ANTALYA ALGEBRA DAYS XVI
9-13 MAY 2014

FRIDAY, 9 MAY

09:30-10:30: Christophe Ritzenthaler (University Rennes 1)
How big is 4?

10:30-11:00: Coffee Break

11:00-12:00: Jennifer Balakrishnan (University of Oxford)
Coleman integration and integral points on hyperelliptic curves

12:00-13:50: Lunch Break

13:50-15:30: Workshops (Combinatorics I / Lie Algebras)

15:30-16:00: Coffee Break

16:00-17:00: Yves Aubry (Université de Toulon and Université Aix-Marseille)
Algebraic geometry and Abelian varieties over finite fields

17:00-18:00: Arzu Boysal (Boğaziçi Üniversitesi)
Bernoulli series and volumes of moduli spaces

18:30: Welcome gathering!

SATURDAY, 10 MAY

09:00-10:00: Christian Mauduit (Université Aix-Marseille)
Prime numbers, determinism and pseudorandomness

10:00-10:30: Coffee Break

10:30-11:30: Jonathan Jedwab (Simon Fraser University)
The structure of Costas arrays

11:30-12:30: Gerriet Martens (Universitaet Erlangen-Nuernberg)
The gonality sequence of an algebraic curve

12:30-14:00: Lunch Break

14:00-15:20: Workshops (Combinatorics II / Ring Theory I)

15:20-16:00: Coffee Break

16:00-18:50: Workshops (Module Theory / Number Theory I / Algebraic Geometry I)

SUNDAY, 11 MAY

09:30-10:30: Eva Bayer-Fluckiger (EPFL)
Euclidean Number Fields and Euclidean Minima

10:30-11:00: Coffee Break

11:00-12:00: William D. Gillam (Boğaziçi Üniversitesi)
Motivic cohomology and algebraic cycles

12:00-13:45: Lunch Break

13:45-19:00 (?): Excursion to Phaselis and Kemer

MONDAY, 12 MAY

09:00-10:00: Michel Lavrauw (Universitá degli Studi di Padova)
On rank and orbits in tensor products over finite fields

10:00-10:30: Coffee Break

10:30-11:30: Arne Winterhof (RICAM, Austrian Academy of Sciences)
Covering sets
11:30-12:30: Mercede Maj (Università degli Studi di Salerno)
Some recent results on small doubling problems in orderable groups

12:00-13:50: Lunch Break

13:50-15:30: Workshops (Group Theory I / Number Theory II / Algebraic Geometry II)

15:30-16:00: Coffee Break

16:00-17:00: Patrizia Longobardi (Universitá degli Studi di Salerno)
Sums of dilates and direct and inverse problems in Baumslag-Solitar groups

17:00-18:00: Francesco de Giovanni (University of Napoli "Federico II")
Large soluble groups

18:10-19:10: Workshops (Group Theory II / Algebraic Geometry III / Ring Theory II)

TUESDAY, 13 MAY

09:00-10:00: Ian Morrison (Fordham University)
GIT and birational geometry of moduli spaces of curves
10:00-10:30: Coffee Break

10:30-11:30: Ali Ulaş Özgür Kişisel (Middle East Technical University)
Graphs of Varieties Associated to Multiplicative or Additive Group Actions

WORKSHOPS

FRIDAY, 9 MAY

Combinatorics I:

13:50-14:10: Ş. Yazıcı
A polynomial embedding of pairs of orthogonal partial latin squares
14:10-14:30: F. Demirkale
Linearly independent latin squares
14:30-14:50: B. Özkaya
Multidimensional quasi-cyclic and convolutional codes
14:50-15:10: S. Özkan
The Hamilton - Waterloo problem with uniform cycle sizes
15:10-15:30: E. Kolotoğlu
On large sets of projective planes of orders 3 and 4

Lie Algebras:

13:50-14:10: H. Adimi
Index of Hom-Lie algebras by central extension
14:10-14:30: K. Dekkar
Cohomology and deformations of hom-bialgebras and hom-hopf algebras
14:30-14:50: I. Demir
On Leibniz algebras
14:50-15:10: N. S. Öğüşlü
The test rank of a soluble product of free abelian Lie algebras

SATURDAY, 10 MAY

Combinatorics II:

14:00-14:20: C. Çalışkan
New infinite families of 2-edge-balanced graphs
14:20-14:40: M. M. Tan
Generalized multipliers, Weil numbers and circulant weighing matrices
14:40-15:00: M. Taşkın
Tower tableaux
15:00-15:20: H. Topçu
On the spectral determination of some special graphs

Ring Theory I:

14:00-14:20: E. Albaş
Generalized derivations with some related conditions on Lie ideals
14:20-14:40: B. A. Saylam
Density theorems for rings of Krull type
14:40-15:00: C. Hatipğolu
Injective hulls of simple modules over differential operator rings
15:00-15:20: Ö. Özkan
Involution of structural matrix algebras

Module Theory:

16:00-16:20: P. Aydoğdu
G-Dedekind primeness of Morita context
16:20-16:40: Y. Alagöz
Strongly (non)cosingular modules
16:40-17:00: M. T. Akçin
Betti series of the universal modules of second order derivations

Number Theory I:

17:10-17:30: A. Özkoç ,
Pell form and Pell equation in terms of Oblong numbers
17:30-17:50: Y. Akbal
Piatetski Shapiro meets Chebotarev
17:50-18:10: O. Uzunkol
Smaller generators for some class fields
18:10-18:30: Ö. D. Polat
Factorization of places in coverings of algebraic curves

Algebraic Geometry I:

18:30-18:50: N. Şahin
Arf rings for singularities

MONDAY, 12 MAY

Group Theory I:

13:50-14:10: A. Arıkan
Zaitsev type results
14:10-14:30: A. Arıkan
Infinitely generated periodic groups
14:30-14:50: M. Bouchelaghem
Groups whose proper subgroups have polycyclic-by-finite conjugacy classes
14:50-15:10: M. Hamitouche
Some properties of a generalized 3-abelian groups
15:10-15:30: A. Souad
On minimal non-hypercentral groups

Number Theory II:

13:50-14:10: L. Işık
On the minimum distance of cyclic codes
14:10-14:30: S. Tutdere
Recursive Artin-Schreier towers of function fields over F_2
14:30-14:50: M. Cenk
On the fast computation of Toeplitz matrix vector products over F_2
14:50-15:10: N. Anbar
On quadratic functions and Artin-Schreier curves

Algebraic Geometry II:

15:10-15:30: A. Erdoğan
Canonical lifting of abelian varieties

Group Theory II:

18:10-18:30: V. Tolstykh
The small index property for relatively free algebras
18:30-18:50: İ. Tuvay
Brauer indecomposability of Scott modules of Park-type groups

Algebraic Geometry III:

18:10-18:30: A. Iezzi
On the maximal number of points on singular curves over finite fields

Ring Theory II:

18:30-18:50: A. Koç
Representations of Leavitt and Cohn-Leavitt path algebras
18:50-19:10: S. Esin
A survey on recent advances about irreducible representation of Leavitt path algebras

INVITED TALKS

WORKSHOP TALKS

POSTERS

Invited Talks

Algebraic geometry and Abelian varieties over finite fields

Yves Aubry

The first part of the talk will be devoted to an historical overview on the development of algebraic geometry. Starting from the exploration age with Descartes, we will explore the golden age of projective geometry with Segre, the birational geometry with Riemann, development and chaos with Kronecker, new structures with Hilbert and to finish by sheaves and schemes with Grothendieck.

The second part of the talk will be concerned with abelian varieties over finite fields. After the description of the action of the Frobenius endomorphism on the Tate module, we will derive new bounds on the number of rational points.

Université de Toulon and Aix-Marseille Université

email: `yves.aubry@univ-tln.fr`

Coleman integration and integral points on hyperelliptic curves

Jennifer S. Balakrishnan

We discuss explicit computations of p-adic line integrals (Coleman integrals) on hyperelliptic curves and some applications. In particular, we relate a formula for the component at p of the p-adic height pairing to a sum of iterated Coleman integrals. We use this to give a Chabauty-like method for computing p-adic approximations to integral points on such curves when the Mordell-Weil rank of the Jacobian equals the genus. This is joint work with Amnon Besser and Steffen Müller.

University of Oxford

email: `balakrishnan@maths.ox.ac.uk`

web: `http://people.maths.ox.ac.uk/balakrishnan/`

Euclidean Number Fields and Euclidean Minima

Eva Bayer-Fluckiger

If a and b are two integers, with $b \neq 0$, then there exist two integers q and r such that $a = bq + r$, and that $|r| < |b|$. This so-called Euclidean division property plays a fondamental role in the arithmetic of the usual integers. It is natural to try to generalise this to more general rings, for instance rings of integers of algebraic number fields. This idea leads to the notions of Euclidean number fields and Euclidean minima. Both are very classical topics of number theory. The aim of this talk is to survey old and new results concerning this subject, such as new Euclidean number fields and upper bounds for Euclidean minima. In particular, we will survey the history and recent developments concerning a classical conjecture of Minkowski.

EPFL, Lausanne email: eva.bayer@epfl.ch

Bernoulli series and volumes of moduli spaces

Arzu Boysal

I will introduce Witten series associated to classical Lie algebras. Particular instances of these series compute volumes of moduli spaces of flat bundles over surfaces, and also certain multiple zeta values. I will explain how one actually computes these series using residue techniques on multiple Bernoulli series introduced by A. Szenes.

This talk is based on our joint work with Velleda Baldoni and Michèle Vergne.

Boğaziçi Üniversitesi

email: arzu.boysal@boun.edu.tr

Motivic cohomology and algebraic cycles

William D. Gillam

Motivic cohomology is a remarkable cohomology theory for algebraic varieties whose existence was conjectured by Grothendieck in the 1960s, with later elaborations by Beilinson and Lichtenbaum. One can now construct such a cohomology theory either by using Voevodsky's approach via presheaves with transfers or by Bloch's approach in terms of higher Chow groups. Suslin and Voevodsky ultimately established the equivalence of the two approaches. In this talk we will survey these constructions and discuss some of the remarkable properties of motivic cohomology. If there is time at the end I will say something about the motivic cohomology of toric varieties.

Boğaziçi Üniversitesi email: wdgillam@gmail.com

Large Soluble Groups

Francesco de Giovanni

The aim of this lecture is to show that in a large group (like for instance can be considered a group of infinite rank) the behaviour of small subgroups (in the above case those of finite rank) with respect to an embedding property can be neglected.

University of Napoli "Federico II"

email: degiovan@unina.it

web: http://www.dma.unina.it/~degiovan/

The structure of Costas arrays

Jonathan Jedwab

A Costas array is a permutation array in which the vectors joining pairs of 1s are all distinct. This property was identified by J. Costas in the 1960s for use in sonar. The central problem is to determine all orders for which a Costas array exists.

The classical constructions, due to Welch and Golomb, use finite fields to generate infinite families of Costas arrays. These constructions, together with exhaustive search results, show that Costas arrays exist for all orders less than 32. Numerical evidence suggests that some orders of Costas arrays might not exist, but no nonexistence result has yet been found. The smallest orders for which existence is open are 32 and 33, and this has been the case for at least 25 years.

I shall describe some new results that shed light on the structure of Costas arrays, including a proof of a recent conjecture due to Russo, Erickson and Beard.

This is joint work with J. Wodlinger.

Simon Fraser University, Canada

email: jed@sfu.ca

web: http://people.math.sfu.ca/~jed/

Graphs of Varieties Associated to Multiplicative or Additive Group Actions

Ali Ulaş Özgür Kişisel

The concept of the T-graph of a standard or multigraded Hilbert scheme was defined by Altmann and Sturmfels using Gröbner degenerations. The T-graph retains certain properties of the Hilbert scheme in question. We define T-graphs in a more general setting when X is a scheme carrying a torus action, and prove that the T-graph of X is connected if and only if X is connected. If X has additional automorphisms, then under suitable hypotheses one can define a subgraph of the T-graph, which will be called the A-graph of X. We prove that X is connected if and only if its A-graph is connected. As an application, we give another proof of the classical theorem stating that the Hilbert scheme is connected. This is joint work with Engin Özkan.

Middle East Technical University

email: akisisel@metu.edu.tr

On rank and orbits in tensor products over finite fields

Michel Lavrauw

Tensor products play an important role in both mathematics and physics, with applications in e.g. complexity theory, algebraic statistics, tensor networks in quantum information theory, and representation theory (see e.g. Landsberg [1]). One can easily say that there is no lack of motivation to study tensor products, and, although there are still many interesting open problems, tensor products are well studied objects. However, most of the research on tensor products (including [1]) only considers tensor products over the complex numbers. Sometimes this is extended to general algebraically closed fields, but few consider the case where the ground field is finite.

