

ANTALYA ALGEBRA DAYS XVI
9-13 MAY 2014

FRIDAY, 9 MAY

09:30-10:30: Christophe Ritzenthaler (University Rennes 1)

How big is 4?

10:30-11:00: Coffee Break

11:00-12:00: Jennifer Balakrishnan (University of Oxford)

Coleman integration and integral points on hyperelliptic curves

12:00-13:50: Lunch Break

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

15:30-16:00: Coffee Break

16:00-17:00: Yves Aubry (Université de Toulon and Université Aix-Marseille)

Algebraic geometry and Abelian varieties over finite fields

17:00-18:00: Arzu Boysal (Boğaziçi Üniversitesi)

Bernoulli series and volumes of moduli spaces

18:30: Welcome gathering!

SATURDAY, 10 MAY

09:00-10:00: Christian Mauduit (Université Aix-Marseille)

Prime numbers, determinism and pseudorandomness

10:00-10:30: Coffee Break

10:30-11:30: Jonathan Jedwab (Simon Fraser University)

The structure of Costas arrays

11:30-12:30: Gerriet Martens (Universität Erlangen-Nürnberg)

The gonality sequence of an algebraic curve

12:30-14:00: Lunch Break

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

15:20-16:00: Coffee Break

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

SUNDAY, 11 MAY

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

10:30-11:00: Coffee Break

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

12:00-13:45: Lunch Break

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

MONDAY, 12 MAY

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

10:00-10:30: Coffee Break

10:30-11:30: Arne Winterhof (RICAM, Austrian Academy of Sciences)
Covering sets

11:30-12:30: Mercede Maj (Università degli Studi di Salerno)
Some recent results on small doubling problems in orderable groups

12:00-13:50: Lunch Break

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

15:30-16:00: Coffee Break

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

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

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

TUESDAY, 13 MAY

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

10:00-10:30: Coffee Break

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

WORKSHOPS

FRIDAY, 9 MAY

Combinatorics I:

13:50-14:10: Ş. Yazıcı

A polynomial embedding of pairs of orthogonal partial latin squares

14:10-14:30: F. Demirkale

Linearly independent latin squares

14:30-14:50: B. Özkaya

Multidimensional quasi-cyclic and convolutional codes

14:50-15:10: S. Özkan

The Hamilton - Waterloo problem with uniform cycle sizes

15:10-15:30: E. Kolotoğlu

On large sets of projective planes of orders 3 and 4

Lie Algebras:

13:50-14:10: H. Adimi

Index of Hom-Lie algebras by central extension

14:10-14:30: K. Dekkar

Cohomology and deformations of hom-bialgebras and hom-hopf algebras

14:30-14:50: I. Demir

On Leibniz algebras

14:50-15:10: N. S. Öğüşlü

The test rank of a soluble product of free abelian Lie algebras

SATURDAY, 10 MAY

Combinatorics II:

14:00-14:20: C. Çalışkan

New infinite families of 2-edge-balanced graphs

14:20-14:40: M. M. Tan

Generalized multipliers, Weil numbers and circulant weighing matrices

14:40-15:00: M. Taşkın

Tower tableaux

15:00-15:20: H. Topçu

On the spectral determination of some special graphs

Ring Theory I:

14:00-14:20: E. Albaş

Generalized derivations with some related conditions on Lie ideals

14:20-14:40: B. A. Saylam

Density theorems for rings of Krull type

14:40-15:00: C. Hatipgölu

Injective hulls of simple modules over differential operator rings

15:00-15:20: Ö. Özkan

Involution of structural matrix algebras

Module Theory:

16:00-16:20: P. Aydoğdu

G-Dedekind primeness of Morita context

16:20-16:40: Y. Alagöz

Strongly (non)cosingular modules

16:40-17:00: M. T. Akçin

Betti series of the universal modules of second order derivations

Number Theory I:

17:10-17:30: A. Özkoç ,

Pell form and Pell equation in terms of Oblong numbers

17:30-17:50: Y. Akbal

Piatetski Shapiro meets Chebotarev

17:50-18:10: O. Uzunkol

Smaller generators for some class fields

18:10-18:30: Ö. D. Polat

Factorization of places in coverings of algebraic curves

Algebraic Geometry I:

18:30-18:50: N. Şahin

Arf rings for singularities

MONDAY, 12 MAY

Group Theory I:

13:50-14:10: A. Arıkan

Zaitsev type results

14:10-14:30: A. Arıkan

Infinitely generated periodic groups

14:30-14:50: M. Bouchelaghem

Groups whose proper subgroups have polycyclic-by-finite conjugacy classes

14:50-15:10: M. Hamitouche

Some properties of a generalized 3-abelian groups

15:10-15:30: A. Souad

On minimal non-hypercentral groups

Number Theory II:

13:50-14:10: L. Işık

On the minimum distance of cyclic codes

14:10-14:30: S. Tutdere

Recursive Artin-Schreier towers of function fields over F_2

14:30-14:50: M. Cenk

On the fast computation of Toeplitz matrix vector products over F_2

14:50-15:10: N. Anbar

On quadratic functions and Artin-Schreier curves

Algebraic Geometry II:

15:10-15:30: A. Erdoğan

Canonical lifting of abelian varieties

Group Theory II:

18:10-18:30: V. Tolstykh

The small index property for relatively free algebras

18:30-18:50: İ. Tuvay

Brauer indecomposability of Scott modules of Park-type groups

Algebraic Geometry III:

18:10-18:30: A. Iezzi

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

Ring Theory II:

18:30-18:50: A. Koç

Representations of Leavitt and Cohn-Leavitt path algebras

18:50-19:10: S. Esin

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

Invited Talks

Algebraic geometry and Abelian varieties over finite fields

Yves Aubry

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

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

Université de Toulon and Aix-Marseille Université

email: yves.aubry@univ-tln.fr

Coleman integration and integral points on hyperelliptic curves

Jennifer S. Balakrishnan

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

University of Oxford

email: balakrishnan@maths.ox.ac.uk

web: <http://people.maths.ox.ac.uk/balakrishnan/>

Euclidean Number Fields and Euclidean Minima

Eva Bayer-Fluckiger

If a and b are two integers, with $b \neq 0$, then there exist two integers q and r such that $a = bq + r$, and that $|r| < |b|$. This so-called Euclidean division property plays a fundamental role in the arithmetic of the usual integers. It is natural to try to generalise this to more general rings, for instance rings of integers of algebraic number fields. This idea leads to the notions of Euclidean number

fields and Euclidean minima. Both are very classical topics of number theory. The aim of this talk is to survey old and new results concerning this subject, such as new Euclidean number fields and upper bounds for Euclidean minima. In particular, we will survey the history and recent developments concerning a classical conjecture of Minkowski.

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

Bernoulli series and volumes of moduli spaces

Arzu Boysal

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

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

email: arzu.boysal@boun.edu.tr

Motivic cohomology and algebraic cycles

William D. Gillam

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

Boğaziçi Üniversitesi email: wdgillam@gmail.com

Large Soluble Groups

Francesco de Giovanni

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

University of Napoli "Federico II"

email: degiovan@unina.it

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

The structure of Costas arrays

Jonathan Jedwab

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

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

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

This is joint work with J. Wodlinger.

Simon Fraser University, Canada

email: jed@sfu.ca

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

Graphs of Varieties Associated to Multiplicative or Additive Group Actions

Ali Ulaş Özgür Kışisel

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

Middle East Technical University

email: akisisel@metu.edu.tr

On rank and orbits in tensor products over finite fields

Michel Lavrauw

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

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

$$\tau = \sum_{i=1}^k v_{1i} \otimes \dots \otimes v_{mi} \quad (*)$$

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

- (E) Existence: given a tensor τ and an integer k , does there exist an expression of the form $(*)$?
- (U) Uniqueness: given an expression of the form $(*)$ for a tensor τ , is this expression essentially unique?
- (A) Algorithm: given a tensor τ and an integer k , does there exist an algorithm that decomposes τ into an expression of the form $(*)$ (in the case where it exists)?
- (O) Orbits: can we determine the number of orbits and describe the orbits of the natural group action of $\mathrm{GL}(V_1) \times \dots \times \mathrm{GL}(V_m)$ on $\bigotimes_{i=1}^m V_i$?

