Construction of New Algebraic Structure of Permutation Group with Prime Order That Has Fix Element

ISMAILA YUSHAU JEGA
Department of Mathematics, Kebbi State University of Science and Technology, Aliero, Nigeria

Abstract- In this work, a new modified algebraic structure is constructed using modular arithmetic. Some algebraic properties of the structure were studied using a particular sequence (a_n). Composition of permutation is also used in studying some of these properties. It is discovered that the elements of the structure formed group under composition of permutation.

Indexed Terms- Permutation, Image, Cycle, Transposition, Symmetric group and Alternating group.

I. INTRODUCTION

One important application of counting principles is in determining the number of ways that *n*-elements can be arranged (in order). An ordering of n-elements is called permutation of the elements. A permutation of n-elements is an ordering of the elements such that one is first, another one is second, and another one is third and so on.

The notion of permutation is used with several other slightly different meanings but all related to the act of permuting (rearranging) objects or values. For example, there are six permutations of the set {1, 2, 3} namely {1, 2, 3}, {1, 3, 2}, {2, 1 ,3}, {2, 3, 1}, {3, 1, 2}, {3, 2, 1}. One might define an anagram of a word as a permutation of its letters. The number of permutations of n distinct objects is *n*(*n*-1)(*n*-2)…2.1. In other word, the number is called n!

Permutations occur in more or less prominent ways in almost every domain of mathematics. They often arise when different orderings on certain finite sets are considered possibly only because one wants to ignore such orderings and needs to know how many configurations are thus identified. For similar reasons permutation arises in the study of sorting algorithm in computer science. In high school mathematics, the words permutation and arrangement are used interchangeably. If the word arrangement is used at all, we draw the distinction between them. If X is a set, then a list in X is a function $f:\{1, 2, 3\ldots n\} \rightarrow X$. If a list f in X is a bijection (so that X is now finiteset with $|X| = n$), then f is called an arrangement of X.

I. FORMULATION OF THE PROBLEM

Let Ω be a non-empty, totally ordered and finite subset of N .

Let 𝔾p $=\{\omega_1, \omega_2 \ldots\ldots \omega_{P-1}\}$ be a structure such that each ω_i is generated from the arbitrary set Ω, for any prime $p \geq 5$, using the scheme

$$\omega_i = \left((2)(2+i)_{mP}(2+2i)_{mP}\ldots(2+(P-1)i)_{mP}\right) \quad (3.2.1)$$

Then each ω_i is called a Cycle and the elements in each ω_i are distinct and called Successors. We denote n^{th} successor in a Cycle ω_i as

$$a_n = (2+(n-1)i)_{mP} \quad (3.2.2)$$

Where the subscript m_P indicates that the numbers are taken *modulo* $p, 1 \leq n \leq P$, and $1 \leq i \leq P-1$. The number of distinct successors in a cycle is called the Length of the Cycle.

II. SOLUTION TO THE PROBLEM

Example 1.1: For $p = 5$, equation (3.21) and (3.22) can generate

𝔾5= $\{(23451), (24135), (25314), (21543)\}$

Where

$\omega_1 = (23451),\ \omega_2 = (24135),\ \omega_3 = (25314),\ \omega_4 = (21543)$

Each with length 5.

Example 1.2: Let verify Group properties on permutation 𝔾p for $p = 5$, (where *p* is prime)

Closure Property:

$$(23451)(24135) = (25314)$$
$$(25314)(21543) = (24135)$$
$$(21543)(23451) = (21543)$$

Associative property:

$$(13524)[(15432)(14253)] = (13524)(13524) = (15432)$$
$$[(13524)(15432)](14253) = (14253)(14253) = (15432)$$

Existence of Identity:
It is observed that

$$\forall \omega_i \in G_p \exists \ e = \omega_1$$
$$\ni \omega_i.\omega_1 = \omega_1.\omega_i = \omega_i \forall \omega_i \in G_p$$
$$(23451)(25314) = (25314)$$

Existence of Inverse:
Also for each

$$\forall \omega_i \in G_p \exists \ \omega_i^{-1}$$
$$\ni \omega_i.\omega_i^{-1} = \omega_i^{-1}.\omega_i = \omega_1 = e \quad \forall \omega_i \in G_p$$
$$(24135)(25314) = (23451)$$

composition of ω_i for $p = 5$, (where p is prime)

