

# 81. Arbeitstagung Allgemeine Algebra 81st Workshop on General Algebra

University of Salzburg, February 3 – 6, 2011

---

## Abstracts

---

**Erhard Aichinger** (Johannes Kepler University Linz)

A REMARK ON THE COMPOSITION OF POLYNOMIAL FUNCTIONS OVER ALGEBRAICALLY CLOSED FIELDS

In 1969, M. D. Fried and R. E. MacRae proved that for univariate polynomials  $p, q, f, g \in \mathbb{K}[t]$  ( $\mathbb{K}$  a field) with  $p, q$  nonconstant,  $p(x) - q(y)$  divides  $f(x) - g(y)$  in  $\mathbb{K}[x, y]$  if and only if there is  $h \in \mathbb{K}[t]$  such that  $f = h(p(t))$  and  $g = h(q(t))$ . In 1995, F. Binder and the author provided short algebraic proofs of this theorem, and J. Schicho gave a proof from the viewpoint of category theory, thereby providing several generalizations to multivariate polynomials.

In this talk, we give an algebraic proof of one of these generalizations. The theorem by Fried and MacRae yields a way to prove the following fact for nonconstant functions  $f, g$  from  $\mathbb{C}$  to  $\mathbb{C}$ : if both the composition  $f \circ g$  and  $g$  are polynomial functions, then  $f$  has to be a polynomial function as well. We give an algebraic proof of this fact and present a generalization to multivariate polynomials over algebraically closed fields. As an application, one obtains a generalization of a result by L. Carlitz from 1963 that describes those univariate polynomials over finite fields that induce injective functions on all of their extensions. Part of this research is joint work with S. Steinerberger (Bonn, Germany).

**Goulnara Arzhantseva** (Universität Wien)

AMENABILITY AND BEYOND

This is an expository talk on the amenability, discovered by von Neumann in 1929, and its recently appeared relatives: coarse amenability, introduced by Yu in 2000, and coarse embeddings, defined by Gromov in 1993, in relation with the Novikov conjecture.

**Mike Behrisch** (Technische Universität Dresden)

#### ON ALGEBRAS DERIVED FROM MINIMAL MAJORITY CLONES

We assign to every unitary Menger algebra of rank three an algebra of a new signature, which is a subalgebra of a certain term reduct of the given Menger algebra. The class of algebras derived in this way can be shown to be a variety and to be categorically equivalent to the full subcategory of non-terminal unitary Menger algebras of rank three that consist only of selectors and majority elements. These Menger algebras arise as ternary parts of clones generated by majority operations. The minimal clones generated by majority operations correspond to minimal such Menger algebras and to minimal derived algebras (having only trivial subuniverses, i.e. the empty set and the whole carrier set). We show that the subvariety of derived algebras generated from algebras corresponding to known minimal majority clones does not contain any new finite minimal algebras. That is, it is impossible to construct new minimal majority clones on finite sets using just the HSP-closure operator.

**Daniel Bernstein** (University of Illinois at Chicago)

#### A CLASSIFICATION OF DETOURS IN PROOFS OF THE GENERALIZED NULLSTELLENSATZ

Textbooks on commutative algebra often include a standard generalization (1947 Zariski, 1951 Goldman, 1952 Krull) of the classical Nullstellensatz. Several different several-page proofs of this generalized Nullstellensatz have appeared in the literature. It turns out that all of the proofs fit naturally into a complete lattice, where the top of the lattice is a much shorter proof of the same theorem.

