AAA70 – 70th Workshop on General Algebra

Institute of Discrete Mathematics and Geometry, TU Wien
Wien (Vienna), Austria

Version 2005-05-24

Contents

Boundedness of topological rings of endomorphisms of torsion Abelian groups

Horea Abrudan
Technical College "Constantin Brancusi", Oradea, ROMANIA
abrudan_horea@yahoo.com
Coauthors: Mihail Ursul (University of Oradea, ROMANIA)

Fri 16:30, Diss (8th floor)

The ring End(A) of endomorphisms of an Abelian group A is considered as a topological ring furnished with the finite topology. We give some sufficient conditions on a torsion group A under which End(A) is bounded, i.e., has a fundamental system of neighborhoods of zero consisting of ideals. In all these cases End(A) is compact.

Types of polynomial completeness of expanded groups

Erhard Aichinger
Universität Linz
erhard@algebra.uni-linz.ac.at
Coauthors: Jürgen Ecker (Fachhochschule Hagenberg, Austria) and Mario Kapl (Universität Linz, Austria).

Sat 17:00, ZS 3 (7th floor)

From results of Maurer, Rhodes, and Fröhlich, we know that every function on a finite simple non-abelian group is a polynomial function; these groups are called *polynomially complete*. Later, it was studied when every congruence preserving function on an algebra is a polynomial function; such algebras were called *affine complete*. In 2001, P. Idziak and K. Słomczyńska introduced the concept of *polynomial richness*. We give some results that characterize algebras with these properties.

It is not known if there is an algorithm that decides whether a given finite algebra (of finite type, with given operation tables for all operations) is affine complete. However, we will show that it is decidable whether a finite nilpotent group (given by its multiplication table) is affine complete: having computed its nilpotent class k, it is sufficient to check whether every $(k+1)$-ary congruence preserving function is a polynomial function.

Epireflective subcategories in the category of compact modules

Daciana Alina Alb
Mathematics Department, University of Oradea, Romania
dalb@uoradea.ro

Sat 14:30, 101 A (3rd floor)

We will consider the category ${}_R\mathbf{C}$ of all compact R-modules over a fixed topological ring R with identity and the corresponding dual category $\mathbf{D}_R$ of all discrete topological R-modules.

A subcategory $\mathcal{A}$ of ${}_R\mathbf{C}$ is epireflective if and only if its image $\mathcal{B}$ in $\mathbf{D}_R$ under the functor * is closed under taking direct sums and homomorphic images.

We give examples of simple subcategories of ${}_{\mathbb{Z}}\mathbf{C}$. We construct an example of an epireflective subcategory $\mathcal{N}$ in the category GAT_2 of all Hausdorff topological Abelian groups different from the subcategory of all complete topological Abelian groups, having the property: for every $A \in \mathcal{N}$ the homomorphism $r_A : A \to r_A(A) \in \mathcal{N}$ is a topological embedding.

Engel elements in groups and dynamical systems defining nilpotency in finite groups

Jorge Almeida
Dep. Matematica Pura, Faculdade de Ciencias, Universidade do Porto, Porto, Portugal
jalmeida@fc.up.pt

Fri 17:30, Diss (8th floor)

Given n group terms $(w_1, \ldots, w_n)$ in the letters $x_1, \ldots, x_n$, consider the transformation which maps an n-tuple $(g_1, \ldots, g_n)$ of elements of a group G to the n-tuple obtained from the w_i by evaluating each x_j to g_j. This defines a transformation of the set G^n which is obviously uniformly continuous with respect to the profinite uniform structure on G and thus can be viewed as a topological dynamical system on $(\hat{G})^n$, where $\hat{G}$ is the profinite completion of G. The behaviour of the dynamical system naturally reflects structural properties of the group. For example, take $n = 2$ and consider the transformations defined by the pairs of terms $([x, y], y)$ and $(y^{-1}xy, x)$, where $[x, y] = x^{-1}y^{-1}xy$. It turns out that there is a close relationship between these two dynamical systems which leads to another characterization of Engel elements. Using this connection, it is shown that the set of left Engel elements is closed under multiplication by elements of the hypercenter subgroup. Some other dynamical systems and their relationship with nilpotency for finite groups are also considered.

Bezout semigroups

Pham Ngoc Anh
Hungarian Academy of Science
anh@renyi.hu
Coauthors: L. Marki and P. Vamos

Sat 14:00, Diss (8th floor)

We discuss the structure of Bezout semigroups as well as their realization as the semigroup of principal ideals of a Bezout rings.

On symmetries of quasi-crystals

Vyacheslav A. Artamonov
Moscow State University
artamon@mech.math.msu.su

Sun 09:00, 101 A (3rd floor)

A complete classification of symmetries of crystals was known since thirties in the last century. But in 1984 a new alloy $Al_{0,86}Mn_{0,14}$ was discovered with an icosahedral symmetry which was forbidden in the symmetry theory of crystals and which is known as *Penrose tiling*. These new metallic alloys whose diffraction patterns sharp spots with non-crystallographic symmetries are called *quasicrystals*. In my talk I am going to expose a mathematical approach to the theory of quasicrystals.

Let E be a finite dimensional Euclidean space which is called a *hyperspace*. Fix an orthonormal base $\mathbf{e}$ in E and consider the lattice M consisting of all vectors whose coordinates in the base $\mathbf{e}$ are integer. Suppose also that E has a *physical* subspace V such that $E = V \oplus V^{\perp}$. Denote by P the unit cube in E constructed from $\mathbf{e}$ such that the origin is one of its vertices. Put $K = P + V$ and assume that the origin does not belong to the boundary of K. A *quasi-crystal* $Q \subset V$ is the orthogonal projection of $K \cap M$ into V along $V^{\perp}$.

Theorem. *A quasi-crystal Q is a discrete subset in V. Let S be the unit disk in V. Then there exist finitely many quasi-crystals $Q' \subset V$ such that $Q \cap S = Q' \cap S$. Let X be a finite subset in Q such that some neighborhood of the inverse image of X in $K \cap M$ under the orthogonal projection $E \to V$ is contained in $K \cap M$. For any positive integer t there exists a vector $a \in K \cap M$ of a length at least t such that $X + a \subset Q$.*

According to this theorem we introduce the inverse semigroup $S(Q)$ of a quasicrystal Q as the set of affine transformations f of E such that there exist subsets $A, B \subset K \cap M$ such that

$f(A) = B$. The group of invertible elements of $S(Q)$ is the symmetry group Sym$Q$ of Q. In the talk I am going to speak about properties of $S(A)$ and Sym$Q$.

References

[1] On symmetries of quasicrystals. Contemp. Math. to appear in 2005, Proceedings of XV Colloquium Latinoamericano. de la Pena Ed.

[2] Le Ty Quok Thang, S. A. Piunikhin, V. A. Sadov. Geometry of quasi-crystals. Uspekhi Mat. Nauk. – 1993. – 48, N 1. – 41-102.

[3] Aragón G., Aragón J.,L., Davila F., Gomez A., Rodriguez M. A. Geometric Algebra with Applications in Science and Engineering. Eds. E. Bayro-Corrochano and G. Sobczyk Birkhäuser (Boston, 2001) pp.371-386.

Irreducible linear groups over a quaternion division algebra that contain a root subgroup

Evgenii L. Bashkirov
Belorussian State University of Informatics and Radioelectronics
kafvm@gw.bsuir.unibel.by

Sat 17:00, 101 A (3rd floor)

Let D be an associative division ring and n an integer, $n \geq 2$. If $a \in D$ and i, j are integers such that $1 \leq i \neq j \leq n$, then $t_{ij}(a)$ is a matrix of degree n all of whose diagonal entries are 1, the (ij)-position is a and zeros are everywhere else. If k is a subgroup of the additive group of D, then by a root k-subgroup of the general linear group $GL_n(D)$ we mean any subgroup of $GL_n(D)$ that is a conjugate in $GL_n(D)$ of the group of all matrices $t_{12}(a)$, $a \in k$.

Now let D be a quaternion division algebra over a field F of characteristic $\neq 2$. Let k be a subfield of F such that the extension F/k is algebraic. We describe irreducible subgroups of $GL_n(D)$ that contain a root k-subgroup.

Commutativity-or-finiteness conditions for rings

Howard E. Bell
Brock University
hbell@brocku.ca
Coauthors: Abraham A. Klein

Sat 16:30, 101 A (3rd floor)

We proved some years ago, with Franco Guerriero, that a periodic ring R must be either finite or commutative if it satisfies one of the following conditions:

(a) R has only finitely many noncentral subrings of zero divisors;

(b) every proper noncentral subring of zero divisors is finite.

We now discuss arbitrary rings satisfying (a) or (b), as well as rings having only finitely many noncentral subrings. The results represent joint work with Abraham A. Klein.

On injective hulls

Ladislav Bican
Charles University, Fakulty of Mathematics and Physics, Department of Algebra
bican@karlin.mff.cuni.cz

Sat 15:00, 101 A (3rd floor)

It follows immediately from the proof of the existence of the injective hull $E(M)$ of a module M, that an upper bound for the cardinality of $E(M)$ is $|M|^{|R|}$. On the other hand, over left noetherian rings the injective hull $E(M)$ has the same size as M whenever $|M| \geq \tilde{\mu}_0 = \max(|R|, \aleph_0)$. Denoting $\tilde{\mu} = \sup\{\mu_I \mid I \leq R\}$, where μ_I denotes the smallest cardinality of a set of generators of the left ideal I and I ranges through all the left ideals of the ring R, we put $\mu = \tilde{\mu}$ and $\mu_0 = \tilde{\mu}_0$ if $\tilde{\mu}$ is regular and $\mu_I < \tilde{\mu}$ for any left ideal I of R, and we put $\mu = \tilde{\mu}^+$ and $\mu_0 = \tilde{\mu}_0^+$ in the opposite case. The above estimation can be improved by showing that for a module M of the size $|M| = \lambda \geq \mu_0^{<\mu}$ the cardinality of $E(M)$ is at most $\lambda^{<\mu}$. As a corollary under the generalized continuum hypotesis we obtain that if M is an arbitrary module with $|M| = \lambda \geq 2^{\mu_0^+}$, where $\mu_0 = \max(|R|, \aleph_0)$, then $|E(M)| = |M| = \lambda$ whenever λ is a regular cardinal.

