Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

Volume-2 Issue-3 || June 2023 || PP. 250-256

https://doi.org/10.55544/jrasb.2.3.33

Special Applications of Cyclic Groups

Zaki Zurmati[1], Hayatullah Saeed[2] and Samimullah Miakhel[3]

[1]Assistant Professor, Department of Mathematics, Education Faculty Paktia University, AFGHANISTAN.

[2]Teaching Assistant, Department of Mathematics, Education Faculty Paktika University, AFGHANISTAN.

[3]Teaching Assistant, Department of Mathematics, Education Faculty Paktika University, AFGHANISTAN.

Correspondence Author: Hayatullah Saeed

www.jrasb.com || Vol. 2 No. 3 (2023): June Issue

Received: 11-06-2023 **Revised:** 25-06-2023 **Accepted:** 03-07-2023

ABSTRACT

Cyclic groups are common in our everyday life. A cyclic group is a group with an element that has an operation applied that produces the whole set. A cyclic group is the simplest group. A cyclic group could be a pattern found in nature, for example in a geometric pattern we draw ourselves. Cyclic groups can also be thought of as rotations, if we rotate an object enough time we will eventually return to the original position. In this research paper we explore further applications of cyclic groups in number theory like division algorithm and Chinese remainder theorem and other applications including chaos theory, 12-hour clock, modular system, bell ringing, linear codes. If someone can recognize a cyclic group, they could use the generator to find the fastest simple circuit for use in other real-world applications and in pure mathematics.

Keywords- Group, cyclic group, rotation, 12-hour clock, code, codeword, linear code.

I. INTRODUCTION

Cyclic groups are the simplest groups. A cyclic subgroup is closed. Cyclic groups are the building blocks of abelian groups.

There is a difference between an ordinary group and a cyclic group. The rational numbers are a group under addition, but there is no rational number that generates all the rational numbers. The integers have a generator of 1 and -1, We have clarified this concept by example.

First, we will define group and their properties.

Definition. A group is an ordered pair $(G,*)$, where G is a nonempty set and $*$ is a binary operation on G such that the following properties hold:

(A_1) For all $a,b,c \in G,\ a*(b*c)=(a*b)*c$ (associative law).

(A_2) There exists , $e \in G$ such that for all , $a \in G,\ a*e=e*a$ (existence of an identity).

(A_3) For all $b \in G$, there exists $b' \in G$ such that $b*b'=e=b'*b$ (existence of an inverse).

Thus, a group is a mathematical system $(G,*)$ satisfying axioms A_1 to A_3 [2].

Examples of Groups:

1. $(\mathbb{Z},+)$ is a group with identity 0. The inverse of $x \in \mathbb{Z}$ is $-x$.
2. $(\mathbb{Q},+)$ is a group with identity 0. The inverse of $x \in \mathbb{Q}$ is $-x$.
3. $(\mathbb{R},+)$ is a group with identity 0. The inverse of $x \in \mathbb{R}$ is $-x$.

Associative law is also satisfying [7]. A group G is called cyclic if there is an element than generates the entire set by repeatedly applying an operation [4], for more clarification we have the following definition.

Definition 1. If a group $G=\langle a\rangle$ for some $a \in G$ then we say G is a cyclic group. Moreover, any element b for which $\langle b\rangle = G$ is called a generator of G.

That said, let me just give a few examples to get used to the idea of a generator.

Example 1. A nice infinite group example is found in $(\mathbb{Z},+)$. Observe,

$$\langle 1\rangle = \{n(1)\ n \in \mathbb{Z}\} = \mathbb{Z}.$$

likewise, $\langle -1\rangle = \{n(-1)\ n \in \mathbb{Z}\} = \mathbb{Z}$. Thus Z is generated by both 1 and -1.

Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

Volume-2 Issue-3 || June 2023 || PP. 250-256

https://doi.org/10.55544/jrasb.2.3.33

Example 2. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ has $\langle 1\rangle = \{0, 1, 2, 3\}$ and $\langle 2\rangle = \{0, 2\}$ and $\langle 3\rangle = \{0, 3, 2, 1\}$ hence 1 and $3 = -1$ serve as generators for $\mathbb{Z}_4$ [3].

Cyclic groups can be thought of as rotations. An object with rotational symmetry is also known in biological contexts as radial symmetry.

