XII. Antalya Cebir Günleri

19–22 Mayıs 2009

Contents

It is a pleasure to welcome you to Antalya Algebra Days XII.

Having begun as an informal meeting of approximately 40 mathematicians in 1999, Antalya Algebra Days have evolved into meetings that most algebraists and number theorists in Turkey look forward to each year.

For those of us who have been involved in organization since the beginning, this year's meeting is a sad occasion. We lost one of the founders, and a great friend, Professor Cemal Koç. He passed away on 1 April 2010. We remember him very dearly.

One of the main aims of AAD has been to provide a platform for enabling and strengthening national as well as international collaboration in various topics in algebra. The participation of guests from abroad greatly helps in realizing this goal. We deeply thank them for their contribution.

All of the organizers of this meeting have put in a lot of effort, but Ayşe, David, and Henning join me in expressing our gratitude to Cem for his dedication and extremely hard work.

Special thanks go to Tamer Koç and Şükran Demir of Tivrona Tours who have been able to meet our endless wishes.

TÜBİTAK (the Scientific and Technological Research Council of Turkey), Sabancı University, and the Turkish Mathematical Society have provided financial support; Middle Eastern Technical University hosts the website. We thank them all.

We hope that you will have a wonderful time here.

Alev Topuzoğlu
For the Organizers of AAD XII

Invited talks

Towers of algebraic function fields and their applications

Alp Bassa

In this talk I will introduce towers of algebraic functions fields and outline some of their applications. I will discuss some of the questions about towers, which emerge naturally from these applications.

Centrum Wiskunde & Informatica, Amsterdam
Alp.Bassa@cwi.nl

Pseudofinite groups and groups of finite Morley rank: proof of concept

Alexandre Borovik

The talk will discuss recent progress in a joint project with Pınar Uğurlu and Şükrü Yalçınkaya.

Our project looks at relations between two major conjectures in the theory of groups of finite Morley rank, a modern chapter of model theoretic algebra. One conjecture, the famous the Cherlin-Zilber Algebraicity Conjecture formulated in 1970-s states that infinite simple groups of finite Morley rank are isomorphic to simple algebraic groups over algebraically closed fields. The other conjecture, due to Hrushovski and more recent, states that a generic automorphism of a simple group of finite Morley rank has pseudofinite group of fixed points. Hrushovski showed that the Cherlin-Zilber Conjecture implies his conjecture. Proving Hrushovski's Conjecture and reversing the implication would provide a new efficient approach to proof of Cherlin-Zilber Conjecture.

Meanwhile, the machinery already developed for work at the pseudofinite/finite Morley rank interface yields an interesting and powerful result: an alternative proof of the Larsen-Pink Theorem (the latter says, roughly speaking, that "large" finite simple groups of matrices are Chevalley groups over finite fields):

Theorem (Larsen and Pink [1]). *For any finite simple group G possessing a faithful linear or projective representation of dimension n over a field k we have either*
(a) $|G|$ is bounded by a function which depends only on n, or
(b) $p := \mathrm{char}\,(k)$ is positive and G is a group of Lie type in characteristic p.

This alternative proof is based on ideas from the classification theory of groups of finite Morley rank; it *does not* use the classification of finite simple groups and can be seen as "proof of concept" for our research programme.

References

[1] M.J. Larsen and R. Pink. Finite subgroups of algebraic groups. Preprint, 1998. Available at http://mlarsen.math.indiana.edu/~larsen/papers/LP5.pdf.

University of Manchester
borovik@manchester.ac.uk
http://www.maths.manchester.ac.uk/~avb/

Permutations with small differential uniformity

Pascale Charpin

Differential cryptanalysis is the first statistical attack proposed for breaking iterated block ciphers. Its presentation then gave rise to numerous works which investigate the security offered by different types of functions with respect to differential attacks. This security is quantified by the so-called differential uniformity of the Substitution box used in the cipher. The study of algebraic properties of functions over finite fields (most important are the finite fields of order 2), replaced in this context, is a major topic for the last fifteen years. Although the purpose is to obtain new efficient designs for block ciphers, the theoretical aspects of this research are of great interest.

Monomial permutations, form a class of suitable candidates since they usually have a lower implementation cost in hardware. Moreover, their properties regarding differential attacks can be studied more easily since they are related to the weight enumerators of some cyclic codes with two zeroes. However, using power permutations which are optimal for differential cryptanalysis might not be suitable in a cryptographic context: Such permutations on $\mathbb{F}_{2^n}$ are generally not known for even n and optimal functions usually correspond to extremal objects, which possess very strong algebraic structures.

For all these reasons, it is important to find some permutations which have an almost optimal low differential uniformity, and a sparse polynomial expression. Also, other properties appear as necessary, because of the active research on other statistical attacks.

In this context, we first investigate the differential properties, namely the whole differential spectrum, of power permutations which have a low differential uniformity. Further, we present recent results on polynomials in $\mathbb{F}_{2^n}[X]$ of the shape

$$G(X) + \lambda Tr(H(X)), \qquad G(X), H(X) \in F_{2^n}[X], \qquad \lambda \in \mathbb{F}_{2^n}.$$

We notably identify such permutations when G and H are monomials.

INRIA, B.P. 105, 78153 Le Chesnay Cedex, France
Pascale.Charpin@inria.fr
http://www-rocq.inria.fr/secret/Pascale.Charpin/index.html

Definability versus definability-up-to-isomorphism, in groups and fields

Wilfrid Hodges

Many algebraic constructions F, where $F(A)$ is a structure built on the structure A, are defined up to isomorphism over A. (A typical example is algebraic closure, where $F(A)$ is the algebraic closure of a field A.) Suppose we ask whether such a construction F can be defined outright and not just up to isomorphism. In general the answer calls on some interactions of cohomology and set theory. The talk will survey examples from groups and fields, and will mention recent joint work with Saharon Shelah.

Herons Brook, Sticklepath, Okehampton EX20 2PY, England
wilfrid.hodges@btinternet.com
http://wilfridhodges.co.uk

The structure of valued function fields in positive characteristic: known results and open problems

Franz-Viktor Kuhlmann

The structure theory of valued function fields has important applications in many areas, two of the most prominent being local uniformization (i.e., local resolution of singularities) and the model theory of valued fields. In positive characteristic, these two areas offer deep open problems: neither resolution of singularities nor local uniformization have been proved, and the question whether Laurent series fields over finite fields have a decidable theory has not been answered. I will show how these problems are connected with the structure theory of valued function fields and its open problems. One of these problems is the elimination of ramification, a necessary but not sufficient step towards local uniformization. In positive characteristic, one phenomenon we have to struggle with is the defect of valued field extensions (which is connected with wild ramification). I will present two main theorems that deal with the defect in valued function fields, and their application to local uniformization and the model theory of so-called tame valued fields.

Using a purely valuation-theoretical proof, I have shown that local uniformization is always possible after a separable extension of the function field of the algebraic variety (separable "alteration"). Local uniformization by alteration also follows from de Jong's resolution by alteration, but our result gives more detailed information on the extension of the function field. Recently, Michael Temkin has proved local uniformization by purely inseparable alteration. However, a classification of Artin-Schreier extensions with non-trivial defect shows that separable alteration and purely inseparable alteration are just two ways to eliminate particularly malicious defects. So the existence of these two seemingly "orthogonal" local uniformization results does not necessarily indicate that local uniformization without alteration is possible.

The structure theory of valued function fields in positive characteristic and the theory of the defect offer many deep and exciting questions, with applications to important open problems. My goal is to attract more young mathematicians to this particular area of research.

References

[1] Knaf, H., Kuhlmann, F.-V.: Abhyankar places admit local uniformization in any characteristic. Ann. Scient. Ec. Norm. Sup., **38**, 833–846 (2005)

[2] Knaf, H., Kuhlmann, F.-V.: Every place admits local uniformization in a finite extension of the function field. Adv. Math., **221**, 428–453 (2009)

[3] Kuhlmann, F.-V.: Valuation theoretic and model theoretic aspects of local uniformization. In: Resolution of Singularities — A Research Textbook in Tribute to Oscar Zariski. H. Hauser, J. Lipman, F. Oort, A. Quiros (eds.), Progress in Mathematics, Vol. **181**, Birkhäuser Verlag Basel, 381–456 (2000)

[4] Kuhlmann, F.-V.: Elimination of Ramification I: The Generalized Stability Theorem. To appear in: Trans. Amer. Math. Soc. arXiv:[1003.5678]

[5] Kuhlmann, F.-V.: A classification of Artin-Schreier defect extensions and a characterization of defectless fields. To appear. arXiv:[1003.5639]

[6] Kuhlmann, F.-V.: The defect. To appear. arXiv:[1004.2135]

[7] Temkin, M.: Inseparable local uniformization. Preprint, arXiv:[0804.1554]

Department of Mathematics and Statistics, University of Saskatchewan, 106 Wiggins Road, Saskatoon, Saskatchewan, Canada S7N 5E6

fvk@math.usask.ca

http://math.usask.ca/~fvk

Universal groups

Mahmut Kuzucuoğlu

A group is called a **locally finite group** if every finitely generated subgroup is a finite group. A locally finite group U is called **universal** if

(a) every finite group can be embedded into U,

(b) any two isomorphic finite subgroups of U are conjugate in U.

Existence and basic properties of countable universal locally finite groups are given by P. Hall in [2] see also in [3]. For any given uncountable cardinality κ, existence of 2^{κ} non-isomorphic universal locally finite groups of cardinality κ is given by S. Shelah and A. J. Macintyre in [5].

We are interested in centralizers of finite subgroups in simple non-linear locally finite groups. In particular the following question. Is the centralizer of every finite subgroup in a non-linear locally finite simple group infinite ? We answer this question for direct limit of finite alternating groups. Particular case gives an answer to the centralizers of finite subgroups in universal groups.

Theorem 1. *(Ersoy-Kuzucuoğlu) Let G be a simple locally finite group which is a direct limit of finite alternating groups, and F be a finite subgroup of G. Then $C_G(F)$ contains an abelian subgroup A which is isomorphic to $\operatorname{Dr}_{p\ prime} \mathbb{Z}_p$.*

We also mention universal groups that are not necessarily locally finite groups constructed by O. H. Kegel in [4]. We will discuss basic properties of this regular limit group S_λ of symmetric groups. We also discuss the following result.

Lemma 2. *(O. H. Kegel, M. Kuzucuoğlu) Let B be a bounded subgroup of a regular limit group S_λ with trivial center. Then $C_{S_\lambda}(B)$ is isomorphic to S_λ.*

References

[1] Ersoy, K; Kuzucuoğlu M. Centralizers of subgroups in simple locally finite groups, Submitted.

[2] Hall, P. Some constructions for locally finite groups, J. London Math. Soc. **34** (1959) 305–319.

[3] Kegel, O. H., Wehrfritz, B. (1973) *Locally Finite Groups*, North-Holland Publishing Company.

[4] Kegel, O. H. Regular limits of infinite symmetric groups, Ischia Group Theory 2008, World Scientific

[5] Macintyre, A.J. and Shelah, S. Uncountable Universal Locally Finite Groups, J. Algebra 43(1976) 168-175.

Middle East Technical University, Department of Mathematics, 06531 Ankara, TURKEY

matmah@metu.edu.tr

metu.edu.tr/~matmah

Computing class numbers via elliptic units

Ömer Küçüksakallı

The class number is a powerful invariant in algebraic number theory which can be used to investigate the integer solutions of polynomials, such as Fermat's Equation. It can be computed for extensions with small degree and discriminant, however computations take a very long time for higher extensions. In this talk, we will describe a heuristic method to compute the class numbers of some abelian extensions of imaginary quadratic fields. This is the elliptic analogue of an algorithm of Schoof used for cyclotomic fields. We will use elliptic units analytically constructed by Stark and the Galois action on them given by Shimura's reciprocity. In the end we will give a counter-example to Vandiver's conjecture in the elliptic curve case.

References

[1] *Class numbers of ray class fields of imaginary quadratic fields.* To appear in Mathematics of Computation.

Middle East Technical University, Department of Mathematics, 06531 Ankara Turkey
komer@metu.edu.tr
www.metu.edu.tr/~komer/

The Bloch–Kato theorem and Hodge type conjectures

James D. Lewis

The Bloch–Kato conjecture was recently proven by V. Voevodsky and his collaborators. It is a generalization of the Merkurjev–Suslin theorem and the Milnor conjecture [theorem]. This conjecture [theorem] turns out to be under the same general umbrella as the Hodge conjecture and its generalizations (due to Beilinson). We will explain the Bloch–Kato theorem and its connection to the Hodge type conjectures.

University of Alberta
lewisjd@gpu.srv.ualberta.ca
http://www.math.ualberta.ca/Lewis_JD.html

Injective hulls of simple modules over down-up algebras

Christian Lomp

The module theoretical properties of indecomposable injective modules over a Noetherian ring R are important for the structure theory of R. For a commutative Noetherian ring R, Eben Matlis showed in [1] that any injective hull of a simple R-module is Artinian, a property that, in general does not hold for non-commutative rings. However Randall Dahlberg showed in [2] that injective hulls of simple modules over $U(\mathfrak{sl}_2)$ are locally Artinian. The enveloping algebra $U(\mathfrak{sl}_2)$ is an instance of a larger class of Noetherian domains, the Down-Up algebras, introduced by Georgia Benkart and Tom Roby in [3]. The Down-Up algebras $A(\alpha, \beta, \gamma)$ form a three parameter family of associative algebras. For any parameter set $(\alpha, \beta, \gamma) \in \mathbb{C}^3$ one defines a $\mathbb{C}$-algebra, denoted by $A(\alpha, \beta, \gamma)$, generated by two elements u and d subject to the relations

$$d^2u = \alpha dud + \beta ud^2 + \gamma d$$
$$du^2 = \alpha udu + \beta u^2 d + \gamma u$$

which is a Noetherian domain if and only if $\beta \neq 0$. In particular $A(2, 1, 1) = U(\mathfrak{sl}_2)$ holds.

During the *X. Antalya Algebra Days*, *Patrick Smith* asked in a private conversation with Paula Carvalho, which Noetherian Down-Up algebras satisfy the condition that their injective hulls of simple modules are locally Artinian.