On varieties of semigroups of relations with the operation of reflexive double cylindrification

Dmitry Bredikhin
Saratov, Lermontova 7-22, 410002, Russia
bredikhin@mail.ru

Fri 17:00, ZS 1 (8th floor)

In the investigation of algebras of relations, one of the most important problems is to study their identities [Tarski 1941, Tarski 1953]. For any set Ω of operations on binary relations, let $R\{\Omega\}$ be the class of algebras whose elements are binary relations and whose operations are members of Ω, and let $Var\{\Omega\}$ be a variety generated by $R\{\Omega\}$.

We shall consider the operations of relation product $\circ$ and unary primitive positive operation [Börner-Pöschel 1991] of reflexive double cylindrification which is defined as follows:

$$\nabla(\rho) = \{(x, y) : (\exists z)(z, z) \in \rho\}.$$

The following theorem gives a basis of identities for the variety $Var\{\circ, \nabla\}$.

Theorem. The variety $Var\{\circ, \nabla\}$ is not finitely based. *An algebra* $(A, \cdot, ^\star)$ *of type* $(2, 1)$ *belongs to the variety* $Var\{\circ, \nabla\}$ *if and only if it satisfies the identities:*

$(xy)z = x(yz)$, $(x^\star)^2 = x^\star$, $x^\star x x^\star = x^\star$, $(x^\star y)^2 = x^\star y$, $(xy^\star)^2 = xy^\star$,
$(xy)^\star = (yx)^\star$, $x^\star xy = y^\star xy$, $xyy^\star = xyx^\star$, $x^\star yz^\star = z^\star yx^\star$,
$(xy^\star z)^\star = y^\star zxy^\star$, $x^\star yx^\star zx^\star = x^\star zx^\star yx^\star$, *and* $x^\star(x^p)^\star = x^\star$ *for any prime number* $p > 1$.

References

[1] Tarski A., On the calculus of relations. J. Symbolic Logic. 6(1941), pp.73 – 89.

[2] Tarski A., Some methodological results concerning the calculus of relations. J. Symbolic Logic 18 (1953), pp.188–189.

[3] Börner F. and Pöschel R., Clones of operations on binary relations. Contributions to general algebra 7. – Wien (1991), pp.50–70.

RAK: A new factoring algorithm

Gary P. Carter
Queensland University of Technology
g.carter@qut.edu.au

Sun 09:30, ZS 1 (8th floor)

The ability to factor large integers with few factors is at the heart of the security of many public key cryptosystems. Recent years have seen an upsurge in algorithm development for factoring large integers of the types used in modern public key cryptosystems. Algorithms are of two general types, namely special purpose and general purpose. Special purpose algorithms use properties of the numbers they are attempting to factor or properties of the factors of these numbers. General purpose algorithms on the other hand can be applied to factor any number. In this paper we introduce a new special purpose algorithm called RAK. We will show that RAK compares more than favourably with Fermat factorization, a commonly used algorithm after trial division has been tried, in factoring numbers of the form pq, p and q different primes. Like Fermat, RAK is more successful when the factors being sought are "close" but is able to factor numbers where the difference between the factors sought is 4 orders of magnitude larger. RAK can also be adapted to check for "special cases" and can be adapted for the cases where the number to be factored is of the form pqr or p^2q.

Cauchy complete l-ideals of a lattice ordered group

Štefan Černak
Technical University of Košice, Slovakia
Stefan.Cernak@tuke.sk

Sat 11:30, Diss (8th floor)

Vulikh has defined the notion of convergence of sequences with a regulator in a vector lattice V. A "Convergence regulator" depends on a sequence. This type of convergence was studied by Martinez and Koldunov in l-groups. Luxemburg and Zaanen introduced the notion of a convergence with a fixed regulator in V for all seqences in V.

In the present note the notion of convergence with a fixed regulator u (u-convergence) is examined in an Archimedean l-group G. The main results:

The Dedekind completion D(G) of G is u-Cauchy complete (C-complete) and a u-Cauchy completion C(G) of G is an l-subgroup of D(G).

The system of all C(b)-complete l-ideals of G has a greatest element.

An l-ideal of G generated by C-complete l-ideals of G need not be C-complete.

The system of all C-complete l-ideals of G containing a convergence regulator u has a greatest element.

Implication reducts of propositional logics

Ivan Chajda
Palacký University Olomouc
chajda@inf.upol.cz
Coauthors: Helmut Länger, Radomir Halaš, Jan Kühr

Fri 17:00, ZS 3 (7th floor)

We will present axiom systems in simple identities characterizing the logical connective "implication" in several logics of quantum mechanics and in a many-valued logic. We will compare these identities with those of the classical propositional calculus.

The number of automorphisms of finite cyclic or dihedral groups with a given number of fixed points

Mihai Chis
West University of Timisoara, Faculty of Mathematics and Computer Science, Timisoara, Romania
chis@mail.math.uvt.ro
Coauthors: Codruta Chis (University of Agricultural Sciences of Banat, Timisoara, Romania)

Sat 17:30, ZS 1 (8th floor)

In our paper, we determine the number of automorphisms of finite cyclic or dihedral groups, which have a given number of fixed points. We prove formulas for these numbers and deduce two identities concerning Eulers totient function.

Finitizing projection algebras

Jānis Cīrulis
University of Latvia, Riga, Latvia
jc@lanet.lv

Fri 16:30, ZS 1 (8th floor)

A projection operator, or cylindrification, on a Boolean algebra A is an additive closure operator whose range is a subalgebra of A. If T is a lattice, then a T-shaped projection algebra is defined to be an algebra $(A, p_t)_{t\in T}$ such that A is a Boolean algebra, each p_t is a projection operator on A, and, for all $s, t \in T$, $p_s p_t = p_{s\wedge t}$. For each T, the class of all T-shaped projection algebras is a variety, which is finitely based only if T is finite.

Given a projection algebra A, denote the range of p_t by A_t. The algebra A is said to be nested if A is the union of all A_t. The direct sum A^* of all subsets A_t is treated as an algebra of type $(2, 2, 1)$.

Let $\mathbf{P}$ stand for the class of all nestedprojection algebras with T arbitrary. We show that (1) the class $\mathbf{P}^*$ of all algebras A^* with A in $\mathbf{P}$ is axiomatizible by a small number of equations, (2) up to isomorphisms, the transformation $A \mapsto A^*$ is bijective; in fact, the classes $\mathbf{P}$ and $\mathbf{P}^*$ are categorically equivalent. Moreover, we describe explicitly a construction which restores (again, up to isomorphism) each A from A^*.

The axiomatizability of topological quasi-varieties

David M. Clark
State University of New York at New Paltz (REH 114, New Paltz, NY 12561 USA)
clarkd@newpaltz.edu
Coauthors: Brian A. Davey, Ralph S. Freese, Miroslav Haviar, Marcel Jackson, Jane G. Pitkethly, M. Rashed Talukder (on 3 related papers)

Fri 12:00, ZS 3 (7th floor)

A natural duality is a dual equivalence between an algebraic quasi-variety and topological quasi-variety. A profusion of natural dualities has led to a search for axiomatic descriptions of topological quasi-varieties. We find that, for a finitely generated topological quasi-variety, there are exactly three possibilities: among Boolean topological structures, it either consists of all models of its underlying universal Horn theory, of all models of some first order theory but no universal theory, or it is not first order axiomatizable at all. Term finite principle congruences, inverse limits and ultraproducts can be used to describe examples of each. For instance, a finite group, ring, semi-group or lattice generates a topological quasi-variety that is axiomatized by the universal Horn theory of its generator provided that it generates a quasi-variety that is a variety. In contrast, every finite lattice generates a topological quasi-variety that is first order definable, but not always universally definable. And the class of Boolean topological simple graphs is exactly the class of finitely continuously colorable graphs, but the class of continuously k-colorable graphs is not first order definable at all.

Types of universality of some varieties close to bands

Marie Demlová
Czech Technical University in Prague
demlova@math.feld.cvut.cz
Coauthors: V. Koubek

Fri 16:00, Diss (8th floor)

During the last decades universality and recently weaker versions of universality were studied for varieties and quasivarieties of algebras. It is known that alg-universality excludes α-determinancy for any cardinal α. This is not true for all weaker versions of universality. On the other hand, Adams and Dziobiak [AD] showed connections between finite-to-finite alg-universality and Q-universality (introduced by Sapir in [S]) by proving:

Theorem 1: *Any finite-to-finite alg-universal quasivariety of algebraic systems is Q-universal.*

When studying these notions for semigroup varieties, the authors of the abstract showed that an important role is played by three finite semigroups M_1, M_2 and M_3. (M_1 is a non-commutative semigroup with three elements 1, a and 0, where $1 \cdot x = x$, else $y \cdot x = 0$; M_2 is a commutative semigroup with elements $a, b, c, 0$ where $a \cdot b = b \cdot a = c$ else $x \cdot y = 0$; M_3 is a non-commutative semigroup with elements a, b, c, d where a, b, c are left zeros and $d \cdot c = b$, else $d \cdot x = a$.)

In [DK1], [DK2] there is proved:

Theorem 2: *The variety $VAR(M_1)$ generated by M_1 is not (weakly) var-relatively universal and is 3-determined.*

Theorem 3: *The varieties $VAR(M_2)$, $VAR(M_3)$ and $VAR(D(M_3))$ ($D(M_3)$ is the dual of M_3) are var-relatively universal, Q-universal and α-determined for no cardinal α.*

Hence varieties $\mathcal{V}$ (called *remarquable varieties*) for which $M_2, M_3, D(M_3) \notin \mathcal{V}$ are of special importance.

