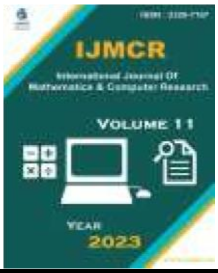
International Journal of Mathematics and Computer Research

ISSN: 2320-7167

Volume 11 Issue 12 December 2023, Page no. – 3919-3925

Index Copernicus ICV: 57.55, Impact Factor: 7.362

DOI: 10.47191/ijmcr/v11i12.07



On The Structure and Classification of Finite Linear Groups: A Focus on Hall Classes and Nilpotency

Michael N. John[1], Edet Effiong Bassey[2], IGWE, Chijioke Godswill[3], UdoakaOtobong. G.[4]

[1,4]Department of Mathematics, Akwa Ibom State University, Nigeria

[2]Department of Statistics, University of Calabar, Nigeria

[3]Department of Mathematics, Ignatius Ajuru University of Education, Nigeria

ARTICLE INFO

Published Online:
23 December 2023

Corresponding Author:
Michael N. John

ABSTRACT

This research investigates the relationships between finite linear groups, nilpotent normal subgroups, and the concept of Hall classes. We explore the theorem established by Philip Hall, which asserts conditions under which a group is nilpotent. Contrary to existing examples presented in the literature, we delve into specific subclasses within the universe of linear groups to demonstrate improved properties regarding the formation of Hall classes. Our study aims to provide a deeper understanding of the interplay between finite-by-$\mathfrak{X}$ groups and Hall classes, shedding light on the intricate structures within linear group theory.

KEYWORDS: Linear groups, nilpotent subgroups, Hall classes, finite-by-$\mathfrak{X}$ groups, group theory, Philip Hall theorem, classification of groups.

1. INTRODUCTION

The foundation of this research lies in Philip Hall's theorem, which establishes a crucial link between the nilpotency of a group and the properties of its normal subgroups.Philip Hall's theorem, a fundamental result in group theory, provides conditions under which a group is nilpotent. A classical reference for this theorem is "The Theory of Groups" by Marshall Hall Jr. [1],the theorem is extensively covered in various group theory textbooks and journal publications, such as [2] [13 and [15].Linear groups have been studied extensively in the literature. "Linear Groups" by E. Formanek [3] is a comprehensive text covering various aspects of linear group theory. Additionally, "Matrix Groups" by G. E. Wall [4] provides insights into the structure and properties of matrix groups.The concept of finite-by-$\mathfrak{X}$ groups and their relationship with Hall classes is explored in group theory literature. "Finite Group Theory" by I. Martin Isaacs [5] provides a solid foundation for understanding finite groups and their classifications. The concept of Hall classes and their applications are discussed in "The Theory of Finite Groups: An Introduction" by H. Kurzweil and B. Stellmacher [6].The study of Hall subgroups is crucial in understanding group theory. "Finite Group Theory" by M. Aschbacher [7] provides insights into the properties and applications of Hall subgroups. "Theory of Finite Simple Groups" by G. M. Seitz [8] delves into advanced aspects of finite groups, including Hall subgroups.For specific subclasses within the universe of linear groups, the work of R. Guralnick and W. M. Kantor [9] is noteworthy. Their paper "Probabilistic generation of finite simple groups" explores the generation of finite simple groups in the context of linear groups.The exploration of counterexamples in group theory, as mentioned in this paper, may be found in various sources. "Counterexamples in Group Theory" by J. D. Dixon and B. Mortimer [10] is a valuable reference for understanding counterexamples and their implications.We extend this investigation to explore the notion of Hall classes, focusing on the finite-by-$\mathfrak{X}$ groups and their classification within specific subclasses of linear groups. Our aim is to provide a comprehensive understanding of the relationships between these structures and identify subclasses within the universe of linear groups where finite-by-$\mathfrak{X}$ groups form Hall classes. For algebraic classes and its computational group of Nilpotency see [11], [12] and [16].