**Michal Botur** (Palacký University Olomouc)

#### NEW EXAMPLES OF COMMUTATIVE BASIC ALGEBRAS

Basic algebras are MV-like algebras (more precisely, algebras of type  $\langle 2, 1, 0 \rangle$ ) which are derived from lattices which possess an antitone involution on every principal filter. The class of all basic algebras form a variety which contains many important classes (for example Boolean algebras, MV-algebras, algebras equivalent with ortho-modular lattices or algebras equivalent with lattice ordered effect algebras). The binary operation  $\oplus$  is generally non-commutative and non-associative. Basic algebras with commutative  $\oplus$  (commutative basic algebras) form an important subvariety. Firstly, commutative basic algebras can be represented as non-associative residuated structures satisfying a lot of logical identities (double negation law, prelinearity, divisibility, Łukasiewicz axiom, contra-position law, ...). Simply, commutative basic algebras are natural non-associative generalizations of MV-algebras. The previous result shows that finite commutative basic algebras are necessarily associative and thus are just finite MV-algebras. Moreover, complete commutative basic algebras are subdirect products of linearly ordered ones. Although there are many papers and results which describe the class of commutative basic algebras, it is not easy find an example of a commutative basic algebra which is not an MV-algebra. Just constructions of non-associative basic algebras are the main aim of the talk. We will present new ideas and examples of non-associative and commutative basic algebras.

**Sinan Cevik** (Selcuk University)

#### DEFICIENCIES ON GROUPS AND MONOIDS

In this talk, I would like to give some fundamental facts, theories and specific examples about deficiencies (or efficiencies) on groups and monoids. The examples on the theory will be presented by considering the split extension of a finite cyclic group by a free abelian group having rank two, and also by considering the split extension of a free abelian monoid having finite rank by a finite monogenic monoid. The main references on these two subjects can be as follows:

- [1] F. Ates, E.G. Karpuz, A.D. Gungor, A.S. Cevik, A new example of minimality of monoids, *Asian-European Journal of Mathematics*, Vol 3(4), 2010, 531–545.
- [2] A.S. Cevik, F. Ates, E.G. Karpuz, A.D. Gungor, I.N. Cangul, A new example of deficiency one groups, “Generating functions of special numbers and polynomials and their applications” with in *International Conference of Numerical Analysis and Applied Mathematics 2010 (ICNAAM 2010)* (Edt. T.E. Simos, G. Psihoyios and Ch. Tsitouras), *AIP Conference Proceedings*, Volume 1281, 2010, 1111–1116.

**Ivan Chajda** (Palacký University Olomouc)

#### BASIC ALGEBRAS

Basic algebras were introduced as a common generalization of MV-algebras and orthomodular lattices for the sake to give a common basis for both the multiple-valued Lukasiewicz logic and the logic of quantum mechanic. It turns out that they can be simultaneously described as bounded lattices with antitone involutions in sections (i.e. intervals  $[a, 1]$  for every element  $a$ ). A basic algebra is an MV-algebra if and only if it is associative and we get an identity which characterizes when it is an orthomodular lattice. Concerning the description by means of lattices with section antitone involutions, a basic algebra is an orthomodular lattice if and only if every section involution is a relative complementation and it is an MV-algebra if the lattice is distributive and it satisfies the so-called exchange condition. Varieties of basic algebras are intensively studied by the group of algebraists from UP Olomouc. Connections with so-called effect algebras (describing the domain of observables in the logic of quantum mechanics) will be presented.

**Jānis Cīrulis** (University of Latvia)

#### ORTHOPOSETS: A CONSTRUCTION OF QUANTIFIERS

We show that every maximal orthogonal subset of an orthoposet induces a quantifier (a symmetric closure operator), and study the structure of the set of all quantifiers of this kind.

**Miguel Couceiro** (University of Luxembourg)

ON THE ARITY GAP OF ORDER-PRESERVING FUNCTIONS

The arity gap of a function  $f: A^n \rightarrow B$  ( $n \geq 2$ ) that depends on all of its variables, denoted  $\text{gap}f$ , can be defined as the minimum decrease in the number of essential variables when variables of  $f$  are identified. In this talk we briefly survey earlier and recent results concerning the arity gap of functions, and present a complete classification of order-preserving functions according to their arity gap which is shown to be either 1 or 2. In the particular case of chains  $A$  and  $B$ , we obtain the following explicit description of those order-preserving functions that have arity gap 1 and those that have arity gap 2.

**THEOREM.** *Let  $A$  and  $B$  be chains, and  $f: A^n \rightarrow B$  be an order-preserving function. Then  $\text{gap}f = 2$  if and only if  $n = 3$  and  $f = \text{med}(h(x_1), h(x_2), h(x_3))$  for some nonconstant order-preserving unary function  $h: A \rightarrow B$  (here  $\text{med}$  denotes the median function on the range of  $h$ ). Otherwise  $\text{gap}f = 1$ .*

Most of the results we are going to present were obtained in joint works with Erkki Lehtonen and Tamás Waldhauser.

