AGTA 2025

Francesco de Giovanni

Advances in Group Theory and Applications

In Loving Memory of Francesco

June 23th-28th 2025

Napoli

Dipartimento di Matematica e Fisica "Ennio De Giorgi"

INdAM Istituto Nazionale di Alta Matematica GNSAGA

Università degli Studi della Campania *Luigi Vanvitelli*

AGTA 2025
Francesco de Giovanni
Advances in Group Theory and Applications

Advances in Group Theory and Applications 2025

In Loving Memory of Francesco

June 23th-28th 2025
Napoli

SCIENTIFIC COMMITTEE

Maria De Falco
Carmela Musella
Alessio Russo
Salvatore Siciliano
Paola Stefanelli
Marco Trombetti

ORGANIZING COMMITTEE

Andrea Albano
Mattia Brescia
Maria Ferrara
Marzia Mazzotta
Giulia Sabatino

Foreword

Advances in Group Theory and Applications 2025 marks the ninth edition of a series of international conferences that began in 2007, initiated by Francesco de Giovanni and Francesco Catino. The focus of the series is on recent developments in group theory and its applications. In fact, the origins of this initiative trace back to the Intensive Bimester organized by the University of Napoli "Federico II" and the University of Galway, with financial support from the National Institute of Higher Mathematics (INdAM). For this reason, this year's edition can be regarded as the tenth, considering also that the 2021 edition could not be held due to the tragic global pandemic.

This edition is particularly special to us, as it is the first without its main founder, Francesco, who has left an irreplaceable void in our hearts for over a year now. He was the soul of this conference series, and while we will do our best to make him proud — in this and in future editions — we are fully aware that nothing will ever be quite the same. For this reason, we would like to permanently associate his name with this series of conferences, in loving memory of him, so that we may continue to feel his presence close to us.

The conference is also organized by the non-profit association *AGTA — Advances in Group Theory and Applications*, which was founded by Francesco. The activities of AGTA include not only the organization of conferences, but also the awarding of the *Reinhold Baer Prize*, the publication of a journal bearing the same name, the monograph series *AGTA Lost Monographs*, the *Genealogy* of group theorists, the *Group Theory Impact Factor*, and a prize for solving selected open problems in infinite group theory.

We would like to express our deep gratitude to all those who share our passion for group theory and continue to work with us for its advancement and dissemination. We wish all participants an enjoyable and inspiring conference.

The Scientific Committee

Index of talks

Main Speakers

On factorised skew left braces

Adolfo Ballester-Bolinches
Universitat de València, Spain
✉ adolfo.ballester@uv.es

The main objective of the talk is to present some results about factorisations of skew left braces through abelian subbraces. A skew left brace theoretical analog of the classical Itô's theorem about products of two abelian groups and some structural results about such factorised braces are showed.

Ordering groups and the Identity Problem

Laura Ciobanu
Heriot-Watt University, Edinburgh, UK
✉ L.Ciobanu@hw.ac.uk

To order a group means to find a total ordering of its elements that is invariant under (right, or left) multiplication.

In this talk I will explore in which groups and situations a partial order can be extended to a total order. For example, in nilpotent groups the question about extending partial to total orders is connected to the Identity Problem: this asks if the subsemigroup generated by a given finite set of group elements contains the identity element of the group. I will explain the connections between orderability, the Identity Problem, and the Word Problem in lattice-ordered groups, and present instances where these problems are decidable.

Joint work with Corentin Bodart and George Metcalfe.

Around the words

Daniele D'Angeli
Università Cusano, Rome, Italy
✉ daniele.dangeli@unicusano.it

In the relationship between Algebra and Theoretical Computer Science, it has been shown that Group Theory and Formal Language Theory have important connections that have stimulated interesting and fruitful generalizations and conjectures on the topic in recent years. This presentation intends to review some classical results that link the Group Theory and the Word Problem. Then we will proceed to discuss some new results related to the generalized word problem for groups generated by automata and to describe some combinatorial structures that fit into the context of the discussion and research on the Lehnert conjecture.

(The results presented are part of an ongoing collaboration with A. Bishop, F. Matucci, T. Nagnibeda, D. Perego, E. Rodaro)

The binary actions of simple groups

Nick Gill
The Open University, Milton Keynes, UK
✉ nick.gill@open.ac.uk

Let G be a finite group acting on a set X. Write X^k for the set of k-tuples with entries in X. Roughly speaking, the action is called binary if the action of G on X^n, for any $n \geq 2$, can be deduced from the action of G on X^2. This definition is due to the model theorist, Gregory Cherlin, and can be used to study sporadic behaviour in the universe of finite group actions.

I describe work with Pierre Guillot, Martin Liebeck, Pablo Spiga and Coen del Valle aimed at classifying the binary actions of simple groups. To this end I describe a new graph which can be defined on a conjugacy class of a group G. Connectivity properties of this graph can be used to study the binary actions of G.

Skew braces with prime multiple size

Daniel Gil–Muñoz
Università di Pisa, Italy
✉ daniel.gil-munoz@mff.cuni.cz

Skew braces are objects that are typically defined as a set with two group laws satisfying a twisted version of the distributive property. They come under the realm of group theory but admit connections with other topics such as the Yang–Baxter equation, Hopf–Galois theory or triply factorizable groups, among others. In this talk, we discuss the problem of enumerating all skew braces of size np, where n is an integer number and p is a prime number coprime with n and such that every group of order np possesses a unique normal subgroup of order p. We shall see that any such a skew brace can be described in terms of skew braces of size n and the trivial brace of size p, in connection with the theory of products of skew braces. We will derive a close formula for the number of skew braces of size np and the exact number of skew braces of size $12p$. This is a joint work with Teresa Crespo, Anna Rio and Montserrat Vela.

On a simultaneous ping-pong game

Geoffrey Janssens
Vrije Universiteit Brussel, Belgium
✉ geoffrey.janssens@vub.be

Given any field F and a finitely generated subgroup G of $\mathrm{GL}_n(F)$, the celebrated Tits alternative says that G contains either a free subgroup or it contains an abundance of relations, namely it is solvable (up to finite index). Interestingly, when it exists, Tits proof explains how to construct such a free subgroup via dynamics on some associated geometric space, a method called 'playing ping-pong'. In this talk we will first give an overview on the alternative and its developments. Thereafter we will consider a conjecture of Bekka-Cowling-de la Harpe stating: given any finite subset S of a Zariski-dense subgroup Γ in a semisimple Lie group $\mathbf{G}$, there exists a $\gamma \in \Gamma$ such that $\langle a, \gamma \rangle \cong \langle a \rangle \star \langle \gamma \rangle$ for all $a \in S$ simultaneously. Moreover, there is densely many such γ. The main aim of the talk is to present the current state of the question and recent joint work with Doryan Temmerman and François Thilmany. For instance we will explain how the problem reduces to one on conjugacy classes and representations of simple algebraic groups. If time allows, we will also present some applications to classical problems on the unit group of group rings.

