to denote$a + a + \cdots + a$ (n-times) by na. Let Gbe a group written additively; if $a, b \in G$ and m and n are (not necessarily positive) integers, then:

(i) $n(a + b) = na + nb$
(ii) $m(na) = (mn)a$
(iii) $ma + na = (m + n)a$

1.1.24 Proposition (Laws of Exponents) [1]

Let G be a group, let $a, b \in G$, and let$m$and$n$ be integers.

(i) If a and b commute, then $(ab)n = anbn$.
(ii) $(an)m = amn$.

1.1.25 Definition [1]

A subset H of a group $G$is a *sub group* if

(i) $1 \in H$;
(ii) $If\ x, y \in H$,then$xy \in H$;
(iii) $Ifx \in H$,then$x^{-1} \in H$.

If$H$is a subgroup of$G$,we write $H \leq G$;A subgroup H ≠ G is called a *proper subgroup*, then we write $H < G$.

1.1.26 Proposition [1]

A subset H of a group G is a subgroup if and only if H is nonempty and, whenever $x, y \in H$, then $xy^{-}1 \in H$.

1.1.27 Proposition [1]

The intersection $\bigcap_{i=1} H_i$ of any family of subgroups of a group G is again a subgroup of G. In particular, if$H$ and K are subgroups of G, then $H \cap K$ is a subgroup of G.

1.1.28 Definition [2]

The *order of the group*G, denoted by $|G|$, is simply the number of elements in G

1.1.29 Definition [6]

A finite group can in principle be specified by a Kayley table, a table whose rows and columns are indexed by group elements, with the entry in row a and column b being$a \circ b$.

1.1.30 Examples [6]

Here are two examples (Table 1)

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table 1(a)

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 1(b)

Table 1 Kayley table

1.1.31 Definition [1]

If G is a group and $a \in G$, write $< a >= \{an: n \in Z\} = \{$all powers of $a\}$;

$< a >$ is called the *cyclic subgroup* of G *generated* by a. A group G is called *cyclic* if there exists $a \in G$ with $G =< a >$, in which case a is called a *generator* of G.

1.1.32 Lemma [2]

A finite cyclic group generated by a is necessarily abelian, and can be written as $\{1, a, a^2, \ldots, a^{n-1}\}$ where $a^n = 1$, or in additive notation, $\{0, a, 2a, \ldots, (n-1)a\}$, with $na = 0$.

1.1.33 Proposition [1]

Let G be a finite group and let $a \in G$.Then the order of a is $| < a > |$, the number of Elements in $< a >$.

1.1.34 Definition [6]

The *order* of an element a of a group G is the smallest positive integer m such that $a^m = 1$, if one exists; if no such m exists, we say that a has *infinite order*.

1.1.35 Theorem [1]

If $a \in G$ is an element of order n, then $a^m = 1$ if and only if $n \mid m$.

1.1.36 Lemma [1]

A cyclic group of order n has a unique subgroup of order d, for each divisor d of n, and this subgroup is cyclic.

1.1.37 Theorem (Lagrange's Theorem) [6]

The order of a subgroup of a group G divides the order of G.

1.1.38 Proposition [1]

If G is a finite group, then every $x \in G$ has finite order.

1.1.39 Definition [1]

If p is a prime, then a finite group G is called a *p-group* if $|G| = p^n$ for some $n \geq 0$.

1.1.40 Theorem (Higman, Neumann and Neumann) [14]

Any countable group can be embedded in a group with two generators.

2. Normal Subgroups

2.1 Definition [2]

Let H be a subgroup of the group G.If $g \in G$, the *right coset* of H generated by g is

$$Hg = \{hg : h \in H\};$$

similarly, the *left coset* of H generated by g is

$$gH = \{gh : h \in H\}.$$

It follows from the definitions that if $a, b \in G$, then

$Ha = Hb$ if and only if $ab^{-1} \in H$, and

$aH = bH$ if and only if $a^{-1}b \in H$.

Thus, if we define a and b to be equivalent if $ab^{-1} \in H$, we have an equivalence relation, and the equivalence class of a is

$$\{b : ab^{-1} \in H\} = Ha.$$

2.2 Lemma [1]

Let H be a subgroup of a group G, and let $a, b \in G$.

(i) $aH = bH$ if and only if $b^{-1}a \in H$. In particular, $aH = H$ if and only if $a \in H$.

(ii) If $aH \cap bH \neq \emptyset$, then $aH = bH$.

(iii) $|aH| = |H|$ for all $a \in G$

2.3 Definition [7]

A subgroup N of the group G is a *normal subgroup* if

$g^{-1}Ng = N$ for all $g \in G$.

We indicate that N is a normal subgroup of G with the notation N⊴ G.

2.4 Proposition [2]

If $H \leq G$ and $K \leq G$, then $HK \leq G$ if and only if $HK = KH$. In this case, HK is the subgroup generated by $H \cup K$.

2.5 Definition [7]

The group of cosets of a normal subgroup N of the group G is called the *quotient group* or the *factor group* of G by N. This group is denoted by G/N which is read "G $modulo$ N" or "G mod N".

2.6 Proposition [2]

Let N be a subgroup of G. If any of the following equivalent conditions holds, we say that N is normal subgroup of G, or that N is normal in G:

(i) $gNg^{-1} \subseteq N$ for all $g \in G$ (equivalently, $g^{-1}Ng \subseteq N$ for all $g \in G$)

(ii) $gNg^{-1} = N$ for all $g \in G$ (equivalently, $g^{-1}Ng \subseteq N$ for all $g \in G$)

(iii) $gN = Ng$ for all $g \in G$

(iv) Every left coset of N in G is also a right coset

(v) Every right coset of N in G is also a left coset

2.7 Definition [18]

The *centre of group* G is

$$\{x \in G : xa = ax \; for \; all \; a \in G\}$$

It is denoted by $Z(G)$.

2.8 Corollary [18]

The centre of group G is a normal subgroup of G.

2.9 Definition [1]

The *index* of a subgroup H in G, denoted by $[G : H]$, is the number of left cosets of H in G.

2.10 Lemma [6]

Let H be a subgroup of G of index 2. Then $a^2 \in$ H for all a $\in$ G.

3. Homomorphism

3.1 Definition [2]

If $f: G \rightarrow H$, where G and H are groups, then f is said to be a *homomorphism* if for all a, b in G, we have

$$f(ab) = f(a)f(b).$$

This idea will look familiar if G and H are abelian, in which case we write, using additive notation, $f(a + b) = f(a) + f(b)$;

thus, a linear transformation on a vector space is, in particular, a homomorphism on the underlying abelian group.

3.2 lemma [12]

Set of all homomorphism from G to H is denoted by $Hom(G, H)$ or $Hom_R(G, H)$

3.3 Proposition [2]

A homomorphism f is injective if and only if its kernel K is trivial, that is, consists only of the identity.

3.4 Lemma [2]

Some Standard Terminology

Monomorphisms = injective homomorphism

Epimorphism = surjective homomorphism

Isomorphism = bijective homomorphism

Endomorphism = homomorphism of a group to itself

Automorphism = isomorphism of a group to itself

3.5 Definition [1]

Two groups G and H are called *isomorphic*, denoted by $G \cong H$, if there exists an isomorphism $f : G \to H$ between them.

3.6 Definition [1]

A property of a group G that is shared by any other group isomorphic to it is called an *invariant* of G.

3.7 Example [1]

The order $|G|$ is an invariant of G, for isomorphic groups have the same orders. Being abelian is an invariant [if f is an isomorphism and a and b commute, then

$ab = ba$ and

$f(a) f(b) = f(ab) = f(ba) = f(b) f(a)$;

hence, $f(a)$ and $f(b)$ commute.

3.8 Definition [1]

If $f: G \to H$ is a homomorphism, define

kernel $f = \{x \in G : f(x) = 1\}$

and image $f = \{h \in H : h = f(x)$ for some $x \in G\}$.

We usually abbreviate kernel f to $ker\ f$ and image f to $im\ f$.

3.9 Example [1]

(i) If $\mu 2$ is the multiplicative group $\mu 2 = \{\pm 1\}$, then $sgn: S_n \to \mu 2$ is a homomorphism. The kernel of sgn is the alternating group A_n, the set of all even permutations.

