Adamawa State University Journal of Scientific Research
Volume 7 Number 1, April, 2019; Article no. ADSUJSR 0701024
ISSN:2705-1900(Online); ISSN: 2251-0702 (Print)
http://www.adsujsr.com

A Derived Method for Construction and Classification of Morphisms and Representations between Finite Groups

D. Samaila[1], S. G. Ngulde[2] and B. A. Madu[2]
[1]Department of Mathematics, Adamawa State University, Mubi, Nigeria.
[2]Department of Mathematical Sciences, University of Maiduguri, Nigeria.

Abstract

This paper aimed at constructing new group presentations from known presentations using direct product of two or more groups. We established the fact that for any prime number $p > 2$ and any positive integer n, $|U(p^n)| = |U(2p^n)|$ and then used symmetries to construct groups and their respective subgroups, characteristics and the unique factorization of the elements. Functions f_i on finite group G such that each f_i is a morphism are constructed and the fact that if G is any finite Abelian group, H a subgroup of G, then the factor group G/H is a finite Abelian group is proved. We finally established that if $|G| = n$ such that $n = r \cdot s \cdot t$, then $G \cong Z_r \otimes Z_s \otimes Z_t$ where $r,s,t \in Z^+$ and then identify some homomorphism and automorphism on finite groups by listing all the possible maps from the group to itself with the help of GAP.

Keywords: Finite group; Cartesian product; Homomorphism; Isomorphism; Automorphism; Factor group

Introduction

In mathematics, one can often define a direct product of objects already known, giving a new one. This generalizes the Cartesian product of the underlying sets, together with a suitably defined structure on the product set. More abstractly, one talks about the product in category theory, which formalizes these notions. Examples are the product of sets, groups, the product of rings and of other algebraic structures. We limit ourselves to product in groups.

In group theory, *direct product* is an operation that takes two groups K and H and constructs a new group, usually denoted $K \otimes H$. This operation is the group-theoretic analogue of the Cartesian product of sets and is one of several important notions of direct product in mathematics.

In the context of Abelian groups, the direct product is sometimes referred to as the direct sum, and is denoted $K \oplus H$ (Herstein, 1996). Direct sums play an important role in the classification of Abelian groups: according to the fundamental theorem of finite Abelian groups, every finite Abelian group can be expressed as the direct sum of cyclic groups.

An Abelian group $(G, +)$ is called finitely generated if there exist finitely many elements $x_1, x_2 \ldots, x_r$ in G such that every x in G can be written in the form $x = n_1x_1 + n_2x_2 + \ldots + n_rx_r$ with integers $n_1, n_2, \ldots, n_r$. In this case, we say that the set $\{x_1, \ldots, x_r\}$ is a generating set of G or that $x_1, \ldots, x_r$ generate G (Dummit, 2004). Clearly, every finite Abelian group is finitely generated. The finitely generated Abelian groups are of a rather simple structure and can be completely classified. Examples of some groups that are finitely generated are the group of integers $(Z, +)$, the group of integers modulo n $(Z_n, +)$, e.t.c. Again, any direct sum of finitely many finitely generated Abelian groups is again a finitely generated Abelian group and every lattice forms a finitely generated free Abelian group. Some groups that are not finitely generated are $(Q, +)$ of rational numbers and $(Q^*, \cdot)$ of non-zero rational numbers. The groups of real numbers under addition $(\Re, +)$ and real numbers under multiplication $(\Re, \times)$ are also not finitely generated (Lang, 2002).

The fundamental theorem of finitely generated Abelian groups is viewed in two different ways; The first aspect is the Primary decomposition formulation which states that every finitely generated Abelian

group G is isomorphic to a direct sum of primary cyclic groups and infinite cyclic group. A primary cyclic group is one whose order is a power of a prime. That is, every finitely generated Abelian group is isomorphic to a group of the form $Z^n \otimes Z_{q_1} \otimes ... \otimes Z_{q_t}$ where the rank $n \geq 0$, and the numbers q_1, ..., q_t are powers of (not necessarily distinct) prime numbers. In particular, G is finite if and only if $n = 0$. The values of n, q_1, ..., q_t are (up to rearranging the indices) uniquely determined by G. The second aspect is the Invariant factor decomposition. We can also write any finitely generated Abelian group G as a direct sum of the form $Z^n \otimes Z_{k_1} \otimes ... \otimes Z_{k_u}$ where k_1 divides k_2, which divides k_3 and so on up to k_u. Again, the rank n and the invariant factors k_1, ..., k_u are uniquely determined by G (here with a unique order).

Preliminaries

Group Homomorphism

Given two groups $(G, *)$ and $(H, \cdot)$, a group homomorphism from $(G, *)$ to $(H, \cdot)$ is a function $\phi : G \to H$ such that for all x and y in G we have $\phi(x * y) = \phi(x) \cdot \phi(y)$ where the group operation on the left hand side of the equation is that of G and on the right hand side that of H. From this property, one can deduce that ϕ maps the identity element e_G of G to the identity element e_H of H, and it also maps inverses to inverses in the sense that $\phi(x^{-1}) = \phi(x)^{-1}$. Hence one can say that ϕ "is compatible with the group structure". Older notations for the homomorphism $\phi(x)$ may be x_ϕ, though this may be confused as an index or a general subscript. A more recent trend is to write group homomorphism on the right of their arguments, omitting brackets, so that $\phi(x)$ becomes simply $x\phi$. In areas of mathematics where one considers groups endowed with additional structure, a *homomorphism* sometimes means a map which respects not only the group structure (as above) but also the extra structure. For example, a homomorphism of topological groups is often required to be continuous.

Image and Kernel of Homomorphism

The kernel of a homomorphism ϕ is the set of elements in G which are mapped to the identity in H, i.e.

$$\mathrm{Ker}(\phi) = \{u \in G \mid \phi(u) = e_H\},$$

and the image of ϕ is defined as

$$\mathrm{Im}(\phi) = \phi(G) = \{\phi(u) : u \in G\}.$$

The kernel and image of a homomorphism can be interpreted as measuring how close it is to being an isomorphism. The First Isomorphism Theorem states that the image of a group homomorphism, $\phi(G)$ is isomorphic to the quotient group $G/\ker \phi$. The kernel of ϕ is a normal subgroup of G and the image of ϕ is a subgroup of H, for given $g \in G$ and $h \in \mathrm{Ker}(\phi)$, we have

$$\phi(g^{-1}hg) = \phi(g^{-1})\phi(h)\phi(g) = \phi(g)^{-1}\phi(h)\phi(g) = \phi(g)^{-1}e_H\phi(g) = \phi(g)^{-1}\phi(g) = e_H.$$

If and only if $\ker(\phi) = \{e_G\}$, the homomorphism, ϕ, is a group Monomorphism, i.e., ϕ is injective. Injection directly gives that there is a unique element in the kernel, and a unique element in the kernel gives injection such that for all $x,y \in G$,

$$\phi(x) = \phi(y) \text{ iff } \phi(x) \cdot \phi(y)^{-1} = e_H \text{ iff } \phi(x \cdot y^{-1}) = e_H, \mathrm{Ker}(\phi) = \{e_G\}, \text{ iff } x \cdot y^{-1} = e_G \text{ iff } x = y.$$

Some of the common examples are as follows: Consider the cyclic group $Z/3Z = \{0, 1, 2\}$ and the group of integers Z with addition. The map $\phi: Z \to Z/3Z$ with $\phi(x) = x \ mod \ 3$ is a group homomorphism. It is surjective and its kernel consists of all integers which are divisible by 3. Also the multiplicative group of positive real numbers $(\Re^+, \cdot)$, for any complex number c, the function $f_c : \mathrm{R}^+ \to \mathrm{C}$ defined by: $\phi_c(x) = x^c$ is a group homomorphism. The exponential map also yields a group homomorphism from the group of real numbers $\Re$ with addition to the group of non-zero real numbers $\Re^*$ with multiplication. The kernel is $\{0\}$ and the image consists of the positive real numbers.