The main problems that turn up from the applications are concerned with the *decomposition*

$$\tau = \sum_{i=1}^{k} v_{1i} \otimes \ldots \otimes v_{mi} \tag{$*$}$$

of a tensor $\tau \in \bigotimes_{i=1}^{m} V_i$. This naturally leads to the following four essential issues.

(E) Existence: given a tensor τ and an integer k, does there exist an expression of the form $(*)$?

(U) Uniqueness: given an expression of the form $(*)$ for a tensor τ, is this expression essentially unique?

(A) Algorithm: given a tensor τ and an integer k, does there exist an algorithm that decomposes τ into an expression of the form $(*)$ (in the case where it exists)?

(O) Orbits: can we determine the number of orbits and describe the orbits of the natural group action of $\mathrm{GL}(V_1) \times \ldots \times \mathrm{GL}(V_m)$ on $\bigotimes_{i=1}^{m} V_i$?

In this talk, we will elaborate on these problems, focus on tensor products over finite fields, and explain the connections with finite geometry. We will survey what is known, including some recent results concerning rank, decomposition and invariant orbits, from [2, 3, 4].

References

[1] J . M. Landsberg. Tensors: Geometry and Applications. 2012. Graduate Studies in Mathematics, 128. American Mathematical Society, Providence, RI, 2012. xx+439 pp. ISBN: 978-0-8218-6907-9.

[2] M. Lavrauw and J. Sheekey. Orbits of the stabiliser group of the Segre variety product of three projective lines. *Finite Fields Appl.* 26 (2014) 1–6.

[3] M. Lavrauw, A. Pavan and C. Zanella. On the rank of 3 × 3 × 3-tensors. *Linear and Multilinear Algebra* (2013) 61 (5) 646–652.

[4] M. Lavrauw. Finite semifields and nonsingular tensors. *Des. Codes Cryptogr.* (2013) 68 (1-3) 205–227.

Università degli Studi di Padova, Italy

email: michel.lavrauw@unipd.it

web: http://cage.ugent.be/~ml

Sums of dilates and direct and inverse problems in Baumslag-Solitar groups

Patrizia Longobardi

Subsets of the set of the integers of the form

$$n \star A = \{rx : x \in A\},$$

where r is a positive integer and A is a finite subset of the set of the integers are called r-dilates.

We obtain new direct and inverse results for sums of two dilates. Then we apply them to solve certain direct and inverse problems in Baumslag-Solitar groups.

A new result on dilates is the following. If A is a finite set of integers and $|A + 2 \star A| < 4|A| - 4$, then A is a subset of an arithmetic progression of size $\leq 2|A| - 3$.

The Baumslag-Solitar groups are defined as follows:

$$BS(m, n) = \langle a, b \ \mid \ b^{-1}a^m b = a^n \rangle$$

where m, n are integers.

We concentrate on the groups $BS(1, n)$ and their subsets of the type

$$S = \{b^r a^{x_1}, b^r a^{x_2}, \ldots, b^r a^{x_k}\} = b^r a^A$$

where r is a positive integer and $A = \{x_1, x_2, \ldots, x_k\}$ denotes a finite sequence of integers.

A sample result is the following. If $S = ba^A \subseteq \ BS(1, 2)$, $|S| \geq 3$ and $|S^2| < 4|S| - 4$, then A is a subset of an arithmetic progression of size $\leq 2|S| - 3$.

We also investigate the structure of arbitrary subsets of $BS(1, 2)$ satisfying small doubling properties. We consider the submonoid

$$BS^+(1, 2) = \{b^m a^x \in BS(1, 2) \mid x, m \in Z, m \geq 0\}$$

of $BS(1, 2)$.

We prove that if S is a finite non-abelian subset of $BS^+(1, 2)$ and $|S^2| < \frac{7}{2}|S| - 4$, then $S = ba^A$, where A is a set of integers of size $|S|$, which is contained in an arithmetic progression of size less than $\frac{3}{2}|S| - 2$.

References

[1] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y. V. Stanchescu, Direct and inverse problems in Additive Number Theory and in non-abelian group theory, *European Journal of Combinatorics 40 (2014) 42-54*, to appear.

[2] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y. V. Stanchescu, Inverse problems in Additive Number Theory and in Non-Abelian Group Theory, *arXiv*:1303.3053 (2013), preprint, 1–31.

[3] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y. V. Stanchescu, A small doubling structure theorem in a Baumslag- Solitar group, to appear.

Patrizia Longobardi, University of Salerno, Italy

email: `plongobardi@unisa.it`

Some recent results on small doubling problems in orderable groups

Mercede Maj

Let G denote an arbitrary group. If S is a subset of G, we define its square S^2 by

$$S^2 = \{x_1x_2 \mid x_1, x_2 \in S\}.$$

We are concerned with the following general problem: let S be a finite subset with k elements of a group G, determine the **structure** of S, if $|S^2|$ satisfies the following inequality:

$$|S^2| \leq \alpha|S| + \beta$$

for some small $\alpha \geq 1$ and small $|\beta|$.

Problems of this kind are called **inverse problems** of **small doubling** type. Inverse problems of small doubling type have been first investigated by G. A. Freiman in the additive group of the integers. Our aim is to investigate the structure of finite subsets S of *orderable groups* satisfying the small doubling property with $\alpha = 3$ and small β's, and also the structure of the subgroup generated by S. This is a step in a program to extend the classical Freiman's inverse theorems (see [1]) to nonabelian groups.

Let G be a group and suppose that a total order relation $\leq$ is defined on the set G. We say that $(G, \leq)$ is an *ordered group* if for all $a, b, x, y \in G$, the inequality $a \leq b$ implies that $xay \leq xby$. A group G is *orderable* if there exists a relation $\leq$ such that $(G, \leq)$ is an ordered group. Nilpotent torsion-free groups are examples of orderable groups.

Let G be an ordered group and let S be a finite subset of G of size $|S| = k \geq 2$. We proved in [2] that if $|S| > 2$ and $|S^2| \leq 3|S| - 3$, then $\langle S\rangle$ is abelian, and if $|S^2| \leq 3|S| - 4$, then S is a subset of a geometric progression.

In this talk we present some recent results, contained in [3] and in [4], concerning the structure of the subset S of an ordered group and the structure of $\langle S\rangle$, if $|S^2| \leq 3|S| - 3 + b$, for some integer $b \geq 1$.

References

[1] G. A. Freiman, Foundations of a structural theory of set addition. Translations of mathematical monographs, v. 37. American Mathematical Society, Providence, Rhode Island, 1973.

[2] G. A. Freiman, M. Herzog, P. Longobardi, M.Maj, Small doubling in ordered groups, *J. Australian Math. Soc.*, to appear.

[3] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y. V. Stanchescu, Direct and inverse problems in Additive Number Theory and in non-abelian group theory, *European Journal of Combinatorics* 40C (2014), pp. 42-54.

[4] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, A. Plagne and Y. V. Stanchescu, Small doubling - generators and structure, in preparation.

Mercede Maj, University of Salerno, Italy

email: `mmaj@unisa.it`

The gonality sequence of an algebraic curve

Gerriet Martens

For a smooth irreducible projective curve X defined over the complex numbers, let $d_r = d_r(X)$ denote the minimal degree of a linear series on X of dimension $r > o$. These numbers form a strictly increasing sequence which is called the gonality sequence of X since d_1 is the gonality of X (i.e. the minimal number of sheets of a covering of X over $\mathbb{P}^1$). One expects a certain pattern in the growth of this sequence which, however, is violated for some families of curves with special moduli. In this talk I want to present some new results about such families.

Univ. Erlangen-Nürnberg

email: `martens@mi.uni-erlangen.de`

Prime numbers, determinism and pseudorandomness

Christian Mauduit

The difficulty of the transition from the representation of an integer in a number system to its multiplicative representation (as a product of prime factors) is at the source of many important open problems in mathematics and computer science. We will present a survey on recent results concerning the study of independence between the multiplicative properties of integers and various "deterministic function", i. e. function produced by a dynamical system of zero entropy or defined using a simple algorithm, in connection with the Chowla and Sarnak conjectures on Mobius randomness principle. *Universit d'Aix-Marseille*

email: `mauduit@iml.univ-mrs.fr`

GIT and birational geometry of moduli spaces of curves

Ian Morrison

Geometric questions about the moduli space $\overline{M}_g$ of stable curves of genus g are of interest in many cognate areas of algebraic geometry. For example, $\overline{M}_g$ has been extensively studied as a test case for general questions from the minimal model program in birational geometry, where its modular interpretation provides extra tools for answering these questions. A paradoxical aspect of this work is that, although the questions deal with the *intrinsic* geometry of $\overline{M}_g$, their solutions often depend on *extrinsic* constructions of GIT quotients, and on interpretations of these quotients as alternate compactifications of M_g. I will review the history of these interactions and the parallel progress in our understanding of the birational geometry of $\overline{M}_g$ and of these GIT quotients.

Fordham University

email: morrison@fordham.edu

web: http://www.fordham.edu/morrison

How big is 4

Christophe Ritzenthaler

The aim of the talk is to introduce some arithmetic properties of plane curves over finite fields, in particular the distribution of their number of points. Considering the case of conics, cubics and quartics, we will wonder how close we get to the typical behavior. *University Rennes 1*

email: christophe.ritzenthaler@univ-rennes1.fr

Covering Sets

Arne Winterhof

For a set $\mathcal{M} = \{-\mu, -\mu+1, \dots, \lambda\} \setminus \{0\}$ with non-negative integers $\lambda, \mu < q$ not both 0, a subset $\mathcal{S}$ of the residue class ring Z_q modulo an integer $q \geq 1$ is called a $(\lambda, \mu; q)$-*covering set* if

$$\mathcal{MS} = \{ms \bmod q \ : \ m \in \mathcal{M},\ s \in \mathcal{S}\} = Z_q.$$

Small covering sets play an important role in codes correcting limited-magnitude errors. Note that any $(\lambda, \mu; q)$-covering set is of size at least $\lceil q/(\lambda+\mu) \rceil$.

We give an explicit construction of a $(\lambda, \mu; q)$-covering set $\mathcal{S}$ which is of the size $q^{1+o(1)} \max\{\lambda, \mu\}^{-1/2}$ for almost all integers $q \geq 1$ and of optimal order of magnitude (that is up to a multiplicative constant) $p \max\{\lambda, \mu\}^{-1}$ if $q = p$ is prime.

Furthermore, using a bound on the fourth moment of character sums of Cochrane and Shi that there is a $(\lambda, \mu; q)$-covering set of size at most

$$q^{1+o(1)} \max\{\lambda, \mu\}^{-1/2}$$

for any integer $q \geq 1$, however the proof of this bound is not constructive.

The proof of the first result is elementary. For the proof of the second result we include a short tutorial on character sums.

References

[1] Z. Chen, I.E. Shparlinski, A. Winterhof: Covering sets for limited-magnitude errors, IEEE Trans. Inf. Th., to appear.

RICAM, Austrian Academy of Sciences

email: arne.winterhof@oeaw.ac.at

web: http://www.ricam.oeaw.ac.at/people/page.cgi?firstn=Arne;lastn=Winterhof

Workshop Talks

Index of Hom-Lie Algebras By Central Extension

H.Adimi

A Hom-algebra structure is a multiplication on a vector space where the structure is twisted by a homomorphism. In this paper we introduse the notation of the index of hom-Lie algebras in the case of coadjoint and an arbitrary representation. give also the index of semidirect products of hom Lie algebras. and we give The index of a Hom Lie algebra by central extension.

References

[1] Adimi H. and A Makhlouf.,*Index of Graded Filiform and Quasi Filiform Lie Algebras,* Filomat 27:3 (2013), 467–483 DOI 10.2298/FIL1303467A

[2] Andriy Panasyuk *Reduction by stages and the Raïs-type formula for the index of a Lie algebra with an ideal.* Ann Glob AnalGeom (2008) 33:1-10 DOI 10.1007/s10455-007-9070-z

[3] Yunhe Sheng, *Representations of hom-Lie algebras,* arXiv:1005.0140v2 [math-ph] (2011).

Bordj Bou-Arreridj University

email: h.adimi@univ-bba.dz

Piatetski Shapiro meets Chebotarev

Yıldırım Akbal

This is a joint work with Ahmet Muhtar Güloğlu.

