Journal of Scientific Research & Reports
11(1): 1-10, 2016; Article no.JSRR.26080
ISSN: 2320-0227

SCIENCEDOMAIN *international*
www.sciencedomain.org

A Constructive Method for Using Known Groups as Building Blocks to form More Groups

D. Samaila[1*] and M. Pius Pur[1]

[1]Department of Mathematics, Faculty of Science and Science Education, Adamawa State University, P.O.Box 25 Mubi, Nigeria.

Authors' contributions

This work was carried out in collaboration between both authors. Author DS designed the study, wrote the program and wrote the first draft of the manuscript. Author MPP managed the literature searches and analyses the properties of the finite groups and also identified some method of constructing groups. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JSRR/2016/26080
Editor(s):
(1) Stefanka Chukova, School of Mathematics, Statistics and Operation Research, Victoria University of Wellington, New Zealand.
Reviewers:
(1) R. P. Tripathi, Graphic Era University, Dehradun (UK), India.
(2) A. Shehata, Assiut University, Assiut, Egypt.
Complete Peer review History: http://sciencedomain.org/review-history/14770

Review Article

Received 31st March 2016
Accepted 9th May 2016
Published 24th May 2016

ABSTRACT

In this paper, we present some methods of constructing new groups from given ones. We first examined the direct product $\prod_{i=1}^{n} G_i$ of the finite groups G_i for $n \geq 2$ and then observed that $|\prod_{i=1}^{n} G_i| = |G_1||G_2|...|G_n|$. We also established the fact that for any prime number p > 2 and any positive integer k, $|U(p^k)| = |U(2p^k)|$ where U(n) is the set of all integers less than n and relatively prime to n, and finally conclude on symmetries by constructing groups and their respective subgroups, characteristics and the unique factorization of the elements.

Keywords: Cartesian product; group; isomorphism; symmetry; cyclic.

**Corresponding author: E-mail: danjuma1981@gmail.com;*

1. 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, 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 $K \oplus H$ [1]. 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.

Now, it is known that the first class of groups to undergo a systematic study is permutation groups [2]. Given any set X and a collection G of all bijection of X onto itself (also known as *permutations*) that is closed under compositions and inverses, G is a group acting on X. If X consists of n elements and G consists of *all* permutations, then G is the symmetric group S_n, generally, referred by [3], as subgroup of the symmetric group of X.

Permutation groups and matrix groups are special cases of transformation groups; groups that act on a certain space X preserving its inherent structure. In the case of permutation groups, X is a set. An early construction due to Cayley, exhibited any finite group as a permutation group, acting on itself (X = G) [4]. The concept of transformation group is closely related to the concept of symmetric group. Transformation groups frequently consist of all transformations that preserve a certain structure [5].

In view of this, group theory can be addressed as the way in which certain collections of mathematical “objects” are related to each other [6]. For example, the set $\mathbb{Z}$ of integers constitute a group because under certain conditions (particularly, addition), the relationships between the integers obey the rules of group theory. Group theory is also the mathematical application of symmetry to an object to obtain knowledge of its physical properties [7]. Hence, the concept of symmetries is an important tool for constructing finite groups in algebra [8].

2. CARTESIAN PRODUCT

The Cartesian product of sets $S_1, S_2, \ldots, S_n$ is the set of all ordered n-tuples $(x_1, x_2, \ldots, x_n)$, where $x_i \in S_i$ [3]. The Cartesian product is usually denoted by either

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

Now, let the binary operations on the groups $G_1, G_2, \ldots, G_n$ be multiplication. Regarding the G_i assets, we can form the Cartesian product $\prod_{i=1}^{n} G_i$ of the groups $G_1, G_2, \ldots, G_n$. 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 1: Let $G_1, G_2, \ldots, G_n$ be groups. For $(x_1, x_2, \ldots, x_n)$ and $(y_1, y_2, \ldots, y_n)$ in $\prod_{i=1}^{n} G_i$, define $(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$. Then $\prod_{i=1}^{n} G_i$ is a group called the External Direct Product of the groups $G_1, G_2, \ldots, G_n$ under this binary operation [9].