(ii) Determinant is a surjective homomorphism $det: GL(n, R) \to R^{\times}$, the multiplicative group of nonzero real numbers, whose kernel is the special linear group $SL(n, R)$ of all $n \times n$ matrices of determinant 1.

3.10 Theorem [12]

If V and W are vector spaces over F of dimensions m and n respectively, then $Hom(V,W)$ is of dimension mn over F.

3.11 Corollaries [13]

If $f: G \longrightarrow H$ is a homomorphism, the following hold:

(i) If e is the identity of G, then $f(e)$ is the identity of H;

(ii) For all x in G and for all n in Z, $f(x^n) = \{f(x)\}^n$.

in particular, $f(x^{-1}) = \{f(x)\}^{-1}$;

(iii) If K is a subgroup of G, then $f(K)$ is a subgroup of H;

(iv) If L is a subgroup of H, then $f^{-1}(L)$ is a subgroup of G;

(v) If $x \in G$ is of finite order, then $|f(x)|$ divides $|x|$;

(vi) $f(\langle x \rangle) = \langle xf(x) \rangle$;

(vii) If G is abelian, so is $f(G)$.

3.12 Theorem [13]

Let K be a normal subgroup of the group G and denote the set right (or left) cosets by G/K on G/K define an operation "." by

$$Kg.Kh = Kgh$$

Then "."is a well-defined operation and $(G/K,.)$ is a group called the factor group $G\ mod\ K$. Furthermore, the map

$$V: G \longrightarrow G/K$$

defined by $$V(g) = Kg$$

is an epimorphism, called the *natural homomorphism* from G onto G/K, whose kernel is K.

3.13 Theorem (Factor Theorem) [2]

Any homomorphism f whose kernel K contains N can be factored through G/N. In other words, there is a unique homomorphism $\bar{f}: G/N \rightarrow H$ such that $\bar{f} \circ \pi = f$. Furthermore,

(i) $\bar{f}$ is an epimorphism if and only if f is an epimorphism;

(ii) $\bar{f}$ is a monomorphism if and only if $K = N$;

(iii) $\bar{f}$ is an isomorphism if and only if f is an epimorphism and $K = N$.

3.14 Theorem (First Isomorphism Theorem) [2]

If $f: G \rightarrow H$ is a homomorphism with kernel K, then the image of f is isomorphic to G/K.

3.15 Theorem (Second Isomorphism Theorem) [2]

If H and N are subgroups of G, with N normal in G, then

$H/(H \cap N) \cong HN/N$.

3.16 Theorem (Third Isomorphism Theorem) [2]

If N and H are normal subgroups of G, with N contained in H, then

$$G/H \cong (G/N)/(H/N),$$

a "cancellation law".

4. Direct Products

4.1 Definition [8]

Let G be a group with identity e, and let K and N be normal subgroups of G such that $K \cap N = \{e\}$. *The internal direct product* of K and N is the subgroup

$K \times N = \{kn: k \in K, n \in N\}$ of G

4.2 Definition [8]

let$G$ and H be groups with operations $\circ_G$ and $*_H$ respectively. *The external direct product*$G \oplus H$ of G and H is the Cartesian product $G \times H$, together with an operation that is,

$$(g_1, h_1)\,(g_2, h_2) = (g_1 \circ_G g_2, h_1 *_H h_2)$$

Where $g_1, g_2 \in$ G and $h_1, h_2 \in H$and $(g_1, h_1), (g_2, h_2) \in G \oplus H$.

4.3 Proposition [24]

The following properties hold, which concern the direct product of groups.

(i) The commutative property: $A \times B \simeq B \times A$.

(ii) The associative property: $A \times (B \times C) \simeq (A \times B) \times C$. This allows us to simply write multiple products without brackets, e.g., $A \times B \times C$.

(iii) The substitution property:

If $A \simeq A'$and $B \simeq B'$, then $A \times B \simeq A' \times B'$.

(iv) The cancellation property:

If $A \simeq A'$and $A \times B \simeq A' \times B'$, then $B \simeq B'$.

4.4 Theorem [8]

Let G and H be groups. Then $G \oplus H$ is also agroup.

4.5 Theorem [8]

Let G and H be groups with identities e_G and e_H, respectively. Then

$$G \oplus \{e_H\} = \{(g, e_H): g \in G\}$$

And

$$\{e_H\} \oplus H = \{(e_G, h): h \in H\}$$

are both subgroups of $G \oplus H$.

4.6 Proposition [2]

If G is the internal direct product of H and K, then G is isomorphic to the external direct product $H \times K$.

4.7 Proposition [7]

A group G is a direct product of subgroups H_1, H_2 if and only if

(i) $G = H_1H_2$,

(ii) $H_1 \cap H_2 = \{e\}$, and

(iii) every element of H_1 commutes with every element of H_2.

4.8 Proposition [7]

A group G is a direct product of subgroups H_1, H_2 if and only if

(i) G =H_1H_2,

(ii) $H_1 \cap H_2$={e}, and

(iii) H_1 and H_2 are both normal in G.

5. Abelian Group

5.1 Definition [1]

If S and T are subgroups of an abelian group G, then G is the *direct sum*, denoted by

$G = S \oplus T$,

If $S + T = G$ (i.e., for each $a \in G$, there are $s \in S$ and $t \in T$ with $a = s + t$) and $S \cap T = \{0\}$.

5.2 Theorem [24]

Let G be a group with two normal subgroups H and K, with the conditions that

$H \cap K = \{e\}$ and $HK = G$.

Then $G \simeq H \times K$.

Where $HK = \{hk: h \in H$ and $k \in K\}$

The hypothesis of this theorem is sometimes used as the definition of G being the internal direct product of H and K. In other words, the theorem states that internal implies external. Conversely, given $G = H \times K$, we have two normal subgroups, i.e., $H \times \{e\} \simeq H$ and $\{e\} \times K \simeq K$, whose internal direct product recovers G. Hence, the two notions of external and internal direct products are actually equivalent.

Proof. We first show that every element of H commutes with any other of K. Let $h \in H$ and $k \in K$. We note that

$$hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$$

Because K is normal, and similarly

$$hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$$

However, $H \cap K = \{e\}$, so we see that

$$hkh^{-1}k^{-1} = e,$$

i.e., $$hk = kh.$$

This result opens the way for a homomorphism $\theta : H \times K \to HK$ defined by

$\theta(h,k) = hk.$

As we can check,

$$\begin{aligned}\theta\big((h,k)(h',k')\big) &= \theta(hh',kk') \\ &= hh'kk' \\ &= hkh'k' \\ &= \theta(h,k)\theta(h',k')\end{aligned}$$

Since $HK = G$, we are only left with showing that θ is one-to-one and onto. Well, onto is obvious by the very definition of HK. For one-to-one, let

$$\theta(h,k) = \theta(h',k'),$$

so that $$hk = h'k'.$$

then $$h^{-1}h' = k(k')^{-1}.$$

the left side belongs to H and the right to K.

this is possible only if both be the identity element. Thus

$h = h'$ and $k = k'$,

Completing the proof.

5.2 Proposition [1]

The following statements are equivalent for an abelian group G and subgroups S and T of G.

(i) $G = S \oplus T$.

(ii) Every $g \in G$ has a unique expression of the form

$g = s + t,$

Where $s \in S$ and $t \in T$.

(iii) There are homomorphisms $p : G \to S$ and $: G \to T$, called *projections*, and $i : S \to G$ and $j : T \to G$, called *injections*, such that

$pi = 1_S, \quad qj = 1_T, \quad pj = 0, \quad qi = 0,$ and $ip + jq = 1_G$.

5.3 Remark [1]

The equations $pi = 1_S$ and $qj = 1_T$ imply that the maps i and j must be injections and the maps p and q must be surjections.

Proof. (i) ⇒ (ii) By hypothesis, $G = S + T$, so that each $g \in G$ has an expression of the form $g = s + t$ with $s \in S$ and $t \in T$. To see that this expression is unique, suppose also that $g = s' + t'$, where $s' \in S$ and $t' \in T$. Then $s + t = s' + t'$ gives $s - s' = t' - t \in S \cap T = \{0\}$. Therefore, $s = s'$ and $t = t'$, as desired.

(ii)⇒(iii) If $g \in G$, then there are unique $s \in S$ and $t \in T$ with $g = s + t$. The functions p and q, given by

$$p(g) = s \quad \text{and} \quad q(g) = t,$$

are well-defined because of the uniqueness hypothesis. It is routine to check that p and q are homomorphisms and that all the equations in the statement hold.

