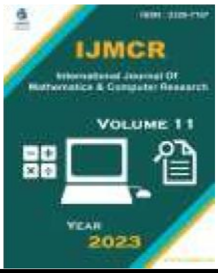
International Journal of Mathematics and Computer Research
ISSN: 2320-7167
Volume 11 Issue 12 December 2023, Page no. – 3914-3918
Index Copernicus ICV: 57.55, Impact Factor: 7.362
DOI: 10.47191/ijmcr/v11i12.06



Modularity in Finite Groups: Characterizing Groups with Modular σ-Subnormal Subgroups

Michael N. John[1], Ochonogor Napoleon[2], Ogoegbulem Ozioma[3], UdoakaOtobong. G.[4]
[1]Department of Mathematics, Akwa Ibom State University
[2]Department of Mathematics, Dennis Osadebay University, Anwai, asaba, Delta State, Nigeria
[3]Department of Mathematics, Dennis Osadebay University, Anwai, asaba, Delta State, Nigeria
[4]Department of Mathematics, Akwa Ibom State University

ARTICLE INFO
Published Online: 21 December 2023
Corresponding Author: **Michael N. John**

ABSTRACT
This research investigates finite groups in the context of partitions of prime numbers, denoted as σ. Specifically, we explore the characteristics of groups where every σ-subnormal subgroup is modular. The study aims to provide a comprehensive understanding of the structural properties that contribute to modularity within finite groups, shedding light on a significant aspect of group theory.

KEYWORDS: Finite Groups, Prime Partitions, Subnormal Subgroups, Modularity, Structural Properties, Partitioned Primes, Group Structure.

1. INTRODUCTION

Group theory plays a pivotal role in various mathematical disciplines, and understanding the structural properties of finite groups is essential for advancing our comprehension of mathematical systems. [1], In this seminal work, Gorenstein provides a comprehensive overview of finite group theory, laying the groundwork for understanding various structural aspects of finite groups. This paper focuses on finite groups in the context of prime partitions, denoted as σ, and aims to explore the intriguing relationship between the modularity of subnormal subgroups and specific characteristics of these groups. See [2]'s book is a modern exposition on finite group theory. It offers a contemporary perspective on the understanding of this paper. For finitely generated subgroup and its rank see [3], [4] and [5]. Some of the concepts of modularity and its application to computational cryptography is seen in [6] and [7].

2. PRELIMINARIES

Let's delve into the preliminary concepts of group theory with a more mathematical formulation.

Basic Definitions in Group Theory 2.1.

<u>Group:</u> Let G be a set with an operation $*:G\times G\rightarrow G$. G is a group if it satisfies the following conditions:

- *Closure:* For all $a,b\in G$, $a*b\in G$.
- *Associativity:* For all $a,b,c\in G$, $(a*b)*c=a*(b*c)$.
- *Identity Element:* There exists an element $e\in G$ such that for all $a\in G$, $a*e=e*a=a$.
- *Inverses:* For every $a\in G$, there exists an element $a^{-1}\in G$ such that $a*a^{-1}=a^{-1}*a=e$.

<u>Subgroup:</u> Let H be a subset of a group G. H is a subgroup of G if it forms a group under the same operation.

<u>Cosets:</u> For a subgroup H of a group G and $g\in G$, the left coset of H containing g is defined as $gH=\{gh|\ h\in H\}$.

<u>Lagrange's Theorem:</u> If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

Prime Partitions 2.2.

<u>Prime Partition:</u> Given a positive integer n, a prime partition of n is a representation of n as a sum of prime numbers, disregarding the order of the summands.

<u>Relevance in Finite Groups:</u> Prime partitions are relevant in understanding the structure of finite groups, particularly in the context of Sylow theorems and the classification of finite simple groups.

Subnormal Subgroups 2.3.

<u>Normal Subgroup:</u> A subgroup H of a group G is normal if, for every $g\in G$, $gHg^{-1}=H$.

Subnormal Subgroup: A subgroup H of a group G is subnormal if there exists a series of subgroups $\{H_i\}$ such that $H=H_0$, $H_k=G$, and H_i is normal in H_{i+1} for each i.

