

## ABSTRACTS

Gene Abrams\*, University of Colorado; Gonzalo Aranda Pino, Universidad de Malaga, Spain.

Abstract Title: The Leavitt path algebra of a graph.

Abstract: For any row finite graph  $E$  and any field  $K$  we construct the *Leavitt path algebra*  $L(E)$  having coefficients in  $K$ . When  $K$  is the field of complex numbers, then  $L(E)$  is the algebraic analog of the Cuntz Krieger algebra  $C^*(E)$ . The matrix rings  $M_n(K)$  and the Leavitt algebras  $L(1, n)$  appear as algebras of the form  $L(E)$  for various graphs  $E$ . In our main result, we give necessary and sufficient conditions on  $E$  which imply that  $L(E)$  is simple.

abrams@ math.uccs.edu, gonzalo@ agt.cie.uma.es

Mekei Abish, Institute of Mathematics of the National University of Mongolia, Mongolia.

Abstract Title: On local finite varieties of associative rings.

Abstract: The variety of associative rings is called *finite embedding variety* if all finite rings of it are embeds in matrix rings over some commutative rings.

Theorem. local finite variety of associative rings satisfying the identities of the following type:

$$p^k x = 0, x^3 f(x) + x^2 = 0,$$

where  $f(x) \in Z[x]$ ,  $p$ -prime number,  $p \neq 2$ ,  $k \geq 2$  natural number, is finitely embedding variety.

Corollary. local finite variety of associative rings satisfying identities of type:

$$nx = 0, x^3 f(x) + x^2 = 0$$

where  $n > 1$ ,  $n$  is natural number,  $(n, 2) = 1$ ,  $f(x) \in Z[x]$ , is finitely embedding variety.

mekei@ yahoo.com

Adel N. Alahmadi, Ohio University; S.K.Jain, Ohio University; Pramod Kanwar\*, Ohio University - Zanesville; J.B.Srivastava, Indian Institute of Technology, Delhi, India.

Abstract Title: Group rings with generalized injectivity conditions (Preliminary Report).

Abstract: In this paper we study group algebras satisfying certain generalized injectivity conditions like almost injectivity (considered by Y. Baba et.al), and continuity (considered by von-Neumann). We are investigating structure of continuous group rings and in particular, regular continuous group rings.

aa272991@ohio.edu, jain@math.ohiou.edu, pkanwar@math.ohiou.edu, jbsrivas@maths.iitd.ernet.in

Adem Ozturk, Umh Universite de Mons Hainaut, Belgium.

Abstract Title: Wedderburn Polynomials over Division Rings, II.

Abstract: A polynomial  $f(t)$  in an Ore extension  $K[t; S, D]$  over a division ring  $K$  is a Wedderburn polynomial if  $f(t)$  is monic and is the minimal polynomial of an algebraic subset of  $K$ . These polynomials have been studied in [?]. In this paper, we continue this study and give some applications to triangulation, diagonalization and eigenvalues of matrices over a division ring in the general setting of  $(S, D)$ -pseudo-linear transformations. In the last section we introduce and study the notion of  $G$ -algebraic sets.

ozturk@umh.ac.be

Asma Ali, Department of mathematics, Aligarh Muslim University, India.

Abstract Title: Decomposition of Certain Periodic Rings and Near Rings.

Abstract: An interesting result which appeared in Amer. Math. Monthly 93(1986) establishes a decomposition theorem for rings satisfying the condition  $(xy)^n = xy$ , for all  $x, y \in R$  with  $n = n(x, y) > 1$ . Later Ligh and Luh [Amer. Math. Monthly 96(1989)] proved that such rings are direct sums of  $J$ -rings( i.e., the rings satisfying Jacobson's " $x^n = x$ " property) and zero rings. Further, Bell and Ligh [Math. J. Okayama Univ. 31(1989)] considered the related properties like  $xy = (xy)^2p(xy)$  or  $xy = (yx)^2p(yx)$  where  $p(X) \in Z[X]$ . In the present paper we shall establish a decomposition theorem for rings satisfying any one of the conditions (i)  $xy = (xy)^n p(x, y)$ , (ii)  $xy = (yx)^n p(x, y)$ , (iii)  $xy = (yx)^n p(y, x)$ , (iv)  $xy = y^m x^n p(x, y)$ , where  $m = m(x, y) \geq 1$ ,  $n = n(x, y) \geq 1$  and  $p(x, y) \in Z[X, Y]$ , the ring of polynomials in two noncommuting indeterminates  $X$  and  $Y$ . Further we shall deduce the commutativity of such rings. Finally some related theorems are obtained for near rings.

asma786@postmark.net

Pere Ara\* and Maria Moreno, Universitat Autònoma de Barcelona, Spain.

Abstract Title: Nonstable  $K$ -theory for graph algebras.

Abstract: We introduce a new class of  $K$ -algebras associated with an oriented graph  $E$ , the Leavitt path algebras  $L_K(E)$ . These algebras generalize Leavitt algebras of type  $(1, n - 1)$ , which are algebras with a universal isomorphism between the free module of rank 1 and the free module of rank  $n$ . We compute the

monoid  $V(L_K(E))$  of isomorphism classes of finitely generated projective modules over  $L_K(E)$ , and we show that this monoid satisfies the refinement property and separative cancellation. We also show that there is a natural isomorphism between the lattice of graded ideals of  $L_K(E)$  and the lattice of order-ideals of  $V(L_K(E))$ . When  $K$  is the field  $C$  of complex numbers, the algebra  $L_C(E)$  is a dense subalgebra of the Cuntz-Krieger graph  $C^*$ -algebra  $C^*(E)$ , and we show that the inclusion map induces an isomorphism between the corresponding monoids.

para@mat.uab.es

Sushil Kumar Azad\*, Rajdhani College, University of Delhi, India; Manmohan, Delhi College of Engineering, India.

Abstract Title: LFSR based Shift Register.