We also note that if $\phi: G \to H$ and $\varphi: H \to K$ are group homomorphisms, then so is their composition $\varphi \circ \phi: G \to K$.

This shows that the class of all groups, together with group homomorphisms as morphisms, forms a category. In case of Abelian groups, if G and H are Abelian groups, then the set $Hom(G, H)$ of all group homomorphisms from G to H is itself an Abelian group, where the sum $\phi + \varphi$ of two homomorphisms is defined by

$\phi + \varphi)(x) = \phi(x) + \varphi(x)$ for all $x \in G$.

The commutativity of H is needed to prove that $\phi + \varphi$ is again a group homomorphism.

The addition of homomorphisms is compatible with the composition of homomorphisms in the following sense: if ϕ is in Hom(K, G), φ, ψ are elements of Hom(G, H), and η is in Hom(H, L), then

$(\phi + \varphi) \circ \psi = (\phi \circ \psi) + (\varphi \circ \psi)$ and $\eta \circ (\phi + \varphi) = (\eta \circ \phi) + (\eta \circ \varphi)$.

Since the composition is associative, this shows that the set End(G) of all endomorphisms of an Abelian group forms a ring, the endomorphism ring of G. For example, the endomorphism ring of the Abelian group consisting of the direct sum of m copies of Z/nZ is isomorphic to the ring of m-by-m matrices with entries in Z/nZ. The above compatibility also shows that the category of all Abelian groups with group homomorphisms forms a pre-additive category; the existence of direct sums and well-behaved kernels makes this category the prototypical example of an Abelian category (Dummit, 2004).

Group Isomorphism

In group theory, a group isomorphism is a function between two groups that sets up a one-to-one onto correspondence between the elements of the groups in a way that respects the given group operations. If there exists an isomorphism between two groups, then the groups are said to be isomorphic. From the standpoint of group theory, isomorphic groups have the same properties and need not be distinguished. We therefore formulate the definition as follows: Given two groups $(G, *)$ and $(H, \bullet)$, a group isomorphism from $(G, *)$ to $(H, \bullet)$ is a bijective group homomorphism from G to H. That is, a group isomorphism is a bijective function $\xi: G \to H$ such that for all x and y in G, we have $\xi(x * y) = \xi(x) \bullet \xi(y)$.

The two groups $(G, *)$ and $(H, \bullet)$ are isomorphic if there exists an isomorphism between them. This is written mathematically as $(G, *) \cong (H, \bullet)$ (Jacobson, 2009).

Intuitively, group theorists view two isomorphic groups as follows: For every element g of a group G, there exists an element h of H such that h behaves in the same way as g (operates with other elements of the group in the same way as g). For instance, if g generates G, then h also generates H. This implies in particular that G and H are in bijective correspondence. Thus, the definition of an isomorphism is quite natural.

An isomorphism of groups may equivalently be defined as an invertible morphism in the category of groups, where invertible here means has a two-sided inverse. Examples of isomorphism are as follows: The group of all real numbers with respect to addition, $(\Re, +)$ is isomorphic to the group of positive real numbers with respect to multiplication $(\Re^+, \times)$, the Klein four-group is isomorphic to the direct product of two copies of $Z_2 = Z/2Z$ and can therefore be written as $Z_2 \times Z_2$, e.t.c.

Few among the properties of isomorphism are: The Kernel of an isomorphism from $(G, *)$ to $(H, \bullet)$, is always $\{e_G\}$ where e_G is the identity of the group $(G, *)$; If $(G, *)$ is isomorphic to $(H, \bullet)$, and if G is Abelian then so is H; If $(G, *)$ is a group that is isomorphic to $(H, \bullet)$ with φ as the isomorphism, and if x belongs to G and has order n, then so does $\varphi(x)$ and if $(G, *)$ is a locally finite group that is isomorphic to $(H, \bullet)$, then $(H, \bullet)$ is also locally finite.

Cyclic Groups

It is observed that all cyclic groups of a given order are isomorphic to $(Z_n, +_n)$. Given a cyclic group G and n be the order of G, then G is the group generated by $< x > = \{e, x, x^2, \ldots, x^{n-1}\}$. It is easy to see that $G \cong (Z_n, +_n)$. Now define a function $\varphi: G \to Z_n$ by $\varphi(x^n) = n$ where $Z_n = \{0, 1, 2, \ldots, n-1\}$. Then clearly, φ is bijective. Then

$\varphi(x^m \cdot x^n) = \varphi(x^{m+n}) = m + n = \varphi(x^m) +_n \varphi(x^n)$, which shows that $G \cong (Z_n, +_n)$.

From the definition, it follows that any isomorphism $\varphi: G \to H$ will map the identity element of G to the identity element of H, i.e. $\varphi(e_G) = e_H$ and inverses to inverses $\varphi(x^{-1}) = [\varphi(x)]^{-1}$ and more generally, nth powers to nth powers, $\varphi(x^n) = [\varphi(x)]^n$ for all x in G, where the inverse function φ^{-1}: $H \to G$ is again an isomorphism. The relation "isomorphic" is an equivalence relation. If φ is an isomorphism between two groups G and H, then everything that is true about G that is only related to the group structure can be translated via φ into a true ditto statement about H, and vice versa (Rose, 2012).

Automorphism

An isomorphism from a group $(G, *)$ to itself is called an automorphism of this group. Thus, it is a bijection $\varphi: G \to G$ such that $\varphi(x * y) = \varphi(x) * \varphi(y)$ for all $x, y \in G$. An automorphism always maps the identity to itself. The image under an automorphism of a conjugacy class is always a conjugacy class (the same or another). The image of an element has the same order as that element. The composition of two automorphism is again an automorphism, and with this operation the set of all automorphism of a group G, denoted by Aut(G), forms itself a group, the *automorphism group* of G. For all Abelian groups there is at least the automorphism that replaces the group elements by their inverses. However, in groups where all elements are equal to their inverse, this is the trivial automorphism; example is the Klein four-group. For that group all permutations of the three non-identity elements are automorphism, so the automorphism group is isomorphic to S_3 and D_3.

In Z_p for a prime number p, one non-identity element can be replaced by any other, with corresponding changes in the other elements. The automorphism group is isomorphic to Z_{p-1}. For example, for $n = 7$, multiplying all elements of Z_7 by 3, modulo 7, is an automorphism of order 6 in the automorphism group, because $3^6 \equiv 1$ (modulo 7), while lower powers do not give 1. Thus this automorphism generates Z_6. There is one more automorphism with this property: multiplying all elements of Z_7 by 5, modulo 7. Therefore, these two correspond to the elements 1 and 5 of Z_6, in that order or conversely. The automorphism group of Z_6 is isomorphic to Z_2, because only each of the two elements 1 and 5 generate Z_6, so apart from the identity we can only interchange these (Rose, 2012).