Complete mappings for semigroups

Michael Kinyon
University of Denver, USA
✉ michael.kinyon@du.edu

A complete mapping of a finite magma $(M, \cdot)$ is a bijection $\alpha : M \to M$ such that the mapping $\theta : M \to M; x \mapsto x \cdot \alpha(x)$ (called an orthomorphism) is also a bijection. A complete mapping can be viewed as a permutation of the columns of the Cayley table of M such that the new diagonal contains all the elements of M exactly once. In groups, the existence of a complete mapping is equivalent to the existence of an orthogonal mate. The Hall–Paige Conjecture, which characterizes those finite groups with complete mappings, was recently resolved using the classification of finite simple groups. Complete mappings have also been extensively studied for quasigroups and latin squares.

In this talk, after a general overview and history, I will discuss complete mappings for finite semigroups, with the ultimate (and not yet attained) goal of characterizing semigroups for which complete mappings exist. A (perhaps surprising) necessary condition is (von Neumann) regularity. It turns out that we can reduce the problem to that of characterizing which Rees 0-matrix semigroups over groups have complete mappings. In the special case of Rees matrix (i.e., completely simple) semigroups over groups, we can give a complete (pun intended) characterization. In the general 0-matrix case, we can further assume that the underlying group is trivial, thus "reducing" the problem to (hard!) combinatorics, which is where it stands right now. This is joint work with João Araújo (U. Nova de Lisboa), Wolfram Bentz (U. Aberta) and Peter Cameron (St. Andrews U.)

Finite and locally finite groups containing an element with small centralizer

Evgeny Khukhro

University of Lincoln, USA

✉ ekhukhro@lincoln.ac.uk

It is proved that if a finite group G has an automorphism of order n with m fixed points, then G has a soluble subgroup whose index and Fitting height are bounded in terms of m and n. As a corollary, a problem of B. Hartley recorded in 1995 in "Kourovka Notebook" [5] by V. Belyaev is solved in the affirmative: if a locally finite group G has an element with finite centralizer, then G has a subgroup of finite index which has a finite normal series with locally nilpotent factors (with both the index of this subgroup and the length of the series bounded in terms of the order of the centralizer).

Hartley's generalization [2] of the Brower–Fowler theorem based on the classification provides reduction to the case of (locally) soluble groups. The proof essentially uses the special case of the theorem when n is a product of two prime powers considered earlier independently by Hartley [3] and the author [4] and uses a theorem of G. Busetto and E. Jabara [1] on the Fitting height of a finite soluble group with a triple factorization by Hall subgroups.

References

[1] G. Busetto, E. Jabara, *On the Fitting length of finite soluble groups I - Hall subgroups*, Arch. Math. (Basel) 106 (2016), 409-416.

[2] B. Hartley, *A general Brauer–Fowler theorem and centralizers in locally finite groups*, Pacific J. Math. 152 (1992), 101-117.

[3] B. Hartley, *Automorphisms of finite soluble groups.* Preliminary version, MIMS EPrint: 2014.52 `http://eprints.ma.man.ac.uk/2188/01/covered/MIMS_ep2014_52.pdf`.

[4] E. I. Khukhro, *On finite soluble groups with almost fixed-point-free automorphisms of non-coprime order*, Siberian Math. J. 56 (2015), 541-548.

[5] *Unsolved Problems in Group Theory. The Kourovka Notebook*, no. 13, Institute of Mathematics, Novosibirsk, 1995.

On some generalizations of normal and pronormal subgroups

Mercede Maj
Università degli Studi di Salerno, Italy
✉ mmaj@unisa.it

Let G be a group, H a subgroup of G. H is said to be near normal (near subnormal, near pronormal) in G if it is normal (subnormal, pronormal) in every proper subgroup of G containing it. Obviously every normal (subnormal, pronormal) subgroup of G is near normal (subnormal, pronormal) in G, maximal subgroups are near normal (subnormal, pronormal). Recently in [1] and [2] near subnormal subgroups have been studied, in finite simple groups. In [3], we investigated near normal (subnormal, pronormal) subgroups in finite and infinite groups. We study groups with "many" near normal (subnormal, pronormal) subgroups. In particular, we investigate finite groups with all Sylow subgroups near normal. Then we investigate groups in which near normality (near pronormality) is a transitive relation. Finally we study groups in which near normal subgroups form a sublattice of the lattice of all subgroups of G.

This is a joint work with L.A. Kurdachenko and P. Longobardi.

References

[1] R. M. Guralnick, H.P. Tong-Viet, G. Tracey, *Weakly subnormal subgroups and variations of the Baer-Suzuki theorem*, J. London Math. Soc. 111 (2025).
[2] B. Baumeister, T. C. Burness, R. M. Guralnick, *On the maximal overgroups of Sylow subgroups of finite groups*, Advances in Math. 444 (2024).
[3] L. A. Kurdachenko, P. Longobardi, M. Maj, *On some generalizations of normal and pronormal subgroups*, in preparation.

Enumeration of quandles: Part II

David Stanovský
Charles University in Prague, Czech Republic
✉ david.stanovsky@matfyz.cuni.cz

Part I focused mainly on enumeration techniques that apply to quandles in general. In Part II, we will present two techniques that apply to specific, yet important subclasses of quandles.

Binary reducts of modules over commutative rings, and affine quandles in particular, satisfy the identity $(xy)(uv) = (xu)(yv)$, called mediality. Medial quandles may not admit an affine representation, but they do admit a heterogeneous representation by a mesh of abelian groups interconnected by homomorphisms. An efficient isomorphism theorem greatly reduces brute force, and Burnside's theorem allows handling the combinatorial explosion in the largest and least structured subclass of reductive quandles. The technique allows to calculate, for instance, that there are 563753074951 medial quandles with 15 elements up to isomorphism.

Nilpotent algebraic structures, under mild universal algebraic assumptions, admit representation by central extensions, and there is a machinery to address the isomorphism problem. In the context of quandles, I will present two ideas. First, both sided latin quandles (distributive quasigroups) admit a linear representation over commutative Moufang loops, and finite commutative Moufang loops are nilpotent. Second, connected racks are central coverings of connected quandles.