Proof: Now, since each G_i is a group for $i = 1, 2, \ldots, n$ 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:

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

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 $(x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1})$, for ($x_1$, x_2, …, x_n) $(x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}) = (x_1x_1^{-1}, x_2x_2^{-1}, \ldots, x_nx_n^{-1})$ = (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 $r_1r_2\ldots r_n$ 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:

We noticed that for the groups G_1, G_2, …, G_n with orders r_1, r_2, …, r_n respectively, we have $|G_1 \otimes G_2 \otimes \ldots \otimes G_n| = |G_1|\,|G_2| \ldots |G_n| = r_1r_2\ldots r_n$ where the product $G_1 \otimes G_2 \otimes \ldots \otimes G_n$ is a new group which may or may not be isomorphic to the group $G_{r1r2\ldots m}$. 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 $\overline{a}$, and the residue class of a (mod q) by a^*. Obviously, $\overline{a} \in Zp$ and $a^* \in Zq$. Consider the function $\phi: Z \to Zp \otimes Zq$. Then ϕ is a homomorphism for

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

for all $a,b \in Z$. Again, $Z/\mathrm{Ker}\,\phi \cong \mathrm{Im}\phi$. Now $a \in \mathrm{Ker}\phi$ if and only if $\overline{a} = \overline{0}$ 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 $\mathrm{Ker}\phi = pqZ$ and $Z/pqZ \cong \mathrm{Im}\phi$, where the image $\mathrm{Im}\phi$ is a subgroup of $Z/pZ \otimes Z/qZ$. Finally, from

$$pq = |Z/pqZ| = |\mathrm{Im}\phi| \le |Z/pZ \otimes Z/qZ| = |Z/pZ|\,|Z/qZ| = pq$$

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

Hence, we have:

Theorem 2: The group $Z_m \otimes Z_n$ is isomorphic to Z_{mn} if and only if (m, n) = 1 [9].

Proof: Consider the Cyclic subgroup of $Z_m \otimes Z_n$ generated by (1, 1). The order of this cyclic subgroup is the smallest positive integer j for which $(1, 1)^j = e$, the identity element (0, 0) of $Z_m \otimes Z_n$. Now, taking the power of (1, 1) consecutively, the first component $1 \in Z_m$ yields zero only after m, $2m$, … times and the second component $1 \in Z_n$ yields zero only after n, $2n$, … times. For them to yield zero simultaneously, the number of times must be a multiple of m and n and the smallest number which is a multiple of both m and n is mn if and only if the gcd of m and n is 1. In this case (1, 1) generates a cyclic subgroup of order mn which is the order of the group $Z_m \otimes Z_n$ as required.

Example: 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 $\sigma(q)$ = (sgn q, $|q|$) where sgn$|q|$ = $\pm$1. Then σ is a homomorphism for

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

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

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

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: 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 $G_1 \otimes G_2 \otimes \ldots \otimes G_n \cong H_1 \otimes H_2 \otimes \ldots \otimes H_n$ [10].

Proof: 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

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

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 $g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n$ with $g_1\xi_1 = h_1, g_2\xi_2 = h_2, \ldots, g_n\xi_n = h_n$. 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 4: Let p and q be prime numbers, where $p < q$ and $q \neq 1 \pmod p$. Then any group of order pq is cyclic [5].

Proof: Let G be a group of order pq. Then by Sylows theorem, G contains Sylow subgroups N_p and N_q of orders p and q respectively. But the number n_p of Sylow p-subgroups divides pq and satisfies $n_p \equiv 1 \pmod p$, by the second Sylow theorem. Clearly, n_p cannot be divisible by p, and therefore either $n_p = 1$ or $n_p = q$. But $q \neq 1 \pmod p$. It follows that $n_p = 1$. Thus the group G has just one subgroup of order p.

Now, given any element g of G, the subgroups N_p and gN_pg^{-1} are of order p. It follows that $gN_pg^{-1} = N_p$ for all elements g of G. Thus N_p is a normal subgroup of G. Similarly, N_q is a normal subgroup of G since $p < q$ and thus, $p \neq 1 \pmod q$.

Now, $N_p \cap N_q$ is a subgroup of both N_p and N_q. Therefore by Lagrange's theorem, the order of $N_p \cap N_q$ divides both of the prime numbers p and q, and thus $|N_p \cap N_q| = 1$ and $N_p \cap N_q = \{e\}$, the identity element of G.

