# Noncommutative Rings and their Applications

**Lens $29^{th}$ June-$2^{nd}$ July 2009**

ABSTRACTS

## A generalization of projective covers

M. Alkan
University of Hacettepe, Ankara, Turkey.

## Prime spectrum and primitive Leavitt path algebras

G. Aranda Pino (joint work with E. Pardo and M. Siles Molina)
University of Málaga, Spain.

Leavitt path algebras of row-finite graphs have been recently introduced in [1] and [2]. They have become a subject of significant interest, both for algebraists and for analysts working in C*-algebras. The Cuntz-Krieger algebras $C^*(E)$ (the C*-algebra counterpart of these Leavitt path algebras) are described in [5].

For a field $K$, the algebras $L_K(E)$ are natural generalizations of the algebras investigated by Leavitt in [4], and are a specific type of path $K$-algebras associated to a graph $E$ (modulo certain relations). The family of algebras which can be realized as the Leavitt path algebras of a graph includes matrix rings $\mathbb{M}_n(K)$ for $n \in \mathbb{N} \cup \{\infty\}$ (where $\mathbb{M}_\infty(K)$ denotes matrices of countable size with only a finite number of nonzero entries), the Toeplitz algebra, the Laurent polynomial ring $K[x,x^{-1}]$, and the classical Leavitt algebras $L(1,n)$ for $n \geq 2$ (the latter being universal algebras without the Invariant Basis Number condition).

In this work we determine the prime and primitive Leavitt path algebras. The main inspiration springs out of the complete description of the primitive spectrum of a graph C*-algebra $C^*(E)$ carried out by Hong and Szymański in [3]. Concretely, in [3, Corollary 2.12], the authors found a bijection between the set $\mathrm{Prim}(C^*(E))$ of primitive ideals of $C^*(E)$ and some sets involving maximal tails and points of the torus $\mathbb{T}$. We give the algebraic version of this by exhibiting a bijection between the set of prime ideals of $L_K(E)$, and the set formed by the disjoint union of the maximal tails of the graph $\mathcal{M}(E)$ and the cartesian product of maximal tails for which every cycle has an exit $\mathcal{M}_\tau(E)$ and the nonzero prime ideals of the Laurent polynomial ring $\mathrm{Spec}(K[x,x^{-1}])^*$.

In addition, the primitive Leavitt path algebras are characterized. Concretely, $L_K(E)$ is left primitive if and only if $L_K(E)$ is right primitive if and only if every cycle in the graph $E$ has an exit and $E^0 \in \mathcal{M}(E)$.

## Références

[1] G. Abrams, G. Aranda Pino, The Leavitt path algebra of a graph, *J. Algebra* **293 (2)** (2005), 319–334.

[2] P. Ara, M.A. Moreno, E. Pardo, Nonstable K-Theory for graph algebras, *Algebra Represent. Theory* **10** (2007), 157–178.

[3] J. H. Hong, W. Szymański, The primitive ideal space of the $C^*$-algebras of infinite graphs, *J. Math. Soc. Japan* **56 (1)** (2004), 45–64.

[4] W.G. Leavitt, The module type of a ring, *Trans. Amer. Math. Soc.* **103** (1962), 113–130.

[5] I. Raeburn, *Graph algebras*, CBMS Regional Conference Series in Mathematics, **103**, Amer. Math. Soc., Providence, (2005).

## A Generalization of Semiregular and Almost Principally Injective Rings

Pıýnar AYDOĞDU
Hacettepe University, Ankara Turkey.