In 1953 Ilya Piatetski-Shapiro proved in [2] an analog of the prime number theorem for primes of the form $\lfloor n^c \rfloor$, where $\lfloor x \rfloor = \max\{n \in \mathbb{N} : n \leq x\}$, n runs through positive integers and $c > 0$ is fixed. He showed that the number $\pi_c(x)$ of these primes not exceeding a given number x is asymptotic to $x^{1/c}/\log x$ provided that $c \in (1, 12/11)$. Since then, the admissible range of c has been extended by many authors and the result is currently known for $c \in (1, 2817/2426)$ (cf. [3]). In this talk, we give an asymptotic formula for Shapiro primes lying in a specified Chebotarev class. We shall also apply our theorem to show that there are infinitely Shapiro primes of the form $x^2 + ny^2$.

References

[1] Y. Akbal, A. M. Güloğlu . Piatetski Shapiro meets Chebotarev (Submitted).

[2] I. I. Piatetski-Shapiro. *On the distribution of prime numbers in sequences of the form [f(n)],* (Russian) Mat. Sbornik N.S. 33 (75), (1953). 559 - 566.

[3] J. Rivat, P. Sargos. *Nombres premiers de la forme* $\lfloor n^c \rfloor$, Canad. J. Math, 53 (2001), no. 2, 414-433.

Bilkent University

email: yildirim.akbal@bilkent.edu.tr

Betti series of the universal modules of second order derivations

Melis Tekin Akçin

Let R be a commutative $k-$ algebra where k is a field of characteristic zero. We have the following exact sequence

$$0 \to I \to R \otimes_k R \overset{\varphi}{\to} R \to 0$$

where φ is defined as $\varphi(\sum\limits_{i=1}^{n} a_i \otimes b_i) = \sum\limits_{i=1}^{n} a_i b_i$ for $a_i, b_i \in R$ and I is the kernel of φ. Here, $\ker \varphi$ is generated by the set $\{1 \otimes r - r \otimes 1 : r \in R\}$.
Let $d_n : R \to (R \otimes_k R)/I^{n+1}$ be a $k-$linear map defined as

$$d_n(r) = 1 \otimes r - r \otimes 1 + I^{n+1} \text{ and } d_n(1) = 0.$$

Here d_n is called the universal derivation of order n. The left $R-$module $\frac{I}{I^{n+1}}$ is called the universal module of nth order derivations and is denoted by $\Omega_n(R)$. Let m be a maximal ideal of R, the Betti series of $\Omega_n(R)$ is defined to be the series

$$B(\Omega_n(R), t) = \sum_{i \geq 0} \dim_{R/m} Ext^i(\Omega_n(R), \frac{R}{m})t^i \text{ for all } n \geq 1.$$

We proved that the Betti series of $\Omega_2(R_m)$ is a rational function under some conditions, where R is a coordinate ring of an affine irreducible curve represented by $\frac{k[x_1, x_2, \ldots, x_s]}{(f)}$ and m be a maximal ideal of R.

References

[1] Çimen, N., Erdoğan, A., Projective dimension of the universal modules for the product of a hypersurface and affine t-space, Comm. Algebra 27(10), (1999), 4737-4741 .

[2] Erdoğan, A., Results on Betti series of the universal modules of the second order derivation, Hacet.J.Math. Stat. 40(3), (2011), 449-452.

[3] Erdoğan, A., Homological dimension of the universal modules for hypersurfaces, Comm. Algebra 24(5), (1996), 1565-1573.

[4] Nakai, Y., High order derivations 1, Osaka J.Math.7, (1970), 1-27.

Hacettepe University

email: hmtekin@hacettepe.edu.tr

Strongly (non)cosingular modules

Yusuf Alagöz

Let R be a ring with an identity element and M be a unital right R-module. A submodule N of M is called a small submodule of M if, whenever $N + L = M$ for some submodule L of M, we have $M = L$. M is called small module if it is a small submodule of its injective hull $E(M)$. For an R-module M, the submodule $Z^*(M) = \{m \in M \mid Rm \text{ is a small module } \}$ is called the cosingular submodule of M. If $Z^*(M) = M$, then M is called cosingular (see, [3,5]). Small modules are cosingular. In [6], the authors call M noncosingular module if M has no small homomorphic image. Motivated by the noncosingular modules, we investigate strongly noncosingular modules. Namely we call M *strongly noncosingular* if M has no *cosingular* homomorphic image. Strongly noncosingular modules are properly contained in the class of noncosingular modules. An R-module M is strongly noncosingular if and only if it is noncosingular and coatomic. In this talk we shall investigate some properties of strongly noncosingular modules, and their relation with some classes of rings and modules.

This is a joint work with Yılmaz Durğun.

References

[1] S. Crivei, Neat and coneat submodules of modules over commutative rings, Bull. Aust. Math. Soc. (2013)

[2] L. Fuchs, Neat submodules over integral domains, Period. Math. Hungar. 64 (2012), no. 2, 131- 143.

[3] M. Harada, Nonsmall modules and noncosmall modules, Ring theory (Proc. Antwerp Conf. (NATO Adv. Study Inst.), Univ. Antwerp, Antwerp, 1978), 1979, pp. 669-690.

[4] T. Y. Lam, Lectures on modules and rings, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999.

[5] A. Ç Özcan, Modules with small cyclic submodules in their injective hulls, Comm. Algebra 30 (2002), no. 4, 1575-1589.

[6] Y. Talebi and N. Vanaja, The torsion theory cogenerated by M-small modules, Comm. Algebra 30 (2002), no. 3, 1449-1460.

[7] H. Zöschinger, Koatomare Moduln, Math. Z. 170 (1980), no. 3, 221-232.

[8] H. Zöschinger, Schwach-injektive Moduln, Period. Math. Hungar. 52 (2006), no. 2, 105-128.

Izmir Institute of Technology, Izmir, Turkey

email: yusufalagoz@iyte.edu.tr

Generalized Derivations with Some Related Conditions on Lie Ideals

Emine ALBAŞ

This is joint work with V. De Filippis and N. Argaç. Let R be a prime ring of characteristic different from 2. In this talk unless specially states $Z(R)$ always denotes the center of R, U the Utumi quotient ring of R and $C = Z(U)$, the center of U (C is usually called the extended centroid of R). A well known result of Posner [7] states that if d is a derivation of R such that $[d(x), x] \in Z(R)$, for any $x \in R$, then either $d = 0$ or R is commutative. Later in [4] Lanski proves that if d is a nonzero derivation of R so that $[d(x), x] \in Z(R)$ for all $x \in L$, a non-central Lie ideal of R, then $char(R) = 2$ and $R \subseteq M_2(C)$, the ring of 2×2 matrices over C. More recently Chebotar, Lee and Wong [1] generalize the previous results in case the characteristic of R is different from 2 or 3. More precisely they prove that if L is a non central Lie ideal of R, then the additive subgroup S generated by $\{[d(x), x] : x \in L\}$ contains a non central Lie ideal W of R. In particular S is not contained in $Z(R)$, unless $d = 0$. Moreover, since both the left (right) annihilator $Ann_R(W)$ and the centralizer $C_R(W)$ of a Lie ideal W of a prime ring are trivial, that is $Ann_R(W) = (0)$ and $C_R(W) = Z(R)$, then both the left (right) annihilator and centralizer of S are trivial and these facts in a prime ring are natural tests which evidence that the set $\{[d(x), x] : x \in L\}$ is rather large in R.

This work follows the line of investigation of the previous ones, by replacing the derivation d with some additive maps which generalize the concept of usual derivation on R.

An additive map $G : R \to R$ is called generalized derivation of R if there exists a derivation d of R such that $G(xy) = G(x)y + xd(y)$, for all $x, y \in R$. The simplest example of generalized derivation is a map of the form $g(x) = ax + xb$, for some $a, b \in R$: such generalized derivations are called inner. Generalized inner derivations have been primarily studied on operator algebras. Therefore any investigation from the algebraic point of view might be interesting (see for example [3], [5], [6]). Here we will consider some related problems concerning identities with generalized derivations in prime rings. In [2], V. De Filippis et al. prove that if R is a prime ring of characteristic different from 2, L a non-central Lie ideal of R and F is a non-zero generalized derivations of R such that $[F(u), u]F(u) = 0$, for all $u \in L$, then one of the following holds:

1. there exists $\alpha \in C$ such that $F(x) = \alpha x$, for all $x \in R$;
2. $R \subseteq M_2(C)$ and there exist $a \in U$ and $\alpha \in C$, such that $F(x) = ax + xa + \alpha x$, for all $x \in R$.

In this talk, we aim to generalize this study as follows:

Theorem. *Let R be a non-commutative prime ring of characteristic different from 2 with Utumi quotient ring U and extended centroid C, L a non-central Lie ideal of R, F and G two non-zero generalized derivations of R. If $[F(u), u]G(u) = 0$ for all $u \in L$, then one of the following holds:*

1. *there exists $\lambda \in C$ such that $F(x) = \lambda x$, for all $x \in R$;*

2. $R \subseteq M_2(C)$, the ring of 2×2 matrices over C, and there exist $a \in U$ and $\lambda \in C$ such that $F(x) = ax + xa + \lambda x$, for all $x \in R$.

References

[1] M.A. Chebotar, P.H. Lee, T.L. Wong, A note on derivations, additive subgroups and Lie ideals of prime rings, Comm. Algebra 30/10 (2002), 5011-5021.

[2] V. De Filippis, G. Scudo, M.S. Tammam El-Sayiad, An identity with generalized derivations on Lie ideals, right ideals and Banach algebras, Czechoslovak Math. J. 62(137) (2012), 453-468.

[3] B. Hvala, Generalized derivations in rings, Comm. Algebra 26(4) (1998), 1147-1166.

[4] C. Lanski, Differential identities, Lie ideals, and Posner's theorems, Pac. J. Math. 134/2 (1988), 275-297.

[5] T.K. Lee, Generalized derivations of left faithful rings, Comm. Algebra 27(8) (1999), 4057-4073.

[6] T.K. Lee, W.K. Shiue, Identities with generalized derivations, Comm. Algebra 29(10) (2001), 4435-4450.

[7] E.C. Posner, Derivations in prime rings, Proc. Amer. Math. Soc. 8 (1958), 1093-1100.

Ege University

email: emine.albas@ege.edu.tr

On Quadratic Functions and Artin-Schreier Curves

Nurdagül Anbar

For an odd prime p and an even integer n with $\gcd(n, p) = 1$, we consider quadratic functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of codimension k. For various values of k, we obtain classifications of quadratic functions giving rise to maximal and minimal Artin-Schreier curves over $\mathbb{F}_{p^n}$. We completely classify all maximal and minimal curves obtained from quadratic functions of codimension 2 whose coefficients lie in the prime field $\mathbb{F}_p$. In particular, to obtain these results we compute the sign of Walsh coefficients of special classes of (non-monomial) quadratic functions. This is a joint work with Wilfried Meidl.

References

[1] N. Anbar, W. Meidl, Quadratic Functions and Maximal Artin-Schreier Curves, submitted.

Sabanci University, MPI

email: nurdagulanbar2@gmail.com

Zaitsev Type Results

Ahmet Arıkan

This is a joint work with Aynur Arıkan and Nadir Trabelsi. In a series of papers [2, 3, 4, 5], Zaitsev has been proved many interesting results on soluble and nilpotent groups (see also [1]). In particular he proved that "every infinite soluble (nilpotent) group of derived length d (of class c) has a proper subgroup of derived length d (of class c)". In the present talk we generalize his results to general contexts, in particular to groups which satisfy an outer commutator law.

References

[1] Kirichenko V. V., Kurdachenko L. A., Otal J. and Subbotin I. Ya., On the contribution of D. I. Zaitsev to the Theory of Infinite Groups. *Algebra and Discrete Mathematics.* **13** (2012). Number 1. 59-91.

[2] Zaĭcev, D. I., Stably solvable groups. (Russian) *Izv. Akad. Nauk. SSSR Ser. Mat.* **33** (1969), 765-780; translated as Soviet Math. Dokl. **8** (1967), 1122-1125.

[3] Zaĭcev, D. I., The existence of stably nilpotent subgroups in locally nilpotent groups. (Russian) *Mat. Zametki* **4** (1968), 361-369.

[4] Zaĭcev, D. I., Stably nilpotent groups. Math. Notes **2** (1967), 690-694 (1968); translated from *Mat. Zametki* **2** (1967), 337-346.

[5] Zaĭcev, D. I., Stably solvable and stably nilpotent groups. (Russian) *Dokl. Akad. Nauk. SSSR* **176** (1967), 509-511.

Gazi University

email: arikan@gazi.edu.tr

web: http://websitem.gazi.edu.tr/site/arikan

Infinitely generated periodic groups

Aynur Arıkan

Let G be a group and let $\wp$ be a group theoretical property. If every proper subgroup of G satisfies $\wp$ but G itself dose not satisfy $\wp$, Then G is called a minimal non-$\wp$-group (MNP-group for short). For example $\wp$ may stand for "solvable", "hypercentral", "finite exponent", "finite conjugacy class" and then the group may be called as MNS-group, $MNHC$-group, $MNFE$-group or $MNFC$-group, respectively.