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

References

- [1] J. M. Landsberg. *Tensors: Geometry and Applications*. 2012. Graduate Studies in Mathematics, 128. American Mathematical Society, Providence, RI, 2012. xx+439 pp. ISBN: 978-0-8218-6907-9.
- [2] M. Lavrauw and J. Sheekey. Orbits of the stabiliser group of the Segre variety product of three projective lines. *Finite Fields Appl.* 26 (2014) 1–6.

- [3] M. Lavrauw, A. Pavan and C. Zanella. On the rank of $3 \times 3 \times 3$ -tensors. *Linear and Multilinear Algebra* (2013) 61 (5) 646–652.
- [4] M. Lavrauw. Finite semifields and nonsingular tensors. *Des. Codes Cryptogr.* (2013) 68 (1-3) 205–227.

Università degli Studi di Padova, Italy

email: michel.lavrauw@unipd.it

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

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

Patrizia Longobardi

Subsets of the set of the integers of the form

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

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

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

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

The Baumslag-Solitar groups are defined as follows:

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

where m, n are integers.

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

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

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

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

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

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

of $BS(1, 2)$.

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

References

- [1] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y. V. Stanchescu, Direct and inverse problems in Additive Number Theory and in non-abelian group theory, *European Journal of Combinatorics* 40 (2014) 42-54, to appear.
- [2] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y. V. Stanchescu, Inverse problems in Additive Number Theory and in Non-Abelian Group Theory, *arXiv:1303.3053* (2013), preprint, 1–31.
- [3] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y. V. Stanchescu, A small doubling structure theorem in a Baumslag- Solitar group, to appear.

Patrizia Longobardi, University of Salerno, Italy

email: plongobardi@unisa.it

Some recent results on small doubling problems in orderable groups

Mercede Maj

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

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

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

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

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

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

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

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

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

References

- [1] G. A. Freiman, Foundations of a structural theory of set addition. Translations of mathematical monographs, v. 37. American Mathematical Society, Providence, Rhode Island, 1973.
- [2] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Small doubling in ordered groups, *J. Australian Math. Soc.*, to appear.
- [3] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y. V. Stanchescu, Direct and inverse problems in Additive Number Theory and in non-abelian group theory, *European Journal of Combinatorics* 40C (2014), pp. 42-54.
- [4] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, A. Plagne and Y. V. Stanchescu, Small doubling - generators and structure, in preparation.

Mercede Maj, University of Salerno, Italy

email: mmaj@unisa.it

The gonality sequence of an algebraic curve

Gerriet Martens

For a smooth irreducible projective curve X defined over the complex numbers, let $d_r = d_r(X)$ denote the minimal degree of a linear series on X of dimension $r > 0$. These numbers form a strictly increasing sequence which is called the gonality sequence of X since d_1 is the gonality of X (i.e. the minimal number of sheets of a covering of X over \mathbb{P}^1). One expects a certain pattern in the growth of this sequence which, however, is violated for some families of curves with special moduli. In this talk I want to present some new results about such families.

Univ. Erlangen-Nürnberg

email: martens@mi.uni-erlangen.de

Prime numbers, determinism and pseudorandomness

Christian Mauduit

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

email: mauduit@iml.univ-mrs.fr

GIT and birational geometry of moduli spaces of curves

Ian Morrison

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

Fordham University

email: morrison@fordham.edu

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

How big is 4

Christophe Ritzenthaler

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

email: christophe.ritzenthaler@univ-rennes1.fr

Covering Sets

Arne Winterhof

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

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

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

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

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

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

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

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

References

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

RICAM, Austrian Academy of Sciences

email: `arne.winterhof@oeaw.ac.at`

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