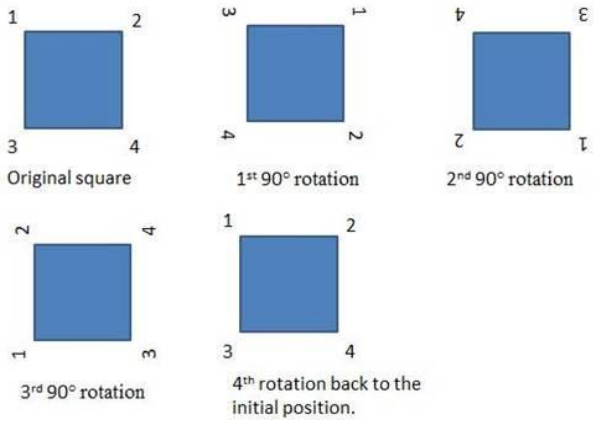


Figure 1: 90 degree rotations of a square

We can draw a square moving 90 degrees 4 times (Figure 2). For a polygon with n sides, we can divide $360/n$ to determine how may degrees each rotation will be to return to the original position.

Not all shape rotations are considered cyclic. The rotation of a circle is not cyclic. It is not like the infinite cyclic group because it is not countable. A circle has an infinite number of sides. We cannot map every side to the integers therefore a circle's rotations are not countable.

II. APPLICATIONS OF CYCLIC GROUP IN NUMBER THEORY

Cyclic groups are found in nature, patterns, and other fields of mathematics. A common application of a cyclic group is in number theory. The division algorithm is a fundamental tool for the study of cyclic groups.

Division algorithm for integers: if m is a positive integer and n is any integer, then there exist unique integers q and r such that,

$$n = mq + r \text{ and } 0 \leq n < m.$$

Example 1. Find the quotient q and remainder r when 45 is divided by 7 according to the division algorithm.
The positive multiples of 7
are $7, 14, 21, 28, 35, 42, 49, \ldots$

$$45 = 42 + 3 = 7(6) + 3$$

The quotient is $q = 6$ and the remainder is $r = 3$.

You can use the division algorithm to show that a subgroup $(H,*)$ of a cyclic group $(G,*)$ is also cyclic.

Theorem 1. A subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group generated by a and let H be a subgroup of G. If $H = e$, then $H = \langle e\rangle$ is cyclic. If $H \neq e$, then $a^n \in H$ for some $n \in \mathbb{Z}^+$.Let m be the smallest integer in $\mathbb{Z}^+$ such that $a^m \in H$. $C = a^m$ generates H. $H = \langle a^m\rangle = \langle c\rangle$.

We must show that every $b \in H$ is a power of c. Since $b \in H$ and $H \leq G$, we have $b = a^n$ for some N. Find a q and r such that

$$n = mq + r \text{ and } 0 \leq r < m.$$

Then

$$a^n = a^{mq+r} = (a^m)^q a^r,$$

So

$$a^r = (a^m)^{-q} a^r$$

Since $a^n \in H, a^m \in H$ H and H is a group, both $(a^m)^{-q}$ and a^n are in H. Thus $(a^m)^{-q} n \in H$, $a^r \in H$ then Since m was the smallest positive integer such that $a^m \in H$ and $0 \leq r < m$, we must have that $r = 0$. Thus $n = mq$ and

$$b = a^n = (a^m)^q = c^q,$$

So b is a power of c

■

Definition: Let r and s be two positive integers. The positive integer d of the cyclic group

$$H = rn + ms/n, m \in \mathbb{Z}$$

under addition is the greatest common divisor of both $r = 1r + 0s$ and $s = 0s + 1s$ are in H. Since $d \in H$ we can write

$$d = nr + ms$$

For some integers n and m. We see every integer dividing both r and s divides the right hand side of the equation, and hence must be a divisor of d also. Thus, d must be the largest number dividing both r and s.

Example 2. Find the GCD of 24 and 54.

The positive dividers of 24 are$1, 2, 3, 4, 6, 8, 12,$ and 24. The positive dividers of 54 are
$1, 2, 3, 6, 9, 18, 27$ and 54. The greatest common divisor is 6. $6 = 1(54) + (-2)24$.

A different result of congruencies in number theory is the Chinese remainder theorem. The Chinese remainder theorem determines the number n that when divided by some given divisors leave given remainders.

