

Contributions to General Algebra 17

(Proceedings of the conference AAA 70 in Vienna, 2005)

Horea Abrudan

Mihail Ursul

Boundedness of topological endomorphism rings of torsion Abelian groups

The endomorphism ring $\text{End}(A)$ of an Abelian group A is considered as a topological ring furnished with the finite topology. We give some sufficient conditions on a group A under which $\text{End}(A)$ is bounded, i.e., has a fundamental system of neighborhoods of 0 consisting of ideals.

Erhard Aichinger

The polynomial functions of certain algebras that are simple modulo their center

We describe the polynomial functions of a finite algebra \mathbf{A} in a congruence permutable variety that has a congruence $\gamma \neq 1_A$ such that \mathbf{A}/γ is simple, and the (term condition) commutator satisfies $[1_A, 1_A] = 1_A$ and $[\gamma, 1_A] = 0_A$.

Ladislav Bican

On injective hulls

It follows immediately from the proof of the existence of the injective hull $E(M)$ of a module M (see e.g. [?]) 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 $|M| \geq \tilde{\mu}_0 = \max(|R|, \aleph_0)$ (see [?]). 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 purpose of this note is to improve the above estimation by showing that for a module M of the size $|M| = \lambda \geq \mu_0^{<\mu}$ the cardinality of $E(M)$ is at most $\lambda^{<\mu}$.

Ivan Chajda

Helmut Länger

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

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.

M. Chiş

C. Chiş

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

In this article, we determine, for a finite cyclic or dihedral group, formulas for the number of automorphisms with given number of fixed points.

Jānis Cīrulis

Finitizing projection algebras

A projection algebra is a generalization of Halmos quantifier algebras, where quantifiers on a Boolean algebra are indexed by elements of an arbitrary lattice rather than by subsets of a fixed set of variables. Generally, a projection algebra has infinitely many operations. Rich projection algebras are, roughly, algebras with “enough” operations; they correspond in some sense to locally finite quantifier algebras. It is shown in the paper that the category of all rich projection algebras (with various index sets) is equivalent to a finitely based variety of lattices with an additional unary operation; we call algebras in this variety implicit projection algebras. In one direction, the proof of this equivalence rests on the triple construction of a certain kind for the implicit projection algebras.

K. Denecke
P. Glubudom

Generalized Power Menger Algebras and Generalized Non-deterministic Hypersubstitutions

Tree languages are sets of terms of a given type. Operations defined on tree languages are operations on the power set of the set of all terms of this type. Besides the Boolean operations of intersection, union and complement (see [?]) one considers one more binary operation which is called the product of tree languages. This operation is defined by means of a superposition of sets of terms which does not preserve the arities of the terms. For any fixed $n \geq 1$, the power set of the set of all n -ary terms forms an algebra with respect to this superposition operation and with respect to infinitely many nullary operations. We prove that this algebra satisfies the so-called superassociative law and three more identities. Such algebras are called unitary Menger algebras of rank n with infinitely many nullary operations. Generalized hypersubstitutions were introduced in [?]. The definition of a generalized hypersubstitution will be extended to non-deterministic generalized hypersubstitutions. Then we prove that the extensions of non-deterministic generalized hypersubstitutions are endomorphisms of the unitary Menger algebras of rank n with infinitely many nullary operations.

Wojciech Dzik

Splittings of lattices of theories and unification types

We show that the lattice of all theories extending the equational theory of Heyting algebras is split into two parts, “upper” and “lower”. Such a splitting is related to unification types: the upper part contains all theories having unitary unification type (and some of nullary type), the lower part contains all theories having finitary unification type (and some of nullary type, plus some with infinitary type, if there are such). The same splitting determines a limit between theories of constructive (upper part) and non-constructive (lower part) character.

Similar results are proved for the lattice of all theories extending the equational theory of interior algebras (or topological Boolean algebras).

Marcel Erné

Prime Decomposition and Pseudocomplementation

In algebra, topology and order theory, decompositions into prime elements or substructures play a crucial role. Often, the mathematical objects in question carry an order structure such that each element x has a \vee -pseudocomplement, that is, a least element whose supremum with x gives the top element. In such posets P , one finds that the essential primes, i.e. those join-prime elements whose \vee -pseudocomplement is not the least element, are just the atoms of the skeleton P_* (the Boolean poset of all pseudocomplements). A convenient necessary and sufficient condition for the existence of a (unique) irredundant prime decomposition of the top element 1 is that $P \setminus \{1\}$ has a cofinal subset not containing any binary forks (a specific kind of binary trees). In that case, the Dedekind-MacNeille completion of P_* is isomorphic to the powerset of the irredundant prime decomposition. The exclusion of infinite upper antichains even guarantees a least finite prime decomposition. Our results also provide some interesting consequences concerning the cellularity of ordered sets and topological spaces. As expected, relative pseudocomplements entail still stronger decomposition properties. For example, the existence of at least one essential prime for each non-zero element in a Brouwerian \vee -semilattice already guarantees unique irredundant prime decompositions for all elements.

Orderings and groups: a survey of recent results

A. M. W. Glass

I will give a survey of recent results in the subject which are most likely to be of interest to universal algebraists. I will approach this by asking some natural questions and stating the answers. These often start positively but quickly come to a grinding halt. This leads to the natural suspicion that the Devil wins every time. However, in the last part of my talk I will show “*aber nicht immer*” (but not always).