Let $\omega_1 = (23451)$, $\omega_2 = (24135)$, $\omega_3 = (25314)$, and $\omega_4 = (21543)$

Then

	ω_1	ω_2	ω_3	ω_4
ω_1	ω_1	ω_2	ω_3	ω_4
ω_2	ω_2	ω_4	ω_1	ω_3
ω_3	ω_3	ω_1	ω_4	ω_2
ω_4	ω_4	ω_3	ω_2	ω_1

Table 4.4: Composition of ω_i for $i = 1, 2, 3, 4$

Example 1.3: For $p = 7$, equation (1) and (2) can generate
$\mathbb{G}_7$=
$$\{(2345671), (2461357), (2514736), (2637415), (2753164), (2176543)\}$$
where

$\omega_1 = (2345671)$, $\omega_2 = (2461357)$,
$\omega_3 = (2514736)$, $\omega_4 = (2637415)$,
$\omega_5 = (2753164)$ $\omega_6 = (2176543)$

Each with length 7.

	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6
ω_1	ω_1	ω_2	ω_3	ω_4	ω_5	ω_6
ω_2	ω_2	ω_4	ω_6	ω_1	ω_3	ω_5
ω_3	ω_3	ω_6	ω_2	ω_5	ω_1	ω_4
ω_4	ω_4	ω_1	ω_5	ω_2	ω_6	ω_3
ω_5	ω_5	ω_3	ω_1	ω_6	ω_4	ω_2
ω_6	ω_6	ω_5	ω_4	ω_3	ω_2	ω_1

Table 4.5: Composition of ω_i for $i = 1, 2, 3, 4, 5, 6$

Example 1.4: On direct substitution in equation (3.2.2), for each i, the first successor in ω_i, $1 \le i \le p-1$, is 2 as established in the above example. Similarly, the second successor in ω_6, for instance, is 1 and the third is 7, since, 0 and 7 are equivalent in mod7.

Example 1.5: For $P = 11$, equation (3.2.1) and (3.2.2) can generate the structure $\mathbb{G}_{11}$=
$$\{(23456789(10)(11)1), (2468(10)13579(11)), (258(11)36$$
$$(26(10)37(11)48159), (2716(11)5(10)4938), (28394(10$$
$$(295184(11)73(10)6), (2(10)741963(11)85), (2(11)9753$$
$$(21(11)(10)9876543)\}$$
Where

$$\omega_1 = (23456789(10)(11)1)$$
$$\omega_2 = (2468(10)13579(11))$$
$$\omega_3 = (258(11)369147(10))$$
$$\omega_4 = (26(10)37(11)48159)$$
$$\omega_5 = (2716(11)5(10)4938)$$
$$\omega_6 = (28394(10)5(11)617)$$
$$\omega_7 = (295184(11)73(10)6)$$
$$\omega_8 = (2(10)741963(11)85)$$
$$\omega_9 = (2(11)97531(10)864)$$
$$\omega_{10} = (21(11)(10)9876543)$$

Each with length 11.

Example 1.6: On direct substitution in equation (3.22), for each i, the first successor in ω_i, $1 \le i \le p-1$, is 2 as established in the above example. Similarly, the second successor in ω_{10}, for instance, is 1 and the third is 11, since, 0 and 11 are equivalent in mod11.

Example 1.7: For $P = 13$, equation (3.21) and (3.22) can generate the structure $\mathbb{G}_{13}$=

$$\{(23456789(10)(11)(12)(13)1), (2468(10)(12)13579(11)(13)), (258(11)147(10)(13)369(12)),$$
$$(26(10)159(13)48(12)37(11)), (27(12)4916(11)38(13)5(10)), (2817(13)6(12)5(11)4(10)39),$$
$$(293(10)4(11)5(12)6(13)718), (2(10)5(13)83(11)6194(12)7), (2(11)73(12)84(13)951(10)6),$$
$$(2(12)963(13)(10)741(11)85), (2(13)(11)97531(12)(10)864), (21(13)(12)(11)(10)9876543)\}$$