**Karin Cvetko-Vah** (University of Ljubljana)

ON SKEW LATTICES AND DUAL DISCRIMINATOR VARIETIES

In their 1995 Algebra Universalis paper Bignall and Leech investigated a certain non-commutative analogue of Boolean algebras, the so called skew Boolean intersection algebras, and proved that any algebra  $A$  in a discriminator variety with a constant term has a skew Boolean intersection algebra polynomial reduct whose congruences coincide with those of  $A$ . We shall present a generalization of this result yielding a connection between meet-distributive intersection skew lattices (i.e. a non-commutative analogue of distributive lattices) and dual discriminator varieties with three constant terms.

**Dietmar Dorninger** (Technische Universität Wien)

ON SPACES OF MULTIDIMENSIONAL PROBABILITIES

The probability  $p(s)$  of the occurrence of an event pertaining to a physical system which is observed in different states  $s$  determines a function  $p$  from the set  $S$  of states of the system to the unit interval  $[0, 1]$ . Such a function  $p$  is called a multidimensional probability or numerical event. We consider sets  $P$  of multidimensional probabilities which can be partially ordered in such a way that orthomodular posets arise. These orthoposets  $P$  are known as spaces of numerical events due to the fact that they can be regarded as a generalization of classical fields of events. Indeed, by means of spaces  $P$  of numerical events one can distinguish between the quantum mechanical and classical behaviour of a physical system. One deals with a classical system if and only if the underlying space  $P$  is a Boolean algebra. We characterize spaces  $P$  of multidimensional probabilities, provide various examples and derive necessary and sufficient conditions for a space  $P$  to be a lattice and a Boolean algebra, respectively. Moreover, we show how one can apply the obtained results to real world data.

**Eylem Guzel Karpuz** (Karamanoglu Mehmetbey University)

STRONGLY  $\pi$ -INVERSE MONOIDS UNDER SCHÜTZENBERGER PRODUCT

In [1], Ateş defined the semidirect product version of the Schützenberger product for any two monoids and examined the regularity on it. Since this is a new product and there are so many algebraic properties that need to be checked on it, in this work we determine necessary and sufficient conditions for this new version to be strongly  $\pi$ -inverse and inverse. Then we give some related results.

- [1] Ateş, F., Some new monoid and group constructions under semidirect products, *Ars Comb.* 91, 203–218, 2009.
- [2] Ateş, F., Karpuz, E. G., Çevik, A. S., Regular and  $\pi$ -inverse monoids under Schützenberger products, *Algebras, Groups and Geometries* (accepted).
- [3] Çevik, A. S., The p-Cockcroft property of the semidirect products of monoids, *Int. Journal of Algebra and Comp.* 13(1), 1–16, 2003.
- [4] Howie, J. M., *Fundamentals of semigroup theory*, Clarendon Press-Oxford, 1995.
- [5] Howie, J. M. and Ruskuc, N., Constructions and presentations for monoids, *Comm. in Algebra* 22(15), 6209–6224, 1994.
- [6] Zhang, Y., Li, S. and Wang, D., Semidirect products and wreath products of strongly  $\pi$ -inverse monoids, *Georgian Math. Journal* 3(3), 293–300, 1996.

**Radomír Halaš** (Palacký University Olomouc)

EFFECT ALGEBRAS AS CONDITIONALLY RESIDUATED STRUCTURES

The aim of the talk is to link up the structures used in foundations of quantum logic and that arising in many-valued reasoning. We shall characterize effect and pseudoeffect algebras as conditionally residuated structures.

**Eszter K. Horváth** (University of Szeged)

CD-INDEPENDENT SUBSETS IN POSETS AND IN PARTICULAR LATTICE CLASSES

It is proved by G. Czédli, M. Hartmann and E. T. Schmidt that any two CD-bases in a finite distributive lattice have the same number of elements. We investigate CD-bases in posets, semilattices and lattices. It is shown that their CD-bases can be characterized as maximal chains in a related poset or lattice. We point out two known lattice classes whose CD-bases satisfy the mentioned property.