In this article, we call a ring $R$ *right almost I–semiregular* if, for any $a \in R$, there exists a left $R$–module decomposition $l_R r_R(a) = P \oplus Q$ such that $P \subseteq Ra$ and $Q \cap Ra \subseteq I$, where $I$ is an ideal of $R$, $l$ and $r$ are the left and right annihilators, respectively. This definition generalizes the right almost principally injective rings defined by Page and Zhou , $I$–semiregular rings defined by Nicholson and Yousif, and right generalized semiregular rings defined by Xiao and Tong. We prove that $R$ is $I$–semiregular if and only if, for any $a \in R$, there exists a decomposition $l_R r_R(a) = P \oplus Q$, where $P = Re \subseteq Ra$ for some $e^2 = e \in R$ and $Q \cap Ra \subseteq I$. Among the results for right almost $I$–semiregular rings, we are able to show that if $I$ is the left socle $Soc(_RR)$ or the right singular ideal $Z(R_R)$ or the ideal $Z(_RR) \cap \delta(_RR)$, where $\delta(_RR)$ is the intersection of essential maximal left ideals of $R$, then $R$ being right almost $I$–semiregular implies that $R$ is right almost $J$–semiregular, where $J$ is the Jacobson radical of $R$. We show that $\delta_l(eRe) = e\delta(_RR)e$ for any idempotent $e$ of $R$ satisfying $ReR = R$ and, for such an idempotent, $R$ being right almost $\delta(_RR)$–semiregular implies that $eRe$ is right almost $\delta_l(eRe)$–semiregular.

*(Joint work with A. Çiğdem ÖZCAN)*

## Les courbes elliptiques et leurs applications en cryptographie

Nabila Bouchakour, University of Blida, Algeria.

## Les mathématiques et la cryptographie

M'Hammad Boulagouaz
University of Fes, Marocco.

## Suites récurrentes linéaires, le cas non commutatif

A. Cherchem, T. Garici
University of USTHB-Alger, Algeria.

Les suites récurrentes linéaires ont dŠabord été étudiées sur des corps commutatifs, on trouvera dans ([1]) une très bonne bibliographie et une liste dŠapplications intéressantes de ces objets (cryptographie, codes correcteurs dŠerreurs, calcul rapide, arithmétique, etc.). Depuis les années 80, les suites récurrentes linéaires sur des modules sur des anneaux commutatifs sont apparues et ont intéressé quelques auteurs voir ([8]) pour une bibliographie complète. La notion de suite récurrente linéaire s'étend naturellement au cas de modules (à gauche) sur un anneau non commutatif. Cette généralisation peut trouver des applications en théorie des codes correcteurs d'erreurs, en particulier dans la construction de codes quasi-cycliques autoduaux ([7]). Généralement, dans le cas non commutatif, il y a perte de la structure de module : la somme de deux suites récurrentes linéaires n'est pas toujours une suite récurrente linéaire, il en est de même du produit d'une suite récurrente linéaire par les éléments de l'anneau de base. Dans la première partie de ce travail, nous donnons des conditions nécessaires pour que la somme de suites ń géométriques ż ainsi que le produit (à gauche) d'une suite géométrique par des éléments de l'anneau soit une suite récurrente linéaire. Nous établissons en particulier que l'anneau de base doit être un anneau de Ore et nous nous intéressons également à la réciproque. Dans une autre partie, nous montrons que, dans le cas dŠun anneau de matrices à coefficients dans un anneau commutatif, les suites récurrentes linéaires (de matrices ou de vecteurs) forment un module à gauche sur l'anneau de base. La preuve utilise un résultat basé sur les systèmes récursifs obtenu par l'un d'entre nous ( voir [6]). Nous en déduisons par exemple que tout anneau de matrices à coefficients dans un anneau commutatif est un anneau de Ore.

Dans la troisième partie, nous abordons le cas où l'anneau de base est un corps (non commutatif) et nous nous intéressons plus particulièrement au cas où le corps est de dimension finie sur son centre et donnons un algorithme (basé sur un résultat de Jacobson ([[5], p. 185]) qui permet, connaissant des polynômes caractéristiques de deux suites récurrentes linéaires sur le corps (non commutatif), de déterminer un polynôme caractéristique de leur somme.

*This is a joint work with A. Necer, Limoges, France*

**Références**

[1] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, Recurrence Sequences, American Mathematical Society, 2003.

[2] N. Bourbaki. Eléments de mathématique, AIII, Hermann,1970.

[3] P. M. Cohn, Skew fields, Cambridge University Press. [4] T.Y.Lam. A First course in Noncommutative Rings, Springer-Verlag, 1991.

[5] T.Y.Lam. Exercices in Classical Ring Theory, Springer-Verlag, 1995.

