GROUPS AND SUBGROUPS IN CRYPTOGRAPHY

ADESHOLA, A. D.
ALIU, T.

ABSTRACT

This study looks into the Mathematical applications of groups and subgroups in cryptography through Eulier's Phi Function and Lagrange's Theorem with some definitions, theorems, illustrations and examples.

INTRODUCTION

An algebraic system in a set X together with one or two binary operations which satisfies some rules known as axioms. There are many types of algebraic systems. The most popular of them are groups. Others are semigroups, rings, fields, etc. More work has been done on groups than any other algebraic systems.

A number of its results have been applied to solve difficult problems in other area of Mathematics and Computer Science and in other subjects such as Chemistry and Physics.

On the other hands, Cryptography from the words " Crypt " meaning "Secret" and " Graph" meaning " Writing " is the science of transforming meaningful information into unintelligible text.

Groups

A group $G = (S, \oplus)$ is a set S with a binary operation $\oplus$, for which the following properties hold:

(1) Closure: For all $a, b \in S$, we have $a \oplus b \in S$.

(2) Identity: There is an element $e \in S$, called the identity of the group, such that $e \oplus a = a \oplus e = a$, for all $a \in S$.

(3) Associativity: For all elements $a, b, c \in S$, we have $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

ADESHOLE, A. D. and **ALIU, T.** are Lecturers in the Department of Mathematics, Kwara State Univeristy, Maete, Nigeria.

International Journal of Engineering and Technical Mathematics Vol. 2, No.1 & 2
©2009 by The Development Universal Consortia. All Rights Reserved

(4) Inverses: For each $a \in S$, there exists a unique element $b \in S$, called the inverse of a, such that $a \oplus b = b \oplus a = e$.

Definition: For $n \geq 2$, the additive group Z_n is: $S = \{0, 1, \ldots, n-1\}$– the n residues modulo n, and $\oplus$ is addition modulo n. Example: The additive group $Z_6 = (\{0, 1, 2, 3, 4, 5\}, +_6)$:

Table 1.1.1: Additive Group

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Theorem: For $n \geq 2$ the system Z_n is an abelian group.

Proof: Closure: For all $a, b \in \{0, 1, \ldots, n-1\}$,
we have $((a + b) \bmod n) \in \{0, 1, \ldots, n-1\}$.

Identity: The element 0 is the identity for addition modulo n.

Associativity: For all $a, b, c \in \{0, 1, \ldots, n-1\}$, we have

$((((a + b) \bmod n) + c) \bmod n) = ((a + ((b + c) \bmod n)) \bmod n)$.

Inverses: For all $a \in \{0, 1, \ldots, n-1\}$, we have $-a = ((n - a) \bmod n)$, since $a + (n - a) = 0 \pmod n$.

Abelian: For all $a, b \in \{0, 1, \ldots, n-1\}$, we have $((a + b) \bmod n) = ((b + a) \bmod n)$.

Definition: For $n \geq 2$, the multiplicative group Z_n^* is:
$S = \{1 \leq a \leq n-1 : \gcd(a, n) = 1\}$ relative primes to n. between 1 and n-1 $\oplus$ is multiplication modulo n.

Example: Multiplicative group $Z_{18}^* = (\{1, 5, 7, 11, 13, 17\}, *_{18})$:

$*_{18}$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	7	17	1	11	13
7	7	17	13	5	1	11
11	11	1	5	13	17	7
13	13	11	1	17	7	5
17	17	13	11	7	5	1

Table 1.1.2: Multiplicative Group

Theorem: For all $n \geq 2$, the system Z_n^* is an abelian group.

Proof: Closure: For all $\leq a, b \leq n-1$, if $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(a * b, n) = 1$ and $1 \leq ((a * b) \bmod n) \leq n-1$.

Identity: The element is the identity for multiplication modulo n, and 1 is the Z_n^* since $\gcd(1, n) = 1$.