The automorphism group of $Z_2 \times Z_2 \times Z_2 = D_2 \times Z_2$ has order 168, as can be found as follows. All 7 non-identity elements play the same role, so we can choose which plays the role of (1,0,0). Any of the remaining 6 can be chosen to play the role of (0,1,0). This determines which corresponds to (1,1,0). For (0,0,1) we can choose from 4, which determines the rest. Thus we have $7 \times 6 \times 4 = 168$ automorphism. They correspond to those of the Fano plane, of which the 7 points correspond to the 7 non-identity elements. The lines connecting three points correspond to the group operation: a, b, and c on one line means $a + b = c$, $a + c = b$, and $b + c = a$. For Abelian groups all automorphism except the trivial one are called outer automorphism. Non-Abelian groups have a non-trivial inner automorphism group, and possibly also outer automorphism.

One can also apply the fundamental theorem to count (and sometimes determine) the automorphism of a given finite Abelian group G. To do this, one uses the fact that if G splits as a direct sum $H \oplus K$ of subgroups of coprime order, then $\mathrm{Aut}(H \oplus K) \cong \mathrm{Aut}(H) \oplus \mathrm{Aut}(K)$. Given this, the fundamental theorem shows that to compute the automorphism group of G it suffices to compute the automorphism groups of the Sylow p-subgroups separately (that is, all direct sums of cyclic subgroups, each with order a power of p). Fix a prime p and suppose the exponents e_i of the cyclic factors of the Sylow p-subgroup are arranged in increasing order as $e_1 \le e_2 \le \ldots \le e_n$ for some integer $n > 0$. One needs to find the automorphism of $Z_p e_1 \oplus Z_p e_2 \oplus \ldots \oplus Z_p e_n$. One special case is when $n = 1$, so that there is only one cyclic prime-power factor in the Sylow p-subgroup P. In this case the theory of automorphism of a finite cyclic group can be used. Another special case is when n is arbitrary but $e_i = 1$ for $1 \le i \le n$. Here, one is considering P to be of the form $Z_p \oplus Z_p \oplus \ldots \oplus Z_p$ (n-times), so elements of this subgroup can be viewed as comprising a vector space of dimension n over the finite field of p elements F_p. The automorphism of

this subgroup are therefore given by the invertible linear transformations, so Aut(P) ≅ GL(n, F_p), where GL is the appropriate general linear group. This is easily shown to have order |Aut(P)| = (p^n – 1)…(p^n – p^{n-1}) (Hillar, 2007).

Cartesian product

The Cartesian product of sets S_1, S_2, …, S_n is the set of all ordered n-tuples (x_1, x_2, …, x_n), where $x_i \in S_i$ (Lang, 2005). The Cartesian product is usually denoted by either

$$S_1 \otimes S_2 \otimes ... \otimes S_n \text{ or by } \prod_{i=1}^{n} S_i .$$

Now, let the binary operations on the groups G_1, G_2, …, G_n be multiplication. Regarding the G_i as sets, we can form the Cartesian product $\prod_{i=1}^{n} G_i$ of the groups G_1, G_2, …, G_n. It is also easy to make $\prod_{i=1}^{n} G_i$ into a group by means of a binary operation of multiplication by components. Consider the following theorems:

Theorem 3.1: Let G_1, G_2, …, G_n be groups. For (x_1, x_2, …, x_n) and (y_1, y_2, …, y_n) in $\prod_{i=1}^{n} G_i$, define (x_1, x_2, …, x_n)(y_1, y_2, …, y_n) = (x_1 y_1, x_2 y_2, …, x_n y_n). Then $\prod_{i=1}^{n} G_i$ is a group called the External Direct Product of the groups G_1, G_2, …, G_n under this binary operation (John, 1976).

Proof: Now, since each G_i is a group for i = 1, 2, …, n and $x_i, y_i \in G_i$ for all i, then $x_i y_i \in G_i$. Thus the definition of the binary operation on $\prod_{i=1}^{n} G_i$ given in the statement of the theorem is well defined, i.e. the binary operation is closed on $\prod_{i=1}^{n} G_i$.

The associativity law in $\prod_{i=1}^{n} G_i$ is thrown back onto the associativity law in each component as follows:

(x_1, x_2, …, x_n)[(y_1, y_2, …, y_n)(z_1, z_2, …, z_n)] = (x_1, x_2, …, x_n)(y_1z_1, y_2z_2, …, y_nz_n)
= ($x_1(y_1z_1)$, $x_2(y_2z_2)$, …, $x_n(y_nz_n)$)
= ((x_1y_1)z_1, (x_2y_2)z_2, …, (x_ny_n)z_n)
= ((x_1y_1), (x_2y_2), …, (x_ny_n))(z_1, z_2, …, z_n)
= [(x_1, x_2, …, x_n)(y_1, y_2, …, y_n)](z_1, z_2, …, z_n).

If e_i is the identity element in G_i for all i, then clearly, with multiplication by components, (e_1, e_2, …, e_n) is the identity in $\prod_{i=1}^{n} G_i$. The inverse of (x_1, x_2, …, x_n) is $(x_1^{-1}, x_2^{-1}, ..., x_n^{-1})$, for

(x_1, x_2, …, x_n) $(x_1^{-1}, x_2^{-1}, ..., x_n^{-1}) = (x_1x_1^{-1}, x_2x_2^{-1}, ..., x_nx_n^{-1})$ = (e_1, e_2, …, e_n). Hence $\prod_{i=1}^{n} G_i$ is a group as required.

We also note that if the group G_i has r_i elements for i = 1, 2, …, n, then $\prod_{i=1}^{n} G_i$ has $r_1r_2…r_n$ elements, for in an n-tuple, there are r_1 choices for the first component from G_1, and for each of these there are r_2 choices for the next component from G_2, e.t.c.

Remark 3.2: We noticed that for the groups G_1, G_2, …, G_n with orders r_1, r_2, …, r_n respectively, we have $|G_1 \otimes G_2 \otimes \dots \otimes G_n| = |G_1|\ |G_2|\ \dots\ |G_n| = r_1r_2…r_n$ where the product $G_1 \otimes G_2 \otimes \dots \otimes G_n$ is a new group which may or may not be isomorphic to the group $G_{r1r2…rn}$. This will be our specific objective for this article.

We shall now make a conjecture on the direct product of two finite cyclic groups of relatively prime orders.

Consider the groups Z/pZ and Z/qZ. Let p and q be relatively prime positive integers. For any integer a, denote the residue class of a (mod p) by $\bar{a}$, and the residue class of a (mod q) by a^*. Obviously, $\bar{a} \in Zp$ and $a^* \in Zq$. Consider the function $\phi: Z \to Zp \otimes Zq$. Then ϕ is a homomorphism for

$$(a+b) = (\overline{a+b}, (a+b)^*) = (\bar{a}+\bar{b}, a^*+b^*) = (\bar{a}, a^*) + (\bar{b}, b^*) = a\phi + b\phi$$

for all $a,b \in Z$. Again, $Z/\text{Ker}\ \phi \cong \text{Im}\phi$. Now $a \in \text{Ker}\phi$ if and only if $\bar{a} = \bar{0}$ and $a^* = 0^*$, that is, if and only if $p|a$ and $q|a$. Since p and q are relatively prime, the latter condition is equivalent to $pq|a$. Hence the kernel $\text{Ker}\phi = pqZ$ and $Z/pqZ \cong \text{Im}\phi$, where the image $\text{Im}\phi$ is a subgroup of $Z/pZ \otimes Z/qZ$. Finally, from

$$pq = |Z/pqZ| = |\text{Im}\phi| \leq |Z/pZ \otimes Z/qZ| = |Z/pZ|\ |Z/qZ| = pq$$

We conclude that $|\text{Im}\phi| = pq$ and hence, $\text{Im}\phi = Z/pZ \otimes Z/qZ$ which shows that ϕ is onto and $Z/pqZ \cong Z/pZ \otimes Z/qZ$.