Abstract: Stream Cipher are very popular cryptosystems used in cryptography because of their high encryption rate . We propose a new Stream Cipher based on LFSR whose encryption rate is comparable to the existing standard algorithms. The time complexity for our algorithm is improved over the others . We have extensively checked the randomness of the sequence produced by our cryptosystem.

azadsk2000@ yahoo.co.in, rock\_instyle@ yahoo.com

Mamadou Barry, Universite Cheikk Anta Diop Dakar, Senegal.

Abstract Title: On Commutative FGI rings.

Abstract: Let  $R$  be a ring. An  $R$ -module  $M$  is said to have property  $(I)$  if every injective endomorphism of  $M$  is an automorphism of  $M$ . Let  $F_R$  be the class of finitely generated  $R$ -modules and  $I_R$  the class of  $R$ -modules satisfying property  $(I)$ . In this note we characterize commutative rings for which  $F_R = I_R$ .

mansabadion1@hotmail.com

Silvana Bazzoni, Dipartimento di Matematica Pura e Applicata, Dolors Herbera\*, Universitat Autònoma de Barcelona, Spain.

Abstract Title: Tilting modules are of finite type.

Abstract: A right  $R$ -module  $T_R$  is said to be a tilting module if the class of modules generated by  $T_R$  coincides with  $T_R^\perp = \text{Ker Ext}_R^1(T_R, -)$ . In this talk

we want to present the result that tilting modules are of finite type. That is, if  $T_R$  is a tilting module then there exists a set  $\mathcal{S}$ , consisting of finitely presented right  $R$ -modules of projective dimension at most one, such that

$$T_R^\perp = \mathcal{S}^\perp = \bigcap_{S \in \mathcal{S}} \text{Ker Ext}_R^1(S, -).$$

dolors@mat.uab.es

Gary Birkenmeier\*, University of Louisiana at Lafayette; Adnan Tercan, Hacettepe University, Turkey; Evrim Yurttagul, University of Warwick, England.

Abstract Title: Close to the Extending Condition but not There.

Abstract: In this talk we introduce the concept of an E-extending (i.e., essentially extending) Module. A module  $M$  is "E-extending" if each submodule  $Y$  is an essential extension of a submodule  $X$ , where  $X$  is also essential in a direct summand of  $M$ . We present numerous examples and basic results for E-extending modules. Moreover, connections between the E-extending concept and other generalizations of the extending concept are considered.

gfb1127@ louisiana.edu

Matej Bresar, University of Maribor, Slovenia.

Abstract Title: Characterizing homomorphisms and derivations in rings with idempotents.

Abstract: An additive map  $d$  from a ring  $A$  into an  $A$ -bimodule  $M$  is called a *local derivation* if for every  $x \in A$  there exists a derivation  $d_x : A \rightarrow M$  such that  $d(x) = d_x(x)$ . A map  $h$  from a ring  $A$  into a ring  $B$  is called a *zero product preserving* map if  $xy = 0$  with  $x, y \in A$  implies  $h(x)h(y) = 0$ . These two types of maps have different backgrounds, and they are seemingly unrelated. However, we shall present a condition that covers both of them, and makes it possible for us to obtain new results for each of them. Our approach is based on the existence of nontrivial idempotents.

bresar@ uni-mb.si

Hans H Brungs, University of Alberta, Edmonton, Canada.

Abstract Title: Rank one Chain Domains.

Abstract: A classification of rank one chain domains based on the group of divisorial ideals is given. Examples for the infinitely many classes of exceptional chain domains are constructed where this problem is first solved for exceptional cones in groups.

brungs@ualberta.ca

Jungyoon Byun, University of Pennsylvania.

Abstract Title: Renormalization, Bonsai and Homological Algebra.

Abstract: As an approximation to the Hopf algebra introduced by Connes-Kreimer, we construct a new Hopf algebra structure by considering actual shapes of Feynman diagrams. It has a basis consisting of forests of tree diagrams having a finite upper bound of their branching numbers. We call such a tree diagram.

jbyun@ math.upenn.edu

Victor Camillo, University of Iowa; Dinesh Khurana, Punjab University, India; T.Y.Lam\*, University of California, Berkeley.

Abstract Title: Continuous Modules Are Clean.

Abstract: The title means that the endomorphism ring of any continuous module  $M$  is a clean ring. In other words, any endomorphism of  $M$  is the sum of a projection and an automorphism. This implies the well-known result that continuous modules satisfy the (finite) exchange property. Our results also show that the class of clean modules is quite rich: for instance, semisimple modules, quasi-injective modules, Harada modules, discrete modules, and co-Hopfian CS modules are all clean. On the ring-theoretic level, right continuous rings and right self-injective rings are clean. This expository talk will place the above results in the larger context of exchange theory and the theory of direct sum decompositions of modules.

lam@math.berkeley.edu

Alexander DIESL\*, Gautam BOROORAH, and Thomas J. DORSEY; University of California Berkeley.

Abstract Title: Local Rings  $R$  for which  $T_n(R)$  is Strongly Clean.

Abstract: A ring  $R$  is called clean if every element  $r$  in  $R$  can be written in the form  $r = e + u$  for some idempotent  $e$  and some unit  $u$  in  $R$ . A ring is further called strongly clean if such a decomposition exists with  $eu = ue$ . If  $R$  is a local ring, then  $R$  is strongly clean, and the ring,  $T_n(R)$ , of upper-triangular matrices over  $R$  is clean. We will investigate conditions on the local ring  $R$  which force  $T_n(R)$  to be strongly clean and also give some examples of such rings.

adies1@math.berkeley.edu

Marten van DIJK; MIT Computer Science and Artificial Intelligence Laboratory.

Abstract Title: Dynamical ElGamal based Signature Verification.