In the talk remarquable varieties will be treated and results will be presented concerning var-relative universality, Q-universality and α-determinancy of such varieties.

References

[AD] M. E. Adams and W. Dziobiak, *Finite-to-finite universal quasivarieties are Q-universal*, Algebra Universalis **46** (2001), 253-283.

[DK1] M. Demlová and V. Koubek, *Weaker universalities in semigroup varieties*, Proceedings of NSAC03, Novi Sad J. Math. **34** (2004), 37-86.

[DK2] M. Demlová and V. Koubek, *Weak alg-universality and Q-universality of semigroup quasivarieties*, to appear in Comment. Math. Unive. Carolin.

[S] M. V. Sapir, *The lattice of quasivarieties of semigroups*, Algebra Universalis **21** (1985), 172-180.

Non-deterministic hypersubstitutions

Klaus Denecke
Universität Potsdam, Institut für Mathematik
kdenecke@rz.uni-potsdam.de
Coauthors: P. Glubudom, J. Koppitz

Sat 14:00, ZS 1 (8th floor)

Hypersubstitutions map operation symbols to terms of the corresponding arity. Any hypersubstitution can be extended to a mapping defined on the set $W_\tau(X)$ of all terms of type τ. If $\sigma : \{f_i \mid i \in I\} \to W_\tau(X)$ is a hypersubstitution and $\hat{\sigma} : W_\tau(X) \to W_\tau(X)$ its canonical extension, then the set

$$T_\sigma := \{(t, \hat{\sigma}[t]) \mid t \in W_\tau(X)\}$$

is a tree transformation where the original language and the image language are of the same type. Tree transformations of the type T_σ can be produced by tree transducers. Here $T_{\hat{\sigma}}$ is the graph of the function $\hat{\sigma}$. Non-deterministic tree transducers produce tree transformations which are not graphs of some functions. If such tree transformations have the form T_σ, then σ is not longer a function. Therefore, there is some interest to study *non-deterministic hypersubstitutions.* That means, there are operation symbols which have not only one term of the corresponding arity as image, but a set of such terms. To define the extensions of non-deterministic hypersubstitutions, we have to extend the superposition operations for terms to a superposition defined on sets of terms. Let $\mathcal{P}(W_\tau(X_n))$ be the power set of the set of all n-ary terms of type τ. Then we define a superposition operation

$$\hat{S}_m^n : \mathcal{P}(W_\tau(X_n)) \times (\mathcal{P}(W_\tau(X_m)))^n \to \mathcal{P}(W_\tau(X_m))$$

and get a heterogeneous algebra

$$\mathcal{P}\text{-clone}\tau := ((\mathcal{P}(W_\tau(X_n))_{n\in\mathbb{N}^+}, (\hat{S}_m^n)_{m,n\in\mathbb{N}^+}, (\{x_i\})_{i\leq n, n\in\mathbb{N}^+}),$$

which is called the *power clone* of type τ. We prove that the algebra $\mathcal{P}$-cloneτ satisfies the well-known clone axioms (C1), (C2), (C3), where (C1) is the superassociative law. It turns out that the extensions of non-deterministic hypersubstitutions are precisely the endomorphisms of the heterogeneous algebra $\mathcal{P}$-cloneτ.

Collapsing inverse monoids

Miklós Dormán
University of Szeged, Szeged, Hungary
dorman@math.u-szeged.hu

Sat 12:00, ZS 3 (7th floor)

We investigate a class of maximal inverse transformation monoids constructed from finite lattices, and describe a necessary and sufficient condition for such a transformation monoid to be collapsing.

Polynomial permutations on bounded lattices with an antitone involution

Dietmar Dorninger
TU Wien
d.dorninger@tuwien.ac.at
Coauthors: H. Länger

Sat 11:30, ZS 1 (8th floor)

Motivated by cryptography we study permutations on bounded lattices with an antitone involution, i. e. with an involutory antiautomorphism, which are induced by polynomials. We first investigate some properties of such lattices, in particular, we prove a factorization theorem generalizing that holding for ortholattices, then we characterize a set of involutory polynomial permutations and finally we prove that for de Morgan algebras this set already exhausts all possible polynomial permutations. The central role play elements that are defined in the same way as central elements in orthomodular lattices except for the fact that the commuting relation is not assumed symmetric and an antitone involution is not an orthocomplementation in general.

On the existence of states for linear pseudo BL-algebras

Anatolij Dvurečenskij
Mathematical Institute, Slovak Academy of Sciences, Bratislava
dvurecen@mat.savba.sk
Coauthors: Marek Hyčko

Fri 11:30, ZS 1 (8th floor)

Pseudo BL-algebras are non-commutative generalizations of BL-algebras. They include pseudo MV-algebras as well as MV-algebras. As it was shown by the first author, there are pseudo MV-algebras which do not admit any state. However, every linearly ordered MV-algebra does.

We solve an open problem whether a linear pseudo BL-algebra admits a state. We show that the answer is positive under very natural conditions.

Splittings of lattices of theories and unification types

Wojciech Dzik
Institute of Mathematics, Silesian University
dzikw@silesia.top.pl

Sat 14:00, 101 A (3rd floor)

We will show that for some equational theories T there is a splitting of the lattice L(T) of all subtheories of T into two parts: A and B. In the part A all theories having unitary unification type are situated plus some having nullary unification type. The part B contains all theories having unification type ω plus some having nullary unification type (plus all theories having unification type ∞, if there are such).
This holds in particular if one takes for T the theory of all Heyting algebras or the theory of all topological Boolean algebras (or closure algebras).
It is known that any equational theory can have one of the four unification types: unitary (1), ω, ∞ or nullary (0).

Pseudocomplementation — Old and New

Marcel Erné
Institut für Mathematik, Universität Hannover
erne@math.uni-hannover.de

Fri 14:00, main building

In an ordered set with top element $\top$, an element is the (lower) pseudocomplement of an element a if it is the least element having no other common upper bound with a than $\top$. Classical examples of pseudocomplemented lattices are Boolean lattices, coframes (in particular, all lattices of closed sets in topological spaces), and completely join-semidistributive lattices.

In the first part of the talk, we shortly review the historical development of the theory of pseudocomplementation in lattices and ordered sets, starting with the old controversy between Schröder and Peirce about the provability of the distributive law, passing to the Glivenko-Frink construction of the skeleton for pseudocomplemented structures, and ending with modern aspects of pseudocomplements in pointfree topology and formal concept analysis.

In the second part, we show that, somewhat surprisingly, a great part of the prime decomposition theory for distributive lattices or (co)frames remains valid in the rather general setting of pseudocomplemented posets. Various decomposition theorems for topological spaces, ordered sets and diverse algebraic or combinatorial structures are immediate consequences.

Finally, we touch upon some set-theoretical aspects, showing that a wealth of prime or maximal ideal theorems and related choice principles follows from the corresponding facts in the very restricted classical setting of power set lattices, and that in some sense the maximal class of ordered structures in which such ideal theorems hold are again the pseudocomplemented ones, or slight variants of them.

Lying over in near-ring extensions

Mark Farag
Dept. of Mathematics, Wagner College, Staten Island, New York, USA
mfarag@wagner.edu

Fri 17:00, 101 A (3rd floor)

Among the most important examples of extensions in ring theory are matrix, polynomial, and group rings. Although straightforward attempts to generalize these extensions to near-rings fail to yield near-ring structures in general, near-ring theorists have studied methods of constructing matrix, polynomial, and group near-rings that reduce to the known extensions in case the base near-ring is a ring. These near-ring extensions share the characteristic of being defined via function spaces. In this talk, we provide a unifying framework for matrix, polynomial, and group near-rings. We provide structural results in this general context; in particular, we prove a new "lying over" result.

The independence of the conditions in Rado's generalization of Hall's marriage theorem

Jonathan Farley
Harvard University
lattice@math.harvard.edu

Sun 09:00, ZS 3 (7th floor)

A *restricted Boolean polynomial* $\rho(x_1, \ldots, x_n)$ is a finite expression involving $x_1, \ldots, x_n$ (variables that range over sets) formed by means of unions and intersections. Let $\mathcal{R}$ be a class of pairwise inequivalent restricted Boolean polynomials. It is shown that the conditions

$$|\rho(A_1, \ldots, A_n)| \geq |\rho(B_1, \ldots, B_n)| \quad (\rho \in \mathcal{R})$$

are independent. That is, given $\rho \in \mathcal{R}$, there exist sets $A_1, \ldots, A_n, B_1, \ldots, B_n$ such that the condition

$$|\sigma(A_1, \ldots, A_n)| \geq |\sigma(B_1, \ldots, B_n)|$$

holds for all $\sigma \in \mathcal{R}$ where σ is not equivalent to ρ, but

$$|\rho(A_1, \ldots, A_n)| < |\rho(B_1, \ldots, B_n)|.$$

This solves a problem (attributed to Rado) from Mirsky's 1971 text *Transversal Theory*.

Relations between lattice-properties

Ervin Fried
ELTE Budapest, Hungary
efried@cs.elte.hu

Fri 11:30, Diss (8th floor)

It is well-known that for lattices both associativities are equivalent to the transitivity of the corresponding partially ordered set. It is also well-known that both distributivities are equivalent to the medial identity. We shall prove that "in general" this is not the case. Some related topics will be investigated. As a frame we shall omit all the lattice identities except the eight(!) absorption laws. This is enough to represent the structure (which will be called weak lattice) as a relational system.

Orderings and groups: a survey of recent results.

