2nd Mile High Conference on Nonassociative Mathematics
June 21–27, 2009, University of Denver, Denver, Colorado

Abstracts of Talks

Murray Bremner (University of Saskatchewan, Canada)
Enveloping algebras of Malcev algebras

In 2004, Pérez-Izquierdo and Shestakov extended the Poincaré-Birkhoff-Witt theorem from Lie algebras to Malcev algebras: for any Malcev algebra M (over a field of characteristic $\neq 2, 3$), they constructed a universal nonassociative enveloping algebra $U(M)$, which shares many of the attractive properties of the associative enveloping algebras of Lie algebras. In particular, $U(M)$ has a monomial basis of PBW type and a natural Hopf algebra structure. In part one of this talk, I will review Pérez-Izquierdo and Shestakov's construction of $U(M)$. In part two, I will describe how this construction can be used to compute explicit structure constants for the enveloping algebras of low-dimensional Malcev algebras. These computations can be simplified using differential operators on the associated graded algebra of $U(M)$ (a polynomial algebra in $\dim M$ variables) and derivations defined by two elements of M (which is contained in the generalized alternative nucleus of $U(M)$). Since $U(M)$ is not alternative in general, it is also of interest to calculate its maximal alternative quotient, which is the universal alternative enveloping algebra $A(M)$. In part three, I will describe the resulting new examples of infinite dimensional alternative algebras. This program has been carried out for the 4-dimensional (solvable) Malcev algebra and for the 5-dimensional nilpotent Malcev algebra, and is currently underway for the 5-dimensional non-solvable Malcev algebra (which is the semidirect product of the simple 3-dimensional Lie algebra and its unique non-Lie module of dimension 2). The next step is to study the one-parameter family of 5-dimensional solvable Malcev algebras. The ultimate goal of this research program is to calculate the structure constants for $A(M)$ where M is the 7-dimensional simple Malcev algebra; this will be the "universal alternative envelope" of the octonions. This is joint work with Irvin Hentzel, Luiz Peresi, Marina Tvalavadze and Hamid Usefi.

Jung Rae Cho (Pusan National University, Korea)
Decomposition of graphs into cycles of a fixed length

The Oberwolfach Problem formulated by Ringel in 1967 was to determine whether it is possible to seat an odd number n of people at t round tables for k different meals so that each person has every other person next to him/her exactly once? Here, the capacities of the tables are $m_1, m_2, \ldots, m_t$, respectively, with $m_1 + m_2 + \ldots + m_t = n$ and $m_i \geq 3$. This problems is in fact a graph decomposition problem which asks if it is possible or not to partition the edge set of K_n into k classes so that each class constitutes an m_1-cycle, an m_2-cycle, …, and an m_t-cycle which are mutually vertex-disjoint.

Decompositions of graphs into edge-disjoint cycles have been an active research area for many years. Especially, decompositions by cycles of a fixed length have been considered in a number of different ways. Recently, it was shown that a complete graph of odd order, or a complete graph of even order minus an 1-factor, has a decomposition into k-cycles if k divides the number of edges (see [1], [10], [11]). One of the key factors for all these works was the cycle decomposition of complete bipartite graphs appeared in [12]. Many authors began to consider cycle decompositions with special properties ([4], [5], [8], [9]). Then, Billington and Hoffman [2] introduced the notion of a *gregarious cycle*, which is now settled as a cycle in a multipartite graph involving at most one vertex from any given partite set. We will see some results of $K_{n(2t)}$, the n-partite graph with $2t$ vertices in each partite set, into gregarious cycles of the same lengths ([3], [6], [7]).