Group Theory and Machine Learning: Symmetries, Equivariance, and Dimensionality Reduction

Hamid Usefi
Memorial University of Newfoundland, Canada
✉ usefi@mun.ca

This talk explores how ideas from group theory are used in machine learning. I will first discuss equivariant neural networks, which are designed to respect symmetries in data, and explain how group actions help structure these models. Then I will describe a method I developed for dimensionality reduction based on singular vectors. This method identifies important features in high-dimensional datasets and has applications in areas such as biology and medical imaging.

Enumeration of quandles: Part I

Petr Vojtěchovský
University of Denver, USA
✉ Petr.Vojtechovsky@du.edu

Quandles are the algebras of knot theory arising naturally from Reidemeister moves. Enumeration and classification of quandles relies on a number of techniques and results from group theory but often leads to open questions in group theory. I will give a general overview of enumerative results for quandles, covering the Joyce-Blackburn representation, small quandles, connected quandles and principal quandles, including Hayashi's conjecture. I will also remark on the more general problem of enumerating left-distributive groupoids.

Contributed Talks

Set-theoretic solutions of the Yang–Baxter equation associated with g-digroups

Andrea Albano

Università del Salento, Lecce, Italy

✉ andrea.albano@unisalento.it

The Yang–Baxter equation forms a fundamental topic in mathematical physics, attracting much attention on the algebraic and combinatoric side also thanks to its set-theoretic version [2].

This talk focuses on a technique that provides bijective non-degenerate solutions through generalized digroups, which are structures first introduced by Kinyon [3] and later generalized in [5]. In particular, we explore the properties of these novel solutions through the guiding structure of the *conjugation rack* associated with a g-digroup [4]. Moreover, we show that some collateral results on arbitrary bijective non-degenerate solutions naturally arise from our investigations. Based on a joint work with Paola Stefanelli.

References

[1] A. Albano, P. Stefanelli, *Generalized digroups, di-skew braces and solutions of the set-theoretic Yang-Baxter equation*, preprint arXiv.2505.15387.

[2] V. G. Drinfeld, *On some unsolved problems in quantum group theory*, in Quantum groups, Lecture Notes in Math. 1510 (1990), 1-8.

[3] M. K. Kinyon, *Leibniz algebras, Lie racks, and digroups*, J. Lie Theory 17 (2007), 99-114.

[4] G. G. Restrepo-Sanchez, J. G. Rodríguez-Nieto, O. P. Salazar-Díaz, R. Velásquez, *A correspondence between racks and g-digroups*, Ricerche Mat. (2024), 1–22.

[5] O. Salazar-Díaz, R. Velásquez, L. Wills-Toro, *Generalized digroups*, Comm. Algebra 44 (2016), 2760–2785.

Generalizations of Totally Imprimitive Permutation Groups

Rümeysa Sacide Altınkaya
Gazi University, Turkey
✉ rsgolcu@gazi.edu.tr

Let G be a group acting on an infinite set Ω. The support of x in G is defined by $\text{supp}(x) = \{\alpha \in \Omega \mid \alpha^x \neq \alpha\}$. If $\text{supp}(x)$ is finite for all $x \in G$, then G is called a finitary permutation group on Ω. Totally imprimitive subgroups of finitary permutation groups are defined by Peter M. Neumann in [2].

Let G be a transitive finitary permutation group on an infinite set Ω. If G has no maximal G-block, that is, if G has an ascending family of finite G-blocks

$$\Delta_0 \subset \Delta_1 \subset \Delta_2 \subset \dots$$

such that $\Omega = \bigcup_{i \in \omega} \Delta_i$, then G is called totally imprimitive permutation group [1].

We aim to obtain for subgroups of symmetric groups the results obtained for totally imprimitive subgroups of finite symmetric groups. We define the support-block property for symmetric groups. Let G be a transitive permutation group on an infinite set Ω. We say that G satisfies the support-block property ($\mathcal{SBP}$) if for every finitely generated subgroup F of G, there is a proper G-block Δ (i.e. $\Delta \neq \Omega$) such that

$$\text{supp}(F) \subseteq \Delta \,.$$

Consequently, we can generalize some of Neumann's results on totally imprimitive groups given in [2] and [3] for symmetric groups with support-block property.

References
[1] J. D. Dixon, Brian Mortimer, *Permutation Groups*, Springer 163 (1996).
[2] P. M. Neumann, *The lawlessness of groups of finitary permutations*, Arch. Math. 26 (1975), 561-566.
[3] P. M. Neumann, *The structure of finitary permutation groups*, Arch. Math. 27 (1976) 3-17.

Infinitely supported groups

Ahmet Arikan
Gazi University, Turkey
✉ arikan@gazi.edu.tr

Let G be an infinite group and X be an infinite set of generators of G. If every infinite subset of X also generates G, then we call G an *infinitely supported group* (**IS**-*group for short*) *by* X. In the present talk, we investigate main properties of such groups, especially in the abelian case.

We give some examples in the non-abelian case. We see that some celebrated constructions of groups are infinitely supported such as Čarin's groups with *min*-n, Ol'shanskiĭ's and Obraztsov's constructions, Heineken-Mohamed type groups and non-perfect minimal non-**FC**-groups.

Influence of vanishing conjugacy class on group structure

Sonakshee Arora
Indian Institute of Technology, Jammu, India
✉ sonakshee.arora@iitjammu.ac.in

The character table of a group (over $\mathbb{C}$) contains arithmetic information of representations of the group. It is widely used in the study of structure of groups, for example in the classification of finite simple groups and in Burnside's $p^m q^n$-theorem.

The aim of this talk is to show in one direction the influence of character table on the group structure. In brief, an element $x \in G$ is said to be *vanishing* if $\chi(x) = 0$ for some irreducible character χ of G (over $\mathbb{C}$); in this case, the conjugacy class of x is called a *vanishing conjugacy class*. I will summarize the progress on the influence of vanishing conjugacy classes on the structure of group (by others) and my current work (with some new questions).

This is a joint work with Rahul Kitture.

Cohomology and extensions of relative Rota–Baxter groups

Pragya Belwal
Indian Institute of Science Education and Research, Mohali, India
✉ pragyabelwal.math@gmail.com

Relative Rota–Baxter groups are generalisations of Rota–Baxter groups and are known to be intimately related to skew left braces, which, in turn, are a rich source to yield bijective non-degenerate solutions to the Yang–Baxter equation. In this talk, we see an extension theory of relative Rota–Baxter groups and introduce their low dimensional cohomology groups. We also observe the connections between this cohomology and the cohomology of associated skew left braces. We see that for bijective relative Rota–Baxter groups, the two cohomologies agree in dimension two.