Again, let $x \in N_p$ and $y \in N_q$. Then $yx^{-1}y^{-1} \in N_p$ and $xyx^{-1} \in N_q$, since N_p and N_q are normal subgroups of the group G. But then $xyx^{-1}y^{-1} \in N_p \cap N_q$, since $xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) = (xyx^{-1})y^{-1}$, and hence $xyx^{-1}y^{-1} = e$. Thus $xy = yx$ for all $x \in N_p$ and $y \in N_q$. It therefore follows that the function $\phi: N_p \otimes N_q \to G$ which sends $(x, y) \in N_p \otimes N_q$ to $xy \in G$ is a homomorphism. This homomorphism is injective for if $xy = e$ for some $x \in N_p$ and $y \in N_q$, then $x = y^{-1}$, and hence $x \in N_p \cap N_q$, from which it follows that $x = e$ and $y = e$. But any injective homomorphism between two finite groups of the same order is necessarily an isomorphism. Thus the function $\phi: N_p \otimes N_q \to G$ is an isomorphism, i.e. $G \cong N_p \otimes N_q$.

Finally, any finite group of prime order is cyclic. Therefore the groups N_p and N_q are cyclic. Now let $x \in N_p$ generates N_p and let $y \in N_q$ generates N_q. Then $(x, y)^n = (x^n, y^n)$ for all integers n. It then follows that the order of (x, y) cannot be 1, p or q, and must therefore be equal to pq. Hence $N_p \otimes N_q$ is a cyclic group generated by (x, y) and thus G is a cyclic group generated by xy, as required.

3. MAIN RESULTS

3.1 Construction by Product

We start this section by constructing groups in favor of theorem 2, with any positive integers m and n such that $(m, n) = 1$ by the use of the programming language GAP (Group Application Package).

Now, since $U(n)$ is defined as 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 using the 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
gap> quit;
```

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
gap> quit;
```

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.

3.2 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°, (e.g. r = (1, 2, 3, 4)(5, 6, 7, 8) is a rotation through 90°) see [11].

```
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* $\cong$ 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` from GAP 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* [12]. 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.

The index [G : K] of the subgroup K in G is 2. Hence, the subgroup N is normal in G, i.e. $N \lhd G$.

4. CONCLUSION

It is necessary to note that symmetries and Cartesian product of groups play a major role in the construction of new groups whether finite or infinite. And that given any two finite groups G_1 and G_2, the order $|G_1||G_2| = |G_1 \otimes G_2|$ and by induction, for all $i = 1, 2, \ldots, n$, $|G_1||G_2|...|G_n| = \left|\prod_{i=1}^{n} G_i\right|$. We therefore conclude that with the use of GAP (Group Application Package), construction of new groups from known ones is always possible.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Herstein, Israel Nathan. Abstract algebra (3rd ed.). Upper Saddle River, NJ: Prentice Hall Inc; 1996.
   ISBN 978-0-13-374562-7, MR1375019
2. Kleiner I. The evolution of group theory: A brief survey. Mathematics Magazine. 1986;59(4):195–215.
3. Lang Serge. Undergraduate Algebra (3rd ed.), Berlin, New York: Springer-Verlag; 2005.
   ISBN 978-0-387-22025-3
4. Nummela E. Cayley's theorem for topological groups; American mathematical monthly. Mathematical Association of America. 1980;87(3):202–203.
5. Robinson Derek, John Scott. A course in the theory of groups. Berlin, New York: Springer-Verlag; 1996.
   ISBN 978-0-387-94461-6
6. Carter NC. Visual group theory classroom resource materials series. Mathematical Association of America; 2009.
7. Robert BV. Crystal symmetry groups. Los Alamos Science Summer, Los Alamos. 1990;152-157.
8. Samaila D, Mshelia IB, Adamu MS. A derived model for the construction of double dihedral groups (q_{2n}) and their properties. Jolorn Leaque of Researchers in Nigeria. 2010;11(2):115-123.
   ISSN: 1595-532X
9. John B. Fraleigh. A first course in abstract algebra, second edition, Addison-Wesley publishing company. Inc; 1976.
10. Lang Serge. Algebra, graduate texts in mathematics 211 (Revised third ed.), New York: Springer-Verlag; 2002.
    ISBN 978-0-387-95385-4, MR1878556.
11. Samaila D, Pius Pur M, Ibrahim Abba B. Visualizing the homomorphic image through abstract characterization of the symmetry group D_n. International Journal of Pure and Applied Sciences and Technology. 2013;15(2):33-42.
    ISSN 2229-6107
12. Samaila D. Counting the subgroups of the one-headed group s_5 up to automorphism. IOSR Journal of Mathematics (IOSR-JM).
    2013;8(3):87-93.
    ISSN: 2278-5728, p-ISSN: 2319-765X

Peer-review history:
The peer review history for this paper can be accessed here:
http://sciencedomain.org/review-history/14770