A.M.W. Glass
Queens' College, University of Cambridge, UK
A.M.W.Glass@dpmms.cam.ac.uk

Fri 09:15, main building

I will give a survey of some of the most exciting recent results in the subject, restricting myself to those advances that every intelligent algebraist should know.

Weak isomorphisms, equivalent hypersubstitutions and Mal'tsev correspondence

Kazimierz Głazek
University of Zielona Góra
k.glazek@wmie.uz.zgora.pl
Coauthors: Dietmar Schweigert

Sun 09:30, 101 A (3rd floor)

The Mal'tsev correspondence for Lie algebras allows under some conditions to pass from Lie-theoretic problems to group theoretic ones and vice versa. This correspondence can be approached in several ways. We suggest the way by using hypersubstitutions and we can transfer the Lie algebras and the Lie groups and varieties over them by weak isomorphisms.

M-hyperquasi-equational logic

Ewa Graczyńska
Technical University of Opole, Poland
egracz@po.opole.pl
Coauthors: Dietmar Schweigert

Fri 17:30, 101 A (3rd floor)

In [GS 2004] we considered the notion of M-hyper-qusivariety and proved several Birkhoff Mal'cev type theorems. The aim of my talk is to present a solution of problem 32 of the monograph [DW 2000] by presenting derivation rules for M-hyperquasi-equational logic, for a given monoid M of hypersubstitutions of a given type. We generalize some results of [G 2003] and discuss properties between the operators H, S, P and D_M and the derivation rules of quasiequational logic and so called M-hypersubstitution. We show some similarities with classical results.

References

[DW 2000] Klaus Denecke and Shelley L. Wismath, *Hyperidentities and clones*, Algebra, Logic and Applications, Gordon and Breach Science Publishers 2000, ISBN 90-5699-235-X, ISSN 1041-5394.

[G 2003] Ewa Graczyńska, *Algebras and coalgebras*, Opole 2003. ISSN 1429-6063, ISBN 83-88492-25-X

[GS 2004] Ewa Graczyńska and Dietmar Schweigert, *M-hyperquasivarieties*, arXiv:math.GM/0412245 v2, 16 Dec. 2004.

Sectionally pseudocomplemented semilattices

Radomír Halaš
Dept. of Algebra and Geometry, Palacký University Olomouc
halas@inf.upol.cz
Coauthors: Jan Kühr

Sat 11:00, ZS 1 (8th floor)

We present a simple axiomatic system for semilattices having sections which are pseudocomplemented lattices. With respect to this approach the class of sectionally pseudocomplemented semilattices forms a variety. We describe all SI members of this variety.

When is a full duality strong?

Miroslav Haviar
M. Bel University, Banska Bystrica, Slovakia
haviar@pdf.umb.sk
Coauthors: Brian A. Davey, Todd Niven

Fri 11:30, ZS 3 (7th floor)

The relationship between full and strong dualities in the theory of natural dualities is not yet understood. Our aim is to present partial solutions to the *Full versus Strong* Problem, which asks if every full duality is necessarily strong.

We introduce local versions of this problem and prove that they have affirmative solutions for full dualities based on an arbitrary finite algebra in the four well-known classes of algebras: abelian groups, semilattices, relative Stone Heyting algebras and bounded distributive lattices. Along the way we present some useful additions to the general theory.

Maximal cyclic subgroups and prime divisors in finite groups

Wolfgang Herfort
Institute for Analysis and Scientific Computing
w.herfort@tuwien.ac.at
Coauthors: Zvi Arad

Sat 12:00, Diss (8th floor)

Let G be a finite group with no chief factor simple of Lie type $E_8(q)$ and C a cyclic subgroup of largest order in G. Using the CFSG, it is shown that at most two primes in the open interval $([|C|/2], |C|)$ divide $|G|$.

Order affine completeness of lattices

Kalle Kaarli
Institute of Pure Mathematics, University of Tartu
kaarli@math.ut.ee
Coauthors: Vladimir Kuchmei

Sat 17:30, ZS 3 (7th floor)

When we started this work, our aim was to describe locally order affine complete modular lattices of finite height. The general problem easily reduced to the case of subdirect products of two simple lattices. Quite surprisingly, it turned out that in this special case the description can be obtained even without the modularity assumption. Our main result is the following.

Theorem. *Let L be a nontrivial subdirect product of simple lattices L_1 and L_2, both of finite height. The lattice L is locally order affine complete if and only if both L_1 and L_2 are tolerance trivial and one of the following cases holds:*

(1) $L = L_1 \times L_2$;

(2) *L is a maximal sublattice of $L_1 \times L_2$;*

(3) *L is the intersection of two maximal sublattices of $L_1 \times L_2$, one containing $(0,1)$ and other $(1,0)$.*

Prime ideals in the near-ring of formal power series

Hermann Kautschitsch
Universität Klagenfurt, Department of Mathematics
hermann.kautschitsch@uni-klu.ac.at

Fri 11:30, 101 A (3rd floor)

In this talk a review of all prime ideals in the near-ring of formal power series over a commutative ring R with 1 with respect to addition and composition is given and the connection to ideals of R is shown.

M-solid varieties of n-semigroups

Jörg Koppitz
University Potsdam
koppitz@rz.uni-potsdam.de

Sat 14:30, ZS 1 (8th floor)

Using the concept of an M-solid variety of a given type τ, for a monoid M of hypersubstitutions of type τ, introduced by Graczynska and Schweigert in 1990, one can get a better description of the complete lattice of all varieties of that type τ. This was already done for varieties of semigroups, varieties of groups, and varieties of semirings. We will consider varieties of n-semigroups and especially varieties of 3-semigroups.
A 3-semigroup $(S;\cdot)$ is a set with a ternary operation $\cdot$, satisfying the 3-superassociative law: $(x_1x_2x_3)x_4x_5 \approx x_1(x_2x_3x_4)x_5 \approx x_1x_2(x_3x_4x_5)$. We give a characterization of all *Pre*-solid varieties of 3-semigroups and determine M-solid varieties of n-semigroups for $n \geq 4$ and for several monoids M of hypersubstitutions of type $\tau = (n)$ (an n-semigroup is defined by the n-superassociative law).

On skew formal power series

Werner Kuich
Technische Universität Wien
kuich@tuwien.ac.at

Fri 11:00, 101 A (3rd floor)

We investigate the theory of skew formal power series introduced by Droste and Kuske. We show some Kleene Theorems for skew formal power series, whose supports contain finite and infinite words.

The Membership Problem and the equational bound

Gábor Kun
Eötvös University, Budapest
kungabor@cs.elte.hu
Coauthors: Vera Vertesi

Sun 10:30, ZS 3 (7th floor)

The computational complexity of algebraic questions plays an important role in the last years. The Membership problem for a given variety ν asks whether a finite algebra B belongs to ν. In the sequel ν is assumed to be generated by a single finite algebra A. Székely has constructed an algebra A such that the corresponding Membership Problem is NP-complete. It is not known whether the Membership Problem is always in NP.

Varieties are equational classes. To get a decision we may test some or all identities of the variety in B. In the case when A is a finite group we should check only finitely many identities. The equational bound or β-function is a measure of the complexity of the Membership Problem in some sense. $\beta(n)$ is the minimum length of equations sufficient to check to determine that an n-element algebra is in the variety or not. This function exists and it is recursive. The construction of the free algebra shows that it is at most triple-exponential. Székely has constructed an algebra A for which the β-function is at least sublinear. In this talk we investigate the β-function for hypergraph algebras. We prove that the order of magnitude of the β-function can be a polynomial of arbitrary degree.

Weak Boolean products of bounded (dually) residuated lattices

Jan Kühr
Palacký University Olomouc, Czech Republic
kuhr@inf.upol.cz
Coauthors: Jiří Rachůnek

Fri 12:00, ZS 1 (8th floor)

We deal with weak Boolean products of certain bounded dually residuated lattices (DRl-monoids) that are a natural generalization of pseudo MV-algebras (GMV-algebras). Among others, we show that every non-trivial bounded DRl-monoid is a weak Boolean product of directly indecomposable DRl-monoids.

Hereditary generalized Boolean quasirings, MV-algebras and de Morgan algebras

Helmut Länger
Institute of Discrete Mathematics and Geometry, Vienna University of Technology
h.laenger@tuwien.ac.at
Coauthors: Ivan Chajda

Sun 11:00, 101 A (3rd floor)

Generalized Boolean quasirings were introduced as generalizations of Boolean rings corresponding to bounded lattices with an antitone involution. We define a modification of these quasirings which is in a bijective correspondence to MV-algebras. Moreover, we characterize distributivity conditions in ring-like structures corresponding to de Morgan algebras.

On subfunctions of Boolean functions

Erkko Lehtonen
Tampere University of Technology, Institute of Mathematics
erkko.lehtonen@tut.fi

Sun 09:30, ZS 3 (7th floor)

Various notions of subfunctions (or minors) of Boolean functions have been presented in the literature. In general outline, a Boolean function f is called (some variant of) a subfunction of a Boolean function g, if f can be obtained by substituting variables, negated variables, or constants (or some subset thereof) for arguments of g. These conditions can be rephrased in terms of functional composition: f is a subfunction of g, if $f = g(h_1, \ldots, h_n)$ where the inner functions h_i belong to one of the smallest Boolean clones that contain only variables, negated variables, or constant functions.

We generalize the notion of subfunction in a natural way. Let $\mathcal{C}$ be any class of Boolean functions. We say that f is a *$\mathcal{C}$-subfunction* of g, denoted $f \leq_{\mathcal{C}} g$, if $f = g(h_1, \ldots, h_n)$, where all the inner functions h_i belong to $\mathcal{C}$. Two functions are *$\mathcal{C}$-equivalent,* denoted $f \equiv_{\mathcal{C}} g$, if they are $\mathcal{C}$-subfunctions of each other. The relation $\leq_{\mathcal{C}}$ is a preorder on the set Ω of all Boolean functions if and only if $\mathcal{C}$ is a clone. If $\mathcal{C}$ is a clone, $\equiv_{\mathcal{C}}$ is an equivalence relation, and, as for preorders, the $\mathcal{C}$-subfunction relation induces a partial order $\preceq_{\mathcal{C}}$ on the quotient set $\Omega/\equiv_{\mathcal{C}}$.