Theorem 2. The Chinese remainder theorem. The system of congruencies.

$$x \equiv a_i (mod\ m_i), i = 1, 2, 3, \ldots, k$$

where $(m_i, m_j) = 1$ *if* $i \neq j$, *has a unique solution modulo* $m_1 m_2\ m_3 \ldots\ m_k$.

Proof: We first show by induction, that system (1) has a solution. The result is obvious when $k = 1$. Let us consider the case $k = 2$. If $xa_1 (mod\ m_1)$, then $x = a_1 + k_1 m_1$for some k_1. If in addition $x \equiv a_2 (mod\ m_2)$, then

$$a_1 + k_1 m_2 \equiv a_2 (mod\ m_2)$$

or

$$k_1 m_1 \equiv a_2 - a_1 (mod\ m_2).$$

Because $(m_2 m_1) = 1$, we know that this congruence, with k_1 as the unknown, has a unique solution modulo m_2. Call it t. Then $k_1 = t + k_2 m_2$ for some k_2, and

$$x \equiv a_i (mod\ m_i), i = 1, 2, 3, \ldots, r - 1.$$

Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

Volume-2 Issue-3 || June 2023 || PP. 250-256

https://doi.org/10.55544/jrasb.2.3.33

But the system

$$x \equiv s(mod\ m_1m_2m_3 \dots m_{r-1}),$$

$$x \equiv a_r(mod\ m_r)$$

Has a solution modulo the product of the moduli, just as in the case $k = 2$, because $(m_1m_2m_3 \dots m_{k-1}, m_k) = 1$. This statement is true because no prime that divides m_i. The solution is unique. If r and s are both solutions to the system then $r \equiv s \equiv a_i(mod\ m_i), i = 1, 2, 3, \dots, k$. So $m_i \mid (r - s), i = 1, 2, \dots, k$.Thus $r - s$ is a common multiple of $m_1m_2m_3 \dots m_k$, and because the moduli are relatively prime in pairs, we have $m_1m_2m_3 \dots m_k \mid (r - s)$. Since r and s are least residuals modulo $m_1m_2m_3 \dots m_k$

$$-m_1m_2m_3 \dots m_k < r - s < m_1m_2m_3 \dots m_k$$

Hence,

$$r - s = 0.$$

III. APPLICATION OF CYCLIC GROUPS IN BELL RINGING

Method ringing, known as scientific ringing, is the practice of ringing the series of bells as a series of permutations. A permutation $f: 1, 2, \dots, n \longrightarrow 1, 2, \dots, n$, where the domain numbers represent positions and the range numbers represent bells. $f(1)$ would ring the bell first and bell $f(n)$ last. The number of bells n has $n!$ possible changes.

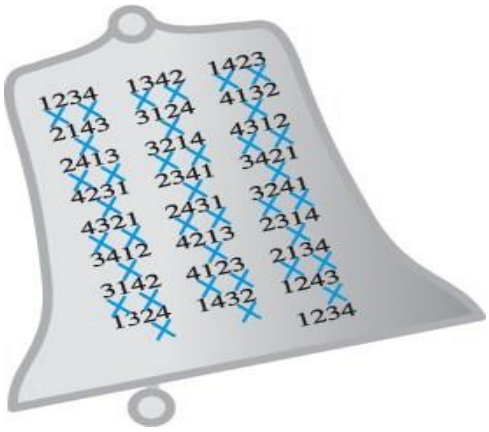


Figure 2: Plain Bob Minimus permutation

The bell ringer cannot choose to ring permutations in any order because some of the bells continue to ring up to 2 seconds. Therefore, no bell must be rung twice in a row. These permutations can all be played until it eventually returns to the original pattern of bells.

A common permutation pattern for four bells is the Plain Bob Minimus permutation (Figure 2). The Plain Bob pattern switches the first two bells then the second set of bells. They would start the bell ringing with 1234. The first bell would go to the second position and third would go to the fourth; therefore, the next bell combination would be 2143. The next bell switch would be the two middle bells. Therefore, the bell 2143 would turn to 2413. The bell ringers would repeat this pattern of switching the first two and second two, followed by switching the middle until about $1/3$ of the way through the permutations. At the pattern 1324, we cannot switch the middle two. If we switched the middle two, we would get back to 1234. Therefore, the bell ringers figured out to switch the last two bells every 8 combinations. Then after 24 moves (4!) we get back to the bell combination of 1234. Since we made rotations of the bells and generated every combination of the set and are now back at the beginning, we can say that the bell ringing pattern is cyclic [4].