Uncountable groups whose proper large subgroups have a permutability transitive relation

Martina Capasso
Università degli Studi di Napoli “Federico II”, Italy
✉ martina.capasso2@unina.it

A subgroup H of a group G is said to be *permutable in* G if $HK = KH$ for every subgroup K of G. Permutability is not in general a transitive relation, and a group G is called a PT*-group* if, whenever K is a permutable subgroup of G and H is a permutable subgroup of K, then H is permutable in G.

In a long series of papers, it has been shown that the structure of an uncountable group of cardinality $\aleph$ is strongly influenced by the behaviour of its proper subgroups of cardinality $\aleph$, at least within a suitable universe of generalized soluble groups.

In this talk, we are going to explore the behaviour of uncountable (generalized) soluble groups of regular cardinality $\aleph$ whose proper subgroups of cardinality $\aleph$ have the PT-property.

Groups with Finiteness Conditions on commutator subgroups

Rosa Cascella
Università degli Studi di Napoli “Federico II”, Italy
✉ rosa.cascella@unina.it

A finiteness condition is a group theoretical property satisfied by every finite group. In many cases, the imposition of a finiteness condition produces strong restrictions on the structure of a group. Here, the structure of groups with some finiteness conditions on commutators is investigated. More precisely, we shall say that a group G has the property $\bar{\mathcal{K}}$ if the set $\{[X, H] \mid H \leq G\}$ is finite for each subgroup X of G. We will prove that within the class of locally (soluble-by-finite) groups, the property $\bar{\mathcal{K}}$ is equivalent to the finiteness of the derived subgroup.

A group G will be said to have the more general property $\bar{\mathcal{K}}_\infty$ if the following set $\{[X, H] \,|\, H \leq G,\ H \text{ is infinite}\}$ is finite for each subgroup X of G. We will show that $\bar{\mathcal{K}}_\infty$-groups with infinite derived subgroup have a very restricted structure.

Analyzing indecomposable involutive set-theoretic solutions to the Yang-Baxter equation through the displacement group

Marco Castelli
Università del Salento, Lecce, Italy
✉ marco.castelli@unisalento.it

In 1992, Drinfeld addressed the study of the Yang-Baxter equation to its set-theoretical version. Following the seminal papers of Gateva-Ivanova and Van den Bergh, and of Etingof, Schedler, and Soloviev, many mathematicians have investigated the so-called involutive set-theoretic solutions, with particular focus on the indecomposable ones, which can be seen as fundamental building blocks. Numerous results have been obtained by analyzing the action of the associated permutation group and of a specific subgroup known as the displacement group. In this talk, we will present some structural results concerning indecomposable involutive solutions in which the displacement group plays a central role.

Rational Representations and Rational Group Algebras of Metacyclic p-Groups

Ram Karan Choudhary
Indian Institute of Technology, Bhubaneswar
✉ rc13@iitbbs.ac.in

In this talk, we present a combinatorial formula for the Wedderburn decomposition of rational group algebras of metacyclic p-groups. Additionally, we provide a combinatorial method to determine the number of irreducible rational representations of distinct degrees of these groups. Furthermore, we describe an algorithm for constructing all inequivalent irreducible rational matrix representations of metacyclic p-groups.

Hopf-Galois Structures on Parallel Extensions

Andrew Darlington
Vrije Universiteit Brussel, Belgium
✉ andrew.darlington@vub.be

Hopf-Galois theory allows for a Galois-theoretic approach to studying potentially non-Galois field extensions L/K by studying situations in which Hopf algebras act on L/K in a way that mimics the Galois group. Given a separable but non-normal field extension L/K of degree n with normal closure E, there may be other degree n sub-extensions L'/K of L/K (we say that L'/K is parallel to L/K) which can be related to L/K in many different ways. It is then an interesting question to ask whether, given an extension L/K admitting a Hopf-Galois structure, can we say anything about the Hopf-Galois structures on all of the extensions L'/K parallel to L/K? This talk will take a first look at answering this question, approaching the problem from a group-theoretical perspective, outlining some interesting results along the way.

Dedekind skew braces

Massimiliano Di Matteo
Università della Campania "Luigi Vanvitelli", Caserta, Italy
✉ massimiliano.dimatteo@unicampania.it

In 2024, A. Ballester-Bolinches, R. Esteban-Romero, L.A. Kurdachenko and V. Pérez-Calabuig have introduced the class of Dedekind braces, defined as braces in which every subbrace is an ideal, and focusing their work on the finite case. We have extended this class to the more general setting of skew braces, improving the known results and also extending some of them to the infinite case.

The Pseudocentre of a Group

Bernardo Giuseppe Di Siena
Università degli Studi di Napoli “Federico II”, Italy
🖂

In 1973, Jim Weigold [1] introduced a new characteristic subgroup of a group G, called the pseudocentre $P(G)$, defined as the intersection of the normal closures of the centralizers of its elements. In his work, he proved that the pseudocentre of every non-trivial finite group is non-trivial, and observed that it appears to have no clear connection with other canonical subgroups. In this paper, jointly written with M. Brescia, E. Ingrosso, and M. Trombetti, we investigate the structural properties of the pseudocentre. We show that the pseudocentre of a group is significantly influenced by the commutator subgroup. Moreover, we demonstrate that if a group coincides with its pseudocentre, then imposing certain generalized solubility or generalized nilpotency conditions forces the group to be abelian. Finally, through a variety of examples, we highlight how difficult is to determine the nature of the pseudocentre of a group, even the fact that it is trivial or not.

References

[1] J. Weigold:, *“Pseudonilpotent groups”*, J. Austral. Math. Soc. 18 (1973), 468–469.

Steiner loops

Ágota Figula
University of Debrecen, Hungary
🖂 figula@science.unideb.hu

Steiner triple systems ($STSs$) are block designs consisting of a set S of elements and a family T of 3-subsets of S, called triples, with the property that every 2-subset of S occurs in exactly one triple of T. Basic examples of STSs include the point-line geometry of any affine space over $GF(3)$ or of any projective space over $GF(2)$. To any STS one can associate two different commutative loops, the so-called Steiner loop of projective or affine type ([1], [2]). Steiner loops of affine type, respectively projective type behave to elementary abelian 3-groups, respectively 2-groups, as STSs behave to affine geometries over $GF(3)$, respectively to projective geometry over $GF(2)$. In the talk we wish to investigate algebraic and geometric properties of these loops in connection to configurations and study their multiplication group [5], [6]. Currently, a general extension theory for loops does not exist. The lack of associativity makes the situation less controllable and different from the theory of group extensions. Many authors have contributed to this field, working on specific kinds of extensions for some classes of loops. Examples include nuclear extensions [4], [8], [9], Schreier extensions [10], Chein's extensions for Moufang loops [2], doubling construction of “products” of Steiner triple systems [3]. We wish to report about extensions for Steiner loops [5], [6].

