APPLICATIONS OF LAGRANGE'S THEOREM IN GROUP THEORY

MAMIDISAIAKASH
12TH STANDARD
FIITJEE JR COLLEGE
HYDERABAD

D.No.74-13/2-23/1A, Ramdoot Nagar, New R.T.C.Colony, Patamata,VIJAYAWADA, ANDHRA PRADESH, INDIA-520007
Email: akash.davinci@gmail.com
Mobile: 0091+7095714978

Abstract: The objective of the paper is to present applications of Lagrange's theorem, order of the element, finite group of order, converse of Lagrange's theorem, Fermats little theorem and results, we prove the first fundamental theorem for groups that have finite number of elements. In this paper we show with the example to motivate our definition and the ideas that they lead to best results. It can be used to prove Fermat's little theorem and its generalization, Euler's theorem. These special cases were known long before the general theorem was proved. In this paper some Corollaries gives the famous result called the Fermat's Little Theorem. In this paper we see that given a subgroup H of a group G, it may be possible to partition the group G into subsets that are in some sense similar to H itself

Keywords: Keywords for this paper Lagrange's theorem and converse of the Lagrange's theorem.

INTRODUCTION:

A consequence of the theorem is that the order of any element *a* of a finite group (i.e. the smallest positive integer number *k* with $a^k = e$, where *e* is the identity element of the group) divides the order of that group, since the order of *a* is equal to the order of the cyclic subgroup generated by *a*. If the group has *n* elements, it follows

$a^n = e$. we now prove that in general, the converse of Lagrange's Theorem is not true.

The theorem also shows that any group of prime order is cyclic and simple. This in turn can be used to prove Wilson's theorem, that if *p* is prime then *p* is a factor of $(p-1)! + 1$.

Lagrange's theorem can also be used to show that there are infinitely many primes: if there was a largest prime *p*, then a prime divisor *q* of the Mersenne number $2^p - 1$ would be such that the order of *p* in the multiplicative group $((\mathbb{Z}/q)\backslash 0), \cdot$ (see modular arithmetic) would divide the order of this group which is $q - 1$. Hence $p < q$, contradicting the assumption that *p* is the largest prime.[1]

DEFINITION: 1. 1.1 (Order of an Element). Let G be a group and let g ∈G. Then the smallest positive integer m such that g m = e is called the order of g. If there is no such positive integer then g is said to have infinite order. The order of an element is denoted by O(g).

Example1. 2. 1. The only element of order 1 in a group G is the identity element of G.

2. In D4, the elements r^2 , f, rf, r^2f, r^3f have order 2,

whereas the elements r and r 3 have order 4.

With the definition of the order of an element, we now prove that in general, the converse of Lagrange's Theorem is not true. To see this consider the group G discussed in Example 3.2.1.2a. This group has 12 elements and 6 divides 12. Whereas it can be shown that G doesn't have a subgroup of order 6. We give a proof for better understanding of cosets.

Proof. Let if possible, H be a subgroup of order 6 in G, where

G = {e,(234),(243),(124),(142),(123),(132),(134),(143),(12)(34),(13)(24),(14)(23)}.

Observe that G has exactly 8 elements of the form (ijk), for distinct numbers i, j and k, and each has order 3. Hence, G has exactly 8 elements of order 3. Let a $\in$ G with O(a) = 3.

Then using Theorem we see that cosets of H in G will be exactly 2 and at the same time, the possible cosets could be H, aH and a^2H (as a 3 = e, no other coset exists).

Hence, at most two of the cosets H, aH and a^2H are distinct. But, using Theorem, it can be easily verified that the equality of any two of them gives a $\in$H. Therefore, all the 8 elements of order 3 must be elements of H. That is, H must have at least 9 elements (8 elements of order 3 and one identity). This is absurd as |H| = 6.

We now prove that in general, the converse of Lagrange's Theorem is not true. The observation that for each g $\in$G, the set H = {e, g, g^2 , g^3 , . . .} forms a subgroup of any finite group G gives the proof of the next result.

Corollary1. 3.1 Let G be a finite group and let g $\in$G. Then O(g) divides |G|.

Remark1. 4.1 Corollary 3.5.3 implies that if G is a finite group of order n then the possible orders of its elements are the divisors of n. For example, if |G| = 30 then for each g $\in$G, O(g) $\in${1, 2, 3, 5, 6, 10, 15, 30}.