Where

$$\omega_1 = (23456789(10)(11)(12)(13)1)$$
$$\omega_2 = (2468(10)(12)13579(11)(13))$$
$$\omega_3 = (258(11)147(10)(13)369(12))$$
$$\omega_4 = (26(10)159(13)48(12)37(11))$$
$$\omega_5 = (27(12)4916(11)38(13)5(10))$$
$$\omega_6 = (2817(13)6(12)5(11)4(10)39)$$
$$\omega_7 = (293(10)4(11)5(12)6(13)718)$$
$$\omega_8 = (2(10)5(13)83(11)6194(12)7)$$
$$\omega_9 = (2(11)73(12)84(13)951(10)6)$$
$$\omega_{10} = (2(12)963(13)(10)741(11)85)$$
$$\omega_{11} = (2(13)(11)97531(12)(10)864)$$
$$\omega_{12} = (21(13)(12)(11)(10)9876543)$$

Each with length 13.

Example 1.8: On direct substitution in equation (3.22), for each i, the first successor in ω_i, 1 ≤ i ≤ p − 1, is 2 as established in the above example. Similarly, the second successor in ω_{12}, for instance, is 1 and the third is 13 since, 0 and 13 are equivalent in mod13.

Example 1.9: For $P = 17$, equation (3.21) and (3.22) can generate the structure $\mathbb{G}_{17}$=

$$(23456789(10)(11)(12)(13)(14)(15)(16)(17)1)$$
$$(2468(10)(12)(14)(16)13579(11)(13)(15)(17))$$
$$(258(11)(14)(17)369(12)(15)147(10)(13)(16))$$
$$(26(10)(14)159(13)(17)48(12)(16)37(11)(15))$$
$$(27(12)(17)5(10)(15)38(13)16(11)(16)49(14))$$
$$(28(14)39(15)4(10)(16)5(11)(17)6(12)17(13))$$
$$(29(16)6(13)3(10)(17)7(14)4(11)18(15)5(12))$$
$$(2(10)19(17)8(16)7(15)6(14)5(13)4(12)3(11))$$
$$(2(11)3(12)4(13)5(14)6(15)7(16)8(17)91(10))$$
$$(2(12)5(15)81(11)4(14)7(17)(10)3(13)6(16)9)$$
$$(2(13)71(12)6(17)(11)5(16)(10)4(15)93(14)8)$$
$$(2(14)94(16)(11)61(13)83(15)(10)5(17)(12)7)$$
$$(2(15)(11)73(16)(12)84(17)(13)951(14)(10)6)$$
$$(2(16)(13)(10)741(15)(12)963(17)(14)(11)85)$$
$$(2(17)(15)(13)(11)97531(16)(14)(12)(10)864)$$
$$(21(17)(16)(15)(14)(13)(12)(11)(10)9876543)$$

Range of a Cycle

We define the Range of a Cycle $\omega \in \mathbb{G}_p$ as $\pi(\omega) := \left|\Delta_f^1(\omega)\right|$ where $\Delta_f^1(\omega)$ is the difference between the first and the last successors in a Cycle ω.

General Setting

Let $\mathbb{G}_p = \{\omega_1, \omega_2 \ldots\ldots \omega_{P-1}\}$ Define an operator

$$\pi : \mathbb{G}_p \to X \tag{3}$$

Such that $\forall \omega \in \mathbb{G}_p$ we have

$$\pi(\omega) := \Delta_f^1(\omega) \tag{4}$$

The operator $\pi(\omega)$ is said to have defined a range for any such ω. Then we have the following:

Proposition 1

The operator π defines an Isomorphism on $\mathbb{G}_p$.

Proof:

Each ω is a Cycle structure and so the first successor is always 2. Thus π is well defined and non-empty. Furthermore, each ω is distinct up modularity.

Thus, $\pi(\omega_i) := \pi(\omega_j)$ if and only if $i = j$, which implies that π is injective. In addition, suppose $x = \pi(\omega)$ for some cycle ω. Then $x \in X$. This implies that $\pi(x) = \omega$. Hence π is onto. The result follows.

Theorem 1.1

For any $\omega \in \mathbb{G}_p$ $p \geq 5$ a prime, $\exists\ x \in X$ such that $\pi(\omega) = x$ mod p.

