Young Researchers Algebra Conference 2023

25.07.2023 - 29.07.2023
L'Aquila (Italy)

25.07.2023 - 29.07.2022 — L'Aquila (Italy)

Young Researchers Algebra Conference 2023

Book of abstracts

Organizers

Andrew Darlington
Margherita Paolini
Giuseppe Nozzi

Scientific Committee

Riccardo Aragona
Roberto Civino
Ilaria Colazzo
Maria Ferrara
Marco Trombetti

Foreword

Young Researchers Algebra Conference 2023 is the third edition of the conference series YRAC. The goal is to bring together young algebraists and to give them the opportunity to present their latest research. Particular focuses of this year's edition are Group Theory, Cryptography, Ring Theory, and algebraic structures related to the Yang–Baxter Equation, but all topics within algebra are very welcome.

Riccardo Aragona
Roberto Civino
Ilaria Colazzo
Maria Ferrara
Marco Trombetti

Index of Talks

Wednesday, July 26

Thursday, June 27

Friday, June 28

List of Speakers

On the theory of polynomial identities

12:30
12:50

Antonio Ioppolo
University of L'Aquila
E-mail: antonio.ioppolo@univaq.it

A polynomial (in non-commuting variables) is said to be an identity for an algebra A if it vanishes under all evaluations in elements of A. Algebras satisfying at least one of these non-trivial relations are called PI-algebras and the research field studying them is known as PI-theory. The first goal of this seminar is to introduce the basic notions, to present the most used techniques and to enunciate some of the main results of PI-theory in the setting of associative algebras. In the last part, we will look at some of the latest developments in this area, when it comes to algebras with additional structure.

Weak instances of ECDLP

14:30
15:05

Daniele Taufer
KU Leuven
E-mail: daniele.taufer@kuleuven.be

The discrete logarithm problem over the point group of elliptic curves (ECDLP) has historically been one of the favorite choices for designing public-key cryptographic algorithms, due to several convenient features of these curves. In a nutshell, given two points P and Q of an elliptic curve, the security of such protocols relies on the conjectured complexity of recovering an integer N such that $Q = NP$. However, elliptic curves are not all equivalent for this purpose, and a poor choice of the underlying algebraic objects may undermine the goodness of the protocol. In this talk, we will explore some bad choices of these curves that allow to efficiently recover the ECDLP over prescribed subgroups or even the complete point group. In particular, we present some recent results for addressing ECDLP for points at infinity over finite rings, which advice paying close attention when dealing with such families of curves in cryptography.

Main features of fundamental (graded) algebras

15:10
15:30

Elena Pascucci
Sapienza Università di Roma
E-mail: elena.pascucci@uniroma1.it

One of the main questions in PI-theory is the so-called Specht Problem: the T-ideal of identities of a PI-algebra over a field of characteristic zero is finitely generated as a T-ideal? A positive solution was given by Kemer in 1987. The key step in its solution is known as "Kemer Representability Theorem", which states that any affine PI (super)algebra over a field F of characteristic zero has the same (super)identities as a finite dimensional (super)algebra over an appropriate field extension L of F. A key role in this last theorem is played by fundamental (super)algebras. In the present talk we will look at well-known results and examples of fundamental algebras and we will provide new examples of fundamental superalgebras. Finally, if time allows, we shall give a characterization of fundamental superalgebras in terms of the representation theory of the hyperoctahedral group. This is based on a joint work with Antonio Giambruno and Ernesto Spinelli.

15:30
15:50

Hopf-Galois structures on separable extensions

Andrew Darlington
University of Exeter
E-mail: ad788@exeter.ac.uk

Hopf-Galois structures play a central role in the study of a Galois theory for separable (but not necessarily normal) extensions. In short, they are algebriac constructions which consist of a Hopf algebra acting on an extension L/K in some special way, essentially mimicking the role played by a Galois group, but may not be unique. A couple of key theorems now mean that finding and describing HGS on separable extensions boils down to looking at particular subgroups of the holomorph of a group. In this talk, I will introduce these objects, give a few explicit results, and end by discussing a few open problems.