Abstract: We investigate the problem of speeding up signature verification by a slow processor in an application with no power limitation and where communication costs are not an issue. To verify a generalized ElGamal signature the verifier computes exponentiations in a finite field by using the square and multiply method. To reduce the costs of signature verification we increase the signature by including the intermediate results of the square and multiply method. This means that, instead of the verifier, the signer performs the exponentiations. If the finite field has characteristic 2 (such that squaring is a linear operation), the verifier can use cheap linear binary checks to verify the correctness of the intermediate and final results. If  $s$  is the number of binary checks, then an adversary can successfully impersonate a signature with probability  $2^{-s}$ . If for each verification the  $s$  binary checks are randomly selected, then the probability of a successful impersonation is independent of previous successful attempts (assuming that the secret of the signer remains private). This means that  $s$  can be small and since  $s$  is proportional to the workload of the verifier, our method speeds up the signature verification.

marten@csail.mit.edu

Rad Dimitric, Texas A &M University.

Abstract Title: Algebraic Compactness of  $\prod M_\alpha / \oplus M_\alpha$ .

Abstract: For most part this note is about modules over countable rings. If the ring in question is the integers or if all the  $M_\alpha$  coincide, the question has been settled well. We are interested in the remaining cases, where not all is known, as far as pure injectivity of the quotient from the title.

dimitric@ tamug.edu

Jintai Ding, University of Cincinnati.

Abstract Title: Perturbation of Multivariable Public Key Cryptosystems.

Abstract: Public key cryptography is an indispensable part of our modern communication systems. However, quantum computers can break cryptosystems like RSA, which are based on “hard”; number theory problems. Recently a great effort has been put into the search for alternative public key cryptosystems. Multivariable public key cryptosystems (MKPC) provide one such promising alternative. Their theoretical security assumption comes from the fact that solving a system of polynomial equations over a finite field is in general NP-hard and quantum computers are not yet shown to be effective in solving this problem. Furthermore, computations in a finite field can be more efficient than manipulating larger and larger numbers, as required by the systems based on number theoretical problems. There are a few such systems, for example, the Matsumoto-Imai, the Sflash, the HFE, the HFEv, the Dragon, the Oil-Vinegar, the TTM. Though some of them are broken, the promising future of this new family of cryptosystems is manifested in Sflash, which was accepted as one of the final selections for low cost smart cards in the New European Schemes for Signatures, Integrity, and Encryption (NESSIE). Recently we proposed a new idea, *internal perturbation* to improve the security and therefore the efficiency of MPKC. The idea comes from a similar idea in a continuous system where in order to understand the structure of the system, one often perturbs the system in a controlled way to see how the system changes accordingly. Roughly speaking, the perturbation should be small-scale controlled “noise”. More specifically, for any MPKC, a small dimensional subspace of the message space  $k^n$  is used to perform the small-scale perturbation. Here  $k$  is a small finite field. The dimen-

sion  $r$  of this subspace is chosen to be very small compared with  $n$  so that we maintain control of the system. In this talk, we will first give a brief introduction of multivariable public key cryptosystems, then we will present our results on internal perturbation of MKPCs: the perturbed Matsumoto-Imai cryptosystems, the internal perturbed Hidden Field Equation (HFE) cryptosystems and the perturbed Hidden Matrix (HM) cryptosystems.

ding@math.uc.edu

Jintai Ding, University of Cincinnati; Jason E. Gower, University of Cincinnati; Dieter Schmidt, University of Cincinnati; Christopher Wolf, Belgium; and Zhijun Yin\*, University of Cincinnati.

Abstract Title: Attack Complexity of the  $F_4$  on the Perturbed Matsumoto-Imai Cryptosystem

Abstract: Using Magma's implementation of the  $F_4$  Gröbner basis algorithm, we attack the perturbed Matsumoto-Imai (PMI) cryptosystem proposed at PKC 2004 by Ding with parameters  $q = 2$ ,  $14 \leq n \leq 59$ , and  $0 \leq r \leq 10$ . Here,  $q$  is the number of field elements,  $n$  the number of equations/variables, and  $r$  the perturbation dimension. Based on our experimental results, we give estimates for the running time for such an attack. We use these estimates to judge the security of some proposed schemes, and we suggest more efficient schemes. In particular, we estimate that an attack using  $F_4$  against the parameters  $q = 2$ ,  $n = 97$ ,  $r = 5$  (suggested in the original paper by Ding) has a time complexity of less than  $2^{50}$  3-DES computations, i.e., would be considered insecure for nowadays applications.

ding@math.uc.edu

Hai Q Dinh, Kent State University, Trumbull .

Abstract Title: Some classes of Repeated-Root Constacyclic Codes over Integer Modulo  $2^m$

Abstract: We investigate the classes of  $(2^\theta - 1)$ -constacyclic codes of length  $2^t$  over  $Z_{2^m}$ , for positive integers  $t, m, \theta$  such that  $2 \leq \theta \leq m$ , which are generalizations of repeated-root negacyclic codes. It will be showed that the ring  $\frac{Z_{2^m}[x]}{\langle x^{2^t} + 1 - 2^\theta \rangle}$  is a finite chain ring, and such codes form a chain as ideals of this ring. Among other results, Hamming distances of such codes are also obtained for  $t = 2, 3, 4$ .

hdinh@kent.edu

Driss Drissi; Kuwait University, Kuwait.

Abstract Title: On positive definite solutions of generalized Lyapunov type matrix equations.

Abstract: Using Schur-Hadamard multiplier and Bochner's classical theorem, we establish the positive definiteness of solutions of matrix equations Lyapunov type.

drissi@mcs.sci.kuniv.edu.kw

Nguyen Viet Dung, Ohio University-Zanesville.

Abstract Title: Endofinite modules and pure semisimple rings.

Abstract: Let  $R$  be a right pure semisimple ring, i.e. a ring  $R$  such that every right  $R$ -module is a direct sum of finitely generated modules. It is proved that  $R$  is of finite representation type if and only if every finitely presented indecomposable right  $R$ -module is endofinite, if and only if every finitely presented right  $R$ -module has a left artinian endomorphism ring. As applications, we obtain various new criteria for a right pure semisimple ring to be of finite representation type. (This is joint work with Jose Luis Garcia, University of Murcia, Spain).

nguyend2@ohiou.edu

Noyan Er, University of Rio Grande.