Associativity: For all $\leq a, b, c \leq n-1$, we have

$$((((a * b) \bmod n) * c) \bmod n) = ((a * ((b * c) \bmod n)) \bmod n).$$

Inverses: For all $1 \leq a \leq n-1$, if $\gcd(a, n) = 1$ then there exist integers x and y, Such that $ax + ny = 1$ This implies $ax = 1 \pmod n$, which means that $x = a^{-1} \pmod n$.

Abelian: For all $\leq a, b \leq n-1$, we have $((a * b) \bmod n) = ((b * a) \bmod n)$.

Sub group

If $(S, \oplus)$ is a group, if $S' \subseteq S$, and if $(S', \oplus)$ is also a group, then $(S', \oplus)$ is a sub-group of $(S, \oplus)$.

Examples: The even integers with addition are a subgroup of the integers with addition.

Theorem: If $(S, \oplus)$ is a finite group and S' is a non-empty subset of S, such that for all $a, b \in S'$ we have $a \oplus b \in S'$, then $(S', \oplus)$ is a subgroup of $(S, \oplus)$.

Examples: The set $\{0, 2, 4, 6\}$ forms a subset of Z_8 that is, closed under operation $+_6$ and is therefore a subgroup of Z_8.

Euler's Phi Function: The size of Z_n^* is:

$$\Phi(n) = n \prod_{p|n} (1 - (1/p))$$

Where:

P runs over all the primes that divide

Examples:

$\Phi(7) = 7 * (1 - (1/7)) = 6$ and $Z_7^* = \{1, 2, 3, 4, 5, 6\}$

$\Phi(10) = 10 * (1 - (1/2)) * (1 - (1/5)) = 4$ and $Z_{10}^* = \{1, 3, 7, 9\}$

$\Phi(18) = 18 * (1 - (1/2)) * (1 - (1/3)) = 6$ and $Z_{18}^* = \{1, 5, 7, 11, 13, 17\}$.

Lagrange's Theorem

If $(S, \oplus)$ is a finite group, and if $(S', \oplus)$ is a subgroup $(S, \oplus)$, of then $|S'|$ is a divisor of $|S|$.

A subgroup S' of group S is said to be a proper subgroup of if $S' = S$.

Corollary:

If S' is a proper subgroup of a finite group S then $|S'| \leq |S|/2$.

If $(S, \oplus)$ is a group, and if $a \in S$, we denote successive applications of the group operator $\oplus$ to a by $a^{(k)}$, then $< a > = \{a^{(k)} : k \geq 1\}$.

Lemma: If $(S, \oplus)$ is a finite group, and if $a \in S$, then $< a >$ is a subgroup of S.

Proof: $< a >$ is closed under the operator $\oplus$.

Definition: If $(S, \oplus)$ is a group, and if $a \in S$, then the subgroup generated by successive applications of $\oplus$ to is called the subgroup generated by a and is denoted by $< a >$. The element a is called the generator of $< a >$.

Definition: For all finite group $(S, \oplus)$, the order of element $a \in S$, denoted by $ord(a)$, is the smallest k, such that $a^{(k)} = e$ (the identity element).

Theorem: For any finite group $(S, \oplus)$ and any element $a \in S$, the order of a is equal to the size $< a >$, of that is $ord(a) = |< a >|$.

Proof: If $ord(a) = k$, then for all $t \geq 0$, we have $a^{(k+t)} = a^{(t)}$ $(since\ a^{(k)} = e)$. This implies that $|< a >| \leq k = ord(a)$. If $k = ord(a) > |< a >|$, then there are $1 \leq i < j \leq k$, such that $a^{(i)} = a^{(j)}$, but $i, j < k$ is contradiction. Thus, $ord(a) \leq |< a >|$.

RESULTS AND DISCUSSION

Let: Q be the set of rational numbers. Define $G = \{(a, b) \mid a, b \in Q, a \neq 0\}$, Also define a composition $*$ on G by $(a, b) * (c, d) = (ac, ad + b)$, then $< G, * >$ forms a non-abelian group.