15:50
16:10

Invertible Quadratic Non-Linear Functions over $\mathbb{F}_p^n$ via multiple local maps

Ginevra Giordani
University of L'Aquila
E-mail: ginevra.giordani@graduate.univaq.it

The construction of invertible non-linear layers over $\mathbb{F}_p^n$ that minimize the multiplicative cost is crucial for the design of symmetric primitives targeting Multi Party Computation (MPC), Zero-Knowledge proofs (ZK), and Fully Homomorphic Encryption (FHE). At the current state of the art, only few non-linear functions are known to be invertible over $\mathbb{F}_p$, as the power maps $x \mapsto x^d$ when $\gcd(d, p-1) = 1$.

When working over F_p^n for n 2, a possible way to construct invertible nonlinear layers $\mathcal{S}$ over $\mathbb{F}_p^n$ is by making use of a local map $F : \mathbb{F}_p^m \to \mathbb{F}_p$ for m n, that is, $\mathcal{S}_F(x_0, x_1, \cdots, x_{n-1}) = y_0\|y_1\|\cdots\|y_{n-1}$ where $y_i = F(x_i, x_{i+1}, \cdots, x_{i+m-1})$. This possibility has been recently studied by Grassi, Onofri, Pedicini and Sozzi at FSE/ToSC 2022. Given a quadratic local map $F : \mathbb{F}_p^m \to \mathbb{F}_p$ for $m \in \{1, 2, 3\}$, they proved that the shift-invariant non-linear function $\mathcal{S}_F$ over $\mathbb{F}_p^n$ defined as before is never invertible for any n $2 \cdot m - 1$.

In this talk we face the problem by generalizing such construction. Instead of a single local map, we admit multiple local maps, and we study the creation of nonlinear layers that can be efficiently verified and implemented by a similar shift-invariant lifting. After formally defining the construction, we focus our analysis on the case $\mathcal{S}_{F_0,F_1}(x_0, x_1, \cdots, x_{n-1}) = y_0\|y_1\|...\|y_{n-1}$ for $F_0, F_1 : \mathbb{F}_p^2 \to \mathbb{F}_p$ of degree at most 2. As main result, we prove that if n 3, then $\mathcal{S}_{F_0,F_1}$ is never invertible if both F_0 and F_1 are quadratic, and that if n 4, then $\mathcal{S}_{F_0,F_1}$ is invertible if and only if it is a Type-II Feistel scheme.

Joint work with Lorenzo Grassi, Silvia Onofri and Marco Pedicini.

16:10
16:30

Automorphisms and classification of particular $\mathbb{F}_2$-braces

Valerio Fedele
University of L'Aquila
E-mail: valerio.fedele@graduate.univaq.it

Let $(V, +, \cdot)$ be a commutative associative radical $\mathbb{F}_2$-algebra of $\mathbb{F}_2$-dimension n, such that $V^3 = 0$ (i.e. for every $u, v, w \in V$, $u \cdot v \cdot w = 0$). Define the circle operation on V by $u \circ v = u + v + u \cdot v$. It is known that $(V, +, \circ)$ is a bi-skew brace, which we call binary bi-brace. Motivated by the interest of the automorphism groups of these structures in the context of symmetric cryptography, we provide a characterization of $\mathrm{Aut}(V, +, \circ)$ and a description of the isomorphism classes in terms of the isometry group of suitable subspaces of alternating bilinear forms over $\mathbb{F}_2$ (i.e. whose associated matrices are symmetric and 0-diagonal). In particular, a complete classification is provided for $n \leqslant 7$ and for some subcases when $n > 7$.

A common divisor graph for skew braces

17:00
17:20

Silvia Properzi

Vrije Universiteit Brussel
E-mail: Silvia.Properzi@vub.be

In the combinatorial study of solutions to the Yang–Baxter equation (YBE), recently introduced ring-theoretical objects play a fundamental role: skew braces. A skew brace is a set with two group operations + and $\circ$ satisfying a compatibility condition. In a skew brace $(A,+,\circ)$, the group $(A,\circ)$ acts on $(A,+)$ by automorphism via $\lambda\colon (A,\circ)\to(A,+)$. This action is involved in the (universal) construction of the set-theoretic solutions to the YBE provided by skew braces. Furthermore, the λ-action deeply influences the structure of a finite skew brace, as e.g. ideals are λ-invariant normal subgroups (for both group structures). Motivated by similar ideas in representation theory of finite groups and by the work of of Bertram, Herzog, and Mann, we study a common divisor graph: the simple undirected graph whose vertices are the non-trivial λ-orbits and two vertices are adjacent if their sizes are not coprime. We provide some examples and prove that it has at most two connected components and that, in the connected case, its diameter is at most four. The main result is a complete classification of finite skew braces with a one-vertex graph. In particular, the number of non-isomorphic skew braces of size $2^m d$ (with d odd) whose graph has only one vertex is $m\cdot a(d)$ if m 3 and $2a(d)$ if m 4, where $a(d)$ is the number of isomorphism classes of abelian groups of order d.