Joint work with Sándor Radeleczki.

**Milan Jaseň** (Slovak Technical University)

WEAK RELATIVELY UNIFORM CONVERGENCE IN DUALY RESIDUATED LATTICE ORDERED SEMIGROUPS

In this paper the notion of a weak relatively uniform convergence in dually residuated lattice ordered semigroups is introduced and basic properties of this convergence are established. Further, a Cauchy completion of a dually residuated lattice ordered semigroup is investigated.

**Sebastian Kerkhoff** (Technische Universität Dresden)

#### DUALIZING CLONES

When it comes to dualizing clones, the usual approach is to consider a clone as a term algebra and then try to prove or disprove that the corresponding algebra is dualizable. In the talk, we will introduce a different and somewhat more general approach to dualizing clones. The framework is based on the idea of generalizing clones to certain sets of morphisms in categories. As we will see, we will be able to dualize any given clone over a finite set  $A$  to a clone of dual operations over a structure with base set  $A$ . We will discuss how this approach can be used to obtain new results for clones over sets.

**Miroslav Kolařík** (Palacký University Olomouc)

#### DYNAMIC EFFECT ALGEBRAS

We introduce the so-called tense operators in lattice effect algebras. Tense operators express the quantifiers “it is always going to be the case that” and “it has always been the case that” and hence enable us to express the dimension of time in the logic of quantum mechanics. We present an axiomatization of these tense operators and prove that every lattice effect algebra whose underlying lattice is complete can be equipped with tense operators. Such an effect algebra is called dynamic since it reflects changes of quantum events from past to future.

**Michiro Kondo** (Tokyo Denki University)

#### WEAK UNINORM BASED LOGIC AND ITS FILTER THEORY

We give an axiomatic system of a logic wUL (called a *weak uninorm-based logic*), which is characterized by the class of all (not necessary integral) commutative residuated lattices. Since many well-known logics, e.g., UL by Metcalfe and Montanga, ML by Höhle, MTL by Esteva and L.Godo, BL by Hájek, are axiomatic extensions of our logic, those logics are all algebraizable. Moreover, we give an answer to the problem left open in [WK].

**Jörg Koppitz** (Universität Potsdam)

#### COREGULAR SEMIGROUPS

Coregular semigroups are particular complete regular semigroups. A coregular element  $s$  of a semigroup is characterized by the property  $s^3 = s$ . For example, such elements arise in Linear Algebra (pseudoinverse matrix). We give an introduction to the structure of coregular semigroups and characterize particular coregular transformation semigroups in order to illustrate the properties of such semigroups.

**Marcin Kozik** (Jagiellonian University)

#### LACK OF ABSORPTION AND MALCEV CONDITIONS

I will present results concerning lack of absorption (as used in the algebraic approach to CSP) and its impact on the Taylor varieties.

**Jan Kühn** (Palacký University Olomouc)

#### LATERAL COMPLETIONS OF PSEUDO-BCK-ALGEBRAS

Pseudo-BCK-algebras are the residuation subreducts of integral residuated lattices. We prove that some pseudo-BCK-algebras have a unique lateral completion, i.e., a completion in which the initial algebra is dense and where every set of pairwise disjoint elements has infimum.

**Tanja Lange** (Technische Universiteit Eindhoven)

#### ELLIPTIC CURVE CRYPTOGRAPHY

This talk gives an overview of several results; not all of these results are by me but several involved me and my co-authors. In 2007 Harold Edwards' paper "A normal form for elliptic curves" provided a new way to write elliptic curves. This form offers many advantages for elliptic curve cryptography but is also easier to explain to students. The main advantages are that for suitably chosen curves the set of affine points forms an abelian group – there is no need to consider points at infinity for explaining the group law and it is even possible to give a single addition formula which holds without exceptions. This *completeness* of the addition formula depends on the finite field and points at infinity appear after a quadratic extension. To cover addition of any pair of points over any Edwards curve over any field it is sufficient to consider 2 addition formulas which each hold on an open subset of  $E \times E$  and these formulas are surprisingly short. For cryptographic applications the simplicity of the addition law translates to a particular fast algorithm to add points on the curve leading to particularly efficient implementations. Edwards' paper has prompted a lot of research into alternative curve shapes for elliptic curves and many improvements were found since 2007. A summary of the formulas can be found at <http://www.hyperelliptic.org/EFD/>. The progress described thus far leads to faster implementations of key exchange and signature schemes. Details of several implementations and speed comparisons are part of eBACS: ECRYPT Benchmarking of Cryptographic Systems <http://bench.cr.yp.to/>. Elliptic curves can also be used to attack systems: the elliptic curve method of factorization is the best method to factor general large numbers and is an important ingredient in the number field sieve, used to factor RSA numbers. Edwards curves lead to faster factoring methods not only because of the better operation count but also because carefully constructed Edwards curves have a higher probability of finding small factors. So Edwards curves turn out to be good for ECC and bad for RSA.