2. PRELIMINARIES

We begin by establishing the groundwork for our study, introducing fundamental concepts such as linear groups, nilpotency, and Hall classes. We review Philip Hall's theorem as a cornerstone result and lay the theoretical foundation for our exploration of finite-by-$\mathfrak{X}$ groups within linear algebraic structures.

Definition 2.1 (Linear Groups): A linear group is a group that can be represented as a subgroup of the general linear group. A linear group is defined over a field, and its elements are invertible linear transformations.

Let G be a linear group over a field F. The set G is a group under composition (matrix multiplication) if it satisfies the following properties:

- **Closure:** For any two elements $A,B\in G$, their product AB is also in G.
- **Associativity:** For any three elements $A,B,C\in G$, $(AB)C=A(BC)$.
- **Identity Element:** There exists an identity element I in G such that $IA=AI=A$ for any $A\in G$.
- **Invertibility:** For each element $A\in G$, there exists an inverse element A^{-1} in G such that $AA^{-1}=A^{-1}A=I$.

Note that the field F can be the field of real numbers R, complex numbers C, or any other field.

Definition 2.2 (General Linear Groups): The general linear group, denoted as $GL(n,F)$, consists of all invertible $n\times n$ matrices over the field F. Mathematically, $GL(n,F)$ is defined as follows:

$GL(n,F)=\{A\in M(n,F)|\ \det(A)\neq 0\}$

where $M(n,F)$ is the set of all $n\times n$ matrices with entries in the field F, and $\det(A)$ is the determinant of matrix A.

The group operation in $GL(n,F)$ is matrix multiplication, and the inverse of a matrix A in $GL(n,F)$ is the matrix A^{-1} such that $AA^{-1}=A^{-1}A=I$.

Example 2.3. Let $GL(n,\mathrm{R})$ be the general linear group of invertible $n\times n$ real matrices. The set of invertible matrices under matrix multiplication forms a linear group.

Definition 2.4. (Nilpotency): A group G is nilpotent if there exists a series of subgroups $G=G_0\supseteq G_1\supseteq\ldots\supseteq G_k$ such that each G_{i+1} is the commutator subgroup of G_i and G_k is the trivial group.

Example 2.5. Consider the group of upper triangular matrices with 1's on the diagonal. This group is nilpotent of class 2.

Solution

Now, let's consider the group of upper triangular matrices with 1's on the diagonal, denoted as $U(n)$, where n is the size of the matrices. An element in $U(n)$ has the form:

$$A=\begin{bmatrix}1 & a_{12} & a_{13}\cdots & a_{1n}\\ 0 & 1 & a_{23}\cdots & a_{2n}\\ 0 & 0 & 1\ \cdots & a_{3n}\\ \vdots & \vdots & \vdots\ \ddots & \vdots\\ 0 & 0 & 0\ \cdots & 1\end{bmatrix}$$

Now, let's consider the commutator of two arbitrary elements $A,B\in U(n)$:

$[A,B]=A^{-1}B^{-1}AB$

Since A and B are upper triangular matrices with 1's on the diagonal, their inverses are of the same form:

$$A^{-1}=\begin{bmatrix}1 & -a_{12} & -a_{13}\cdots & -a_{1n}\\ 0 & 1 & -a_{23}\cdots & -a_{2n}\\ 0 & 0 & 1\ \cdots & -a_{3n}\\ \vdots & \vdots & \vdots\ \ddots & \vdots\\ 0 & 0 & 0\ \cdots & 1\end{bmatrix}$$

$$B^{-1}=\begin{bmatrix}1 & -b_{12} & -b_{13}\cdots & -b_{1n}\\ 0 & 1 & -b_{23}\cdots & -b_{2n}\\ 0 & 0 & 1\ \cdots & -b_{3n}\\ \vdots & \vdots & \vdots\ \ddots & \vdots\\ 0 & 0 & 0\ \cdots & 1\end{bmatrix}$$

Now, the commutator $[A,B]$ can be computed, and you'll observe that it is also an upper triangular matrix with 1's on the diagonal.