[6] A. Necer , Systèmes récursifs et algèbre de Hadamard de suites récurrentes linťeaires sur des anneaux commutatifs, Communications in Algebra, 27 (12), 6175Ű6189, 1999.

[7] P.-L. Cayrel, C. Chabot, A. Necer, Quasi-cyclic codes over rings of matrices, soumis ‘a -Finite Fields and their Applications

[8] A. S. Kuzmin, V. L. Kurakin, and A. A. Nechaev, Linear recurrences over rings and modules, J. Math. Sci., 76 (6), 2793Ű2915, 1995.

## Centers of Exchange Leavitt Path Algebras

Kathi Crow
American University, Cairo, Egypt.

Given a directed graph $E$ and a field $K$ one can construct the Leavitt path algebra of $E$ with coefficients in $K$, denoted $L(E)$. When $L(E)$ enjoys some finiteness condition such as being artinian, semisimple, noetherian and locally noetherian, the structure of $L(E)$ is well understood and a basis as a $K$-vector space can be found for its center. For Leavitt path algebras without these finiteness conditions we do not have structure theorems to provide us with a basis for the center, however we can still calculate the center in certain situations. For example, a simple Leavitt path algebra $L(E)$ is central (i.e. the center reduces to the base field $K$) when $L(E)$ is unital and has zero center otherwise. Moreover, this result can be extended, under some mild conditions, to the case of exchange Leavitt path algebras. (This is joint work with Gonzalo Aranda Pino.)

## Self-dual codes over rings

Steven Dougherty
Scranton University, USA.

## Relating nodal curves to finite dimensional algebras

Yuriy Drodz
University Taras Schevchenko, Ukraina.

## Partial actions of groups on algebras

Miguel Ferrero
Universty of Grande do sul, Brasilia.

In this survey lecture we recall the definition of partial actions of groups on algebras. We define enveloping action and partial skew group rings. The partial skew group ring is not always associative, but it is associative under some assumptions. We study some cases in which it is associative. Finally we will study properties relating the given ring and the enveloping ring. The results in this lecture are contained in several papers whcih have appeared recently.

## On filial and left filial algebras

Marzena Filipowicz-Chomko
Technical University of Białystok, Poland

The aim of the talk is to present some results on filial and left filial algebras over a commutative ring $K$ with identity, i.e. algebras (usually without identity) in which the relation "of being ideal (left ideal)" is transitive. It turns out that the structure of such algebras and relations between the class of filiality and left filiality $K$-algebras depend on $K$. At the talk we will discuss the general situation (i.e. the results obtained for an arbitrary $K$) and also describe what one can get more in cases when $K$ is a field or the ring of integers.

## Suites récurrentes linéaires sur des anneaux de matrices

Tarek Garici, A. Cherchem
University of USTHB-Alger, Algeria.

Cf. abstract of A. Cherchem, above.

## Some properties of tensor rings

Armenak Gasparayan
University of Pereslavl-Zalesskii, Russia.

## Infinitely generated projective modules over pullbacks of rings

Dolors Herbera
Universitat Autònoma de Barcelona, Spain

Let $R$ be a ring. The set $V^*(R_R)$ of isomorphism classes of countably generated projective right $R$-modules has a structure of commutative monoid with the sum induced by the direct sum of countably generated projective modules. Similarly one can define $V^*({}_RR)$ as the monoid of isomorphism classes of countably generated projective left $R$-modules.

In this talk we will show that ring pullbacks can have a very rich supply of infinitely generated projective modules that are not direct sums of finitely generated ones. We will illustrate that explaining which monoids can appear as $V^*(R_R)$ for $R$ a noetherian semilocal ring.

For noetherian semilocal rings $V^*(R_R) \cong V^*({}_RR)$, we will also show how to construct examples of rings where this is not true. There are examples of (semilocal) rings such that any projective right module is a direct sum of finitely generated ones but there are nonzero projective left modules with no nonzero finitely generated direct summands.

Our use of pullbacks is based on a well known result of Milnor that describes, under mild restrictions, the category of all projective modules over pullbacks. Another essential tool is a recent result of Pavel Příhoda showing that two arbitrary projective modules are isomorphic if and only if they are isomorphic modulo the Jacobson radical.

This is a report on joint work with P. Příhoda.