Locally recoverable codes over Galois ring

17:20
17:40

Giulia Cavicchioni

University of Trento
E-mail: giulia.cavicchioni@unitn.it

In the past decade, there has been significant interest in the study of Locally Recoverable Codes (LRC) over finite fields. The goal of a local recovery technique is to enable the retrieval of lost encoded data using only a small portion of the available information, rather than requiring access to the complete codeword. Many research efforts have focused on establishing bounds on the minimum distance and developing techniques for constructing LRC codes. In 2012, it was proved that for a linear code C of length n dimension k and locality r, the minimum distance of the code is upper bounded by d $n-k-\lceil\frac{k}{r}\rceil+2$ [1]. C is said to be optimal if its distance meets this bound with equality. In 2014 Tamo and Barg, in [2], have given a construction for a new family of optimal LRC evaluation codes.
In our work, we have explored Locally Recoverable codes over Galois rings. Through an extension of the classical result, we have derived an upper bound or the minimum distance for LRC codes over rings. In this context, we also have introduced a Tamo-Barg-like construction method, enabling us to construct a novel family of optimal codes.

References

[1] Gopalan, Parikshit and Huang, Cheng and Simitci, Huseyin and Yekhanin, Sergey: On the locality of codeword symbols, IEEE Transactions on Information theory, volume 58,11,6925-6934, IEEE (Publisher), 2012.

[2] Tamo, Itzhak and Barg, Alexander: A family of optimal locally recoverable codes, IEEE Transactions on Information theory, volume 60,8,4661-4676, IEEE (Publisher), 2014.

17:40
18:00

Central Endomorphisms of Groups and Radical Rings

Mario Viscusi

Università degli studi della Campania Luigi Vanvitelli
E-mail: mario.viscusi@studenti.unicampania.it

An endomorphism γ of a group G is called a central endomorphism if $x^{-1}x^{\gamma}$ lies to the centre $Z(G)$ of G for each element x of G. It is easy to show that every central non-zero endomorphism of G is an automorphism if and only if the ring $R = Hom(G, Z(G))$ of all homomorphisms of G into $Z(G)$ is a (Jacobson) radical ring, i.e. R is a group via the circle operation $f \circ g = f + g + fg$ for all $f, g \in R$. In this talk a necessary and sufficient condition will be given in the case R is an Artinian radical ring, along with some corollaries and examples. Moreover, it will be pointed out how central automorphisms can be used to produce solutions of the Yang–Baxter equation.

18:00
18:20

Germs and Sylows for structure group of solutions to the Yang-Baxter equation

Edouard Feingesicht

University of Caen Normandie
E-mail: edouard.feingesicht@unicaen.fr

In 1992, Drinfeld addressed the question of classifying set-theoretical solutions to the Yang-Baxter equation. In 2015, Dehornoy published an article on cycle sets (equivalent to involutive left non-degenerate solutions) introducing a calculus to re-obtain well-known results (I-structure, Garsideness) along with new constructions (the class of a solution, the germ associated to the structure group). We will first briefly mention some results on the class, such as a conjecture on a bound that is verified in a specific case. The main goal is the construction of the Zappa-Szép product of two solutions, allowing us to reduce the problem of classifying all solutions to only the ones with Dehornoy's class a prime power.

Thursday, June 27

On the algebraic structure of dual weak braces and the Yang–Baxter equation 10:00 10:35

Paola Stefanelli

University of Salento

E-mail: paola.stefanelli@unisalento.it

In 1992, Drinfel'd [3] suggested the study of set-theoretical solutions of the Yang-Baxter equation, a basic equation of statistical mechanics that arose from two independent works by Yang (1968) and Baxter (1971). To this day, a complete description of these solutions is still unknown.

In 2007, Rump [5] found a surprising connection between Jacobson radical rings and solutions. Moreover, he introduced the more general structure of the brace and showed a correspondence between braces and involutive non-degenerate solutions. The interest in braces and their generalizations has considerably grown in the last few years, and particular attention is devoted to the interplay between the properties of these structures and the behaviour of solutions associated to them.