I will present the findings on Patrick's question from our joint work [4] with *Paula Carvalho and Dilek Pusat-Yilmaz*, namely that a Noetherian Down-Up algebra $A(\alpha, \beta, \gamma)$ has the desired property if the roots of the polynomial $X^2 - \alpha X - \beta$ are distinct roots of unity or both equal to 1. If time permits I will also report on the progress made by Paula Carvalho and Ian Musson in [5].

References

[1] Matlis, E., *Modules With Descending Chain Condition*, Trans. Amer. Math. Soc. 97(3), 495-508 (1960)

[2] Dahlberg, R.L., *Injective Hulls of Simple sl(2, C) Modules are Locally Artinian*, Proc. Amer. Math. Soc. 107(1), 35-37 (1989)

[3] Benkart, G. and Roby, T., *Down-up algebras.*, J. Algebra 209 (1998), no. 1, 305-344.

[4] Carvalho, P.A.A.B, Lomp C. and Pusat-Yilmaz, D., *Injective Modules over Down-Up Algebras*, to appear in Glasgow Math. J.

[5] Carvalho, P.A.A.B and Musson, I., *Monolithic modules over Noetherian Rings*, arXiv:1001.1466

University of Porto

clomp@fc.up.pt

www.fc.up.pt/mp/clomp

Introduction to APN functions and related topics

Gary McGuire

In this talk we will introduce PN (perfect nonlinear) and APN (almost perfect nonlinear) functions. Without assuming any previous knowledge, we present and discuss the definitions, applications, and connections to areas like coding theory and cryptography. We will also discuss the Fourier transforms of such functions.

University College Dublin
gmg2010@gmail.com
http://mathsci.ucd.ie/~gmg/

Quadratic forms of codimension 2 over finite fields containing $\mathbb{F}_4$ and Artin-Schreier type curves

Ferruh Özbudak

Let $\mathbb{F}_q$ be a finite field containing $\mathbb{F}_4$. Let $k \geqslant 2$ be an integer. We give a full classification of quadratic forms over $\mathbb{F}_{q^k}$ of codimension 2 provided that certain three coefficients are from $\mathbb{F}_4$. As an application of this we obtain new results on the classification of maximal and minimal curves over $\mathbb{F}_{q^k}$. We also give some nonexistence results on certain systems of equations over $\mathbb{F}_{q^k}$.

This is a joint work with Elif Saygı and Zülfükar Saygı.

Middle East Technical University
ozbudak@metu.edu.tr

Normal bases in finite fields

Daniel Panario

This talk surveys normal bases and normal elements in finite fields. These concepts were defined, and their existence proved, 150 years ago. However, due to their many recent applications, they have been vastly studied in the last 20 years.

Let q be a prime power. An element α in a finite field $\mathbb{F}_{q^n}$ is called *normal* if $N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this case, the basis N is called a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

First we briefly give an account of basic properties and results of normal elements including existence and number of normal elements.

Then we focus on how to operate with normal basis. As Hensel noted, in a normal basis qth powers are for free. This can be exploited to have fast exponentiation algorithms. As a consequence, normal elements are important in cryptographic applications where exponentiation and discrete logarithm computations are employed.

Next we discuss how to find normal elements. It turns out that not all normal elements behave in the same way, the so called *optimal normal elements* being preferable for most computations with normal elements. These special elements are directly related to Gauss periods in finite fields and have been characterized by Gao and Lenstra. Unfortunately, optimal normal elements only exists for some extension fields. This makes the study of *low complexity* normal elements relevant. We comment on several old and new results to produce low complexity normal elements. We conclude giving some open problems.

Carleton University, Canada

daniel@math.carleton.ca

http://www.math.carleton.ca/~daniel/

APN and PN functions: Differences and Similarities

Alexander Pott

Motivated by cryptography, one is interested in functions

$$f : \mathbb{F}_p^n \to \mathbb{F}_p^n$$

such that the equations (given $a \neq 0$ and b)

$$f(x+a) - f(x) = b$$

have only a few solutions $\delta(a,b)$. More precisely, the maximum value of all the numbers $|\delta(a,b)|$ should be small. It is easy to see that the maximum is 2 if $p = 2$, and it is 1 if p is odd. In the case $p = 2$, functions which achieve this minimum are called **almost perfect nonlinear** (APN), in the case p odd **perfect nonlinear** (PN).

Both for the PN and the APN case, some (but not too many) examples are known: infinite families as well as sporadic examples. It seems that there are more APN functions known since the defining property for APN functions is less restrictive: Some of the $\delta(a,b)$ are 0, some are 2. In the PN case, all these numbers must be 1. Similarly, the absolute values of the Walsh coefficients in the APN case are not determined by the APN property, but they are determined in the PN case.

Another important difference seems to be the underlying algebraic structure: Quadratic PN functions (and all PN functions except those constructed by Coulter and Matthews are quadratic) give rise to a strong algebraic structure (semifields). Nothing comparable seems to be true for quadratic APN functions.

PN functions can be used to construct finite projective planes. APN functions also describe certain incidence structures, but these have, in general, less structure than projective planes.

However, there are also similarities between APN and PN functions: Some constructions, described in terms of polynomials in $\mathbb{F}_{p^n}$, work both for the PN and the APN case. Moreover, a switching construction which has been shown to be quite powerful in the APN case has the potential to be useful also in the PN case.

In my talk, I will discuss these similarities and differences between APN and PN functions. In particular, I will cover the following topics:

- Incidence structures defined by PN and APN functions.
- Automorphism groups of these incidence structures.
- Semifields and the equivalence of functions.
- The switching construction of PN and APN functions.

Otto-von-Guericke-University Magdeburg

alexander.pott@ovgu.de

http://fma2.math.uni-magdeburg.de/~pott/

News on the Arf invariant

Peter Roquette

The 10-Lira note of Turkish currency carries the portrait of the mathematician Cahit Arf, accompanied with a formula for the Arf invariant of a quadratic form. I shall explain the notion of Arf invariant and its place within the general theory of quadratic forms. The talk is relying not only on published papers but also on letters and other documents of Arf's time. Recently it has turned out that some of Arf's results have to be modified.

References

[1] Roquette, Peter and Lorenz, Falko: *On the Arf invariant in historical perspective.* Math. Semesterberichte 57 (2010) 73-102.

University of Heidelberg, Germany
roquette@uni-hd.de
roquette.uni-hd.de

Elliptic curves and Drinfeld modules

Hans-Georg Rück

This is an introductory talk to the theory of Drinfeld modules. We want to explain how Drinfeld modules can be defined analogously to elliptic curves, following the path from an analytic torus to an algebraic structure.

References

[1] David Goss: Basic Structures of Function Field Arithmetic, Springer, 1998.

[2] Hans-Georg Rück, Ulrich Tipp: Heegner points and L-series of automorphic cusp forms of Drinfeld type, Documenta Mathematica 5 (2000), 365-444.

Universität Kassel, Germany
rueck@mathematik.uni-kassel.de
http://www.mathematik.uni-kassel.de/~rueck

Efficiency of random matrices over finite fields

Amin Shokrollahi

A "random" $m \times n$ matrix over a field K is a matrix sampled from some probability distribution over the space of such matrices. In this talk, we will investigate properties of such matrices over finite fields using several interesting probability distributions. The final goal is to construct matrices that behave like uniform random matrices (where the probability distribution is uniform) as far as their rank properties are concerned, and at the same time allow for very fast algorithms for solving systems of linear equations. Such matrices are used in the design of state of the art codes which allow for recovery of data in the face of data erasures.

École Polytechnique Fédérale de Lausanne (EPFL) - ALGO
amin.shokrollahi@epfl.ch
http://algo.epfl.ch/

Homological properties and chain conditions

Patrick F. Smith

There are many results linking homological properties of rings and modules with other properties, in particular chain conditions. The famous Auslander-Buchsbaum-Serre Theorem is one such. We shall investigate some of these results starting with the Auslander-Buchsbaum-Serre Theorem and including the work of Cohn on free ideal rings and more generally hereditary rings. Cohn's work is related to a theorem of Schreier on free groups.

University of Glasgow
pfs@maths.gla.ac.uk

New construction of $\tilde{D}_5$-singularities

Meral Tosun

For a given pair of special elements in the Lie algebra $\mathfrak{sl}(2,\mathbb{C})+\mathfrak{sl}(2,\mathbb{C})$, we can define a slice whose intersection with the nilpotent subvariety is a $\tilde{D}_5$-singularity. Here by special element we mean an element in the Lie algebra which has semi-simple component and nilpotent component simultaneously. We also calculated the j-function of the exceptional curves in the minimal resolutions of $\tilde{D}_5$-singularities by using pairs of special elements. This is one of analogies of Grothendieck–Brieskorn theory.

This is joint work with K. Nakamoto.

Galatasaray University
mrltosun@gmail.com

Groups, representations and codes

Wolfgang Willems

Extremal self-dual doubly-even codes are for several reasons of particular interest. However only for small lengths n such codes have been contructed. The largest one has length $n = 136$. On the other hand, by a result of Zhang, we know that such codes might exist up to $n = 3928$. Thus there is a large gap between the bound and what we have constructed so far. In order to find larger examples 'symmetries' or in other words 'non-trivial automorphisms' may be helpful. In this spirit the talk deals with automorphisms of putative extremal self-dual doubly-even codes which induce a module structure of the ambient space. The known examples and what we can prove about the primes which do not occur in the order of the automorphism groups lead to interesting conjectures. On the way we classify all extremal doubly-even extended quadratic residue and quadratic double circulant codes. The results are joint work with Stefka Bouyuklieva (Veliko Tarnovo) and Anton Malevich (Magdeburg).

Otto-von-Guericke-Universität Magdeburg

willems@ovgu.de

http://fma2.math.uni-magdeburg.de/~willems/

Exponential sums and linear complexity of nonlinear pseudorandom number generators

Arne Winterhof

Let p be a prime, r a positive integer, $q = p^r$ and denote by $\mathbb{F}_q$ the finite field of q elements. Given a polynomial $f(X) \in \mathbb{F}_q[X]$ of degree $d \geqslant 2$, we define the *nonlinear pseudorandom number generator* (μ_n) by the recurrence relation

$$\mu_{n+1} = f(\mu_n), \qquad n = 0, 1, \ldots, \tag{$*$}$$

with $\mu_0 \in \mathbb{F}_q$ such that (μ_n) is purely periodic with period $T \leqslant q$.

Niederreiter and Shparlinski developed a method to study the exponential sums

$$S_{\mathbf{a},N}(f) = \sum_{n=0}^{N-1} \chi\left(\sum_{j=0}^{s-1} \alpha_j \mu_{n+j}\right), \quad 1 \leqslant N \leqslant T,$$

where χ is a nontrivial additive character of $\mathbb{F}_q$ and $\mathbf{a} = (\alpha_0, \ldots, \alpha_{s-1}) \in \mathbb{F}_q^s \setminus \mathbf{0}$, see also the survey [2]. In general this method leads only to a nontrivial bound if $d = q^{o(1)}$.

For a nonnegative integer we define its *p-weight* as

$$\sigma\left(\sum_{i=0}^{l} n_i p^i\right) = \sum_{i=0}^{l} n_i \quad \text{if } 0 \leqslant n_i < p.$$

For $0 \neq f(X) = \sum_{i=0}^{d} \gamma_i X^i \in \mathbb{F}_q[X]$ we define its *p-weight degree* as

$$\mathrm{w}(f) = \max\{\sigma(i) \ \mid \gamma_i \neq 0, \ 0 \leqslant i \leqslant d\}.$$

Therefore, $\mathrm{w}(f) \leqslant \deg(f)$. Under certain restrictions on $f(X)$ we proved in [1] a bound on $S_{\mathbf{a},N}(f)$ which is nontrivial if $\mathrm{w}(f)$ is small enough but the degree can be large.

We also use the p-weight to bound the *Nth linear complexity* of the sequence defined in $(*)$. The linear complexity is a measure for the unpredictability and thus suitability in cryptography.

References

[1] Alvar Ibeas and Arne Winterhof. Exponential sums and linear complexity of nonlinear pseudorandom number generators with polynomials of small p-weight degree. *Unif. Distrib. Theory*, to appear.

[2] Alev Topuzoğlu and Arne Winterhof. Pseudorandom sequences. In *Topics in geometry, coding theory and cryptography*, volume 6 of *Algebr. Appl.*, pages 135–166. Springer, Dordrecht, 2007.

Austrian Academy of Sciences (Linz)

arne.winterhof@oeaw.ac.at

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

Contributed Talks

Some progress on minimal non $\mathfrak{X}$-groups

Ahmet Arıkan

Let $\mathfrak{X}$ be a class of groups. A group G is called a minimal non $\mathfrak{X}$-group if every proper subgroup of G is an $\mathfrak{X}$-group but G itself is not.

We consider certain classes like "minimal non-solvable groups", "minimal non-Baer groups" and some others here, and give some recent results relevant to them.

Infinite perfect groups will be under consideration and the results will be displayed mostly in Fitting p-group case.

References

[1] Arıkan, A., *Characterizations of minimal non-solvable Fitting p-groups*. J. Group Theory 11, no. 1, 95-103 (2008).

[2] Arıkan, A., Sezer, S. and Smith, H., *Locally finite minimal non-solvable groups*, to appear in Central European Journal of Mathematics.

[3] Arıkan, A., Trabelsi N., *Perfect minimal non-Baer groups*, submitted.

[4] Asar, A. O., *Locally nilpotent p-groups whose proper subgroups are hypercentral or nilpotent-by-Chernikov*. J. London Math. Soc. (2) 61 (2000), no. 2, 412-422.

