Advances in Mathematics: Scientific Journal **10** (2021), no.8, 3049–3053
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.8.4

A STUDY ON THE USE OF PROBABILITY LAWS IN FINITE GROUPS

Mithun Bhadra

ABSTRACT. In this paper different lows of probability for finite groups were introduced and used for proving two important results.

(1) For any finite group G of order pq, where p and q are prime and $p > q$, there exists exactly one subgroup of order p in G.
(2) If G is a finite group of order $2p$ and $p > 2$, then G must have exactly one group of order p.

This paper also investigates the use of probability lows in finite groups problems with some other example and further investigation.

1. INTRODUCTION

The aim of this paper is to prove that for any finite group G of order pq, where p and q are prime and $p > q$, there exist exactly one subgroup of order p in G. We have seen many works for a group of order pq where $p < q$ and p, q are prime like 'An Addition Theorem for Abelian Groups of Order pq', but there is no direct theorem or result showing that a group of order pq where p and q are prime, $p > q$, has exactly one subgroup of order p. For example group of order 15 has exactly one subgroup of order 5. We can prove it using Sylow's third

2020 *Mathematics Subject Classification.*
Key words and phrases. conditional probability, finite group, order of a subgroup, relatively prime.
Submitted: 26.07.2021; *Accepted:* 10.08.2021; *Published:* 23.08.2021.

theorem [1]. In this paper we introduce a theorem which will give direct prove of that result. For the proof we use a very interesting concept of probability.

In the past 40 years, and particularly during the last two decade, there has been a growing interest in the use of probability in finite groups. It has been my experience that many pure mathematicians still look on probability theory as an "applied" subject and are dubious about the validity of using probabilistic reasoning in their own discipline. However, no-one should be uncomfortable in a discussion of the applications of probability theory to finite groups, since in these cases the probabilistic statements can be always be simply understood in terms of proportions ([2]).

Gustafson (Gustafson, 1973) and MacHale (MacHale, 1974) used this concept for finite groups and showed that the probability is less than or equal to 5/8. However, various research then have been done on this topic and more results are obtained. The probability that a random element in a group commute with another one in the same group is denoted with the following ratio:

$$P(G) = \frac{|\{(x, y) \in G \times G | xy = yx\}|}{|G|^2}.$$

It is clear that this probability is equal to one, if, and only if, the group is Abelian ([3]).

Here this ratio group G is considered as sample space and event $K = |\{(x, y) \in G \times G | xy = yx\}|$, which we can say is centre of G. We know that the centre of G is a subgroup of G. Therefore, in reference to the work of Gustafson (Gustafson, 1973) and MacHale (MacHale, 1974), we can consider a finite group G as sample space. Subgroup H of G satisfies all condition of group G and it is subset of G. Therefore we can consider H as an event of G whose every element satisfies properties of group G. Now, in reference to the above discussion, we can say that if finite group G is a sample space and subgroup H of G is an event of G, then the probability of the event H is, $P(H) = \frac{o(H)}{o(G)}$, where $o(G)$ means number of element of G and $o(H)$ means number of element of H. If K is another subgroup of G, i.e., K is another event of G whose elements satisfy all the condition of group G and probability of K and $P(K) \neq 0$. Then the conditional probability is $P(H|K) = \frac{P(H \cap K)}{P(K)}$ [4].

2. Preliminaries

In this section we give some basic definition of lows of probability and results of finite groups.

Definition 2.1. *If E and F are two events associated with the same sample space of a random experiment, then the conditional probability of the event E given that F has occurred, i.e., $P(E|F)$ is given by*

$$P(E|F) = \frac{P(E \cap F)}{P(F)} \quad \textit{provided} \quad P(F) \neq 0.$$

Lows of conditional Probability 2.2. Let E and F are two events associated with the same sample space S of a random experiment, then we have $P(E|F) = P(F|F) = 1$. We know that $P(E|F)= \frac{P(E \cap F)}{P(F)} = \frac{P(F)}{P(F)} = 1$. As $F \subset S$, $P(F|F)= \frac{P(F \cap F)}{P(F)} = \frac{P(F)}{P(F)} = 1$. Therefore, $P(E|F) = 1$ implies $E \subset F$ or $E = F$.

If H and k are finite subgroups of a group G, then $o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)}$.

3. Main Result

Theorem 3.1. *If G is finite group of order pq where p and q are prime and $p > q$, then G must have exactly one sub group of order p.*

Proof. Let G be a finite group of order pq, where p and q are prime and $p > q$. Let H and K are two subgroup of same order p, where p is prime, $O(H) = p$ and $o(K) = p$, $P(H) = P(K) = \frac{p}{pq} = \frac{1}{p}$, $o(H \cap K) = 1$ or p. But if $o(H \cap K) = 1$, then

$$o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap k)} = \frac{p \cdot p}{1} = p^2 > pq = o(G).$$

This is not possible. Therefore $o(H \cap K) = p$.