In this talk, we focus on dual weak braces, structures recently introduced in [2] (see also [1]) that are triples $(S,+,\circ)$ with $(S,+)$ and $(S,\circ)$ Clifford semigroups satisfying the relations

$$a\circ(b+c) = a\circ b - a + a\circ c \qquad \text{and} \qquad a\circ a^{-} = a - a, \tag{$*$}$$

for all $a,b,c \in S$, where a^{-} and $-a$ are the inverses of a with respect to $+$ and $\circ$, respectively. If $(S,+)$ and $(S,\circ)$ are groups, then they have the same identity 0, and the second equality in $(*)$ trivially holds; in this case, $(S,+,\circ)$ is a skew brace [4] and, more specifically, if in addition $(S,+)$ is abelian, then $(S,+,\circ)$ is a brace. We show that every dual weak brace determines a solution and explore their properties.

References

[1] F. Catino, M. Mazzotta, M.M. Miccoli, P. Stefanelli, Set-theoretical solutions of the Yang-Baxter equation associated to weak braces, Semigroup Forum 104 (2022), no. 2, 228 - 255.

[2] F. Catino, M. Mazzotta, P. Stefanelli, Rota–Baxter operators on Clifford semigroups and the Yang–Baxter equation, J. Algebra 622 (2023) 587 - 613.

[3] V. G. Drinfel'd, On some unsolved problems in quantum group theory, in: Quantum groups (Leningrad, 1990), vol. 1510 of Lecture Notes in Math., Springer, Berlin, (1992), pp. 1 - 8.

[4] L. Guarnieri, L. Vendramin, Skew braces and the Yang-Baxter equation, Math. Comp. 86 (307) (2017), 2519 - 2534.

[5] W. Rump, Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra 307 (1) (2007), 153 - 170.

Centrally nilpotent skew braces 10:40 11:00

Arne Van Antwerpen

Vrije Universiteit Brussel

E-mail: arne.vanantwerpen@telenet.be

This talk will be based on joint work with Eric Jespers and Leandro Vendramin. The class of multipermutation solutions is a particularly interesting class of solutions of the celebrated Yang-Baxter equation (coming from mathematical physics) with a beautiful combinatorial structure. It was shown that this class corresponds to right nilpotent skew left braces of nilpotent type. In this talk we delve deeper into this class of skew left braces and identify the class of centrally nilpotent skew braces. We discuss that these behave very similar to nilpotent groups and will identify several possible central series for these objects. If time permits, we use this class to illustrate several other key concepts of skew left braces. The talk will be rife with examples and exciting open problems.

12:30
12:50

On quadratic rational groups

Marco Vergani
University of Firenze
E-mail: marco.vergani@unifi.it

In this seminar I will talk about families of groups that have a characterization of their integral central units inside the rational group algebra. Quadratic rational groups are finite groups that have a rational field of values for any irreducible character with degree at most two over $\mathbb{Q}$. From a character table perspective, they are the "dual" concept of the well-studied semirational groups.

15:30
15:50

Continuum quantum groups and the Yang–Baxter equation

Margherita Paolini
University of L'Aquila
E-mail: margherita.paolini@graduate.univaq.it

In the fundamental manuscript [1] Emil Artin has introduced the sequence of Braid Group B_n. B_n is a group whose elements are equivalence classes of n-braids up to isotopy. The Braid Group admits different equivalent definitions, in particular, we will introduce the Birman-Ko-Lee presentation [2] whose generators are $a_{l,m}$ (the $a_{l,m}$ braid is the elementary interchange of the l-th and the m-th strand of the braid with all the other strands held fixed). We will use the BKL generators to define a continuum analogue of the Braid group B_n called T (Tapes group). This work is a primary step in order to define an action of T on the continuum Quantum Group introduced by Appel and Sala [3].

References

[1] E. Artin: Theorie der Zopfe, Amburg Abh., volume 4,42-72, 1925.

[2] J. Birman, K.H. Ko, S.J. Lee: A new approach to the word and conugacy problem in the braid group,Adv. Math., volume 139(2), 253-322, 1998.

[3] A. Appel, F. Sala: Quantization of Continuum Kac Moody Algebras, Pure Appl. Math., Q.16, 439-493, 2020.