Abstract Title: On rings and lifting modules.

Abstract: A module  $M$  is called a lifting module if every submodule  $A$  of  $M$  contains a direct summand  $K$  of  $M$  such that  $A/K$  is a small submodule of  $M/K$ . This property is not preserved by direct sums. In a recent paper we have obtained the following results: A ring  $R$  is right Noetherian with indecomposable injective right  $R$ -modules hollow iff every injective is a direct sum of lifting modules. This is a non-Artinian generalization of Harada rings. Consider a family  $\{N_i : i \in I\}$  of finitely generated modules such that  $M = \bigoplus_{i \in I} N_i$  is lifting with  $J(M)$  small in  $M$ . Then for any countable sequence  $(f_k : N_{i_k} \rightarrow N_{i_{k+1}})$  of epimorphisms with distinct  $i_k$ , all but finitely many terms are isomorphisms. If  $N_i$  are local (possibly without local endo-ring), then the family  $\{N_i : i \in I\}$  is locally semi-T-nilpotent. Corollaries relate the lifting property to Hopficity and the exchange property, and characterize finitely generated modules  $M$  such that  $M^N$  is lifting with small radical. In particular, for any local module  $M$  over a (right)  $B$ (Bass)-ring,  $M^N$  is lifting iff  $M$  is quasi-projective.

noyaner@yahoo.com

Alberto Facchini, University of Padova, Italy. Abstract Title: On the Weak Krull-Schmidt Theorem.

Abstract: Let  $R$  be a ring. Two right  $R$ -modules  $U$  and  $V$  belong to the same monogeny class ( $[U]_m = [V]_m$ ) if there exist a monomorphism  $U \rightarrow V$  and a monomorphism  $V \rightarrow U$ . Dually,  $U$  and  $V$  belong to the same epigeny class ( $[U]_e = [V]_e$ ) if there exist an epimorphism  $U \rightarrow V$  and an epimorphism  $V \rightarrow U$ . A module is biuniform if it is uniform and couniform, that is has Goldie dimension one and dual Goldie dimension one. **Weak Krull-Schmidt Theorem for biuniform modules** Let  $U_1, \dots, U_n, V_1, \dots, V_t$  be biuniform right modules over an arbitrary ring  $R$ . Then the direct sums  $U_1 \oplus \dots \oplus U_n$  and  $V_1 \oplus \dots \oplus V_t$  are isomorphic if and only if  $n = t$  and there are two permutations  $\sigma, \tau$  of  $\{1, 2, \dots, n\}$  such that  $[U_i]_m = [V_{\sigma(i)}]_m$  and  $[U_i]_e = [V_{\tau(i)}]_e$  for every  $i = 1, 2, \dots, n$ . We will make a survey on results about the Weak Krull-Schmidt Theorem obtained by A. Facchini, N. V. Dung, G. Puninski and P. Prihoda during the past ten years.

facchini@math.unipd.it.

Edward Formanek, Pennsylvania State University.

Abstract Title: Some Approaches to the Jacobian Conjecture in Two Variables  
Abstract: Let  $f(x, y), g(x, y) \in C[x, y]$ . Then  $x \rightarrow f(x, y), y \rightarrow g(x, y)$  defines an endomorphism  $\varphi : C[x, y] \rightarrow C[x, y]$ . Associated with  $\varphi$  is its Jacobian matrix.

$$J(\varphi) = \begin{pmatrix} \partial f / \partial x; \partial f / \partial y \\ \partial g / \partial x; \partial g / \partial y \end{pmatrix}$$

The chain rule shows that if  $\varphi$  is invertible, then  $J(\varphi)$  is invertible. The Jacobian Conjecture is the converse: If  $J(\varphi)$  is invertible, then  $\varphi$  is invertible. I will discuss some aspects of this conjecture.

formanek@math.psu.edu

Pedro A Guil-Asensio, Universidad de Murcia, Spain.

Abstract Title: Hereditary rings with countably generated injective hull  
Abstract: Let  $R$  be a right hereditary ring. We prove that if the injective envelope of  $R_R$  is countably generated, then  $R$  is right noetherian. As a corollary, we show that  $R$  is right noetherian when its injective hull is finitely generated. This solves an open question posed by N.V. Dung, J.L. Gomez Pardo and R. Wisbauer fifteen years ago. (Joint with Hai Q Dinh and Sergio R Lopez-Permouth).

paguil@um.es

Pedro A Guil-Asensio, Universidad de Murcia; Husain Alhazmi\* and Adel Alahmadi, Ohio University.

Abstract Title: On Countably Sigma CS Modules.

Abstract: A module  $M$  is called CS if every submodule is essential in a direct summand. And it is called  $\Sigma$ -CS if every direct sum of copies of  $M$  is CS. It is known that any  $\Sigma$ -CS module is a direct sum of indecomposable and that  $M$  is  $\Sigma$ -CS whenever an uncountable direct sum of copies of  $M$  is CS. There exist examples of countably  $\Sigma$ -CS modules that are not  $\Sigma$ -CS but in all of them the module fails to be a direct sum of uniforms. In this work we study sufficient conditions that force a direct sum of uniform modules to be  $\Sigma$ -CS provided that it is countably  $\Sigma$ -CS.

paguil@fcu.um.es, h3497@yahoo.com, adelnife2@yahoo.com

Lakhdar Hammoudi, Ohio University, Chillicothe.

Abstract Title: Combinatorial methods in nil-algebras.

Abstract: A finitely generated non-nilpotent nil-algebra is of the form  $\mathcal{F}/I$  where,  $\mathcal{F}$  is a finitely generated free algebra and  $I$  is an ideal. In constructing such algebras we have to deal with two problems. The first one is a question of quantity. How many polynomials of each degree should we put in  $I$ ? The second one is a question of quality. Which polynomials should we put in  $I$ ? In this talk we will explore through concrete examples the impact of our choices of polynomials on the constructed algebras  $\mathcal{F}/I$ .

hammoudi@ohio.edu

Ivo Herzog; The Ohio State University.