Hence, we have:

Theorem 3.3: The group $Z_m \otimes Z_n$ is isomorphic to Z_{mn} if and only if $(m, n) = 1$ (John, 1976).

Example 3.4: Consider the group $[-1, +1] \otimes Q^+$ where Q^+ is the set of all positive rational numbers. The elements of the group $[-1, +1] \otimes Q^+$ is the set of all ordered pairs (x, q) such that $x \in [-1, +1]$ and $q \in Q^+$. Define a mapping $\sigma: Q\backslash\{0\} \to [-1, +1] \otimes Q^+$ by $\sigma(q) = (\text{sgn}\ q, |q|)$ where $\text{sgn}|q| = \pm 1$. Then σ is a homomorphism for

$$(q_1q_2)\sigma = (\text{sgn}q_1q_2,\ |q_1q_2|) = (\text{sgn}q_1\text{sgn}q_2,\ |q_1||q_2|) = (\text{sgn}q_1, |q_2|)(\text{sgn}q_2,\ |q_2|) = (q_1\sigma)(q_2\sigma)$$

for all $q_1, q_2 \in Q\backslash\{0\}$. The kernel of σ is

$$\text{Ker}\ \sigma = \{q \in Q\backslash\{0\} : q\sigma = (1, 1)\} = \{q \in Q\backslash\{0\} : \text{sgn}\ q = 1, |q| = 1\}$$
$$= \{q \in Q\backslash\{0\} : q > 0, |q| = 1\} = \{1\},$$

that is, σ is one-to-one. But any $(x, q) \in [-1, +1] \otimes Q^+$ is the image of $x|q| \in Q\backslash\{0\}$, i.e. σ is an onto homomorphism and hence, σ is an isomorphism so that $Q\backslash\{0\} \cong [-1, +1] \otimes Q^+$.

The theorem 2 above can be extended to a product of more than two groups by induction argument. It is also true that two groups are isomorphic if and only if they have the same order.

Lemma 3.5: Let $G_1, G_2, \ldots, G_n, H_1, H_2, \ldots, H_n$ be groups and assume that
$G_1 \cong H_1, G_2 \cong H_2, \ldots, G_n \cong H_n$, then $G_1 \otimes G_2 \otimes \ldots \otimes G_n \cong H_1 \otimes H_2 \otimes \ldots \otimes H_n$ (Lang, 2002).

Proof (Review): Let $\xi_i: G_i \to H_i$ be an isomorphism for $i = 1, 2, \ldots, n$. Then the mapping
$\xi: G_1 \otimes G_2 \otimes \ldots \otimes G_n \to H_1 \otimes H_2 \otimes \ldots \otimes H_n$ where $(g_1, g_2, \ldots, g_n) = (g_1\xi_1, g_2\xi_2, \ldots, g_n\xi_n)$
Is a homomorphism since

$$\begin{aligned}((g_1, g_2, ..., g_n)(g_1', g_2', ..., g_n'))\xi &= (g_1g_1', g_2g_2', ..., g_ng_n')\xi \\ &= ((g_1g_1')\xi_1, (g_2g_2')\xi_2, ..., (g_ng_n')\xi_n) \\ &= (g_1\xi_1g_1'\xi_1, g_2\xi_2g_2'\xi_2, ..., g_n\xi_ng_n'\xi_n) \\ &= (g_1\xi_1, g_2\xi_2, ..., g_n\xi_n)(g_1'\xi_1, g_2'\xi_2, ..., g_n'\xi_n) \\ &= (g_1, g_2, ..., g_n)\xi(g_1', g_2', ..., g_n')\xi\end{aligned}$$

for all $(g_1, g_2, ..., g_n), (g_1', g_2', ..., g_n') \in G_1 \otimes G_2 \otimes ... \otimes G_n$. Also since

$$\begin{aligned}Ker\,\xi &= \{(g_1, g_2, ..., g_n) \in G_1 \otimes G_2 \otimes ... \otimes G_n : (g_1\xi_1, g_2\xi_2, ..., g_n\xi_n) = (1,1,...,1)\} \\ &= \{(g_1, g_2, ..., g_n) \in G_1 \otimes G_2 \otimes ... \otimes G_n : g_1\xi_1 = 1, g_2\xi_2 = 1, ..., g_n\xi_n = 1\} \\ &= \{(g_1, g_2, ..., g_n) \in G_1 \otimes G_2 \otimes ... \otimes G_n : g_1 = 1, g_2 = 1, ..., g_n = 1\} \\ &= \{(1,1,...,1)\} = 1,\ \xi \text{ is one-to-one.}\end{aligned}$$

Again, ξ is onto, for given $(h_1, h_2, \ldots, h_n) \in H_1 \otimes H_2 \otimes \ldots \otimes H_n$ we always have $g_i \in G_i$ with $g_i\xi_i = h_i$. Hence, $(h_1, h_2, \ldots, h_n)$ is the image of $(g_1, g_2, \ldots, g_n) \in G_1 \otimes G_2 \otimes \ldots \otimes G_n$ under ξ. Thus, ξ is an isomorphism and

$G_1 \otimes G_2 \otimes \ldots \otimes G_n \cong H_1 \otimes H_2 \otimes \ldots \otimes H_n$ as required.

The next theorem is telling us that given two groups H and K such that $|H| = p$ and $|K| = q$ where p and q are prime numbers with $p < q$ and $q \neq 1 \pmod{p}$. Then the group formed by the product of H and K, given by $G = H \otimes K$ of order pq is cyclic.

Theorem 3.6: Let p and q be prime numbers, where $p < q$ and $q \neq 1 \pmod{p}$. Then any group of order pq is cyclic (Robinson, 1996).

Morphisms between Representations

Given two representations $\rho: G \to GL(n, C)$ and $\tau: G \to GL(m, C)$, a morphism between ρ and τ is a linear map $T: C^n \to C^m$ so that for all g in G we have the following commuting relation: $T \circ \rho(g) = \tau(g) \circ T$. According to Schur's lemma, a non-zero morphism between two irreducible complex representations is invertible, and moreover, is given in matrix form as a scalar multiple of the identity matrix. This result holds as the complex numbers are algebraically closed.

Again, since a representation ρ defines an action on a vector space C^n, it may turn out that C^n has an invariant subspace $V \subset C^n$. The action of G is given by complex matrices and this in turn defines a new representation $\sigma: G \to GL(V)$. We call σ a sub-representation of ρ. A representation without sub-representations is called irreducible.

To construct new representations from old, there are number of ways in which one can combine representations to obtain new ones. Each of these methods involves the application of a construction from linear algebra to representation theory.

Given two representations ρ_1, ρ_2 we may construct their direct sum $\rho_1 \oplus \rho_2$ by $(\rho_1 \oplus \rho_2)(g)(v, w) = (\rho_1(g)v, \rho_2(g)w)$;
The tensor representation of ρ_1, ρ_2 is defined by $(\rho_1 \otimes \rho_2)(v \otimes w) = \rho_1(v) \otimes \rho_2(w)$;
Let $\rho: G \to GL(n,C)$ be a representation. Then ρ induces a representation ρ^* on the dual vector space $\mathrm{Hom}(C^n, C)$; Let $\phi: C^n \to C$ be a linear functional. The representation ρ^* is then defined by the rule $\rho^*(g)(\phi) = \phi \circ \rho(g)^{-1}$. The representation ρ^* is called either the dual representation or the contra-gradient representation of ρ. Furthermore, if a representation ρ has a sub-representation σ then the quotient of the representing vector spaces for ρ and σ has a well defined action of G on it. We call the resulting representation the quotient representation of ρ by σ. We shall now see how to apply Schur's lemma between morphisms of representations.