Proof:

Let: $(a, b), (c, d) \in G$ be any two elements. Then $a \neq 0, \ c \neq 0.$

Now: $(a, b) * (c, d) = (ac, ad + b) \in G$

As $a, c \neq 0 \Rightarrow ac \neq 0.$ and also ac and $ad + b$ belong to Q whenever $a, b, c, d \in Q$

Hence closure holds.

Associativity: Let $(a, b), (c, d), (e, f)$ be any three members of $G.$

Then:

$$[(a, b) * (c, d)] * (e, f) = (ac, ad + b) * (e, f) \quad a, c, e \neq 0$$

$$= (ace, acf + ad + b) \quad (a, b) * [(c, d) * (e, f)] = (a, b) * (ce, cf + d)$$

$$= (ace, a(cf + d) + b)$$

$$= (ace, acf + ad + b)$$

$\Rightarrow$ Associativity holds. Existence of identity. We observe

$(a, b) * (1, 0) = (a, a \cdot 0 + b) = (a, b) = (1, 0) * (a, b) \quad \forall (a, b) \in G$

$\Rightarrow (1, 0) \in G$ is the identity.

Existence of inverse. If $(a, b) \in G$ be any element then $(c, d) \in G$ will be inverse of (a, b) if $(a, b) * (c, d) = (c, d) * (a, b) = (1, 0)$

Now $(a, b) * (c, d) = (1, 0)$

$$\Leftrightarrow (ac, ad + b) = (1, 0)$$

$$ac = 1 \text{ and } ad + b = 0$$

$$c = \frac{1}{a} \text{ and } d = -\frac{b}{a} \quad a \neq 0$$

Since $a \neq 0$, we can talk of $\frac{1}{a}$ clearly then $\left(\frac{1}{a}, -\frac{b}{a}\right)$ is the inverse of $(a, b).$

Hence $< G, *$ is a group. To show that it is not abelian, let us consider the elements $(2, 3), (1, 4) \in G.$

Now:

$$(2, 3) * (1, 4) = (2 \times 1, 8 + 3) = (2, 11) \text{ and}$$

$$(1, 4) * (2, 3) = (1 \times 2, 3 + 4) = (2, 7)$$

Since $(2, 11) \neq (2, 7)$, then we conclude that $< G, * >$ is not abelian.

Illustrations:

In the additive group Z_6, we have:

$$<0> = \{0\},$$

$$<1> = <5> = \{0, 1, 2, 3, 4, 5\},$$

$$<2> = <4> = \{0, 2, 4\},$$

$$<3> = \{0, 3\}$$

In the multiplicative group Z_7^*, we have:

$$<1> = \{1\},$$

$$<2> = <4> = \{0, 2, 4\},$$

$$<3> = <5> = \{0, 1, 2, 3, 4, 5, 6\} \quad <6> = \{1, 6\}$$

CONCLUDING REMARKS

Taking cognizance of the Cryptography principle and then it can be seen that cryptography has strong scientific background supported by mathematical principles which are of interest to both mathematicians and scientists.

REFERENCES

Bruce, S. (1996). *Applied Cryptography. Protocols, Algorithms, and Source Code in C, (2nd edition).* John Wiley and Sons.

Charlie, K.; Radia, P. and **Mike, S.** (2002). *Network Security. Private Communication in a Public World,* (2nd edition). Prentice Hall.

David, N. (1998). *Penguin Dictionary of Mathematics.* England: Penguin Books Ltd.

Douglas, R. S. (2003). *Cryptography. Theory and Practice.* Chapman and Hall.

Falaki, S. O. and **Alese, B. K.** (2007). *Research Oriented Course in Cryptography and Encryption Algorithms.* National Mathematical Centre, Abuja.

Howie, J. M. (1991). *Automata and Languages.* Oxford University Press, Oxford. Joakin Von Zur, G. and Jurgen, G. *Modern Computer Algebra. Chapter 20. Makanjuola, S. O.*

William, S. (2004). *Computer Networking with Internet Protocols and Technology.*

William, S. (2003). *Cryptography and Network Security:* Principles and Practice, (3rd edition). Prentice Hall.