Gazi University

arikan@gazi.edu.tr

http://websitem.gazi.edu.tr/~arikan

Barely transitivity and hypercentrality in locally finite p-Groups

A. O. Asar

In this work it is shown that if there exists a perfect locally finite barely transitive p-group, then it has a finite subgroup whose centralizer has finite exponent. As an application of this result it follows that there does not exist a totally imprimitive p-subgroup of $FSym(\Omega)$ which is a minimal non-FC-group , where Ω is infinite. This result together with the earlier results answers the following question in the negative: Does there exist a perfect locally finite minimal non-FC-group? Of course an imperfect locally finite minimal non-FC-group exist. It is an extension of its commutator subgroup which is a divisible abelian q-group of finite rank by a cyclic p-group. Furthermore it is shown

that the existence of a perfect locally finite minimal non-hypercentral p-group satisfying certain properties implies the existence of a perfect locally finite barely transitive p-group. Finally a sufficient condition is given for a perfect locally finite countable minimal non-hypercentral and non-(residually finite) group to contain a finite subgroup whose centralizer has finite exponent.

aliasar@gazi.edu.tr

Varieties of power groups

Tengiz Bokelavadze

A. Myasnikov and V. Remeslennikov refined in his paper [1] the notion of a power series due to Lindon by introducing one more additional axiom, by which all abelian subgroups of a power group are ordinary modules. This refinement is the identical generalization of a module to the non-commutative case. In [1], the basic notions of the theory of power series are introduced and also the tensor completion construction, which is a key construction in the category of power groups, is defined. The papers [1-4] marked the beginning of a systematic study of the category of power groups in the sense of Myasnikov.

The present paper continues the series of the papers [1], [2], [3] and is dedicated to the construction of basic principles of the theory of power series varieties and tensor completions of groups in a variety. We study the relationship between free groups of a given variety for various rings of scalars. Varieties of abelian power groups are described. Besides, in the category of power groups we give various analogues of the notion of an n-step nilpotent group and prove their coincidence for $n = 1; 2$. It is shown that the tensor completion of a 2-step nilpotent group is also 2-step nilpotent.

This is joint work with Mikheil Amaglobeli, mikheil.amaglobeli@tsu.ge.

References

[1] A. G. Myasnikov and V. N. Remeslennikov, Exponential groups. I. Foundations of the theory and tensor completions, (Russian) Sibirsk. Mat. Zh. 35(1994), No. 5, 1106-1118. Internat. J. Algebra Comput. 6(1996), No. 6, 687-711.

[2] A. G.Myasnikov and V. N. Remeslennikov, Exponential groups. II. Extensions of centralizers and tensor completion of CSA-groups, Internat. J. Algebra Comput. 6(1996), No. 6, 687-711.

[3] M. G. Amaglobeli and T. Z. Bokelavadze, Exponential groups. III. Groups wich are exact for tensor complement, (Russian) Herald of Omsk University, 2009, No. 2, 31-42

[4] H. Neumann, Varieties of Groups, Springer-Velarg New York, Inc., New York, 1967.

Faculty of Exact and Natural Sciences, A. Tsereteli State University. 59, Tamar Mepe St., Kutaisi, 4600, Georgia

bokel71@yahoo.com

Irreducible actions of Hopf algebras

Inês Margarida Rodrigues Pais da Silva Borges

A theorem by Bergen, Cohen and Fishman states that if a Hopf algebra H acts finitely on a module algebra A with finite Goldie dimension, such that A is a simple $A\#H$-module, then A has finite vector space dimension over A^H. At the heart of its proof is the Jacobson's Density Theorem. In this talk we extend this theorem to certain operator algebras using Julius Zelmanowitz' density theorems.

ISCAC, Coimbra
iborges@iscac.pt

Rings over which flat covers of simple modules are projective

Engin Büyükaşık

Throughout, R is a ring with a unit element and all modules are unital right R-modules. In [3] L. Bican et al. proved that all modules have flat covers over arbitrary rings. It is known that, a ring R is right perfect if and only if flat cover of any right R-module is projective. The rings over which flat covers of finitely generated modules are projective are characterized in [1] and [2].

The aim of this talk is to introduce and give several characterization of the rings R over which flat covers of simple right R-modules are projective. A ring R is said to be *right B-perfect* if $Hom(F, R) \to Hom(F, R/I)$ is an epimorphism for every flat right module F and maximal right ideal I of R.

Theorem 1. *For a ring R the following are equivalent.*

1. *R is right B-perfect.*
2. *Flat covers of simple modules are projective.*
3. *R is semiperfect and flat covers of simple modules are local.*

Theorem 2. *For a ring R the following are equivalent.*

1. *R is right B-perfect.*
2. *Every right ideal of R containing $J(R)$ is cotorsion.*
3. *R is semilocal and $J(R)$ is right cotorsion.*

References

[1] B. Amini, A. Amini and M. Ershad, Almost-perfect rings, Comm. Alg., 37,2009, 4227-4240.

[2] A. Amini, M. Ershad and H. Sharif, Rings over which flat covers of finitely generated modules are projective, Comm. Alg., 36, 2008, 2862-2871.

[3] L. Bican, R. El Bashir and E. Enochs, All modules have flat covers, Bull. London. Math. Soc., 33, 2001, 385-390.

[4] P. A. Guil Asensio, I. Herzog, Left cotorsion rings, Bull. London Math. Soc., 36, 2004, 303-309.

[5] J. Xu, Flat covers of modules, Lecture notes in mathematics, vol.1634, Springer, 1996.

Izmir Institute of Technology
enginbuyukasik@iyte.edu.tr
http://web.iyte.edu.tr/~enginbuyukasik/

A characterization of the codes over F_3

Yasemin Çengellenmiş

It is introduced v-cyclic and cyclic codes over the ring $F_3 + vF_3$ where $v^2 = 1, F_3 = \{0, 1, 2\}$. It is proved that the Gray image of the linear v-cyclic code over the commutative ring $F_3 + vF_3$ of length n is a distance invariant ternary linear cyclic code and it is proved that if n is odd, then every code over F_3 which is the Gray image of a linear cyclic code over $F_3 + vF_3$ of length n is permutation equivalent to a linear cyclic code.

References

[1] Maria Carmen V.Amarra, Fidel R.Nemenzo, On $(1-u)-$ cyclic codes over $F_{p^k} + uF_{p^k}$, *Applied Mathematics Letters*,**21**,(2008),1129-1133.

[2] R.Chapman, S.T.Dougherty,P.Gaborit,P.Sole,2-modular lattices from ternary codes, *Journal de Theorie des Nombres de Bordeaux*,Tome 14, no 1,(2002),73-85.

[3] Y.Cengellenmis, On $(1-u^2)-$ cyclic codes over $F_p + uF_p + u^2F_p$, *Journal of Discrete Mathematical Science Cryp.*,**12**,no 2,(2009),239-243.

[4] Jian-Fa Qian, Li-Na Zhang and Shi-Xin Zhu, $(1+u)$ constacyclic and cyclic codes over $F_2 + uF_2$,*Applied Mathematics Letters*, **19**,(2006), 820-823.

[5] Jian-Fa Qian, Li-Na Zhang and Shi-Xin Zhu, Constacyclic and cyclic codes over $F_2 + uF_2 + u^2F_2$,*IEICE Trans. Fundamentals*, **E89-A**, No 6,(June 2006)1863-1865.

[6] Jian-Fa Qian, Wen-ping MA, Constacyclic and cyclic codes over finite chain rings,*The Journal of China Universities of Post and Telecommunications*,**16**(3),June 2009,122-125.

[7] Patanee Udomkavanich, S.Jitman, On the Gray image of $(1-u^m)$-cyclic codes over $F_{p^k} + uF_{p^k} + ... + u^mF_{p^k}$, *Int.J.Cont.Math.Sci* , vol 4,no 26,(2009),1265-1272.

Department of Mathematics, Faculty of Science, Trakya University,22030 Edirne, Turkey
ycengellenmis@yahoo.com

Subgroup separability and efficiency

Ahmet Sinan Çevik

Let G be a group and let H be a subgroup of G. Then G is said to be *H-separable* if, for each $x \in G - H$, there exists $N \lhd G$ with finite index such that $x \notin NH$. Moreover G is called *s*ubgroup separable if G is H-separable for all finitely generated subgroups H of G. The newest known results about subgroup separability can be found, for instance, in a joint paper "(Cyclic) Subgroup Separability of HNN and Split Extensions" written by Ateş and Çevik (published in Math. Slovaca, Vol **57**(1) (2007), 33-40). Furthermore let S be a generating set for G. We also recall that the *Cayley graph* of G, denoted by Γ_G, with respect to S has a vertex for every element of G, with an edge g to gs for all elements $g \in G$ and $s \in S$. Thus the initial vertex of the edge is g and the terminal is gs. Finally we let remind the definition of "efficiency" on finitely presented groups. So let us suppose that G is such a group with a finite presentation $\mathcal{P}_G = \langle X; R \rangle$. Then the *E*uler characteristic of $\mathcal{P}_G$ is defined by $\chi(\mathcal{P}) = 1 - |X| + |R|$, where $|.|$ denotes the number of elements in the related set. Also there exists an upper bound $\delta(G) = 1 - rk_{\mathbb{Z}}(H_1(G)) + d(H_2(G))$, where $rk_{\mathbb{Z}}(.)$ denotes the $\mathbb{Z}$-rank of the torsion-free part and $d(.)$ denotes the minimal number of generators. In fact, by a paper written by Epstein in 1961, it always true that $\chi(\mathcal{P}_G) \geqslant \delta(G)$. We then define $\chi(G) = min\{\chi(\mathcal{P}) : \mathcal{P}$ is a finite presentation for $G\}$. Hence the presentation $\mathcal{P}_G$ is called *e*fficient if $\chi(\mathcal{P}_G) = \delta(G)$. In addition, G is called *efficient* if $\chi(G) = \delta(G)$.

In this talk we are mainly interested in separability and efficiency on groups under standard wreath products. To do that we will first give a new geometric way to get a presentation for the standard wreath product in terms of Cayley graphs. Then we will express the first result of the talk about efficiency. Moreover, by considering the standard wreath product G of any finite groups B by A, we will give the relationship between B-separability and efficiency on G as another result of the talk. We note that these two results have been obtained by Çevik and Ateş in a joint work which was published in the Rocky Mountain J. Math. **38**(3) (2008), 779-800.

References

[1] F. Ateş and A.S. Çevik, *Separability and Efficiency under Standard Wreath Product in terms of Cayley Graphs*, Rocky Mountain J. Math. **38**(3) (2008), 779-800.

[2] D.B.A. Epstein, *Finite Presentations of Groups and 3-manifolds*, Quart. J. Math. Oxford Ser(2), **12** (1961), 205-212.

Selcuk University, Konya-Turkey

sinan.cevik@selcuk.edu.tr

http://asp.selcuk.edu.tr/asp/personel/web/goster.asp?sicil=8857

On the basic k-nacci sequences in the direct product $D_n \times \mathbb{Z}_{2^i}$

Ömür Deveci

In this work, defining basic k-nacci sequences and the basic periods of these sequences in finite groups then we obtain the basic periods of basic k-nacci sequences and the periods of k-nacci sequences in the direct product $D_n \times Z_{2^i}$.

This is joint work with Erdal Karaduman, eduman@atauni.edu.tr.

Department of Mathematics, Faculty of Science and Letters, Kafkas University, 36100 Kars, TURKEY

odeveci36@hotmail.com

Euclid alone has looked on beauty bare

Edna St. Vincent Millay, 1892–1950

Euclid alone has looked on Beauty bare.
Let all who prate of Beauty hold their peace,
And lay them prone upon the earth and cease
To ponder on themselves, the while they stare
At nothing, intricately drawn nowhere
In shapes of shifting lineage; let geese
Gabble and hiss, but heroes seek release
From dusty bondage into luminous air.

O blinding hour, O holy, terrible day,
When first the shaft into his vision shone
Of light anatomized! Euclid alone
Has looked on Beauty bare. Fortunate they
Who, though once only and then but far away,
Have heard her massive sandal set on stone.

The least proper class containing weak supplements

Yılmaz Durgun

This study deals with the classes *Small*, S and WS of short exact sequence of R-modules determined by small, supplement and weak supplement submodules respectively, and the class $\overline{WS}$ which is the least proper class contain all of them over a hereditary ring R. *Small* is the class of all short exact sequences $0 \longrightarrow A \longrightarrow^{\alpha} B \longrightarrow C \longrightarrow 0$ where $Im(\alpha) \ll B$, WS is the class of all short exact sequences $0 \longrightarrow A \longrightarrow^{\alpha} B \longrightarrow C \longrightarrow 0$ where $Im(\alpha)$ has(is) a weak supplement in B. S is the class of all short exact sequence $0 \longrightarrow A \longrightarrow^{\alpha} B \longrightarrow C \longrightarrow 0$ where $Im(\alpha)$ has a supplement in B defined by Zöschinger in [4] may not form proper classes. The classes are different from each other, in general. On the other hand the proper classes generated by these classes, that is the least proper classes containing these classes are equivalent: $\langle Small \rangle = \langle S \rangle = \langle WS \rangle$ (The least proper class containing a class $\mathcal{A}$ is denoted by $\langle \mathcal{A} \rangle$ see [3]). WS-elements are preserved under $Ext(g, f) : Ext(C, A) \longrightarrow Ext(C', A')$ with respect to the second variable, they are not preserved with respect to the first variable. We extend the class WS to the class $\overline{WS}$, which consists of all images of WS-elements of $Ext(C, A')$ under $Ext(f, 1_A) : Ext(C', A) \longrightarrow Ext(C, A)$ for all homomorphism $f : C \longrightarrow C'$.