Lemma 4.1 (Schur's lemma): If $\xi: A \otimes B \to C$ is a morphism of representations, then the corresponding linear transformation obtained by dualizing B is: $\xi': A \to C \otimes B^*$ which is also a morphism of representations. Similarly, if $\tau: A \to B \otimes C$ is a morphism of representations, dualizing it will give another morphism of representations $\tau': A \otimes C^* \to B$ (La, 2000).

If ρ is an n-dimensional irreducible representation of G with the underlying vector space V, then we can define a $G \times G$ morphism of representations, for all g in G and x in V as

$\xi: C[G] \otimes (1_G \otimes V) \to (V \otimes 1_G)$ by $\xi: (g \otimes x) = \rho(g)[x]$

where 1_G is the trivial representation of G. This defines a $G \times G$ morphism of representations.

Results

Construction by Product

We start this section by constructing groups in favor of theorem 3.3, using positive integers m and n such that $(m, n) = 1$ (Samaila, 2016).

Let $U(n)$ be the set of all positive integers less than n and relatively prime to n. Then $U(n)$ is a group under multiplication modulo n. Now, we shall begin with the help of GAP, by making a conjecture about the size of the group $U(pq)$ in terms of the groups $U(p)$ and $U(q)$ where p and q are relatively prime numbers greater than 2.

Let $p = 11$ and $q = 13$, then we obtained $U(11)$, $U(13)$ and $U(143)$ using GAP as follows:

```
gap> ulist(11);
```

```
[ Z(11)^0, Z(11), Z(11)^8, Z(11)^2, Z(11)^4, Z(11)^9, Z(11)^7, Z(11)^3,
Z(11)^6, Z(11)^5 ]
gap> Size(ulist(11));10
gap> ulist(13);
[ Z(13)^0, Z(13), Z(13)^4, Z(13)^2, Z(13)^9, Z(13)^5, Z(13)^11,
Z(13)^3, Z(13)^8, Z(13)^10, Z(13)^7, Z(13)^6 ]
gap> Size(ulist(13));12
gap> Size(ulist(11))*Size(ulist(13));120
gap> ulist(143);
[ ZmodnZObj( 1, 143 ), ZmodnZObj( 2, 143 ), ZmodnZObj( 3, 143 ),
ZmodnZObj( 4, 143 ), ZmodnZObj( 5, 143 ),
ZmodnZObj( 6, 143 ), ZmodnZObj( 7, 143 ), ZmodnZObj( 8, 143 ),
ZmodnZObj( 9, 143 ), ZmodnZObj( 10, 143 ),
ZmodnZObj( 12, 143 ), ZmodnZObj( 14, 143 ), ZmodnZObj( 15, 143 ),
ZmodnZObj( 16, 143 ), ZmodnZObj( 17, 143 ),
ZmodnZObj( 18, 143 ), ZmodnZObj( 19, 143 ), ZmodnZObj( 20, 143 ),
ZmodnZObj( 21, 143 ), ZmodnZObj( 23, 143 ),
ZmodnZObj( 24, 143 ), ZmodnZObj( 25, 143 ), ZmodnZObj( 27, 143 ),
ZmodnZObj( 28, 143 ), ZmodnZObj( 29, 143 ),
ZmodnZObj( 30, 143 ), ZmodnZObj( 31, 143 ), ZmodnZObj( 32, 143 ),
ZmodnZObj( 34, 143 ), ZmodnZObj( 35, 143 ),
ZmodnZObj( 36, 143 ), ZmodnZObj( 37, 143 ), ZmodnZObj( 38, 143 ),
ZmodnZObj( 40, 143 ), ZmodnZObj( 41, 143 ),
ZmodnZObj( 42, 143 ), ZmodnZObj( 43, 143 ), ZmodnZObj( 45, 143 ),
ZmodnZObj( 46, 143 ), ZmodnZObj( 47, 143 ),
ZmodnZObj( 48, 143 ), ZmodnZObj( 49, 143 ), ZmodnZObj( 50, 143 ),
ZmodnZObj( 51, 143 ), ZmodnZObj( 53, 143 ),
ZmodnZObj( 54, 143 ), ZmodnZObj( 56, 143 ), ZmodnZObj( 57, 143 ),
ZmodnZObj( 58, 143 ), ZmodnZObj( 59, 143 ),
ZmodnZObj( 60, 143 ), ZmodnZObj( 61, 143 ), ZmodnZObj( 62, 143 ),
ZmodnZObj( 63, 143 ), ZmodnZObj( 64, 143 ),
ZmodnZObj( 67, 143 ), ZmodnZObj( 68, 143 ), ZmodnZObj( 69, 143 ),
ZmodnZObj( 70, 143 ), ZmodnZObj( 71, 143 ),
ZmodnZObj( 72, 143 ), ZmodnZObj( 73, 143 ), ZmodnZObj( 74, 143 ),
ZmodnZObj( 75, 143 ), ZmodnZObj( 76, 143 ),
ZmodnZObj( 79, 143 ), ZmodnZObj( 80, 143 ), ZmodnZObj( 81, 143 ),
ZmodnZObj( 82, 143 ), ZmodnZObj( 83, 143 ),
ZmodnZObj( 84, 143 ), ZmodnZObj( 85, 143 ), ZmodnZObj( 86, 143 ),
ZmodnZObj( 87, 143 ), ZmodnZObj( 89, 143 ),
ZmodnZObj( 90, 143 ), ZmodnZObj( 92, 143 ), ZmodnZObj( 93, 143 ),
ZmodnZObj( 94, 143 ), ZmodnZObj( 95, 143 ),
ZmodnZObj( 96, 143 ), ZmodnZObj( 97, 143 ), ZmodnZObj( 98, 143 ),
ZmodnZObj( 100, 143 ), ZmodnZObj( 101, 143 ),
ZmodnZObj( 102, 143 ), ZmodnZObj( 103, 143 ), ZmodnZObj( 105, 143 ),
ZmodnZObj( 106, 143 ), ZmodnZObj( 107, 143 ),
ZmodnZObj( 108, 143 ), ZmodnZObj( 109, 143 ), ZmodnZObj( 111, 143 ),
ZmodnZObj( 112, 143 ), ZmodnZObj( 113, 143 ),
ZmodnZObj( 114, 143 ), ZmodnZObj( 115, 143 ), ZmodnZObj( 116, 143 ),
ZmodnZObj( 118, 143 ), ZmodnZObj( 119, 143 ),
ZmodnZObj( 120, 143 ), ZmodnZObj( 122, 143 ), ZmodnZObj( 123, 143 ),
ZmodnZObj( 124, 143 ), ZmodnZObj( 125, 143 ),
ZmodnZObj( 126, 143 ), ZmodnZObj( 127, 143 ), ZmodnZObj( 128, 143 ),
ZmodnZObj( 129, 143 ), ZmodnZObj( 131, 143 ),
ZmodnZObj( 133, 143 ), ZmodnZObj( 134, 143 ), ZmodnZObj( 135, 143 ),
ZmodnZObj( 136, 143 ), ZmodnZObj( 137, 143 ),
```

```
ZmodnZObj( 138, 143 ), ZmodnZObj( 139, 143 ), ZmodnZObj( 140, 143 ),
ZmodnZObj( 141, 143 ), ZmodnZObj( 142, 143 ) ]
gap> Size(ulist(143));120
gap> (Size(ulist(143)))=(Size(ulist(11))*Size(ulist(13)));
true
```

From the above conjecture, we have seen that the order $|U(11)|\cdot|U(13)| = |U(143)| = 120$. Hence, $U(11) \otimes U(13) \cong U(143)$, where $U(143)$ is the new group obtained from the product of $U(11)$ and $U(13)$. The output ZmodnZObj(5, 143) for example, means the element 5 mod 143.