15:50
16:10

The dual and the hull code in the framework of the two generic constructions

Virginio Fratianni
University of Paris VIII
E-mail: virginio.fratianni@gmail.com

We contribute to the knowledge of linear codes from special polynomials and functions, which have been studied more intensively in the past few years by C. Ding [1] and S. Mesnager [2]. Such codes have several applications in secret sharing, authentication codes, association schemes and strongly regular graphs.

This is the first work in which we study the dual codes in the framework of the two generic constructions; in particular, we propose a Gram-Schmidt process to compute them explicitly. The originality of this contribution is in the study of the existence or not of functions f' (respectively of defining sets D'), which can be used as ingredients to construct the dual code $\mathcal{C}'$ for a given code $\mathcal{C}$ in the context of the two generic constructions. In particular, with the study of the dual in the second generic construction, we are able to give alternative proofs of the known results about these codes [3]. We also determine a necessary condition expressed by employing the Walsh transform for a codeword of $\mathcal{C}$ to belong in the dual. This achievement was done in general and when the involved functions are weakly regularly bent. We shall give a novel description of the Hull code in the framework of the two generic constructions. Our primary interest is constructing linear codes of fixed Hull dimension and determining the (Hamming) weight of the codewords in their duals.

References

[1] C. Ding: A construction of binary linear codes from Boolean functions, Discrete mathematics, volume 339, Elsevier (Publisher), 2016.

[2] S. Mesnager: Linear codes from functions, Chapter 20 in A Concise Encyclopedia of Coding Theory CRC Press/Taylor and Francis Group (Publisher) London, New York, 2021. Cryptogr. 87 (2019), no. 2-3, 225–247.

[3] C. Xiang: It is indeed a fundamental construction of all linear codes, arXiv preprint arXiv:1610.06355 (2016).

Graph-restrictive and exponent-restrictive actions 16:10 16:30

Marco Barbieri

University of Pavia

E-mail: marco.barbieri07@universitadipavia.it

We consider the pairs (Γ, G), where Γ is a connected graph, and G $\mathrm{Aut}(\Gamma)$ is a subgroup of automorphism which is transitive on the vertices of Γ. We say that (Γ, G) is locally-L if, for any vertex $\alpha \in V\Gamma$, the permutation group induced by the action of the vertex-stabiliser G_α on the neighbourhood of α is isomorphic to L. Following [1], a permutation group L is graph-restrictive if there exists a constant $\mathbf{c}(L)$ such that,

$$\text{for any locally-}L\text{ pair }(\Gamma, G),\quad |G_\alpha|\ \mathbf{c}(L),$$

and exponent-restrictive if there exists a constant $\mathbf{e}(L)$ such that,

$$\text{for any locally-}L\text{ pair }(\Gamma, G),\quad \exp(G_\alpha)\ \mathbf{e}(L).$$

The study of graph-restictive actions can be traced back to a celebrated theorem of W. Tutte, which states that $\mathbf{c}(L)$ 48 for any pair (Γ, G) with Γ cubic and L transitive (see [2]). The main conjecture of this field was posed by R. Weiss in [3], and it is still unsettled.

Weiss Conjecture. Any primitive group is graph-restrictive.

We observe that, if L is graph-restrictive, then the number of generators of G and the exponent of G_α are bounded from above by a function of the valency of the graph Γ. On the other hand, there are infinite families (Γ_h, G_h) whose common local action L is not primitive and where the number of generators of G_h cannot be bounded by a function of the valency of Γ_h. An analogous result is not known for the exponent: this is what prompted the definition of exponent-restrictive actions and the following question.

Question. Is any arbitrary group exponent-restrictive?

This is joint work with Valentina Grazian, Primož Potočnik and Pablo Spiga.

References

[1] P. Potočnik, P. Spiga, and G. Verret, On graph-restrictive permutation groups. Journal of Combinatorial Theory, Series B102 (2012) pp. 820–831.

[2] W. T. Tutte, On the symmetry of cubic graphs. Canadian Journal of Mathematics 11 (1959) pp. 621–624. Cryptogr. 87 (2019), no. 2-3, 225–247.

[3] R. Weiss, *s*-transitive graphs. Colloquia Mathematica Societatis János Bolyai 25 (1978) pp. 827–847.

