# Some Applications Of Lagrange's Theorem In Group Theory Using Numerical Examples.

Kwasi Baah Gyamfi[1], Abraham Aidoo[1], Dickson Y. B. Annor[1]

1. *Department of Mathematics, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.*
***Email:****kwasibaahgyamfi1@gmail.com, abramkhems09@gmail.com, dbannor1111@yahoo.com*

**Abstract:** We present Lagrange's theorem and its application in group theory. We use Groups, Subgroups, Cyclic group, and Subcyclic groups, Fermat's Little theorem and the Wilson's theorem to illustrate the results.

**Mathematics Subject Classification:** 20D99
**Keywords:** Group,Subgroup, Cyclic group,Subcyclic group.

### 1.0 Introduction

Theorems are paramount because of how they can be applied in Mathematics. As such, a good theorem should contribute substantially to develop new ideas. We want to introduce the single most important theorem in finite group theory; The Lagrange theorem.

The Lagrange theorem states that the order of any subgroup of a finite group divides the order of the group itself and is equal to the number of cosets of the subgroup of the group. The Lagrange theorem is critical in analysing groups and other concepts in Mathematics and is very useful in connecting group theory and number theory because many theorems in elementary number theory and their proofs require advanced algebraic know-how.

Mamidi Sai Akash [1], presented applications of Lagranges theorem in relation to the order of the element in a finite group, the order of a group, the converse of Lagranges theorem, and the Fermats little theorem.

Domenico Cantone et al [3], reported on the computerized verification of Lagranges theorem, carried out with the proof assistant ÆtnaNova/Referee.

The Lagrange theorem has many applications but these applications are not widely known in Mathematics and hence make knowledge of the Lagrange theorem nominal and sometimes underappreciated.

This piece of work sees to give a methodological presentation on the various applications of the Lagrange theorem and some numerical examples are presented.

### 2.0 Preliminaries

In this section we give some supporting theorems and their proofs.

### 2.3 Theorem

Let $G$ be a group. A nonempty subset $H$ of $G$ is a subgroup of $G$ if and only if either of the following holds;

a. For all $a, b \in H$, $ab \in H$ and $a^{-1} \in H$.

b. For all $a, b \in H$, $ab^{-1} \in H$.

**Proof:**

If H is a subgroup, (1) and (2) are obviously true. Conversely, suppose H satisfies (i). Then for any $a \in H$, $a^{-1} \in H$. Hence,$e = aa^{-1} \in H$. Therefore, H is a subgroup. Next, suppose that H satisfies (ii). Let $a, b \in H$, Then $e = bb^{-1} \in H$. Hence $b^{-1} = eb^{-1} \in H$. Therefore $a(b^{-1})^{-1}$ . Hence H is a subgroup of G.

### 2.4 Theorem

Every cyclic group is Abelian.

**Proof:**

The elements of cyclic groups are of the form $a^i$. Commutativity amounts to proving that

$a^i a^j = a^j a^i$.

$a^i a^j = a^{i+j}$

$= a^{j+i}$ addition of integers is commutative

$= a^j a^i$

### 2.5 Fundamental Theorem

Every subgroup of a cyclic group is cyclic.

**Proof:** See [2] for proof.

### 2.6 Lagrange's Theorem

Let $G$ be a finite group, and $H$ any subgroup of $G$. The order of $G$ is a multiple of the order of $H$. Thus the order of H divides the order of $G$.

**Proof:**

Suppose that $G$ has order n and that $H$ has order $m$. We prove that $m$ divides $n$. Since the cosets of $H$ partition $G$, each element of $G$ lies in exactly one coset. Let the number of distinct cosets be $k$. Each coset has exactly $m$ elements, the same number as $H$. Thus, as each of the $k$ cosets has $m$ elements, there are $km$ elements in all. Therefore, $n = km$, and $m$ divides $n$.

### 2.7 Theorem

If p is a prime and $gcd(a, p) = 1$, then $a^{p-1} \equiv 1(modp)$. In the notation of modular arithmetic, this is expressed as, if $a = 2$ and $p = 7$, $2^7 = 128$, and $128 - 2 = 7 \times 18$ is an integer multiple of 7.