Given the partially ordered set $(\Omega/\equiv_{\mathcal{C}}, \preceq_{\mathcal{C}})$, two questions arise immediately. First, is the descending chain condition satisfied? Second, what is the size of the largest antichain of incomparable functions in the sense that they are not $\mathcal{C}$-subfunctions of each other? We present an overview of the topic and some of our results.

Finitely arithmetically fixed elements of a field

Günter Lettl
Institut für Mathematik, Karl-Franzens-Universität Graz, Heinrichstraße 36, Österreich
guenter.lettl@uni-graz.at

Sat 11:00, Diss (8th floor)

We call an element r of a field L "finitely arithmetically fixed (f.a.f.)" if there exists a non-empty finite subset A of L containing r, such that any map f from A to L, which "behaves like a homomorphism" on A, leaves r fixed.

Recently A. Tyszka showed that the f.a.f. elements of the field of real (or p-adic) numbers are just the algebraic ones.

We generalize the notion of f.a.f. to relative extensions and present several results, which also yield an alternative proof of Tyszka's theorem.

Properties of linear compactifications of topological abelian groups

Andrei Loriana
Department of Mathematics, University of Oradea, Romania
dalb@uoradea.ro

Fri 17:00, Diss (8th floor)

For any topological abelian group (A, τ) we consider the group topology τ_0, having a fundamental system of 0 consisting of open subgroups V of (A, τ) such that the quotient group A/V satisfies D.C.C. for subgroups. In the case when τ is a discrete topology on A, we will denote (A, τ_0) briefly by $A^{\#}$ (as in the case of Bohr topology for A).

We will expose some elementary properties of groups of type $A^{\#}$. We have proved, for example, that when $|A| > \omega$, the group $A^{\#}$ is not Baire. When A is a ring, the ring operations of A can be extended to the completion $\widehat{A^{\#}}$ of A such that $\widehat{A^{\#}}$ becomes a right topological ring whose additive group is linearly compact.

A note on polynomial interpolation in Mal'cev algebras

Dragan Mašulović
Department of Mathematics and Informatics, University of Novi Sad, Trg Dositeja Obradovića 4, 21000 Novi Sad, Serbia and Montenegro
masul@im.ns.ac.yu
Coauthors: Erhard Aichinger (Johannes Kepler University, Linz, Austria) and Reinhard Pöschel (Dresden University of Technology, Dresden, Germany)

Sat 11:00, ZS 3 (7th floor)

A classical result in near-ring theory tells that the 4-interpolation property implies the n-interpolation property for all positive integers n. In the present note we show that the same holds in a more general setting which includes clones containing a Mal'cev operation and we provide three short proofs for this generalization. We also give an estimate of the complexity of interpolation in this setting.

A topological property of polynomial functions on some general linear groups

Peter Mayr
Department of Algebra, Universität Linz, Austria
peter.mayr@jku.at
Coauthors: Günter Landsmann, Josef Schicho

Sun 09:30, Diss (8th floor)

A function from a group to itself is called polynomial if it can be written as some product of constant functions, the identity function, and the function that maps every element to its inverse.

On arbitrary general linear groups we characterize the locally polynomial functions. These are the functions that can be interpolated by a polynomial function on any given finite set of points. For the automorphism group of the vector space of dimension 2 over the reals, we give a necessary topological condition for a function to be polynomial. As a consequence, we obtain that transposition is locally polynomial but not polynomial.

Density in residuated lattices

George Metcalfe
Technical University Vienna
metcalfe@logic.at
Coauthors: Franco Montagna

Sat 12:00, 101 A (3rd floor)

We describe a uniform strategy for proving that a class of residuated lattices obeying prelinearity is generated by its dense linearly ordered members, and hence that the corresponding fuzzy logics are complete with respect to algebras based on the unit interval [0,1]. The strategy consists of two parts. First, it is shown that derivability in a logic extended with the Takeuti-Titani density rule is equivalent to validity in all dense linearly ordered members of the corresponding class of algebras. A syntactic elimination of the density rule from the logic is then given using hypersequents.

On the definability of a planar automaton by its semigroup of input symbols

Vladimir Molchanov
Saratov State University, Astrakhanskaya Str.,83, Saratov, 410071, Russia
MolchanovVA@saratov.fio.ru

Sat 14:30, Diss (8th floor)

In recent years there has been considerable interest in the investigation of automata in which the state set and the exit set are objects of some category **K** (see, for example, a survey in [Plotkin,Greenglas,Gvaramiya1]). We investigate this kind of automata when **K** is the category of projective plane together with homomorphisms. The purpose of this talk is to investigate the interplay between the algebraic structure of such an automaton and its semigroup of input signals.

Following [Plotkin,Greenglas,Gvaramiya], by an automaton we mean a system $A = (S, \Gamma, B, \delta, \lambda)$ consisting of a state set S, a semigroup Γ of input signals, a set B of output signals, a transition function $\delta : S \times \Gamma \to S$ and an exit function $\lambda : S \times \Gamma \to B$ such that $\delta(\gamma_1\gamma_2) = \delta(\gamma_2) \circ \delta(\gamma_1)$ for any $\gamma_1, \gamma_2 \in \Gamma$. For every $\gamma \in \Gamma$, define the mappings $\delta_\gamma : S \to S$, $\lambda_\gamma : S \to B$ by $\delta_\gamma(s) = \delta(s, \gamma)$, $\lambda_\gamma(s) = \lambda(s, \gamma)$ $(s \in S)$.

An automaton $A = (S, \Gamma, B, \delta, \lambda)$ is said to be planar if its sets S and B are endowed with a structure of projective planes such that, for any $\gamma \in \Gamma$, the mappings δ_γ, λ_γ are homomorphisms. For any projective planes S, B the universal planar automaton $\mathrm{Atm}(S, B)$ is the system $\mathrm{Atm}(S, B) = (S, \mathrm{End(S)} \times \mathrm{Hom}(S, B), B, \delta, \lambda)$, where $\mathrm{End}(S)$ is the endomorphism semigroup of S, $\mathrm{Hom}(S, B)$ is the set of all homomorphisms from S to B and, for every $s \in S$, $(\varphi, \psi) \in \mathrm{End}(S) \times \mathrm{Hom}(S, B)$, $\delta(s, (\varphi, \psi)) = \varphi(s)$, $\lambda(s, (\varphi, \psi)) = \psi(s)$. Obviously, for any planar automaton $A = (S, \Gamma, B, \delta, \lambda)$, there exists the unique homomorphism of A to the universal planar automaton $\mathrm{Atm}(S, B)$.

The solution of the well-known problem by L.Gluskin and L.Skornyakov on definability of projective planes by their endomorphism semigroups (see, for example, [Molchanov]) states that any universal planar automaton without output signals is determined up to isomorphism by its semigroup of input signals. We extend this result on universal planar automata in the following direction.

Theorem. *For any universal planar automata* $\mathrm{Atm}(S_1, B_1)$, $\mathrm{Atm}(S_2, B_2)$ *the following statements are equivalent:*

(1) *the automata* $\mathrm{Atm}(S_1, B_1)$, $\mathrm{Atm}(S_2, B_2)$ *are isomorhpic;*

(2) *the projective planes* S_1 *and* B_1 *are isomorphic respectively to the projective planes* S_2 *and* B_2;

(3) *the semigroups of input signals of the automata* $\mathrm{Atm}(S_1, B_1)$, $\mathrm{Atm}(S_2, B_2)$ *are isomorphic.*

Applications of this result to the theory of planar automata are considered.

References

[1] B.I. Plotkin, L.Y. Greenglas, A.A. Gvaramiya, *Elements of algebraic automaton theory*, Moscow, High School, 1994. (Russian).

[2] V.A.Molchanov, *Semigroups of mappings on graphs*, Semigroup Forum **27** (1983), 155–199.

Permutation polynomials based on multivariate rational functions

Willi More
Institut für Mathematik, Universität Klagenfurt
willi.more@uni-klu.ac.at

Sun 09:00, ZS 1 (8th floor)

Multivariate rational functions which are invertable with respect to a certain composition can be used to describe permutation polynomials over finite fields. Properties, examples and some recent results are presented in this talk.

Stone duality for Dedekind sigma-complete lattice-ordered groups with order-unit

Daniele Mundici
University of Florence, Italy
mundici@math.unifi.it
Coauthors: Roberto Cignoli

Sat 09:00, main building

Building on the Goodearl-Handelman-Lawrence functional representation theorem, we provide a purely topological representation (specifically, a categorical duality) for a large class of Dedekind sigma-complete lattice-ordered groups G with order-unit u, including all G where u has a finite index of nilpotence. Our duality is a far-reaching generalization of the well known Stone duality between sigma-complete Boolean algebras and basically disconnected compact Hausdorff spaces.

Computation in orthomodular lattices

Mirko Navara
Faculty of Electrical Engineering, Czech Technical University, Praha, Czech Republic
navara@cmp.felk.cvut.cz

Sat 11:00, 101 A (3rd floor)

Because of non-distributitivity, symbolic computation in orthomodular lattices is rather difficult. Nevertheless, there are techniques which allow it at least in some special cases (see [G, MP, N]). These allowed to implement algorithms which can simplify or compare formulas in orthomodular lattices [HN,MP]. We discuss the possibilities and limitations of the use of computer algebra in this field.

[G] Greechie, R.J.: On generating distributive sublattices of orthomodular lattices. Proc. Amer. Math. Soc. 67 (1977), 17-22.

[HN] Hyčko, M., Navara, M.: Decidability in orthomodular lattices. Submitted.