17:00
17:20

Irreducible representations of the Hecke–Kiselman algebras

Magdalena Wiertel

University of Warsaw

E-mail: m.wiertel@mimuw.edu.pl

To every finite oriented graph Θ with n vertices one can associate a finitely presented monoid HK_Θ, called the Hecke–Kiselman monoid. It is a monoid generated by n idempotents with relations of the form $xy = yx$ or $xyx = yxy = xy$, depending on the edges between vertices x and y in Θ. By the Hecke–Kiselman algebra we mean the monoid algebra $K[HK_\Theta]$ of the monoid HK_Θ over an algebraically closed field K.

We investigate the structure and representations of the Hecke–Kiselman algebras. It turns out that the case of the monoid C_n associated to an oriented cycle of length $n \geqslant 3$ plays a crucial role. The unexpected ideal chain inside this monoid is constructed. This result is then used to describe all irreducible representations of C_n. It is the crucial step to characterize the irreducible representations of any Hecke–Kiselman algebra that satisfies a polynomial identity. Irreducible representations come either from idempotents in the Hecke–Kiselman monoid or are induced by the representations of certain semigroups of matrix type arising from HK_Θ. The result shows a surprising similarity to the classical theorems on the representations of finite semigroups.

17:20
17:40

On the non-transitivity of group actions in cryptography

Giuseppe D'Alconzo

Politecnico di Torino

E-mail: giuseppe.dalconzo@polito.it

Cryptographic group actions are becoming a viable option for post-quantum assumptions. In recent years, many primitives have been designed based on problems related to isogenies of elliptic curves, tensors, and linear code equivalence. However, all these schemes use transitive actions or they restrict to a single orbit. In this talk, based on joint work with A. Flamini and A. Gangemi, we introduce a novel and general framework that exploits the non-transitivity propriety and makes use of orbit-invariant functions. We call this construction Group Action with Canonical Elements (GACE), and as a first implementation, we propose a bit commitment scheme, i.e., the cryptographic realization of a locked box, allowing a party to commit to a chosen value while keeping it hidden, with the ability to reveal the committed value later. Our construction represents the first non-interactive bit commitment based on group actions. Furthermore, we provide an example instantiation of the scheme using tensors. In this specific case, the invariant function employed is the tensor rank, and the cryptographic assumption is linked to the Tensor Isomorphism problem.

Component group of the centralizer of a nilpotent orbit

17:40
18:00

Emanuele Di Bella
University of Trento
E-mail: emanuele.dibella@unitn.it

In the Seventies, P. Bala and R. Carter provided a significant theorem to classify nilpotent orbits in a semisimple Lie algebra $\mathfrak{g}$. In particular, it turned out that the nilpotent orbits in g are in bijection with pairs $(\mathfrak{l}, e)$, where $\mathfrak{l}$ is a Levi subalgebra of $\mathfrak{g}$ and e is a distinguished nilpotent element in $\mathfrak{l}$. Twenty years later, E. Sommers provided a generalization of the Bala-Carter theory, establishing a bijection between pairs $(\mathfrak{l}, e)$ as above and pairs (e, C), with again e a distinguished nilpotent element in $\mathfrak{l}$ and C a conjugacy class of the component group $A(e)$. The latter is defined as the quotient of the centralizer of a nilpotent element in a connected simple algebraic group over its identity component. The results of E. Sommers provided a systematic approach to the determination of the component groups of the centralizers. In this talk I discuss how to determine the elements of the component groups explicitly; this can be tough due to computational problems but in many cases it can be done taking advantage of computer algebra packages like GAP and Magma.

Some recent results on the conformal superalgebra CK_6

18:00
18:20

Lucia Bagnoli
University of Zagreb
E-mail: lucia.bagnoli@math.hr

In this talk we recall the definition and the main properties of conformal superalgebras and, in particular, the classification of irreducible finite conformal modules over the conformal superalgebra CK_6 that was obtained by Boyallian, Kac, Liberati and Martinez, Zelmanov with different techniques. Then we present a result on the bound on the degree of singular vectors of finite Verma modules over the exceptional Lie superalgebra $E(1,6)$ that is isomorphic to the annihilation superalgebra associated with the conformal superalgebra CK_6. We present the computation of the homology of the first and third quadrants of the complexes of finite Verma modules, that were classified by Boyallian, Kac and Liberati, over the annihilation superalgebra $A(CK_6) = E(1,6)$. The computation of the homology provides an explicit realization of all irreducible quotients. Finally, we discuss some open problems.