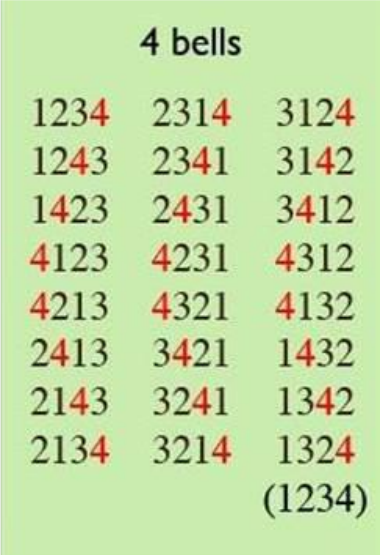


Figure 3: Permutation of 4 bells

IV. CLOCK ARITHMETIC AND MODULAR SYSTEM

One of the fantastic usage of the cyclic group is in the 12-hour clock system, which is based on an ordinary clock face, except 12 is replace with 0 and only a single hand, say the hour hand, is used. See figure 1.

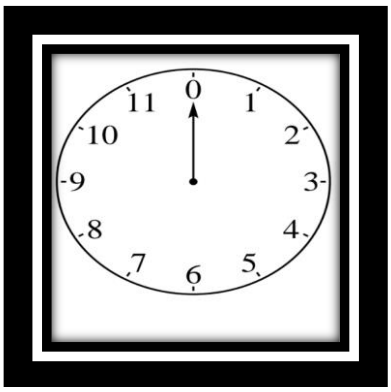


Figure 1

Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

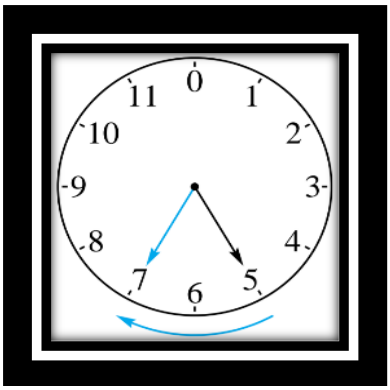
Volume-2 Issue-3 || June 2023 || PP. 250-256

https://doi.org/10.55544/jrasb.2.3.33

The clock face yields the finite set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. As on operation for this clock system, addition is defined as follows: add by moving the hour hand in a clockwise direction. For example, to add 5 and 2 on a clock, first move the hour hand to 5, as in figure 2. Then, to add 2, move the hour hand 2 more hours in a clockwise direction. The hand stop at 7, so

$$5 + 2 = 7.$$

See figure 2 for more clarification.



Plus 2 hours

$5 + 2 = 7$

Figure 2

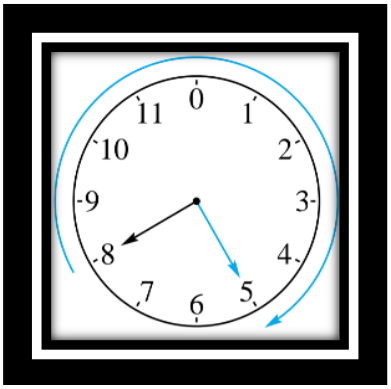
This result agrees with traditional addition. However, the sum of tow numbers from the 12- hour clock system is not always what might be expected, as the following example shows.

Example 1. Find each sum in 12-hour clock arithmetic.

(a) $8 + 9$

Move the hour hand to 8, as in figure 3. Then advance the hand clockwise through 9 more hours. It stop at 5, so

$$8 + 9 = 5.$$



Plus 9 hours

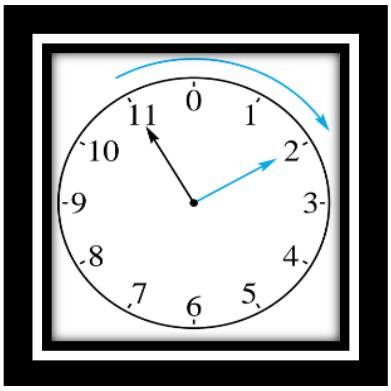
$8 + 9 = 5$

Figure 3

(b) $11 + 3$

Proceed as shown in figure 4. Check that

$$11 + 3 = 2.$$



Plus 3 hours

$11 + 3 = 2$

Figure 4

Since there are many infinitely whole numbers, it is not possible to write a complete table of addition facts for that set. Such a table, to show the sum of every possible pair of whole numbers, would have an infinite number of rows and columns, making it impossible to construct.