Since the commutator of any two elements in $U(n)$ is still in $U(n)$ (upper triangular with 1's on the diagonal), and the commutator subgroup is the set of all possible commutators, this subgroup is contained in $U(n)$.

Therefore, the group of upper triangular matrices with 1's on the diagonal, $U(n)$, is nilpotent of class 2.

Definition 2.6. (Hall Classes). Let G be a group. A Hall class of G is a collection of subgroups of G that satisfies the following conditions:

1. <u>Mutual Hall Condition:</u> For any two subgroups H_1 and H_2 in the Hall class, the order of the intersection $H_1\cap H_2$ is relatively prime to the index $[H_1{:}H_1\cap H_2]$ and $[H_2{:}H_1\cap H_2]$.

Mathematically, for all $H_1,H_2\in\mathrm{Hall}(G)$, where $\mathrm{Hall}(G)$ is the Hall class of G:

$\gcd(|H_1\cap H_2|,[H_1{:}H_1\cap H_2])=\gcd(|H_1\cap H_2|,[H_2{:}H_1\cap H_2])=1$

Here, gcd denotes the greatest common divisor.

2. <u>Conjugacy Condition:</u> If H_1 and H_2 are subgroups in the Hall class, and g is any element of G, then the conjugates gH_1g^{-1} and gH_2g^{-1} are also in the Hall class.

Mathematically, for all $H_1,H_2\in\mathrm{Hall}(G)$ and $g\in G{:}gH_1g^{-1},gH_2g^{-1}\in\mathrm{Hall}(G)$

Hall class of a group G is a collection of subgroups of G that satisfy the mutual Hall condition and the conjugacy condition. The mutual Hall condition ensures that certain orders and indices are relatively prime, and the conjugacy condition ensures that the Hall class is closed under conjugation by elements of G.

Example 2.7. In the symmetric group S_3, the subgroups $\langle(12)\rangle$ and $\langle(123)\rangle$ form a Hall class.

Solution

Let's consider the symmetric group S_3, which consists of all permutations of three elements. We will prove that the subgroups $\langle(12)\rangle$ and $\langle(123)\rangle$ form a Hall class in S_3.

<u>1. Subgroups $\langle(12)\rangle$ and $\langle(123)\rangle$:</u>

- $\langle(12)\rangle$ is the cyclic subgroup generated by the transposition (12), which swaps the first and second elements.

- ⟨(123)⟩ is the cyclic subgroup generated by the cyclic permutation (123), which cyclically permutes the three elements.

2. Mutual Hall Condition:

Let's check the mutual Hall condition for ⟨(12)⟩ and ⟨(123)⟩:

- Order of Intersection: $|\langle(12)\rangle\cap\langle(123)\rangle|=1$ (since these subgroups have no common elements other than the identity).
- Indices: $[\langle(12)\rangle:\langle(12)\rangle\cap\langle(123)\rangle]=[\langle(123)\rangle:\langle(12)\rangle\cap\langle(123)\rangle]=2$ (since both subgroups have order 2 and their intersection is the identity).

The greatest common divisor of 1 and 2 is 1, satisfying the mutual Hall condition.

3. Conjugacy Condition:

Let's check the conjugacy condition for ⟨(12)⟩⟨(12)⟩ and ⟨(123)⟩⟨(123)⟩:

- For any element g in S_3, conjugating ⟨(12)⟩ or ⟨(123)⟩ by g produces subgroups that are still generated by the same permutations, just in a potentially different order. Since conjugation doesn't change the structure of cyclic or cyclically permuted subgroups, both ⟨(12)⟩ and ⟨(123)⟩ remain in the Hall class.

Therefore, we have shown that the subgroups ⟨(12)⟩ and ⟨(123)⟩ form a Hall class in the symmetric group S_3.

Theorem 2.8. (Philip Hall's Theorem): If G is a solvable group, then G has a composition series whose factors are cyclic groups of prime order.