In the present paper we consider infinitely generated periodic groups and give positive result about the problem stated in [3, p.262].

Definition. Let G be a group. As is well-known, G is called an FC-group if for all $x \in G$,

$$|G : C_G(x)| < \infty.$$

G is called a minimal non FC-group if every proper subgroup of G is an FC-group but does not have this property.

Let us consider the following problem given in [3, p.262]

Problem. Suppose that the group G is the union of conjugates of a subgroup H. What conditions on H and G allow us to deduce that $G = H$?

The following is a positive result about this problem.

Theorem 1. *Let G be an infinitely generated perfect periodic group in which every proper subgroup is hypercentral and residually (nilpotent of finite exponent) and every proper normal subgroup is an FC-group. Then there exists a proper subgroup of G that contains a conjugate of every element of G.*

Corollary 2. *Let G be a perfect locally finite barely transitive group such that a point stabilizer is hypercentral and every proper normal subgroup is an FC-group. Then there exist a proper subgroup of G that contains a a conjugate of every element of G. In particular G cannot be an $MNFE$-group.*

In general it is not known whether a barely transitive group can be the union of the conjugates of a proper subgroups. However a group of finitary permutations on a infinitary set has this property by [3, Theorem 1].

References

[1] Asar, A. O., *On infinitely generated groups whose proper subgroups are solvable.* J. Algebra 399 (2014), 870-886.

[2] Belyaev. V.V.,*On the question of existence of minimal non-FC-groups.* Siberian Math. J. 39 (1998) no.1093-1095.

[3] Cutolo, C.,Smith, H.,Wiegold,J.,*Locally Finite Groups.* J. Algebra 293 (2005), 261-268

[4] Martinelli, A., *Hepercentral groups with all subgroups subnormal.* J. Group Theory 11, no. 1, (2010).743-757.

Gazi University

email: yalincak@gazi.edu.tr

G-Dedekind primeness of Morita context

Pınar Aydoğdu

A short time after Morita had come up with the idea of Morita contexts in 1958, it was understood that Morita contexts are a very useful and connective tool. For instance, in 1962, Bass used Morita contexts to prove Wedderburn Theorems on the structure of simple rings. In 1971, Amitsur used it to prove Wedderburn Theorems for semisimple rings and Goldie Theorems for the quotient rings of semisimple rings, and to work on the endomorphism ring of a module. Morita contexts are very suitable structures to work on transfering properties from a ring R to a ring S. In this work, the problem of determining the G-Dedekind primeness of Morita contexts is investigated. We extend the usage of Morita contexts from the point of view of order rings. This work is essentially a continuation of the paper [1]. This is a joint work with E. Akalan, H. Marubayashi and B. Saraç.

References

[1] Marubayashi, Hidetoshi; Zhang, Yang; Yang, Po; On the rings of the Morita context which are some well-known orders. Comm. Algebra 26 (1998), no. 5, 14291444.

Hacettepe University email: paydogdu@hacettepe.edu.tr

Groups Whose Proper Subgroups Have Polycyclic-By-Finite Conjugacy Classes

Mounia Bouchelaghem

This is a joint work with Nadir Trabelsi (University Setif 1, Algeria).

A group G is said to be an FC-group (respectively, PC-group, PFC-group), if $G/C_G(x^G)$ is a finite (respectively, polycyclic, polycyclic-by-finite) group for all $x \in G$. Note that the classes of PC-groups and PFC-groups are generalizations of the familiar property of being an FC-group. If $\mathfrak{X}$ is a class of groups, then G is said to be a minimal non-$\mathfrak{X}$-group if it is not an $\mathfrak{X}$-group but all of whose proper subgroups are $\mathfrak{X}$-groups. Many results have been obtained on minimal non-$\mathfrak{X}$-groups, for various choices of $\mathfrak{X}$. In particular, in [1] and [2], Belyaev and Sesekin characterized minimal non-FC-groups when they have a non-trivial finite or abelian factor group. They proved that such minimal non-FC-groups are finite cyclic extensions of divisible p-groups of finite rank, where p is a prime. In [3], De Giovanni and Trombetti studied minimal non-PC-groups that have a non-trivial abelian factor group and they proved that if G is such a minimal non-PC-group, then G is a minimal non-FC-group. Here we generalize the previous result to minimal non-PFC-groups, we prove that if G is a group that has a non-trivial abelian factor group then G is a minimal non-PFC-group if and only if G is a minimal non-FC-group.

References

[1] Belyaev, V.V., Sesekin, N.F.: Infinite groups of Miller-Moreno type. Acta Math. Hungar. 26, 369–376 (1975).

[2] Belyaev, V.V.: Minimal non-FC-groups. In: Prooceedings of the VI all union symposium group theory, Cerkassy, 1978. Naukova Dumka, Kiev, 221, 97–102 (1980)

[3] De Giovanni, F., Trombetti, M.: Groups whose proper subgroups of infinite rank have polycyclic conjugacy classes, to appear.

University Setif 1

email: bouchelaghem_math@yahoo.fr

New infinite families of 2-edge-balanced graphs

Cafer Çalışkan

A graph G of order n is called *t-edge-balanced* if G satisfies the property that there exists a positive λ for which every graph of order n and size t is contained in exactly λ distinct subgraphs of K_n isomorphic to G. We call λ the *index* of G. In this talk, I present how to obtain new infinite families of 2-edge-balanced graphs.

Kadir Has University

email: cafer.caliskan@khas.edu.tr

On the fast computation of Toeplitz matrix vector products over $\mathbb{F}_2$

Murat Cenk

Toeplitz matrix vector products (TMVP) over $\mathbb{F}_2$ are required for cryptographic computations and digital signal processing. The recent work has revealed that finite field multiplications can be represented by such kind of products, and several efficient algorithms have been proposed [1], [2], [3]. In this work, after presenting known efficient algorithms for TMVP, the relation between the polynomial multiplication and TMVP is introduced. Then, the algebraic method for the binary polynomial multiplication proposed in [3] is presented. Finally, we show how the computational complexity of TMVP can be further improved significantly.

References

[1] OH. Fan and M.A. Hasan, A New Approach to Subquadratic Space Complexity Parallel Multipliers for Extended Binary Fields, IEEE Trans. Computers, 56(2),224-233, 2007

[2] M. Anwar Hasan, Christophe Negre, Subquadratic Space Complexity Multiplier for a Class of Binary Fields Using Toeplitz Matrix Approach, IEEE Symposium on Computer Arithmetic, 67-75, 2009

[3] Murat Cenk, Christophe Negre and M. Anwar Hasan, Improved Three-Way Split Formulas for Binary Polynomial and Toeplitz Matrix Vector Products, IEEE Trans. Computers 62(7): 1345-1361, 2013

Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

email: mcenk@metu.edu.tr

web: www.metu.edu.tr/~mcenk

Cohomology and Deformations of Hom-bialgebras and Hom-Hopf algebras

K. Dekkar

In Hom-bialgebra structures, the associativity, and the coassociativity conditions $(xy)z = x(yz)$ and $(\Delta \otimes id) \circ \Delta = (id \otimes \Delta) \circ \Delta$ are twisted to $\alpha(x)(yz) = (xy)\alpha(z)$ and $(\Delta \otimes \alpha) \circ \Delta = (\alpha \otimes \Delta) \circ \Delta$, respectively, with α a map in the appropriate category. In the present paper, we consider the deformation theory of Hom-bialgebra, there is a natural concept of infinitesimal deformation. These infinitesimals are elements of a cohomology group, there is also a natural concept of rigidity.

References

[1] F. Ammar, A. Makhlouf, Hom-Lie algebras and Hom-Lie admissible superalgebras, . arxiv:0906.1668, (2009).

[2] S. Caenepeel, and I. Goyvaerts, Hom-Hopf algebras, arxiv 0907.0187v1(2009).

[3] K. Dekkar, A. Makhlouf, Bialgebra structures of 2-associative algebras, The arabian journal for science and engineering, volume 33, number 2C (2008).

Bordj Bou-Arreridj University

email: k.dekkar@univ-bba.dz

On Leibniz algebras

Ismail Demir

Leibniz algebras are certain generalization of Lie algebras. In studying the properties of the homology of Lie algebras, Loday observed that the antisymmetry of the product was not needed to prove the derivation property defined on chains. This motivated him to introduce the notion of Leibniz algebras. Since the introduction of Leibniz algebras around 1993 several researchers have tried to find analogs of important theorems in Lie algebras. We define an analogue of the Killing form and show that if the Leibniz algebra is semisimple then this form is nondegenerate, but the converse is not true. We prove the classification of non-Lie nilpotent three dimensional Leibniz algebras using a new approach involving the canonical forms for the congruence classes of matrices for bilinear forms which can easily be used to classify higher dimensional Leibniz algebras. This is a joint work with Kailash C. Misra and Ernie Stitzinger.

References

[1] Demir, I., Misra, K.C., Stitzinger, E. *On some structures of Leibniz algebras*, arXiv:1307.7672v1 [math.RA], (2013).

[2] Turnbull, H.-W., Aitken, A.-C. An introduction to the Theory of Canonical Matrices, *Dover*, 1961(First published by: Blackie& Son Limited, 1932).

[3] Gorbatsevich, V. On some basic properties of Leibniz algebras, arXiv:1302:3345v2 [math.RA], (2013).

North Carolina State University

email: idemir@ncsu.edu

Linearly Independent Latin Squares

Fatih Demirkale

In this talk, we will first define the linear independence of Latin squares. Later we will identify a set of $s(s-1)^2$ Latin squares and represent these as vectors. We will show these vectors can be used to form intercalates which form a basis for a linear space which contains all Latin trades. We will also show that $(s-1)^3+1$ of these vectors are linearly independent. We will use this theory to study an asymptotic formula for the number of $OA(N,3,s,2)$ for $s \geq 3$, and we will show that for a given s, the number of $OA(N,3,s,2)$ is $\lambda^{(s-1)^3(1-o(1))}$ as $\lambda \to \infty$.

Koç University

email: fdemirkale@ku.edu.tr

On large sets of projective planes of orders 3 and 4

Emre Kolotoğlu

A t-(v,k,λ) design is a pair $(X,\mathcal{B})$, where X is a set of v elements, called *points*, and $\mathcal{B}$ is a set of k-subsets of X, called *blocks*, where each t-subset of X is contained in precisely λ blocks.

Let $\binom{X}{k}$ denote the set of all k-subsets of a set X. A large set $LS[N](t,k,v)$ is a pair $(X,\mathbb{B}=\{\mathcal{B}_i\}_{i=1}^N)$, where $(X,\mathcal{B}_i)$ is a t-(v,k,λ) design for all $\mathcal{B}_i \in \mathbb{B}$, and $\{\mathcal{B}_i\}_{i=1}^N$ is a partition of $\binom{X}{k}$. Arithmetically, for a large set $LS[N](t,k,v)$, we have $N=\binom{v-t}{k-t}/\lambda$.

A projective plane of order n, if such exists, is a 2-$(n^2+n+1,n+1,1)$ design. It is known that a projective plane of order n exists when n is a prime power, and these are the only orders for which a projective plane is known to exist. If a large set of projective planes of order n exists, it is an $LS[N](2,n+1,n^2+n+1)$, where $N=\binom{n^2+n-1}{n-1}$.

In 1850, Cayley [1] proved by a brief argument that a large set $LS[5](2,3,7)$ of Fano planes (projective planes of order 2) does not exist. In 1978, Magliveras conjectured that a large set of projective planes of order n will exist for all

$n \geq 3$, provided that n is the order of a projective plane. In 1983, Chouinard II [2] constructed such large sets for $n = 3$, namely $LS[55](2,4,13)$, by prescribing an automorphism of order 11 which acts semiregularly on the set of 55 planes. In 2013, Magliveras and I [3] constructed new large sets $LS[55](2,4,13)$ by prescribing an automorphism of order 13. We classified all such large sets and determined their full automorphism groups.

The existence, or otherwise, of a large set of projective planes of order n for $n \geq 4$, is still an unsettled problem. For $n = 4$, such a large set would consist of 969 planes. Kramer and Magliveras have constructed over 600 mutually disjoint projective planes of order 4 by probabilistic means. In our effort to construct a large set $LS[969](2,5,21)$, we constructed 912 mutually disjoint projective planes of order 4 by prescribing C_{19}^9 as an automorphism group.

In this talk, I will present the methods we used in these new constructions.