(iii)⇒(i) If $g \in G$, the equation $1_G = ip + jq$ gives

$$g = ip(g) + jq(g) \in S + T,$$

because $S = im\, i$ and $T = im\ j$.

If $g \in S$, then $g = ig$ and $pg = pig = g$; if $g \in T$, then $g = jg$ and $pg = pjg = 0$. Therefore, if $g \in S \cap T$, then $g = 0$. Hence,

$$S \cap T = \{0\}, \qquad S + T = G, \text{and} G = S \oplus T.$$

5.4 Corollary [1]

Let S and T be subgroups of an abelian group G. If $G = S \oplus T$, then

$$S \oplus T \cong S \times T.$$

Conversely, given abelian groups S and T, define subgroups $S' \cong S$ and $T' \cong T$ of $S \times T$ by

$$S' = \{(s, 0) : s \in S\} \quad and \quad T' = \{(0, t) : t \in T\};$$

then $S \times T = S' \oplus T'$.

Proof. Define $f : S \oplus T \to S \times T$ as follows. If $\in S \oplus T$, then the proposition says that there is a unique expression of the form $a = s + t$, and so $f : a \mapsto (s, t)$ is a well-defined function. It is routine to check that f is an isomorphism.

Conversely, if $= (s, t) \in S \times T$, then

$$g = (s, 0) + (0, t) \in S' + T'$$

And $S' \cap T' = \{(0, 0)\}.$

Hence, $S \times T = S' \oplus T'.$

5.5 Definition [1]

If $S_1, S_2, \ldots, S_n$ are subgroups of an abelian group G, define the *finite direct sum* $S_1 \oplus S_2 \oplus \cdots \oplus S_n$ using induction on $n \geq 2$:

$$S_1 \oplus S_2 \oplus \cdots \oplus S_{n+1} = [S_1 \oplus S_2 \oplus \cdots \oplus S_n] \oplus S_{n+1}.$$

We will also denote the direct sum by

$$\sum S_i = S_1 \oplus S_2 \oplus \cdots \oplus S_n.$$

5.6 Proposition [1]

If $G_1, G_2, \ldots, G_n$ are abelian groups and $H_i \subseteq G_i$ are subgroups, then

$$(G_1 \oplus \cdots \oplus G_n)/(H_1 \oplus \cdots \oplus H_n) \cong (G_1/H_1) \times \cdots \times (G_n/H_n).$$

Proof. Define $f : G_1 \oplus \cdots \oplus G_n \to (G_1/H_1) \oplus \cdots \oplus (G_n/H_n)$ by

$$(g_1, \ldots, g_n) \mapsto (g_1 + H_1, \ldots, g_n + H_n).$$

Since f is a surjective homomorphism with

$$\ker f = H_1 \oplus \cdots \oplus H_n,$$

the first isomorphism theorem gives the result.

If G is an abelian group and m is an integer, let us write

$$mG = \{ma : a \in G\}.$$

It is easy to see that mG is a subgroup of G.

5.7 Definition [1]

Let $F = \langle x_1, \ldots, x_n \rangle$ be an abelian group. If $F = \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle$,

Where each $\langle x_i \rangle \cong Z$, then F is called a (finitely generated) *free abelian group* with *basis* $x_1, \ldots, x_n$.

More generally, any group isomorphic to F is called a *free abelian group.*

5.8 Theorem [7]

Le F be free abelian with basis $X = \{x_i : i \in I\}$, G an arbitrary abelian group and $f : X \to G$ any function. Then there is a unique homomorphism $\theta : F \to G$ such that

$$\theta(x_i) = f(x_i), \text{ for all } i \in I$$

Proof. If $Z_i = \langle x_i \rangle$, define $f_i : Z_i \to G$ by $f_i(mx_i) = mf(x_i)$. It is easy to see that f_i is a homomorphism. To define θ let $x \in F$. Then there are uniquely determined integer coefficients such that $x = \sum_{i \in I} c_i x_i$. We define θ by

$$\theta(x) = \sum_{i \in I} f_i(c_i x_i) = \sum_{i \in I} c_i f(x_i).$$

Because each f_i is a homomorphism it follows that θ is a homomorphism. If $\psi : F \to G$ is another homomorphism such that $\psi(x_i) = f(x_i)$, for all $i \in I$, then $\psi(x) = \sum_i \psi(c_i x_i) = \sum_i c_i \psi(x_i) = \sum_i c_i f(x_i) = \theta(x)$.

5.9 Theorem [7]

Every abelian group G is a quotient of a free abelian group.

5.10 Proposition [1]

If Z^m denotes the direct sum of m copies of Z, then $Z^m \cong Z^n$ if and only if $m = n$.

Proof. First, for any abelian group G, that if

$G = G_1 \oplus \cdots \oplus G_n$, then $2G = 2G_1 \oplus \cdots \oplus 2G_n$. It follows that

$$G/2G \cong (G_1/2G_1) \oplus \cdots \oplus (G_n/2G_n),$$

so that $|G/2G| = 2^n$.

Similarly, if $H = Z^m$,

then $|H/2H| = 2^m$.

Finally, if $G = Z^n \cong Z^m = H$,

Then $G/2G \cong H/2H \quad and \quad 2^n = 2^m$.

We conclude that $n = m$.

Proof. If $x_1, \ldots, x_n$ is a basis of F, then $F \cong Z^n$, and if $y_1, \ldots, y_m$ is another basis of F, then $F \cong Z^m$. Therefore, $m = n$.

5.11 Definition [1]

If F is a free abelian group with basis $x_1, \ldots, x_n$, then n is called the *rank* of F, and we write $rank(F) = n$.

5.12 Definition [7]

An abelian group G has generators $X = \{x_1, x_2, \ldots, x_n\}$ and relations

$$\sum_{j=1} a_{ij} x_n = 0 \, , i = 1,2, \ldots, m$$

in case $G \cong F/R$, where F is a free abelian on X and R is the subgroup generated by $\{\sum_{j=1}^{n} a_{ij} x_n : i = 1,2, \ldots, m\}$

5.13 Proposition [6]

Let H be a normal subgroup of G. Then G/H is abelian if and only if $[x, y] \in H$ for all $x, y \in G$.

Proof. First assume that G/H is abelian and take any x, y in G. Then the product of the factor groups' xH and yH can be written as

$$(xy)H = (xH)(yH) = (yH)(xH) = (yx)H.$$

The factor group containing $[x, y]$ can be written as

$$\begin{aligned}(xyx^{-1}y^{-1})H &= ((xy)(yx)^{-1})H \\ &= (xy)H(yx)^{-1}H \\ &= (yx)H(yx)^{-1}H \\ &= ((yx)(yx)^{-1})H \\ &= H.\end{aligned}$$

Therefore, we conclude that $xyx^{-1}y^{-1} = [x, y]$ must be in H.

Assume that $[x, y] \in H$ for any $x, y \in G$. Since H is normal, then G/H is defined and $[\, y^{-1}, x^{-1}]H = H$. Recall this is the identity element, so

$$\begin{aligned}(xy)H &= (xy)H\,[y^{-1}, x^{-1}]H \\ &= ((xy)\,[y^{-1}, x^{-1}])H \\ &= ((xy)(y^{-1}x^{-1})(yx))H \\ &= (yx)H.\end{aligned}$$

Hence,

$$(xH)(yH) = (xy)H$$
$$= (yx)H$$
$$= (yH)(xH).$$

Therefore, G/H is abelian.

5.14 Proposition [6]

Let G be a group.

(i) The derived subgroup G' is normal in G.

(ii) The derived subgroup G' is the smallest normal subgroup of G such that G/G' is abelian, or more precisely, if H is a normal subgroup of G, then G/H is abelian if and only if $G' \subseteq H$.