Let G be a finite group. Then in the first corollary, we have shown that for any g $\in$G, O(g) divides |G|. Therefore, |G| = m · O(g), for some positive integer m. Hence $g^{|G|} = g^{m\cdot O(g)} = (g^{O(g)})^m = e^m = e$.

This observation gives our next result.

1.5.1 APPLICATIONS OF LAGRANGE'S THEOREM

Corollary1. 3.2 Let G be a finite group. Then, for each g $\in$G, $g^{|G|}$ = e. Let P be an odd prime and consider the set $\mathbb{Z}_{*p}$ = {1, 2, . . . , p − 1}. Then, check that $\mathbb{Z}_{*p}$ forms a group with respect to the binary operation

a $\odot$b = the remainder, when ab is divided by p.

Applying Corollary 3.2 to $\mathbb{Z}$ ∗ p gives the famous result called the Fermat's Little Theorem. To state this, recall that for a, b $\in\mathbb{Z}$, the notation "a ≡ b (mod p)" indicates that p divides a − b.

Corollary1. 3.3. Let a be any positive integer and let p be a prime. Then a p−1 ≡ 1 (mod p),if p does not divide a. In general,a p ≡ a (mod p).

We now state without proof a generalization of the Fermat's Little Theorem, popularly known as the Euler's Theorem. to do so, let Un = {k : 1 ≤ k ≤ n, gcd(k, n) = 1}, for each positive integer n. Then Un, with binary operation

a ⊙b = the remainder, when ab is divided by n forms a group.

Also, recall that the symbol φ(n) gives the number of integers between 1 and n that are coprime to n. That is, |Un| = φ(n), for each positive integer n. Now applying Corollary 3.5.5 to Un, gives the next result.

Corollary1. 3.4 Let a, n ∈Z with n > 0. If gcd(a, n) = 1 then a φ(n) ≡ 1 (mod n).

Example1. 2.2 1. Find the unit place in the expansion of 13^{1001} .

Solution : Observe that 13 ≡ 3 (mod 10). So, $13^{1001} \equiv 3^{1001}$ (mod 10). Also, 3 ∈U10 and therefore by Corollary 3.5.5, $3^{|U10|} = 1$ (mod 10). But |U10| = 4 and 1001 = 4·250+1. Thus,

$13^{1001} \equiv 3^{1001} \equiv 3^{4\cdot 250+1} \equiv (34)^{250} \cdot 3^{1} \equiv 1 \cdot 3 \equiv 3$ (mod 10).

Lagrange's Theorem In this section, we prove the first fundamental theorem for groups that have finite number of elements. To do so, we start with the following example to motivate our definition and the ideas that they lead to.

Example 2.2.2. Consider the set R 2 = {(x, y) : x, y ∈R}. Then R 2 is an abelian group with respect to component wise addition. That is, for each (x1, y1),(x2, y2) ∈R 2 , the binary operation is defined by (x1, y1) + (x2, y2) = (x1 + x2, y1 + y2).

Check that if H is a subgroup of R 2 then H represents a line passing through (0, 0). Hence, H1 = {(x, y) ∈R 2 : y = 0}, H2 = {(x, y) ∈R 2 : x = 0} and H3 = {(x, y) ∈R 2 : y = 3x} are subgroups of R 2 . Note that H1 represents the X-axis, H2 represents the Y -axis and H3 represents a line passes through the origin and has slope 3. Fix the element (2, 3) ∈R 2 . Then 1. (2, 3) + H1 = {(2, 3) + (x, y) : y = 0} = {(2 + x, 3) : x ∈R}.

This is the equation of a line that passes through the point (2, 3) and is parallel to the X-axis. 2. verify that (2, 3) + H2 represents a line that passes through the point (2, 3) and is parallel to the Y -axisHence, the unit place in the expansion of 13^{1001} is 3. 3. (2, 3) + H3 = {(2 + x, 3 + 3x) : x ∈R} = {(x, y) ∈R 2 : y = 3x − 3}. So, this represents a line that has slope 3 and passes through the point (2, 3).