10:00
10:35

On algebraically closed groups

Mattia Brescia
University of Napoli
E-mail: mattia.brescia@unina.it

In analogy with algebraically closed fields, a group G is said to be algebraically closed if every finite set of equations defined over G that is soluble in a group containing G is soluble in G. Ever since they were defined in 1951 by W. R. Scott, algebraically closed groups have proven to be a great source of highly non-constructive examples of groups connecting group theory, model theory, game theory and many other fields.

In this talk we will present many striking results about algebraically closed groups, together with some recent advances in their study. Special attention will be paid to the class of κ-existentially closed groups for an infinite cardinal κ. A group G is said to be κ-existentially closed if every set of at most κ equations and inequalities defined over G that is soluble in a group containing G is soluble in G.

10:40
11:00

Classes of set-theoretical solutions to the pentagon equation

Marzia Mazzotta
Università del Salento
E-mail: marzia.mazzotta@unisalento.it

The pentagon equation classically originates from Mathematical Physics, whose problem of finding solutions is still open. Our attention is placed on determining its set-theoretical solutions, namely, if X is a non-empty set, we investigate maps $s : X \times X \to X \times X$ satisfying the relation

$$s_{23}\, s_{13}\, s_{12} = s_{12}\, s_{23},$$

with s_{ij} the map from $X \times X \times X$ into itself acting as s on the (i, j)-component and as the identity on the remaining one. Writing $s(x, y) = (xy, \theta_x(y))$, where $\theta_x : X \to X$ is a map, for every $x \in X$, one has that s is a solution if and only if X is a semigroup and they hold

$$\theta_x(yz) = \theta_x(y)\theta_{xy}(z) \quad \& \quad \theta_y = \theta_{\theta_x(y)}\theta_{xy},$$

for all $x, y, z \in X$.

In this talk, we present some classes of solutions achieved starting from particular semigroups. Into the specific, considered a Clifford semigroup X, we characterize idempotent-invariant solutions on X that are those for which θ_x remains invariant on the set of idempotents $E(X)$. In addition, we will focus on the class idempotent solutions, which are solutions fulfilling $s^2 = s$, by showing that the idempotents of X have a key role in such an investigation.

12:30
12:50

On the arithmetic and geometric means of element orders in a finite group

Carmine Monetta
Università degli studi di Salerno
E-mail: cmonetta@unisa.it

In this talk we present some recent results concerning functions depending on element orders in a finite group. More precisely, we consider two functions related to the arithmetic and geometric means of element orders of a finite group, showing that certain bounds on such functions strongly affect the group structure.

Describing Hopf–Galois structures via skew braces

15:30
15:50

Lorenzo Stefanello

Università di Pisa

E-mail: lorenzo.stefanello@phd.unipi.it

Hopf–Galois theory, a generalisation of Galois theory in which the action of a Galois group is replaced by a suitable action of a Hopf algebra, has been showed to be valuable in dealing with classical arithmetic problems in a more general context. The goal of this talk, based on a joint work with Senne Trappeniers, is to present an overview of this theory in the setting of Galois extensions, showing how in this case the Hopf–Galois structures can be described explicitly and bijectively with skew braces. As a consequence, we show that the study of the surjectivity of the Hopf–Galois correspondence, a long-standing problem of the theory, assumes a more manageable form in this point of view.

Cryptanalysis of protocols using conjugacy search problem in certain semidirect product platform groups

15:50
16:10

Martina Vigorito

University of Salerno

E-mail: marvigorito@unisa.it

Group theory and in particular non-abelian groups offer a rich supply of complex and varied problems for cryptography. In this talk, I will present a technique of solving Conjugacy Search Problem (CSP) in certain classes of groups which could be split as a semidirect product of groups. CSP and variation of it has been used in group-based cryptography, based on its difficulty in certain infinite groups.

On conjugation quandle coloring of torus knots - A characterization of GL(2,q)-colorability

16:10
16:30

Filippo Spaggiari

Charles University Prague

E-mail: spaggiari@karlin.mff.cuni.cz

The classification of knots is a wide problem that has been addressed through various methods. Notably, the study of knot invariants supported by tools of quandle theory has proven to be highly advantageous in the research of a quandle coloring, that is, a way to distinguish one knot from another by assigning a mathematical object to each strand of its diagram. In this talk, we present a characterization for determining the colorability of torus knots using matrices in $GL(2,q)$.