To prove that $\overline{WS}$ is a proper class we will use the result of [2] that states that a class $\mathcal{P}$ of short exact sequences is proper if $Ext_{\mathcal{P}}(C, A)$ is a subfunctor of $Ext_R(C, A)$, then $Ext_{\mathcal{P}}(C, A)$ is a subgroup of $Ext_R(C, A)$ for every R-modules A, C and the composition of two $\mathcal{P}$-monomorphism (epimorphism) is a $\mathcal{P}$-monomorphism (epimorphism). We obtain the following results:

Lemma 1. *If $f : A \longrightarrow A'$, then $f_* : Ext(C, A) \longrightarrow Ext(C, A')$ preserves $\overline{\mathrm{WS}}$-elements.*

Lemma 2. *If $g : C' \longrightarrow C$, then $g^* : Ext(C, A) \longrightarrow Ext(C', A)$ preserves $\overline{\mathrm{WS}}$-elements.*

Corollary 3. *The $\overline{\mathrm{WS}}$-elements of $Ext(C, A)$ form a subgroup.*

Lemma 4. *Let R be hereditary ring. For a $\overline{\mathrm{WS}}$ class of short exact sequences of R modules, the composition of an Small-epimorphism and a $\overline{\mathrm{WS}}$-epimorphism is a $\overline{\mathrm{WS}}$-epimorphism.*

Lemma 5. *Let R be hereditary ring. For a $\overline{\mathrm{WS}}$ class of short exact sequences of R modules, the composition of two $\overline{\mathrm{WS}}$ monomorphism is a $\overline{\mathrm{WS}}$ monomorphism.*

Theorem 6. *If R is a hereditary ring, $\overline{\mathrm{WS}}$ is a proper class.*

Corollary 7. *If R is hereditary ring, then $\langle \mathrm{Small} \rangle = \langle \mathrm{S} \rangle = \langle \mathrm{WS} \rangle = \overline{\mathrm{WS}}$.*

Joint work with: Prof. Rafail Alizade.

References

[1] Butler, M. C. R. and G. Horrocks. 1961. Classes of Extensions and Resolutions. *Philos. Trans. R. Soc. London* 254(A):155-222.

[2] Nunke, R. J. 1963. Purity and Subfunctor of the Identity. *Topics in Abelian groups* (Proc. Sympos., New Mexico State Univ., 1962) 121-171.

[3] Pancar, A. 1997. Generation of Proper Classes of Short Exact Sequences. *Internat. J. Math. and Math. Sci.* 20(3):465-474.

[4] Zöschinger, H. 1978. Über Torsions- und κ-Elemente von Ext(C,A). *Journal of Algebra* 50:299-336.

IZMIR INSTITUTE OF TECHNOLOGY

yilmazdurgun@iyte.edu.tr

Squares and cubes in elliptic divisibility sequences

Betül Gezer

Elliptic divisibility sequences (EDSs) are generalizations of a class of integer divisibility sequences called Lucas sequences. There has been much interest in cases where the terms of Lucas sequences are squares and cubes. But the question of when a term of an EDS can be a square has not been answered yet. We answer this question by using the general terms of these sequences. In this work, we give the general terms of the elliptic divisibility sequences with zero terms and then we determine which terms of these are squares and cubes.

This is joint work with Osman Bizim, obizim@uludag.edu.tr.

References

[1] A. Bremner, N. Tzanakis, *Lucas sequences whose 12th or 9th term is a square*, J. Number Theory **107** (2004), 215-227.

[2] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, 104, AMS, Providence, RI, 2003.

[3] B.Gezer, O. Bizim, *Squares in Elliptic divisibility sequences,* Acta Arithmetica, to appear.

[4] P. Ribenboim, W. McDaniel, *The square terms in Lucas sequences*, J. Number Theory **58** (1996), 104-123.

[5] M. Ward, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31-74.

Uludag University, Faculty of Science, Department of Mathematics, Görükle 16059, Bursa, TÜRKIYE

betulgezer@uludag.edu.tr

Model category structures arising from Drinfeld vector bundles

Pedro A. Guil Asensio

We present a general construction of model category structures on the category

$$\mathbb{C}(\mathfrak{Qco}(X))$$

of unbounded chain complexes of quasi-coherent sheaves on a semi-separated scheme X. This construction is based on making compatible the filtrations of individual modules of sections at open affine subsets of X. We apply this to describe the homotopy category $\mathbb{K}(\mathbb{C}(\mathfrak{Qco}(X)))$ via various model structures on $\mathbb{C}(\mathfrak{Qco}(X))$. As particular instances, we recover recent results on the flat model structure for quasi-coherent sheaves. Our approach also includes the case of (infinite-dimensional) vector bundles, and of restricted flat Mittag-Leffler quasi-coherent sheaves, as introduced by Drinfeld. However, we show that the unrestricted case does not induce a model category structure as above.

University of Murcia, Spain

paguil@um.es

The bounds for distance Estrada index

Ayşe Dilek Güngör

Let G be a connected graph on n vertices, and let $\mu_1, \mu_2, \cdots, \mu_n$ be the D-eigenvalues of its distance matrix D. In this talk, we will present the definition and some properties of the *distance Estrada index*

$$DEE = DEE(G) = \sum_{i=1}^{n} e^{\mu_i}$$

of the graph G (see [3]). We further present lower and upper bounds for $DEE(G)$ and relations between $DEE(G)$ and the distance energy.

References

[1] De la Peña, J.A., Gutman, I. and Rada, J. *Estimating the Estrada Index*, Linear Algebra Appl. **427** (2007), 70-76.

[2] Deng H., Radenković S. and Gutman I. *The Estrada index, in:* Cvetković, D., Gutman I. (Eds.), *Applications of Graph Spectra*, Math. Inst., Belgrade, 2009 pp. 123-140.

[3] A. D. Güngör, Ş. B. Bozkurt, On the Distance Estrada Index of Graphs, *Hacettepe J. Math. Stats.* **38**(3) (2009), 277-283.

[4] Indulal, G., Gutman, I. and Vijaykumar, A. *On the Distance Energy of a Graph,* MATCH Commun. Math. Comput. Chem. **60** (2008), 461-472.

Selcuk University, Konya-Turkey
agungor@selcuk.edu.tr
http://asp.selcuk.edu.tr/asp/personel/web/goster.asp?sicil=4568

Co-coatomically supplemented modules

Serpil Güngör

M will mean an R-module where R is an arbitrary ring with identity. A module M is called coatomic if every submodule is contained in a maximal submodule of M. A proper submodule N of M is called co-coatomic if M/N is coatomic. A module M is co-coatomically supplemented if every co-coatomic submodule U of M has a supplement V, i.e. V is minimal in the collection of submodules L of M such that $M = N + L$.
We have the following results.

Proposition 1. *Let M be a co-coatomically supplemented module. Then M/N is co-coatomically supplemented.*

Proposition 2. *Let M be a co-coatomically supplemented R-module. Then every co-coatomic submodule of the module $M/Rad(M)$ is a direct summand.*

Theorem 3. *Let R be any ring. The following are equivalent for an R-module M.*
1. Every co-coatomic submodule of M is a direct summand of M.
2. Every maximal submodule of M is a direct summand of M.
3. $M/Soc(M)$ does not contain a maximal submodule.

Joint work with Prof. Dr. Rafail Alizade

References

[1] Robert Wisbauer, Foundations of Module and Ring Theory, Gordon and Breach Science Publishers, (1991).

[2] R. Alizade, G. Bilhan, P.F. Smith, Modules Whose Maximal Submodules Have Supplements,Communications in Algebra, 29:6, 2389-2405, (2001).

İzmir Institute of Technology
serpilgungor@iyte.edu.tr

A note on the products $(1^\mu + 1)(2^\mu + 1)\dots(n^\mu + 1)$

Erhan Gürel

Let $\Omega_\mu(n) = (1^\mu + 1)(2^\mu + 1)\dots(n^\mu + 1)$ where $\mu \geqslant 2$ is an integer. We prove that $\Omega_3(n)$ is never squarefull, and in particular never a square, using arguments similar to those in [2], where Cilleruelo proves that $\Omega_2(n)$ is not a square for $n \neq 3$. In [1], among many other results, Amdeberhan, Medina and Moll claim that $\Omega_\mu(n)$ is not a square if μ is an odd prime and $n > 12$. However, we have found a gap in the proof of this statement in [1], which we illustrate by giving counterexamples.

References

[1] Amdeberhan, T. , Medina, L. A. , Moll, V. H. *Arithmetical properties of a sequence arising from an arctangent sum*, J. Number Theory **128** (2008), 1807–1846.

[2] Cilleruelo, J. *Squares in* $(1^2 + 1)\dots(n^2 + 1)$, J. Number Theory **128** (2008), 2488–2491.

Middle East Technical University, N.C.C., SZ-32, Güzelyurt, KKTC, Mersin 10, Turkey

egurel@metu.edu.tr

www.ncc.metu.edu.tr/cv.php?id=85

Nonbinary quantum stabilizer codes from codes over Gaussian integers

Murat Güzeltepe

There has been a great deal of work on trying to create efficient codes since Shor and Steane showed that it was possible to create quantum error-correcting codes [1-2]. The most successful technique to date for constructing binary quantum codes is the additive or stabilizer construction [3]. This construction takes a classical binary code, self-orthogonal under a certain symplectic inner product, and produces a quantum code, with the minimum distance determined from the classical code. Later, some results were generalized to the case of nonbinary stabilizer codes [4-7], but the theory is not nearly as complete as in the binary case. In [7], comprehensive theory of nonbinary stabilizer codes was submitted. In this paper, we obtain some nonbinary quantum stabilizer codes using classical codes over Gaussian integers. Some of these codes are MDS.

This is joint work with Mehmet ÖZEN (ozen@sakarya.edu.tr, www.mehmetozen.com) and is supported by Sakarya University Research funds as a Research Project with Project number 2009-50-02-001.

References

[1] P. W. Shor, "Scheme for reducing decoherence in quantum memory", Phys. Rev. A, vol. 52, no. 4, pp. 2493-2496, 1995.

[2] A. M. Steane, "Simple quantum error correcting codes," Phys. Rev. Lett., vol. 77, pp. 793-797, 1996.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane, "Quantum error correction via codes over GF(4)," IEEE Trans. Inf. Theory, vol. 44, no. 4, pp. 1369-1387, 1998.

[4] E. Knill, "Non-binary unitary error bases and quantum codes," LANL Preprint, quant-ph/9608048, 1996.

[5] E. Knill, "Group representations, error bases and quantum codes," LANL Preprint, quant-ph/9608049, 1996.

[6] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," IEEE Trans. Inf. Theory, vol. 47, pp. 3065-3072, 2001.

[7] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary Stabilizer Codes over Finite Fields", IEEE Trans. Inf. Theory, vol. 52, no. 11, pp. 4892-4914, 2006.

Sakarya University Arts and Science Faculty Department of Mathematics 54187 Esentepe Campus Serdivan/SAKARYA

mguzeltepe@sakarya.du.tr

http://web.sakarya.edu.tr/~mguzeltepe/

Finite generation of ideals in rings of finite character

Sevgi Harman

A ring R is said to be of finite character if each nonzero element of it is contained in only finitely many maximal ideals. Let R be a ring and I an ideal of R. Then by the J-radical of the ideal I we mean the intersection of all maximal ideals of R containing I, and the J_{max}-radical of I the intersection of all maximal ideals of R of maximal height that contains I. It is shown that over a finite dimensional integral domain R of finite character, each maximal ideal of $R[X]$ of maximal height is the J-radical of an ideal generated by three elements and J_{max}-radical of an ideal generated by two elements. We also show that over a one dimensional S-domain R of finite character each prime ideal of $R[X]$ that does not contract to the zero ideal of R is the radical of an ideal generated by at most two elements.

References

[1] V. Erdoğdu, Efficient Generation of prime ideals in polynomial rings up to radical, *Communications in Algebra* (to appear).

[2] I. Kaplansky, *Commutative Rings*, University of Chicago Press, Boston, 1974.

Istanbul Technical University

harman@itu.edu.tr

Generalized Bruck-Reilly $*$-extension of monoids

Eylem Güzel Karpuz

This is a joint work with Firat Ateş and Ahmet Sinan Çevik. Let M be a monoid and $\theta : M \to M$ be an endomorphism. Then the *Bruck-Reilly extension* $BR(M, \theta)$ is the set

$$\mathbb{N}^0 \times M \times \mathbb{N}^0 = \{(p, m, q) : p, q \geqslant 0, m \in M\}$$

with multiplication

$$(p_1, m_1, q_1)(p_2, m_2, q_2) = (p_1 - q_1 + t, (m_1\theta^{t-q_1})(m_2\theta^{t-p_2}), q_2 - p_2 + t),$$

where $t = max(q_1, p_2)$. $BR(M, \theta)$ is a monoid with identity $(0, 1_M, 0)$. If M is defined by the presentation $< A; R >$, then $BR(M, \theta)$ is defined by

$$< A, b, c\,;\ R,\ bc = 1,\ ba = (a\theta)b,\ ac = c(a\theta)\ (a \in A) >,$$

in terms of generators $(0, a, 0)$ $(a \in A)$, $(0, 1_M, 1)$ and $(1, 1_M, 0)$ [2]. This extension is considered a fundamental construction in the theory of semigroups. In [1], the author defined a monoid, namely *generalized Bruck-Reilly $*$-extension* and studied some Green's relations on it.

In this talk, we give a presentation for generalized Bruck-Reilly $*$-extension of monoids and then by using Bruck-Reilly and and this generalized Bruck-Reilly $*$-extensions we answer the following question negatively.

Question. Does the group of units of a finitely presented monoid have to be finitely generated?

References

[1] U. Asibong-Ibe, *$*$-Bisimple type A w-semigroups-I*, Semigroup Forum, **31** (1985), 99-117.

[2] J. M. Howie, N. Ruskuc, *Constructions and presentations for monoids*, Communications in Algebra, **22**(15) (1994), 6209-6224.

[3] Y. Shung, L. M. Wang, *$*$-Bisimple type A w^2-semigroups as generalized Bruck-Reilly $*$-extensions*, Southeast Asian Bulletin of Math., **32** (2008), 343-361.

Balikesir University

eguzel@balikesir.edu.tr

http://w3.balikesir.edu.tr/~eguzel/

The lattice of fully invariant subgroups of a cotorsion hull

Tariel Kemoklidze

The report deals with the questions of abelian group theory and the term group always means an additively written abelian group. The notation and terms used in the talk are taken from the monographs [1], [2].