So, we see that if we fix a subgroup H of R 2 and take any point (x0, y0) ∈R 2 , then the set (x0, y0) + H gives a line that is a parallel shift of the line represented by H and (x0, y0) + H contains

the point (x0, y0). Hence, it can be easily observed that 1. (x1, y1) lies on the line (x0, y0) + H if and only if (x0, y0) + H = (x1, y1) + H. 2. for any two (x0, y0),(x1, y1) ∈R 2 , either (x0, y0) + H = (x1, y1) + H or they represent two parallel lines which themselves are parallel to the line represented by H. 3. S x∈R S y∈R (x, y) + H = R 2 . That is, if we define a relation, denoted ∼, in R 2 by (x1, y1) ∼(x2, y2), whenever (x1 − x2, y1 − y2) ∈H, then the above observations imply that this relation is an equivalence relation. Hence, as (x, y) vary over all the points of R 2 , we get a partition of R 2 .

Moreover, the equivalence class containing the point (x0, y0) is the set (x0, y0) + H. Therefore, we see that given a subgroup H of a group G, it may be possible to partition the group G into subsets that are in some sense similar to H itself. Example 2.2.2 also implies that for each g ∈G, we need to consider the set g + H, if G is an additive group or either the set gH or the set Hg, if G is a multiplicative group. So, we are led to the following definition.

Definition 2.2.3 (Left and Right Coset). Let G be a group and let H be a subgroup of G. Then for each g ∈G the set 1. gH = {gh : h ∈H} is called the left coset of H in G. 2. Hg = {hg : h ∈H} is called the right coset of H in G.

Remark 1.4.2. Since the identity element e ∈H, for each fixed g ∈G, g = ge ∈gH. Hence, we often say that gH is the left coset of H containing g. Similarly, g ∈Hg and hence Hg is said to be the right coset of H containing g.

Example 2.2.3. Consider the group D4 and let H = {e, f} and K = {e, r2} be two subgroups of D4. Then observe the following: H = {e, f} = Hf,

Hr = {r, f r} = H f r,

H r2 = {r 2 , f r2 } = H f r2 and H r3 = {r 3 , f r3 } = H f r3 . (2.1)

H = {e, f} = fH, rH = {r, rf} = rf H,

r 2 H = {r 2 , r2 f} = r 2 f H and r 3 H = {r 3 , r3 f} = r 3 f H. (2.2)

K = {e, r2 } = Kr2 = r 2K,

Kr = {r, r3 } = rK = Kr3 = r 3K Kf = {f, r2 f} = fK = K r2 f = r 2 f K and K f r = {f r, f r3 } = f r K = K f r3 = f r3 K. (2.3) .

LAGRANGE'S THEOREM From (2.1) and (2 .2), we note that in general Hg 6= gH, for each g ∈ D4, whereas from (2.3), we see that Kg = gK, for each g ∈ D4. So, there should be a way to

distinguish between these two subgroups of D4. This leads to study of normal subgroups and beyond. The interested reader can look at any standard book in abstract algebra to go further in this direction. This can be used to prove Fermat's little theorem and its generalization, Euler's theorem. These special cases were known long before the general theorem was proved.

References:

- *Algebra* by Michael Artin, ISBN 0130047635, 13-digit ISBN 978-0130047632, More info, Page 50, Points (6.10) and (6.11)
- Gallian, Joseph (2006), *Contemporary Abstract Algebra* (6th ed.), Boston: Houghton Mifflin, ISBN 978-0-618-51471-7
- Dummit, David S.; Foote, Richard M. (2004), *Abstract algebra* (3rd ed.), New York: John Wiley & Sons, ISBN 978-0-471-43334-7, MR 2286236
- Roth, Richard R. (2001), "A History of Lagrange's Theorem on Groups", *Mathematics Magazine* **74** (2): 99–108, doi:10.2307/2690624, JSTOR 2690624
- Gallian, J. A. "On the Converse of Lagrange's Theorem." *Math. Mag.* **66**, 23, 1993.
- Judith V. Grabiner, The Origins of Cauchy's Rigor in Calculus, MIT Press, Cambridge, 1981.
- June Barrow-Green, From cascades to calculus: Rolle's Theorem, In: Robson, Eleanor and Stedall, Jacqueline eds. The Oxford Handbook of the History of Mathematics, Oxford Handbooks in Mathematics, Oxford University Press, Oxford, 737-754., 2009.
- Hogan, G. T. "More on the Converse of Lagrange's Theorem." *Math. Mag.* **69**, 375-376, 1996.