To improve extension theory of Steiner loops leads to effective methods for constructing and classifying specific Steiner triple systems [7].

References
[1] R. H. Bruck, *A Survey of Binary Systems*, Springer (1958).
[2] O. Chein, *Examples and methods of construction*, in Quasigroups and loops: theory and applications, Sigma Ser. Pure Math. 8 (1990), 27-93.
[3] C. J. Colbourn, A. Rosa, *Triple Systems*, Oxford mathematical monographs (1999).
[4] A. Drápal, P. Vojtěchovský, *Explicit constructions of loops with commuting inner mappings*, Eur. J. Comb. 29 (2008), 1662–1681.
[5] G. Falcone, Á. Figula, C. Hannusch, *Steiner loops of affine type*, Results Math. 75 (2020).
[6] G. Falcone, Á. Figula, M. Galici, *Extensions of Steiner Triple systems*,J. Combinatorial Designs 33 (2025), 94-108.
[7] G. Filippone, M. Galici, *On the number of small Steiner triple systems with Veblen points*, Discrete Mathematics 348 (2025).
[8] M. K. Kinyon, J. D. Phillips, P. Vojtěchovský, *C-loops: extensions and constructions*, J. Algebra Appl. 6 (2007), 1–20.
[9] P. T. Nagy, *Nuclear Properties of Loop Extensions*, Results Math. 74 (2019).
[10] P. T. Nagy, K. Strambach, *Schreier loops*, Czech. Math. J. 58 (2008), 759–786.

Some results about the nilpotent graph of a finite group

Michele Gaeta
Università degli Studi di Salerno, Italy
✉ migaeta@unisa.it

The association of graphs to groups goes back to the 19th century when Cayley introduced a graph that encodes the abstract structure of a group. Later other graphs have been considered. More precisely, given a group property $\mathcal{P}$ and a group G one can consider the graph whose set of vertices is G and two vertices x and y are adjacent if and only if the subgroup generated by x and y has the property $\mathcal{P}$. In particular if the property $\mathcal{P}$ denotes nilpotency, then the resulting graph is called the nilpotent graph of the group G.

In discussing the connection and the diameter of this graph, it is customary to exclude the unit of the group and sometimes all universal vertices. This talk aims to provide some results about the connectivity and the diameter of the nilpotent graph.

Indecomposable components of Fibered Burnside rings

Benjamin García Hernández
Universidad Nacional Autónoma de México
✉ benjamingarcia@matmor.unam.mx

Fibered Burnside rings were introduced by Dress as a generalization of monomial representation rings and the Burnside ring, to give a common framework for some induction theorems. These commutative rings associated to finite groups have been extensively studied not only as rings but also in the context of Mackey functors and biset functors, for which they are a source of important examples. In this talk, we will present a characterization of their blocks and their corresponding indecomposable components, as well as some connections to classic results on finite group theory.

Tensor products of representations of $\mathrm{GL}_2(\mathfrak{o}_\ell)$

Archita Gupta
Indian Institute of Technology, Kanpur
✉ architagup20@iitk.ac.in

Let F be a non-Archimedean local field with ring of integers $\mathfrak{o}$, maximal ideal $\mathfrak{p}$, and finite residual field $\mathbb{F}_q$, where q is a power of an odd prime p. Let $l \geq 2$ be an integer. Define $\mathfrak{o}_\ell = \mathfrak{o}/\mathfrak{p}^l$ as the finite local principal ideal ring. Let $G = \mathrm{GL}_2(\mathfrak{o}_\ell)$ be the group of invertible 2×2 matrices over $\mathfrak{o}_\ell$ or the general unitary group $\mathrm{GU}_2(\mathfrak{o}_\ell)$.

The tensor product problem is a well known problem in representation theory which consists of finding a complete decomposition of the tensor product modules of two representations of a group. In this talk, we discuss the tensor product problem for G and give some results on multiplicities of regular constituents of the tensor products of regular representations of G.

On Pronormalizers in Finite Groups

Ernesto Ingrosso
Università degli Studi di Napoli "Federico II", Italy
✉ ernesto.ingrosso2@unina.it

Let G be a group. A subgroup U of G is said to be *pronormal* if U and U^g are conjugate in $\langle U, U^g \rangle$, for each $g \in G$. Given a subgroup H of G, a *pronormalizer* M of H in G is a subgroup in which H is pronormal and maximal with respect to this property. Although in general a subgroup may have very different pronormalizers, we explore and identify conditions under which these share a common structure.

This is a joint work with M. Brescia and M. Trombetti.

Skew-braces of finite Morley rank

Moreno Invitti
Université Claude-Bernard Lyon 1, France
✉ morenoinv99@gmail.com

Skew braces are a class of algebraic structures introduced by Guarnieri and Vendramin to study set-theoretic solutions of the Yang–Baxter equation. A skew brace consists of a set equipped with two group operations satisfying a compatibility condition known as skew-left distributivity. This framework bridges group theory, ring theory, and mathematical physics, and has attracted growing interest from an algebraic perspective in recent years. Notions such as solvability and nilpotency — particularly (strong) left nilpotency — have been developed and explored within this context. In this talk, we investigate skew braces under the assumption of finite Morley rank, a model-theoretic concept that generalizes the idea of dimension from algebraic geometry. In particular, we present a complete classification of skew braces of Morley rank at most 3. Additionally, we prove that if both the additive and multiplicative groups of a skew brace are nilpotent, then the skew brace is strong left nilpotent. Finally, under an assumption concerning the length of chains of left ideals, we show that if both the additive and multiplicative groups are solvable, then the skew brace is also solvable.

On the theory of polynomial identities for algebras graded by a group

Antonio Ioppolo
Università degli Studi dell'Aquila, Italy
✉ antonio.ioppolo@univaq.it

In this talk, I will discuss the theory of polynomial identities for algebras graded by a group. I will highlight the role of graded algebras — especially superalgebras — in the development of this theory. Along the way, I will present classical results that hold in this setting and examine some pathological behaviors that arise in the graded structure.