Now,

$$P(H \cap k) = \frac{p}{pq} = \frac{1}{q}$$

$$P(H|K) = \frac{P(H \cap K)}{P(K)} = \frac{\frac{1}{q}}{\frac{1}{q}} = 1.$$

Further, using properties of conditional probability, if $P(E|F) = 1$, then either $F \subset E$, or $F = E$. Therefore, $K \subset H$ or $k = H$.

When $K \subset H$ and $o(H) = o(K)$, all the element of K are in H, but H and K have same number of element. This implies that $K = H$.

Therefore, if G is finite group of order pq, where p and q are prime and $p > q$, then G must have exactly one sub group of order p. □

Example 1. *A group of order 15 will have only one sub group of order 5. Using the above theorem we can directly say that G must have exactly one subgroup of order 5. It can also be proven using Sylow's third theorem that $o(G) = 15 = 5.3$, where $5 > 3$. Let H be the subgroup of order 5. Then let suppose the number of subgroups be N_5. By Sylow's third theorem, $N_5 = 1 + 5n | o(G)$=15, where $n \in \mathbb{Z}$. There is exactly one choice of n which is 0. Therefore $N_5 = 1$. Hence, there is exactly one subgroup of order 5.*

Theorem 3.2. *If G is a group of order $2p$ and $p > 2$, then G must have exactly one group of order p.*

Proof. Let G is finite group of order $2p$, where p is odd prime and $p > 2$. Let H and K are two subgroup of order P. Then,

$$o(H) = p \quad \text{and} \quad o(K) = p$$

$$P(H) = P(K) = \frac{p}{2p} = \frac{1}{2}$$

$$o(H \cap K) = 1 \quad \text{or} \quad p.$$

But, if $o(H \cap K) = 1$, then

$$o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)} = \frac{p \cdot p}{1} = p^2 > 2p = o(G),$$

which is not possible. Therefore, $o(H \cap K) = p$. Now,

$$P(H \cap K) = \frac{p}{2p} = \frac{1}{2}$$

$$P(H|K) = \frac{P(H \cap K)}{P(K)} = \frac{\frac{1}{2}}{\frac{1}{2}} = 1.$$

Therefore, $K \subset H$ or $K = H$ (according to the previous result), and further, G must have exactly one subgroup of order P.

Hence G is a group of order $2p$ and $p > 2$, and G must have exactly one group of order p. □

4. CONCLUSION

In this paper the use of different lows of probability for finite group are investigated, and two important result are established.

1. If G is finite group of order pq, where p and q are prime and $p > q$, then G must have exactly one sub group of order p.
2. If G is a group of order $2p$ and $p > 2$, then G must have exactly one group of order p.

Further investigation can be done to extend the above theorem if we consider p as odd prime. Then by above result the group G is either cyclic [5] or Dihedral of order $2p$, where p is odd prime [6]. Therefore we can say Theorem 2 also holds for cyclic and dihedral group of order $2p$, where p is odd prime. And we know that if a result holds for cyclic group, then it also holds for Abelian group. Hence, our result also holds for Abelian group of order $2p$, where p is odd prime.

REFERENCES

[1] K.S. BROWN: *A Generalization of Sylow'Third Theorem*, Journal of Algebra, **115**(2) (1988), 414-430.

[2] J.D. DIXON: *Probabilistic Group Theory*, Carleton University, September 27, 2004.

[3] S.M.S. OMER, N.H. SARMIN, K. MORADIPOUR, A. ERFANIAN: *The Probability That an Element of a Group Fixes a Set and the Group Act on Set by Conjugation*, International Journal of Applied Mathematics and Statistics **32**(2) (2013), 111-117.

[4] G. SHAFER: *Conditional Probability*, International Statistical Review / Revue Internationale de Statistique **53**(3) (1985), 261-275.

[5] J.-X. ZHOU, Y.Q. FENG: *Edge-transitive dihedral or cyclic covers of cubic symmetric graphs of order $2p$*, Combinatorica **34** (2014), 115–128.

[6] M.P. LEE: *Integral Representations Of Dihedral groups of order $2p$*, Transactions of the American Mathematical Society **110**(2) (1964), 213-231.

DEPARTMENT OF MATHEMATICS
PRANAB JUBILEE COLLEGE
BOKAJAN, KARBI ANGLONG, ASSAM
INDIA 782480.
Email address: `lid.bhadra@gmail.com`