Abstract Title: Flat cotorsion modules.

Abstract: The category  $R$ -Flat of flat left  $R$ -modules is a locally finitely presented additive category and so admits a theory of purity. The pure-injective objects of  $R$ -Flat are the cotorsion flat  $R$ -modules. We will survey our work (joint with P.A. Guil Asensio) which attempts to generalize to flat cotorsion modules classical results on pure-injective modules.

ihertzog@lima.ohio-state.edu

Tim Hodges, University of Cincinnati.

Abstract: To be inserted.

timothy.hodges@uc.edu

J. Carmelo Interlando, Notre Dame University.

Title: Multiplicative Complexity of Quadratic Boolean Functions.

Abstract: Motivated by applications of gate complexity to cryptography, we consider the following problem. Given a quadratic Boolean function  $q: B^n \rightarrow B$ , where  $B = \{0, 1\}$ , determine the minimum number  $g$  of AND gates needed to compute  $q$ . This number is called the multiplicative complexity of  $q$ . Through the use of linear transformations, we give an algebraic criterion to compute  $g$ . Moreover, a constructive algorithm to compute  $q$  with  $g$  multiplications is provided. Finally, we show that at most  $\lceil n/2 \rceil$  multiplications are required, where  $\lceil \cdot \rceil$  denotes the greatest integer function.

jinterla@nd.edu

Charles R. Johnson; William and Mary.

Abstract Title: Eigenvalues, Multiplicities and Graphs.

Abstract: The graphs of an  $n$ -by- $n$  real symmetric matrix  $A=(a_{ij})$  is the undirected graph  $G(A)$  on vertices  $1, \dots, n$  in which there is an edge between  $i$  and  $j$  iff  $a_{ij}$  is not 0. Let  $S(G)$  denote the set of all  $n$ -by- $n$  real symmetric matrices whose graph is  $G$ . There is no restriction placed by  $G$  upon the diagonal entries of matrices in  $S(G)$ . We are interested in the possible lists of multiplicities of the eigenvalues among matrices in  $S(G)$ . In general, the graph places significant restrictions on those multiplicities. Recent work on this problem, including maximum multiplicity, minimum number of distinct eigenvalues and the number of 1.

crjohnso@math.wm.edu

S.K.Jain, Ohio University; Ajit Iqbal Singh, University of Delhi, India; Ashish K. Srivastava\*, Ohio University.

Abstract Title: Self-injectivity of Group Algebras of Locally Compact Groups (Preliminary Report).

Abstract: In this paper, it is shown that the group algebra  $L^1(G, A)$  of a locally compact group  $G$  over a commutative Banach algebra  $A$  with identity is right self-injective if and only if  $A$  is self-injective and  $G$  is finite. A part of the intersection of  $L^1(G)$  and maximal right ring of quotients of classical group algebra  $K[G]$  is described for the case when  $G$  is an infinite discrete group possessing a properly ascending chain of subgroups.

jain@math.ohiou.edu, aisingh@sify.com, ashish@math.ohiou.edu

Benjamin Johnson and Nuh Aydin\*, Kenyon College.

Abstract Title: An improved algorithm to search for multitwisted codes.

Abstract: Observing that many important classes of linear codes such as cyclic and quasi-cyclic codes are weight invariant under certain transformations, we develop new algorithms to compute weight enumerators of some classes of codes more efficiently. The most general class that the algorithms applies to is what we call the class of multitwisted codes that include quasi-cyclic codes as a special case. The computer implementation of the algorithm is ongoing.

aydinn@kenyon.edu

Delaram Kahrobaei\*, University of St Andrews, Scotland; Bettina Eick, Institut Computational Mathematics, TU Braunschweig, Germany.

Abstract Title: Removing Commutativity from the Classical Cryptography: An Algebraic Approach.

Abstract: The idea I am discussing in this talk, is removing commutativity from the classical cryptology schemes (which uses finite fields (special cyclic groups)); initiated by Anshel-Anshel-Goldfeld in 1999. We introduced polycyclic groups as the best new platform for cryptology. The novelty of our approach is that

polycyclic groups are a natural generalization of cyclic groups with much more complex algorithmic structures this promises to be a more substantial platform and more secure than the existing cryptosystems. Note that nilpotent groups could be regarded as an example of polycyclic groups and the solvable groups which are not polycyclic, are not appropriate. In this talk I will explain Eick-Kahrobaei cryptosystem.

dk16@st-and.ac.uk,

Oukhtite Lahcen, Département de Mathématiques, F.S.T. Errachidia, Morocco.  
Abstract Title: Witt group over a noncommutative discrete valuation ring.

Abstract: In this work, we investigate hermitian forms on finitely generated torsion modules over a noncommutative discrete valuation ring. We also give some results for lattices, which still are satisfied even if the base ring is not commutative. Moreover, for a noncommutative discrete valued division algebra  $D$  with valuation ring  $R$  and residual division algebra  $\bar{D}$ , we prove that  $W(\bar{D}) \cong WT(R)$ , where  $WT(R)$  denotes the Witt group of regular hermitian forms on finitely generated torsion  $R$ -modules.

oukhtite@ math.net

Saad Mohamed, Ain Shams University, Cairo, Egypt.

Abstract Title: Internal Exchange Rings.

Abstract: The exchange property was established for injective, quasi-injective and continuous modules. Quasi-continuous modules do not enjoy even the finite exchange property. However, quasi-continuous modules possess the internal exchange property, and if it has the finite exchange property, then it has the full exchange property. Extending modules, do not have the finite internal exchange property. For such modules we investigate whether the finite (internal) exchange property implies the full (internal) exchange property. We obtain some partial results, but the general case is still wide open. Besides we characterize the (finite) internal exchange property in terms of the endomorphism rings. Similar to exchange rings, we define internal exchange rings. We prove that a module has the finite internal exchange property if and only if its ring of endomorphisms is an internal exchange ring.

saad323@hotmail.com

Yuri Movsisyan, Iowa State University.