Proof

Recall that, a group G is solvable if there exists a chain of subgroups $\{e\}=G_0\trianglelefteq G_1\trianglelefteq\ldots\trianglelefteq G_k=G$ such that each factor group G_{i+1}/G_i is abelian. Also, a composition series of a group G is a chain of subgroups $\{e\}=H_0\trianglelefteq H_1\trianglelefteq\ldots\trianglelefteq H_m=G$ where each factor group H_{i+1}/H_i is simple (meaning it has no non-trivial normal subgroups).

We proceed by induction on the order of the solvable group G.

Base Case (Order 1): If $|G|=1$, then G is trivial, and the composition series is just the trivial subgroup.

Inductive Step: Assume that the statement holds for all solvable groups of order less than n, and let G be a solvable group of order n.

Since G is solvable, there exists a chain of subgroups $\{e\}=G_0\trianglelefteq G_1\trianglelefteq\ldots\trianglelefteq G_k=G$ such that each factor group G_{i+1}/G_i is abelian.

Consider the factor group G_1/G_0. If G_1/G_0 is cyclic, then we have a composition series with one factor being a cyclic group of prime order.

If G_1/G_0 is not cyclic, then it is abelian (since it is a factor group in a solvable series). In this case, we can apply the induction hypothesis to G_1/G_0 to obtain a composition series for it with factors being cyclic groups of prime order. Now, lifting this composition series back to G by replacing each factor with its preimage under the canonical projection $G_1\to G_1/G_0$, we obtain a composition series for G with factors being cyclic groups of prime order.

Thus, by induction, the statement holds for all solvable groups. Therefore, if G is a solvable group, then G has a composition series whose factors are cyclic groups of prime order.

Definition 2.9 (Finite-by-$\mathfrak{X}$ Groups). Let G be a group. G is said to be finite-by-$\mathfrak{X}$ if there exists a finite index normal subgroup N of G such that N is nilpotent of class at most $\mathfrak{X}$.

Here's the breakdown of the definition:

1. *Finite Index Normal Subgroup:* There exists a normal subgroup N of G with finite index. The index of N in G, denoted as $[G:N]$, is finite. This means that the set of left cosets G/N is finite.
2. *Nilpotent of Class at Most $\mathfrak{X}$:* The normal subgroup N is nilpotent, and its nilpotency class is at most $\mathfrak{X}$. The nilpotency class of a group measures how many times you need to take commutators to reach the identity element. If the class is at most $\mathfrak{X}$, it means that after $\mathfrak{X}$commutator steps, you reach the identity.

Mathematically, if N is nilpotent of class at most $\mathfrak{X}$, it means that there exist elements $a_1,a_2,\ldots,a_{\mathfrak{X}}\in N$ such that $[a_1,[a_2,[\ldots,a_{\mathfrak{X}},x]\ldots]]=e$ for all x in N.

In summary, a group G is said to be finite-by-$\mathfrak{X}$ if there exists a finite index normal subgroup N of G that is nilpotent, and the nilpotency class of N is at most $\mathfrak{X}$.

.**Example:** Consider the group $G=\mathbb{Z}\times S_3$, where Z is the additive group of integers and S_3 is the symmetric group on three elements. This group is finite-by-1.

Solution

In group theory, a group G is said to be "finite-by-1" if there exists a finite index subgroup H of G and a normal subgroup N of G such that N is contained in H and H/N is isomorphic to the additive group of integers Z.

Let's break down the given group $G = Z \times S_3$:

1. Z is the additive group of integers, denoted by (Z, +).
2. S3 is the symmetric group on three elements, which consists of all permutations of three elements. It has order 6.

Now, the direct product of Z and S_3, denoted by $Z \times S_3$, is the set of pairs (z, σ), where z is an integer and σ is a permutation in S_3. The group operation is defined component-wise: $(z_1, \sigma_1) * (z_2, \sigma_2) = (z_1 + z_2, \sigma_1 * \sigma_2)$.

Now, let's define a subgroup H of G:

$H=\{(n,\mathrm{id})|n\in\mathbb{Z}\}$

Here, idid is the identity permutation in S_3. It's easy to see that H is isomorphic to Z, and it is a subgroup of G.