## Actions of Lie superalgebras on semiprime algebras with central invariants

Małgorzata Hryniewicka
University of Białystok, Poland.

In [BG] Bergen and Grzeszczuk examined the situation where semiprime algebras $R$ of characteristic zero were acted on by finite dimensional nilpotent Lie algebras $L$ as algebraic derivations. In this situation, they show that if the subalgebra of invariants $R^L$ is central then the action of $L$ on $R$ is trivial. In this talk we will discuss the possibility of extending the above result to the action of Lie superalgebras.

# Références

[BG] J. Bergen, P. Grzeszczuk, *Invariants of Lie superalgebras acting on associative rings*, Israel J. Math. **94** (1996), 403–428.

## Endomorphism Ring of a Uniserial module

Irawati Irawati
University of Bandung, Indonesia.

## Rings Determined by Properties of Cyclic Modules

S K Jain
Ohio University, USA.

This survey talk addresses to the classical questions on determining rings whose cyclic modules or proper cyclic modules have certain homological property, chain condition, or combination of these. The question of classifying commutative noetherian rings $R$ such that each proper homomorphic image is self-injective was initiated by Levy and later continued by Klatt-Levy without assuming the noetherian condition. Later on several authors including Ahsan, Boyle, Byrd, Courter, Cozzens, Damiano, Faith, Goel, Goodearl, Hajarnavis, Hill, Huynh, Ivanov, Jain, Leroy, Kanwar,Koehler, Mohamed, Osofsky, Singh, Skornyakov, Smith, Srivastava, and Symonds studied classes of noncommutative rings whose all cyclic modules, a proper subclass of cyclic modules, injective hulls of cyclic modules, right ideals, or a proper subclass of right ideals have properties, such as, injectivity, quasi-injectivity, continuity, quasi-continuity (=$p$-injectivity), complements are summands ($CS$), weak-injectivity, projectivity, quasi-projectivity, noetherian, or artinian. We will briefly highlight some results and conclude with classical open questions.

## Derived lengths of symmetric and skew symmetric elements in group algebras

Tibor Juhász
Eszterházy Károly College, Eger, Hungary

For a subset $S$ of an associative ring $R$ we define the Lie derived series of $S$ by induction as follows: let $\delta^{[0]}(S) = S$ and let $\delta^{[n+1]}(S)$ be the additive subgroup generated by the Lie commutators $[x,y] = xy - yx$ with $x,y \in \delta^{[n]}(S)$. The subset $S$ is said to be Lie solvable if there exists a natural number $n$ such that $\delta^{[n]}(S) = 0$, and the smallest such $n$ is called the Lie derived length of $S$.

Let $FG$ be the group ring of a group $G$ over a field $F$ of characteristic $p > 2$. Let us consider the involution on $FG$ sending each group element to its inverse, and denote by $(FG)^+$ the set of symmetric elements, by $(FG)^-$ the set of skew symmetric elements of $FG$ with respect to this involution. We show that if $G$ is a nilpotent $p$-abelian group with cyclic derived subgroup, then the Lie derived length of both $(FG)^+$ and $(FG)^-$ are equal to $\lceil \log_2(|G'| + 1)\rceil$, and this value is not else than the Lie derived length of the whole group ring $FG$. This nice equality is no longer true if $G$ is not nilpotent.

## Lie regular generators of general linear groups

Pramod Kanwar
Ohio University Zanesville, USA.

An element $a$ of a ring $R$ is called unit regular if $a = aua$ for some unit $u$ in $R$. Equivalently, $a$ is unit regular if and only if $a = eu$ for some idempotent $e$ and some unit $u$ in $R$. $a \in R$ is called clean if $a = e + u$ for some idempotent $e$ and some unit $u$ in $R$. We call an element of a ring $R$ *Lie regular* if it can be expressed as a Lie product of an idempotent element in $R$ and a unit in $R$. A unit in $R$ is said to be a *Lie regular unit* if it is Lie regular as an element of $R$. We show that any Lie regular element in $M_2(R)$ where $R$ is a commutative domain in which 2 is invertible and in the group algebra $KD_\infty$ of infinite dihedral group over a field of characteristic not equal to 2 can be expressed as $[u_1,u_2]$ where $u_1$ and $u_2$ are units. Among other things we give Lie regular generators of the general linear groups $GL(2,\mathbb{Z}_{2p})$ where $p$ is an odd prime, $GL(2,\mathbb{Z}_{2^n})$, and $GL(2,\mathbb{Z}_{p^n})$ where $p$ is an odd prime and give presentations of these groups in some special cases. (This is a joint work with R.K.Sharma and Pooja Yadav)

## Some generalizations of reduced rings

Jan Krempa
University of Warsaw, Poland.