Labelling Hasse diagrams of modular geometric lattices

17:00
17:20

Carsten Dietzel

Vrije Universiteit Brussel

E-mail: carstendietzel@gmx.de

An observation of Rump is that every modular Garside group can be described by a suitable labelling of the Hasse diagram of a finite modular geometric lattice. In particular, solutions to the Yang-Baxter equation can be described by certain labellings of the diagram of a finite Boolean lattice.

In this talk, I will present several ways of constructing these labellings and pose some questions about the labellability of bounded modular geometric lattices.

17:20
17:40

Exploring the use of Pell hyperbolas in DLP-based cryptosystems

Gessica Alecci
Politecnico di Torino
E-mail: gessica.alecci@polito.it

The group structure of Pell hyperbolas has a wide range of applications in various cryptosystems, particularly in Public-Key Encryption (PKE) schemes that rely on the Discrete Logarithm Problem (DLP), such as the ElGamal PKE scheme. In this talk, we will exhibit a generalization of the group structure on Pell hyperbolas. We will provide a parameterization using both an algebraic approach and a geometrical interpretation. Additionally, we will introduce new ElGamal schemes based on the Pell hyperbola, highlighting their computational advantages through a specific parametrization.

17:40
18:00

Lie semisimple algebras of derivations and varieties of almost polynomial growth

Sebastiano Argenti
University of Basilicata
E-mail: sebastiano.argenti@unibas.it

In this talk we are interested in the growth of the differential identities of finite dimensional associative algebras, i.e., polynomial identities of algebras with an action of a Lie algebra by derivations.
In this context Gordienko and Kochetov proved that, over fields of characteristic zero, the exponent always exists and is a positive integer. As a consequence of their proof, the codimension sequence associated of the differential identities either grows polynomially or exponentially [1].
We are interested in characterizing associative algebras A of almost polynomial growth, that is the codimension sequence of A grows exponentially but for any finite dimensional algebra in the variety generated by A, generating a proper subvariety, the corresponding growth is only polynomial.
This problem appears naturally in the study of varieties of PI-algebras with (or without) some additional structure and was solved for associative algebras [2], graded algebras [3], algebras with involution [4], trace algebras [5], etc.
A common flavor of these results is the existence of a finite number of such varieties and the indication of a concrete list of generating algebras. Our main result concerns the characterization of varieties of almost polynomial growth in case the Lie algebra acting by derivations is sl_2. In this case we obtain two infinite classes of algebras generating distinct differential varieties of almost polynomial growth.
We also discuss the more general case in which L is any finite dimensional semisimple Lie algebra. We exhibit a list of algebras such that the codimension growth of a variety is exponential if and only if it contains one of the algebras in the list.

References

[1] A. S. Gordienko, M. V. Kochetov: Derivations, gradings, actions of algebraic groups,and codimension growth of polynomial identities, Algebras and Representation Theory, 17(2):539-563, mar 2014.

[2] A. R. Kemer: Nonmatrix varieties, Algebra i Logika 19 no. 3, 255–283,382, 1980.

[3] A. Valenti: Group graded algebras and almost polynomial growth, J. Algebra 334 247–254, 2011.

[4] A. Giambruno, S. Mishchenko: On star-varieties with almost polynomial growth,Algebra Colloq. 8,no. 1, 33–42,2001.

[5] A. Ioppolo, P. Koshlukov, D. La Mattina: race identities and almost polynomial growth, J. Pure Appl. Algebra 225,no. 2, Paper No. 106501, 20 pp, 2021.

Bi-Skew Braces and Hopf–Galois structures with a surjective Hopf–Galois correspondence

18:00
18:20

Senne Trappeniers

Vrije Universiteit Brussel

E-mail: senne.trappeniers@vub.be

Bi-skew braces were defined by L. N. Childs as those skew brace where we can swap the role of the two operations and once again obtain a skew brace.
The notion of a brace block was later introduced by A. Koch and is a set with a family of group structures such that any choice of two group structures yields a bi-skew brace. We will discuss a new characterization of bi-skew braces and brace blocks. As these characterizations are quite technical, we also consider a less general, but more manageable construction of brace blocks. This can then be used to construct several new examples of brace blocks. One such family of examples leads to new examples of Hopf–Galois structures such that the Hopf–Galois correspondence is surjective, and moreover all such Hopf–Galois structures whose associated skew brace is a bi-skew brace are of this form.
This talk is based on joint work with L. Stefanello.

List of Speakers