Investigating some products of groups by means of the tensor product

Luigi Iorio
Università degli Studi di Napoli "Federico II", Italy
✉ luigi.iorio2@unina.it

A famous theorem of R. Baer states that a finite group which is the product of normal supersoluble subgroups is itself supersoluble, provided that its derived subgroup is nilpotent. In recent years (2023, [1]), this result has been extended by replacing normality with a weaker condition: permutability with the maximal subgroups of the Sylow subgroups.

In collaboration with Professor M. Trombetti (2025, [2]), we have studied this situation from a new perspective, making insightful use of a celebrated theorem of D.J.S. Robinson concerning the relation between tensor products and the lower central series. This allowed us to prove the aforementioned result in more general hypotheses, and to extend it, in a certain sense, to infinite groups. Hopefully, this new approach will inspire further research on products of groups.

References

[1] A. Ballester-Bolinches, S. Y. Madanha, M. C. Pedraza-Aguilera, X. Wu, *On Some Products of Finite Groups*, Proceedings of the Edinburgh Mathematical Society 66 (2023), 89–99.

[2] L. Iorio, M. Trombetti, *On Some Products of Groups*, Proceedings of the Edinburgh Mathematical Society (2025), 1–29.

Divisibility relation between number of certain surjective group and ring homomorphisms

Sonu Kumar
Manipal Institute of Technology, India
✉ sonu.mitmpl2024@learner.manipal.edu

Counting homomorphic structures in certain finite groups has been well explored. In 1984, *Joseph A. Gallian* and *James Van Buskirk* gave a closed form of the number of ring homomorphisms and in 2015, Javier Diaz-Vargas and *Gustavo Vargas de los Santos* explored the number of homomorphisms from $\mathbb{Z}_m$ to $\mathbb{Z}_n$. While past works determine the number of group and ring homomorphisms severally, there has been no study on the relation between the number of group and ring homomorphisms. We explore the relation between the number of ring homomorphisms and the number of surjective group homomorphisms in finite cyclic algebraic structures and find a certain divisibility relation. Using the direct product of groups, we further extend the result to abelian structures. We also find a relation between the number of ring homomorphisms and the number of elements of the highest order in an abelian structure.

On IBIS groups

Dmitry Malinin
Università degli Studi di Padova, Italy
✉ dmalinin@gmail.com

Let $G \subseteq Sym(\Omega)$ be a finite permutation group. An ordered sequence of elements of Ω, $\Sigma := (\omega_1, \ldots, \omega_t)$, is irredundant for G if no element in Σ is fixed by the stabiliser of its predecessors; if Σ is a base of G and it is irredundant, we call it an irredundant base. If all irredundant bases of G have the same size, G is called an IBIS group. In [2], Cameron and Fon-Der-Flaass showed that all irredundant bases for a permutation group G have the same size if and only if all the irredundant bases for G are preserved by reordering. Groups satisfying one of the previous equivalent properties are called Irredundant Bases of Invariant Size groups, IBIS groups for short. Moreover, Cameron and Fon-Der-Flaass [2] also proved that for a permutation group G to be IBIS is a necessary and sufficient for the irredundant bases of G to be the base of a combinatorial structure known with the name of matroid. If this condition hold, then G acts geometrically on the matroid and when G acts primitively and is not cyclic of prime order, then the matroid is geometric (see [2] for more details). This brought Cameron to ask for a possible classification of the IBIS groups. As explained by Cameron himself in [1, Section 4-14], there is no hope for a complete classification of IBIS groups, when the cardinalities of the bases are large. But it might be reasonable to pose this question for primitive groups. The first attempt of classifying finite primitive IBIS groups has been done in [3]. We give a classification of quasi-primitive soluble irreducible IBIS linear groups, and we also describe nilpotent, metacyclic IBIS linear groups and IBIS linear groups of odd order.

References
[1] P. J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts, Cambridge University Press, 1999.
[2] P. J. Cameron, D. G. Fon-Der-Flaass, *Bases for Permutation Groups and Matroids*, Europ. J. Combin. 16 (1995), 537–544.
[3] A. Lucchini, M. Morigi, M. Moscatiello, *Primitive permutation IBIS groups*, J. Combin. Theory Ser. A 184 (2021).

Base size and minimal degree of finite primitive groups

Fabio Mastrogiacomo
Università degli Studi di Milano-Bicocca, Italy
✉ fabio.mastrogiacomo01@universitadipavia.it

Let G be a finite primitive group of degree n. Two classical invariants of G are the base size and the minimal degree. The base size is the smallest possible size of a base of G, where a base is a sequence of points of the domain of G with trivial pointwise stabilizer. The minimal degree of G is the minimum number of points moved by a non-identity element of G. In this talk, we first present a new bound on the base size of a finite primitive group, which depends on the degree n. Building on this result, we then establish a new theorem linking the base size and the minimal degree of a finite primitive group. In particular, our result shows that the product of these two invariant is at most $n \log_2 n$. This bound is asymptotically best possible, up to a multiplicative constant.

On finite groups in which the twisted conjugacy classes satisfy some conditions

Chiara Nicotera
Università degli Studi di Salerno, Italy
✉ cnicotera@unisa.it

If G is a group and $\varphi \in \mathrm{Aut}(G)$, then we may consider the relation of φ-conjugation that is an equivalence relation in G. This relation is the usual conjugation if $\varphi = id_G$. The sizes of conjugacy classes have a big influence on the structure of a finite group. We investigate finite groups G having an automorphism $\varphi \in \mathrm{Aut}(G)$ such that the sizes of φ-conjugacy classes satisfy some conditions.

Lower central series of some groups acting on trees

Marialaura Noce
Università degli Studi di Salerno, Italy
🖂 mnoce@unisa.it

In 1996, Zelmanov conjectured that a just infinite pro-p group of lower central width is either soluble, p-adic analytic, or commensurable to a positive part of a loop group or to the Nottingham group. This conjecture was settled in the negative by Rozhkov, who proved that the (first) Grigorchuk group (and as a consequence also its profinite completion) has lower central width 3.

The result by Rozhkov, and later works by Bartholdi and Grigorchuk, do not only determine the lower central width of the Grigorchuk group, but also provide a detailed description of the terms of its lower central series.

In this talk, we first survey some known results about the lower central series and lower central width in known groups acting on regular rooted trees such as the aforementioned Grigorchuk group and the Gupta-Sidki 3-group (which is an example of a GGS-group). Then, we present some new results regarding the lower central series and lower central width of a wide class of non-torsion GGS-groups.

This is joint work with M. E. Garciarena-Perez and G. A. Fernández-Alcober.