In this survey talk IŠm going to consider only associative rings, not necessarily with 1: A ring is reduced if it has no nontrivial nilpotent elements or, equivalently, if it satisfies the following quasi-identity:

$$x^2 = 0 \Rightarrow x = 0.$$

The following characterization of reduced rings is well known:

**Theorem 1. Thierrin and others For a ring R the following conditions are equivalent:**

1. **$R$ is reduced;**
2. **$R$ is semiprime and all minimal prime ideals of $R$ are completely prime;**
3. **$R$ is a subdirect product of domains;**
4. **All subrings of $R$ are semiprime.**

IŠm going to begin my talk by exhibiting some generalizations of reduced rings motivated by the following result:

**Theorem 2.** *Let $R$ be a reduced ring. Then for any $n \geq 1$ and every $\sigma \in S_n$ the following quasi-identity is satisfied:*

$$x_1 \cdots x_n = 0 \Rightarrow x_{\sigma(1)} \cdots x_{\sigma(n)} = 0.$$

*In particular, for every $x,y,z \in R$ we have:*

$$xy = 0 \Rightarrow yx = 0, \quad xyz = 0 \Rightarrow xzy = 0 \quad \text{and} \quad xy = 0 \Rightarrow xzy = 0.$$

In the sequel I'll present some classes of rings, or rather algebras over commutative rings, having only small nil-subalgebras.

## Cyclic maximal left ideals of the Weyl algebra: an algorithm

Yves Lequain
University of Rio de Janeiro, Brasilia

Let $n > 1$ be an integer, $K$ a field of characteristic zero and $A_n(K)$ the $n^{th}$ Weyl algebra over $K$. J.T. Stafford has shown that there exists some non-holonomic irreducible $A_2(K)$-modules by constructing a differential operator of $A_2(K)$ that generates a maximal left ideal of $A_2(K)$. Later, Bernstein and lunts have shown that the "generic" differential operator $F$ of $A_n(K)$ generates a maximal left ideal of $A_n(K)$ (and therefore that the quotient $\frac{A_n(K)}{/}FA_n(K)$ is a non-holonomic irreducible $A_n(K)$-module). Their result however is non-effective and up to now, there are only very sporadic concrete examples of cyclic maximal left ideals of $A_n(K)$. In this talk, I will present an algorithm that allows one to recognize whether any given order-one differential operator associated to a "Shamsuddin" derivation generates a maximal left ideal of $A_n(K)$.

## Double Ore Extensions versus Iterated Ore Extensions

Jerzy Matczuk
University of Warsaw, Poland.

Motivated by the construction of new examples of Artin-Schelter regular algebras of global dimension four, J.J.Zhang and J.Zhang [ZZ] introduced an algebra extension $A_P[y_1,y_2;\sigma,\delta,\tau]$ of $A$, which they called a double Ore ex- tension. This construction seems to be similar to that of a two-step iterated Ore extensions over $A$. The aim of the talk is to present the Zang's construction and to describe those double Ore extensions which can be presented as iterated Ore extensions of the form $A[y_1;\sigma_1,\delta_1][y_2;\sigma_2,\delta_2]$. Partial answers to some questions posed in [ZZ] will be given.

## Elliptic Curve Weak Class Identification for The Security of Cryptosystem

Intan Muchtadi-Alamsyah, Ahmad Muchlis
University of Bandung, Indonesia

In 1988 Buchmann and Williams described the use of the class groups of imaginary quadratic orders for the construction of cryptosystem. These imaginary quadratic orders are closely related to non-supersingular elliptic curves over finite fields. Thus an understanding of imaginary quadratic orders may lead to a better understanding of the security of elliptic curve cryptosystems. In this paper we explain the close relation between elliptic curves and imaginary quadratic orders, especially totally non-maximal imaginary quadratic orders. Then we use this relation to identify a weak class of elliptic curves, a specific class which gives low level security of cryptosystems. We give a necessary condition for elliptic curves so that the logarithm problem can be reduced to the logarithm problem in some finite field.