We can also generates different subgroups for each group, for example in $U(143)$, the cyclic subgroup generated by ZmodnZObj(5, 143) is

```
gap> cyclic(143, 5);
[ZmodnZObj( 5, 143 ), ZmodnZObj( 25, 143 ), ZmodnZObj( 125, 143 ),
ZmodnZObj( 53, 143 ), ZmodnZObj( 122, 143 ),ZmodnZObj( 38, 143 ),
ZmodnZObj( 47, 143 ), ZmodnZObj( 92, 143 ), ZmodnZObj( 31, 143 ),
ZmodnZObj( 12, 143 ),ZmodnZObj( 60, 143 ), ZmodnZObj( 14, 143 ),
ZmodnZObj( 70, 143 ), ZmodnZObj( 64, 143 ), ZmodnZObj( 34, 143 ),
ZmodnZObj( 27, 143 ), ZmodnZObj( 135, 143 ), ZmodnZObj( 103, 143 ),
ZmodnZObj( 86, 143 ), ZmodnZObj( 1, 143 ) ]
gap> Size(cyclic(143, 5));
20
```

Taking different values for *n*, *p* and *q* as defined above, gives more group structures and their respective subgroups.

The next conjecture is about the relationship between the size of the groups $U(p^k)$ and $U(2p^k)$ where *p* is a prime number greater than 2, and k is any positive integer. Now let $p = 3$ and $k = 2$.

```
gap> ulist(9);
[ ZmodnZObj( 1, 9 ), ZmodnZObj( 2, 9 ), ZmodnZObj(4,9), ZmodnZObj(5,9),
ZmodnZObj( 7, 9 ), ZmodnZObj( 8, 9 ) ]
gap> Size(ulist(9));
6
gap> ulist(18);
[ ZmodnZObj( 1, 18 ), ZmodnZObj( 5, 18 ), ZmodnZObj(7,18),
ZmodnZObj(11,18 ), ZmodnZObj( 13, 18 ),ZmodnZObj( 17, 18 ) ]
gap> Size(ulist(18));
6
gap> Size(ulist(9))=Size(ulist(18));
true
```

The above result shows that the order $|U(p^k)| = |U(2p^k)|$. We therefore conclude that the two groups are isomorphic to each order. This is true for all prime numbers $p>2$. For $p = 2$, $|U(2p^k)| = 2|U(p^k)|$.

Again, consider the direct product of the cyclic subgroup C_8 of S_8 with the Symmetric group S_4. If we denote the direct product by *D*, then $D = C_8 \otimes S_4$ as presented below.

```
gap> C8:= CyclicGroup(IsPermGroup, 8);
Group([ (1,2,3,4,5,6,7,8) ])
gap> Size(C8);
8
gap> S4:= SymmetricGroup(4);
Sym( [ 1 .. 4 ] )
gap> Size(S4);
24
```

```
gap> D:= DirectProduct(C8, S4);
Group([ (1,2,3,4,5,6,7,8), (9,10,11,12), (9,10) ])
gap> orderFrequency(D);
[ [ 1, 1 ], [ 2, 19 ], [ 3, 8 ], [ 4, 44 ], [ 6, 8 ], [ 8, 64 ], [ 12,
16 ], [ 24, 32 ] ]
gap> Size(D);
192
gap> (Size(C8)*Size(S4))=Size(D);true
gap> IsNormal(D, C8);
true
gap> IsNormal(D, S4);
false
```

From the above result, the constructed group D is isomorphic to the direct product $C_8 \otimes S_4$ of the groups C_8 and S_4. The subgroup C_8 of D is normal in D while the subgroup S_4 is not normal in D. The output orderFrequency(D) means the group D has one element of order 1, nineteen elements of order 2, eight elements of order 3, fourty four elements of order 4, eight elements of order 6, sixty four elements of order 8, sixteen elements of order 12 and thirty two elements of order 24.

Construction by Symmetries

In this section, we formulate some groups based on the movements of the edges of a cube, take Rubik's cube as an example and label the eight vertices with numbers 1 to 8. We shall use G* to denote the group of the rotational symmetries of the cube (of order 8) which is a subgroup of the symmetric group S_8. Note that each rotation is 90^0, (e.g. r = (1, 2, 3, 4)(5, 6, 7, 8) is a rotation through 90^0) (Samaila, 2013).

```
gap> S:= SymmetricGroup(8);
Sym( [ 1 .. 8 ] )
gap> r:= (1, 2, 3, 4)(5, 6, 7, 8);;
gap> H:= Subgroup(S, [r]);
Group([ (1,2,3,4)(5,6,7,8) ])
gap> Elements(H);
[ (), (1,2,3,4)(5,6,7,8), (1,3)(2,4)(5,7)(6,8), (1,4,3,2)(5,8,7,6) ]
gap> s:= (1, 5, 8, 4)(2, 6, 7, 3);;
gap> R:= Subgroup(S, [s]);
Group([ (1,5,8,4)(2,6,7,3) ])
gap> Elements(R);
[ (), (1,4,8,5)(2,3,7,6), (1,5,8,4)(2,6,7,3), (1,8)(2,7)(3,6)(4,5) ]
gap> t:= (1, 2, 6, 5)(3, 7, 8, 4);;
gap> K:= Subgroup(S, [t]);
Group([ (1,2,6,5)(3,7,8,4) ])
gap> Elements(K);
[ (), (1,2,6,5)(3,7,8,4), (1,5,6,2)(3,4,8,7), (1,6)(2,5)(3,8)(4,7) ]
gap> Size(H); Size(R); Size(K);
4
4
4
gap> H = R; H = K; R = K;
false
false
false
gap> L:= Subgroup(S, [r, t]);
Group([ (1,2,3,4)(5,6,7,8), (1,2,6,5)(3,7,8,4) ])
gap> Elements(L);
[ (), (2,4,5)(3,8,6), (2,5,4)(3,6,8), (1,2)(3,5)(4,6)(7,8),
(1,2,3,4)(5,6,7,8), (1,2,6,5)(3,7,8,4), (1,3,6)(4,7,5),
```

```
  (1,3)(2,4)(5,7)(6,8), (1,3,8)(2,7,5), (1,4,3,2)(5,8,7,6),
(1,4,8,5)(2,3,7,6), (1,4)(2,8)(3,5)(6,7),
  (1,5,6,2)(3,4,8,7), (1,5,8,4)(2,6,7,3), (1,5)(2,8)(3,7)(4,6),
(1,6,3)(4,5,7), (1,6)(2,5)(3,8)(4,7), (1,6,8)(2,7,4),
  (1,7)(2,3)(4,6)(5,8), (1,7)(2,6)(3,5)(4,8), (1,7)(2,8)(3,4)(5,6),
(1,8,6)(2,4,7), (1,8,3)(2,5,7),
  (1,8)(2,7)(3,6)(4,5) ]
gap> Size(L);
24
gap> IsCyclic(L);
false
gap> u:= (1,2,4,5,8,6,7,3);;
gap> v:= (2,4,6,8);;
gap> M:= Subgroup(S, [u, v]);
Group([ (1,2,4,5,8,6,7,3), (2,4,6,8) ])
gap> Size(M);
40320
gap> IsCyclic(M);
false
gap> IsNormal(S, M);
true
gap> S = M;
true
gap> Factorization(M, (1,8,3,6,4,5,2,7));
x2^-1*x1^2*x2^2
gap> Factorization(M, (1,6,4,5,3,2,7,8));
x2^2*x1^-1*x2^2*x1^2*x2^-1*x1
gap> Factorization(M, ((1,3,5,7)(2,4,6,8)));
x2^2*x1^-1*(x2^-1*x1^2)^2*x1
gap> Factorization(M, ((1,8)(2,7,4)(3,6,5)));
x1*x2^-1*x1^-2*x2*x1*x2*x1^-2
gap> Factorization(M, ((1,4,2)(3,5,6,8,7)));
x1^-1*x2^-1*(x1^2*x2)^2*x1^-1*x2*x1^2
gap> Factorization(M, (3,8));
x2*x1^-1*(x2*x1)^2*x2^-1*x1^4
gap> quit;
```