**Helmut Länger** (Technische Universität Wien)

#### THE ZERODIVISOR GRAPH OF A POSET

The zerodivisor graph  $G$  of a poset  $(P, \leq)$  with  $0$  has vertex-set  $P$ , and different vertices  $a, b$  of  $G$  are connected by an edge if  $0$  is the only common lower bound of  $a$  and  $b$ . The chromatic number and the clique number of  $G$  coincide. We sketch an algebraic proof of this result.

**Thomas Laux** (Technische Universität Dresden)

ON CONVEX SUBSETS OF A METRIC SPACE

Let  $(M, d)$  be a metric space. The associated betweenness relation  $S_d := \{(a, b, c) \in M^3 \mid d(a, c) = d(a, b) + d(b, c)\}$  gives rise to the notion of  $d$ -convex sets, which with any two points contain every point between them with respect to  $S_d$ . Some properties of the hull system of  $d$ -convex subsets of  $M$  will be identified, as well as a possible way to reconstruct a generating metric for any hull system satisfying these properties.

**Erkko Lehtonen** (University of Luxembourg)

EMBEDDABILITY OF COUNTABLE POSETS WITH FINITE PRINCIPAL IDEALS INTO PARTIAL ORDERS INDUCED BY CLONES

Two partially ordered sets are said to be *equimorphic* if each one can be embedded to the other. It is well-known that the set  $(\mathcal{P}_f(\omega), \subseteq)$  of finite subsets of the natural numbers, ordered by inclusion, is a countable poset, its principal order ideals are finite, and it admits an embedding of every countable poset whose principal order ideals are finite. Thus, every poset that is equimorphic to  $(\mathcal{P}_f(\omega), \subseteq)$  enjoys the same properties. Let  $\mathcal{C}$  be a clone on  $A$ , and let  $f$  and  $g$  be operations on  $A$ . We say that  $f$  is a  $\mathcal{C}$ -minor of  $g$ , if  $f = g(h_1, \dots, h_n)$  for some  $h_1, \dots, h_n \in \mathcal{C}$ , and we denote this fact by  $f \leq_c g$ . If  $f \leq_c g$  and  $g \leq_c f$ , we say that  $f$  and  $g$  are  $\mathcal{C}$ -equivalent, and we denote this fact by  $f \equiv_c g$ . The relation  $\leq_c$  is a quasi-order on the set  $\mathcal{O}_A$  of all operations on  $A$ , and it induces a partial order  $\preceq_c$  on the set  $\mathcal{O}_A/\equiv_c$  of  $\mathcal{C}$ -equivalence classes.

**THEOREM.** *Let  $\mathcal{C}$  be a clone on a finite set  $A$  with at least two elements. If*

- $\mathcal{C}$  is a clone that contains only essentially at most unary operations; or
- $\mathcal{C}$  is a subclone of the clone of polynomial operations of the semimodule  $(A; +, \text{End}(A))$ , where  $(A; +)$  is a commutative inverse monoid and  $\text{End}(A)$  is the semiring of endomorphisms of  $(A; +)$ , and  $\mathcal{C}$  contains an operation of the form  $x_1 + x_2 + \dots + x_m$ , for some  $m \geq 2$ ; or
- $\mathcal{C}$  is Burle's clone on  $A$ ,

*then the  $\mathcal{C}$ -minor partial order  $(\mathcal{O}_A/\equiv_c, \preceq_c)$  is equimorphic to  $(\mathcal{P}_f(\omega), \subseteq)$ .*

This talk is based on joint work with Ágnes Szendrei.