References

[1] B. Alspach and H. Gavlas, *Cycle decompositions of K_n and $K_n - I$.* J. Combin. Theory Ser. B **81**(2001), 77–99.
[2] E. Billington and D. G. Hoffman, *Decomposition of complete tripartite graphs into gregarious 4-cycles.* Discrete Math. **261**(2003), 87–111.
[3] E. Billington and D. G. Hoffman, *Equipartite and almost-equipartite gregarious 4-cycle decompositions*, preprint.
[4] E. Billington, D. G. Hoffman and C. A. Rodger, *Resolvable gregarious cycle decompositions of complete equipartite graphs.* Preprint.
[5] N. J. Cavenagh and E. J. Billington, *Decompositions of complete multipartite graphs into cycles of even length.* Graphs and Combinatorics **16**(2000), 49–65.
[6] J. R. Cho, M. J. Ferrara, R. J. Gould and J. R. Schmitt, *A difference set method for circular decompositions of complete mutipartite graphs into gregarious 4-cycles.* Research article (unpublished).
[7] J. R. Cho and R. J. Gould, *Decompositions of complete multipartite graphs into gregarious 6-cycles using difference sets.* To appear in J. Korean Math. Soc. 45(2008), No 6, 1623-1634.
[8] J. Liu, *A generalization of the Oberwolfach problem with uniform tables.* J. Combin. Theory Ser. A **101**(2003), 20–34.
[9] J. Liu, *The equipartite Oberwolfach problem and C_t-factorizations of complete equipartite graphs.* J. Combin. Designs **9**(2000), 42–49.
[10] M. Šajna, *On decomposiing $K_n - I$ into cycles of a fixed odd length.* Descrete Math. **244**(2002), 435–444.
[11] M. Šajna, *Cycle decompositions III: complete graphs and fixed length cycles.* J. Combin. Designs **10**(2002), 27–78.
[12] D. Sotteau, *Decomposition of $K_{m,n}$ ($K^*_{m,n}$) into cycles (circuits) of length $2k$.* J. Combin. Theory Ser B. **30**(1981), 75-81.

Adam Christov (Charles University in Prague, Czech Republic)
Quadratic quasigroups in public-key cryptography

Public-key cryptographic schemes based on the complexity of solving multivariate quadratic equations over a finite field represent an alternative to widely used schemes relying on the complexity of factorization or on the discrete logarithm. Such a scheme was proposed by D. Gligoroski et al. Keys in this scheme are constructed using a special kind of quasigroups, the so-called quadratic quasigroups. In this talk I describe quadratic quasigroups and classify them according to their properties.

Piroska Csörgő (Eötvös Loránd University, Hungary)
On Moufang loops that have nilpotency class at most two over the nucleus

TBA.

Daniel Daly* (University of Denver, USA)
Petr Vojtěchovský (University of Denver, USA)
Enumerating nilpotent loops

We will discuss the isomorphism problem for centrally nilpotent loops. Using techniques from cohomology and linear algebra, we can enumerate the isomorphism classes for nilpotent loops of order n for $n < 24$ and of order $2p$ for p a prime. This research is heavily computer aided and we will discuss how to teach the computer to count nilpotent loops.

Ricardo Diaz (UNAM Cuernavaca, Mexico)
The Magnus' map for free loops

In the theory of loops analogies with group theory always played a great role. In 1963 Graham Higman has shown that free loops are residually nilpotent. For groups there is a proof of this fact going back to Magnus which uses a monomorphism from the free group $F(X)$ into the ring of non-commutative power series over the set X. We show that in the varieties of IP-loops and of diassociative loops the analogue of Magnus' map is not injective. In addition we present some results for the variety of Moufang loops.

Geoffrey Dixon
Ternary comples algebra

A ternary generalization of the algebra of complex numbers is presented.

Diane Donovan (University of Queensland, Australia)
Latin squares, latin trades and related problems

In this talk I will begin by discussing early problems concerning the completion of partial latin squares. By reviewing this early work I will highlight the importance of the study of latin trades. Given two latin squares L and M, of the same order, the differences between the squares gives rise to a latin trade. That is, the partial latin squares L/M and M/L are said to form latin trades. Throughout this talk I will present a number of open problems in the study of latin squares and latin trades.

Andrew Douglas* (City University of New York, USA)
Murray Bremner (University of Saskatchewan, Canada)
Generalized Lie-Yamaguti Structures on $sl(3)$-Modules $V(n,n)$

The Lie algebra $sl(3)$ of dimensions 8 has an irreducible representation $V(2,2)$ of dimension 27. By projecting the exterior square of $V(2,2)$ onto itself and onto the adjoint representation, we may define a binary-ternary structure on $V(2,2)$. We will describe how computer algebra was implemented to determine the polynomial identities satisfied by this structure in degrees less than or equal to 7, and see that it precisely satisfies the defining identities of Lie-Yamaguti algebras. We will also discuss the extension of the computations to $V(3,3)$ and $V(4,4)$ whose structures are shown to be generalizations of Lie-Yamaguti algebras.

Aleš Drápal (Charles University in Prague, USA)
A class of noncommutative A-loops

We define a binary operation on certain sets of 2×2 matrices over fields and show that the operation yields an A-loop. We discuss isomorphism and isotopism questions regarding these loops.