**Proof:**

Let $S = \{a \mid a^p \equiv a(modp)\}$ for $p$ prime and $a \in N$. Then $0 \in S$ because $0^p = 0$ for all $p$ so $0^p \equiv 0(modp)$. Now assume $k \in S$ and $k^p \equiv k(modp)$.We want to show that for $k+1 \in S$,$(k+1)^p \equiv (k+1)(modp)$. By the Binomial Theorem, $(k+1)^p = k^p + 1^p + \sum_{j=1}^{p-1} \begin{pmatrix} p \\ j \end{pmatrix} k^{p-j}$ $\equiv k + 1(modp)$.

If $gcd(a, p) = 1$, then by cancellation $a^p \equiv a(modp)$ implies $a^{p-1} \equiv 1(modp)$.If $a$ is negative,then $a \equiv r(modp)$ for some $r$, where $0 \leq r \leq p - 1$. Thus $a^p \equiv r^p \equiv r \equiv a(modp)$.

### 2.8 Theorem

If $p$ is prime, then $(p - 1)! \equiv -1(modp)$.

***Lemma:*** *Let $d = gcd(a, m)$. If $d \mid b$ , then $ax \equiv b(modm)$ has exactly $d$ solutions $(modm)$.*

**Proof:** If $p = 2$ then $(2 - 1)! = 1 \equiv -1(mod2)$ and if $p = 3$ then $(3 - 1)! = 2 \equiv -1(mod3)$ .Thus assume $p$ is a prime greater than 3. Since $(p - 1) \equiv -1(modp)$ it suffices to show that $(p-2)! \equiv 1(modp)$.By Lemma above, for each $j$ such that $1 \leq j \leq p - 1$ there exists an integer $k$ such that $1 \leq k \leq p - 1$ such that $jk \equiv 1(modp)$.If $k = j$ , then $j^2 \equiv 1(modp)$ so $j = 1$ or $j = p - 1$.Thus if $2 \leq j \leq p - 2$, then there exists an integer $k$ such that $j \neq k$ and $2 \leq k \leq p - 2$ and $jk \equiv 1(modp)$. Since there are $\frac{1}{2}(p - 3)$ such pairs, multiplying them together yields $(p - 2)! \equiv 1(modp)$. Then $(p - 1)(p - 2)! \equiv (-1)(1)(modp) \Rightarrow (p - 1)! \equiv -1(modp)$.

### 2.9 Orbit-Stabilizer Theorem

If a group G acts on a set X, then the map;
$\alpha : G/Stab(x) \to Orb(x); \quad gStab(x) \mapsto g \cdot x$
is a bijection. When G a finite group, this shows that , $|G| = |Orb_G(x)| \cdot |Stab_G(x)|$, for each $x \in X$.
**Proof:** See [4] for details.

### 3.0 Main Result

In this section we present some applications of Lagrange's theorem together with example to illustrate the results.

### 3.1 Groups and Subgroups

Let G be a group, where G = $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ Then the order of G denoted $|G| = 8$. Let H be a subgroup of G where $H = \{0, 2, 4, 6\}$ Then the order of H denoted $|H| = 4$. Hence by Lagranges theorem $|G|$ is a multiple of the $|H|$.

### 3.2 Cyclic group and Sub-cyclic group

Let G = $Z_{15} = \{1, 2, 4, 7, 8, 11, 13, 14\}$ be a cyclic group of order 8 with generator 7.
Let $H = \{1, 4, 7, 13\}$ be a subcyclic group of the cyclic group generated by $< 7 >$ of order 4.The order of $H$ divides the order of $G$.

On the other hand, let $Z_5 = \{1, 2, 3, 4\}$ be a cyclic group of order 4 with generator 2.
Let $H = \{1, 2, 4\}$ be a subcyclic group of the cyclic group generated by $< 2 >$ of order 2.
Then by lagrange's theorem, the order of $G$ is a multiple of the order of $H$.

### 3.3 Fermats Little theorem In Relation to Lagrange's theorem.

Now we look at Fermats Little theorem in relation to Lagrange theorem; by **theorem 2.7** we know that $a^{p-1} \equiv 1(modp)$ where p is a prime element.
$\Rightarrow a^{p-1} - 1 \equiv 0(modp)$ where p divides $a^{p-1} - 1$.

Let $p = 7$ and $\mathbf{a} = 2$.