Hermann Kautschitsch

Prime Ideals in the Nearing of Formal Power Series

The study of the composition ring of formal power series is motivated by the composition ring of entire functions as Cartan mentioned in [?]. So one gets ideals in case of entire functions f with $f(0) = 0$ by intersection with those of formal power series with constant term 0. In [?] it is shown how special ideals of formal power series can be obtained from ideals of the corresponding coefficient ring. The determination of ideals is reduced to that of ideals with derivation ideal (0). In this paper nearing ideals, which are also ring ideals are considered, especially all prime nearing ideals of formal power series over certain noetherian rings are determined.

On subquasivarieties of finitely generated varieties of distributive double p -algebras

V. Koubek J. Sichler

A quasivariety \mathbb{V} is Q -universal if the lattice $L(\mathbb{Q})$ of all subquasivarieties of any quasivariety \mathbb{Q} of algebraic systems of a finite similarity type is isomorphic to a quotient lattice of a sublattice of the lattice $L(\mathbb{V})$ of all subquasivarieties of \mathbb{V} . We investigate Q -universality of finitely generated varieties of distributive double p -algebras. In particular, we show that any categorically universal finitely generated variety of distributive double p -algebras is Q -universal.

Erkko Lehtonen

An infinite descending chain of Boolean subfunctions consisting of threshold functions

For a class \mathcal{C} of Boolean functions, a Boolean function f is a \mathcal{C} -subfunction of a Boolean function g , if $f = g(h_1, \dots, h_n)$, where all the inner functions h_i are members of \mathcal{C} . Two functions are \mathcal{C} -equivalent, if they are \mathcal{C} -subfunctions of each other. The \mathcal{C} -subfunction relation is a preorder on the set of all functions if and only if \mathcal{C} is a clone. An infinite descending chain of U_∞ -subfunctions is constructed from certain threshold functions (U_∞ denotes the clone of clique functions).

Willi More

Permutation polynomials based on multivariate rational functions

Multivariate rational functions which are invertible with respect to a certain composition are called global \mathcal{P} -forms. In this paper we analyse their basic properties and give examples for specific cases. Global \mathcal{P} -forms can be used to describe permutation polynomials over finite fields by applying standard computations for multivariate polynomials over the underlying prime field.

Josef Šlapal

Thin relations and associated closure operators

We introduce the concept of thin n -ary relations (n a natural number) and study closure operators which are associated with them. It turns out that such closure operators are well-behaved with respect to connectedness. We outline the possibility of using these closure operators in digital topology. For each natural number $n > 1$, we define a certain thin n -ary relation on the set of all integers and discuss the associated closure operator. In the case $n = 2$ we get the well-known Khalimsky topology, which is frequently used for solving problems of digital topology.

Modular elements of the lattice of semigroup varieties. II

Boris M. Vernikov

Mikhail V. Volkov

We completely determine all semigroup varieties that are both modular and upper-modular elements of the lattice of all semigroup varieties as well as nilsemigroup varieties that are upper-modular elements of this lattice.

Non-extendability of semilattice-valued measures on partially ordered sets

Friedrich Wehrung

For a poset P and a distributive $\langle \vee, 0 \rangle$ -semilattice S , an S -valued poset measure on P is a map $\mu: P \times P \rightarrow S$ such that $\mu(x, z) \leq \mu(x, y) \vee \mu(y, z)$, and $x \leq y$ implies that $\mu(x, y) = 0$, for all $x, y, z \in P$. In relation with congruence lattice representation problems, we consider the problem whether such a measure can be extended to a poset measure $\bar{\mu}: \bar{P} \times \bar{P} \rightarrow S$, for a larger poset \bar{P} , such that for all $\mathbf{a}, \mathbf{b} \in S$ and all $x \leq y$ in \bar{P} , $\bar{\mu}(y, x) = \mathbf{a} \vee \mathbf{b}$ implies that there are a positive integer n and a decomposition $x = z_0 \leq z_1 \leq \dots \leq z_n = y$ in \bar{P} such that either $\bar{\mu}(z_{i+1}, z_i) \leq \mathbf{a}$ or $\bar{\mu}(z_{i+1}, z_i) \leq \mathbf{b}$, for all $i < n$.

In this note we prove that this is not possible as a rule, even in case the poset P we start with is a chain and S has size \aleph_1 . The proof uses a “monotone refinement property” that holds in S provided S is either a lattice, or countable, or strongly distributive, but fails for our counterexample. This strongly contrasts with the analogue problem for *distances* on (discrete) sets, which is known to have a positive (and even *functorial*) solution.

Kenneth Koon-Ho Wong

Gary Carter

Ed Dawson

Implementation of extension field arithmetic with applications to torus-based cryptography

We investigate the use of Karatsuba multiplication and squaring algorithms over finite extension fields with respect to different bases. The notions of multiplication tables and their complexities for normal bases are extended to general bases. Some implementation issues of the Karatsuba method on different bases are presented. Comparisons are made between complexities of multiplication and squaring tables and their algorithms. Applications of extension field arithmetic to torus-based cryptography is described, and we give costs of arithmetic in the implementations.

Alle books in the series “Contributions to General Algebra” can be ordered from

Verlag Johannes Heyn

Friedensgasse 23

9020 Klagenfurt

Kramergasse 2-4

Telefon: +43 463 / 33 631

Fax: 43 463 / 33 631 33

email: verlag@heyn.at

See also <http://dmg.tuwien.ac.at/fg1/aaa/>.