**Hannes Leitgeb** (Ludwig-Maximilians-Universität München)

ALGEBRAIC AND PROBABILISTIC STRUCTURES IN EPISTEMOLOGY

Epistemology, one of the traditional areas of philosophy, deals with the topic of rational belief: under what conditions is it rational to hold something to be true? There are two kinds of belief that are of interest here: qualitative belief — believing that some proposition is the case — and quantitative belief (degrees of belief) — assigning subjective probabilities to propositions. While the formal theories that are underlying belief in the first sense are logical-algebraic, the mathematical theory for belief in the second sense is standard probability theory, But how do these two kinds of belief relate to each other formally? We prove that given reasonable assumptions, it is possible to give an explicit definition of qualitative belief in terms of subjective probability, such that it is neither



the case that belief is stripped of any of its usual logical properties, nor is it the case that believed propositions are bound to have probability 1. Qualitative belief is not to be eliminated in favour of degrees of belief, rather, by reducing it to assignments of consistently high degrees of belief, both quantitative and qualitative belief turn out to be governed by one unified theory. The algebraic structures of qualitative belief are to be found “within” the probabilistic structures of quantitative belief. This is but one instance of the many applications of mathematical methods in philosophy that are currently explored.

**Peter Mayr** (Universidade de Lisboa)

#### RECOGNIZING PARTIAL TERM FUNCTIONS

Fix a finite algebra  $\mathbf{A}$ . What is the complexity of deciding whether a given partial  $k$ -ary function on  $A$  is the restriction of a term function on  $\mathbf{A}$ ? In 2007 Marcin Kozik constructed algebras for which this decision problem is Exptime-complete. In the same year Ross Willard observed that for groups and rings there is a polynomial-time algorithm. We show that the problem is in NP for arbitrary Malcev algebras and obtain some bounds on representations of term functions.

**Jan Paseka** (Masaryk University Brno)

#### MEAGER ELEMENTS IN ARCHIMEDEAN ATOMIC LATTICE EFFECT ALGEBRAS

We thoroughly study the set of meager elements  $M(E)$ , the center  $C(E)$  and the compatibility center  $B(E)$  in the setting of atomic Archimedean lattice effect algebras  $E$ . The main result is that in this case the center  $C(E)$  is bifull (atomic) iff the compatibility center  $B(E)$  is bifull (atomic) whenever  $E$  is sharply dominating. As a by-product, we give a new description of the smallest sharp element over  $x$  in  $E$  via the basic decomposition of  $x$ . As an application, a solution of Jenca’s question concerning the Triple Representation Theorem is given.

**Agata Pilitowska** (Warsaw University of Technology)

#### IDENTITIES IN VARIETIES GENERATED BY ALGEBRAS OF SUBALGEBRAS

In a natural way we can “lift” any operation defined on a set  $A$  to an operation on the set of all non-empty subsets of  $A$  and obtain from any algebra  $(A, \Omega)$  its *power algebra* of subsets. G. Grätzer and H. Lakser proved that for a variety  $\mathcal{V}$ , the variety  $\mathcal{V}\Sigma$  generated by power algebras of algebras in  $\mathcal{V}$  satisfies precisely the consequences of the linear identities true in  $\mathcal{V}$ . In particular,  $\mathcal{V}\Sigma = \mathcal{V}$  if and only if  $\mathcal{V}$  is defined by a set of linear identities. For certain types of algebras, the sets of their subalgebras form a subalgebra of their power algebras. They are called the *algebras of subalgebras*.

In this talk we present a solution of a long-standing problem concerning identities satisfied by varieties  $\mathcal{V}\mathcal{S}$  generated by algebras of subalgebras of algebras in a given variety  $\mathcal{V}$ . We will show that if  $\mathcal{V}$  is a variety of modes - idempotent and entropic algebras, then the variety  $\mathcal{V}\mathcal{S}$  satisfies precisely the consequences of the idempotent and the linear identities true in  $\mathcal{V}$ . (Recall that an algebra is *idempotent* if each singleton is a subalgebra and it is *entropic* if any two of its operations commute.) As a consequence we obtain that in the

case of any variety of modes,  $\mathcal{V} = \mathcal{VS}$  if and only if  $\mathcal{V}$  is defined only by idempotent and linear identities.