$p-$denotes a fixed prime number. Z and Q respectively the groups of integer and rational numbers. The investigation of the lattice of fully invariant subgroups of a group is an important task of the theory of groups. This question is a less studied for cotorsion groups. A group A is called cotorsion if any extension of A by a torsion-free group C splits, i. e. $Ext(C, A) = 0$. The importance of the class of cotorsion groups is related to two facts (see [1, §§54, 55]): for any groups A, B the group $Ext(A, B)$ is a cotorsion group; any reduced group G is isomorphically embeddable into the group $G^\bullet = Ext(Q/Z, G)$ called the cotorsion hull of the group G. If G is a torsion-complete $p-$group or a direct sum of cyclic $p-$groups or a countable direct sum of torsion-complete $p-$groups, then the lattice of fully invariant subgroups of group $G^\bullet$ was studied respectively in the works [3],[4],[5]. In this work the mentioned points is studied in case when G is any direct sum of torsion-complete $p-$groups. With the help of projections and indicators (see [2, §65])every element of the group $G^\bullet$ is corresponded to infinite matrix, with the help of their necessary properties semilatice Ω is built. The lattice of fully invariant subgroups of the group $G^\bullet$ is isomorphic to the lattice of filters of semilattice Ω.

References

[1] L. Fuchs, Infinite abelian groups. I. Pure and Applied Mathematics, vol. 36, Academic Press, New York-London, 1970.

[2] L. Fuchs, Infinite abelian groups. II. Pure and Applied Mathematics, vol. 36-II, Academic Press, New York-London, 1973.

[3] A. Mader, The fully invariant subgroups of reduced algebraically compact groups. Publ. Math. Debrecen 17(1970), 299-306 (1971).

[4] A. I. Moskalenko, Cotorsion hull of a separable $p-$group. (Russian)Algebra i Logika 28(1989), No. 2, 207-226, 245; English transl.: Algebra and Logic 28(1989), No. 2, 139-151(1990)

[5] T. Kemoklidze, The lattice of fully invariant subgroups of a cotorsion hull. Georgian Math. J. 16(2009), No. 1, 89-104.

A. Tsereteli State University, 59, Tamar Mepe st., Kutaisi, 4600, Georgia

kemoklidze@gmail.com

Polytope method over rings containing non zero-divisors

Fatih Koyuncu

For any field F, there is a relation between the factorization of a polynomial $f \in F[x_1, ..., x_n]$ and the integral decomposition, with respect to Minkowski sum, of the Newton polytope of f. We extended this result to polynomial rings $R[x_1, ..., x_n]$ for an arbitrary ring R containing non zero-divisors.

References

[1] S. Gao, *Absolute irreducibility of polynomials via Newton polytopes*, Journal of Algebra **237** (2001), No.2 501-520.

Muğla University, Department of Mathematics
fatih@mu.edu.tr

Locally derivations and locally isomorphisms of matrix rings

V. M. Levchuk

A bijective linear map ψ of an arbitrary algebra $\mathcal{A}$ is said to be a local isomorphism if it acts on each element $v \in \mathcal{A}$ as a suitable isomorphism of $\mathcal{A}$. Also ψ is said to be a proper local isomorphism if is an isomorphism of $\mathcal{A}$. Similarly we define local automorphisms and local derivations of algebras and rings, see [1], [2], [3]. For the algebra of certain triangular complex 3×3 matrices R. Crist [4] constructed examples of a proper local automorphisms.

Let K be an associative ring with the identity and Γ be an arbitrary linear ordered set. We study local derivations and local isomorphisms of certain rings of finitary Γ-matrices $\| a_{ij} \|_{i,j \in \Gamma}$ over K (in particularly see [5], [6]) and also for the associated Lie and Jordan rings.

The work is supported by the Russian Foundation for Basic Research (grant 09-01-00717).

References

[1] *R. Kadison,* Local derivations, J. Algebra 130 (1990), 494-509.

[2] *R. Crist,* Local derivations on operator algebras, J. Funct. Anal. 135 (1996), 72-92.

[3] *D. Hadwin and J. Li,* Local derivations and local automorphisms, J. Math. Analysis and Applications 290 (2004), 702-714.

[4] *R. Crist,* Local automorphisms, Proc. Amer. Math. Soc. 128 (2000), 1409-1414.

[5] *M. Nader and Ghosseiri,* Jordan derivations of some classes of matrix rings, Taiwanese J. Math. 11 (2007), 51-62.

[6] *V. M. Levchuk and E.V. Minakova,* Elementary equivalence and isomorphisms of locally nilpotent matrix groups and rings, Doklady Mathematics, 79 (2009), 185-188.

Inst. Math. of Siberian Federal University, Svobodny 79, Krasnoyarsk 660041, Russia
levchuk@lan.krasu.ru

The undertaking

John Donne (1572–1631)

I HAVE done one braver thing
Than all the Worthies did ;
And yet a braver thence doth spring,
Which is, to keep that hid.

It were but madness now to impart
The skill of specular stone,
When he, which can have learn'd the art
To cut it, can find none.

So, if I now should utter this,
Others—because no more
Such stuff to work upon, there is—
Would love but as before.

But he who loveliness within
Hath found, all outward loathes,
For he who color loves, and skin,
Loves but their oldest clothes.

If, as I have, you also do
Virtue in woman see,
And dare love that, and say so too,
And forget the He and She ;

And if this love, though placèd so,
From profane men you hide,
Which will no faith on this bestow,
Or, if they do, deride ;

Then you have done a braver thing
Than all the Worthies did ;
And a braver thence will spring,
Which is, to keep that hid.

$\mathcal{P}$-pure submodules and its relation with neat and coneat submodules

Engin Mermut

Let R be an arbitrary ring with unity. Take all modules to be *left* R-modules.

A subgroup A of an abelian group B is said to be a *neat subgroup* if $A \cap pB = pA$ for all prime numbers p ([3], [1, p. 131]). This is a weakening of the condition for being a pure subgroup. There are several reasonable ways to generalize this concept to modules.

Following Stenström ([6, 9.6] and [5, §3]), we say that a submodule A of an R-module B is *neat* in B if for every simple module S, the sequence $\mathrm{Hom}(S, B) \longrightarrow \mathrm{Hom}(S, B/A) \longrightarrow 0$ obtained by applying the functor $\mathrm{Hom}(S, -)$ to the canonical epimorhism $B \longrightarrow B/A$ is exact.

Another natural generalization of neat subgroups is what is called $\mathcal{P}$-*purity*. Denote by $\mathcal{P}$ the collection of all *left primitive ideals* of the ring R. We say that a submodule A of an R-module B is $\mathcal{P}$-*pure* in B if $A \cap PB = PA$ for all $P \in \mathcal{P}$. In [4], the relation of $\mathcal{P}$-purity with complements and supplements have been used to describe the structure of c-injective modules over Dedekind domains.

A natural question to ask is when neatness and $\mathcal{P}$-purity coincide. Suppose that the ring R is *commutative*. Then $\mathcal{P}$ is the collection of all *maximal ideals* of R. Recently Fuchs ([2]) has characterized the commutative domains for which these two notions coincide. Fuchs calls a ring R to be an *N-domain* if R is a commutative domain such that neatness and $\mathcal{P}$-purity coincide. Unlike expected, Fuchs shows that N-domains are not just Dedekind domains. For a commutative domain R, Fuchs proves that R is an N-domain if and only if all maximal ideals of R are projective (and so all maximal ideals are invertible ideals and finitely generated). We slightly generalize this result by taking instead of domains commutative rings R such that every maximal ideal contains a regular element so that the ideals of R that are invertible in the total quotient ring of R will be just projective ones as in the case of commutative domains. On the way, we also obtain some properties for a dual concept to neat: *coneat submodules*. A monomorphism $f : K \to L$ is called coneat if each module M with $\mathrm{Rad}\, M = 0$ is injective with respect to it, that is, the Hom sequence $\mathrm{Hom}(L, M) \to \mathrm{Hom}(K, M) \to 0$ obtained by applying the functor $\mathrm{Hom}(-, M)$ to the monomorphism $f : K \to L$ is exact. We use a description of coneat short exact sequences to show that over commutative *small rings* (these are the rings such that the radical of every injective module is itself), the splitting of every coneat short exact sequence ending with a simple module implies that all simple modules have projective dimension $\leqslant 1$ (that is every maximal ideal is projective).

References

[1] L. Fuchs. *Infinite Abelian Groups*, volume 1. Academic Press, New York, 1970.

[2] L. Fuchs. Neat submodules over integral domains. 2009. Preliminary notes, in preparation.

[3] K. Honda. Realism in the theory of abelian groups I. *Comment. Math. Univ. St. Paul*, 5:37–75, 1956.

[4] Engin Mermut, Catarina Santa-Clara, and Patrick F. Smith. Injectivity relative to closed submodules. *J. Algebra*, 321(2):548–557, 2009.

[5] Bo T. Stenström. High submodules and purity. *Arkiv för Matematik*, 7(11):173–176, 1967.

[6] Bo T. Stenström. Pure submodules. *Arkiv för Matematik*, 7(10):159–171, 1967.

Dokuz Eylül University, İzmir/TURKEY
engin.mermut@deu.edu.tr
http://kisi.deu.edu.tr/engin.mermut/

On extensions of a valuation on K to $K(x)$

Figen Öke

Let v be a valuation of a field K, G_v its value group and k_v its residue field and w be an extension of v to $K(x)$. w is called residual transcendental extension of v if k_w/k_v is a transcendental extension and w is called residual algebraic extension of v if k_w/k_v is an algebraic extension. In this study residual transcendental and residual algebraic extensions of v to $K(x)$ are represented.

References

[1] V. Alexandru, N.Popescu, A.Zaharescu, A theorem of characterization of residual trancendental extensions of a valuation, *J. Math. Kyoto Univ. (JMKYAZ)* **28** (1988) 579–592.

[2] V.Alexandru, N.Popescu, A.Zaharescu, Minimal pair of definition of a residual transcendental extension of a valuation, *J. Math. Kyoto Univ (JMKYAZ)* **30** (1990) 207–225.

[3] V.Alexandru, N.Popescu, A.Zaharescu, All valuations on $K(x)$ *J. Math. Kyoto Univ.* **30-2** (1990) 281–296.

Trakya University, Department of Mathematics, 22030 Edirne, TURKEY
figenoke@gmail.com

An application of strong Groebner basis to coding theory

Hakan Özadam

Let $GR(p^a, m)$ be the Galois ring with characteristic p^a and cardinality p^{am}. Since $GR(p^a, m)[x]$ is not a principal ideal ring, the study of the ideal structure of $\frac{GR(p^a,m)[x]}{\langle x^N-1\rangle}$, and therefore the study of cyclic codes of length N over $GR(p^a, m)$, is much more complicated compared to the case of cyclic codes over finite fields. This motivates applying the theory of Groebner basis to cyclic codes over Galois rings. It is well-known that the classical theory of Groebner basis can be extended to the theory of Groebner basis over rings. In [1], the authors introduce a special type of Groebner basis over principal ideal rings which they call *strong Groebner basis*. Given a cyclic code of length N over $GR(p^a, m)$, which is an ideal of $\frac{GR(p^a,m)[x]}{\langle x^N-1\rangle}$, it has been explained in [2] and [3] how to determine the minimum Hamming distance of C, using strong Groebner basis. Recently, Lopez-Permouth, Özadam, Özbudak and Szabo determined the minimum Hamming distance of certain constacyclic codes of length np^s over $GR(p^a, m)$ via strong Groebner basis in [4]. In this talk, I will give an overview of this result.

References

[1] G. Norton and A. Sălăgean, *"Strong Gröbner bases for polynomials over a principal ideal ring"*, Bull. Austral. Math. Soc. 64, no. 3, pp. 505-528, 2001.

[2] G. H. Norton and A. Sălăgean, "Cyclic codes and minimal strong Gröbner bases over a principal ideal ring", Finite fields and their app. 9, pp. 237-249, 2003.

[3] A. Sălăgean, *"Repeated-root cyclic and negacyclic codes over a finite chain ring"*, Discrete App. Math, vol 154, no. 2, pp. 413-419, 2006.

[4] S. R. López-Permouth, H. Özadam, F. Özbudak and S. Szabo, *"Polycyclic codes and repeated-root constacyclic codes"*, preprint, 2009.

Middle East Technical University

ozhakan@metu.edu.tr

Cotorsion modules and pure-injectivity

Dilek Pusat-Yılmaz

A module C is called cotorsion if $\mathrm{Ext}^1(F, C) = 0$ for any flat module F. We show that any cotorsion module satisfies a compactness condition on certain finite definition subgroups. Namely, those associated to divisibility conditions on pp-formulae in the First Order Logic of Modules. Using this characterization, we obtain a new proof of the fact that the endomorphism ring of any flat cotorsion module is f-semiperfect and idempotents

lift modulo the Jacobson radical, thus completing some characterizations obtained in [1]. We apply these results to the particular case of hereditary rings and obtain conditions that force a hereditary ring to be semiperfect in terms of the presentation of its cotorsion envelope.

Joint work with Deniz Erdemirci and Pedro Guil Asensio.

References

[1] P.A. Guil Asensio and I. Herzog, Pure-injectivity in the category of flat modules, Contemporary Mathematics American Mathematical Society 419, (2007).

[2] B.L. Osofsky, A generalization of quasi-Frobenius rings, J. Algebra 4 (1966) 373-387.

[3] J. Xu, Flat Covers of Modules, Lecture Notes in Mathematics; 1634, Springer 1996.

Izmir Institute of Technology
dilekyilmaz@iyte.edu.tr

Soft near-rings

Aslıhan Sezgin

This is a joint work with Akın Osman Atagün. Soft set theory, which can be used as a new mathematical tool for dealing with uncertainty was introduced by Molodtsov. In this paper, we indicate the study of soft near-rings by using Molodtsov's definition of the soft sets. The notions of soft near-rings, soft subnear-rings, soft (left, right) ideals, (left, right) idealistic soft near-rings and soft near-ring homomorphisms are introduced. Moreover, several related properties are investigated and illustrated by a great deal of examples.