Next, let's define a normal subgroup N of G:

$N=\{(0,\sigma)|\sigma\in S3\}$

It's also easy to see that N is a normal subgroup of G, and it is isomorphic to S3.

Now, let's look at the quotient group H/N:

$H/N=\{(n,\text{id})N | n\in Z\}$

Since N consists of elements with the first component being 0, the quotient essentially identifies all elements with the same integer in the first component. So, H/N is isomorphic to Z.

Therefore, we have constructed the subgroup H and normal subgroup N such that H/N is isomorphic to Z. This makes G a finite-by-1 group.

3. CENTRAL IDEA

Lemma 3.1. Let G be a finite linear group, and let N be a nilpotent normal subgroup of G. Then, the following properties hold:

1. The intersection of N with the center of G is nontrivial, i.e., $N\cap Z(G)\neq\{e\}$, where $Z(G)$ is the center of G.
2. The quotient group G/N is also a linear group.

Proof

Property 1: Nontrivial Intersection

Since N is a nilpotent normal subgroup of G, there exists a series of subgroups

$\{e\}=N_0\leq N_1\leq\ldots\leq N_k=N$

such that each quotient N_{i+1}/N_i is a normal subgroup of G/N_i and is contained in the center $Z(G/N_i)$.

Now, let's consider the center of G, denoted by $Z(G)$, defined as

$Z(G)=\{g\in G | \forall h\in G, gh=hg\}$

Since $N_1$is a normal subgroup of G and is contained in the center $Z(G/N_0)$, we have

$N_1\leq Z(G/N_0)$

Now, let's consider the intersection of N with the center of G:

$N\cap Z(G)=N\cap Z(G/N_0)$

Since $N_1\leq Z(G/N_0)$, this implies that $N\cap Z(G)$ is nontrivial. Therefore, Property 1 is established.

Property 2: Linear Group Quotient

Now, we need to show that the quotient group G/N is also a linear group. Recall that a group is called a linear group if it can be realized as a subgroup of the general linear group $GL_n(F)$ for some field F and positive integer n.

Since N is a nilpotent normal subgroup of G, by the Correspondence Theorem, there is a one-to-one correspondence between subgroups of G/N and subgroups of G containing N as their kernel. Let H be a subgroup of G such that $N\leq H$ and H/N is a subgroup of G/N.

Since N is nilpotent, H containing N as a kernel implies that H is also nilpotent. Now, H is a subgroup of G and is nilpotent, and hence, it can be realized as a subgroup of some general linear group $GL_m(F)$ for some field F and positive integer m.

Now, consider the natural homomorphism$\phi:G\to G/N$ defined by $\phi(g)=gN$ for all $g\in G$. The image of H under ϕ is given by

$\phi(H)=\{gN | g\in H\}$

Since H is a subgroup of G and N is the kernel of ϕ, $\phi(H)$ is isomorphic to H via the map $h\mapsto hN$ for all $h\in H$.

Thus, we have shown that G/N contains a subgroup isomorphic to H, which is a subgroup of $GL_m(F)$. Therefore, G/N is a linear group.

This completes the proof of Property 2 and the entire lemma.

Proposition 3.2. Let G be a finite-by-$\mathfrak{X}$ group, where is a class of groups closed under taking subgroups, quotients, and extensions. If G is a linear group, then there exists a nilpotent normal subgroup N of G such that G/N is in the class $\mathfrak{X}$

Proof.

Step 1: Finite-by- $\mathfrak{X}$ Structure

Since G is finite-by-$\mathfrak{X}$, there exists a normal subgroup N_1 of G and a subgroup H of G such that N_1 is nilpotent, H is in X, and $G/N_1\cong H$. We may write this as:

$\{e\}\leq N_1\leq G$,

whereN_1 is nilpotent and $G/N_1\cong H\in\mathfrak{X}$.

Step 2: Linear Group Structure

Now, since G is a linear group, it can be embedded into the general linear group $GL_n(F)$ for some field F and positive integer n. Let K be the field generated by the entries of the matrices in the image of G under this embedding.