On the other hand, the 12-hour clock system uses only the whole numbers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ and 11. A table of all possible sums for this system requires only 12 rows and 12 columns. The 12-hour clock addition table is shown in table 1. Since the 12-hour system is built upon a finite set, it is called a finite mathematical system.

Table 1: 12-Hour Clock Addition

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

Example 2. Use the 12-hour clock addition table to find each sum.

(a) $7 + 11$

Find 7 on the left of the addition table and 11 across the top. The intersection of the row headed 7 and the column headed 11 gives the number 6. Thus, $7 + 11 = 6$.

(b) Also from the table, $11 + 1 = 0$.

So far, our 12-hour clock system consists or the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, together with the operation of clock addition. Next we will check wither this system has the closure, commutative, associative, identity, and inverses properties. These properties described in the section 1 of the article.

Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

Volume-2 Issue-3 || June 2023 || PP. 250-256

https://doi.org/10.55544/jrasb.2.3.33

Table 1 shows that the sum of tow numbers on a clock face is always a number on the clock face. That is, if a and b are any clock numbers in the set of the system, then $a + b$ is also in the set of the system. The system has the closure property. (the set of the system is closed under clock addition.)

Notice also in this system, $5 + 9$ and $9 + 5$ both yield 2. Also $7 + 11$ and $11 + 7$ both yield 6. The order in which elements are added does not seem to matter. In fact, you can see in Table 1 that the part of the table above the colored diagonal line is a mirror image of the part below diagonal line. This shows that, for any clock numbers a and b, $a + b = b + a$. The system has the commutative property.

Modular systems: We now expand this idea of clock arithmetic to modular system in general. Recall that 12-hour clock arithmetic was set of so that answers were always whole numbers less than 12. For example, $8 + 6 = 2$. The traditional sum, $8 + 6 = 14$, reflects the fact that moving the clock hand forward 8 hours from 0, and then forward another 6 hours, amounts to moving it forward 14 hours total. But since the final position of the clock is at 2, we see that 14 and 2 are, in a sense, equivalent. More formally we say that 14 and 2 are congruent modulo 12 (or congruent mod 12), which is written

$$14 \equiv 2(mod\ 12)$$

By observing clock hand movements, you can also see that, for example,

$26 \equiv 2(mo\ 12)$, $38 \equiv 2(mod\ 12)$, and so on.

In each case, the congruence is true because the difference of the tow congruent numbers is a multiple of 12:

$14 - 2 = 12 = 1 \times 12$, $26 - 2 = 24 = 2 \times 12$, $38 - 2 = 36 = 3 \times 12$. [1]

V. APPLICATION OF CYCLIC GROUP IN CHAOS THEORY

Chaos theory involves examining deterministic behavior that can fluctuate so unpredictability that it looks random. Chaos is the belief is that tiny changes to the starting conditions can result in wildly different behavior. Edward Lorenz was studying computer models and was astonished to find out that if he ran the model half way through the circulation then restart the computer program from there, would produce dramatically different results after the restart. The computer completed a large number of calculations and the tiny differences amplified into a huge discrepancy. Lorenz called this the Butterfly Effect; he told the audience that because of the sensitivity of the weather to tiny changes, a butterfly flapping its wings in the United States could theoretically cause a typhoon in China. This is why weather predictions are only accurate for a few days.

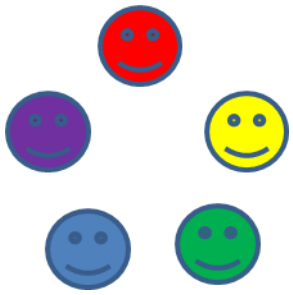


Figure 5: coin objects that can be moved around to produce a cyclic group

Even though probability may seem chaotic it can produce the same event consistently. An example would be placing 5 different color coins in a circle on a table (Figure 5), if we move a coin clockwise we would repeatedly move coins along and the first coin would visit all of the other coins. Imagine a bag containing instructions to move coins 1 through 5 along, or to leave them alone. As long as we do not pick the choice where we leave them as they are instruction we will eventually wind up with the same arrangement of the coins. What makes this work is that we have a prime number of tokens. As the number of coins increases the chance of picking leaving the coins alone goes down. With around 997 coins the chance is 1 in 1000. There for most likely we will get a move that produces a cyclic group [4].