[MP] Megill, N.D., Pavičić, M.: Orthomodular lattices and a quantum algebra. Internat. J. Theoret. Phys. 40 (2001), 1387-1410.

[N] Navara, M.: On generating finite orthomodular sublattices. Tatra Mt. Math. Publ. 10 (1997), 109-117.

Power-hereditary congruence lattices

Péter P. Pálfy
Eötvös University, Budapest, Hungary
ppp@cs.elte.hu

Sat 14:00, ZS 3 (7th floor)

Let us call a congruence lattice $L = Con(A; F)$ power-hereditary, if every 0-1 sublattice of L^n in $Eq(A^n)$ is the congruence lattice of a suitable algebra on A^n. John Snow showed that $Eq(3) = M_3$ is power-hereditary. Pál Hegedüs and I proved that certain gluings of M_3's can also be represented as power-hereditary congruence lattices, in particular $Con(Z_2 \times Z_2) = M_3$ is power-hereditary. John Snow has recently obtained that every congruence lattice representation of the pentagon N_5 is power-hereditary. In contrast, I will construct a congruence lattice representation of M_3 which is not power-hereditary.

The general prime ideal theorem

Jan Paseka
Dept. of Mathematics, Masaryk University Brno, Janáčkovo nám. 2a
paseka@math.muni.cz

Sun 10:30, 101 A (3rd floor)

A useful separation lemma for partial cm-lattices is proved equivalent to **PIT**, the Prime Ideal Theorem. The relation of various versions of the Lemma to each other and to **PIT** is also explored. The General Prime Ideal Theorem is formulated and proved to be equivalent to the **PIT**.

On the t-vertex condition for strongly regular graphs

Christian Pech
TU Dresden
pech@math.tu-dresden.de

Sun 11:00, Diss (8th floor)

The structure of Tarski-clones of operations on binary relations was studied by Mašulović and Pöschel. The binary relation that is obtained as result of some Tarski-operation on binary relations can be obtained by testing the existence of certain types of subgraphs in a colored graph.

Here we are interested not only in the existence of certain subgraphs but also in their number. In particular, we are interested in such graphs where the number of given subgraphs with a fixed edge or non-edge does not depend on the chosen edge or non-edge, respectively. E.g., strongly regular graphs (*srg*s) are simple regular graphs with the property that the number of common neighbors of a pair of vertices depends only on whether or not the two vertices are connected by an edge. Examples of such graphs are given by the orbitals of rank-3-permutation groups. However, most *srg*s do not arise in this fashion. One open problem in algebraic combinatorics is to give a combinatorial characterization of *srg*s that come from rank-3-groups. The t-vertex condition is a candidate for such a combinatorial characterization. An *srg* is said to fulfill the t-vertex-condition if the number of subgraphs with $\leq t$ vertices of a given isomorphism type over a fixed pair of vertices is only depending on whether the vertices are connected by an edge or not. It was conjectured that there is a number t_0 such that an *srg* arises from a rank-3-group if and only if it fulfills the t_0-vertex-condition. In order to attack this conjecture it is necessary to have good methods for deciding weather a given *srg* fulfills the t-vertex-condition.

In this talk a basis of isomorphism types of graphs is characterized such that in order to test the t-vertex-condition for an *srg* it suffices to test it for the types from the basis.

Local methods for traces of maximal clones

Maja Pech
Department of Mathematics and Informatics, University of Novi Sad, Serbia and Montenegro
maja@im.ns.ac.yu

Sat 11:30, ZS 3 (7th floor)

In this talk the characterization of the inclusions between traces of maximal clones will be completed. It turns out that the remaining cases can be solved using similar techniques. In particular, it is not essential how a relation looks globally, but it is sufficient to have local knowledge. This approach will be described for bounded partial orders, central and h-regular relations.

Complex condition in algebras of subalgebras

Agata Pilitowska
Warsaw University of Technology, Warsaw, Poland
irbis123@o2.pl
Coauthors: Kira Adaricheva (Harold Washington College, Chicago, US), David Stanovsky (Charles University, Prague, Czech Republic)

Sat 17:30, 101 A (3rd floor)

The complex (power or global) algebra (AUS, F) of sets of an algebra (A, F) is the family of all non-void subsets of A with operations of complex f-products given for each n-ary operation $f \in F$ and every $A_1, \ldots, A_n \subseteq A$, by

$$f(A_1, \ldots, A_n) = \{f(a_1, \ldots, a_n) | a_i \in A_i\}.$$

If instead of all subsets of A we will consider only the set AS of all non-empty subalgebras of (A, F), we may obtain the so called *complex algebra of subalgebras* (AS, F). But, in general, the algebra (AS, F) is not always defined. If AS is a subalgebra of (AUS, F) for every algebra A in the variety V, we denote VS the variety generated by all (AS, F), where $(A, F) \in V$.

We say that an algebra (A, F) satisfies the *complex condition*, if for every n-ary $f \in F$ and m-ary $g \in F$ there exist m-ary terms $t_1, \ldots, t_n$ such that the identity

$$g(f(x_{11}, \ldots, x_{n1}), \ldots, f(x_{1m}, \ldots, x_{nm})) = f(t_1(x_{11}, \ldots, x_{1m}), \ldots, t_n(x_{n1}, \ldots, x_{nm}))$$

holds in A. VS is defined if and only if V satisfies the complex condition. The entropic law is a special case of the complex condition, where the terms $t_1, \ldots, t_n$ are equal to g.

We investigate the relationship between the complex condition and the entropic law. In general, the two properties are different. But under additional assumptions they are equivalent, for instance in commutative groupoids, groupoids with a unit element or in idempotent semigroups.

Refinable decomposition systems in distributive semilattices

Miroslav Ploščica
Šafárik University, Košice, Slovakia
ploscica@science.upjs.sk

Sat 14:30, ZS 3 (7th floor)

This research is connected with the problem of characterizing the congruence lattices of various kinds of algebras, especially with the well known Congruence Lattice Representation Problem: *Is every algebraic distributive lattice isomorphic to the congruence lattice of some lattice?*

We show that, for a large class of lattices, the semilattices of their compact congruences contain rich refinable decomposition systems, which is not necessarily true for arbitrary (abstract) semilattices. This gives rise to a new uniform refinement property, which seems to play an important role in congruence lattices of algebras in congruence distributive varieties.

Generalized universal algebra

Libor Polák
Dept. Mathematics, Masaryk University Brno, Czech Republic
polak@math.muni.cz

Sat 16:30, ZS 3 (7th floor)

We introduce $\mathbb{C}$-varieties and generalized $\mathbb{C}$-varieties of homomorphisms from free algebras onto algebras of a given type, where $\mathbb{C}$ is a category of free algebras of this type. We formulate and prove (in fact, we generalize) the classical results of universal algebra for them. We study all in detail in the case of mono-unary algebras and abelian groups for concrete very natural categories.

Situation logic and bridges

Bertalan Pécsi
PhD student (ELTE, Budapest)
aladar@renyi.hu
Coauthors: Ildikó Sain

Sat 16:30, Diss (8th floor)

We introduce a model theoretic approach of mathematical languages in terms of category theory. Our sentences are built up not by terms or words, but as trees of "abstract situations" what may be interpreted in the models and are reflected by homomorphisms. In our setting we are given a category $\mathbb{S}$ of *situations* and a category $\mathbb{M}$ of *models*, with a collection of *interpretations*. An interpretation of a situation A in a model m will be just a *morphism* from A to m (in a wider category $\mathbb{L}$ which contains both $\mathbb{S}$ and $\mathbb{M}$).

We introduce therefore the purely algebraic notion of a *bridge* as such a category which links up two given categories by morphisms between them. It turns out that bridges are in a strong connection with other category theorietical notions like functors, adjoint situations, natural transformations or category equivalence.

In situation logic we can prove general Birkhoff type theorems (stating that a class of models is closed under taking subalgebras/homomorphic images/ultraproducts if (and only if) it can be defined by certian types of formulas), which theorems may be applied e.g. for partial algebras.

We also prove that, in a sense, [each mathematical sentence can be written of the form "$\forall A \exists B$" for some situations A and B].

An interesting thing can happen if we allow trees with infinite branches as formulas: in a certain interpretation, an *antiparadox* appears, a logical sentence which is true and its negation is itself (hence true, too).

Probabilistic averaging in bounded residuated ℓ-monoids

Jiří Rachůnek
Dept. Algebra and Geometry, Palacký Univ. Olomouc, Czech Republic
rachunek@inf.upol.cz
Coauthors: Anatolij Dvurečenskij

Fri 11:00, ZS 1 (8th floor)

Bounded commutative residuated $R\ell$-monoids ($R\ell$-monoids), or commutative integral residuated lattices, generalize MV-algebras and BL-algebras. Analogously, non-commutative $R\ell$-monoids are a generalization of GMV-algebras (= pseudo MV-algebras) and pseudo BL-algebras. Such monoids, in contrast to MV-algebras and GMV-algebras, do not admit in general an analogue of the addition. Nevertheless, we introduce the notions of states (analogues of probability measures) on $R\ell$-monoids which generalize those on MV- and GMV-algebras. We exhibit topological properties of the state spaces and the spaces of extremal states.

Compatible relations on majority algebras

Sándor Radeleczki
Institute of Mathematics, University of Miskolc
matradi@gold.uni-miskolc.hu
Coauthors: Ivan Chajda, University of Olomouc

Fri 16:00, ZS 1 (8th floor)

First, we establish a new characterization for majority algebras. Using this characterization we derive new properties of their tolerance lattice. Our results generalize the results of H-J. Bandelt concerning the properties of the tolerance lattice of a lattice and extend some earlier joint results of D. Schweigert, G. Czédli, E. K. Horváth, I. Chajda and of the present speaker. We also prove that the compatible reflexive relations of a majority algebra form a pseudocomplemented 0-modular lattice, and that the lattice of quasiorders is the homomorphic image of this lattice.