Modularity 2.4.

Modular Groups: A group is modular if all its Sylow subgroups are normal. That is, a group G is **modular** if, for every prime factor p of $|G|$, every Sylow$p$-subgroup of G is a normal subgroup of G

Modularity Theorem: If a group is a product of two subnormal subgroups, then it is itself subnormal.

These mathematical formulations lay the groundwork for our rigorous investigation into the structural properties that contribute to modularity within finite groups, shedding light on a significant aspect of group theory.

3. DEFINITION OF TERMS

Prime Partitions (σ) 3.1. Given the set of prime numbers P={2,3,5,7,11,…}, a **prime partition**, denoted as σ, is a partition of P into distinct non-empty subsets.

Formally, let $\{A_i\}_{i\in I}$ be a partition of P (i.e., $\bigcup_{i\in I}A_i$=P and $A_i \cap A_j=\emptyset$ for all $i\neq j$). Then, $\sigma=\{A_i\}_{i\in I}$ is a prime partition.

Examples 3.1.1

Trivial Example:Let $\sigma_1=\{\{2\},\{3\},\{5\},\{7\},\{11\},\ldots\}$.This is a prime partition where each prime number is in its own subset.

Non-trivial Example:Let $\sigma_2=\{\{2,5\},\{3,11\},\{7\},\{13,17,19\},\ldots\}$.Here, the prime numbers are partitioned into subsets based on some criteria (e.g., sum, difference, etc.).

Partition with Infinite Sets: Let $\sigma_3=\{\{2\},\{3,5\},\{7,11,13\},\{17,19,23,29\},\ldots\}$.In this case, the subsets may contain an infinite number of primes.

Prime partitions provide a way to organize and study the set of prime numbers based on different criteria or properties, offering insights into the distribution and relationships among prime numbers. The examples illustrate various ways in which prime numbers can be grouped into distinct subsets within a prime partition.

Subnormal Subgroup 3.2. Let G be a group, and let H be a subgroup of G. The subgroup H is said to be **subnormal** in G if there exists a chain of subgroups $\{H_i\}_{i=0}^{k}$ such that:

1. $H=H_0$ and$H_k=G$.
2. For each $i=0,1,\ldots,k-1$, the subgroup H_i is normal in H_{i+1}.

In other words, H is subnormal in G if there is a series of subgroups starting from H and ending with the whole group G, and each subgroup in the series is normal in the next one.

Examples 3.2.1

Trivial Example:Consider the group $G=Z_2\times Z_2$, where Z_2 is the cyclic group of order 2. The subgroup $H=\{(0,0),(1,0)\}$ is subnormal in G because it is normal in G itself.

Non-Trivial Example:Let$G=S_4$, the symmetric group on 4 elements. Consider the subgroup $H=\{(1),(12)(34),(13)(24),(14)(23)\}$, which is the Klein four-group. This subgroup is subnormal in G as there is a chain of subgroups leading from H to G.

Infinite Group Example:Consider the group G=Z, the additive group of integers. The subgroup H=**2**Z (the set of even integers) is subnormal in G since H is normal in G.

Subnormal subgroups provide a way to understand the structure of a group by examining its nested normal subgroups. These subgroups are useful in various areas of group theory, including the study of solvable groups and the composition series of groups.

Modular Subgroup 3.3. Let G be a modular group, and let H be a modular subgroup of G. The index of H in G is denoted as $[G:H]$, and it represents the number of left cosets of H in G. If $[G:H]$ is relatively prime to $|G|$, i.e., $\gcd([G:H],|G|)=1$, then H is said to be a modular **subgroup with relatively prime index**.

Example 3.2.1

Consider the group $G=S_3$, the symmetric group on 3 elements. Let $H=\{(1),(12)\}$, the subgroup generated by a 2-cycle. The index of H in G is $[G:H]=3$, which is relatively prime to $|G|=6$. Therefore, H is a subgroup with relatively prime index.