Proof. For (i), it will suffice to show that any element $x' = [x, y] \in G'$ and $g \in G$ exhibits $g^{-1}x'g\ G'$. Since we have $x' = [x, y] = xyx^{-1}y^{-1}$, then we will insert $e = g^{-1}g$ between each element of $xyx^{-1}y^{-1}$to obtain

$$xyx^{-1}y^{-1} = x(gg^{-1})y(gg^{-1})x^{-1}(gg^{-1})y^{-1}$$

From the product$g^{-1}[x, y]g$ we obtain

$$g^{-1}[x, y]g = g^{-1}(xgg^{-1}ygg^{-1}x^{-1}gg^{-1}y^{-1})g$$
$$= (g^{-1}xg)(g^{-1}yg)(g^{-1}x^{-1}g)(g^{-1}y^{-1}g)$$
$$= (g^{-1}xg)(g^{-1}yg)(g^{-1}xg)^{-1}(g^{-1}yg)^{-1}$$
$$= [g^{-1}xg, g^{-1}yg].$$

Therefore, $g^{-1}x'g \in G'$.

For (ii), first note that if $G' \subseteq H$, then any element $[x, y] \in G'$ is also in H. From here, we can directly apply Proposition 3.1.16to justify the claim that G/H is abelian if and only if $G' \subseteq H$.

5.15 Theorem [13]

If $G/Z(G)$is cyclic, then G is abelian.

Proof. Letting $Z(G) = Z$, we have $G = \bigcup_{m\in Z} a^m Z$ since G/Z is cyclic. If b and c are elements of G there exist z_1 and z_2 in Z and p and q in Z such that $b = a^p z_1$ and c= $a^q z_2$. Therefore

$bc = a^p z_1 a^q z_2 = a^{q+q} z_1 z_2 = a^p a^q z_1 z_2$=$a^q z_2 a^p z_1 = cb$

since z_1 and z_2 are in the centre of G.

6. Basis Theorem

It will be convenient to analyze abelian groups "one prime at a time." Recall that a *p-group* is a finite group G of order p^k for some $k \geq 0$. When working wholly in the context of abelian groups, p-groups are called

p-primary groups.

6.1 Definition [1]

If p is a prime, then an abelian group G is *p-primary* if, for each $a \in G$, there is $n \geq 1$ with $p^n a = 0$.

If G is any abelian group, then its *p-primary component* is

$G_p = \{a \in G : p^n a = 0 \text{ for some } n \geq 1\}$.

6.2 Theorem (Primary Decomposition) [1]

(i) Every finite abelian group G is a direct sum of its p-primary components:

$$G = G_{p_1} \oplus \cdots \oplus G_{p_n}.$$

(ii) Two finite abelian groups G and G' are isomorphic if and only if $G_p \cong G'_p$ for every prime p.

Proof. (i) Let $x \in G$ be nonzero, and let its order be d. There are distinct primes $p_1, \ldots, p_n$ and positive exponents $e_1, \ldots, e_n$ with

$d = {p_1}^{e_1} \cdots {p_n}^{e_n}$.

Define $r_i = d/{p_i}^{e_i}$, so that $p_i^{e_i} r_i = d$. It follows that $r_i x \in G_{p_i}$ for each i (because $dx = 0$). But the gcd d of $r_1, \ldots, r_n$ is 1 (the only possible prime divisors of d are $p_1, \ldots, p_n$; but no p_i is a common divisor because $p_i \nmid r_i$); hence, there are integers $s_1, \ldots, s_n$ with $1 = \sum_i s_i r_i$. Therefore,

$$x = \sum_i s_i r_i \, x \in G_{p_1} + \cdots + G_{p_n}.$$

Write $H_i = G_{p_1} + G_{p_2} + \cdots + \hat{G}_{p_i} + \cdots + G_{p_n}$. It suffices to prove that if

$$x \in G_{p_i} \cap H_i,$$

then $x = 0$. Since $x \in G_{p_i}$, we have $p_i^{\ell} i x = 0$ for some $\ell \geq 0$; Since $x \in H_I$, we have $x = \sum_{j \neq i} y_j$, where $p_j^{g_i} y_j = 0$; hence, $ux = 0$, where $u = \prod_{j \neq i} p_j^{g_i}$. But p_i^{ℓ} and u are relatively prime, so there exist integers s and t with $1 = sp_i^{\ell} + tu$.

Therefore,

$$x = \left(sp_i^{\ell} + tu\right)x = sp_i^{\ell} x + tux = 0$$

(ii) If $f : G \to G'$ is a homomorphism, then $f(G_p) \subseteq G'_p$ for every prime p, for if $p^{\ell} a = 0$, then

$$0 = f\left(p^{\ell} a\right) = p^{\ell} f(a).$$

If f is an is omorphism then $f^{-1} : G' \to G$ is also an isomorphism [so that $f^{-1}(G'_p) \subseteq G_p$ for all p]. It follows that each restriction $f|G_p : G_p \to G'_p$ is an isomorphism, with inverse $f^{-1}|G'_p$. Conversely, if there are is omorphisms $f_p : G_p \to G'_p$ for all p, then there is an isomorphism $\phi: \sum_p G_p \to \sum_p G'_p$ given by $\sum_p a_p \mapsto \sum_p f(a_p)$.

6.3 Definition [1]

Let p be a prime and let G be a p-primary abelian group. A subgroup $S \subseteq G$ is a *pure subgroup* if, for all $n \geq 0$,

$S \cap p^n G = p^n S.$

6.4 Lemma [1]

If p is a prime and G is a finite p-primary abelian group, then G has a nonzero pure cyclic subgroup.

6.5 Theorem (Cauchy) [24]

Let p be a prime number. If any abelian group G has order,a multiple of p, then G must contain an element of order p.

Proof. Let $|G| = kp$ for some $k \geq 1$. In fact, the claim is true if $k = 1$ because any group of prime order is a cyclic group, and in this case any non-identity element will have order p. We proceed by induction. Take any non-identity element $x \in G$, say of order m. We are done if $p$divides m, for then $x^{m/p}$will have order p. Otherwise, consider the factor group $G' = G/\langle x \rangle$, of order $|G'| = kp/m$. Since m is not a multiple of p, we may write $|G'| = jp$ for some $j < k$. We apply the induction hypothesis to conclude that G' contains an element of order p. According to the preceding exercise, then G contains an element of order a multiple of p, and that suffices.

6.6 Theorem [1]

If $a \in G$ is an element of order n, then $a^m = 1$ if and only if $n \mid m$

Proof. Assume that $a^m = 1$. The division algorithm provides integers q and r with $m = nq + r$,where $0 \leq r < n$. It follows that

$$a^r = 1 = a^{m-nq} = a^m a^{-nq} = 1.$$

If $r > 0$, then we contradict n being the smallest positive integer with $a^n = 1$. Hence, $r = 0$and $n \mid m$. Conversely, if $m = nk$, then

$a^m = a^{nk} = (a^n)^k = 1^k = 1.$

6.7 Theorem (Basis Theorem) [1]

Every finite abelian group G is a direct sum of cyclic groups of prime power orders.

Proof. By the primary decomposition, Theorem 3.2.2, we may assume that G is

p-primary for some prime p. We prove that G is a direct sum of cyclic groups by induction on $d(G) \geq 1$. The base step is easy, G must be cyclic in this case. To prove the inductive step, we begin to find a nonzero pure cyclic subgroup $S \subseteq G$. We have

$$d(G/S) = d(G) - d(S) = d(G) - 1 < d(G)$$

By induction, G/S is a direct sum of cyclic groups, say:

$$G/S = \sum_{i=1}^{q} \langle \bar{x}_i \rangle,$$

where $\bar{x}_i = x_i + S$.

Let $x \in G$ and let $\bar{x}$ have order p^ℓ, where $\bar{x} = x + S$. We claim that there is

$z \in G$ with $z + S = \bar{x} = x + S$ such that

order z = order (x).

Now x has order p^n, where $n \geq \ell$.. But$p^\ell(x + S) = p^\ell \bar{x} = 0inG/S$, so there is some $s \in S$ with $p^\ell x = s$.By purity, there is $s' \in S$ with $p^\ell x$=$p^\ell s'$. If we define $z = x - s'$, then$p^\ell z = 0$ and $z + S = x + S = \bar{x}$. Ifz has order p^m, then

$m \geq \ell$ because $z \mapsto \bar{x}$; since $p^\ell z = 0$, the order of z equals p^ℓ.