References

[1] A. Cayley, *On the triadic arrangements of seven and fifteen things*, London, Edinburgh and Dublin Philos. Mag. and J. Sci. 37 (1850) 50–53.

[2] L. G. Chouinard II, *Partitions of the 4-subsets of a 13-set into disjoint projective planes*, Discrete Math. 45 (1983) 297–300.

[3] E. Kolotoğlu, S. Magliveras, *On large sets of projective planes of orders 3 and 4*, Discrete Math. 313(20) (2013) 2247–2252.

Yıldız Technical University

email: emkolot@yahoo.com

Canonical Lifting of Abelian Varieties

Altan Erdoğan

In this talk we will give a brief review of Serre-Tate theorem on lifting abelian varieties. We will also give some results on the canonical lifting of elliptic curves in terms of the j-invariants and talk on possible generalizations of these results.

Gebze Institute of Technology

email: alerdogan@gyte.edu.tr

A survey on recent advances about irreducible representation of Leavitt path algebras

Songül Esin

This talk is a survey about irreducible representations (or simple modules) of Leavitt path algebras.

For a field K and arbitrary graph E, Chen constructed irreducible representations of Leavitt path algebra,

$L_K(E)$, by using sinks and tail-equivalent classes of infinite paths in the graph E.

Chen's construction was expanded by P. Ara and K.M. Rangaswamy to introduce additional classes of non-isomorphic simple $L_K(E)$-modules. Also, Rangaswamy constructed a new class of simple modules over the Leavitt path algebra $L_K(E)$ by using vertices that emit infinitely many edges in E.

email: songulesin@gmail.com

Some properties of a Generalized 3-Abelian Groups

Meriem Hamitouche

Let $n \geq 2$ be an integer, A group G is called generalized n-abelian whenever there exist elements $c_1, ..., c_n \in G$ such that the map $x \longmapsto x^{c_1}...x^{c_n}$ is an endomorphism of G. For any non-zero integer n, a group G is called n-Levi if $[x, y^n] = [x, y]^n$ for all $x, y \in G$, It is called n-central if $n \geq 1$ and $[x, y^n] = 1$ for all $x, y \in G$. We show that there is a relation between generalized 3-abelian groups G and n-Levi or n-central groups. We also prove that G is 3-nilpotent of class at most 3.

University Abderrahmane Mira-Bejaia, Algeria

email: hamitouche85@yahoo.fr

Injective hulls of simple modules over differential operator rings

Can Hatipoğlu

We consider Noetherian rings over which injective hulls of simple modules are locally Artinian. After a short motivation, we focus on the injective hulls of simple modules over differential operator rings, providing sufficient conditions under which these modules are not locally Artinian. As a consequence we characterize Ore extensions $S = K[x][y; \sigma, d]$ such that the injective hulls of simple S-modules are locally Artinian.

This is a joint work with Paula Carvalho and Christian Lomp of the University of Porto.

Centre of Mathematics of the University of Porto

email: chatipoglu@alunos.fc.up.pt

web: http://www.fc.up.pt/pessoas/up200908307/

On the maximal number of points on singular curves over finite fields

Annamaria Iezzi

1 Introduction

This in a joint with Yves Aubry.

Singular curves arise naturally in many Discrete Mathematics problems. A first example from coding theory is the geometric constructions of error correcting codes defined by the evaluation of points on algebraic varieties. The study of hyperplane sections or more generally of sections of such varieties is needed to find the fundamental parameters of these codes, and we often get singular varieties. Another example comes from the theory of boolean functions. Indeed, we have a geometric characterization of the APN property (Almost Perfect Nonlinear) of a function by determining whether the rational points of a certain algebraic set (which is a singular curve or a singular surface) are included in an union of hyperplanes.

The zeta function of a singular curve has been studied in [1] and [2]. The principal result is that the numerator of the zeta function of such a curve over $\mathbb{F}_q$ is a polynomial not only with inverse root of modulus $\sqrt{q}$ but also of modulus 1.

The geometric genus is not the only invariant which classifies singular curves, there is also the arithmetic genus. For q a power of a prime, g and π non negative integers such that $\pi \geq g$, here we introduce a quantity of interest, denoted by $N_q(g, \pi)$, to be the maximal number of rational points over $\mathbb{F}_q$ that an absolutely irreducible projective algebraic curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π can have. Its study should answer several problems listed above.

2 Bounds for singular curves

Let us recall some results on singular curves from [1].

Let X be an absolutely irreducible projective curve defined over $\mathbb{F}_q$ of arithmetic genus π and geometric genus g. If $\tilde{X}$ is the normalization of X, then:

$$|\sharp\tilde{X}(\mathbb{F}_q) - \sharp X(\mathbb{F}_q)| \leq \pi - g. \tag{\dagger}$$

The zeta function $Z_X(T)$ of X is the product of the zeta function $Z_{\tilde{X}}(T)$ of $\tilde{X}$ and a polynomial of degree

$$\Delta_X = \sharp(\tilde{X}(\overline{\mathbb{F}}_q) \backslash X(\overline{\mathbb{F}}_q)).$$

Its structure allows to determine that:

$$\sharp X(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \omega_i^n - \sum_{i=1}^{\Delta_X} \beta_j^n,$$

for some algebraic integers ω_i of absolute value $\sqrt{q}$ and some roots of unity β_j in $\mathbb{C}$.

In particular, the number of rational points on X verifies:

$$|\sharp X(\mathbb{F}_q)-(q+1)|\leq g[2\sqrt{q}]+\pi-g\leq \pi[2\sqrt{q}]. \qquad (\ddagger)$$

3 The quantity $N_q(g,\pi)$

For q a power of a prime, g and π non negative integers such that $\pi\geq g$, let us define the quantity

$$N_q(g,\pi)$$

as the maximal number of rational points over $\mathbb{F}_q$ that an absolutely irreducible projective algebraic curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π can have.

We have

$$N_q(g,g)=N_q(g),$$

where $N_q(g)$ is the usual notation for the maximal number of rational points over $\mathbb{F}_q$ that a smooth absolutely irreducible projective algebraic curve defined over $\mathbb{F}_q$ of geometric genus g can have (since a curve is smooth if and only if its arithmetic genus equals its geometric one).

If X is an absolutely irreducible projective algebraic curve defined over $\mathbb{F}_q$ of geometric genus g and arithmetic genus π, we obtain from (†):

$$\sharp X(\mathbb{F}_q)\leq \sharp\tilde{X}(\mathbb{F}_q)+\pi-g\leq N_q(g)+\pi-g.$$

Hence:

$$N_q(g,\pi)\leq N_q(g)+\pi-g \qquad (\S)$$

and using the Serre-Weil bound for smooth curves, we obtain as discussed in the previous section:

$$\sharp X(\mathbb{F}_q)\leq q+1+g[2\sqrt{q}]+\pi-g. \qquad (\P)$$

4 Singular curves with many points

Using the construction of Serre of singular curves developed in [4, Chapter 4, 3.4] (adapted to the case of a non-algebraically closed field) and descent theory, we can prove the following theorem:

Theorem 3. *Let Y be a smooth absolutely irreducible algebraic projective curve of genus g defined over $\mathbb{F}_q$. Let π be an integer of the form*

$$\pi=g+a_2+2a_3+3a_4+\cdots+(n-1)a_n$$

with $0\leq a_i\leq B_i(Y)$, where $B_i(Y)$ is the number of closed points of degree i on the curve Y. Then there exists a (singular) absolutely irreducible algebraic projective curve X over $\mathbb{F}_q$ of arithmetic genus π such that Y is the normalization of X (so that X has geometric genus g) and

$$\sharp X(\mathbb{F}_q)=\sharp Y(\mathbb{F}_q)+a_2+a_3+a_4+\cdots+a_n=\sharp Y(\mathbb{F}_q)+\pi-g-(a_3+2a_4+\cdots+(n-2)a_n).$$

In particular if $\sharp Y(\mathbb{F}_q) = N_q(g)$, i.e. Y is an optimal curve, then Theorem 3 implies that we can construct a curve X such that:

$$\sharp X(\mathbb{F}_q) = N_q(g) + \pi - g - (a_3 + 2a_4 + \cdots + (n-2)a_n).$$

Let $\mathcal{Y}_q(g)$ be the set of smooth absolutely irreducible algebraic projective curves Y defined over $\mathbb{F}_q$ with an optimal number of rational points, i.e. such that:

$$\sharp Y(\mathbb{F}_q) = N_q(g).$$

Let $B_2(\mathcal{Y}_q(g))$ be the maximum number of points of degree 2 that a curve of $\mathcal{Y}_q(g)$ can have. Then, we have:

Proposition 4. *For every $g \leq \pi \leq g + B_2(\mathcal{Y}_q(g))$ there exists a (singular) curve X of geometric genus g and arithmetic genus π that attains (§), i.e.*

$$\sharp X(\mathbb{F}_q) = N_q(g) + \pi - g.$$

In other words for every $g \leq \pi \leq g + B_2(\mathcal{Y}_q(g))$ we have

$$N_q(g,\pi) = N_q(g) + \pi - g.$$

4.1 The case of rational curves

Let start from $Y = \mathbb{P}^1$, the projective line, over a finite field $\mathbb{F}_q$. In this case the number of closed points of degree 2 is:

$$B_2(\mathbb{P}^1) = \frac{q^2 - q}{2}.$$

It follows from Proposition 4:

Corollary 5. *If $\pi \leq \frac{q^2-q}{2}$, then*

$$N_q(0,\pi) = N_q(0) + \pi = q + 1 + \pi.$$

In [3], the curve B proposed by Fukasawa, Homma and Kim is an explicit example of rational singular curve that attains $N_q(0, \frac{q^2-q}{2})$. In the same paper, the curve B_n, that is a generalization of the curve B, is an explicit example of rational singular curve such that:

$$\sharp B_n(\mathbb{F}_q) = q + 1 + B_2(\mathbb{P}^1) + B_3(\mathbb{P}^1) + \cdots + B_n(\mathbb{P}^1)$$

Thus we propose the following question:

For all $n \geq 2$,

$$N_q(0, B_2(\mathbb{P}^1) + 2B_3(\mathbb{P}^1) + \cdots + (n-1)B_n(\mathbb{P}^1)) = q + 1 + B_2(\mathbb{P}^1) + B_3(\mathbb{P}^1) + \cdots + B_n(\mathbb{P}^1)?$$

5 Maximal curves

In the set of not necessarily smooth curves, we define maximal curves:

Definition. A (not necessarily smooth) absolutely irreducible projective algebraic curve X defined over $\mathbb{F}_q$ is called maximal if it reaches the bound from equation (¶), i.e. if

$$\sharp X(\mathbb{F}_q) = q + 1 + g[2\sqrt{q}] + \pi - g.$$

We find the classical definition of maximal curve when X is smooth (i.e. it reaches the Serre-Weil bound).

The curve B provided by Fukasawa, Homma and Kim in [3] is an example of maximal singular curve.

Proposition 6. *If X is a maximal curve defined over $\mathbb{F}_q$ with q a square, of geometric genus g and arithmetic genus π, then:*

$$2g(\sqrt{q} + q - 1) + 2\pi \leq q^2 - q.$$

For such a curve X the zeta function is:

$$Z_X(T) = \frac{(1 + \sqrt{q}T)^{2g}(1 + T)^{\pi - g}}{(1 - T)(1 - qT).}$$

Remark: In the case of maximal rational curves, the hypothesis of q a square is not necessary and Proposition 6 implies:

$$\pi \leq \frac{q^2 - q}{2}.$$

It is interesting to note that the maximal singular curve provided by Fukasawa, Homma and Kim in [3] has maximal arithmetic genus $\pi = \frac{q(q-1)}{2}$.

As a consequence of the previous remark and Corollary 5, we can state the following result:

Proposition 7. *We have*

$$N_q(0, \pi) = q + 1 + \pi$$

if and only if $\pi \leq \frac{q^2 - q}{2}$.

References

[1] Y. Aubry, M. Perret, A Weil theorem for singular curves, *Arithmetic, Geometry and Coding Theory (Luminy, 1993)*, Walter de Gruyter, Berlin-New York, (1996), p. 1–7.

[2] Y. Aubry and M. Perret, On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields, *Finite Fields and Their Applications*, 10/3 (2004), p. 412–431.

[3] S. Fukasawa, M. Homma and S. J. Kim Rational curves with many rational points over a finite field, *Arithmetic, Geometry and Coding Theory - 2011*, Contemporary Mathematics 574, AMS, 2012, p. 37–48.

[4] J.-P. Serre, Groupes algébriques et corps de classes, Hermann, Paris, 1959.