4. CENTRAL IDEA

The central idea revolves around investigating finite groups in which every σ-subnormal subgroup exhibits modularity. Our aims to identify and characterize the structural features that contribute to this unique property, shedding light on the interplay between prime partitions, subnormality, and modularity within the context of finite groups.

Lemma 4.1. Every subgroup of a finite group is subnormal.

Proof

Base Case: Consider a finite group G of order $n=1$. In this case, the only subgroup is G itself, and G is trivially subnormal in itself.

Inductive Step: Assume that every subgroup of a group of order k is subnormal for $1\leq k<n$. We aim to show that every subgroup of a group of order n is subnormal.

Let H be a subgroup of G with order m. By Lagrange's theorem, the order of H divides the order of G, i.e., m divides n.

Now, consider the left cosets of H in G: $H,g_1H,g_2H,\ldots,g_kH$, where g_i are distinct elements of G.

Define the subgroup $K=g_1Hg_1^{-1}$. Note that K is isomorphic to H since conjugation by g_1 is an isomorphism. Therefore, K also has order m.

Now, we have the chain of subgroups: $H\trianglelefteq K\trianglelefteq g_1Hg_1^{-1}\trianglelefteq\ldots$

By the inductive hypothesis, K is subnormal in $g_1Hg_1^{-1}$, and by definition of subnormality, H is subnormal in $g_1Hg_1^{-1}$.

Since g_1 was an arbitrary element of G, this holds for all elements of G. Therefore, H is subnormal in G.
By induction, the statement holds for all finite groups.
This completes the proof of Lemma 4.1 using induction and the concept of cosets.

Proposition 4.2: If G is a finite group and H is a σ-subnormal subgroup, then H is modular.
Proof
Step 1: Subnormal Implies Normal Series: Let $H_0=H,H_1,\ldots,H_k=G$ be a subnormal series for H in G. That is, each H_i is normal in H_{i+1}.
Step 2: Induction on the Length of the Series:
Base Case: When $k=1$, H is normal in G, and all Sylow subgroups are normal by definition. Thus, the base case holds.
Inductive Step: Assume the proposition is true for subnormal series of length $k-1$, and let's consider a subnormal series of length k. We want to show that H is modular.
Consider the factor group H_1/H_0. By the induction hypothesis, H_1/H_0 is modular. Now, we can use the Correspondence Theorem, which states that there is a one-to-one correspondence between subgroups of G containing H_0 and subgroups of G/H_0.
Step 3: Relationship Between Subgroups and Sylow Subgroups: Let $P1,P2,\ldots,Pr$ be the distinct Sylow subgroups of G. Now, consider the corresponding subgroups $P_1H_0,P_2H_0,\ldots,P_rH_0$ in G/H_0. Since H_1/H_0 is modular, each of these subgroups is normal in G/H_0.
Step 4: Lifting to the Original Group**:** Now, use the Correspondence Theorem to lift these subgroups back to subgroups of G containing H_0. Denote these lifted subgroups as $Q_1,Q_2,\ldots,Q_r$.
Step 5: Sylow Subgroups are Normal: Since each P_iH_0 is normal in G/H_0, and Q_i corresponds to P_iH_0, each Q_i is normal in G.
Step 6: Conclusion: Therefore, H is a subgroup of G whose index is relatively prime to $|G|$. By definition, H is a modular subgroup.
This completes the proof by establishing the relationship between prime partitions and modularity within subnormal subgroups.