For each i, choose $z_i \in G$ with $z_i + S = x_i = x_i + S$ and with order

z_i = order x_i; define T by

$$T = \langle z_1, \ldots, z_q \rangle.$$

Now $S + T = G$, because G is generated by S and the z_i's. To see that $G = S \oplus T$, it now suffices to prove that $S \cap T = \{0\}$. If$y \in S \cap T$, then $y = \sum_i m_i z_i$, where $m_i \in Z$. Now$y \in S$, and so$\sum_i m_i \bar{x}_i = 0$inG/S. Since this is a direct sum, each $m_i \bar{x}_i = 0$; after all, for each i,

$$-m_i \bar{x}_i = \sum_{j \neq i} m_j \bar{x}_j \in \langle \bar{x}_i \rangle \cap (\langle \bar{x}_1 \rangle + \cdots + \widehat{\langle \bar{x}_i \rangle} + \cdots + \langle \bar{x}_q \rangle) = \{0\}.$$

Therefore, $m_i z_i = 0$ for all i, and hence $y = 0$. Finally, $G = S \oplus T$ implies

$d(G) = d(S) + d(T) = 1 + d(T)$,

so that $d(T) < d(G)$. By induction, T is

a direct sum of cyclic groups, and this completes the proof.

6.8 Theorem (Fundamental Theorem for Finite Abelian Group) [6]

Any finite abelian group is isomorphic to a direct sum of cyclic groups of prime power orders.

Proof. Let $|G| = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$where each of the p_i are distinct primes. We get $G \cong G(p_1) \times \cdots \times G(p_l)$. Then each of the $G(p_i)$ can be decomposed further such that $G(p_i) \cong C_{p_i}^{n_1} \times C_{p_i}^{n_2} \times \cdots \times C_{p_i}^{n_{t_i}}$ where C_x is a cyclic group of order x. Therefore, we have that G is omrophic to a direct product of cyclic groups of prime power order.

6.9 Example [6]

Suppose G is a finite abelian group of order $360 = 2^3 \cdot 3^2 \cdot 5$. Then G is isomorphic to one of the following:

$$C_8 \times C_9 \times C_5 \cong C_{360}$$
$$C_8 \times C_3 \times C_3 \times C_5$$
$$C_2 \times C_4 \times C_9 \times C_5$$
$$C_2 \times C_4 \times C_3 \times C_3 \times C_5$$
$$C_2 \times C_2 \times C_2 \times C_9 \times C_5$$
$$C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5$$

6.10 Theorem [7]

Every finite Abelian group is the direct sum of cyclic p-groups.

Proof. Let A be a finite abelian group. We write

$A = P_1 \oplus P_2 \oplus + \cdots + P_k,$

Where P_i is the Sylow-p_i subgroup of $A, i = 1,2,\ldots,k$. Replace each P_i with a direct sum of cyclic groups.

6.11 Theorem (Existence of Subgroups of Abelian Groups) [1]

If G is a finite abelian group and d is a divisor of $|G|$, then G contains a subgroup of order d.

Proof. We prove the result by induction on $n = |G|$ for a prime divisor p of $|G|$. The base step $n = 1$ is true, for there are no prime divisors of 1. For the inductive step, choose $a \in G$ of order $k > 1$.If $p \mid k$, say $k = p\ell$ so a^{ℓ}

has order p. If $p \nmid k$, consider the cyclic subgroup $H = \langle a \rangle$.

Now $H \lhd G$, because G is abelian, and so the quotient group G/H exists. Note that $|G/H| = n/k$ is divisible by p, and so the inductive hypothesis gives an element $bH \in G/H$ of order p. If b has order m, then $p \mid m$. We have returned to the first case.

Let d be any divisor of $|G|$, and let p be a prime divisor of d. We have just seen that there is a subgroup $S \leq G$ of order p. Now $S \lhd G$, because G is abelian, and G/S is a group of order n/p. By induction on $|G|$, G/S has a subgroup H^* of order d/p. The correspondence theorem gives $H^* = H/S$ for some subgroup H of G containing S, and $|H| = |H^*||S| = d$.

6.12 Example [7]

1) Let G be an Abelian group of order $72 = 2^3 \cdot 3^2$, and suppose we want to create a subgroup of order 12. By the Fundamental Theorem of Finite Abelian Groups, we know G is isomorphic to one of the following:

$$Z_8 \oplus Z_9$$
$$Z_8 \oplus Z_3 \oplus Z_3$$
$$Z_4 \oplus Z_2 \oplus Z_9$$
$$Z_4 \oplus Z_2 \oplus Z_3 \oplus Z_3$$
$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_9$$
$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3$$

we already know that $Z_8 \oplus Z_9 \approx Z_{72}$ has a subgroup of order 12. Suppose that we want to produce a subgroup of order 12in $Z_4 \oplus Z_2 \oplus Z_9$. We can do this by piecing together all of Z_4 and the subgroup of order 3in Z_9. In other words, we get $\{(a, 0, b) \mid a \in Z_4, b \in \{0,3,6\}\}$.

2)Let G be an Abelian group of order $45 = 5 \cdot 3^2$.we know G is isomorphic to one of the following:

$$Z_5 \oplus Z_9$$
$$Z_{15} \oplus Z_3$$
$$Z_5 \oplus Z_3 \oplus Z_3$$

Now we know that $Z_5 \oplus Z_9 \approx Z_{45}$ has a subgroup of order 15.

6.13 Remark [13]

Let p be a prime. We set $G_p := \{x \in G \mid x \text{ is a } p\text{-element}\}$.

6.14 Theorem [13]

Let G be an Abelian group. Then G_p is a characteristic p-subgroup of order $|G|_p$.

Proof. For $x, y \in G_p$ also xy is a p-element; use $xy = yx$. Thus, G_p is a subgroup. Since automorphisms map p-elements to p-elements, this subgroup is characteristic.

Then G contains a subgroup P of order $|G|_p$. Hence, P is a p-group, and thus every element of P is a p-element; in particular $P \leq G_p$. If $P \neq G_p$, then

$$k := |G_p : P| \neq 1$$

and $(k, p) = 1$ (Lagrange's theorem). But now theorem 3.2.12gives a subgroup K of order k in G_p since every element of K is a p-element.

6.15 Theorem [13]

Let G be an Abelian group. Then $G = \times_{p \in \pi(G)} G_p$

Proof. The product G_1 of the subgroups $G_p, p \in \pi(G)$, is a direct product; and theorem 3.2.15yields

$|G_1| = \prod_{p \in \pi(G)} |G_p| = \prod_{p \in \pi(G)} |G|_p = |G|$,

so $G_1 = G$.

In an Abelian group, the product of two cyclic groups of coprime order is again cyclic. Hence, the question whether an Abelian group is cyclic or not can already be decided in the subgroups $G_p, p \in \pi(G)$.

6.16 Definition [13]

An Abelian p-group is *elementary Abelian* if $x^p = 1$ for all $x \in G$.

6.17 Theorem [13]

α_k is an automorphism of the Abelian group G, if and only if $(k, |G|) = 1$.

Proof. If $(k, |G|) = 1$, then Ker $\alpha_k = 1$. Conversely, if $(k, |G|) = 1$, then there exists a common prime divisor p of k and $|G|$. The p-subgroup G_p is nontrivial, and there exists a subgroup of order p in G. This subgroup is contained in Ker α_k. This gives for cyclic groups.

6.18 Lemma [1]

Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times K$, where

$H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$.

Also, $|H| = p^n$.

6.19 Lemma [1]

Let G be an Abelian group of prime-power order and let a be an element of maximal order in G. Then G can be written in the form $< a > \times K$.

6.20 Proposition [6]

Let G be a group with identity element e and suppose $a^2 = e$ for all $a \in G$. Then G is an abelian group.

Proof. Suppose that for every $a \in G, a^2 = e$. Let $a_1, a_2 \in G$. Then

$$(a_1a_2)^2 = (a_1a_2)(a_1a_2) = e,$$

by our hypothesis. Multiplying both sides of the equation $e = (a_1a_2)(a_1a_2)\ by\ a_2a_1$ gives

$$(a_2a_1)e = (a_2a_1)(a_1a_2)(a_1a_2).$$

So

$$a_2a_1 = a_2(a_1a_1)a_2a_1a_2$$
$$= a_2(a_1)^2a_2a_1a_2$$
$$= (a_2)^2(a_1a_2)$$
$$= a_1a_2.$$

Hence, G is indeed abelian.

6.21 Corollary [12]

Any group of order $|G| = p^2$ with p prime is abelian.

6.22 Definition [1]

If G is an abelian group, then its *exponent* is the smallest positive integer m for which $mG = \{0\}$.