Proof:

From the proof of theorem 4.16.1, it follows that π is an isomorphism, that is,

$\forall\ x \in X\ \exists n_i \in N\ , 1 \le n_i < p,$ such that, $x = P - n_i\ , i \in 1$ an index set. It follows from equation (4) that

$$\pi(\omega_i) := (\omega_j) = x \in X$$
$$\Rightarrow X = p \bmod p - n, \bmod p$$
$$= (p - n) \bmod p$$
$$= x \bmod p .$$

Number Theoretic Properties of $\mathbb{G}_p$

The number theoretic properties of this scheme are motivated by the nature of the sequence generated in the pairing of points of the Cycles. Consequently, we have the following proposition.

Proposition 2

For any prime number $p \ge 5$,

$\sum_{i=1}^{n-1} \Delta_i^f(\omega_i)$ is divisible by p

Proof:

By Equations (3.2.1) and (3.2.2) as a general scheme, we have

$$\omega_1 := ((a_1)(a_1+1)(a_1+2)...(a_1+(p-1)))$$
$$\omega_2 := ((a_1)(a_1+2)(a_1+3)...(a_1+(p-2)))$$
$$\omega_3 := ((a_1)(a_1+3)(a_1+4)...(a_1+(p-3)))$$

.

.

.

$$\omega_{p-1} := ((a_1)(a_1+(p-1))(a_1+(p-2))...(a_1+1))$$

Hence

$$\sum_{i=1}^{p-1} \Delta_i^f(\omega_i) = (p-1) + (p-2) + (p-3) + ... + 1$$
$$= \frac{1}{2} np$$
$$= \frac{1}{2}(p-1)p$$

Range of ω_i

We use the concept of parenthesizing in Catalan Numbers to develop the scheme for some primes $11 \le p \le 17$ as follows:

$\mathbb{G}_{11}$=

$\{(23456789(10)(11)1), (2468(10)13579(11)), (258(11)36$

$(26(10)37(11)48159), (2716(11)5(10)4938), (28394(10$

$(295184(11)73(10)6), (2(10)741963(11)85), (2(11)9753$

$(21(11)(10)9876543)\}$

$\mathbb{G}_{13}$=

$\{(23456789(10)(11)(12)(13)1), (2468(10)(12)13579(11)(13)),$

$(26(10)159(13)48(12)37(11)), (27(12)4916(11)38(13)5(10)), ($

$(293(10)4(11)5(12)6(13)718), (2(10)5(13)83(11)6194(12)7), ($

$(2(12)963(13)(10)741(11)85), (2(13)(11)97531(12)(10)864), ($

$G_{17=}$

$$((2)(3)(4)(5)(6)(7)(8)(9)(10)(11)(12)(13)(14)(15)(16)(17)(1))$$
$$((2)(4)(6)(8)(10)(12)(14)(16)(1)(3)(5)(7)(9)(11)(13)(15)(17))$$
$$((2)(5)(8)(11)(14)(17)(6)(3)(9)(12)(15)(1)(4)(7)(10)(13)(16))$$
$$((2)(6)(10)(14)(1)(5)(9)(13)(17)(4)(8)(12)(16)(3)(7)(11)(15))$$
$$((2)(7)(12)(17)(5)(10)(15)(3)(8)(13)(1)(6)(11)(16)(4)(9)(14))$$
$$((2)(8)(14)(3)(9)(15)(4)(10)(16)(5)(11)(17)(6)(12)(1)(7)(13))$$
$$((2)(9)(16)(6)(13)(3)(10)(17)(7)(14)(4)(11)(1)(8)(15)(5)(12))$$
$$((2)(10)(1)(9)(17)(8)(16)(7)(15)(6)(14)(5)(13)(4)(12)(3)(11))$$
$$((2)(11)(3)(12)(4)(13)(5)(14)(6)(15)(7)(16)(8)(17)(9)(1)(10))$$
$$((2)(12)(5)(15)(8)(1)(11)(4)(14)(7)(17)(10)(3)(13)(6)(16)(9))$$
$$((2)(13)(7)(1)(12)(6)(17)(11)(5)(16)(10)(4)(15)(9)(3)(14)(8))$$
$$((2)(14)(9)(4)(16)(11)(6)(1)(13)(8)(3)(15)(10)(5)(17)(12)(7))$$
$$((2)(15)(11)(7)(3)(16)(12)(8)(4)(17)(13)(9)(5)(1)(14)(10)(6))$$
$$((2)(16)(13)(10)(7)(4)(1)(15)(12)(9)(6)(3)(17)(14)(11)(8)(5))$$
$$((2)(17)(15)(13)(11)(9)(7)(5)(3)(1)(16)(14)(12)(10)(8)(6)(4))$$
$$((2)(1)(17)(16)(15)(14)(13)(12)(11)(10)(9)(8)(7)(6)(5)(4)(3))$$