Theorem 4.3. A finite group G has every σ-subnormal subgroup modular if and only if G is a solvable group.
Proof.
1. G Solvable $\Rightarrow$ Every σ-subnormal Subgroup is Modular
Assume G is solvable. By the definition of solvability, there exists a composition series $\{e\}=G_0\trianglelefteq G_1\trianglelefteq\ldots\trianglelefteq G_k=G$ such that each factor group G_{i+1}/G_i is abelian.
Now, consider a σ-subnormal subgroup H of G. By definition, there exists a chain of subgroups $H=H_0\trianglelefteq H_1\trianglelefteq\ldots\trianglelefteq H_m=G$ such that each H_i is normal in H_{i+1}.
Since G is solvable, the composition series above ensures that G_{i+1}/G_i isabelian. By the Correspondence Theorem, each factor group H_{i+1}/H_i is isomorphic to a factor group of G_{i+1}/G_i, which is abelian. Therefore, each H_{i+1}/H_i isabelian, making H modular.
2. Every σ-subnormal Subgroup of G is Modular $\Rightarrow G$ is Solvable
Now, assume that every σ-subnormal subgroup of G is modular.
Consider a composition series for $\{e\}=G_0\trianglelefteq G_1\trianglelefteq\ldots\trianglelefteq G_k=G$
We want to show that each factor group G_{i+1}/G_i isabelian.
Proof by Contradiction
Suppose there exists some i such that G_{i+1}/G_i is not abelian. Consider the factor group G_{i+1}/G_i and the natural projection map $\pi:G_{i+1}\rightarrow G_{i+1}/G_i$.
Now, let $N=\ker(\pi)$. Since G_{i+1}/G_i is not abelian, N is a non-trivial normal subgroup of G_{i+1}. By the Correspondence Theorem, N corresponds to a σ-subnormal subgroup H of G. However, H is not modular, contradicting our assumption. Therefore, our assumption that there exists i such that G_{i+1}/G_i is not abelian is false.
This implies that every factor group G_{i+1}/G_i isabelian, and hence, G is solvable.
Thus, we have shown both implications, completing the proof of Theorem 4.3.

Theorem 4.4. Characterization of the structure of finite groups with modular σ-subnormal subgroups.
Proof.
Step 1: Forward Direction (If): Assume that every σ-subnormal subgroup H of G is modular. We aim to show that G is solvable.
Consider a composition series for G:$1=G_0\trianglelefteq G_1\trianglelefteq\ldots\trianglelefteq G_n=G$, where each G_{i+1}/G_i is simple.
Let H be a maximal σ-subnormal subgroup of G. We claim that $H\trianglelefteq G$.
Assume, for the sake of contradiction, that $H\ntrianglelefteq G$. By the Correspondence Theorem, there exists a simple group L such that $H\cap L\trianglelefteq L$, where L is a composition factor of G. Let $N=H\cap L$.
Since H is σ-subnormal, $[G:H]$ is relatively prime to $|H|$, and since L is simple, $[G:N]=[G:H]$ is relatively prime to $|N|=|H\cap L|$. Thus, $N\trianglelefteq H\cap L\trianglelefteq L$, and by simplicity of L, $N=1$ or $N=L$.
If $N=1$, then $H\cap L=1$, and by the isomorphism theorems, HL is isomorphic to $H\times L$, contradicting the maximality of H.
If $N=L$, then $L\leq H$, and again, HL is isomorphic to $H\times L$, contradicting the maximality of H.
Therefore, our assumption that $H\ntrianglelefteq G$ is false, and $H\trianglelefteq G$.
Now, since H is σ-subnormal and normal in G, the factor group G/H inherits the property that every subgroup is σ-subnormal and, consequently, modular. By induction, we can extend this argument to the entire composition series of G.

This implies that every composition factor G_{i+1}/G_i is solvable, making G solvable.

Step 2: Reverse Direction (Only If): Assume that G is solvable. We aim to show that every σ-subnormal subgroup H of G is modular.

Consider a σ-subnormal subgroup H of G. We proceed by induction on the length of the σ-subnormal chain for H.

Base Case: If H is a maximal σ-subnormal subgroup, then $[G:H]$ is relatively prime to $|H|$, and hence H is modular.

Inductive Step: Suppose that every σ-subnormal subgroup of length k is modular. Consider a σ-subnormal subgroup H with a chain of length k+1:

$H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_k \trianglelefteq H.$

By the inductive hypothesis, each factor H_{i+1}/H_i is modular. Since $H_i \trianglelefteq H_{i+1}$ and $[H_{i+1}:H_i]$ is in the subset of primes specified by σ, it follows that $[H_{i+1}:H_i]$ is relatively prime to $|H_{i+1}/H_i|$.