On subgroup lattices

Vladimir B. Repnitskiĭ
Ural State University, Ekaterinburg, Russia
Vladimir.Repnitskii@usu.ru

Sat 15:00, ZS 3 (7th floor)

We propose a new approach to the study of intervals in subgroup lattices. This approach is based on the concept of so-called valuations. A valuation is a mapping of a group into a $\vee$-semilattice with zero satisfying some natural conditions. Using techniques of valuations, we obtained the following result. (Given a group G, *Sub* G is the subgroup lattice of G. For a subgroup T of G, $N_G(T)$ is the normalizer of T in G.)

THEOREM 1. *Let* **K** *be an abstract class of groups satisfying the following conditions:*

(1) **K** *contains a two-element group;*

(2) **K** *is closed under restricted direct products, semidirect products and direct limits over totally ordered sets;*

(3) **K** *is closed under finitary free products.*

Then every algebraic lattice is isomorphic to an interval $[H, G]$ *in the subgroup lattice of a suitable group* $G \in \mathbf{K}$. *Moreover, the group* G *and the interval* $[H, G]$ *can be chosen such that the group* G *is generated by involutions and* $N_G(T) = T$ *for every subgroup* $T \in [H, G]$.

Applying the theorem to the class **K** of all groups, we obtain the well-known result of Tůma as a corollary: *every algebraic lattice is isomorphic to an interval in the subgroup lattice of a suitable [infinite] group.*

Using our concept of valuations, J. Tůma recently proved that *every finite lattice is isomorphic to an interval in the subgroup lattice of a suitable countable locally finite group.* Our technique allows to prove also the following result.

THEOREM 2. *Every lattice is isomorphic to a sublattice of the subgroup lattice of a suitable locally finite group.*

Vector spaces do not need fields

Gabriele Ricci
Dipartimento di Matematica, Universitá di Parma, I-43100 Parma, Italien
gabriele.ricci@unipr.it

Sun 09:00, Diss (8th floor)

A universal based algebra consisting of the sum of an Abelian monoid and of unary operations is a vector space iff its dilatations satisfy two simple conditions. The former requires that the images of the base elements under any non-null dilatation again form a base. The latter that all algebra elements are "indicators" of the dilatations, which exactly are these unary operations.

An element of a universal based algebra is a *dilatation indicator,* when it defines the "amount" of a dilatation. In our case, vector spaces, such an amount is the linear invariant of the square matrix, whose columns equal the element (vector). Namely, it is the sum of the vector components, when the vector is an n–tuple of elements of some field.

The matrices, flocks, dilatations and their indicators for a universal based algebra have much of the properties we know from vector spaces. Universal Algebra was unable to reach such universal notions, mainly because of its abstract representation-free orientation, whereas we define them and prove their properties through an intensional treatment of universal representations.

This characterization of vector spaces avoids any partial algebra, as it was done by means of the (total) heterogeneous algebras of G. Birkhoff. Yet, contrary to that, it does by avoiding any auxiliary algebra and all equations defining a field or relating it to a vector space. The field with all such equations merely comes out of the two conditions about dilatations.

On Jauch-Piron effect algebras

Zdenka Riečanová
Department of Mathematics, Faculty of Electrical Engineering and Information Technology STU, Ilkovičova 3, SK-81219 Bratislava, Slovak Republic
zdenka.riecanova@stuba.sk

Sat 16:30, ZS 1 (8th floor)

Recently there appeared new algebraic structures weakening the axiomatic systems of orthomodular lattices and MV-algebras. Especially those are effect algebras (introduced by D. Foulis and M.K. Bennett, 1994). Effect algebras may be carriers of states and probabilities in quantum or fuzzy probability theory. On the other hand there are even finite effect algebras admitting no states and probabilities. We show some families of effect algebras admitting sigma-additive or subadditive states (probabilities), even with the Jauch-Piron property. We show sufficient and necessary conditions for atomic lattice effect algebras to be unital and Jauch-Piron.

Some algebraic structures of logic programming

Anna Romanowska
Warsaw University of Technology, Warsaw, Poland
aroman@alpha.mini.pw.edu.pl
Coauthors: Yu. M. Movsisyan, Yerevan, Armenia, J. D. H. Smith, Ames, Iowa, USA

Fri 16:30, ZS 3 (7th floor)

Bilattices were first introduced by M. Ginsberg and M. Fitting (1988, 1989) as a general framework for a variety of applications such as truth maintenance systems, default inference and logic programming, and investigated further by these and other authors. The main feature of these algebras is that they have two separate lattice structures defined on the same set. However different authors propose different connections between the two lattice structures. We will describe several notions of bilattices used by different authors, provide their characterizations and describe their structure. In particular, we show how the notions of hyperidentities (defined in the sense of Belousov and Movsisyan) and of superproduct can be used to characterize certain classes of bilattices.

Commutation and centralizers

Ivo G. Rosenberg
Math. Stat. Universite de Montreal, C.P. 6128, succ. Centre-ville, Montreal, Que. Canada H3C 3J7
rosenb@DMS.Umontreal.CA
Coauthors: Hajime Machida

Sun 11:00, ZS 3 (7th floor)

Commuting operations on a given universe A is an old concept. The corresponding Galois connection (polarity) leads to centralizers and a closure on the set of operations on A. The centralizers are very special clones on A that include endoprimal algebras. We present an overview of the topic and some of our recent results.

Elementary relations and epimorphisms

Philipp Rothmaler
Ohio State University
rothmaler.1@osu.edu

Sat 17:30, Diss (8th floor)

I will introduce the concept of *elementary relation* with special emphasis on that of *elementary epimorphism*. I will discuss inverse systems of such and a dual of the elementary chain lemma. Finally, I will do the same for the related concept of *pure epimorphism* and apply this to certain inverse limits of flat modules and certain inverse limits of absolutely pure modules.

Antichains in powers of ordered sets

Aleksander Rutkowski
Warsaw University of Technology, Faculty of Mathematics and Information Science
arut@mini.pw.edu.pl
Coauthors: Yunis El-mugassabi

Sun 10:30, Diss (8th floor)

For an integer $m \geq 1$, denote by Q_m a bipartite poset on $2m+2$ elements $t_1, t_2, \ldots, t_m$, $b_1, b_2, \ldots, b_m, b, t$ with the only comparabilities $t_1 < b, \ldots, t_m < b, b < t, b_1 < t, \ldots, b_m < t$. Obviously, the width of Q_m is $n+m$ and its levels (sets of elements of the same rank) have size $m+1$, so except for the case $m = 1$, Q_m has no Sperner Property (SP means that one of the levels is a realizer of the width). We investigate antichains in the power $(Q_m)^d$ to find its width.

A good tool for generating antichains in products of ordered sets is the concept of convolution, that is an operation which produces an antichain partition of $P \times Q$ from antichain partitions of posets P and Q, respectively. The partition of $P \times Q$ on levels is a special case of the convolution. Antichains generated by convolution are good candidates for realizers of the width.

It turns out that only for some $m > 1$ and some d, the poset $(Q_m)^d$ has Sperner Property. In other products of Q_m realizers of the width are given by the convolution applied to a special partition of Q_m.

On absolutely ubiquitous structures

Gábor Sági
Rényi Institute of Mathematics, Budapest, Hungary
sagi@renyi.hu

Sat 17:00, Diss (8th floor)

For a first order structure $\mathcal{A}$ the set of isomorphism-types of finitely generated substructures of $\mathcal{A}$ is denoted by $J(\mathcal{A})$. A countable, uniformly locally finite structure $\mathcal{A}$ is defined to be *absolutely ubiquitous* iff for any countable locally finite $\mathcal{B}$, $J(\mathcal{A}) = J(\mathcal{B})$ implies that $\mathcal{A}$ and $\mathcal{B}$ are isomorphic.

We will present structure theorems for absolutely ubiquitous structures. We also discuss $\aleph_0$-stability of these structures.

Pseudocomplemented semilattices are universal — in a sense (preliminary report)

Jürg Schmid
Mathematical Institute, University of Bern, CH-3012 Bern, Switzerland
juerg.schmid@math-stat.unibe.ch
Coauthors: Michael E. Adams, Dept. of Mathematics, State University of New York, New Paltz, NY 12561, U.S.A. (e-mail: adamsm@newpaltz.edu)

Fri 16:30, 101 A (3rd floor)

Every category of algebras of finite type is isomorphic to a subcategory of the variety of all pseudocomplemented semilattices whose morphisms consist of all homomorphisms NOT having a Boolean image. Moreover, the corresponding functor assigns a finite pseudocomplemented semilattice to each finite algebra in the category under consideration.

Fluid varieties

Dietmar Schweigert
TU Kaiserslautern Germany
dietmarschweigert@web.de
Coauthors: Ewa Graczyńska

Sat 15:00, ZS 1 (8th floor)

A modification of the notion of a *fluid* variety is given as a counterpart of the notion of a *solid* variety.

Classification of functions in a cardinal power

Branimir Šešelja
University of Novi Sad
seselja@im.ns.ac.yu

Fri 11:00, Diss (8th floor)

We present a classification of isotone functions from a poset X into a poset P, i.e., of the elements of the cardinal power P^X.

For each isotone function μ from X to P and each $p \in P$ there is a subset μ_p of X, a cut set of X: $\mu_P := \{x \in X \mid \mu(x) \geq p\}$. Each cut set of μ is a down-set on the poset X. Necessary and sufficient conditions under which an arbitrary family of down-sets of X indexed by elements of P represents a family of cut sets of the poset X are given.

If the family of cut sets of $\mu : X \to P$ is considered as a collection of subsets of X, without referring to the elements of P, then it is a point closure system on X. It induces a particular collection of subsets of the poset P. In terms of these we present necessary and sufficient conditions under which different functions from X to P have equal collection of cut sets.