Normality conditions in the Sylow p-subgroups of Sym(p^n) and its associated Lie algebra

Giuseppe Nozzi
Università degli Studi dell'Aquila, Italy
🖂 giuseppe.nozzi@graduate.univaq.it

Let $p > 2$ be a prime and let W_n be the Sylow p-subgroup of $\mathrm{Sym}(p^n)$. This group can be seen as the iterated wreath product $W_n = \wr_{i=1}^n \mathbb{Z}_p$ (see [2]), where $\mathbb{Z}_p$ is the cyclic group of order p. We compute the upper and the lower central series of W_n and we provide a proof, alternative to Kaloujnine's one, of the fact that these two series coincide.

Next, we investigate the normal subgroups N of W_n. Specifically, we prove that if N is contained in the last $n-k$ base subgroups of W_n, then it contains a term of the lower central series with bounded index depending only on k.

We introduce the graded Lie algebra $\mathfrak{L}_n$ associated to the lower central series of W_n. In [3], the authors characterize this Lie algebra as the iterated wreath product $\mathfrak{L}_n = \mathfrak{L}_1 \wr \cdots \wr \mathfrak{L}_1$, where $\mathfrak{L}_1$ is the one-dimensional algebra over $\mathbb{Z}_p$. We introduce a map $\phi\colon W_n \to \mathfrak{L}_n$ that establish a relation between the group and the algebra and which intertwines central series and a special class normal subgroups with ideals. In particular also the upper and lower central series of $\mathfrak{L}_n$ coincide. Finally, using the map ϕ, we relate the normalizer chain originating from the canonical regular elementary abelian subgroup of W_n and the idealizer chain introduced in [1], proving that they exhibit the same growth.

References
[1] R. Aragona, R. Civino and N. Gavioli, *A modular idealizer chain and unrefinability of partitions with repeated parts*, Israel J. Math. 260 (2024), 441-461.
[2] M. Krasner and L. A. Kaluzhnin, *Produit complet des groupes de permutations et problème d'extension de groupes I*, Acta Sci. Math. 13 (1950), 208-230.
[3] V. I. Sushchansky, N. V. Netreba, *Wreath product of Lie algebras and Lie algebras associated with Sylow p-subgroups of finite symmetric groups*, Algebra Discrete Math. 1 (2005), 122-132.

Fischer Matrices of a Factor Group of a Maximal Subgroup of the Baby Monster

Abraham Love Prins
University of Fort Hare, Dikeni, South Africa
✉ aprins@ufh.ac.za

The Baby Monster simple group $\mathbb{B}$ has a maximal subgroup $S = 2^{9+16\cdot}Sp_8(2)$ that contains a normal subgroup $E = 2^8$, an elementary abelian 2-group of order 256. Consequently, the factor group S/E exists with structure $2^{1+16\cdot}Sp_8(2)$. In this presentation, the Fischer matrices and ordinary character table of S/E are constructed using its underlying factor group $2^{16\cdot}Sp_8(2)$.

On the irreducibility of monomial representations for set-theoretical solutions to the Yang-Baxter equation

Silvia Properzi
Vrije Universiteit Brussel, Belgium
✉ silvia.properzi@vub.be

In a joint work with C. Dietzel and E. Feingesicht, we relate the combinatorial structure of set-theoretical solutions (X, r) to the Yang–Baxter equation and the algebraic properties of their associated monomial representations. Focusing on involutive, non-degenerate solutions (solutions for brevity), we study the monomial representation $\Theta : G(X) \to M_X(\mathbb{C}(q))$ of their structure group of and its specializations $\overline{\Theta}_l$, defined on the Coxeter-like quotients $\overline{G}_l(X) = G(X)/ldG(X)$, where d is the Dehornoy class of the solution.

Using the brace structure of these groups, we prove that Θ ($\overline{\Theta}_l$ for $l > 1$ and $\overline{\Theta}_1$ for $d > 2$) is irreducible if and only if X is indecomposable. We also investigate the case $d = 2$ giving sufficient condition for the irreducibility of $\overline{\Theta}_1$.

Finally, in all cases where irreducibility holds, we show that the representations Θ and $\overline{\Theta}_l$ are induced from explicit one-dimensional characters of the stabilizer of a point of X.

On the Occurrence of Groups as the Schur Multiplier of Prime Power Groups

Pradeep Kumar Rai

Mahindra University, Hyderabad, India

✉ pradeepkumar.rai@mahindrauniversity.edu.in

Schur multiplier of a finite group G is defined as the second cohomology group of G with coefficients in the multiplicative group of complex numbers considering the trivial action of G. This originated in a work of Issai Schur on projective representations of groups and plays an important role in the theory of group extensions. In the Kourovka Notebook, Berkovich posed the question of whether every finite abelian p-group is isomorphic to the Schur multiplier of some non-abelian finite p-group? In this talk, we will provide an affirmative answer for the case of elementary abelian p-groups.

Finite p-groups as Generalized Frobenius Complements

Carlo Maria Scoppola

Università degli Studi dell'Aquila, Italy

✉ scoppola@univaq.it

We study the structure of the Sylow p-subgroups of a finite group G under the hypothesis that the complement of their set theoretical union generates a proper (normal) subgroup of G.

From Vaughan Jones' connections to new infinite simple groups

Ryan Seelig

University of New South Wales, Sydney, Australia

✉ r.seelig@unsw.edu.au

About ten years ago Vaughan Jones discovered beautiful and powerful connections between Richard Thompson's groups F, T, V, subfactor theory, and quantum field theory. Inspired by these connections, Arnaud Brothier has recently introduced *forest-skein groups*, which mix the binary forest calculus of Thompson's groups with the skein theory of subfactor planar algebras. In this talk we investigate some examples of FS groups and show they witness new finitely presented infinite simple groups having previously unseen dynamical properties.

This is joint work with Arnaud Brothier.

A Study of Non-inner Automorphisms in Certain Finite p-Groups

Sandeep Singh
Akal University, Bathinda, India
✉ sandeepinsan86@gmail.com

There is a famous conjecture known as the Non-inner Automorphism Conjecture, listed in the renowned book "Unsolved Problems in Group Theory: The Kourovka Notebook", which states that *Every finite non-abelian p-group admits an automorphism of order p which is not an inner* (see [9, Problem 4.13]). In this paper, we discuss the latest developments on the non-inner automorphism conjecture and present our recently proven result for certain finite p-groups.