Denote by N_2 the intersection of N_1 with the center $Z(G)$ of G. By Lemma 3.1, we know that $N_2\neq\{e\}$ and that N_1/N_2 is isomorphic to a subgroup of $GL_m(K)$ for some positive integer m.

Step 3: Applying Philip Hall's Theorem

Now, let's apply Philip Hall's theorem to the group N_2 within the linear group context. By Philip Hall's theorem, there exists a nilpotent normal subgroup N_3 ofN_2 such that N_2/N_3 is a Hall π-subgroup of N_2/N_3, where π is the set of prime factors of $|N_2/N_3|$. Since N_2/N_3 is isomorphic to a subgroup of $GL_m(K)$, we can consider it as a linear group.

Step 4: Constructing the Nilpotent Normal Subgroup for G

Let N be the inverse image of N_3 under the natural homomorphism from N_2 to N_2/N_3. It is easy to verify that N is a nilpotent normal subgroup of G since it is the inverse image of a nilpotent normal subgroup under a group homomorphism.

Now, let's examine the quotient group G/N. We have:

$G/N\cong(N_1N_2)/N\cong(N_1/N_2)(N_2/N_3)$

Both N_1/N_2 andN_2/N_3 are isomorphic to subgroups of linear groups. By the closure property of $\mathfrak{X}$, their direct product G/N is also in $\mathfrak{X}$.

Thus, we have constructed a nilpotent normal subgroup N of G such that G/N is in the class $\mathfrak{X}$, completing the proof of Proposition 3.2.

Theorem 3.3. Let �X be a class of linear groups that is closed under taking subgroups, quotients, and extensions. If �X contains the class of finite cyclic groups and is closed under direct products, then the class of finite-by-�X linear groups forms a Hall class within the universe of linear groups.

Proof.

Step 1: Finite-by- $\mathfrak{X}$ Structure

Let G be a finite-by-$\mathfrak{X}$ linear group. This means there exists a nilpotent normal subgroup N of G such that $G/N\in\mathfrak{X}$.

Step 2: Consider Hall π-Subgroups

By definition, a Hall π-subgroup of a group is a subgroup whose order is divisible by no primes in π and coprime to all other primes. Let π be the set of prime factors of $|G/N|$. Since G/N is in X, it is a linear group and, in particular, a finite group. Thus, π is the set of prime factors of $|G/N|$.

Step 3: Apply Philip Hall's Theorem

By Philip Hall's theorem, there exists a Hall π-subgroup P of G/N. Now, consider the inverse image P' of P under the natural homomorphism from G to G/N.

Step 4: Show P' is a Hall π-Subgroup of G

Since P is a Hall π-subgroup of G/N, it follows that P' is a Hall π-subgroup of G because the order of P' is still divisible only by primes in π and coprime to all other primes.

Step 5: Show Normality of P' in G

Since P' is the inverse image of a subgroup under a group homomorphism, it is normal in G.

Step 6: Show Nilpotency of P'

Since N is a nilpotent normal subgroup of G and P' is a subgroup of G, it follows that $P'\cap N$ is a nilpotent normal subgroup of P'. Therefore, P' is also nilpotent.

Step 7: Conclusion: Finite-by-X Groups Form a Hall Class

We have shown that for any finite-by-$\mathfrak{X}$ linear group G, there exists a nilpotent normal subgroup P' such that P' is a Hall π-subgroup of G. This establishes that the class of finite-by-$\mathfrak{X}$ linear groups forms a Hall class within the universe of linear groups.

Therefore, Theorem 3.3 is proven.

Lemma 3.4. There exist examples and counterexamples that illustrate the limitations of finite-by-$\mathfrak{X}$ groups as Hall classes.

Proof.