6.23 Corollary [1]

If G is a finite abelian group and $G = S(c_1) \oplus S(c_2) \oplus \cdots \oplus S(c_t), S(c_i)$ is a cyclic group of order c_i and $c_1 \mid c_2 \mid \cdots \mid c_t$, then c_t is the exponent of G.

Proof. Since $c_i \mid c_t$ for all i, we have $c_t S(c_i) = 0$ for all i, and so $c_tG = \{0\}$. On the other hand, there is no number e with $1 \leq e < c_t$ with $eS(c_t) = \{0\}$, and so c_t is the smallest positive integer annihilating G.

7. The Sylow Theorem

This section discusses the Sylow's theorem and its related results for finite case only.

7.1 Definition [7]

A finite group G is a *p-group* if $|G| = p^x$, for some prime p and positive integer x. A maximal p-subgroup of a finite group G is called a *Sylow-p subgroup* of G.

7.2 Lemma [7]

If P is a Sylow-p subgroup of G and H is a p-subgroup of G such that $P \subseteq H$, then $H = P$.

7.3 Definition [7]

Let H be a subgroup of a group G. A subgroup S of G is *conjugate* to H if and only if $S = g^{-1}Hg$ for some $g \in G$.

7.4 Definition [7]

Let H be a subgroup of G. The *normalizer* of H in G is

$$N_G(H) = \{g \in G : g^{-1}Hg = H\}$$

7.5 Lemma [1]

Let P be a Sylow p-subgroup of a finite group G.

(i) Every conjugate of P is also a Sylow p-subgroup of G.

(ii) $|N_G(P)/P|$ is prime to p.

(iii) If $a \in G$ has order some power of p and if $aPa^{-1} = P$, then $a \in P$.

7.6 Corollary [1]

A finite group G has a unique Sylow p-subgroup P, for some prime p, if and only if $P \lhd G$.

Proof. Assume that P, a Sylow p-subgroup of G, is unique. For each $a \in G$, the conjugate aPa^{-1} is also a Sylow p-subgroup; by uniqueness, $aPa^{-1} = P$ for all $a \in G$, and so $P \lhd G$.

Conversely, assume that $P \lhd G$. If Q is any Sylow p-subgroup, then $Q = aPa^{-1}$ for some $a \in G$; but $aPa^{-1} = P$, by normality, and so $Q = P$.

7.7 Theorem (Sylow) [1]

If G is a finite group of order $p^e m$, where p is a prime and $p \nmid m$, then G has a subgroup of order p^e.

Proof. We first show that $p \nmid [G : P]$. Now

$$[G : P] = [G : N_G(P)][N_G(P) : P].$$

The first factor, $[G : N_G(P)] = r$, is the number of conjugates of P in G, and so p does not divide $[G : N_G(P)]$ because $r \equiv 1 \bmod p$.

The second factor, $[N_G(P) : P] = |N_G(P)/P|$, is also not divisible by p, by Lemma 3.3.5. Therefore, p does not divide $[G : P]$, by Euclid's lemma.

Now $|P| = p^k$ for some $k \leq e$, and so

$$[G : P] = |G|/|P| = p^e m/p^k = p^{e-k}m.$$

Since p does not divide $[G : P]$, we must have $k = e$; that is, $|P| = p^e$

7.8 Proposition [12]

Let G be a group of order pq where $p > q$ are primes with $q \nmid p - 1$. Then G is cyclic. More precisely, let P be a p-Sylow group (or Sylow p-group) and Q a q-Sylow group of G. Pick $x \epsilon P \setminus \{e\}$ and $y \epsilon Q \setminus \{e\}$. Then xy generates G.

In this section we study the structure of A-groups, finite groups all of whose Sylow subgroups are abelian.

7.9 Definition [6]

An *A-group* is a finite group, all of whose Sylow subgroups are abelian.

7.10 Definition [6]

Let G be a normal subgroup of $G_\circ$. If for every prime p, with $p \mid \mid G \mid$, a Sylow p-subgroup of $G_\circ$ is abelian, then we call $(G_\circ, G)$ an A-*pair*.

7.11 Remark [6]

If $(G_\circ, G)$ is an A-pair, then G is an A-group.

7.12 Theorem [3]

Let G be a group with abelian Sylow p-subgroup. Then

$$p \nmid |G' \cap Z(G)|.$$

7.13 Theorem [7]

Let G be a finite group and $p \neq q$ prime integers. If G does not have any elements of order pq, then one of the following holds:

(i) The Sylow$p$-subgroups or the Sylow q-subgroups of G are abelian.

(ii) $G/O_{\{p,q\}'}(G) = M$ and $\{p, q\} = \{5,13\}$ or $\{7,13\}$.

7.14 Theorem [7]

For a given prime p, all Sylow p-subgroups of G are conjugate to each other.

Proof. If a Sylow p-subgroup is unique, then it is equal to all its conjugations and thus normal. If there are multiple Sylow p-subgroups, they must be conjugate to each other, so none of them can be closed under conjugation, prohibiting normality. Since any subgroup of an abelian group is normal, a Sylow p-subgroup must be unique.

8. Factoring Finite Abelian Groups

8.1 Definition [18]

The sum of subsets $A_1, A_2,\ldots,A_r$ of a group G is the subset of all elements of the form $\sum_{i=1}^{r} a_i$, where $a_i \in A_i$ for each i. If the direct sum of subsets equals G, we call this *a factorization* of the group G.

The notation $A + g$ is used to denote the set of all elements $\{a + g: a \in A\}$. In a factorization, each subset A_i may be replaced by $A_i + g_i$ for any elements $g_i \in G$.

8.2 Definition [18]

A subset A of a group G is said to be *periodic* if there exists a non-zero element g of G such that $A + g = A$.

8.3 Remark [18]

The set H of these periods, together with 0, forms a subgroup of G. Clearly A is a union of cosets of H. Equivalently, there exists a subset D such that $A = H + D$, where D is non-periodic.

If $G = A_1+A_2+\ldots+A_r$ is a factorization in which $A_1 = H + D_1$ then we obtain a factorization of the quotient group G/H. If, again, one factor is periodic, this process may be continued.

8.4 Definition [18]

A group has been called *good* if in every factorization involving two factors one factor must be periodic.

8.5 Definition [18]

The group is called k-*good* if this holds true for factorizations involving k factors.

8.6 Definition [18]

A factorization is said to be *bad* if none of the factors is periodic.

8.7 Proposition [18]

The cyclic group of order n is denoted by $Z(n)$. The subgroup generated by a subset A of a group G is denoted by $\langle A \rangle$. If A and B are non-periodic subsets and if the sum $\langle A \rangle + B$ is direct then it has been shown that $A + B$ is non-periodic.

8.8 Lemma [18]

Let a group G be a direct sum of subgroups H, K of relatively prime orders. Let $G = A + B$ be a factorization of G such that $|A|$ divides $|H|$. Then $G = A_H + B$ is also a factorization.

Proof. Let $|H| = m,\ |K| = n.$ Since m and n are relatively prime, there exists k such that $kn \equiv 1\ (mod\ m)$. Since $|A|$ divides m, it follows that $|A|$ and kn are relatively prime. It follows that $knA + B = G$ is a factorization. Since $knA = a_H$, it follows that $A_H + B = G$ is a factorization. We should note that this implies that the elements $\{a_H : a \in A\}$ are distinct.

8.9 Theorem [18]

Let G be a cyclic group and let there be a factorization of G in which each factor has either prime power order or order equal to the product of two primes. Then one of the factors is periodic.

Proof. Let G have order n and generator g. Let χ be a character of G such that $\chi(g)$ is an nth primitive root of unity. It follows that if $\chi(A_i) = 0$ where $|A_i|$ is a prime power then A_i is periodic. So we may assume that $G = A_1 + \cdots + A_u + \cdots + A_k$, where $\chi(A_i) = 0$ if and only if $i \leq u$ and that, for these values of i, $|A_i| = p_i q_i$ where p_i, q_i are distinct primes. Let B_i be the $(G_{p_i} + G_{q_i})$-component of A_i. By the lemma we may replace A_i by B_i to obtain the factorization $G = B_1 + \cdots + B_u + A_{u+1} + \cdots + A_k$. From above for some value of i we must have $\chi(B_i) = 0$. We may assume that $\chi(B_1) = 0$ and, for convenience, that $|B_1| = pq$.