Abstract Title: Binary Representations of Semigroups and Groups

Abstract: We will discuss binary representations of semigroups and groups. In particular, the characterizations of multiplicative groups of Gratzner algebras are presented.

yurimovsisyan@yahoo.com

R. Cignoli, University of Buenos Aires and D. Mundici, University of Florence  
Abstract Title: Stone duality for Dedekind sigma-complete lattice-ordered groups with order-unit

A fundamental representation theorem [1] by Goodearl, Handelman and Lawrence states that every Dedekind sigma-complete lattice-ordered group  $G$  with order-unit can be represented by continuous functions over the maximal spectrum of  $G$ . On the other hand, Dedekind sigma-complete lattice-ordered group with order-unit are categorically equivalent to sigma-complete MV-algebras, and as such they constitute a basic building block for an interesting non-boolean extension of algebraic probability theory; see [2].

We give a purely topological representation (specifically, a categorical duality) for a large class  $C$  of Dedekind sigma-complete lattice-ordered groups  $G$  with strong unit  $u$ .  $C$  includes the class  $B$  of all  $G$ 's where  $u$  has a finite index of nilpotence. By a result of Goodearl, any such  $G$  arises via  $K_0$  from some regular, biregular ring with bounded index. Our duality is a far reaching generalization of the well known Stone duality between sigma-complete boolean algebras and basically disconnected compact Hausdorff spaces.

mundici@math.unifi.it

Barbara L Osofsky, Rutgers University.

Abstract Title: Quasideterminants, Division Rings, and Twisted Polynomial Rings.

Abstract: T. Y. Lam in a 1986 paper introduced a generalized Vandermonde determinant over a not necessarily commutative division ring  $D$  with an endomorphism  $\sigma$ , and in a 1988 paper he and A. Leroy generalized this to include a  $\sigma$ -derivation  $\delta$  and computed the rank of a generalized Vandermonde matrix. The computation used properties of the principal left ideal domain  $D[t; \sigma, \delta]$ . With a totally different end in mind, I. Gelfand and V. Retakh and others introduced the concept of quasideterminant for noncommutative rings, especially division rings. Their approach gave information for Vandermonde matrices of full rank only, as the quasideterminant is defined only in the case of full rank.

Specifically, it gave some factorizations in the division ring itself. They then used these factorizations to develop very interesting rings  $Q_n$  over a free division ring that have very nice homological properties. Their approach also set the stage for Robert Wilson to prove about the best theorem one can hope for about symmetric functions of independent noncommuting variables in a division algebra. Many concepts from commutative algebra were translated into the language of quasideterminants in the noncommutative case. In this talk I start with a single lemma which is basic to the work of Lam, and show how, in the full rank case, it leads to a factorization of what turns out to be the Vandermonde quasideterminant. I then discuss quasideterminants and some of the results mentioned above.

osofsky@math.rutgers.edu

James M Osterburg, University of Cincinnati.

Abstract Title: The Final Value Problem.

Abstract: A polynomial form  $f$ , is a not necessarily linear map, from an infinite module over a ring  $Z$  to a finite abelian group of exponent  $n$  satisfying some additional conditions. Denote the zeros of  $f$  by  $\Omega_f$ . We show it satisfies a weak closure condition. Among all  $Z$ -submodules of finite index, there is a submodule  $B$  such that  $|f(B)|$  (the order of the subset  $f(B)$ ) is as small as possible.  $f(B)$  is called the *final value of  $f$*  and D. S. Passman asks if  $f(B)$  is necessarily a subgroup of  $S$ . This paper shows that if the degree of  $f \leq 2$  then the final value is a subgroup and if the form  $f$  has arbitrary degree from an f.g. infinite abelian group, then the final value is 0.

james.osterburg@uc.edu

Jae Keol Park, Pusan National University, South Korea.

Abstract Title: An Essential Extension with Nonisomorphic Ring Structures.

Abstract: We call a ring  $T$  a *right essential overring* of a ring  $R$  if  $T$  is an overring of  $R$  such that  $R_R$  is essential in  $T_R$ . Let  $A = Z_4$  and let  $R = \begin{pmatrix} A; 2A \\ 0; A \end{pmatrix}$ .

Osofsky shows that any injective hull of  $R_R$  does not have a ring structure with a multiplication extending the right  $R$ -module multiplication over  $R$ . We discuss all possible distinct right essential overrings of  $R$ . In particular, there exists an essential extension  $S_R$  of  $R_R$  such that  $S$  has exactly four distinct right essential overring structures for which some of them are not ring isomorphic. These considerations motivate the following question: *For a ring  $A$ , assume that  $E(A_A)$  has ring structures with multiplications extending the right  $A$ -module multipli-*

cation over  $A$ . Then are all these ring structures ring isomorphic? Also we discuss various types of right ring hulls of  $R$ , for example, right FI-extending, right extending, right quasi-continuous ring hulls, etc. Furthermore, we see that there exists no right quasi-continuous right ring hull of  $R$  unlike the right quasi-continuous module hull of a module which always exists by a result of Goel and Jain. (This is a joint work with G. F. Birkenmeier and S. T. Rizvi).

jkpark@pusan.ac.kr

Donald S. Passman, University of Wisconsin.

Abstract Title: Ideals in Group Rings of Locally Finite Groups.