Joint work with A. Zamojska-Dzienio.

**Eugene Plotkin** (Bar Ilan University)

ALGEBRAIC LOGIC AND LOGICALLY-GEOMETRIC TYPES IN VARIETIES OF ALGEBRAS

The main objective of the talk is to show that the notion of type which was developed in the frames of logic and model theory has deep ties with geometric properties of algebras. These ties go back and forth from universal algebraic geometry to model theory through the machinery of algebraic logic. We show that types (multi-sorted types) appear naturally as logical kernels in the Galois correspondence between filters in the Halmos algebra of first order formulas with equalities and elementary sets in the corresponding affine space.

Joint work with B. Plotkin and E. Aladova.

**Tatjana Plotkin** (Bar Ilan University)

ALGEBRAIC SYMMETRIES IN KNOWLEDGE BASES

Knowledge base theory stimulates numerous applications of computer algebra and symbolic computations. The talk is aimed to explain how the general ideas of Galois theory work for knowledge bases and help to determine the criterion of knowledge bases informational equivalence. This criterion reduces the problem of informational equivalence of knowledge bases to the conjugacy problem for groups. We give a survey of the recent results and outline the future problems.

**Reinhard Pöschel** (Technische Universität Dresden)

PEIRCEAN ALGEBRAIC LOGIC (PAL) AND RELATION ALGEBRAS

An analogon to the famous CHURCH's thesis is BURCH's thesis stating *All procedures of relational constructions are formalizable in PAL*. In the talk, a short overview on PAL (Peircean Algebraic Logic) and its connections to relation algebras (clones of relations) will be given, some problems and results (obtained in the last decade) shall be reported.

**Jiří Rachůnek** (Palacký University Olomouc)

INTERNAL STATES ON RESIDUATED  $\ell$ -MONOIDS

The class of bounded residuated  $\ell$ -monoids ( $R\ell$ -monoids) contains, among others, certain important classes of algebras behind fuzzy reasoning. States on  $R\ell$ -monoids are analogues of probability measures. We present state  $R\ell$ -monoids, i.e.  $R\ell$ -monoids with a unary operator called an internal state satisfying some basic properties of states.

**Tobias Schlemmer** (Technische Universität Dresden)

#### LINEAR EXTENSIONS OF PARTIAL ORDERS ON ABELIAN GROUPS

Partially ordered groups, also known as po-groups, are groups with a compatible partial order. Results from M. I. Zajceva and H.-H. Teh are combined in order to provide a full characterisation of linear order extensions of a given order on a group. In contrast to Teh this approach provides a method to discuss linear orders of different Abelian rank in a uniform manner. This will be achieved by modelling the linear orders as hyperplanes in a real vector space.

**Karsten Schölzel** (Universität Rostock)

#### GALOIS THEORY FOR PARTIAL CLONES ON FINITE SETS

We consider partial clones on finite sets and establish a Galois connection between partial clones and a new variant of relation algebras. A new elementary operation on relations captures the difference between total and partial clones and enables us to lift the proof from the total case to the partial case with minor modifications. This Galois connection encompasses all partial clones and is not restricted to strong partial clones.

**Sergejs Solovjovs** (University of Latvia)

#### DUAL ATTACHMENT PAIRS IN CATEGORICALLY-ALGEBRAIC TOPOLOGY

The talk continues our development of a fruitful topological theory, based in a categorically-algebraic (catalg) extension of the set-theoretic membership relation “ $\in$ ”. It was inspired by the concept of quasi-coincidence between a fuzzy point and a fuzzy set, which fuzzified the neighborhood approach to topology. The lattice-valued analogue of the relation, dubbed attachment, gave rise to a functor (even an embedding) between the categories of many-valued and crisp topological spaces, thereby providing a rigid justification for the definitions of various notions of many-valued topology. During AAA80 we presented variety-based attachment, extending the obtained results to catalg topology. This talk formulates the notion of duality for the new concept. It also shows the main difference between attachment and topological system: the latter has an internal topology, and the former provides a morphism of topological theories.