Let $n = p^e q^f m$, where m is not divisible by p or by q. Let a, b, c of orders p^e, q^f, m, respectively, be a generating set for G. As already noted, since B_1 is a subset of Z($p^e q^f$), $\chi(B_1) = 0$ implies that B_1 is periodic. Since $|B_1| = pq$, it has a period of order p or of order q. Without loss of generality, we may assume that $p^{e-1}a$ is a period of B_1. Let $H = \langle p^{e-1}a \rangle$. Then there is a subset D of order q such that $B_1 = H + D$. By the lemma, the elements of B_1 and so also of D are distinct. Let $D = \bigcup_{j=1}^{q} (r_j\, a + s_j\, b)$. From the form of H we may assume that $0 \leq r_j < p^{e-1}$. Then from $B_1 = H + D$ it follows that

$$A_1 = \bigcup_{i=0}^{p-1} \bigcup_{j=1}^{q} ((ip^{e-1} + r_j)\, a + s_j\, b + e(i,j)c)$$

where $0 \leq s_j < q^f$, $0 \leq e(i,j) < m$.

Since $\chi(g)$ has order n, it follows that $\chi(a) = \alpha, \chi(b) = \beta, \chi(c) = \gamma$ have orders p^e, q^f, m, respectively. Then $\chi(A_1) = 0$ implies that

$\sum_{i=0}^{p-1} \sum_{j=1}^{q} \alpha^{ip^{(e-1)}+r_j} \beta^{s_j} \gamma^{e(i,j)} = 0$.

It follows that the polynomial obtained by replacing α by x is divisible by $F_{p^e}(x)$. Thus, the coefficients of $x^r, x^{r+p^{e-1}}, \ldots, x^{r+(p-1)p^{e-1}}$ in this polynomial are equal. Hence

$$\sum_{r_j=r} \beta^{s_j} \gamma^{e(i,j)} = \cdots = \sum_{r_j=r} \beta^{s_j} \gamma^{e(p-1,j)}.$$

As before, it follows that $F_{q^f}(x)$ divides, for each i and i', the polynomial

$$\sum_{r_j=r} x^{s_j} \gamma^{e(i,j)} - \sum_{r_j=r} x^{s_j} \gamma^{e(i\prime,j)}.$$

So the coefficients in this polynomial of $x^s, x^{s+qf-1}, \ldots, x^{s+(q-1)qf-1}$ are all equal. Now the pairs (r_j, s_j) are distinct. Thus, for a given pair $(r, s + tq^{f-1})$, there is either a unique j with (r_j, s_j) equal to this pair or else no such j exists at all. So, the coefficient in the above polynomial of $x^{s+t\,qf-1}$ is either of the form $\gamma^{e(i,j)} - \gamma^{e(i',j)}$ or else is 0 as no such j exists.

Suppose for a given r that both situations arise. Then all coefficients are 0 for this value of r. Thus $\gamma^{e(i,j)} = \gamma^{e(i',j)}$ for the v values of t for which such coefficients arise, where $1 \leq v < q$. Since the occurrence of (r_j, s_j) does not involve i, this occurs for all pairs i and i'. So, for this value of r, vp terms are involved. For any other value, say $'$, there must be fewer than pq terms involved and so the same result arises. Hence $e(i,j) = e(i',j)$ for all i, i' and j. Therefore A_1 is periodic with period $p^{e-1}a$.

So we may assume that r, s exist such that all q values of $(r, s + tq^{e-1})$,

$0 \le t < q$, do occur. This gives all pq terms in A_1 and since $0 \in A_1$, it follows that $B_1$is the subgroup of order pq. So in this case we have

$$A_1 = \bigcup_{i=0}^{p-1} \bigcup_{j=1}^{q} ((ip^{e-1}a + jq^{f-1}b + e(i,j)c).$$

Then, as above, we obtain that for all i, i', j, j',

$$\gamma^{e(i,j)} - \gamma^{e(i',j)} = \gamma^{e(i,j')} - \gamma^{e(i',j')}$$

These are complex numbers of modulus 1 and from an Argand diagram it is easy to see that they must be equal in pairs. So three cases can arise as follows:

(Case 1) $e(i,j) = e(i,j')$ and $e(i',j) = e(i',j')$;

(Case 2) $e(i,j) = e(i',j)$ and $e(i,j') = e(i',j')$;

(Case 3) $e(i,j) = e(i',j') + m/2$ and $e(i',j) = e(i,j') + m/2$.

The third case, in which $\gamma^{e(i,j)} = -\gamma^{e(i',j')}$, can only arise if m is even. We recall that $0 \le e(i,j) < m$ and all sums being taken modulo m.

Firstly, let us assume that only cases Case 1 and Case 2 occur. If, for a given i,

$e(i,j) = e(i,j')$ for all j, j' then it follows that for all $i', j, j' we\ have$

$e(i',j) = e(i',j')$. Hence $q^{f-1}b$ is a period of A_1. So we may suppose that for each i there exists s, s' such that $e(i,s) \neq e(i,s')$. Then Case 2 holds for this pair s, s' and for all i'. So $e(i,s) = e(i',s)$. By Case 2, $e(i,j') = e(i',j')$ for alli', j'. Hence $e(i',j') = e(r,j')\big(= e(i,j')\big)$for all i', r, j'. It follows that A_1 is periodic with period$p^{e-1}a$. Now we may suppose that r, r' and s, s' exist such that neither Case 1 nor Case 2 is satisfied. Then m must be even and

$e(r,s) = e(r',s') + m/2, e(r',s) = e(r,s') + m/2$.

Let $\gamma^{e(r,s)} = \rho, \gamma^{e(r',s)} = \sigma$. Then as $\gamma^{m/2} = -1$ we have that $\gamma^{e(r',s')} = -\rho$,

$\gamma^{e(r,s')} = -\sigma$Since neither Case 1 nor Case 2 is satisfied, it follows that

$\rho \neq \sigma, \rho \neq -\sigma$. Since m is even, it follows that pq is odd and so that we may replace A_1 by $2A_1$. If $\chi(2A_1) = 0$ then, as above using $2a, 2b$ as generators, we obtain that

$$\gamma^{2e(i,j)} - \gamma^{2e(i',j)} = \gamma^{2e(i,j')} - \gamma^{2e(i',j')}.$$

For r, r' ands, s', this implies that $\rho^2 - \sigma^2 = \sigma^2 - \rho^2$.This gives $\rho = \sigma$ or $\rho = -\sigma$ Which is false. We may now proceed by induction on u. If $u = 1$, we would have the contradiction of a factorization $G = 2A_1 + A_2 + \cdots + A_k$ in which $\chi(A)$ is not zero for any factor A. Thus, in this case, Case 1 or Case 2 must hold always and from the above we have that A_1 is periodic. For $u > 1$, this new factorization has only $u - 1$ factors, A say, with $\chi(A) = 0$. The required result follows by induction on u. This completes the proof.

8.10 Theorem [18]

Let p be a prime and let G be a group such that the p-component G_p is cyclic. If $G = A_1+A_2+\ldots+A_r + B$ is a factorization of G such that each factor A_i has order equal to a power of p then one of the factors is periodic.

Proof. For each i let B_i be the G_p-component of A_i. By the lemma, A_i may be replaced by B_i and the elements of B_i are distinct. Let H be the subgroup of G which is the complement of G_p. Since the subsets B_i are contained in G_p it follows that, for each $h \in H$,

$$G_p + h = B_1 + \cdots + B_r + (B \cap (G_p + h)).$$

This leads to the factorization

$$G_p = B_1 + \cdots + B_r + (B \cap (G_p + h)) - h).$$

Since G_p is a cyclic group of prime power order it follows that one of the factors must be periodic. Suppose first that no factor B_i is periodic. Let G_p have order p^e and generator a. Then $p^{e-1}a$ is a period of $(B \cap (G_p + h)) - h)$. and so of $B \cap (G_p + h)$ for each $h \in H$. Since, as h varies over H, B is the union of these sets it follows that $p^{e-1}a$ is a period of B.

We may now suppose that one of the other subsets, say B_1, is periodic. Then $p^{e-1}a$ is a period. We should note that this implies that the subsets $B_2,\ldots,B_r$ are not periodic since the sum with B_1 being direct implies that $p^{e-1}a$ cannot also be a period of one of these sets. It follows that if χ is a character such that $\chi(a)$ has order p^e then $\chi(B_i) \neq 0$ for $2 \leq i \leq r$.