Tevian Dray* (Oregon State University, USA)
Corinne A. Manogue (Oregon State University, USA)
Octonions and fermions

We present some tantalizing suggestions of the role the octonions may play in the description of fundamental particles. Starting from an octonionic description of the Lorentz group in 10 spacetime dimensions, a mechanism is introduced for reducing 10 dimensions to 4 without compactification, thus reducing the 10-dimensional massless Dirac equation to a unified treatment of massive and massless fermions in 4 dimensions. Attempts to extend this symmetry-breaking scenario lead naturally to the consideration of a particular real, noncompact form of E_6, and of its subgroups. Along the way, we examine several relevant eigenvalue problems, with surprising results.

Clifton E. Ealy (Western Michigan University, USA)
On the automorphism group of a finitely generated free loop

Informally, a loop is a "group" without associativity or more precisely a quasi-group with identity. In a 1924 paper, Jakob Nielsen determined generators and relations for the automorphism group of a finitely generated free group. In two papers published in 1951 and 1953, Trevor Evans studied free loops and determined the the automorphism group of the free loop on one generator. In this talk, we will study automorphism group of the free loop on n generators.

Anthony Evans (Wright State University, USA)
Which latin squares are based on groups?

It is well-known that the multiplication/addition table of a finite group is a latin square, which we call the Cayley table of the group. It is natural to ask which latin squares can be the Cayley tables of groups. In this paper we survey the tests that have been devised to answer this question, as well as the more general question of which latin squares are isotopic to the Cayley tables of groups.

Stephen Gagola III (University of Arizona, USA)
A conjugacy class of p-subgroups of a triality group G

If G is a finite group with triality S and L is its corresponding Moufang loop with $P_1, P_2 \in Syl_p(L)$ for a "Sylow prime" p then there exist p-subgroups $Q_1, Q_2 \leq G$ that are conjugate in G where Q_i is invariant under S and P_i is its corresponding Moufang loop for $i \in \{1, 2\}$. For certain Moufang loops L of finite order the elements of $\{G(P) \leq G \mid P \in Syl_p(L)\}$ are conjugate in G and can be permuted transitively by $C_G(S)$. From this we get that $|Syl_p(L)| \mid |C_G(S)|$.

Nikolaos Galatos (University of Denver, USA)
Non-associative residuated lattices

Residuated lattices are algebraic structures that include Boolean and Heyting algebras, lattice-ordered groups, relation algebras, MV-algebras, powersets of monoids, and ideal lattices of rings, among others. At the same time they constitute algebraic models of substructural logics. The latter are non-classical logics, including intuitionistic, many-valued, relevance and linear, related to diverse areas from computer science and engineering to philosophy and linguistics.

Although the algebraic study of residuated lattices has focused primarily on associative structures, a substantial part of the theory can be carried out in the non-associative setting. Moreover, some deductive/logical systems associated with substructural logics and residuated lattices lack associativity. We will outline the algebraic theory of non-associative residuated lattices and in particular we will characterize congruence relations by appropriate subsets. We will also prove logical properties about non-associative deductive systems, including the parametrized local deduction theorem, as well as the cut-elimination and the strong separation

---

Maria L. M. Giuliani* (Federal University of ABC, Brazil)
Kenneth W. Johnson (Penn State Abington, USA)
Right division on Moufang loops

Starting from a group $(G, \cdot)$ consider the quasigroup $(G, *)$, obtained from G using right division $x * y = x \cdot y^{-1}$. It is well known that $(G, *)$ satisfies the identity

$$(x * z) * (y * z) = x * y. \tag{1}$$

Our purpose is construct a quasigroup $(L, *)$ starting from a Moufang loop $(L, .)$ instead of the group G. First, we have to find an identity similar to (1), which we call the Fundamental Identity. Then we consider the inverse problem: given a quasigroup $(H, *)$ satisfying the Fundamental Identity, can we define another operation $\circ$ so that $(H, \circ)$ is a Moufang loop? If not, what propertiesdoes $(H, \circ)$ satisfy? In this work I used program Prover9.

Richard Green (University of Colorado, Boulder, USA)
Chevalley bases for Lie algebras and the combinatorics of Kac's asymmetry function

A Chevalley basis for a Lie algebra over $\mathbb{C}$ is a basis for the algebra all of whose structure constants are integers. One of the standard constructions of Chevalley bases for simple Lie algebras over $\mathbb{C}$ involves a certain function ε taking values in the set $\{\pm 1\}$; this function is sometimes called *Kac's asymmetry function*. Although the definition of this function may appear mysterious at first, I will argue that it has some natural combinatorial interpretations. Along the way, I will present combinatorial constructions of some interesting nonassociative algebras, including the somewhat confusingly named "loop algebras" associated to simple Lie algebras over $\mathbb{C}$.