Abstract: Let  $K[H]$  denote the group algebra of an infinite locally finite group  $H$ . In recent years, the lattice of ideals of  $K[H]$  has been extensively studied under the assumption that  $H$  is simple. From these many results, it appears that such group algebras tend to have very few ideals. While some work still remains to be done in the simple group case, we nevertheless move on to the next stage of this program by considering certain abelian-by-(quasi-simple) groups. Standard arguments reduce this problem to that of characterizing the ideals of an abelian group algebra  $K[V]$  stable under the action of an appropriate automorphism group of  $V$ . Specifically, we are interested in the case where  $G$  is a quasi-simple group of Lie type defined over an infinite locally finite field  $F$ , and where  $V$  is a finite-dimensional vector space over a field  $E$  of the same characteristic  $p$ . If  $G$  acts nontrivially on  $V$  by way of the homomorphism  $G \rightarrow \text{GL}(V)$ , and if  $V$  has no proper  $G$ -stable subgroups, then we show that the augmentation ideal  $\omega K[V]$  is the unique proper  $G$ -stable ideal of  $K[V]$  when the characteristic of  $K$  is different from  $p$ . The proof of this result requires, among other things, that we study characteristic  $p$  division rings  $D$ , certain multiplicative subgroups  $M$  of  $D$ , and the action of  $M$  on the group algebra  $K[A]$ , where  $A$  is the additive group of  $D$ . In this talk, we discuss some of the preliminary results required here, some of the techniques used, and some open questions and conjectures.

passman@math.wisc.edu

Michael R. Penkava, University of Wisconsin-Eau Claire.

Abstract Title: Miniversal deformations and moduli spaces of algebra structures.

Abstract: In studying the deformations of algebras, the moduli space of all algebra structures on a space of fixed dimension is studied by classification of the structures up to isomorphism. The moduli space may consist of some families of related structures and some special cases. But how is this moduli space really

glued together? By studying the miniversal deformations of the elements in the moduli spaces, one obtains a more complete picture of what the moduli space looks like geometrically. Some recent examples will be used to illustrate some of the interesting phenomena that arise, including the role that jump deformations play in the picture of the moduli space.

penkavmr@uwec.edu

Edmund Puczyłowski; Institute of Mathematics, University of Warsaw, Poland.

Abstract Title: Some questions and results on nil rings.

Abstract: The aim of the talk is to present some results on nil rings obtained in last years. Several of them are connected with Koethe's nil ideal problem. We would also like to present some related questions.

edmundp@duch.mimuw.edu.pl

Gena Puninski, The Ohio State University, Lima.

Abstract Title: How to construct a 'real' super-decomposable pure-injective module over a string algebra.

Abstract: We give an example of a finite dimensional string algebra  $A$  and an element  $m$  of a countable direct product  $M$  of indecomposable finite dimensional  $A$ -modules, such that a 'minimal' direct summand of  $M$  containing  $m$  is super-decomposable.

puninskiy.1@osu.edu

S.Tariq Rizvi and Cosmin S Roman\*, Ohio State University, Lima.

Abstract Title: Type Decompositions for Nonsingular Extending Modules.

Abstract: A very nice type theory for nonsingular injective modules was provided in the late '70s by Goodearl and Boyle, and decomposition of such a module into five distinct types was shown. Recall that a right  $R$ -module  $M$  is called Baer if the left annihilator in  $\text{End}(M)$  of every submodule of  $M$  is a left direct summand of  $\text{End}(M)$ . We investigate the ring of endomorphisms of a Baer module and apply its properties to provide a similar type decomposition for an arbitrary, nonsingular extending module (which, in fact, holds under a weaker nonsingularity condition). This may help provide a new approach, at

least in the nonsingular case, to the still open problem of when is a direct sum of extending modules, extending. This could be done by reducing the problem to each distinct type.

rizvi.1@osu.edu, cosmin@math.ohio-state.edu

Joachim Rosenthal; University of Zurich, Switzerland and University of Notre Dame.

Abstract Title: Public Key Crypto-Systems built from Finite Simple Semirings.  
Abstract: Cryptography has a long history and its main objective is the transmission of data between two parties in a way which guarantees the privacy of the information. There are other interesting applications such as digital signatures, the problem of authentication and the concept of digital cash to name a few. The proliferation of computer networks resulted in a large demand for cryptography from the private sector. Many cryptographic protocols such as the Diffie-Hellman key exchange and the ElGamal protocol rely on the hardness of the discrete logarithm problem in a finite group. In this talk we will give a generalization of the usual Diffie-Hellman key exchange and ElGamal protocols. Crucial for this generalizations will be semi-group actions on finite sets. Our main focus point will be semi-group actions built from semi-rings and several new examples will be provided. In order to come up with new protocols it is desirable to study matrix semi-groups over finite simple semi-rings and their actions on finite semi-modules. The presented results constitute joint work with Gerard Maze and Chris Monico.

rosen@math.unizh.ch

Juan Jacobo Simón-Pinero, Universidad de Murcia, Spain.

Abstract Title: Properties of a ring reflected in infinite matrix rings.

Abstract: Let  $R$  be an associative ring with identity, and  $\alpha$  an infinite cardinal number. Let us denote by  $RFM_\alpha(R)$  the ring of row-finite  $\alpha \times \alpha$ -matrices over  $R$ . An intermediate subring of  $RFM_\alpha(R)$  is a subring  $E$  containing all matrices with only a finite number of nonzero entries. From Jacobson's notion of dual pairs of vector spaces (*Structure of Rings*, 1956) it is possible to construct intermediate subrings  $E$ , as matrix realizations of "continuous" endomorphisms or endomorphisms-with-adjoint. An old topic in ring theory is the study of the

relationship between properties of a ring  $R$  and rings of (full) matrices (finite and infinite) over  $R$ . In the case of finite matrices Morita Theory provides the necessary machinery. In this talk, we present some results on this topic in the case of some types of infinite matrix rings and subrings, from 1953 to 2004. Among other results we give a ring theoretic classification of some types of infinite matrix subrings in case the basis ring  $R$  be semisimple artinian, semi-primary, perfect, QF, artinian and noetherian.

jsimon@um.es

Mohammad Saleh, Birzeit University, Palestine.

Abstract Title: Some Open Problems On Weak Injectivity and Weak Projectivity.