Now let us consider the factorization $G = A_1 + B_2+\ldots+B_r + B$. For any character χ such that $\chi(a)$ has order p^e, we have that either $\chi(A_1) = 0$ or that $\chi(B) = 0$. Let $\chi_j, j \in J$, be the set of all such characters such that $\chi_j(A_1) = 0$. Let the kernel of χ_j be k_j, i.e. $k_j = \{g \in G: \chi_j(g) = 1\}$. Let the intersection of all these subgroups k_j be K. Let $F = \langle p^{e-1}a \rangle$. We note that the statement that $\chi(a)$ has order p^e is equivalent to $\chi(p^{e-1}a) \neq 1$ and so to the statement that $\chi(F) = 0$.

Let us suppose that $K = 0$. Let $\chi_j(A_1) = 0$. If $h \in H$ and $ra + h \in A_1$ then $ra \in B_1$ and so only one such r can exist. $\chi_j(A_1) = 0$ implies that $\sum \alpha^r \chi_j(h) = 0$, where the summation is taken over all $ra + h \in A_1$. Then $Fp^e(x)$ divides $\sum x^r \chi_j(h)$. Since $p^{e-1}a$ is a period of B_1, it follows that if $sa + h_1$ is in A_1 with $h_1 \in H$ then there exists $h_2 \in H$ such that $(s + p^{e-1})a + h_2 \in A_1$.

From above it follows that $\chi_j(h_1) = \chi_j(h_2)$ and so that $h_1 - h_2 \in K_j$. This is true for all such . Hence $h_1 - h_2$ is in K. It follows that $h_1 = h_2$ and so that $p^{e-1}a$ is a period of A_1.

Finally we have the case in which $K \neq 0$. Let χ be a character such that

$\chi(F) = \chi(K) = 0$. $\chi(K) = 0$implies that $\chi(A_1) \neq 0$. Thus $\chi(B) = 0$. It follows that there exist subsets U, V of G such that B is the disjoint union of the direct sums $F + U$and $+ V$.

Now the sum $B_1 + B$ is direct and $p^{e-1}a$ is a period of B_1. It follows that U is the empty set and so that $B = K + V$. Thus every non-zero element of K is a period of B. This completes the proof.

Conclusion

This research project has mainly focused the structure of the finite abelian groups, basis theorem, Sylow's theorem and factoring finite abelian groups. Further, it compares with groups in general the structure of finite abelian groups is much easier to investigate since commutatively implies many structural properties that almost never hold in non-abelian groups.

References

[1] Pinter, C. (2010). *A book of abstract algebra*. Mineola, N.Y: Dover Publications.

[2] Lial, M., Hornsby, J., Schneider, D. & Daniels, C. (2015). *Essentials of college algebra*. Boston: Pearson.

[3] Cameron, J. (2013). *Notes on finite group theory*, www.maths.qmul.ac.uk/pjs/notes/gt.pdf last access: 8th of October 2017.

[4] Kamke E. (2010), *Theory of sets*, Dover Publication Inc.

[5] Hodge, J., Schlicker, S. & Sundstrom, T. (2014). *Abstract algebra: an inquiry-based approach*. Boca Raton: CRC Press, Taylor & Francis Group.

[6] Bret, B. (2014). *Fundamental theorem of abelian groups/ chapter 24: Sylow theorems*, http://www.users.csbsju.edu/~bbenesh/docs/331/Ch24SylowTheory-FToAGABBREVIATEDHandout.pdf. Last access: 8th of October 2017.

[7] Breuer, J. (2006). *Introduction to the theory of sets*. Mineola, NY: Dover Publications.

[8] Jonathan, K. (2013), Schlicker Steven, Sundstrom Ted, *Abstract algebra An inquiry-based approach*, a chapman and hall book.

[9] Adhikari, M. & Adhikari, A. (2014). *Basic modern algebra with applications*. New Delhi: Springer.

[10] Joseph, B (2006) *Introduction to the theory of sets*, Dover Publications Inc.

[11] Kreher L. (2012), *Group theory notes*, www.math.mtu.edu/~kreher/ABOUTME/syllabus/GTN.pdf. Last access: 8th of October 2010.

[12] Ash, R. (2007). Basic abstract algebra: for graduate students and advanced undergraduates. Mineola, N.Y: Dover Publications.

[13] Kurzweil, H. & Stellmacher, B. (2004). *The theory of finite groups: an introduction*. New York: Springer.

[14] Duckett, G. (2016). *Elementary set theory: questions and answers*. Place of publication not identified: publisher not identified.

[15] Malle Gunter, Moret´o Alexander, *Element orders and Sylow structure of finite groups*, www.mathematik.uni-kl.de/~malle/download/elemords.pdf

[16] Miller, F. (2004), *Combinatorial Group Theory*, www.ms.unimelb.edu.au/~cfm/notes/cgt-notes.pdf. Last access: 8th of October 2017.

[17] Milne J.S. , *Group theory*, 1996, www.jmilne.org/math/CourseNotes/GT310.pdf,

[18] Prakash Nirmala, *Mathematical perspectives on theoretical physics*, Imperial College Press,2003

[19] Reis Clive, *Abstract algebra an introduction to groups, rings and fields*, World Scientific Publishing Co. Pte. Ltd., 2011

[20] Rotman, J. (2003). *Advanced modern algebra*, American Mathematical Society.

[21] Sands, D. (2004), *Factoring finite abelian groups*, Journal of Algebra 275 (2004) 540–549.

[22] Spindler Karlheinz, *Abstract algebra with application in two volumes*: volume 1, Marcel Dekker Inc., 1994

[23] Brooklynn, S. (2016). *On the existence of normal subgroups of prime index*, Rose Hulman Undergraduate Mathematics Journal.

[24] Sundstrom, T. (2017). Mathematical reasoning: writing and proof. Mountain View, CA: Creative Commons.

[25] Amin, W. (2012). *Finite abelian groups*, https://www.philadelphia.edu.jo/math/witno/notes/won7.pdf. Last access: 8th of October 2017.

[26] Monica, A (2015). *Fundamental theorem of finite abelian groups*, Boise State University.

[27] Robert B. (2017), *Abstract algebra*: The basic graduate year, http://onlinebooks.library.upenn.edu

---

ملخص الدراسة :

في الجبر التجريديّ، تتكون الهيكلية الجبرية من واحدة أو أكثر من الزمر المنتهية (عمليات الزمرة المنتهية) التي يتم التعرف عليها من خلال التحقق من شروط وبديهيات الزمر الأبيلية .تشمل الهياكل الجبرية زمرة (مجموعات وظيفية)، ودوائرَ، ومجالاتٍ، وشبكاتٍ مدمجة، إلخ ...). الزمرة (. ،**G**) هي بنية جبرية تتوافق مع عناصر الارتباط والعناصر الحيادية، وكذلك عناصر النظير والمتمم.

الزمرة الأبيلية هي مجموعة يطلق عليها أيضا زمرة تبادلية، هي زمرة تحدث نتيجة تطبيق عملية الزمرة على مجموعة من عنصرين واللذين لا يعتمدانِ على الترتيب الذي جاءا به هذين العنصرين أثناء تطبيق العملية. هذه هي الزمر أو المجموعات الوظيفية التي تتوافق مع الشروط والبديهيات التبادلية. مفهوم الزمرة الأبيلية هو من أوائل

المفاهيم التي تم مصادفتها في الجبر التجريديّ، والتي من خلالها تم تطوير العديد من المفاهيم الرياضية كمفاهيم الحلقات الرياضية، والحلقات التبادلية، وأيضاً مفهوم الفضاء الحلقي والفضاء المتجهي.

تركز هذه الدراسة على الهيكلية الجبرية للزمر الأبيلية وكذلك النظريات الأساسية إلى جانب نظرية سيلو. إضافة إلى ذلك، تتناول هذه الدراسة الخصائص المتعلقة بهذه النظريات الجبرية حيث اتبع الباحث منهج المقارنة والاستكشاف لتحقيق هدف الدراسة. وأظهرت الدراسة بأن نظرية الزمر الأبيلية بشكل عام، أبسط من نظائرها الغير أبيلية، وتعد الزمر الأبيلية المنتهية سهلة الاستيعاب.

الكلمات المفتاحية: الجبر، الزمر، الأبيلية، المنتهية