Robert L. Griess (University of Michigan, USA)
TBA

Alexandr Grishkov* (University of Sao Paulo, Brazil)
Ivan Shestakov (University of Sao Paulo, Brazil)
Commutative alternative algebras

We construct a basis of a commutative alternative algebra with $n \leq 8$ generators. As a corollary we calculate the order of the free commutative Moufang loop of exponent 3 with $n \leq 8$. In the case $n = 7$ our calculation depends on a conjecture (still open) that the free commutative Moufang loop of exponent 3 with 7 generators satisfies a certain identity of length 9.

Jonathan Hall (Michigan State University, USA)
Moufang loops and groups with triality are essentially the same thing

The remark of the title is folklore. But, as Grishkov and Zavarnitsine, Nagy and Vojtěchovský, and others have pointed out, there are many accepted statements about Moufang loops and related objects whose proofs are hard to find. We will discuss some of these, including that of the title.

Irvin Roy Hentzel* (Iowa State University, USA)
Murray Bremner (University of Saskatchewan, Canada)
Ivan Correa (Universidad Metropolitana de Ciencias de la Educacion, Chile)
Luiz Peresi (Universidade de Sao Paulo, Brazil)
Special Bol identities

A Bol algebra is defined in terms of a binary product $[a,b]$ and a ternary product $\langle a,b,c\rangle$. These five identities are assumed to hold:

$$[a,b]+[b,a]=0,$$
$$\langle a,b,c\rangle+\langle b,a,c\rangle=0,$$
$$\langle a,b,c\rangle+\langle b,c,a\rangle+\langle c,a,b\rangle=0,$$
$$\langle a,b,\langle c,d,e\rangle\rangle-\langle\langle a,b,c\rangle,d,e\rangle-\langle c,\langle a,b,d\rangle,e\rangle-\langle c,d,\langle a,b,e\rangle\rangle=0,$$
$$[\langle a,b,c\rangle,d]-[\langle a,b,d\rangle,c]+\langle c,d,[a,b]\rangle-\langle a,b,[c,d]\rangle+[[a,b],[c,d]]=0.$$

The special Bol algebra starts with a right alternative algebra and defines $[a,b]=ab-ba$ and $\langle a,b,c\rangle=J(b,c,a)=(b\circ c)\circ a-b\circ(c\circ a)$ where $x\circ y=xy+yx$ is the symmetric product in the right alternative algebra and $J(b,c,a)$ is the associator computed using the symmetric product. We have found identities which hold in any special Bol algebra which do not hold in the free Bol algebra.

Nora Hopkins (Indiana State University, USA)
Quadratic differential equations in the complex domain

I will begin by reviewing some previous work done jointly with Michael Kinyon concerning nonassociative algebra methods for getting qualitative results for real autonomous quadratic differential equations, in particular, results when a trajectory goes through an eigenspace of an algebra automorphism. I will then present some new results concerning the same issues when all of the variables are allowed to take complex values. The most interesting result is that if a trajectory goes through an eigenspace of a real automorphism where the eigenvalue is not real, then the real solution must blow up in finite time.

John Huerta* (University of California, Riverside, USA)
John Baez (University of California, Riverside, USA)
Division algebras and super-Yang–Mills theory

Thanks to the work of Dray, Manogue, Schray and others, we know how spinors in 10-dimensional spacetime are related to the octonions. In turn, this division algebra structure makes supersymmetric Yang–Mills theories possible in 10-dimensions. Generalizing their construction, we give a uniform treatment of super-Yang–Mills theories using normed division algebras.

Přemysl Jedlička* (Czech University of Life Sciences, Czech Republic)
Michael Kinyon (University of Denver, USA)
Petr Vojtěchovský (University of Denver, USA)
Constructions of commutative A-loops

An A-loop is a loop where all inner mappings are automorphisms. We present a few constructions of commutative A-loops:

- a group based construction that gives any commutative A-loop with the middle nucleus of index two;
- a cocycle construction that gives any commutative A-loop of exponent 2 with non-trivial center;
- a characterization of (presumably all) commutative A-loops of order p^3, for p a prime.

Kenneth Johnson (Penn State Unievrsity Abington, USA)
A naive way to construct loops from groups

I will discuss a way of modifying a group multiplication table to produce a loop. In the case where the group is factorised this construction gives the Bol loops. The basic idea is to use 'coordinates' and to modify one coordinate in a way that ensures that the latin square condition is preserved. I will discuss the kind of loops one can produce in general.

Tomáš Kepka (Charles University in Prague, Czech Republic)
Congruence-simple groupoids

TBA.