References

[1] A. Abdollahi, *Powerful p-groups have non-inner automorphisms of order p and some cohomology*, J. Algebra 323(3) (2010), 779-789.
[2] A. Abdollahi, S. M. Ghoraishi, Y. Guerboussa, M. Reguiat, B. Wilkens, *Non-inner automorphisms of order p for finite p-groups of coclass 2*, J. Group Theory 17(2) (2014), 267-272.
[3] A. Abdollahi, M. Ghoraishi, B. Wilkens, *Finite p-groups of class 3 have non-inner automorphisms of order p*, Beitr. Algebra Geom. 54(1) (2013), 363-381.
[4] M. Deaconescu, G. Silberberg, *Noninner automorphisms of order p of finite p-groups*, J. Algebra 250(1) (2002), 283-287.
[5] S. M. Ghoraishi, *A note on automorphisms of finite p-groups*, Bull. Aust. Math. Soc. 87(1) (2013), 24-26.
[6] S. M. Ghoraishi, *On non-inner automorphisms of finite nonabelian p-groups*, Bull. Aust. Math. Soc. 89(2) (2014), 202-209.
[7] S. M. Ghoraishi, *On non-inner automorphisms of finite p-groups that fix the Frattini subgroup element-wise*, J. Algebra Appl. 17(1) (2018).
[8] S. M. Ghoraishi, Non-inner automorphisms of order p for finite p-groups of restricted coclass, Arch. Math. 117(4) (2021), 361-368.
[9] E. I. Khukhro, V. D. Mazurov, Unsolved Problems in Group Theory: The Kourovka Notebook, No. 20, Russian Academy of Sciences, Siberian Branch, Sobolev Institute of Mathematics (2022).
[10] M. Ruscitti, L. Legarreta, M. K. Yadav, *Non-inner automorphisms of order p in finite p-groups of coclass 3*, Monatsh. Math. 183(4) (2017), 679-697

Hyperdigraphical representations of Frobenius groups

Jacob Smith
The University of Western Australia, Perth
✉ jacob.smith@research.uwa.edu.au

A 3-uniform hyperdigraph is a generalisation of a graph, consisting of a set of vertices and a set of 3-tuples of vertices known as hyperarcs. The automorphism group of a 3-uniform hyperdigraph is always 3-closed. Frobenius groups are also 3-closed. In this talk I discuss the result that every Frobenius group G has a Hyperdigraphical Frobenius Representation (HdFR), that is, a 3-uniform hyperdigraph of which G is the full automorphism group. This is a generalisation of the Digraphical Regular Representation (DRR) problem, solved by Babai in 1980, which asks which regular permutation groups occur as the automorphism group of a digraph.

Right Engel conditions for Orderable Groups

Maria Tota
Università degli Studi di Salerno, Italy
✉ mtota@unisa.it

Let g be an element of a group G. For a positive integer n let $R_n(g)$ be the subgroup generated by all commutators $[...[[g,x],x],\dots,x]$ over $x \in G$, where x is repeated n times. Similarly, $L_n(g)$ is defined as the subgroup generated by all commutators $[...[[x,g],g],\dots,g]$, where $x \in G$ and g is repeated n times. In the literature there are several results showing that certain properties of groups with small subgroups $R_n(g)$ or $L_n(g)$ are close to those of Engel groups. The present talk deals with orderable groups in which, for some $n \geq 1$, the subgroups $R_n(g)$ are polycyclic. Let $h \geq 0$, $n > 0$ be integers and G an orderable group in which $R_n(g)$ is polycyclic with Hirsch length at most h for every $g \in G$. We will see that there are (h,n)-bounded numbers h^* and c^* such that G has a finitely generated normal nilpotent subgroup N with $h(N) \leq h^*$ and G/N nilpotent of class at most c^*. The analogue of this theorem for $L_n(g)$ was established in 2018.

A Lazard correspondence between post-Lie rings and skew braces

Senne Trappeniers
Vrije Universiteit Brussel, Belgium
✉ senne.trappeniers@vub.be

Skew braces are directly related to regular affine actions of groups. Post-Lie rings appear, among other places, in the study of regular affine actions of Lie groups, already hinting at a connection with skew braces. Indeed, results by Burde–Dekimpe–Deschamps, Rump, Smoktunowicz and Bai–Guo–Sheng–Tang give concrete conditions for when a (partial) correspondence exists between skew braces and post-Lie rings.

In this talk, we first recall and explain the statement of the classical Lazard correspondence. Next, we discuss how skew braces are the natural group theoretic counterpart of post-Lie rings. This will provide us with the necessary tools and notions to formulate the Lazard correspondence between skew braces and post-Lie rings and give an idea of its proof. By doing so, the novel notion of L-nilpotency appears as a natural condition.

Cabling solutions of the Yang-Baxter equation

Arne Van Antwerpen
University of Ghent, Belgium
✉ arne.vanantwerpen@ugent.be

Cabling is a method introduced by Lebed, Ramirez and Vendramin to link seemingly different involutive non-degenerate solutions of the Yang-Baxter equation. In particular, the method allows to conceptually explain the link between the decomposability of a solution and the cycle structure of the square map. In this talk we explain how to extend the method to a large class of non-involutive solutions, biquandles, and extend several decomposability results. If time permits, we cover the relation between the cabling method and the Dehornoy class, a complexity parameter associated to a solution. This is based on joint work with I. Colazzo.

New approaches to group-based post-quantum cryptography

Dorota Wedmann
Warsaw University of Technology, Poland
✉ dorota.wedmann.dokt@pw.edu.pl

Group-based post-quantum cryptography uses the problems and properties of groups to build cryptographic schemes that are safe against quantum attacks. The group problems considered for cryptographic applications are usually combinatorial in nature, for example, Dehn's problems and their modifications, membership problems, the factorization problem, the subgroup intersection problem, and so on. In my talk, I will provide the necessary background and examples of group-based schemes. Then, I will focus on presenting new approaches to group-based post-quantum cryptography, specifically usage of rational or algebraic sets of groups instead of subgroups for given problems. I will discuss the pros and cons of this approach. I will conclude the talk by presenting some new ideas on how we can build cryptographic schemes using computationally hard problems defined in certain classes of groups.

Uncountable extended residually finite groups

Antonella Zaccardo
Università degli Studi di Napoli "Federico II", Italy
✉ antonella.zaccardo@unina.it

A subgroup X of a group G is closed (with respect to the profinite topology) if it can be obtained as intersection of a collection of subgroups of finite index of G, and a group G is said to be extended residually finite, or, for short, an ERF-group if all its subgroups are closed. Several authors have studied the structure of ERF-groups belonging to some notable group classes. In this talk, a subgroup H of an uncountable group G is said to be large if it has the same cardinality as G. We will focus our attention on uncountable groups in which every large subgroup is profinitely closed; moreover, uncountable groups in which each proper large subgroup is an ERF-group are considered.

Author Index