University of Aix-Marseille

email: annamaria.iezzi@univ-amu.fr

On the minimum distance of cyclic codes

Leyla Işık

Estimation of the minimum distance of cyclic codes is a classical problem in coding theory. Using the trace representation of cyclic codes and Hilbert's 90 Theorem, Wolfmann found a general estimate for the minimum distance of cyclic codes in terms of the number of the rational points on certain Artin-Schreier curves. In this talk, we present some of conditions, under which the Wolfmann's bound can be improved by the use of permutation polynomials.

Sabancı University

email: isikleyla@sabanciuniv.edu

Representations of Leavitt and Cohn-Leavitt path algebras

Ayten Koç

This is a joint work with Murad Özaydın.

Leavitt and Cohn-Leavitt path algebras of a directed graph Γ are generated by the vertices and the arrows of Γ with relations (also determined by Γ) analogous to those of Cuntz-Krieger C*-algebras. We study their representations, in particular we determine all finite dimensional representations in terms of the semigroup of the digraph Γ and dimension functions. We give an effective algorithm to determine the existence of a finite dimensional representation when Γ is finite.

References

[1] G. Abrams, A. Pino, M.S. Molina,*The Leavitt path algebra of a graph,* Journal of Algebra **293**, 319–334, (2005).

[2] G. Abrams, A. Pino, M.S. Molina, *Finite-dimensional Leavitt path algebras,* Journal of Pure Appl.Algebra **209**, 753–762, (2007).

[3] P. Ara, K.R. Goodearl, *Leavitt path algebras of separated graph,* J. reine angew. Math. **669**, 165–224, (2012).

İstanbul Kültür University

email: akoc@iku.edu.tr

The Test Rank of A Soluble Product of Free Abelian Lie Algebras

Nazar Şahin ÖĞÜŞLÜ

Let L be the lth solvable product of free abelian Lie algebras of finite rank. We prove that the test rank of L is one less than the number of the factors. We also give a test set for endomorphisms of L.

This is a joint work with Naime EKİCİ.

Key words: Free Lie algebras, soluble algebras, test rank

Mathematics Subject Classification: 17B01, 17B40

References

[1] Ekici, N., Öğüşlü, N. Ş., Test rank of an abelian product of a free Lie algebra and a free abelian Lie algebra. Proc. Indian Acad. Sci. Math. Sci., 121, 3, 291-300, 2011.

[2] Esmerligil, Z., Ekici, N., Test sets and test rank of a free metabelian Lie algebra. Comm. Algebra, 31, 11, 5581-5589, 2003.

[3] Esmerligil, Z., Kahyalar, D., Ekici, N., Test rank of F/R' Lie algebras. Internat. J. Algebra Comput., 16, 4, 817-825, 2006.

[4] Gupta, C. K., Timoshenko, E. I., The test rank of a soluble product of free abelian groups, Sb. Math., 199, 4, 495-510, 2008.

[5] Shpilrain, V., On generators of L/R^2 Lie algebras, Proc. Amer. Math. Soc., 119, 4, 1039-1043, 1993.

[6] Timoshenko, E. I., Test sets in free metabelian Lie algebras, Siberian Math. J., 43, 6, 1135-1140, 2002.

Department of Mathematics, Çukurova University, Adana,Turkey

email: noguslu@cu.edu.tr

Involution of Structural Matrix Algebras

Özkay Özkan

This is a joint work with Mustafa Akkurt.

The involutions and automorphism groups of structural matrix algebras and incidence algebras were studied by several authors. Coelho [1] stated the conditions for automorphism group of a structural matrix algebra . Spiegel [2] had the similar results for incidence algebras. Spiegel stated that when a poset has a comparable element then the automorphism group of incidence algebra defined on this poset just consists of inner automorphisms and [3] gave us the involutions of an incidence algebra. But [3] includes some error. So Brusamarello and Lewis [5] published some new results on involutions. They also surveyed some basic results about incidence algebras and their automorphism groups. In [5], when a finite partially ordered set has a comparable element, they presented necessary and sufficient conditions for two involutions on the incidence algebra of X to be equivalent.

References

[1] S. P. Coelho. *The automorphism group of structural matrix algebra.* Linear Algebra and its Appl., 195:35–58, 1993.

[2] E. Spiegel, C. J. O'Donnell, *Incidence algebras*, New York:Marcel Dekker, 1997.

[3] E. Spiegel, *Involutions in incidence algebras.* Linear Alg. Appl. 405: 155-162, 2005.

[4] F.Anderson and B. D'Ambrossia, *Square free algebras and their automorphism groups.* Commun. Alg. 24: 3163-3191, 1996.

[5] Brusamarello R., Lewis D. W., *Automorphisms and involutions on incidence algebras.* Linear and Mult. Alg. 59:1247-1267, 2011.

[6] O. M. Di Vincenzo, P. Koshlukov, R. La Scala, *Involutions for upper triangular matrix algebras.* Adv. Appl. Math. 37: 541-568, 2006.

[7] Y. Drozd, P. Kolesnik, *Automorphisms of incidence algebras.* Commun. Alg. 35: 3851-3854, 2007.

[8] R. P. Stanley *Structure of incidence algebras and their automorphism groups.* Bull. Amer. Math. Soc. 76:1936-1939,1970.

[9] Brusamarello R. Fornaroli E. Z., Santulo A. Jr., *Classification of involutions on incidence algebras.* Comm. Alg. 39: 1941-1955, 2011.

Gebze Institute of Technology

email: ozkayoz@yahoo.com

The Hamilton - Waterloo Problem with Uniform Cycle Sizes

Sibel Özkan

Decomposing graphs into edge-disjoint cycles is may be the most studied graph decomposition problem. If we add the condition that the cycles must be resolved into parallel classes, then this problem becomes a 2-factorization problem where each 2-factor is a parallel class of cycle(s).

A $\{C_m^r, C_n^s\}$-decomposition of the complete graph on v vertices, K_v, asks for a 2-factorization of K_v, where r of the 2-factors consists of m-cycles, and s of the 2-factors consists of n-cycles. (For even v, it is a decomposition of $K_v - F$, where F is a 1-factor.) This is a case of the Hamilton-Waterloo Problem(the HWP) with uniform cycle sizes m and n. The HWP is an extension of the well-known Oberwolfach problem which asks for isomorphic 2-factors. Main focus of this talk will be on the HWP with uniform cycle sizes; some new results on the various lengths of cycles will be presented.

References

[1] P. Adams, E. Billington, D. Bryant, S. El-Zanati, "On the Hamilton-Waterloo Problem", *Graphs and Combinatorics* 18 (2002) 31 - 51.

[2] J.C. Bermond, O. Favaron, M. Mahéo, "Hamiltonian decomposition of Cayley graphs of degree 4", *J. Combin. Theory Ser. B* 46 (1989) 142 - 153.

[3] D. Bryant, C. Rodger, "Cycle Decompositions", In: C.J. Colbourn, J. H. Dinitz as editors, Handbook of Combinatorial Designs, Second Edition, Chapman and Hall/CRC. Boca Raton, FL, 2007, pp. 373 - 382.

[4] P. Danziger, G. Quattrocchi, B. Stevens, "The Hamilton-Waterloo Problem for Cycle Sizes 3 and 4", *Journal of Combinatorial Designs* 17 (2009) 342 - 352.

[5] J.H. Dinitz, A.C.H. Ling, "The Hamilton-Waterloo Problem: The case of Triangle-Factors and One Hamilton Cycle", *Journal of Combinatorial Designs* 17 (2009), 160 - 176.

[6] H.L. Fu, K.C. Huang, "The Hamilton Waterloo Problem for two even cycles factors", *Tawanese Journal of Mathematics* 12 (2008) no: 4 933 - 940.

[7] R. Haggkvist, "A Lemma on Cycle Decompositions", *Annals of Discrete Mathematics*, 27 (1985), 227 - 232.

[8] M.S. Keranen, S. Ozkan, "The Hamilton-Waterloo problem with 4-cycles and one factor of n-cycles", *Graphs and Combinatorics*, 29 (2013), Issue 6, 1827 - 1837.

[9] T.P. Kirkman, "On a Problem on Combinations", *Cambridge and Dublin Math J.*, 2 (1847), 197 - 204.

Gebze Institute of Technology

email: s.ozkan@gyte.edu.tr

web: http://www.gyte.edu.tr/personel/1040/21919/sibel-zkan.aspx

Multidimensional Quasi-Cyclic and Convolutional Codes

Buket Özkaya

For m, l integers with $\gcd(m, q) = 1$, a quasi-cyclic (QC) code of length ml and index l over $\mathbb{F}_q$ is a linear code $\mathcal{C} \subset \mathbb{F}_q^{ml}$ which is invariant under the shift of codewords by l positions (where l is the minimal such number). It is well-known that such a QC code can be viewed algebraically as an R-module of R^l, where $R = \mathbb{F}_q[x]/\langle x^m - 1\rangle$. Alternatively, we can let $S = \mathbb{F}_q[x, y]/\langle x^m - 1, y^l - 1\rangle$ and view a QC code of length ml and index l as an R-submodule of S.

One can decompose a QC code over $\mathbb{F}_q$ into its constituent codes, which are linear codes over certain extensions of $\mathbb{F}_q$ ([3]). Also, a concatenated decomposition structure can be described for QC codes where the inner codes in the decomposition are minimal cyclic codes ([2]). It has been shown in [1] that the constituents in the sense of Ling-Solé and the outer codes in the concatenated structure given by Jensen are the same.

We define multidimensional generalizations of QC codes and investigate their properties. For $n \geq 1$, we let

$$R_n = \mathbb{F}_q[x_1, x_2, \ldots, x_n]/\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle$$

and define the Q-nD-C code of size $m_1 \times \cdots \times m_{n+1}$ as an R_n-submodule of R_{n+1}. It is clear the for $n = 1$, we obtain QC codes (of length $m_1 m_2$ and index m_2). Q-nD-C codes are linear codes of length $m_1 \cdots m_{n+1}$ over $\mathbb{F}_q$ and they can also be viewed as QC codes of index $l = m_2 \cdots m_{n+1}$. However, they have extra shift-invariance properties than ordinary QC codes.

Being QC codes, we can talk about the decomposition of Q-nD-C codes into constituents (or the concatenated structure). We prove that the constituents (or the outer codes in Jensen's concatenated decomposition) of a length $m_1 \cdots m_{n+1}$ Q-nD-C code are Q-(n-1)D-C codes (over various extensions of $\mathbb{F}_q$) of length $m_2 \cdots m_{n+1}$. We also prove that the family of Q-nD-C codes are asymptotically good for any $n \geq 1$.

Quasi-cyclic codes are naturally related to convolutional codes which are defined as rank k $\mathbb{F}_q[x]$-submodules of $\mathbb{F}_q[x]^\ell$. Free distance of a convolutional code can be lower bounded by the minimum distance of an associated QC code (see [4]). Multidimensional generalizations of convolutional codes have also been introduced and studied ([5]). We show that one can naturally associate a QnDC code to any nD convolutional code and prove an analogue of Lally's result for a particular class of nD convolutional codes.

References

[1] C. Güneri and F. Özbudak, "The concatenated structure of quasi-cyclic codes and an improvement of Jensen's bound", *IEEE Trans. Inform. Theory*, vol. 59, no. 2, 979–985, 2013.

[2] J.M. Jensen, "The concatenated structure of cyclic and abelian codes", *IEEE Trans. Inform. Theory*, vol. 31, no. 6, pp. 788-793, 1985.

[3] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: finite fields", *IEEE Trans. Inform. Theory*, vol. 47, pp. 2751-2760, 2001.

[4] K. Lally, "Algebraic lower bounds on the free distance of convolutional codes", *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2101–2110, 2006.

[5] P.A. Weiner, "Multidimensional Convolutional Codes", PhD Thesis, Department of Mathematics, University of Notre Dame, 1998.

Sabancı University

email: buketo@sabanciuniv.edu

Pell Form and Pell Equation in terms of Oblong Numbers

Arzu Özkoç

In this work, we determine the cycle, proper cycle and the set of proper automorphisms of Pell forms $F_{\Delta_k}(x, y) = x^2 - O_k y^2$ of discriminant $\Delta_k = 4O_k$ and determine all integer solutions of the Pell equation $F_{\Delta_k}(x, y) = 1$ via oblong numbers O_k which are the numbers of the form $k(k + 1)$ for an integer $k \geq 0$.

References

[1] E.J. Barbeau. *Pell's Equation.* Springer-Verlag New York, Inc, 2003.

[2] J. Buchmann and U. Vollmer. *Binary Quadratic Forms: An Algorithmic Approach.* Springer-Verlag, Berlin, Heidelberg, 2007.

[3] D.E. Flath. *Introduction to Number Theory.* Wiley, 1989.