Michael Kinyon* (University of Denver, USA)
Přemysl Jedlička (Czech University of Life Sciences, Czech Republic)
Petr Vojtěchovský (University of Denver, USA)
Commutative automorphic loops

TBA.

Jens Koeplinger* (AT&T)
Vladimimr Dzhunushaliev (Kyrgyz-Russian Slavic University, Kyrgyzstan)
Hidden non-associative structures in quantum mechanics

It is shown [V. Dzhunushaliev, arXiv:0805.3221] that some operators in quantum mechanics have hidden structures that are unobservable in principle. These structures are based on a supersymmetric decomposition of the momentum operator, and a nonassociative decomposition of the spin operator. Key open questions will be highlighted, and their relevance for description of physical law on nonassociative algebra will be discussed.

Tomasz Kowalski (University of Cagliari, Italy)
A little more on non-finite basedness of diassociative loops

Power-associative loops (i.e., such that every one-generated subloop is a group) form a non-finitely based variety. For diassociative loops (i.e., such that every two-generated subloop is a group) the question whether they are finitely based was long open, although the conjecture that the answer is negative was folklore. At BLAST-2008 conference in Denver, I presented a proof confirming that conjecture. It shows that diassociative loops are not finitely based relative to power-associative loops. I intend to present that proof again, this time focusing on some of its side effects, such as the following:

Theorem: *The variety D of diassociative loops is not finitely based with respect to any subvariety of power-associative loops properly containing D.*

Jimmie Lawson* (Louisiana State University, USA)
Yongdo Lim (Kyungpook National University, Korea)
Symmetric quasigroups of operators

The set of positive definite matrices, positive operators on a Hilbert space, and positive elements of a Jordan algebra all admit in a natural way symmetric quasigroup structures (symmetric space structures, geometric mean structures, etc). We explore a variety of properties of positive operators that exhibit interesting connections with these quasigroup structures.

Ling Long (Iowa State University, USA)
Finite index subgroups of the modular group and right loops

The modular group consists of 2×2 determinant 1 integral matrices. Finite index subgroups of the modular group are of fundamental importance in number theory, group theory and combinatorics. We will describe several different approaches to the study of these groups, including permutation representation, generalized Farey sequence, and right loop structures of some of these groups suggested by Dr. Jonathan D. H. Smith. In particular, we will discuss an example which motivates the discovery of some special two sided right loops, which are called Catalan loops by Smith.

Shahn Majid (Queen Marry, University of London, UK)
Quasiassociative geometry and seven spheres

TBA.

Gábor P. Nagy (University of Szeged, Hungary)
Groups which are not (right) multiplication groups of loops

Let G be a permutation group acting transitively on the finite set Q. We are interested in the following questions:

Question 1: Is there a loop operation on Q such that the multiplication group is contained in G?

Question 2: Is there a loop operation on Q such that the right multiplication group is contained in G?

Questions 1' and 2': What about equality?

Concerning Question 1, there are negative results by Vesanen and Drápal on classical linear groups. Moreover, Drápal asked in 2001 if in dimension $k \geq 3$, any group G with $PSL(k,q) \leq G \leq P\Gamma L(k,q)$ can be realized as multiplication group of a loop. We show that the answer is yes for all $k \geq 3$ and prime power q. The constructions come from finite geometry: we use the multiplicative loops of finite nearfields modulo their centers.

Beside these results, very little is known. In particular, there are no theoretical methods which could exclude large families of groups. We present a computer program which can deal with groups where $|Q|$ is small and for which a small integer d exists such that the stabilizer of d elements in G is small. For example, the Mathieu group M_{22} of degree 22 can be handled.

Question 2 is usually formulated in the language of sharply transitive sets. The subset S of G is said to be sharply transitive if for any $x, y \in Q$, there is an element $s \in S$ such that s maps x to y. Clearly, the set of right multiplication maps of a quasigroup (loop) is a sharply transitive set (with $1 \in S$). Here, computers can be used for groups of order < 5000. The presently known theoretical tools for showing that a finite permutation group G does not contain a sharply transitive set are following: Lorimer's enumeration method, O'Nan's contradicting subgroup method, and character theoretical methods by Grundhöfer and P. Müller. We will try to give an idea of the latter and show some examples which are still open.

Both questions are even harder if there is a loop whose (right) multiplication group is properly contained in the group G and one wants to show that there is no loop with (right) multiplication group G. The situation gets better if G has not many transitive subgroup. For example, this is the case when G consists of semilinear transformations of a vector space.

Petr Němec (Czech University of Life Sciences, Czech Republic)
Linear quasigroups

Quasigroups constructed from other structures in the same way as medial quasigroups arise from abelian groups are investigated.