Department of Mathematics, Bozok University, 66100, Yozgat, Turkey
aslihan.sezgin@bozok.edu.tr

Decomposability of $(1,2)$-Groups

Ebru Solak

A torsion free abelian group of finite rank is called almost completely decomposable if it has a completely decomposable subgroup of finite index. A p-local, p-reduced almost completely decomposable group of type $(1,2)$ is briefly called a $(1,2)$-group. Almost completely decomposable groups can be represented by matrices over the ring $\mathbb{Z}_h = \mathbb{Z}/h\mathbb{Z}$, where h is the exponent of the regulator quotient. This particular choice of representation allows for a better investigation of the decomposability of the group. Arnold and Dugas showed in several of their works that $(1,2)$- groups with regulator quotient of exponent at least p^7 allow infinitely many isomorphism types of indecomposable groups. It is not known if the exponent 7 is minimal.

References

[1] *D.Arnold, Pure subgroups of finite rank completely decomposable groups,* In Abelian Group Theory, Lecture Notes in Mathematics, volume 874, pages 1-31. Springer Verlag, New York, (1981).

[2] D. Arnold, M. Dugas, *Representation type of posets and finite rank Butler groups.* In *Coll. Math.* 74, (1997), 299-319.

Middle East Technical University, Department of Mathematics, 06531 Ankara, Turkey

esolak@metu.edu.tr

www.metu.edu.tr/~esolak/

MacWilliams identity for M-spotty weight enumerators of linear codes over the finite fields $GF(q)$

Vedat Şiap

Some of the error control codes applies to high-speed memory systems using RAM chips with either 1-bit I/O data ($b = 1$) or either 4-bit I/O data ($b = 4$). However, modern large-capacity memory systems use RAM chips with 8, 16, or 32 bits of I/O data. A new class of codes called m-spotty byte error codes provides good source for correcting / detecting in those memory systems that use high density RAM chips with wide I/O data (e.g. 8, 16, or 32 bits). The MacWilliams identity provides the relation of weight distribution of a code and that of its dual code. This paper presents the MacWilliams identity for m-spotty weight enumerators of linear codes over the finite fields $GF(q)$.

This is a joint work with M. ÖZEN ozen@sakarya.du.tr.

References

[1] E. Fujiwara, Code Design for Dependable Systems, Wiley-Int. Sci., 2006.

[2] K. Suzuki, T. Kashiyama, E. Fujiwara, "A General Class of M-Spotty Byte Error Control Codes," In: Proc. Asian-European Workshop on Inf. Theory, Viraggio, Italy, Oct., pp.24-26, 2004.

[3] G. Umanesan, E. Fujiwara, "A Class of Random Multiple Bits in a Byte Error Correcting and Single Byte Error Detecting ($S_{t/b}EC - S_bED$) Codes," IEEE Trans. Comput. 52(7)(2003)835-847.

[4] S. Kaneda, E. Fujiwara, "Single Byte Error Correcting-Double Byte Error Detecting Codes for Memory Systems," IEEE Trans. Comput. C-31(7)(1982) 596-602.

[5] K. Suzuki, H. Kaneko, E. Fujiwara, "MacWilliams Identity for M-Spotty Weight Enumerator," ISIT 2007, Nice, France, June 24-29, 2007.

[6] F. J. MacWilliams, N. J. A. Sloane, The Theory of Error Correcting Codes, World Scientific, Singapore, 1997.

[7] I. Siap, "MacWilliams Identity for M-Spotty Lee Weight Enumerators,"Applied Mathematics Letters 23 (2010) 13-16.

Sakarya University Arts and Science Faculty Department of Mathematics 54187 Esentepe Campus Serdivan/SAKARYA

vsiap@sakarya.edu.tr

Equiprime ideals of near-ring modules

Funda Taşdemir

This is a joint work with Akın Osman Atagün and Hüseyin Altındiş. In this paper we introduce the notion of equiprime N-ideals (ideals of near-ring modules) where N is a near-ring. We consider the interconnections of equiprime, 3-prime and completely prime N-ideals. The relationship between an equiprime N-ideal P of an N-group Γ and the ideal $(P : \Gamma)$ of the near-ring N is also investigated.

Department of Mathematics, Bozok University, 66100, Yozgat, Turkey

funda.tasdemir@bozok.edu.tr

On the relationship between Fibonacci length of its extensions and dicyclic group

Yasemin Taşyurdu

This paper is concerned with the relationship between Dic_ndicyclic group and Fibonacci lengths of the cyclic groups which are extension of Dic_n dicyclic group for $n = 2^k$. Also, we showed that $LEN\left(C_{m^{r+1}}\right) = LEN\left(C_m\right) m^r$ for $m = p^s$, p is prime ; $s \in \mathrm{Z}^+$

This is joint work with İnci GÜLTEKİN.

References

[1] D. D. Wall, Fibonacci series module m, Amer. Math. Monthly 67 (1960), pp. 525-532.

[2] A. P. Shah, Fibonacci sequence modulo m, Fibonacci Quarterly 6.2 (1968), pp. 139-141.

[3] H. J. Wilcox, Fibonacci sequence of period n in groups, Fibonacci Quarterly 24 (1986), pp. 356-361.

[4] C. M. Campbell, H. Doostie and E. F. Robertson In: G. E. Bergum et al., Editors, Fibonacci Length of Generating Pairs in Groups, Applications of Fibonacci Numbers vol. 3, Kluwer Academic Publishers (1990), pp. 27-35.

[5] Steven W. Knox, Fibonacci sequences in finite groups, Fibonacci Quarterly 30.2 (1992), pp. 116-120.

[6] M. Renault, Master's Thesis Wake Forest University, 1996.

Atatürk University, Science Faculty, Department of Mathematics, 25240 Erzurum, Turkey

yasemintasyurdu@hotmail.com.tr

On cofinitely supplemented lattices

S. Eylem Toksoy

L will mean a complete modular lattice with smallest element 0 and greatest element 1. A lattice L is said to be *supplemented* if every element a of L has a supplement in L, i.e. an element b such that $a \vee b = 1$ and $a \wedge b \ll b/0$. An element c of a complete lattice L is said to be *compact* if for every subset X of L with $c \leqslant \bigvee X$ there exists a finite subset F of X such that $c \leqslant \bigvee F$. A lattice L is called a *compact lattice* if 1 is compact and a *compactly generated lattice* if each of its elements is a join of compact elements. An element a of a lattice L is said to be *cofinite* in L if the quotient sublattice $1/a$ is compact. A lattice L is called a *cofinitely supplemented lattice* if every cofinite element of L has a supplement in L.

For compactly generated compact lattices a supplement of an element is compact (see [2, Proposition 12.2 (2)]). In the following proposition we show that for an arbitrary lattice L a supplement of a cofinite element is compact.

Proposition 1. *Let a be a cofinite element of a lattice L and b be a supplement of a. Then $b/0$ is compact.*

Theorem 2. (cf. [3, Theorem 5.3.33]) *A lattice L is a cofinitely supplemented lattice if and only if every maximal element of L has a supplement in L.*

Theorem 1 is used in the proof of the following theorem which gives a new result for modules.

Theorem 3. *If $a/0$ is a cofinitely supplemented sublattice of L and $1/a$ has no maximal element, then L is also a cofinitely supplemented lattice.*

Corollary 4. *Let M be a module, N be a cofinitely supplemented submodule of M. If $\mathrm{Rad}(M/N) = M/N$, then M is cofinitely supplemented.*

Joint work with: Refail Alizade, İzmir Institute of Technology
e-mail: rafailalizade@iyte.edu.tr

References

[1] Alizade R., Bilhan G., Smith P.F., "Modules whose Maximal Submodules have Supplements", *Communications in Algebra*. Vol.29, No:6, pp.2389-2405 (2001).

[2] Călugăreanu G., Lattice Concepts of Module Theory, Kluwer Academic Publishers, Dordrecht, Boston, London (2000).

[3] Çetindil Y., Generalizations of Cofinitely Supplemented Modules to Lattices, M.Sc. Thesis, İzmir Institute of Technology, İzmir (2005).

İzmir Institute of Technology
eylemtoksoy@iyte.edu.tr
www.iyte.edu.tr/~eylemtoksoy

Posters

Speeding up Montgomery modular multiplication for prime fields

Sedat Akleylek, Murat Cenk

We give faster versions of Montgomery modular multiplication algorithm without pre-computational phase for $GF(p^m)$, where p is prime and $m > 1$, which can be considered as a generalization of [1], [2] and [3]. We propose sets of moduli which can be used in public key cryptographic applications. We eliminate pre-computational phase with proposed sets of moduli. We show that these methods are easy to implement for hardware.

References

[1] M. Knezevic, L. Batina and I. Verbauwhede, *Modular Reduction without Precomputational Phase*, IEEE International Symposium on Circuits and Systems (ISCAS 2009), IEEE, 4 pages, 2009.

[2] M. Knezevic, J. Fan, K. Sakiyama, and I. Verbauwhede, *Modular Reduction in $GF(2^n)$ without Pre-Computational Phase*, International Workshop on the Arithmetic of Finite Fields (WAIFI 2008), LNCS 5130, Ç. K. Koç, J. Luis Imana, and J. Von zur Gathen (eds.), Springer-Verlag, pp. 77-87, 2008.

[3] M. Knezevic, F. Vercauteren, and I. Verbauwhede, *Faster Interleaved Modular Multiplication Based on Barrett and Montgomery Reduction Methods*, COSIC internal report, 8 pages, 2009.

Middle East Technical University and Ondokuz Mayıs University

akleylek@metu.edu.tr

Middle East Techical University

mcenk@metu.edu.tr

Pseudorandom sequences over finite fields

Esen Aksoy

We consider the permutation polynomial $P_n(x) = (...((x^{q-2} + a_1)^{q-2} + a_2)^{q-2} + ... + a_{n-1})^{q-2} + a_n$ of $\mathbb{F}_q$, where $P_0(x) = x$, $P_{n+1}(x) = P_n(x)^{q-2} + a_{n+1}$ for $n \geqslant 0$ as in [1] and define a sequence $(u_n)_{n\geqslant 0}$ with $u_n = P_n(u_0)$. If the sequence (a_n) is periodic and $per(a_n) = t$, then $per(u_n)$ depends on the cycle structure of $P_t(x)$, and the starting value u_0. In particular, if $\mathcal{P}_t$ has full cycle structure, then the sequence (u_n) is balanced and $per(u_n) = pt$ for all initial values $u_0 \in \mathbb{F}_q$.

References

[1] A. Çeşmelioğlu , W. Meidl, A. Topuzoğlu On the cycle structure of permutation polynomials *Finite Fields Appl.* **14** (2008) 593-614.

Sabanci University
eaksoy@su.sabanciuniv.edu

On ramification in extensions of rational function fields

Nurdagül Anbar

Let $K(x)$ be a rational function field, which is a finite separable extension of the rational function field $K(z)$. In the first part, we have studied the number of ramified places of $K(x)$ in $K(x)/K(z)$. Then we have given a formula for the ramification index and the different exponent in the extension $F(x)$ over a function field F, where x satisfies an equation $f(x) = z$ for some $z \in F$ and separable polynomial $f(x) \in K[x]$. In fact, this generalizes the well-known formulas for Kummer and Artin-Schreier extensions.

References

[1] H. Stichtenoth, Algebraic Function Fields and Codes, *Springer, Berlin,* 2008.

[2] R. Lidl, H. Niederreiter, Finite Fields, 2. edition, *Cambrigge University Press, Cambridge,* 1997.

[3] A. Garcia, Lectures notes on Algebraic Curves, *Sabancı University,* 1996.

[4] H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionnkörper, insbesondere bei endlichem Konstantenkörper, *J. Reine Angew. Math.* 172, 005, pp. 37-54.

Sabancı University
nurdagul@su.sabanciuniv.edu

Drinfeld modular curves with many rational points over finite fields

Vural Cam

For some kinds of reasons one is interested to construct curves which have many ratioal points over a finite field. Drinfeld modular curves can be used to construct that kinds of curves over a finite field. In my work I am using reductions of the Drinfeld modular curves $X_0(n)$ with suitable primes to get such nice curves. The main idea is to divide the Drinfeld modular curves by an Atkin-Lehner involution which has many fixed points to obtain a quotient with a better ratio *{number of rational points}/genus*.

Metu

cvural@metu.edu.tr

Polynomial multiplication over finite fields

Murat Cenk

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. Let n and ℓ be positive integers and $f(x)$ be an irreducible polynomial over $\mathbb{F}_q$ such that $\ell deg(f(x)) < 2n-1$. We obtain an effective upper bound for the multiplication complexity of n-term polynomials modulo $f(x)^\ell$. This upper bound allows a better selection of the moduli when Chinese Remainder Theorem is used for polynomial multiplication over $\mathbb{F}_q$. We give improved formulas to multiply polynomials of small degree over $\mathbb{F}_2$ and $\mathbb{F}_3$. In particular, we improve the best known multiplication complexities over $\mathbb{F}_2$ and $\mathbb{F}_3$ in the literature in some cases.

Middle East Techical University

mcenk@metu.edu.tr

Quantum groups

Münevver Çelik

R-matrices are solutions of the Yang-Baxter equation. They give rise to link invariants. R-matrices are derived from a special kind of Hopf algebra, namely quantum group. In this work, I will define quantum groups and present the way to derive link invariants from R-matrices.

METU

mucelik@metu.edu.tr

A remark on permutations with full cycle

Ayça Çeşmelioğlu

For $q > 2$, Carlitz proved in [1] that the group of permutation polynomials (PPs) over $\mathbb{F}_q$ is generated by the linear polynomials and x^{q-2}. Based on this result, we point out a simple method for representing all PPs with full cycle over the prime field $\mathbb{F}_p$, where p is an odd prime. We use the isomorphism between the symmetric group S_p of p elements and the group of PPs over $\mathbb{F}_p$, and the well-known fact that permutations in S_p have the same cycle structure if and only if are conjugate.

References

[1] L. Carlitz, "Permutations in a finite field ", Proc. Amer. Math. Soc. 4, 538, 1953.

Sabancı Üniversitesi
cesmelioglu@sabanciuniv.edu
http://myweb.sabanciuniv.edu/acesmelioglu

On o-minimal structures

Şükrü Uğur Efem

A linearly ordered structure is said to be o-minimal if every definable subset of it is a finite union of intervals and points. The motivating example is the ordered field of reals. The notion of o-minimality was implicitly introduced in the eighties by Lou van den Dries who observed that many non-trivial properties of semi-algebraic sets follow from those simple axioms, and then developed further by Pillay and Steinhorn. In this poster we survey some known results and applications of o-minimality.