**ACKNOWLEDGEMENTS.** The research was supported by the ESF Project 2009/0223/1DP/1.1.1.2.0/09/APIA/VIAA/008 of the University of Latvia. We acknowledge the help of C. Guido and A. Frascella (University of Salento, Italy).

**Filip Švrček** (Palacký University Olomouc)

#### LATTICE-LIKE STRUCTURES DERIVED FROM RINGS

We study lattice-like operations that are term operations in certain rings with restricted powers of elements. We show that every commutative ring with a unit satisfying the identity  $x^{p+1} = x^p$  for some integer  $p \geq 1$  is in fact a Boolean ring. However, if it satisfies  $x^{p+2} = x^p$  for some integer  $p \geq 2$  then it need not be Boolean, but certain lattice-like operations can be introduced such that the original ring can be reconstructed by means of these operations. Similarly it can be done for rings satisfying the identity  $(x^p)^2 = x^p$  for some integer  $p \geq 2$ .

**Ágnes Szendrei** (University of Colorado at Boulder)

#### GENERATING DIRECT POWERS OF ALGEBRAS

For a finite algebra  $\mathbf{A}$  let  $d_{\mathbf{A}}(n)$  denote the size of the smallest generating set for  $\mathbf{A}^n$ . It is known that the growth function  $d_{\mathbf{A}}(n)$  of any finite algebra  $\mathbf{A}$  is at least logarithmic, and at most exponential. We will discuss a theorem that extends the results of Hall, Wiegold, Quick–Ruškuc, Riedel, and others for groups, algebras with an underlying group structure, and algebras in congruence uniform varieties to algebras in arbitrary varieties with a cube term. We will also present the first known examples of finite algebras whose growth functions are neither logarithmic nor linear nor exponential.

Joint with K. A. Kearnes and E. W. Kiss.

**Edith Mireya Vargas** (Technische Universität Dresden)

#### $C$ -CLONES

We study a restricted version of the Galois connection between polymorphisms and invariants, called  $\text{Pol} - C\text{Inv}$ , where the invariant relations are restricted to so-called clausal relations. The lattice of all clones arising from this Galois connection, denominated  $C$ -clones, is investigated. All co-atoms in the lattice of all  $C$ -clones are characterized.

**Rudolf Wille** (Technische Universität Darmstadt)

#### KNOWLEDGE MANAGEMENT IN UNIVERSITY DOMAINS. A SYSTEMATIC ORIENTATION.

In the nineties, business companies have recognized in an increasing measure that knowledge is an important resource for the success of companies. Therefore, large exertions have been made at many places to build up a successful knowledge management in companies; for this, it was first of all necessary to localize, to systematize, to care for and to pass on knowledge suitably. Today substantial perceptions and experiences are already present in considerable size about the effective creation of organizational knowledge management. This knowledge about knowledge management in business is deepened and developed in university domains first of all in operating managements, but also reflected by psychological and social institutes and through research. Vicariously, three books shall here be named which generally inform about economical knowledge management:

- G. Probst, S. Raub, K. Romhardt: Managing knowledge: how companies use optimally their most valuable resource [PRR99].
- T. H. Davenport, L. Prusak: When your company would know what it knows . . . . The practice for knowledge management [DP98].
- K. Devlin: Infosense. Turning information into knowledge [De99].

**Anna Zamojska-Dzienio** (Warsaw University of Technology)

#### A REDUCTION THEOREM FOR FINITARY PREVARIETIES

An abstract class of algebraic systems of a given signature is a *finitary prevariety*, if it is closed under taking substructures and finite Cartesian products. A finitary prevariety

consisting of finite members of some class is called a *pseudo-quasivariety*. V. A. Gorbunov proved a so-called reduction theorem for pseudo-quasivarieties. More specifically, he has proved that the prevariety lattice of any pseudo-quasivariety of a signature with finitely many relation symbols is an inverse limit of finite lower bounded lattices. In this talk, we provide a more general setting for that reduction theorem proving it for finitary prevarieties without putting any restriction on signature. Gorbunov's reduction theorem follows then as a corollary.

Joint work with Marina Semenova.