Then $2^6 - 1 = (2 \times 2 \times 2 \times 2 \times 2 \times 2) - 1 = 64 - 1$ $= 63$, which is divisible by 7.
Let $(p-1)$ be our group $G$ with order $|G|$.
Since $p = 7 \Rightarrow (p-1) = 6$ which has the elements $\{1, 2, 3, 4, 5, 6\}$.
Let **a** be the subgroup with the order of $H$ defined as $\{a^0, a^1, a^2, ..., a^{p-1}\} = \{2^0, 2^1, 2^2, ..., 2^6\}$ $= \{1, 2, 4\}$. Hence $|H| = 3$.
By Lagranges theorem, $|H|$ divides $|G|$.

### 3.4 Wilsons Theorem

Let us consider the Wilsons theorem which is a consequence of Fermats little theorem. Using **theorem 2.8**, we illustrate some examples;

**Example I**

Let $p = 5$, where $p$ is a prime. Consider the elements of $Z_5^* = \{1, 2, 3, 4\}$ where $Z_5^*$ is a subgroup H of order 4.
Then by the theorem; $(p-1)! \equiv -1(mod p)$.
$\Rightarrow p|(p-1)! + 1$. But $(p-1)! + 1$ has 24 elements given by $Z_{25}^* = \{1, 2, 3, 4..., 24\}$.
Representing q by 25, $q > p$, where q is the group G of order 24 and H is a subgroup of G of order 4, hence the order of H divides the order of G. This confirms the Lagrange's theorem.

**Example II**

Let $p = 7$, where $p$ is prime. We know that the elements of $Z_7^*$ are six given by $\{1, 2, 3, 4, 5, 6\}$.
Let $H$ be a subgroup representing $Z_6^*$.
By **theorem 2.8**, $(p-1)! + 1$ has 721 elements. Hence $Z_q^* = Z_{721}^*$ has 720 elements which represents the group G.
Applying the Lagrange's theorem, the order of G is a multiple of the order of H.

### 3.5 Orbit-Stabilizer Theorem

We now look at the Orbit-Stabilizer Theorem in relation to the Lagrange's theorem. Using **theorem 2.9**, we show some examples;

**Examples:**

Consider a group $G = S_3 = \{e, (1\ 2), (1\ 3), (2\ 3),$ $(1\ 2\ 3), (1\ 3\ 2)\}$ and let it act on itself by conjugation. By the theorem 2.9 we know that, $|G| = |Orb_G(x)| \cdot |Stab_G(x)|$, where G is the group whereas $Orb_G(x)$ and $Stab_G(x)$ are the subgroups. It is easy to see that;

i) $Orb_G((1\ 2)) = \{(1\ 2), (2\ 3), (1\ 3)\}$ and $|Orb_G((1\ 2))| = 3$. Also, $Stab_G((1\ 2)) = \{e, (1\ 2)\}$ and $|Stab_G((1\ 2))| = 2$. Hence by Orbit−Stabilizer theorem, $|G| = |Orb_G((1\ 2))| \cdot |Stab_G((1\ 2))| = 3 \times 2 = 6$.
Hence by Lagrange's theorem, $|G|$ is a multiple of both $|Orb_G((1\ 2))|$ and $|Stab_G((1\ 2))|$.

ii) $Orb_G((1\ 2\ 3)) = \{(1\ 2\ 3), (1\ 3\ 2)\}$ and $|Orb_G((1\ 2\ 3))| = 2$. Also, $Stab_G((1\ 2\ 3)) = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ and $|Stab_G((1\ 2\ 3))| = 3$. Therefore by the theorem, $|G| = |Orb_G((1\ 2\ 3))| \cdot |Stab_G((1\ 2\ 3))| = 2 \times 3 = 6$.
Hence by Lagrange's theorem, both $|Orb_G((1\ 2\ 3))|$ and $|Stab_G((1\ 2\ 3))|$ divide $|G|$.

### 4.0 Conclusion

In this piece of work we have been able to give a methodological representation on some applications of Lagrange's theorem whereas practical illustrations have been exhibited using these applications which shows that the order of a subgroup divides the order of a group.

### Reference

[1]Mamidi Sai Akash(2015). Applications Of Lagrange's Theorem In Group Theory, Volume 3, PageNo.1150-1153,ISSN : 2320-7167.
.[2] W. Keith Nicholson(2007). Introduction to abstract algebra 3/E: A John Wiley and sons,Inc., Publication.
.[3] Domenico Cantone et al(2009). A certification of Lagranges theorem with the proof assistant ÆtnaNova/Referee.
.[4] T.K Carne(2012).Geometry and Groups, PageNo. 5, $https : //www.dpmms.cam.ac.uk/\ tkc$ $/GeometryandGroups/GeometryandGroups.pdf$