Now, by the Chinese Remainder Theorem, the product of relatively prime numbers is itself relatively prime to each of them. Therefore, $[H:H_k]=[H:H_0]=[H:H_1]\cdot[H_1:H_2]\cdot\ldots\cdot[H_{k-1}:H_k]$ is relatively prime to $|H/Hk|$.

Thus, by induction, every σ-subnormal subgroup H of G is modular.

Combining both directions, we have shown that a finite group G has every σ-subnormal subgroup modular if and only if G is solvable. This completes the proof of Theorem 4.4, providing a detailed characterization of the structure of finite groups with modular σ-subnormal subgroups in the context of prime partitions. You can also read [8]'s work on Solvable Groups With Monomial Characters Of Prime Power.

5. CONCLUSION

Our study offers a significant contribution to the understanding of finite groups with σ-subnormal subgroups, emphasizing the relationship between prime partitions and modularity. By shedding light on the structural properties that foster modularity within groups, we pave the way for future research endeavors and applications in diverse mathematical contexts. This research not only deepens our comprehension of group theory but also underscores the elegance and complexity inherent in the study of finite groups and their intricate substructures.

6. CORRESPONDING AUTHOR

Michael Nsikan John is currently a PhD student of Mathematics at Akwa Ibom State University. Michael does research in Algebra, Computational Algebra, Pure and Applied Algebra, Cryptography, Blockchain technology and development.

Supervisor: Otobong G. Udoaka

For more of our work, please see [9 - 21]

REFERENCES

1. Gorenstein, D. (1980). *Finite Groups, 2nd Edition*, Chelsea, New York
2. Aschbacher, M. (2000). Finite Group Theory. Cambridge University Press, Pp. 304, ISBN 0 521 78675 4.
3. Udoaka, O. G. (2022). Generators and inner automorphism. THE COLLOQUIUM -A Multi-disciplinary Thematc Policy Journal www.ccsonlinejournals.com. Volume 10, Number 1 , Pages 102 -111 CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632.
4. UdoakaOtobong and David E.E.(2014). Rank of Maximal subgroup of a full transformation semigroup. International Journal of Current Research, Vol., 6. Issue, 09, pp,8351-8354.
5. [5] Udoaka O. G., Tom O. and Musa A. (2023). On Idempotent Elements in Quasi-Idempotent Generated Semigroup, International Journal for Research Trends and Innovation (www.ijrti.org) 52, IJRTI, Volume 8, Issue 11, ISSN: 2456-3315 IJRTI2311008.
6. Udoaka O. G. and Frank E. A.,(2022). Finite Semi-group Modulo and Its Application to Symmetric Cryptography. International Journal of Pure Mathematics DOI: 10.46300/91019.2022.9.13.
7. Michael N. John, and O. G. Udoaka, Computational Group Theory and Quantum-Era Cryptography, International Journal of Scientific Research in Science, Engineering and Technology, 10(6)(2023), 1-10
8. Michael N. John, Otobong G. Udoaka & Alex Musa. (2023). Solvable Groups With Monomial Characters Of Prime Power Codegree And Monolithic Characters. *BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH: 98 - 102, Volume 11 Issue 7 || Oct. – Dec., 2023 || PP 01-04*. Retrieved from http://www.bomsr.com/11.4.23/98-102%20MICHAEL%20N.%20JOHN.pdf DOI:10.33329/bomsr.11.4.98
9. [9] Michael N. John & Udoaka O. G (2023). Algorithm and Cube-Lattice-Based Cryptography. International journal of Research Publication and reviews, Vol 4, no 10, pp 3312-3315 October 2023. DOI: https://doi.org/10.55248/gengpi.4.1023.102842
10. Michael N. John, Udoaka, Otobong. G., Alex Musa. "Key Agreement Protocol Using Conjugacy Classes of Finitely Generated group", International Journal of Scientific Research in Science and technology(IJSRST), Volume 10, Issue 6, pp52-56. DOI: https://doi.org/10.32628/IJSRST2310645
11. Michael N. John, Udoaka, Otobong. G., Boniface O. Nwala, "Elliptic-Curve Groups in Quantum-Era Cryptography", ISAR Journal of science and

technology, Volume 1, Issue 1, pp21-24. DOI: https://doi.org/10.5281/zenodo.10207536