VI. APPLICATION OF CYCLIC GROUPS IN LINEAR CODES

Verbal messages are normally converted to numerical form to electronic transmission. When computers are involved, this is usually done by means of a binary code, in which messages are expressed as strings of $0'$s and $1'$s. Such messages are easily handled because the internal processing units on most computers represent letters, numerals, and symbols in this way. The discussion her deals with such binary codes. Throughout this Paper we assume that we have a binary symmetric channel, meaning that:

1. The probability of a 0 being incorrectly received as a 1 is the same as the probability of a 1 being incorrectly received as a 0;
2. The probability of a transmission error in a single digit is less thane 5; and
3. Multiple transmission errors occur independently.

Here is a simple example that give a flavor of the paper.

Example 1. suppose that the message to be sent is a single digit, either 1 or 0. The message might be, for example, a signal to tell a satellite whether or not to orbit distant planet. With a signal-digit message, the receiver has no way to tell if on error has occurred. But suppose instead that a four-digit message is sent: 1111 for 1 or 0000 for 0. Then this code can correct single errors. For instance, if 1101 is received, then it seems likely that a

Journal for Research in Applied Sciences and Biotechnology

www.jrasb.com

ISSN: 2583-4053

Volume-2 Issue-3 || June 2023 || PP. 250-256

https://doi.org/10.55544/jrasb.2.3.33

single error has been made and that 1111 is the correct message. It is possible, of course, that three errors were made and the correct message is 0000. But this is much less likely than a single error. The code can detect double errors, but not correct them. For instance, if 1100 is received, then two errors probably have made, but the intended message isn't clear. The numerical message words (0 and 1) are translated into codewords (0000 and 1111). Only codeworeds are transmitted, but in the example any four-digit string of 0's and 1's is possible received word.

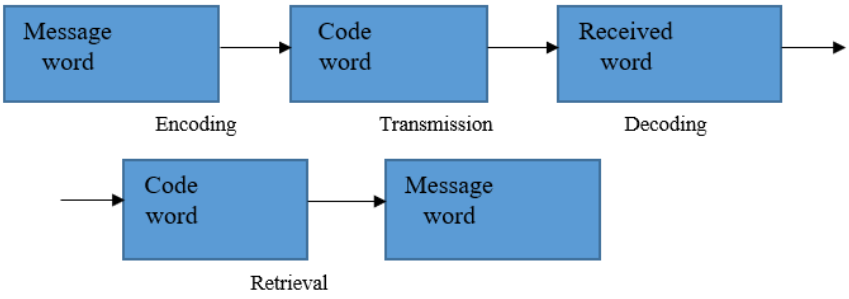
We can develop a usable definition of code in general case by considering the preceding example from a different viewpoint. If we of the message words 0 and 1 as elements of Z_2, then the received words can be considered as element of the additive group $Z_2 \times Z_2 \times Z_2 \times Z_2$ by writing $(1,0,1,1)$, for instance, as 1010 or $(0,0,0,0)$ as 0000. Addition in this group is performed coordinate wise; for example, $1010 + 1011 = 0001$(remember $1 + 1 = 0$ in Z_2). The set of codewords $C = \{0000, 1111\}$ closed under addition, so it is a subgroup of $Z_2 \times Z_2 \times Z_2 \times Z_2$. For each integer n, B^n denotes the Cartesian product.

$Z_2 \times Z_2 \times Z_2 \times \ldots \times Z_2$ of n copies of Z_2.With coordinate wise addition, $B^n$is an additive group of order 2^n. The elements of B^nwill be written as a strings of 0's and 1's of length n. If $0 < k < n$, then an (n,k) binary linear code consist of a subgroup C of $B^n$of order 2^k. For convenience, C are called codoreds. Only codewords are transmitted, but any element of B^ncan be received word.

In the preceding example, $C = \{0000, 1111\}$ is a $(4,1)$ code since C is a subgroup of order 2^1 of the group $B^4 = Z_2 \times Z_2 \times Z_2 \times Z_2$ of order 2^4 [6].