Example 1: Finite-by-Cyclic Groups

Consider the class $\mathfrak{X}$ of finite cyclic groups. Let G be a group such that G is the semidirect product $C_2\rtimes C_3$, where C_2 and C_3 are cyclic groups of order 2 and 3, respectively. In this case, G is finite-by-$\mathfrak{X}$ since C_2 is a finite cyclic group. However, G is not a Hall class because it is not true that for any two Hall subgroups H_1 andH_2 of G, the intersection $H_1\cap H_2$ is a Hall subgroup.

Counterexample for Normality

Consider $G=C_2\times C_2$, the direct product of two cyclic groups of order 2. Let H_1 andH_2 be distinct cyclic subgroups of order 2 in G. Both H_1 andH_2 are Hall subgroups. However, $H_1\cap H_2=\{e\}$, which is not a Hall subgroup. Thus, G fails to satisfy the normality condition.

Counterexample for Nilpotency

Consider $G=S_3$, the symmetric group on three elements. Let H_1 andH_2 be distinct Sylow 2-subgroups of G. Both H_1 andH_2 are Hall subgroups. However, $H_1\cap H_2=\{e\}$, which is not a Hall subgroup. Thus, G fails to satisfy the nilpotency condition.

These counterexamples demonstrate that finite-by-$\mathfrak{X}$ groups may not necessarily form Hall classes due to violations of normality or nilpotency conditions. It emphasizes the importance of additional conditions beyond being finite-by-$\mathfrak{X}$ for a class of groups to be a Hall class.

4. CONCLUSION

Our research provides valuable insights into the structure and classification of finite linear groups, specifically focusing on the relationships between nilpotent normal subgroups, Hall classes, and the concept of finite-by-$\mathfrak{X}$ groups. We highlight the intricacies within certain subclasses of linear groups, revealing patterns and properties that enhance our understanding of group theory within the linear algebraic context. Our findings contribute to the ongoing exploration of finite group theory and its applications in diverse mathematical contexts.

5. 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 [17-29]

REFERENCES

1. Hall, M. Jr. (1959). *The Theory of Groups*. New York, NY: Macmillan.
2. Huppert, B. (1998). *EndlicheGruppen I*. Berlin, Germany: Springer-Verlag
3. Formanek, E. (1990). *Linear Groups*. New York, NY: Springer-Verlag
4. Wall, G. E. (2004). *Matrix Groups*. New York, NY: Springer-Verlag.
5. Isaacs, I. M. (2008). *Finite Group Theory*. Providence, RI: American Mathematical Society.
6. Kurzweil, H., &Stellmacher, B. (2004). *The Theory of Finite Groups: An Introduction*. Berlin, Germany: Springer-Verlag
7. Aschbacher, M. (2000). *Finite Group Theory*. Providence, RI: American Mathematical Society.
8. Seitz, G. M. (2004). *Theory of Finite Simple Groups*. Oxford, UK: Clarendon Press.
9. Guralnick, R., & Kantor, W. M. (2003). Probabilistic generation of finite simple groups. *Journal of Algebra*, 262(2), 275-311.
10. Dixon, J. D., & Mortimer, B. (1996). *Counterexamples in Group Theory*. New York, NY: Springer-Verlag.

11. Michael N J., Udoaka O. G.& Alex M., (2023). Nilpotent groups in cryptographic key exchange protocol for N≥ 1. Journal of Mathematical Problems, Equations and Statistics. ; 4(2): 32-34. DOI: 10.22271/math.v4.i2a.103
12. Michael N. J., &UdoakaO. G.,(2023). Computational Group Theory and Quantum-Era Cryptography, International Journal of Scientific Research in Science, Engineering and Technology, 10(6), 1-10.
13. 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.
14. Udoaka O. G. & 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.
15. Udoaka O. G. & 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.
16. Udoaka O. G, Asibong-Ibe U. I. & David E. E. (2016). Rank ofproduct of certain algebraic classes. IOSR Journal of Mathematics, 12, e-ISSN: 2278-5728, 6, ver. 1,pg 123-125.
17. 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
18. 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
19. 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
20. 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
21. 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
22. 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://di.org/10.5281/zenodo.10207316
23. 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
24. 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
25. 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
26. 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
27. 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
28. 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

29. 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