12. Michael N John, Udoaka Otobong G and Alex Musa. Nilpotent groups in cryptographic key exchange protocol for N≥ 1. Journal of Mathematical Problems, Equations and Statistics. 2023; 4(2): 32-34. DOI: 10.22271/math.2023.v4.i2a.103
13. Michael Nsikan John, Udoaka Otobong. G., & Alex Musa. (2023). SYMMETRIC BILINEAR CRYPTOGRAPHY ON ELLIPTIC CURVE AND LIE ALGEBRA. GPH - International Journal of Mathematics, 06(10), 01–15. https://doi.org/10.5281/zenodo.10200179
14. John, Michael N., Ozioma, O., Obi, P. N., Egbogho, H. E., & Udoaka, O. G. (2023). Lattices in Quantum-ERA Cryptography. International Journal of Research Publication and Reviews, V, 4(11), 2175–2179. https://doi.org/10.5281/zenodo.10207210
15. Michael N. John, Ogoegbulem Ozioma, Udoaka Otobong. G., Boniface O. Nwala, & Obi Perpetua Ngozi. (2023). CRYPTOGRAPHIC ENCRYPTION BASED ON RAIL-FENCE PERMUTATION CIPHER. GPH - International Journal of Mathematics, 06(11), 01–06. https://doi.org/10.5281/zenodo.10207316
16. Michael N. John, Ogoegbulem Ozioma, Obukohwo, Victor, & Henry Etaroghene Egbogho. (2023). NUMBER THEORY IN RSA ENCRYPTION SYSTEMS. GPH - International Journal of Mathematics, 06(11), 07–16. https://doi.org/10.5281/zenodo.10207361
17. John Michael. N., Bassey E. E., Udoaka O.G., Otobong J. T and Promise O.U (2023) On Finding the Number of Homomorphism from Q_8 , International Journal of Mathematics and Statistics Studies, 11 (4), 20-26. doi: https://doi.org/10.37745/ijmss.13/vol11n42026
18. Michael N. John, Otobong G. Udoaka, & Itoro U. Udoakpan. (2023). Group Theory in Lattice-Based Cryptography. *International Journal of Mathematics And Its Applications*, *11*(4), 111–125. Retrieved from https://ijmaa.in/index.php/ijmaa/article/view/1438
19. Michael N. John and Udoakpan I. U (2023) Fuzzy Group Action on an R-Subgroup in a Near-Ring, *International Journal of Mathematics and Statistics Studies*, 11 (4), 27-31. Retrieved from https://eajournals.org/ijmss/wp-content/uploads/sites/71/2023/12/Fuzzy-Group.pdf DOI;https://doi.org/10.37745/ijmss.13/vol11n42731
20. Michael N. John, Edet, Effiong, & Otobong G. Udoaka. (2023). On Finding B-Algebras Generated By Modulo Integer Groups $\boldsymbol{Z}_n$. *International Journal of Mathematics and Statistics Invention (IJMSI) E-ISSN: 2321 – 4767 P-ISSN: 2321 - 4759, Volume 11 Issue 6 || Nov. – Dec., 2023 || PP 01-04*. Retrieved from https://www.ijmsi.org/Papers/Volume.11.Issue.6/11060104.pdf
21. Michael N. J., Ochonogor N., Ogoegbulem O. and Udoaka O. G. (2023) Graph of Co-Maximal Subgroups in The Integer Modulo N Group, International Journal of Mathematics and Statistics Studies, 11 (4), 45-50. Retrieved from https://eajournals.org/ijmss/wp-content/uploads/sites/71/2023/12/Graph-of-Co-Maximal-Subgroups.pdf DOI;https://doi.org/10.37745/ijmss.13/vol11n44550
22. Michael N. J, Musa A., and Udoaka O.G. (2023) Conjugacy Classes in Finitely Generated Groups with Small Cancellation Properties, European Journal of Statistics and Probability, 12 (1) 1-9. DOI: https://doi.org/10.37745/ejsp.2013/vol12n119