J. D. Phillips (Wabash College, USA)
Loops with abelian inner mapping groups

In 1946, R. H. Bruck proved that loops of central nilpotency class no greater than 2 have abelian inner mapping groups. While the converse doesn't hold, still, a great deal can be said, which is what we intend to do in this talk: give a (near) complete summary of what's known in this active area of research.

Peter Plaumann* (University of Erlangen, Germany)
Peter Nagy (University of Debrecen, Hungary)
Bruck decomposition for endomorphisms of quasigroups

In the year 1944 R. H. Bruck has described a very general construction method for quasigroups which he called the extension of a set by a quasigroup. We use it to construct a class of examples for LF-quasigroups in which the image of the map $e(x) = x\backslash x$ is a group. More generally, we consider the variety of quasigroups which is defined by the property that the map e is an endomorphism and its subvariety where the image of the map e is a group. We characterize quasigroups belonging to these varieties using their Bruck decomposition with respect to the map e. Our results will be published in the Journal of General Lie Theory and Applications.

Miikka Rytty (University of Oulu)
Finite loop capability for nilpotent groups

The structure of the inner mapping groups of loops is an open research problem. Even in the abelian and nilpotent cases only partial results are known. I will review some earlier results and show that certain nilpotent groups may not appear as the inner mapping group of a finite loop.

Liudmila Sabinina (UAEM Cuernavaca, Mexico)
The decomposition of a quasigroup with an endomorphic deviation

Recently there was considerable progress in the study of factorizations of isotopes of quasigroups from different subvarieties of the variety of LF–quasigroups. This development began with the work of Kepka, Kinyon and Phillips ([1], [2]). Here Moufang A-loops play a special role. At present the endpoint of this development is a recent paper of Shcherbacov [3]. I will discuss these achievements and our results ([4], [5]) in this area.

For a quasigroup Q call the map $e(x) = x\backslash x$ the *deviation* of Q. It is well known that in an LF–quasigroup the deviation is an endomorphism. In this case one can apply the Fitting decomposition with respect to the deviation.

References

[1] T. Kepka, M. K. Kinyon, J. D. Phillips, *On the structure of F-quasigroups*, J. of Algebra **317** no. **2** (2007), 435–461.
[2] T. Kepka, M. K. Kinyon, J. D. Phillips, *F-Quasigroups isotopic to groups*, arXiv:mathGR/0601077.
[3] V. A. Shcherbacov, *On the structure of left and right F-, SM- and E-quasigroups*, arXiv:0811.1725.
[4] P. Plaumann, L. Sabinina, L. Sbitneva, *A decomposition of LF-quasigroups*, AMS Contemporary Mathematics **483** (2009), pp. 221–227.
[5] P. Nagy, P. Plaumann, *Bruck decomposition for endomorphisms of quasigroups*, to appear in Journal of Generalized Lie Theory and Applications.

Jiřina Scholtzová (Czech Technical University, Czech Republic)
The free alternative nil superalgebra on one odd generator

We constructed the basis of the free alternative nil-superalgebra of index 3 on one odd generator. In addition we counted the index of solvability of this algebra, which is 3. We consider also the corresponding Grassmann algebra and show that the well known Dorofeev's example of solvable non-nilpotent alternative algebra is its homomorphic image.

V. A. Shcherbacov (Academy of Sciences of Moldova, Moldova)
On loop isotopes of some quasigroups

A quasigroup $(Q,\cdot)$ is *left distributive*, if for all $x, y, z \in Q$ $x \cdot uv = xu \cdot xv$; *left F-quasigroup*, if $x \cdot yz = xy \cdot e(x)z$; *right F-quasigroup*, if $xy \cdot z = xf(z) \cdot yz$; *F-quasigroup*, if it is left and right F-quasigroup; *left SM-quasigroup*, if $s(x) \cdot yz = xx \cdot yz = xy \cdot xz$; *right SM-quasigroup*, if $zy \cdot s(x) = zx \cdot yx$; *left E-quasigroup*, if $x \cdot yz = f(x)y \cdot xz$, where $s(x) = x \cdot x, f(x) \cdot x = x, x \cdot e(x) = x$ for all $x \in Q$ [2, 3, 8, 10].