## RINGS CLOSE TO SEMIREGULAR

A. Çiğdem ÖZCAN
Hacettepe University, Ankara Turkey

A ring $R$ is called semiregular if $R/J$ is (von Neumann) regular and idempotents lift modulo $J$, where $J$ denotes the Jacobson radical of $R$. We give some characterizations of rings $R$ such that idempotents lift modulo $J$, and $R/J$ satisfies one of the following conditions: (one-sided) unit–regular, strongly regular, (unit, strongly, weakly) $\pi$–regular.

Joint work with Pınar AYDOGDU.

## On Drazin invertibility over rings

Pedro Patricio
University of Minho, Portugal.

In this talk, we will address Drazin invertibility over rings. A ring element $a$ is said to have a Drazin inverse $x$ provided there exists a natural $k$ for which $a^{k+1}x = a^k$,$xax = x$,$ax = xa$. We will use several contexts where this set of equations are studied, and to which links they correspond to. Additive formulae will be presented, generalizing recent results.

## Lie nilpotence of skew symmetric elements in group rings

Cesar Polcino Milies
University of Sao Paulo, Brasilia.

Let $G$ be a group with an involution $^*$ extended linearly to an involution of $FG$, the group algebra of $G$ over a field $F$ of characteristic different from 2. We shall first survey some of the known results regarding the Lie structure of $(FG)^- = \{\alpha \in FG \mid \alpha^* = -\alpha\}$, the set of skew symmetric elements of $FG$. Also, we shall give necessary and suffiicient conditions on $G$ for this set to be Lie nilpotent, in the case when $G$ is a torsion group with no elements of order 2. This result is joint work with A. Giambruno and S.K. Sehgal.

## Introductory Course on Coding Theory

Patrick Solé
University of Nice, CNRS

## Equivalences and tilting modules

Alberto Tonolo
University of Padova, Italy

I will give a description of the development of tilting theory for arbitrary associative rings. Tilting theory generalizes Morita's theorems on equivalence between categories of modules. I will present some among the principal results obtained in the last years, and in particular the most recent one obtained in the natural context of the derived categories associated to the module categories.

## Coding with skew polynomial rings

Felix A Ulmer
University of Rennes, France

In this approach, we generalize the notion of cyclic code and construct codes via ideals in finite quotients of non commutative polynomial rings, so called skew polynomial rings of automorphism type. Since there is no unique factorization in skew polynomial rings, there are much more ideals and therefore much more codes than in the commutative case.

We propose a method to construct block codes of prescribed rank and a method to construct block codes of prescribed distance (joint work with L. Chaussade and P. Loidreau). Also, using Groebner bases, we computed all Euclidean and Hermitian self-dual linear codes over $\mathbb{F}_4$ of this type of length less than 40, including a [36, 18, 11] Euclidean self-dual code which improves the previously best known self-dual linear codes over $\mathbb{F}_4$ (joint work with D. Boucher)

## Cleanness of Von-Neumann-algebra-like rings

Lia Vas
University of the Sciences in Philadelphia, USA

The study of von Neumann algebras inspired increasing interest in classes of rings and algebras such as Baer *-rings, Rickart $C*$-algebras, and other “rings of operators". Currently, these rings are being studied without involving, sometimes rather complex, methods of operator theory.

In this talk, we consider a class of Baer *-rings defined by certain axioms. For a ring in this class we say that it is von-Neumann-algebra-like. We turn our attention to the question of cleanness of von-Neumann-algebra-like rings.

A ring is clean if its every element is the sum of a unit and an idempotent. We prove that type I von-Neumann-algebra-like Baer *-rings are clean. In particular, we obtain that all finite type I $AW*$-algebras (thus all finite type I von Neumann algebras as well) are clean. Finally, we shall present some examples related to group von Neumann algebras and list some open problems.