If $n \geq 2$, let $B^n = Z_2 \times Z_2 \times Z_2 \times \ldots \times Z_2$

Denote the direct product of n copies of the (additive abelian) group $Z_2 = \{0,1\}$. The elements of $B^n$are called words of length n and, for convenience, we write them as strings of 0's and 1's rather than as n -tuples. Thus, 110101 in B^6 stands for $(1,1,0,1,0,1)$. We call the individual 0's and 1's the bits of the word (an abbreviation for binary digits). A subset C of $B^n$with $|C| \geq 2$, is called an n -binary code (or simply an n-code). The words in C are called code words. We describe the general coding process in the diagram.



A set of words, called message words, is given in B^k. They are paired with a set C of longer words in B^n, $n \geq k$, which will be transmitted. Thus C is an n-code, and the process of passing from a message to the corresponding code word is called encoding. Only code words are transmitted but, as some bits may be altered during transmission, words other than code words may be received. The sole purpose of the encoding process is to enable the receiver to detect errors and, if there are not too many, to correct them. The encoding and transmission processes are usually quite simple. The message words in B^k are paired with code words in B^n in such a way that passing back· and forth is easy [8].

Example 2. Consider the code $C = \{(1010), (1110), (0011)\}$ in Z_2^4. Suppose a codeword in C is transmitted and we receive the vector $r_1 = (1110)$. A quick search of C reveals that $C = (1110)$ is the codeword from which r_1 differs in the fewest positions. Hence, we would correct r_1 to c, and assume that the error in r_1 is $e = r_1 - c = (1000)$. Now, suppose a codeword in C is transmitted and we receive the vector $r_2 = (0010)$. Since two of the codewords in C differ from r_2 in only one position, we cannot uniquely correct r_2 using the nearest neighbor policy. Therefore, in this code C, we are not guaranteed to be able to uniquely correct a received vector in Z_2^4 even if the received vector contains only a single error [5].

VII. CONCLUSION

Human minds are designed for pattern recognition and we can find algebraic structures in common objects and things around us. Cyclic groups are the simplest groups that have an object that can generate the whole set. The object can generate the set by addition, multiplication, or rotations. Cyclic groups are not only common in pure mathematics, but also in patterns, shapes, music, and chaos. Cyclic groups are an imperative part of number theory used with the Chinese remainder theorem and Fermat's theorem. Knowing if a group is cyclic could help determine if there can be a way to write a group as a simple circuit. This circuit could simplify the process of generation to discover the most efficient way to generate the object for use of future applications in mathematics and elsewhere. In this paper we have worked on deferent applications of the

ISSN: 2583-4053

Volume-2 Issue-3 || June 2023 || PP. 250-256

https://doi.org/10.55544/jrasb.2.3.33

cyclic groups, such that the application of cyclic group in number theory, bell ringing, clock arithmetic and modular system, chaos theory and linear codes. In the presented research work we clarified all the matters in very simple ways and useful examples.

REFERENCES

[1] An Addison-Wesley product. Copyright 2004 Pearson Education, Inc. p. 220-224

[2] D. S. Malik, John N. Mordeson, M.K. Sen; Introduction to Abstract Algebra. Creighton University, Calcutta University; Printed in the United States of America 2007. p. 36

[3] James S. Cook; Lecture Notes for Abstract Algebra I. Liberty University, Department of Mathematics. Fall 2016. p. 40

[4] LAUREN SOMMERS; Applications of Cyclic Groups in Everyday Life: Department of Mathematics and Statistics, College of Science, Media Arts, and Technology, California State University. 2014. p. 6-20

[5] Richard E. Klima. Neil Sigmon. Ernest Stitzinger. Applications of Abstract Algebra with MAPLE. Published by CRC Press LLC. Boca Raton London New York Washington, D.C. 1999. p. 52-53.

[6] Thomas W. Hungerford. Abstract algebra an introduction. Cleveland State University. SAUNDERS COLLEGE PUBLISHING. P. 438-439

[7] W. Edwin Clark; Elementary Abstract Algebra, Department of Mathematics University of South Florida. December 23, 2001. p. 9

[8] W. Kit Nicolson. Introduction to Abstract Algebra. Fourth edition. Published by John Wiley & Sons, Inc. Hoboken, New Jersey. Published simultaneously in Canada, 2012. p. 145-146.