A loop $(Q,\cdot)$ is *Moufang loop*, if for all $x, y, z \in Q$ $x(yz \cdot x) = xy \cdot zx$; *left M-loop*, if $x \cdot (y \cdot z) = (x \cdot (y \cdot I\varphi x)) \cdot (\varphi x \cdot z)$, where φ is a mapping of the set Q, $x \cdot Ix = 1$ for all $x \in Q$; *right M-loop*, if $(y \cdot z) \cdot x = (y \cdot \psi x) \cdot ((I^{-1}\psi x \cdot z) \cdot x)$, where ψ is a mapping of the set Q; *M-loop*, if if it is left M- and right M-loop; *left special*, if $S_{a,b} = L_b^{-1}L_a^{-1}L_{ab}$ is an automorphism of $(Q,\cdot)$ for any pair $a, b \in Q$ [2, 3].

Every SM-quasigroup is isotopic to a commutative Moufang loop [8]. A left (right) F-quasigroup is isotopic to a left (right) M-loop [7, 3]. A left F-quasigroup is isotopic to a left special loop [1, 4, 2, 6]. Any F-quasigroup is isotopic to a Moufang loop [9].

If a loop $(Q,\circ)$ is isotopic to a left distributive quasigroup $(Q,\cdot)$ with isotopy the form $x \circ y = R_a^{-1}x \cdot L_a^{-1}y$, then $(Q,\circ)$ will be called a *left S-loop.* In [5, 11] a left S-loop is called an *S-loop.* Any loop which is isotopic to a left F-quasigroup is a left M-loop ([3], Theorem 3.17).

Theorem [12]: *A left F-quasigroup is isotopic to the direct product of a group and a left S-loop. A left SM-quasigroup is isotopic to the direct product of a group and a left S-loop. A left E-quasigroup is isotopic to the direct product of an abelian group and a left S-loop. A left special loop is isotope of a left F-quasigroup if and only if it is isotopic to the direct product of a group and a left S-loop. An F-quasigroup is isotopic to the direct product of a group and a commutative Moufang loop. A loop that is isotopic to an F-quasigroup is isomorphic to the direct product of a group and a Moufang loop [9]. If an M-loop is isotopic to an F-quasigroup, then it is a Moufang loop.*

References

[1] V. D. Belousov, *On one class of quasigroups*, Učen. Zap. Bel'ck. Gos. Ped. Inst., **5** (1960), 29–46, (in Russian).
[2] V. D. Belousov, Foundations of the Theory of Quasigroups and Loops, Nauka, Moscow, 1967. (in Russian).
[3] V. D. Belousov,Elements of Quasigroup Theory: a special course, Kishinev State University, Kishinev, 1981. (in Russian).
[4] V. D. Belousov and I. A. Florja, *On left-distributive quasigroups*, Bul. Akad. Štiince RSS Moldoven, **7** (1965), 3–13, (in Russian).
[5] V. D. Belousov and V. I. Onoi, *On loops that are isotopic to left distributive quasigroups*, Mat. Issled. **3**(**25**) (1972), 135–152, (in Russian).
[6] I. A. Golovko, *F-quasigroups with idempotent elements*, Mat. Issled. **4**(**2**) (1969),

137–143, (in Russian).
[7] I. A. Golovko, *Loops that are isotopic to F-quasigroups*, Bul. Akad. Štiince RSS Moldoven. **2** (1970), 3–13, (in Russian).
[8] T. Kepka, *Structure of triabelian quasigroups*,
Comment. Math. Univ. Carolinae **17** (1976), 229–240, 1976. [9] T. Kepka, M. K. Kinyon, and J. D. Phillips, *The structure of F-quasigroups*, abs/math/0510298, 24 pages, 2005.
[10] M. K. Kinyon and J. D. Phillips, *Axioms for trimedial quasigroups*, Comment. Math. Univ. Carolin. **45**(**2**) (2004), 287–294.
[11] V. I. Onoi, *Left distributive quasigroups and loops, which are isotopic to these quasigroups*, PhD thesis, IM AN MSSR, Kishinev, 1972, (in Russian).
[12] V. A. Shcherbacov, *On the structure of left and right F-, SM- and E-quasigroups*, arXiv:0811.1725, 67 pages, 2008.

Ivan Shestakov (University of Sao Paulo, Brazil)
Structure and representations of Jordan and alternative superalgebras

We will speak on recent results in the theory of representations of Jordan and alternative superalgebras. In case of Jordan superalgebras we present a classification of irreducible modules over finite dimensional simple Jordan superalgebras obtained by C. Martinez, I. Shestakov, and E. Zelmanov. For alternative superalgebras we present a classification of irreducible superbimodules obtained recently by I. Shestakov and M. Trushina.