It is clear that every rotation of the cube is in the subgroup L. Thus G* = L and hence, G* ≅ L. Also from the output, the subgroups H, R and K of G* are distinct proper subgroups of G*. Again, the output `Factorization(M, (1,8,3,6,4,5,2,7)) = x2^-1*x1^2*x2^2` tells us that $(1,8,3,6,4,5,2,7) = (2,4,6,8)^{-1} * (1,2,4,5,8,6,7,3)^2 * (2,4,6,8)^2$ where x1 and x2 are the first and the second generators of the group M respectively, where M = S.

Next, we define a function *f* from a group G to itself, where G is a cyclic subgroup of the permutation group S_8 as follows:

```
gap> G:= CyclicGroup(IsPermGroup, 8);
Group([ (1,2,3,4,5,6,7,8) ])
gap> Elements(G);
[ (), (1,2,3,4,5,6,7,8), (1,3,5,7)(2,4,6,8), (1,4,7,2,5,8,3,6),
(1,5)(2,6)(3,7)(4,8), (1,6,3,8,5,2,7,4), (1,7,5,3)(2,8,6,4),
(1,8,7,6,5,4,3,2) ]
gap> r:= G.1;
(1,2,3,4,5,6,7,8)
gap> f:= x -> x^5;
```

```
function( x ) ... end
gap> N:= Subgroup(G, [f(r)]);
Group([ (1,6,3,8,5,2,7,4) ])
gap> Elements(N);
[ (), (1,2,3,4,5,6,7,8), (1,3,5,7)(2,4,6,8), (1,4,7,2,5,8,3,6),
(1,5)(2,6)(3,7)(4,8), (1,6,3,8,5,2,7,4), (1,7,5,3)(2,8,6,4),
(1,8,7,6,5,4,3,2) ]
gap> Size(N);
8
gap> Size(G) = Size(N);
true
gap> N = G;
true
gap> f:= x -> x^4;
function( x ) ... end
gap> M:= Subgroup(G, [f(r)]);
Group(())
gap> Elements(M);
[ () ]
gap> Size(M);
1
gap> f:= x -> x^6;
function( x ) ... end
gap> K:= Subgroup(G, [f(r)]);
Group([ (1,7,5,3)(2,8,6,4) ])
gap> Elements(K);
[ (), (1,3,5,7)(2,4,6,8), (1,5)(2,6)(3,7)(4,8), (1,7,5,3)(2,8,6,4) ]
gap> Size(K);
4
gap> Size(G)/Size(K);
2
```

The subgroup N of G is the image of G under the function $f(x) = x^5$. The order of the subgroup N is 8, equal to the order of G and the output shows that N = G. Hence the function *f* is an *automorphism*. But the images M and K of G under the functions $f(x) = x^4$ and $f(x) = x^6$ respectively, are proper subgroups of G, where M is the trivial subgroup of G whose only element is the identity element *e*, of G. The pre-image of M under the function $f(x) = x^4$ gives the kernel of the function. Also, the index [G : K] of the subgroup K in G is 2. Hence, the subgroup N is normal in G, i.e. $N \lhd G$.

Fundamental Theorem of Finite Abelian Group

By the fundamental theorem of finitely generated Abelian groups, every finite Abelian group is isomorphic to the direct product of cyclic groups of prime power order. Knowing that a factor group G/H with G finite and Abelian, is also a finite Abelian group (Samaila, 2016), suppose $G = Z_4 \otimes Z_7 \otimes Z_6$, and that H and M are subgroups of G generated by (2, 1, 2) and (3, 1, 2) respectively, (where 1, 2 and 3 are the powers of the generators), then we generate the factor groups G/H and G/M as follows;

```
gap> Z4:= CyclicGroup(IsPermGroup, 4);
Group([ (1,2,3,4) ])
gap> Z7:= CyclicGroup(IsPermGroup, 7);
Group([ (1,2,3,4,5,6,7) ])
gap> Z6:= CyclicGroup(IsPermGroup, 6);
Group([ (1,2,3,4,5,6) ])
gap> G:= DirectProduct(Z4, Z7, Z6);
Group([ (1,2,3,4), (5,6,7,8,9,10,11), (12,13,14,15,16,17) ])
```

```
gap>      H:=      Subgroup(G,      [(1,2,3,4)^2,      (5,6,7,8,9,10,11),
(12,13,14,15,16,17)^2]);
Group([ (1,3)(2,4), (5,6,7,8,9,10,11), (12,14,16)(13,15,17) ])
gap> F:= FactorGroup(G, H);
Group([ f1, f2 ])
gap> Size(F);
4
gap> Size(H);
42
gap> Size(G);
168
gap>      M:=      Subgroup(G,      [(1,2,3,4)^3,      (5,6,7,8,9,10,11),
(12,13,14,15,16,17)^2]);
Group([ (1,4,3,2), (5,6,7,8,9,10,11), (12,14,16)(13,15,17) ])
gap> N:= FactorGroup(G, M);
Group([ f1 ])
gap> Size(N);
2
gap> Size(M);
84
gap> Elements(F);
[ <identity> of ..., f1, f2, f1*f2 ]
gap> Elements(N);
[ <identity> of ..., f1 ]
```

The group Z_4 is isomorphic to Z_4, Z_7 is isomorphic to Z_7 and Z_6 is isomorphic to Z_6. Thus from the output, G is isomorphic to $Z_4 \otimes Z_7 \otimes Z_6$. Also, in the output as direct product, the elements of Z_7 are written as powers of the permutation (5,6,7,8,9,10,11) and that of Z_6 are written as powers of the permutation (12,13,14,15,16,17). The element $(1,2,3,4)^2$ generates a subgroup of order 2 of Z_4. Similarly, the element $(12,13,14,15,16,17)^2$ generates a subgroup of Z_6 of order 3. Thus H is isomorphic to the subgroup of G generated by (2, 1, 2). Similarly, M is isomorphic to the subgroup of G generated by (3, 1, 2). The factor groups G/H and G/M are finite Abelian groups of order 4 and 2 respectively, so G/H is isomorphic to either Z_4 or $Z_2 \otimes Z_2$ while G/M is isomorphic to Z_2. Now, we have;

```
gap> Read("orderFrequency");
gap> orderFrequency(F);

[ [ 1, 1 ], [ 2, 3 ] ]
```

Hence, since the factor group G/H has three elements of order 2 followed by the identity, it must be isomorphic to $Z_2 \otimes Z_2$.

