Antalya Cebir Günleri VIII

www.math.metu.edu.tr/~antalya/

17–21 Mayıs 2006

Termessos

Antalya Algebra Days VIII

May 17–21, 2006

Contents

1 Welcome

It is a pleasure to welcome you to the Antalya Algebra Days (AAD) VIII.

Having begun as an informal meeting of approximately 40 mathematicians in 1999, AADs have evolved into meetings that most algebraists/number theorists in Turkey look forward to each year. We are particularly happy that many graduate students, more than one third of all the participants, have been attending the recent AADs. We largely owe the dynamic atmosphere in these meetings to the presence of our future colleagues.

Naturally one of the main aims of the AADs has been to provide a platform for enabling/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.

One person has taken active part in the organization of ALL the AADs. No doubt her invaluable efforts have been greatly appreciated by all others in organizing committees for all these years: thank you, Ayşe. David Pierce, who joined some years later, also receives gratitude for his dedication and expert handling of everything to do with the web and the book of abstracts.

Special thanks go to Tamer Koç and Şükran Demir of Tivrona Tours who have been able to meet our endless (and not always reasonable) wishes. We gratefully acknowledge the help provided this year, always with a smile, by graduate students Alp Bassa, Ayça Çeşmelioğlu and Canan Kaşıkçı.

TÜBİTAK (the Scientific and Technological Research Council of Turkey) has been the main sponsor of this event from the beginning. The Turkish Mathematical Society, Bilgi and Sabancı Universities also provided financial support this year. We thank them all.

We hope that you will have wonderful time here.

Alev Topuzoğlu for the Organizers of AAD VIII.

2 Schedule

May 17, Wednesday

09:30 – 09:40 Opening Remarks
09:40 – 10:30 **Stephen D. Cohen**
Existence theorems for generator polynomials over finite fields
10:30 – 11:00 Coffee Break
11:00 – 11:50 **Christian Lomp**
Non-singular coalgebras and copolyform modules
12:00 – 12:50 **James B. Carrell**
Singularities of Schubert and other Varieties with a torus action
12:50 – 14:30 Lunch Break
14:30 – 16:00 Parallel sessions
16:00 – 16:30 Coffee Break
16:30 – 18:00 **Özlem İmamoğlu**
Tutorial on Modular forms I
18:30 Welcome Gathering

May 18, Thursday

09:00 – 09:50 **Shuji Saito**
Noether-Lefschetz locus for Beilinson-Hodge cycles on open complete intersections
09:50 – 10:20 Coffee Break
10:20 – 11:10 **Stephen J. Pride**
Relative one-relator groups
11:20 – 12:10 **Michael Zieve**
Polynomial decomposition
12:10 – 16:30 Lunch Break (and Special Sessions)
16:00 – 16:30 Coffee
16:30 – 17:20 **Gilles Lachaud**
The Klein quartic: modular representation and reduction over finite fields
17:30 – 19:00 **Özlem İmamoğlu**
Tutorial on Modular forms II

May 19, Friday

09:00 – 09:50	**Tonny A. Springer**
	Exceptional Groups
09:50 – 10:20	Coffee Break
10:20 – 11:10	**Patrick Smith**
	Compressible and Related Modules
11:20 – 12:10	**K. İlhan İkeda**
	Multi-dimensional Langlands functoriality (after Kapranov)
12:10 – 14:00	Lunch Break
14:00 – 18:30	Excursion

May 20, Saturday

09:00 – 09:50	**Simeon Ball**
	Projective Planes and finite semifields
09:50 – 10:20	Coffee Break [postponed]
10:20 – 11:10	**James D. Lewis** [cancelled]
	Variants of the cycle class map
11:20 – 12:10	**Edmund Puczyłowski** [moved up]
	Some new results on Goldie dimension of modules and modular lattices
12:10 – 15:30	Lunch Break
15:30 – 17:00	Parallel sessions
17:00 – 17:30	Coffee Break
17:30 – 18:20	**Peter Roquette**
	Artin's conjecture on primitive roots in historical perspective

May 21, Sunday

08:45 – 09:35	**A. Sinan Sertöz**
	On $K3$ surfaces and lattices
09:45 – 10:35	**Patrick Solé**
	Four applications of $\mathbb{Z}_4$ codes
10:35 – 11:00	Coffee
12:30	Lunch

3 Parallel sessions

May 17, Wednesday

Session 1

14:30 – 14:55 **Bill Wickless**
A-solvable groups

15:00 – 15:25 **A. Sinan Çevik**
Minimal but inefficient presentations for semi-direct products of finite cyclic monoids