And in general, for any prime p , we have

$$\mathbb{G}_p = \{\omega_1, \omega_2, ... \omega_{p-1}\}$$

Where

$$\omega_1 = ((2)(2+i)_{mP}(2+2i)_{mP} ... (2+(p-1)_{mP})$$

And

$(2+(n-1)i)_{mP}$ is as defined in equation (3.22)

Further Algebraic Properties

Further algebraic theoretic properties of the structure $\mathbb{G}_p$ can be obtained by embedding a special Cycle into it as follows.

Extending $\mathbb{G}_p$

Let Ω be a non-empty set and $\mathbb{G}_p = \{\omega_1, \omega_2, \ldots \omega_{p-1}\}$ be as defined earlier, where $p \geq 5$ is prime and ω_i are Cycles. Define $\mathbb{G}_p$ = $\mathbb{G}_p \bigcup \omega_p$ (7)

Where

$$\omega_p = \{((p)(p)(p)L(p))\} \quad (8)$$

is a special Cycle with Length 1 in which the successors are not distinct. Then we have the following:

Proposition 3

Let $\mathbb{G}_p$ be as defined in equation (7) and $\varphi_{i,j} \coloneqq \mathbb{G}_p \rightarrow \mathbb{G}_p$ be a concatenation map, $1 \leq i, j \leq p,\ \ p = 5 \textit{ and } 13$ is a prime. Then ($\mathbb{G}_p$ $, \varphi)$ is an abelian group.

Proof:

Define $\varphi_{i,j}(\omega_i, \omega_j) \coloneqq \omega_{i+j}$, where $(i+j)$ is reduced to mod p, to be the concatenation map since $(i+j)$ is reduced to mod p, $\varphi_{i,j}(\omega_i, \omega_j) \coloneqq \omega_{i+j} \in$ $\mathbb{G}_p$ and $\varphi_{i,j}(\omega_i, \omega_j) \coloneqq \omega_{i+j} = \omega_{i+j} \in \mathbb{G}_p$ for every $(i+j)$ mod p, implying closure and commutativity. Associativity easily follows.

Similarly, for every $\omega_i \in \mathbb{G}_p$, $\varphi_{i,p}(\omega_i, \omega_p) = \omega_{i+p} = \omega_i$ and that there exist an $i' \in [1, p]$ such that $\varphi_{i,y}(\omega_i, \omega_y) \coloneqq \omega_{i+y} = \omega_p$. this implies that ω_i is the reverse of ω_i and ω_p is the identity.

Proposition 4

Let $\pi \coloneqq \mathbb{G}_p \rightarrow X'$ be as defined in (3). The set X' forms a canonical set of representatives for integer modulo p with identity.

Proof: By theorem (4.3.1),

every $x \in X$ is expressible as $x = p - n_i,\ 1 \leq n_i < p,\ i \in I$, an index set. It follows that the only element that is missing there is the zero element. With the extension $\mathbb{G}_p$ to $\mathbb{G}_p$ we have $x = p - n_i, 1 \leq n_i \leq p,\ \forall x \in X'$.

CONCLUSION

We have so far established some group theoretic and number theoretic properties. Some properties of the new algebraic structure $\mathbb{G}_p$ were investigated using some permutation pattern of numbers. An operator is defined on the $\mathbb{G}_p$ constructed as composition of permutation in order to study the properties of the resulting structure. The structure was also used to generate some integer sequences. The concept of extension was used to extend the $\mathbb{G}_p$ with some algebraic theoretic properties.