[4] M. Jacobson and H. Williams. *Solving the Pell Equation, CMS Books in Mathematics.* Springer, 2010.

[5] R.A. Mollin. *Fundamental Number Theory with Applications.* Second Edition (Discrete Mathematics and Its Applications) Chapman & Hall/ CRC, Boca Raton, London, New York, 2008.

Düzce University

email: arzuozkoc@duzce.edu.tr

Factorization of places in coverings of algebraic curves

Özgür Deniz Polat

In this talk we consider the following question: Given a finite separable non-Galois extension F/K of a global field K, how a prime P of K decomposes in the field F.

We study the Galois extension L/K where L is the Galois closure of F/K. We obtain a one to one correspondence between the double coset space of G with respect to certain subgroups of G (depending on P and F) and the set of primes of F lying over P. Under this correspondence ramification indices and inertia degrees are explicitly determined.

Then we investigate the case where G is a finite group of Lie type defined over $\mathbb{F}_q$ and F is the intermediate field corresponding to a parabolic subgroup of G. Under these assumption we obtain that the number of primes of F lying over an unramified place with given residue degree can be obtained as polynomials in q This polynomials are determined by the length function on the certain subgroups of the Weyl group of G.

Sabanci University

email: polat@sabanciuniv.edu

Density Theorems for Rings of Krull type

Başak Ay Saylam

Let R be a commutative ring and $\mathcal{I}(R)$ denote the multiplicative group of all invertible fractional ideals of R, ordered by $A \leqslant B$ if and only if $B \subseteq A$. If R is a Marot ring of Krull type, then $R_{(P_i)}$, where $\{P_i\}_{i\in I}$ are a collection of prime regular ideals of R, is a valuation ring and that $R = \bigcap R_{(P_i)}$. We denote by G_i the value group of the valuation associated with $R_{(P_i)}$. We prove that there is an order homomorphism from $\mathcal{I}(R)$ into the cardinal direct sum $\coprod_{i\in I} G_i$ and investigate the conditions that make this monomorphism *onto* for R.

References

[1] Saylam Ay B., "On density theorems for rings of krull type with zero divisors", Turkish Journal of Mathematics, to appear.

[2] Brewer J, Klingler L. The Ordered Group of Invertible Ideals of a Prüfer Domain of Finite Character. Communications in Algebra 2005; 33: 4197-4203.

[3] Huckaba JA. Commutative rings with zero divisors. Marcel Dekker Inc. 1988.

Izmir Institute of Technology email: `basakay@iyte.edu.tr`

On minimal non-hypercentral groups

Azra Souad

Let X be a class of groups. A group is said to be minimal non-X if it is not an X-group, while all its proper subgroups belong to X. In this note we prove that a minimal non-hypercentral group a finitely generated is a perfect group which has no proper subgroup of finite index and such that $G/Frat(G)$ is an infinite simple group, where $Frat(G)$ stands for Frattini subgroup of G.

Mohamed El Bachir El Ibrahimi Bordj bou Arréridj University

email: `azrasou@yahoo.fr`

Arf Rings for Singularities

Nil Şahin

In this talk, we describe Arf rings and closures, and Arf's method to compute the Arf closures. Introducing an easily implementable new algo- rithm for computing the Arf closure of an irreducible algebroid curve, we will read the multiplicity sequences of branches from their Arf closures. Moreover, we will talk about a conjecture by Arslan and Sertöz about the relation be- tween the branches with the same regularity indices and give some examples supporting the conjecture that is computed with the new Arf closure algorithm.

Bilkent University

email: `nilsahin@bilkent.edu.tr`

Generalized Multipliers, Weil numbers and Circulant Weighing Matrices

Ming Ming Tan

The study of some combinatorial objects such as relative difference sets and integer weighing matrices is equivalent to the investigation of a certain identity in suitable group rings. For this reason, the interplay of algebra and combinatorics becomes very important. One such powerful algebraic approach is the concept of multipliers.

Definition. Let G be an abelian group of order v and $D \in \mathbb{Z}[G]$. An integer t with $\gcd(t, v) = 1$ is called a **multiplier** of D if

$$D^{(t)} = Dg$$

for some $g \in G$.

Arasu and Ma [1] extended the concept of multipliers to cyclotomic group ring $\mathbb{Z}[\zeta][G]$ where ζ is a suitable complex root of unity. One such application is on circulant weighing matrices.

A **circulant weighing matrix** $CW(v, n)$ is a square matrix of order v of the form

$$M = \begin{pmatrix} a_1 & a_2 & \dots & a_v \\ a_v & a_1 & \dots & a_{v-1} \\ \dots & \dots & \dots & \dots \\ a_2 & a_3 & \dots & a_1 \end{pmatrix}$$

where $a_i \in \{0, \pm 1\}$ and $MM^T = nI$, n is a positive integer and I is the identity matrix. We use the generalized multipliers to derive some non-existence results on infinite families of circulant weighing matrices. In particular, we settled 6 open cases in the Strassler's table [2]. In addition, using other approaches including field descent and weil numberes, we further solved 10 more open cases.

The generalized multiplier concept derived by Arasu and Ma cover only cyclic groups. We generalize the result to abelian groups and give a simpler proof. Such generalization will be useful in studying the structure of many combinatorial objects over general abelian groups, e.g. integer weighing matrices. The potential of further applications of the generalized multipliers on other combinatoric objects will be of interest for discussion.

References

[1] K. T. Arasu, S. L. Ma: Nonexistence of $CW(110, 100)$. Des. Codes Cryptogr. **62** (2012), 273–278.

[2] Y. Strassler: *The Classification of Circulant Weighing Matrices of Weight* 9. Ph.D. Thesis. Bar-Ilan University, Israel 1997.

Nanyang Technological University, Singapore

email: mmtan1@e.ntu.edu.sg

web: http://www3.ntu.edu.sg/home2010/mmtan1/

Tower Tableaux

Müge Taşkın

It is well known that any permutation ω in the symmetric group S_n can be represented as the product of some finite adjacent transpositions $s_i = (i, i+1)$, where the index i runs from 1 to $n-1$. Among all such representations the ones which uses the minimum number of generators are called reduced representations for ω. The notion of reduced words has been catching high attention, because of their appearances in many areas of mathematics. See for examples [1, 2, 3, 4, 5, 6, 7].

We introduce a new combinatorial object called *tower diagrams* and introduce an algorithm that allows one to slide words on $\mathbb{Z}^+$ to these objects. Using this *sliding algorithm*, we construct a bijection between tower diagrams and finite permutations and show that this bijection specializes to a bijection between standard labelings of a given tower diagram and reduced expressions of the corresponding permutation. We also demonstrate how these works interferes with the studies on Schubert polynomials.

This is a joint work with Olcay Coşkun.

References

[1] S. Billey, W. Jockusch, R.P. Stanley, *Some combinatorial properties of Schubert polynomials*, J. of Algebraic Combinatorics **2** (1993), 345 -374.

[2] P. Edelman, C. Greene, *Balanced Tableaux*, Advances in Math. **63** (1987), 42 - 99.

[3] S. Fomin, C. Greene, V. Reiner, M. Shimozono, *Balanced Labelings and Schubert Polynomials*, European J. Combin. **18** (1997), no. 4, 373 - 389.

[4] S. Fomin, A.N. Kirillov, *Reduced words and plane partitions*, J. Algebraic Combin. **6** (1997), no. 4, 311 - 319.

[5] V. Reiner, M. Shimozono, *Plactification*, J. of Algebraic Combinatorics **4** (1995), 331 - 351.

[6] R.P. Stanley, *On the Number of Reduced Decompositions of Elements of Coxeter Groups*, Europ. J. Combinatorics **5** (1984), 359 - 372.

[7] R. Winkel, *A combinatorial bijection between standard Young tableaux and reduced words of Grassmannian permutations*, Seminaire Lotharingien et Combinatoire, **B36h** (1996), 24pp.

Boğaziçi Üniversitesi

email: muge.taskin@boun.edu.tr

The small index property for relatively free algebras

Vladimir Tolstykh

Apart from countable structures, there is no standard definition for the small index property for structures of *arbitrary* infinite cardinality.

Based on the results from the paper [1] by Dixon, Neumann and Thomas, we suggest the following definition for the small index property for *relatively free algebras.*

Definition. Let F be an infinitely generated relatively free algebra. We say that F has the *small index property* if every subgroup Σ of the automorphism group $\Gamma = \mathrm{Aut}(F)$ of index at most $\mathrm{rank}(F)$ contains the pointwise stabilizer $\Gamma_{(U)}$ of a subset U of F of cardinality less than $\mathrm{rank}(F)$.

In our talk we shall discuss some properties of relatively free algebras with the small index property and outline the proofs of the following results.

Proposition 8. *Let N be an infinitely generated free nilpotent group. Then N has the small index property.*

Proposition 1 can be used to prove that

Proposition 9. *All automorphisms of the group* $\mathrm{Aut}(A)$, *where A is an infinitely generated free abelian group, are inner.*

Note that the automorphism groups of infinitely generated free nilpotent groups of class $\geqslant 2$ are *complete* [2].

References

[1] J. Dixon, P. M. Neumann, S. Thomas, Subgroups of small index in infinite symmetric groups, *Bull. London Math. Soc.*, 18 (1986) 580–586.

[2] V. Tolstykh, Infinitely generated free nilpotent groups: completeness of the automorphism groups, *Math. Proc. Camb. Phil. Soc.*, 147 (2009), 541–566.

Istanbul Arel University

email: vladimirtolstykh@arel.edu.tr

On the Spectral Determination of Some Special Graphs

Hatice Topçu

There are some kind of matrices which belongs to the graphs, such as Degree matrix, Adjacency matrix, Laplacian matrix, Signless Laplacian matrix, etc. According to any graph matrix M, when two graphs have the same M-spectrum, they are called M-cospectral. Hence, for a given graph G, if all of the M-cospectral graphs with G are isomorphic to G, then G is called determined by its M-spectrum and it is denoted by DMS. Since the paper "Which graphs are determined by their spectrum?" has published, researchers have great attention to find the answer of this question. Here, we will talk about some special kinds of graphs which are determined by their spectrum. Then, we will present our work on some special graphs whether they are DMS or non-DMS. Additionally, we will give some open problems about this topic.

This talk is based on joint work with my supervisor Sezer Sorgun.

References

[1] W.H. Haemers , E.R. van Dam, Developments on spectral characterizations of graphs, Discrete Math., 309 (2009) 576-586.

[2] W.H. Haemers, X.G. Liu,Y.P. Zhang, Spectral characterizations of lollipop graphs, Linear Algebra Appl. 428 (2008) 2415-2423.

[3] X. Zhang, H. Zhang, Some graphs determined by their spectra, Linear Algebra Appl. 431 (2009) 1443-1454.

[4] E.R. van Dam, W.H. Haemers, Which graphs are determined by their spectrum?, Linear Algebra Appl. 373 (2003) 241-272.

[5] D. Cvetkovic , P. Rowlinson, S. Simic, An Introduction to the Theory of Graph Spectra, Cambridge University Press, 2010.

[6] Y. Zhang, X. Liu, X. Yong, Which wheel graphs are determined by their laplacian spectra?, Comp. Math. And App. (2009) 1887-1890.

[7] F. Liu, Q. Huang, Laplacian spectral characterization of 3-rose graphs, Linear Algebra Appl. 439, Issue 10 (2013) 29142920.

Nevşehir Hacı Bektaş Veli University

email: haticekamittopcu@gmail.com,srgnrzs@gmail.com

Recursive Artin-Schreier Towers of Function Fields over $\mathbb{F}_2$

Seher Tutdere

Let $\mathbb{F}_q$ be a finite field ($q = p^k$ with p a prime and $k \geq 1$ an integer) and $F/\mathbb{F}_q$ be an algebraic function field of one variable with the field $\mathbb{F}_q$ as its full constant field. We denote by $B_r(F)$ and $g(F)$ the number of places of degree r for any positive integer r and the genus of $F/\mathbb{F}_q$, respectively. When $r = 1$, for all $k \geq 2$ and when $r \geq 2$, for all $k \geq 1$ there are many examples of recursive towers $\mathcal{F} = (F_n)_{n\geq 0}$ over $\mathbb{F}_q$ with positive limit $\beta_r(\mathcal{F}) = \lim_{n\to\infty} B_r(F_n)/g(F_n)$. However, it is not known whether there are any recursive towers over prime fields with positive β_1. We call a recursive tower $\mathcal{F} = (F_n)_{n\geq 0}$ an Artin-Schreier tower if each extension F_{n+1}/F_n (with $n \geq 0$) is an Artin-Schreier extension of degree p. In this talk we discuss all polynomials which define recursive Artin-Schreier towers over the field $\mathbb{F}_2$ and the limit β_r of those towers for all $r \geq 1$.