References

[1] L. van den Dries, o-Minimal Structures, in: Logic: from Foundations to Applications, Clarendon Press, Oxford (1996), pp 137-185.

[2] A. Pillay and C. Steinhorn. Definable sets in ordered structures. I. Transactions of American Math. Society, 295:565-592, 1986.

[3] L. Lipshitz and Z. Robinson. Overconvergent real closed quantifier elimination. Bull. London Math. Soc. 38 (2006), no. 6, 897–906

Sabancı Üniversitesi
suefem@sabanciuniv.edu

Maximal subgroups in Hall universal groups

Mehmet İnan Karakuş

In an infinite group, it is a difficult task to decide whether a maximal subgroup exist or not.It is a well known trivial example that the *p-quasicyclic group* (or *Prüfer p-group*, or C_p^∞) has no maximal subgroup. A locally finite group G is called a universal group(see [2]) if

1. Every finite group can be embedded in G
2. Any two isomorphic finite subgroups of G are conjugate in G

We discuss the existence of maximal subgroups in locally finite universal groups. In particular there is a construction of a maximal p-subgroup which is also maximal subgroup of the group.The construction is due to M. Dalle Molle (see [1])

References

[1] M. Dalle Molle, Sylow subgroups which are maximal in the universal locally finite group of Philip Hall, *J. Algebra* **215** (1999), no. 1, 229–234.

[2] P. Hall, Some constructions for locally finite groups, *J. London Math. Soc.* **34** (1959), 305-319.

Middle East Technical University
minan@metu.edu.tr

Classification of finitary linear simple locally ginite groups

Dilber Koçak

A group is called locally finite if every finitely generated subgroup is a finite group. G is called a linear group if it is a subgroup of $GL(n, F)$ for some field F.

The classification of simple locally finite linear groups is completed independently by Belyaev, Borovik, Hartley-Shute and Thomas. They have proved:

Theorem 1. *(BBHST: Belyaev, Borovik, Hartley, Shute, and Thomas [1], [2], [4] and [5]). Each locally finite simple group that is not finite but has a faithful representation as a linear group in finite dimension over a field is isomorphic to a Lie type group $\Phi(K)$, where K is an infinite, locally finite field, that is, an infinite subfield of $\overline{\mathbb{F}}_p$, for some prime p.*

A group of linear transformations is called finitary if each element minus the identity is an endomorphim of finite rank. Then observe that every linear locally finite simple group is a finitary linear simple locally finite group. Recently the classification of finitary simple locally finite groups are completed by J. I. Hall in [3].

Theorem 2. *(Hall). A locally finite simple group that has a faithful representation as a finitary linear group is isomorphic to one of:*

(1) a linear group in finite dimension;
(2) an alternating group $Alt(\Omega)$ with Ω infinite;
(3) a finitary symplectic group $FSp_K(V, s)$;
(4) a finitary special unitary group $FSU_K(V, u)$;
(5) a finitary orthogonal group $F\Omega_K(V, q)$;
(6) a finitary special linear group $FSL_K(V, W, m)$.

Here K is a (possibly finite) subfield of $\overline{\mathbb{F}}_p$, the algebraic closure of the prime subfield $\mathbb{F}_p$. The forms s,u, and q are nondegenerate on the infinite dimensional K-space V; and m is a nondegenerate pairing of the infinite dimensional K-spaces V and W. Conversely, each group in (2)-(6) is locally finite, simple, and finitary but not linear in finite dimension.

References

[1] V. V. BELYAEV, Locally finite Chevalley groups, in *Studies in Group Theory*, Urals Scientific Centre of the Academy of Sciences of USSR, Sverdlovsk (1984), 39-50 (in Russian).

[2] A. V. BOROVIK, Periodic linear groups of odd characteristic, *Dokl. Akad. Nauk. SSSR* **266** (1982), 1289-1291.

[3] J. I. HALL, Periodic simple groups of finitary linear transformations, *Annals of Mathematics* **163** (2006),445-498

[4] B. HARTLEY and G. SHUTE, Monomorphisms and direct limits of finite groups of Lie type, *Quart. J. Math.* **35** (1984), 49-71.

[5] S. THOMAS, The classification of the simple periodic linear groups, *Arch. Math.* **41**(1983), 103-116.

METU

dilber@metu.edu.tr

On stability of free products in bounded balls

Azadeh Neman

In a series of papers, Z. Sela proved that free groups, and more generally torsion-free hyperbolic groups, have a stable first-order theory. It has been conjectured by E. Jaligot [2] that the free product of two arbitrary stable groups is stable. However, a full answer seems to become a very large project of generalization, from free groups to free products, of the famous articles of Sela. Until this monumental task is done, we provide a very preliminary result in the direction of the stability of free products of stable groups, restricting ourselves to quantifer-free definable sets and to bounded balls of free products and including finite amalgamation.

References

[1] A. Neman. Stability and bounded balls of free products, *Accepted*

[2] E. Jaligot. Groups of finite dimension in model theory. In C. Glymour, W. Wang, and D. Westerstahl, editors, *Proceedings from the 13th International Congress of Logic, Methodology, and Philosophy of Sciences, Beijing, august 2007*. Studies in Logic and the Foundations of Mathematics, King's College Publications, London, 2008.

[3] W. Magnus, A. Karrass and D. Solitar *Combinatorial group theory.* Presentations of groups in terms of generators and relations

Istanbul Bilgi University

azadeh.neman@gmail.com

Automorphism groups of generalized Giulietti–Korchmaros curves

Mehmet Özdemir

Giuletti and Korchmaros introduced a new example of a maximal curve which is not covered by the Hermitan curve [1]. Their curve is defined over $GF(q^6)$ for some prime power q. Later, Garcia, Güneri and Stichtenoth introduced a family of maximal curves over $GL(q^{2n})$ for a prime q and an odd integer $n \geqslant 3$ [3]. Amongst these curves the one with $n = 3$ coincides with the curve of Giuletti and Korchmaros, and for $n > 3$ it is not known yet whether these curves are covered by the Hermitian curve. The automorphism group of Giuletti-Korchmaros curve is known, and Fanali and Giuletti found some subfiels of this curve corresponding to some subgroups of its automorphism group [2]. The question is what is the automorphism group of Generalized Giuletti-Korchmaros curves for $n > 3$ and how to find subfields of these curves corresponding to subgroups of their automorphism groups and what are the genera of these subfields.

References

[1] M. Giulietti, G. Korchmaros, A New Family of Maximal Curves Over a Finite Field, Mathematische Annalen 343(1), 2009, pp. 229-245.

[2] M. Giulietti, S. Fanali, Quotient Curves of the GK curve, Preprint.

[3] A. Garcia, C. Güneri, H. Stichtenoth A Generalization of the Giulietti-Korchmaros Maximal Curve, Preprint.

Sabancı University

mehmetozdemir@su.sabanciuniv.edu

Low-density-parity-check codes

Buket Özkaya

Low-density-parity-check (LDPC) codes were first proposed in the PhD thesis of Gallager at MIT, in 1962. They remained largely neglected for over 35 years due to the computational difficulties at that time, which didn't allow to discover their elegant properties. After their rediscovery in 1996, they became one of the most popular research topics of coding and information theory, which also yield many applications in the fields like telecommunication, signal processing, statistical physics etc. The aim of my work was to survey the main concerning approachs and to express them in an unified mathematical language, which would let the subject not only to be understood in a systematic way, but also to be a brief collective tutorial about LDPC codes. After a summary of the most important tasks of coding and information theory, various techniques of LDPC-code constructions are presented in matrix and graph representations, following the historical progression. Their properties are explained in algebraic and combinatorial terms such as their minimal distance can achieve Gilbert-Varshamow bound exponentially and with an optimal decoding the code rate approachs the channel capacity, which provides a constructive proof to the Shannon's theorem. The decoding algorithms used for LDPC codes belong to the class of message passing algorithms. They are iterative and rely on binary or probabilistic decisions about the bit values of the codeword which is sent through a noisy channel. The analysis of the algorithm is carried out by the process called density evolution, which intends to determine a threshold of channel noise for a given LDPC-code ensemble so that the message passing decoder is able to correct the possible errors successfully.

References

[1] Gallager, R.G. , "*Low Density Parity Check Codes*", MIT Press, 1963.

[2] MacKay, D.J.C. and Neil, R.M "*Good Error-Correcting Codes based on Very Sparse Matrices*", IEEE Trans. Inform. Theory, vol. 45 no. 2, pp. 339-431, 1999.

[3] Sipser, M. and Spielman, D.A., "*Expander Codes*", IEEE Trans. Inform. Theory, vol. 42 no. 6, pp. 1710-1722, 1996.

Sabanci University

buketo@sabanciuniv.edu

Numbers and sets

David Pierce

This is about an analogy between numbers and sets that is highlighted when one generalizes both.

Dedekind [1] identified the properties that determine the set $\mathbb{N}$ of natural numbers as an algebraic structure, $(\mathbb{N}, 1, S)$:

(1) there is a distinguished initial natural number 1;
(2) each natural number n has a successor, $S(n)$;
(3) 1 is not a successor;
(4) no two numbers have the same successor;
(5) proof by induction is possible.

These properties are often named for Peano [2], perhaps because he gave them a symbolic formulation; but his understanding of them was apparently less profound than Dedekind's. In any case, their import is that $\mathbb{N}$ is a free algebra in the signature $\{1, S\}$.

Von Neumann [3] gave a set-theoretic definition of the class **ON** of ordinal numbers. This class is well-ordered by membership ($\in$); it can also be understood as an algebraic structure, $(\mathbf{ON}, \varnothing, x \mapsto x \cup \{x\})$; this has the substructure $(\omega, \varnothing, x \mapsto x \cup \{x\})$, which is isomorphic to $(\mathbb{N}, 1, S)$. The isomorphism suggests an analogy:

There are two kinds of numbers:	There are two kinds of sets:
1 and the successors.	empty and not.
The operation of succession takes	Sets contain their elements
a single argument.	in only one way.

If one allows sets to have various "types" (beyond "empty" and "nonempty"), and one allows sets to have various "grades" of elements, then, in any algebraic signature, there is a set-theoretic construction of a free algebra analogous to ω; this is embedded in an ordered class analogous to **ON**.

References

[1] Richard Dedekind. *Essays on the theory of numbers. I: Continuity and irrational numbers. II: The nature and meaning of numbers.* authorized translation by Wooster Woodruff Beman. Dover Publications Inc., New York, 1963.

[2] Giuseppe Peano. The principles of arithmetic, presented by a new method (1889). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 83–97. Harvard University Press, 1976.

[3] John von Neumann. On the introduction of transfinite numbers (1923). In Jean van Heijenoort, editor, *From Frege to Gödel*, pages 346–354. Harvard University Press, 1976.

METU

dpierce@metu.edu.tr

http://metu.edu.tr/~dpierce/

Monomial Gotzmann sets in a quotient by a pure power

Ata Fırat Pir

We study Gotzmann sets in a quotient $R = F[x_1, \ldots, x_n]/(x_1^a)$ of a polynomial ring over a field F. These are monomial sets whose sizes grow minimally when multiplied with the variables. We partition the set of monomials in a Gotzmann set with respect to the multiplicity of x_1 and show that if the size of a component in a partition is sufficiently large, then this component is a multiple of a Gotzmann set in $F[x_2, \ldots, x_n]$. Otherwise we derive lower bounds on the size of a component depending on neighboring components. For $n = 3$, we classify all Gotzmann sets in R and for a given degree, we compute all integers j such that the only Gotzmann set in that degree is the lexsegment set of size j. We also we note down adoptions of some properties concerning the minimal growth of the Hilbert function in $F[x_1, \ldots, x_n]$ to R.

Bilkent University
pir@fen.bilkent.edu.tr

On the number of Boolean functions satisfying strict avalanche criteria

Elif Saygı

Boolean functions play an important role in the design of both block and stream ciphers. In this work, the number of Boolean functions satisfying strict avalanche criteria are considered. Also, the number of functions with particular difference distribution vectors is studied. The exact formula for a special case is given. Results of some statistical observations are compared to the exact values.

This is a joint work with Ali Doğanaksoy and Zülfükar Saygı.

Hacettepe University
esaygi@hacettepe.edu.tr

Quadratic feedback shift registers and maximum length sequences

Zülfükar Saygı

In this work, the properties of the quadratic feedback shift registers generating maximum length sequences are considered. Some necessary conditions for a quadratic feedback function f of a feedback shift register to generate a maximum length sequence is given. Also a method generalizing this condition is presented. Instead of searching all the sequence, looking at the algebraic normal form of the function f one can understand if the corresponding shift register generates a sequence having short period.

This is a joint work with Elif Saygı and Ali Doğanaksoy.

TOBB University of Economics and Technology

zsaygi@etu.edu.tr

http://zsaygi.etu.edu.tr/

Recursive towers of function fields over finite fields

Seher Tutdere

In 1995 Garcia and Stichtenoth gave explicit constructions of towers of function fields over the finite field $\mathbb{F}_q$. Moreover, in the case that $q = p^k$ (for $k \geqslant 2$ and p is a prime) they have given some examples of towers having positive limit which are called asymptotically good and optimal towers (see [1, 2]). Now we deal with the following problem: Are there any such towers of function fields over the prime fields $\mathbb{F}_p$ for any prime p? If so, then how to define polynomials which give such nice towers?

References

[1] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory* **61** (1996) 248-273.

[2] H. Stichtenoth, Algebraic Function Fields and Codes, *Springer, Berlin,* (2009).

[3] S. Tutdere, A Recursive Tower of Function Fields over $\mathbb{F}_2$, *Ms.c. Thesis, Sabancı University,* 2009.