In addition, classification is given for some special cases of posets X and P.

On quasivarieties of distributive double p-algebras

Jiří Sichler
University of Manitoba
sichler@cc.umanitoba.ca
Coauthors: Václav Koubek (Charles University, Prague)

Fri 16:00, 101 A (3rd floor)

A quasivariety Q is q-universal if the lattice $L(V)$ of all subquasivarieties of any quasivariety V of algebraic systems with a finite similarity type is isomorphic to a quotient lattice of a sublattice of $L(Q)$. We discuss q-universality of finitely generated varieties of distributive double p-algebras, and the relationship between q-universality and categorical universality.

Thin relations and associated closure operators

Josef Šlapal
Brno University of Technology
slapal@fme.vutbr.cz

Sat 12:00, ZS 1 (8th floor)

It is well known that closure operators that are more general than the Kuratowski ones have many useful applications in mathematics and other fields. In particular, in computer science they can be used for structuring the digital plane. Here, an especially important role is played by the closure operators that are associated with (n-ary) relations. We will discuss a certain type of such operators with respect to their possible use in digital image processing.

Rewriting and congruence membership problem for polynomial semirings

Olga Sokratova
University of Tartu, Estonia
sokratov@math.uiowa.edu

Fri 12:00, Diss (8th floor)

In this talk we apply rewriting techniques to solve the congruence membership problem for polynomial semirings over natural numbers. We define a reduction relation for a finite set of identities and give a completion procedure for the corresponding rewriting system. If the procedure terminates it gives a convergent rewriting system equivalent to the initial rewriting system, thereby solving the congruence membership problem.

In contrast to the completion procedure for polynomial rings, this procedure may not terminate. However, it is proven that the procedure terminates if and only if there exists a convergent and compatible to a given ordering rewriting system equivalent to the initial one. Examples of termination and non-termination of the procedure are given.

We also discuss rewriting methods for general polynomial semirings in non-commutative setting.

Not all modes satisfy Szendrei identities

Michal Stronkowski
Warsaw University of Technology, Warsaw, Poland
m.stronkowski@mini.pw.edu.pl

Fri 17:30, ZS 1 (8th floor)

We formulate a theorem describing the equational theory of all modes of a fixed type. We use this result to show that a free mode with one basic operation of arity at least three over a set of cardinality at least two, is not a Szendrei mode. This gives a negative answer to the question raised by A. Romanowska: Is it true that each mode is a subreduct of some semimodule?

Lattice problems arising in theory of intuitionistic fuzzy sets

Andreja Tepavčević
University of Novi Sad
etepavce@eunet.yu
Coauthors: Marijana Gorjanac-Ranitović

Sat 11:30, 101 A (3rd floor)

An intuitionistic lattice valued fuzzy set consists of two functions f and g from a set X to a power $[0,1]^L$ of the unit interval such that the sum of values of two functions is less then 1 on each coordinate. To every $p \in [0,1]^L$ there correspond two cut sets f_p and g^p, which are subsets of X. A 'synthesis problem' is solved for some types of lattices L and some cardinalities of X: for two collections of subsets of X whether there exists an intuitionistic fuzzy set such that the given collections are families of cut sets of the constructed fuzzy set. The problem is considered within collections of filters and ideals on the lattice of closed elements of closure operators on $[0,1]^L$ (and dually on open elements under interior operators).

Boolean ultrafilters

Aldo Ursini
Dept. of Mathematics and Computer Science, University of Siena, Italy
ursini@unisi.it

Fri 11:00, ZS 3 (7th floor)

We characterize in several ways those lattices (called *ultras*) which are, up to isomorphism, ultrafilters of boolean algebras or, equivalently, filters of boolean algebras. For instance, up to termwise equivalence, they are: the boolean rings; or the implicative (or Brouwerian) semilattices satisfying Pierce's law; or the Brouwerian lattices in which every prime filter is maximal. Since ultras are exactly boolean rings, we have contacts with **classical algebra**.

Ultras are the algebraic semantics of the fragment of classical logic with conjunction, disjunction and implication (no negation and no constant for the False), thus we have contacts with **algebraic logic**.

We investigate the variety (e.g.: it is a discriminator, ideal determined variety; its first order theory is decidable but has no quantifier elimination) and get topological representations and duality results.

We also deal with the problem of identifying those ultras which are set-theoretic (ultra)filters.

Riesz ideals in generalized effect algebras and in their unitifications

Elena Vincekova
Mathematical Institute, Slovak Academy of Sciences, Bratislava, Slovakia
pulmann@mat.savba.sk
Coauthors: Sylvia Pulmannova

Sat 17:00, ZS 1 (8th floor)

The notion of an effect algebra was introduced as an abstract analogue of the set of Hilbert space effects, that is, self-adjoint operators between the zero and identity operators on a Hilbert space, for the purposes of mathematical foundations of quantum theory.

It is well known that every generalized effect algebra (GEA in short) P, which is, roughly speaking, an effect algebra without the top element, can be embedded into a uniquely defined effect algebra E such that for every $a \in E$, either $a \in P$ or its complement $a' \in P$. In analogy with the theory of rings, we call this effect algebra E the *unitification* of the GEA P.

In the theory of (generalized) effect algebras, an important role is played by so called Riesz ideals; quotients with respect to them have many good properties. In this talk, we study Riesz ideals of generalized effect algebras and their relations to the unitifications. We find conditions under which a Riesz ideal I of a generalized effect algebra P is a Riesz ideal in the unitification E of P. We also show that quotients of GEAs with respect to Riesz ideals preserve some important special properties, e.g., quotients of generalized orthoalgebras, weak generalized orthomodular posets (WGOMP) or generalized orthomodular lattices belong to the same class. Also homogeneity, Riesz decomposition and so-called prelattice properties of GEAs are preserved by quotients with respect to Riesz ideals.

Modular elements of the lattice of semigroup varieties

Mikhail Volkov
Ural State University, Ekaterinburg, Russia
Mikhail.Volkov@usu.ru
Coauthors: Boris Vernikov

Fri 12:00, 101 A (3rd floor)

An element x of the lattice $\langle L; \vee, \wedge \rangle$ is called *modular* if

$$\forall\, y, z \in L: \;\; y \leq z \longrightarrow (x \vee y) \wedge z = (x \wedge z) \vee y,$$

and *upper-modular* if

$$\forall\, y, z \in L: \;\; y \leq x \longrightarrow (z \vee y) \wedge x = (z \wedge x) \vee y.$$

Lower-modular elements are defined dually to upper-modular ones. Semigroup varieties that are simultaneously modular and lower-modular elements of the lattice **SEM** of all semigroup varieties have been completely described in the speaker's paper that will appear in the Proceedings of AAA68. Here we consider the dual restriction and give a complete classification of semigroup varieties that are simultaneously modular and upper-modular elements of the lattice **SEM**.

Recent results on congruence lattices of algebras with permutable congruences

Friedrich Wehrung
University of Caen, Department of Mathematics, 14032 Caen cedex, FRANCE
wehrung@math.unicaen.fr
Coauthors: Pavel Ruzicka, Jiří Tůma

Sun 12:15, main building

It is well-known that the congruence lattice of a congruence-permutable algebra is modular, and in fact Arguesian. The "converse" was proven false by Mark Haiman: there are Arguesian algebraic lattices that do not have a type 1 embedding into any partition lattice. For distributive algebraic lattices, the corresponding question, raised by E.T. Schmidt, was open: Is every distributive algebraic lattice isomorphic to the congruence lattice of some congruence-permutable algebra?

We present a solution of the problem above, together with discussion about the corresponding problems for various algebraic structures such as groups or modules.

Left ideals in 1-primitive near-rings

Gerhard Wendt
Joh. Kepler Universitaet Linz
wendt@algebra.uni-linz.ac.at

Sat 15:00, Diss (8th floor)

We consider the structure of left ideals of zero symmetric and 1-primitive near-rings. We show that each such left ideal has a multiplicative right identity and we also describe the ideal structure of the left ideals when considered as subnear-rings.

On elements of composition semigroups with a small centralizer

Johann Wiesenbauer
TU Wien
j.wiesenbauer@tuwien.ac.at

Sun 11:00, ZS 1 (8th floor)

An element a of a monoid H is called extremely noncommutative, if its centralizer $C(a)$ is smallest possible, i.e. consists only of powers of a. The main goal of the talk is to characterize those elements for some special types of composition semigroups

Preconcept algebras and generalized double Boolean algebras

Rudolf Wille
FB Mathematik, TU Darmstadt, D-64289 Darmstadt
wille@mathematik.tu-darmstadt.de

Fri 16:00, ZS 3 (7th floor)

Boolean Concept Logic as an integrated generalization of Contextual Object Logic and Contextual Attribute Logic can be substantially developed on the basis of preconcept algebras. The main results reported in this contribution are the Basic Theorem on Preconcept Algebras and the Theorem characterizing the equational class generated by all preconcept algebras by the equational axioms of the generalized double Boolean algebras.

On the implementation of torus-based cryptosystems

Kenneth Wong
Information Security Institute, Queensland University of Technology, Brisbane, Australia
kk.wong@qut.edu.au

Sun 10:30, ZS 1 (8th floor)

The XTR public key system was introduced by Lenstra and Verheul in 2000 as an alternative to elliptic curve cryptosystems. Since then this cryptogrphic primitive gave rise to the new area of torus-based cryptography. The torus-based public key system CEILIDH, proposed by Rubin and Silverberg in 2003, was successfully implemented by Granger, Page and Stam in 2004, with efficiency comparable to that of XTR. In this talk, we present an outline of the implementation and propose modifications to allow faster arithmetic in the cyclotomic subgroup $G_{p,6}$ used in CEILIDH. The use of these results on the public key system based on the algebraic torus T_{30} proposed by van Dijk et. al. is also discussed.