This is a joint work with Henning Stichtenoth who was partially supported by TÜBİTAK under the grant no: TBAG-111T234 and Seher Tutdere was partially supported by TÜBİTAK under the grant no: TBAG-112T011.

Gebze Institute of Technology, Gebze/Kocaeli, Turkey

email: stutdere@gmail.com

web: http://www.gyte.edu.tr/tr/personel/573/26219106/display.aspx

Brauer indecomposability of Scott modules of Park-type groups

İpek Tuvay

Let p be a prime number, G be a finite group, P be a p-subgroup of G, and k be an algebraically closed field of characteristic p. We prove that the kG-Scott module with vertex P is Brauer indecomposable for some families of groups closely related to groups constructed by Park in the context of fusion systems.

Gebze Institute of Technology

email: `ituvay@gyte.edu.tr`

Smaller Generators for Some Class Fields

Osmanbey Uzunkol

In this talk, it will be shown that smaller powers of certain quotients of the values of Siegel functions are primitive elements of ray class fields of imaginary quadratic number fields. These values yield smaller generators of such class fields, as in the case of class invariants for Hilbert class fields. Joint work with Ömer Kücüksakalli (METU).

Tübitak Bilgem

email: `osmanbey.uzunkol@uni-oldenburg.de`

A polynomial embedding of pairs of orthogonal partial latin squares

Emine Şule Yazıcı

Let N represent a set of n distinct elements. A non-empty subset P of $N \times N \times N$ is said to be a *partial latin square*, of order n, if for all $(x_1, x_2, x_3), (y_1, y_2, y_3) \in P$ and for all distinct $i, j, k \in \{1, 2, 3\}$,

$$x_i = y_i \text{ and } x_j = y_j \text{ implies } x_k = y_k.$$

If $|P| = n^2$, then we say that P is a *latin square*, of order n.

Two partial latin squares P and Q, of the same order are said to be *orthogonal* if they have the same non-empty cells and for all $r_1, c_1, r_2, c_2, x, y \in N$

$$\{(r_1, c_1, x), (r_2, c_2, x)\} \subseteq P \text{ implies } \{(r_1, c_1, y), (r_2, c_2, y)\} \not\subseteq Q.$$

In 1960 Evans proved that a partial latin square of order n can always be embedded in some latin square of order t for every $t \geq 2n$. In the same paper Evans raised the question as to whether a pair of finite partial latin squares which are orthogonal can be embedded in a pair of finite orthogonal latin squares. We show that a pair of orthogonal partial latin squares of order t can be embedded in a pair of orthogonal latin squares of order at most $16t^4$ and all orders greater than or equal to $48t^4$. This is the first polynomial embedding result of its kind.

email: `eyazici@ku.edu.tr`

web: `http://home.ku.edu.tr/~eyazici`

Posters

New classes of permutation polynomials over finite fields of odd characteristic

Sedat Akleylek, Zülfükar Saygı

We present some new classes of permutation polynomials over finite fields of odd characteristic. The classes are related to the form $(x^{p^k} - x + \delta)^s + L(x)$ where k, s are integers, $L(x)$ is a linearized polynomial in $\mathbb{F}_p[x]$ and $\delta \in \mathbb{F}_p \setminus \{0\}$. The focus is given to finding suitable s. A complete permutation polynomial family is also studied for some cases.

Ondokuz Mayıs University and Middle East Technical University
TOBB University of Economics and Technology
email: sedat.akleylek@bil.omu.edu.tr,zsaygi@etu.edu.tr

Conjugacy classes of extended generalized Hecke groups

Bilal Demir

This is a joint work with zden Koruolu and Recep ahin from Balkesir University. Lehner studied more general class $H_{p,q}$ of Hecke groups $H_{2,q} = H_q$, by taking

$$X = \frac{-1}{z - \lambda_p} \text{ and } V = z + \lambda_p + \lambda_q,$$

where $2 \leq p \leq q$, $p + q > 4$. Here if we take $Y = XV = -\frac{1}{z+\lambda_q}$, then we have the presentation,

$$H_{p,q} =< X, Y : X^p = Y^q = I >\simeq C_p * C_q.$$

We call these groups as *generalized Hecke groups* $H_{p,q}$. All Hecke groups H_q are included in generalized Hecke groups $H_{p,q}$.

Now we define extended generalized Hecke groups $\overline{H}_{p,q}$, by adding the reflection $R(z) = 1/\overline{z}$ to the generators of generalized Hecke groups $H_{p,q}$. Then, extended generalized Hecke groups $\overline{H}_{p,q}$ have a presentation

$$\overline{H}_{p,q} =< X, Y, R : X^p = Y^q = R^2 = I,\ RX = X^{-1}R, RY = Y^{-1}R > .$$

In this study, we determine the conjugacy classes of the torsion elements in extended generalized Hecke groups $\overline{H}_{p,q}$. The conjugacy classes of extended modular group have been studied by Jones and Pinto in [3]. The non-elliptic conjugacy classes of Hecke Groups H_q have been studied by Hoang and Ressler in [4]. Also, the conjugacy classes of the torsion elements in Hecke H_q and extended Hecke groups $\overline{H}_q$ have been found by Yılmaz Ozgur and Sahin in [5]. Here, we generalize the results given in [5] to extended generalized Hecke groups $\overline{H}_{p,q}$ by similar methods.

References

[1] Hecke E. Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung, Math. Ann. 1936; 112: 664-699.

[2] Lehner J. Uniqueness of a class of Fuchsian groups, Illinois J. Math. 1975; 19: 308–315.

[3] Jones GA and Pinto D. Hypermap Operations of Finite Order, Discrete Math. 2010; 310, No.12: 1820-1827.

[4] Hoang G and Ressler W. Conjugacy Classes and Binary Quadratic Forms for the Hecke Groups, Canad. Math. Bull. 2013; 56, no. 3: 570–583.

[5] Yilmaz Ozgür N and Sahin R. On the Extended Hecke Groups $\overline{H}(\lambda_q)$, Turk J. Math. 2003; 27:473-480.

[6] Demir B, Koruoğlu Ö and Şahin R, Conjugacy Classes of Extended Generalized Hecke Groups, submitted for publication

On The Hamilton-Waterloo Problem

Uğur Odabaşı

A $2-factor$ in a graph G is a $2-$regular spanning subgraph of G, and a $2-factorization$ of graph G is a decomposition of all the edges of G into edge-disjoint $2-$factors. $The\ Hamilton-Waterloo\ problem$ is a generalization of the well known $Oberwolfach\ problem$ and asks for a $2-$factorization of K_{2v+1} in which r of the $2-$factors are isomorphic to a given $2-$factor R and s of the $2-$factors are isomorphic to a given $2-$factor S, with $r+s=v$. The $2-$factorization is called $uniform$ when R consists of cycles of length m and S consists of cycles of length n. The family of such $2-$factorizations for all possible r and s is denoted by $(m,n)-HWP(2v+1;r,s)$. There exists no $2-$factorization of K_{2n} since the degree of each vertex is odd. In this case, the $2-$factorization of $K_{2v}-I$ where I is a $1-$factor of K_{2v} is considered and such a factorization also denoted by $(m,n)-HWP(2v;r,s)$.

In this study, some early results and basic constructions on this problem are considered and some new results are discussed.

References

[1] C. J. Colbourn and J. H. Dinitz (Editors), The CRC Handbook of Combinatorial Designs, 2nd edn, CRC Press Series on Discrete Mathematics, CRC Press, Boca Raton, 2007;

[2] J. H. Dinitz and A. C. H. Ling, The Hamilton-Waterloo problem with triangle-factors and Hamilton cycles: the case $n \equiv 3(mod18)$, J Combin Math Combin Comput 70 (2009), 143147;

[3] Melissa S. Keranen, Sibel zkan, The Hamilton-Waterloo Problem with 4-Cycles and a Single Factor of n-Cycles, Graphs and Combinatorics November 2013, Volume 29, Issue 6, pp $1827-1837$;

[4] J. H. Dinitz and A. C. H. Ling, The Hamilton-Waterloo problem: the case of triangle-factors and a Hamilton cyle, J Combin Des 17 (2009), 160-176;

[5] D. Bryant and C. Rodger, Cycle Decompositions, In: C. J. Colbourn and J. H. Dinitz editors, Handbook of combinatorial designs, Second Edition, Chapman and Hall/CRC, Boca Raton, FL, 2007, pp. 373-382;

[6] P. Horak, R. Nedela, and A. Rosa, The Hamilton-Waterloo problem: the case of Hamilton cycles and triangle-factors, Discrete Math 284 (2004), 181188;

[7] P. Adams, E. J. Billington, D. E. Bryant, and S. I. El-Zanati, On the Hamilton-Waterloo problem, Graphs Combin 18 (2002), 3151.

Gebze Institute of Technology

Modular Multiplication Algorithms For Finite Field Multiplication in $\mathbb{F}_p$

Ahmet Sınak, Murat Cenk

Finite field arithmetic plays an important role in applications such as coding theory and cryptography. Since some encryption and signing algorithms such as RSA, DSA, ECC in public key cryptosystems require modular multiplications, the efficiency of modular multiplication for long integers is a significant part of the implementation of these algorithms. The implementation of modular multiplication has to be accelerated in order to obtain practical cryptosystems. Modular multiplication includes both multiplication of integers and reduction of the product modulo an integer. In order for a cryptographic system to be practical, one should use efficient algorithms for both steps. In literature, many efficient modular multiplication algorithms have been constructed for this purpose [2, 3, 4, 5]. The most popular algorithms are *Karatsuba multiplication, Montgomery multiplication, Barrett reduction, Toom-Cook multiplication and Fourier transform.* The performance of these algorithms vary depending on the implementation platform and the structure of prime p. In this work, we survey the existing multiplication algorithms from the aspect of computational complexity. Moreover, we show that better results can be obtained by using combination of the algorithms mentioned above. To this end, we use recursive designing techniques and search the best possible algorithm in each recursion level that yields improved complexities.

References

[1] Aranha, D.F., Fuentes-Castaeda, L., Knapp, E., Menezes, A., Rodrguez-Henrquez, F. Implementing pairings at the 192-bit security level, 7708 LNCS, pp. 177-195, Springer- Verlag, 2013.

[2] Bluemel, R., Laue, R. and Huss, Sorin A. A highly efcient modular Multiplication Algorithm for Finite Field Arithmetic in GF(P). In Proceedings of ECRYPT Workshop, Cryptographic Advances in Secure Hardware, 2005.

[3] Hankerson, D., Menezes, A., and Vanstone, S. Guide to elliptic curve cryptography. Springer Professional Computing. Springer-Verlag, New York, 2004.

[4] Koc, C. Kaya, Acar, T. and J. Kaliski, B.S., Analyzing and comparing Montgomery multiplication algorithms, IEEE Micro, vol. 16, no. 3, pp.26 33, jun 1996.

[5] Montgomery, Peter L. Modular Multiplication Without Trial Division. Mathematics of Computation 4A, 170 (April 1985), 519-521. Available at http://www.ams.org/journals/mcom/1985-44-170/S0025-5718-1985-0777282 X/S0025-5718-1985-0777282-X.pdf

Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

email: sahmet@metu.edu.tr,mcenk@metu.edu.tr

Neat and P-Pure Proper Classes

Zübeyir TÜRKOĞLU

Let R be a ring with unity. A short exact sequence $\mathbb{E}$ of left R-modules is said to be neat-exact if every simple left R-module is projective with respect to it. We call it $\mathcal{P}$-pure-exact if for every left primitive ideal P of R, the sequence obtained by taking the tensor product of $\mathbb{E}$ from the left by R/P is exact. These give proper classes of short exact sequences of left R-modules. The characterization of N-domains, that is, the commutative domains such that neatness and $\mathcal{P}$-purity coincide, has been given recently by László Fuchs: they are the commutative domains where every maximal ideal is projective (and so necessarily finitely generated in the commutative domain case). We extend this sufficient condition to commutative rings using the Auslander-Bridger tranpose of simple R-modules, that is, we prove that if R is a commutative ring where every maximal ideal is projective and finitely generated, then neatness and $\mathcal{P}$-purity coincide. Conversely, we show that the necessary condition holds for commutative rings with zero socle, that is, we show that if R is a commutative ring where neatness and $\mathcal{P}$-purity coincide and if R has zero socle, then every maximal ideal of the ring R is projective and finitely generated.

References

[1] Fuchs, L. (2012). Neat submodules over integral domains. *Periodica Mathematica Hungarica*, *64*(2), 131–143.

DOKUZ EYLÜL UNIVERSITY

email: zubeyirturkoglu@hotmail.com