Sabancı University

sehertutdere@su.sabanciuniv.edu

Regulators on K_1 of product of elliptic curves

İnan Utku Türkmen

Spencer Bloch defined and studied the properties of higher Chow groups, $CH^\bullet(X, m)$, in his seminal work [Blo] and established the relation between these groups and higher K theory which is known as Bloch's version of Grothendieck Reimann Roch theorem;

$$K_m(X) \otimes \mathbb{Q} \simeq CH^\bullet(X, m) \otimes \mathbb{Q}.$$

Both higher K groups and higher Chow groups are complicated objects and it is hard to compute them, so they are studied by mappings to more computable cohomology theories. These maps are named regulators.

In this work, we are going to give a brief introduction to subject, defining the basic objects and methods in the literature and present our results on higher Chow groups of sufficiently general product of elliptic curves and regulator maps to Deligne cohomology.

This work has been carried out under the supervision of Prof. James D. Lewis from University of Alberta.

References

[Blo] Bloch S., Algebraic cycles and higher K-theory, Adv. Math. **61** (1986), 267-304

Bilkent University
turkmen@fen.bilkent.edu.tr

Participants

1. Sedat Akleylek akleylek@metu.edu.tr
2. Esen Aksoy eaksoy@su.sabanciuniv.edu
3. Emine Albaş emine.albas@ege.edu.tr
4. Tuna Altınel altinel@math.univ-lyon1.fr
5. Nurdagül Anbar nurdagul@su.sabanciuniv.edu
6. Nurcan Argaç nurcan.argac@ege.edu.tr
7. Ahmet Arıkan arikan@gazi.edu.tr
8. Aynur Arıkan yalincak@gazi.edu.tr
9. Ali Osman Asar aliasar@gazi.edu.tr
10. Fırat Ateş firat@balikesir.edu.tr
11. Alp Bassa Alp.Bassa@cwi.nl
12. Oleg Belegradek obelegradek@rambler.ru
13. Ayşe Berkman aberkman@metu.edu.tr
14. Mehpare Bilhan mehpare@metu.edu.tr
15. Tengiz Bokelavadze bokel71@yahoo.com
16. Ines Borges iborges@iscac.pt
17. Alexandre Borovik borovik@manchester.ac.uk
18. Ayşe Büte ayse.bute@stu.adu.edu.tr
19. Engin Büyükaşık enginbuyukasik@iyte.edu.tr
20. Vural Cam cvural@metu.edu.tr
21. Murat Cenk mcenk@metu.edu.tr
22. Pascale Charpin Pascale.Charpin@inria.fr
23. Kutay Cingiz
24. Şermin Çam
25. Münevver Çelik mucelik@metu.edu.tr
26. Fatih Çelik
27. Türkü Özlüm Çelik
28. Yasemin Çengellenmiş ycengellenmis@yahoo.com
29. Ayça Çeşmelioğlu cesmelioglu@sabanciuniv.edu
30. Ahmet Sinan Çevik sinan.cevik@selcuk.edu.tr
31. Gülen Çevik gulencevik@gmail.com
32. Büşra Çınar e147988@metu.edu.tr
33. Derya Çıray
34. Ömür Deveci odeveci36@hotmail.com
35. Uğur Doğan
36. Semra Doğruöz sdogruoz@adu.edu.tr
37. Yılmaz Durğun yilmazdurgun@iyte.edu.tr
38. Şükrü Uğur Efem suefem@sabanciuniv.edu
39. Özlem Ejder oejder@ku.edu.tr
40. Ceyhun Erdel
41. Vahap Erdoğdu erdogdu@itu.edu.tr
42. Arnaldo Garcia garcia@impa.br

43. Betül Gezer betulgezer@uludag.edu.tr
44. Pedro A. Guil paguil@um.es
45. Cem Güneri guneri@sabanciuniv.edu
46. Burçin Güneş
47. A. Dilek Güngör agungor@selcuk.edu.tr
48. Serpil Güngör serpilgungor@iyte.edu.tr
49. Sercan Gür
50. Erhan Gürel egurel@metu.edu.tr
51. Murat Güzeltepe mguzeltepe@sakarya.edu.tr
52. Sevgi Harman harman@itu.edu.tr
53. Wilfrid Hodges wilfrid.hodges@btinternet.com
54. Leyla Işık isikleyla@su.sabanciuniv.edu
55. Bahriye Karaca bahriyekaraca@gmail.com
56. Erdal Karaduman eduman@atauni.edu.tr
57. Mehmet İnan Karakuş minan@metu.edu.tr
58. Eylem Güzel Karpuz eguzel@balikesir.edu.tr
59. Canan Kaşıkcı canank@sabanciuniv.edu
60. Tariel Kemoklidze kemoklidze@gmail.com
61. Pınar Kılıçer pinarkilicer@gmail.com
62. Dilber Koçak dilber@metu.edu.tr
63. Fatih Koyuncu fatih@mu.edu.tr
64. Franz-Viktor Kuhlmann fvk@math.usask.ca
65. Hande Kul
66. Berke Kuru bkuru@hacettepe.edu.tr
67. Mahmut Kuzucuoğlu matmah@metu.edu.tr
68. Ömer Küçüksakallı komer@metu.edu.tr
69. Semih Laçin
70. V.M. Levchuk levchuk@lan.krasu.ru
71. James D. Lewis lewisjd@ualberta.ca
72. Christian Lomp clomp@fc.up.pt
73. Nazan Mahsereci
74. Gary McGuire gary.mcguire@ucd.ie
75. Wilfried Meidl wmeidl@sabanciuniv.edu
76. Engin Mermut engin.mermut@deu.edu.tr
77. Cem Mutlugün mutlugun@su.sabanciuniv.edu
78. Ahmet Nedim Narman annarman@bilgi.edu.tr
79. Azadeh Neman azadeh.neman@googlemail.com
80. Ali Derya Nesin
81. Pınar Ongan pinarongan@sabanciuniv.edu
82. Figen Öke figenoke@gmail.com
83. Hakan Özadam ozhakan@metu.edu.tr
84. Ferruh Özbudak ozbudak@metu.edu.tr
85. A. Çiğdem Özcan ozcan@hacettepe.edu.tr
86. Mehmet Özdemir mehmetozdemir@sabanciuniv.edu

87. Buket Özkaya buketo@sabanciuniv.edu
88. Neslihan Ayşen Özkirişçi aysen.1007@gmail.com
89. Daniel Panario daniel@math.carleton.ca
90. David Pierce dpierce@metu.edu.tr
91. Ata Fırat Pir atafirat@gmail.com
92. Özgür Deniz Polat polat@su.sabanciuniv.edu
93. Alexander Pott alexander.pott@ovgu.de
94. Peter Roquette roquette@uni-hd.de
95. Hans-Georg Rück rueck@mathematik.uni-kassel.de
96. Esengül Saltürk mathematicianesen@gmail.com
97. Mehmet Sarıyüce sariyuce@sabanciuniv.edu
98. Zülfükar Saygı zsaygi@etu.edu.tr
99. Elif Saygı esaygi@hacettepe.edu.tr
100. Ali Sinan Sertöz sertoz@bilkent.edu.tr
101. Sezgin Sezer sezgin@cankaya.edu.tr
102. Müfit Sezer sezer@fen.bilkent.edu.tr
103. Aslıhan Sezgin sezgin.nearring@hotmail.com
104. Amin Shokrollahi amin.shokrollahi@epfl.ch
105. Patrick Smith p.smith@maths.gla.ac.uk
106. Ebru Solak esolak@metu.edu.tr
107. Henning Stichtenoth henning@sabanciuniv.edu
108. Vedat Şiap vsiap@sakarya.edu.tr
109. Funda Taşdemir funda.tasdemir@bozok.edu.tr
110. Yasemin Taşyurdu yasemintasyurdu@hotmail.com
111. Kadriye Dilek Tefenlili
112. Eylem Toksoy eylemtoksoy@iyte.edu.tr
113. Alev Topuzoğlu alev@sabanciuniv.edu
114. Meral Tosun mtosun@gsu.edu.tr
115. Nesrin Tutaş ntutas@akdeniz.edu.tr
116. Seher Tutdere sehertutdere@su.sabanciuniv.edu
117. Erkan Murat Türkan
118. İnan Utku Türkmen turkmen@fen.bilkent.edu.tr
119. Özge Ülkem
120. Wolfgang Willems willems@ovgu.de
121. Arne Winterhof arne.winterhof@oeaw.ac.at
122. Fırat Yaşar
123. Hasret Yazarlı hyazarli@cumhuriyet.edu.tr
124. Dilek Pusat Yılmaz dilekyilmaz@iyte.edu.tr
125. Sergey Zyubin sergey.zyubin@gmail.com

Personnel

Meeting coordinator Alev Topuzoğlu (Sabancı)

Scientific committee Mahmut Kuzucuoğlu (METU), Ali Nesin (Bilgi), Sinan Sertöz (Bilkent), Henning Stichtenoth (Sabancı), Simon Thomas (Rutgers)

Organizing committee Ayşe Berkman (METU), Cem Güneri (Sabancı), David Pierce (METU), Henning Stichtenoth (Sabancı)

Booklet editor David Pierce

Acknowledgements

Hospitality Tivrona Tours

Venue Antalya Oteli, Lara Yolu, Antalya

Financial support TÜBİTAK (the Scientific and Technological Research Council of Turkey), the Turkish Mathematical Association, Sabancı University

Website `http://aad.metu.edu.tr/`

Short talks

Wednesday

	I	II
16:50	Gürel	Asar
17:10	Öke	
17:30	Özadam	Levchuk
17:50	Guil Asensio	

Thursday

14:20	Sezgin	Güzeltepe
14:40	Taşdemir	Çengellenmiş
15:00	Durğun	Şiap

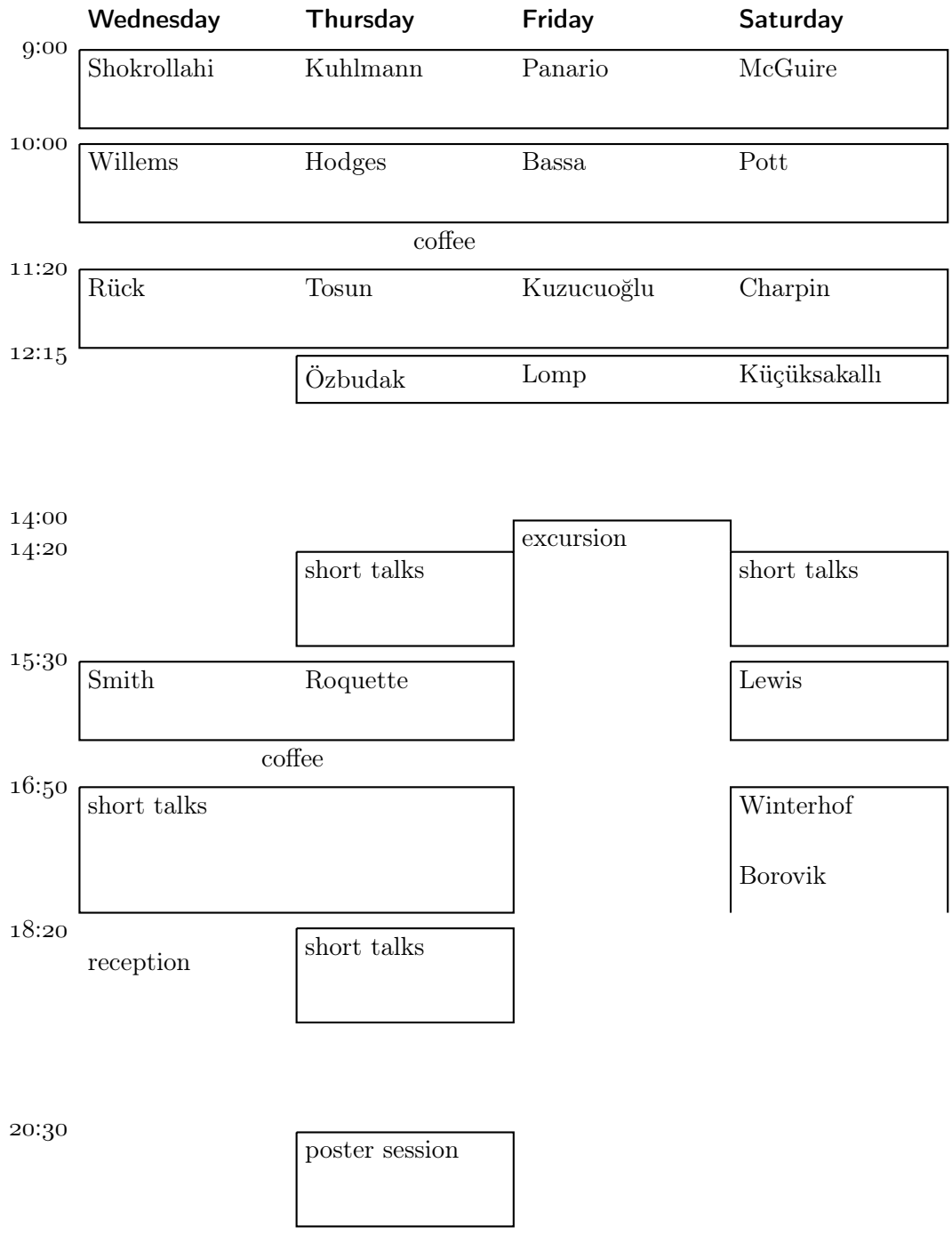
16:50	Bokelavadze	Gezer
17:10	Çevik	S. Güngör
17:30	Solak	Büyükaşık
17:50	Zyubin	Toksoy

18:20	Borges	Arıkan
18:40	Harman	Kemoklidze
19:00	Deveci	Mermut

Saturday

14:20	A. D. Güngör	Taşyurdu
14:40	Pusat-Yılmaz	Koyuncu
15:00	Karpuz	

Timetable


Wednesday
Thursday
Friday
Saturday
9:00
Shokrollahi
Kuhlmann
Panario
McGuire
10:00
Willems
Hodges
Bassa
Pott
coffee
11:20
Rück
Tosun
Kuzucuoğlu
Charpin
12:15
Özbudak
Lomp
Küçüksakallı
14:00
excursion
14:20
short talks
short talks
15:30
Smith
Roquette
Lewis
coffee
16:50
short talks
Winterhof
Borovik
18:20
reception
short talks
20:30
poster session