Jonathan Smith (Iowa State University, USA)
Catalan loops

Let e be a nilpotent (or topologically nilpotent) element of a commutative ring R. Let E be the annihilator of e. A product is defined on the direct square Q of the quotient R/E by $(x, x')(y, y') = (x\lambda^2 + y\lambda, x'\lambda^{-1} + y')$ with $\lambda = 1 + e^2yx'$. Then Q forms a loop, known as the *Catalan loop*. While the multiplication and right division are rational, the left division is given by a quadratic irrationality involving the generating function for the Catalan numbers. The whole construction is motivated by an example from number theory

---

David Stanovský (Charles University in Prague, Czech Republic)
Selfdistributive one-sided quasigroups

I will survey some results on left distributive left quasigroups, motivated by questions raised by my former adviser, Tomáš Kepka. I'd like to stress the connection of LDLQs to knot theory, where, quite recently, several theoretical studies on LDLQs (called racks, or quandles, there) appeared.

Douglas Stones* (Monash University, Australia)
Petr Vojtěchovský (University of Denver, USA)
Ian Wanless (Monash University, Australia)
When is an isotopism an autotopism of a Latin square?

An *isotopism* $\theta = (\alpha, \beta, \gamma)$ is a triplet of permutations. It is used to permute the rows, columns and symbols of a Latin square L. If $\theta(L) = L$ then θ is said to be an *autotopism* of L.

For which θ there exists a Latin square L such that $\theta(L) = L$ is largely unresolved problem. In this talk we will resolve some new cases, with a particular emphasis on when $\alpha = \beta = \gamma$, i.e. isomorphisms.

Petr Vojtěchovský* (University of Denver, USA)
Aleš Drápal (Charles University in Prague, Czech Republic)
Small loops of Csörgő type

Loop of nilpotency class higher than two and with commuting inner mappings is said to be of *Csörgő type*. Using trilinear alternating forms we construct a large family of loops of Csörgő type from certain groups. Within the used method, we characterize all groups that yield loops of order 128. For the first time we obtain a loop of Csörgő type whose inner mapping group is not elementary abelian.

Ian Wanless* (Monash University, Australia)
Andries Brouwer (Technische Universiteit Eindhoven, Netherlands)
Michael Kinyon (University of Denver, USA)
Two combinatorial properties that are loop-isotope invariant

I'll discuss two combinatorial problems that seem suited to a loop theoretic approach.

The first challenge is to construct loops for which there is no loop-isotope in which some pair of non-identity elements commute. The only known examples have order 8.

The second challenge is to construct loops for which all loop-isotopes have exponent three. This is relatively easy for orders that are powers of three. Is it possible for any other orders? An answer would resolve a conjecture due to van Rees.

An alternative title for this talk is "Two combinatorial problems that loop theorists should solve". I can't answer either of them, but then I am not a loop theorist.

Andrew Wells (Iowa State University)
Subloops of the Moufang loop of Zorn vector matrices over the integers modulo four

Paige's construction of simple Moufang loops over finite fields can be generalized over commutative rings. Here we look at the structure of the subloops of the constructed loop over the integers modulo four, focusing in particular on how it extends the subloop lattice of the Paige loop of order 120.

Jens Zumbrägel (University College Dublin, Ireland)
Classification of finite congruence-simple semirings with zero

A set with two binary operations $(R, +, \cdot)$ is called a *semiring* if $(R, +)$ is a commutative semigroup, $(R, \cdot)$ is a semigroup, and both distributive laws hold. We assume that R has always a *zero-element* which is neutral in $(R, +)$ and absorbing in $(R, \cdot)$. Semirings arise in numerous occasions, the natural numbers $(N = \{0, 1, 2, \dots\}, +, \cdot)$ probably being the most well-known example. The structure of a semiring is in a sense the most general over which matrix operations can be defined. Problems from graph theory like shortest path have concise descriptions using certain semirings.

Finite semirings can be applied in public-key cryptography to construct semigroup actions $A \times X \to X$ that may serve as a basis for generalised Diffie-Hellman and ElGamal cryptosystems. For cryptographic purposes it is important that the semiring in use is congruence-simple, meaning that it cannot be homomorphically mapped onto a smaller semiring. This leads to the question whether useful congruence-simple semirings exist.

In the talk a full classification of finite congruence-simple semirings will be presented and the proof will be sketched. The result generalises the classical Wedderburn-Artin theorem on the classification of finite simple rings. A substantial notion in the proof is that of (strongly) irreducible semimodules over semirings. Key results are that 1) any finite congruence-simple semiring R admits an irreducible semimodule M, and 2) a density result stating that R is then a "dense" subsemiring of the endomorphism semiring $\mathrm{End}(M)$ of the commutative monoid $(M, +)$.