Abstract: In this talk we raise some open problems on the theory of weak injectivity and weak projectivity.

msaleh@birzeit.edu

Lance Small; University of California, San Diego.

Abstract Title: Just Infinite Algebras.

Abstract: We present some general properties of these algebras relating to primitivity, semi- primitivity and various questions relating to the radical. There will be applications of generic freeness, etc.

small@math.ucsd.edu

Roxana Smarandache, Dept. of Math. and Stat.,San Diego State University.

Abstract Title : On Minimal Vectors of Codes from Finite Geometries.

Abstract: The performance of a code under maximum-likelihood decoding depends on the minimal codewords; in the context of linear programming decoding, it turns out to be necessary to know the minimal pseudo-codewords, which are vectors that correspond to codewords in a graph cover of the original code graph. In this talk we study the minimal codewords and minimal pseudo-codewords of some families of codes derived from projective and Euclidean planes. These families of codes have concise descriptions and large automorphism groups which may be used to simplify their analysis. Although our numerical results are only

for codes of very modest length, they suggest that these code families exhibit an interesting property. Namely, there seems to be a gap between the minimum pseudo-weight of all minimal pseudo-codewords that are not multiples of minimal codewords and the minimum Hamming distance of the code.

rsmarand@sciences.sdsu.edu

Robert L Snider, Virginia Tech.

Abstract Title: Periodic Groups whose Simple Modules Have Finite Central Endomorphism Dimension.

Abstract: There has been interest over the years in group rings whose simple modules are finite dimensional. A history of the problem will be discussed and the following new theorem proved. Theorem. If  $K$  is an uncountable field of characteristic 0 and  $G$  is a periodic group such that the  $K[G]$  simple modules are finite dimensional over the centers of their endomorphism rings, then  $G$  is abelian-by-finite.

snider@math.vt.edu

George Szeto and Lianyong Xue\*, Bradley University.

Abstract Title: On Galois Extensions with Automorphism Group as Galois Group.

Abstract: Let  $B$  be a ring Galois extension of  $B^G$  with Galois group  $G$  and a projective separable  $C^G$ -algebra where  $C$  is the center of  $B$ . Then it is shown that  $G = \text{Aut}_{B^G}(B)$  and  $K = \langle 1 \rangle$  where  $K = \{g \in G \mid g(c) = c \text{ for all } c \in C\}$  if and only if either  $B$  is an indecomposable DeMeyer-Kanzaki Galois extension of  $B^G$  or  $B = B^G e \oplus B^G(1 - e)$  where  $e$  and  $1 - e$  are minimal central idempotents in  $B$ . This is a generalization of the case for Galois algebras. Moreover, the class of indecomposable Galois extensions are also studied.

lxue@bradley.edu

Maribel Tocon; Universidad de Malaga, Spain, University of Ottawa, Canada.

Abstract Title: A \*-Litoff theorem for associative pairs.

Abstract: Our main task will be to characterize prime associative pairs with polarized involutions and nonzero socle, in terms of continuous operators with respect to a pair of skew-dual vector spaces over a division algebra with involu-

tion. This result was used to obtain a characteristic-free description of strongly prime Jordan pairs with socle [1]. We will show that the so-called \*-Litoff theorem for associative rings with involutions [2, 4.6.15] can be extended in a natural way to associative pairs by using the above characterization. References. [1] A. Fernandez Lopez, M. Tocon Barroso: Strongly prime Jordan pairs with nonzero socle, Manuscripta math. 111, 321-340 (2003). [2] K.I. Beidar, W.I. Martindale, A.V. Mikhaev: Rings with generalized identities. New York Basel Hong Kong, Marcel Dekker, Inc. 1976.

maribel@uma.es

Lia Vas; University of the Sciences in Philadelphia.

Abstract Title: A Class of Baer \*-Rings, Dimension and Torsion Theories.

Abstract: Many known results on finite von Neumann algebras are generalized, by purely algebraic proofs, to a certain class  $\mathcal{C}$  of finite Baer \*-rings. First, I show that a finitely generated module over a ring from the class  $\mathcal{C}$  splits as a direct sum of a finitely generated projective module and a certain torsion module. Then, I define the dimension of any module over a ring from  $\mathcal{C}$  and prove that this dimension has all the nice properties of the dimension for finite von Neumann algebras. This dimension defines a torsion theory that I prove to be equal to the Goldie and Lambek torsion theories. Moreover, every finitely generated module splits in this torsion theory.

l.vas@usip.edu

Effim Zelmanov, University of California, San Diego.

Abstract Title: Towards a Geometric Ring Theory.

Abstract: We will discuss the concepts and problems which originated in the Geometric Group Theory and which may hopefully lead to an emergence of similar methods in the theory of algebras.

ezelmanov@math.ucsd.edu

## Late Arrivals To be scheduled upon some cancellation

Le Van Thuyet, Hue University, Hue, Vietnam.

Abstract Title: GENERALIZED PP-RINGS.

Abstract: A ring  $R$  is called generalized right PP if for any  $x \in R$ , the right nonzero ideal  $x^n R$  is projective for some positive  $n$ , depending on  $x$ . In this paper, we give some characterizations of a generalized PP-ring and its generalizations via P-injectivity, AP-injectivity, or AGP-injectivity. (Received Feb 24)

sciuni@dng.vnn.vn

Ronald L. Smith, University of Tennessee.

Abstract Title: Closure Properties of Schur Complements.

Abstract: The Schur complement  $M/A$  of the square partitioned matrix  $M = [A, B; C, D]$  in which  $A$  is nonsingular is given by  $M/A = D - CA^{-1}B$ . It is well known that the Schur complement of a positive definite matrix is itself positive definite. That is, the class of positive definite matrices are closed under Schur complementation. Often, it is problematic to determine whether a class of matrices is closed under Schur complementation. In this talk we present a general approach for determining whether a given class of matrices is closed under Schur complementation. This approach is then applied to a number of matrix classes.

Ronald-Smith@utc.edu