Group Homomorphism by Image

If we specify any homomorphism, the command "GroupHomomorphismByImages" in GAP will create the specified homomorphism. Now, consider the symmetric group S_4. Then from GAP, we have the following results.

```
gap> S4:= SymmetricGroup(4);
Sym( [ 1 .. 4 ] )
gap> f1:= GroupHomomorphismByImages(S4, S4, [(1,2,3,4), (2,4)],
[(1,4,3,2), (1,3)]);
fail
gap> f2:= GroupHomomorphismByImages(S4, S4, [(1,2,3,4), (1,3,2,4)],
[(1,4,3,2), (1,4,2,3)]);
[ (1,2,3,4), (1,3,2,4) ] -> [ (1,4,3,2), (1,4,2,3) ]
gap> Image(f2, (1,2,4,3));
```

```
(1,2,4,3)
gap> Image(f2, (2,4));
(1,3)
gap> Image(f2, (1,2,4));
(1,4,3)
gap> Size(Image(f2));
24
gap> Kernel(f2);
Group(())
gap> Size(S4) = Size(Image(f2));
true
```

The first output (f1) of the group homomorphism by images is "fail". This is because the defined map is not a homomorphism. From the second output f2, the kernel of f2 is the identity element of S_4 and the size of the image of f2 is the whole of S_4. Hence, f2 is not only a homomorphism, but an automorphism.

Another way to identify if a homomorphism from a finite group G to itself is an automorphism is to determine if it is onto. In this case, we will need the file "GroupHomomorphismByImages" command in GAP to generate homomorphism from D_n to D_n. Then check if they are automorphism by checking to see if the kernel contains only the identity or the image is whole of D_n. Since a homomorphism is completely determined by the image of the generators of a group, we only need to specify where we want to map the two generators of D_n. Then we have the following results:

```
gap> Read("autoDn");
gap> Read("homoDn");
gap> d5:= DihedralGroup(IsPermGroup, 10);
Group([ (1,2,3,4,5), (2,5)(3,4) ])
gap> autoDn(d5);
[ [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (2,5)(3,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (1,2)(3,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (1,3)(4,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (1,4)(2,3) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (1,5)(2,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (2,5)(3,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (1,2)(3,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (1,3)(4,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (1,4)(2,3) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (1,5)(2,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (2,5)(3,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (1,2)(3,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (1,3)(4,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (1,4)(2,3) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (1,5)(2,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (2,5)(3,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (1,2)(3,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (1,3)(4,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (1,4)(2,3) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (1,5)(2,4) ] ]
gap> homoDn(d5);
[ [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (), () ], [ (1,2,3,4,5), (2,5)(3,4)
] -> [ (), (2,5)(3,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (), (1,2)(3,5) ], [ (1,2,3,4,5),
(2,5)(3,4) ] -> [ (), (1,3)(4,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (), (1,4)(2,3) ], [ (1,2,3,4,5),
(2,5)(3,4) ] -> [ (), (1,5)(2,4) ],
```

```
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (2,5)(3,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (1,2)(3,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (1,3)(4,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (1,4)(2,3) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,2,3,4,5), (1,5)(2,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (2,5)(3,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (1,2)(3,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (1,3)(4,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (1,4)(2,3) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,3,5,2,4), (1,5)(2,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (2,5)(3,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (1,2)(3,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (1,3)(4,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (1,4)(2,3) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,4,2,5,3), (1,5)(2,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (2,5)(3,4) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (1,2)(3,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (1,3)(4,5) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (1,4)(2,3) ],
  [ (1,2,3,4,5), (2,5)(3,4) ] -> [ (1,5,4,3,2), (1,5)(2,4) ] ]
gap> Size(autoDn(d5));
20
gap> Size(homoDn(d5));
26
```

The above output from GAP gives all the automorphism and all the homomorphism of the group D_5 to itself. Since a homomorphism is completely determined by its image on a set of generators of the given group, GAP only specifies the image of the sets of the generators.

Conclusion

The Cartesian product of groups play a major role in the construction of new groups. It is seen that for any finite groups G_1 and G_2, the order $|G_1||G_2|=|G_1 \otimes G_2|$ and for all $i = 1, 2, \ldots, n$,

$$|G_1||G_2|...|G_n| = \left|\prod_{i=1}^{n} G_i\right|.$$

Also, the fundamental theorem of finite Abelian group is used for generating and classification of morphisms and then determined the automorphism of a given finite Abelian group. This is achieved from the fact that if the group G is decomposed as a direct sum $H \oplus K$ of subgroups of coprime order, then $\mathrm{Aut}(H \oplus K) \cong \mathrm{Aut}(H) \oplus \mathrm{Aut}(K)$. The result can therefore be generalized as follows: If the group G is decomposed as direct sum $G_1 \oplus G_2 \oplus \ldots \oplus G_n$ of subgroups of coprime order, then $\mathrm{Aut}(G_1 \oplus G_2 \oplus \ldots \oplus G_n) \cong \mathrm{Auto}(G_1) \oplus \mathrm{Auto}(G_2) \oplus \ldots \oplus \mathrm{Auto}(G_n)$. We also used the second part of the theorem which states that every finite Abelian group is isomorphic to the direct product of cyclic groups of prime power order to generate a factor group G/K with G finite and Abelian, K a subgroup of G. Finally, we identify some homomorphism and automorphism from a finite group G to itself.

References

Dummit, D. S.; Foote, R. (2004), Abstract Algebra (3 ed.). Wiley. pp. 71–72. ISBN 9780471433347.

Herstein, Israel Nathan (1996), Abstract algebra (3rd ed.), Upper Saddle River, NJ: Prentice Hall Inc., ISBN 978-0-13-374562-7, MR1375019.

Hillar, Christopher Rhea, (2007), "Automorphisms of finite Abelian groups". American Mathematical Monthly, 114 (10): 917–923.

Jacobson, Nathan (2009), Basic Algebra I (2nd ed.). Dover Publications. ISBN 978-0-486-47189-1.

John B. Fraleigh (1976), A first course in abstract algebra, second edition, Addison-Wesley publishing company. Inc.

La Harpe, Pierre de (2000), Topics in geometric group theory. Chicago lectures in mathematics. University of Chicago Press.ISSBN 978-0-226-31721-2.

Lang, Serge (2002), Algebra, Graduate Texts in Mathematics **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR1878556.

Lang, Serge (2005), Undergraduate Algebra (3rd ed.), Berlin, New York: Springer-Verlag, ISBN 978-0-387-22025-3.

Robinson, Derek John Scott (1996), A course in the theory of groups, Berlin, New York: Springer-Verlag, ISBN 978-0-387-94461-6.

Rose, John S. (2012), [unabridged and unaltered republication of a work first published by the Cambridge University Press, Cambridge, England, in 1978]. A Course on Group Theory, Dover Publications. ISBN 0-486-68194-7.

Samaila D. and Pius P. M. (2016), A Constructive Method for Using Known Groups as Building Blocks to Form More Groups, Journal of Scientific Research & Reports (Science Domain International),11(1): 1-10; Article no.JSRR.26080, ISSN: 2320-0227.

Samaila D. and Pius P. M. (2016), Identification, Generating and Classification of Morphisms between Finite Groups, Journal of Scientific Research & Reports (Science Domain International), 11(1): 1-10; Article no. JSRR. 26346, ISSN: 2320-0227.

Samaila D., Pius P. M and Ibrahim A. B. (2013), Visualizing the Homomorphic Image Through Abstract Characterization of the Symmetry Group D_n, International Journal of Pure and Applied Sciences and Technology; 15(2) pp.33-42, ISSN 2229-6107.