In addition to this, the structure was found to be a group and each cycle of the structure was also found to be a ring. Homomorphism also holds in the structure.

Finally, some functions were also defined on the cycle of the structure to construct a graph where adjacency matrix for each graph is presented.

REFERENCES

[1] Audu, M.S. (1986). Generating sets for transitive permutation groups of prime order, Abacus. The Journal of Mathematical Association of Nigeria,17(2): 22-26.

[2] Audu, M.S. (1991). On transitive permutation groups, Africa Mathematica. Journal of African Mathematical Union, 4(2): 155-160.

[3] Britnell, J. R., & Wildon, M. (2010). Orbit coherence in permutation groups. 2010 Mathematics Subject Classification. 20B10; (secondary) 20E22, 06A12. 456-463.

[4] Cohen, A., Murray, S. H., Pollet, M., & Sorge, V. (2003). to Permutation Group Problems, F. Baader (Ed.): CADE-19, LNAI 2741, pp. 258–273.

[5] Darafsheh, M. R. (2002). Product of the symmetric group with the alternating group on seven letters. Quasigroups and Related Systems 9 (2002), 33−44.

[6] Dhall, S. K. (1993). Symmetry in interconnection networks based on Cayley graphs of permutation groups : A survey. Parallel Computing North-Holland. 361-407.

[7] Garba, A.I. and Ibrahim, A.A. (2010). A New Method of Constructing a Variety of Finite Group Based on Some Succession Scheme. Internal Journal of Physical Science,

2(3): 23-26.

[8] Garba, A.I., Wakil, A. and Modu, B. A. (2010). Some Algebraic and Topological Properties Groups with Prime Order. Internal Journal of Natural and Applied Sciences, 2(3): 23-26.

[9] Gens, R. (1992). Deep Symmetry Networks. cs.washington.edu 1–9. Goulden, I. P., & Jackson, D. M. (1992). The Combinatorial Relationship Between Trees. Cacti and Certain Connection Coefficients for the Symmetric Group, Europ. J. Combinatorics (1992) 13, 357-365.

[10] Ibrahim, A. A. (2006). Correspondence between the length of some class of permutation patterns and primitive elements of automorphism group modulo n, Abacus. The Journal of Mathematical Association of Nigeria, 33: 143-14.

[11] Ibrahim, A.A. (2005). On the combinatorics of succession using a 5-element sample, Abacus. The Journal of Mathematical Association of Nigeria, 32(2B): 410- 415.

[12] Ibrahim, A.A. (2007a). A Counting scheme and some Algebraic Properties of class of special ermutation patterns, Journal of Discrete Mathematical Sciences and Cryptography, 10: 537-546.

[13] Ibrahim, A.A. (2007b). An Enumeration scheme and some algebraic properties of a special (132) - avoiding class of Permutation Patterns. Trends in Applied Sciences Research, 2: 334-340.

[14] Ibrahim, A.A. (2008). Some transformation schemes involving the special (132) – avoiding permutation patterns and a binary coding: An algorithmic approach. Asian Journal of Algebra, 1: 10-14.

[15] Ibrahim, A.A. and Audu, M.S. (2005). Some group theoretic properties of certain class of (123) and (132) avoiding patterns of numbers: An enumeration scheme. African Journal of Natural Sciences, 8: 79-84.

[16] Ibrahim, A.A. and Garba, A.I., (2011). On the use of Automata Models in the study of a class of (123)–Avoiding Permutation Patterns: Application to Circuit Design and in Number Theory. Journal of Science and technology Research,10(1): 71-78.

[17] Ibrahim, M., Ibrahim, A.A. and Garba, A.I. (2012). Algebraic Properties of The (132) – Avoiding Class of Aunu Permutation Patterns: Application to Graphs, International Journal of Mathematical and Computational Analysis,4(1): 48-55.

[18] Road, R. (1981). A New Construction of Young's Seminormal Representation of the Symmetric Group. Journal of Algebra 69(1981) 287–297.

[19] Seress, A., & Results, S. O. F. (1992). On the Diameter of Permutation Groups. Europ. J. Combinatorics (1992) 13, 231-243.