15:30 – 15:55 **Vladimir M. Levchuk**
Growth of the intersection of the centralizer of an involution and its class of conjugated elements in finite simple groups

Session 2

14:30 – 14:55 **Özer Öztürk**
Thom polynomials via Schur functions

15:00 – 15:25 **Alp Bassa**
A simple proof for the limit of the Bezerra–Garcia–Stichtenoth tower over cubic finite fields

15:30 – 15:55 **Nesrin Tutaş**
A generalization of the Weierstrass semigroup

May 20, Saturday

Session 1

15:30 – 15:55 **Emine Albaş**
Generalized derivations with Engel conditions on one-sided ideals

16:00 – 16:25 **S. Eylem Toksoy**
Amply cofinitely supplemented lattices

16:30 – 16:55 **Ali Madanshekaf** [cancelled]
On the Projective S-acts

Session 2

15:30 – 15:55 **Erol Serbest**
Generalized Fesenko reciprocity map: non-abelian local class field theory

16:00 – 16:25 **Pınar Mete**
Hilbert functions of Gorenstein monomial curves

16:30 – 16:55 **Şerban A. Basarab**
A new setting for the co-Galois theory

4 Special sessions

Sequences

May 18, Thursday, 14:30 - 16:30
Coordinator: Alev Topuzoğlu

Arne Winterhof
Comparison of complexity measures for binary sequences
Nina Brandstätter
On the linear complexity of Sidel'nikov–Lempel–Cohn–Eastman Sequences over $\mathbb{F}_d$
Wilfried Meidl
Generalized Marsaglia's lattice test and the linear complexity
Engin Özkan
On truncated Fibonacci sequences

Groups, Rings, Fields, Modules

(date and time to be announced)
Coordinators: Mahmut Kuzucuoğlu, Patrick Smith

Nurullah Ankaralıoğlu
Dunwoody Parameters $(1, 0, c, d-2)$ *and* $(1, b, 0, d-2)$
Gonca Ayık
(m, r)*-rank of finite full transformation semigroups*
Engin Büyükaşık
Totally weak supplemented modules over Dedekind domains
Semra Doğruöz
On the modules for which every submodule has a unique closure relative to a torsion theory
Müge Kanuni
Injectivity and related concepts in incidence algebras
Fatih Koyuncu
Irreducible polynomials by the polytope method over integral domains
Engin Mermut
c-injective modules over Dedekind domains
Dilek Pusat-Yılmaz
Modules over Prüfer domains which satisfy the radical formula

Open Problems in Ring Theory

(date and time to be announced)
Coordinator: Patrick Smith

Christian Lomp
Edmund Puczyłowski
Patrick Smith

5 Abstracts

Talks

Generalized Derivations with Engel Conditions on One-Sided Ideals

E.Albaş

This is joint work with N. Argaç (Ege University, Science Faculty, Department of Mathematics, 35100, Bornova, İzmir, nurcan.argac@ege.edu.tr) and V. De Filippis (Dipartimento di Matematica, Universita di Messina Salita Sperone 31, 98166 Messina, ITALIA, defilippis@unime.it).

Let R be a noncommutative prime ring and I a nonzero left deal of R. Let g be a generalized derivations of R such that $[g(x^k), x^k]_n = 0$ for all $x \in I$, where k, n are fixed positive integers. Then there exists $c \in U$, the left Utumi quotient ring of R, such that $g(x) = xc$ and $I(c - \gamma) = 0$ for a suitable $\gamma \in C$. In particular we have that $g(x) = \alpha x$, for all $x \in I$ and a suitable $\alpha \in C$.

Throughout this paper, R is always a prime ring with center $Z(R)$, extended centroid C, left Utumi quotient ring U, and two sided Martindale quotient ring Q. For any $x, y \in R$, we set $[x, y]_1 = [x, y] = xy - yx$ and $[x, y]_n = [[x, y]_{n-1}, y]$ for $n > 1$. Recall that a ring R is prime if $xRy = 0$ implies $x = 0$ or $y = 0$.

An additive mapping $d : R \to R$ is called derivation if $d(xy) = d(x)y + xd(y)$ holds for all $x, y \in R$. The study of derivations of prime rings was initiated by Posner [5]. He proved that if R is a prime ring and d is a nonzero commuting derivation of R, i.e., $[d(x), x] = 0$ for all $x, y \in R$, then R is commutative. Later in [2] C. Lanski generalized this result to one-sided ideals as follows: Let R be a prime ring with derivation d, I a left ideal of R, and k, n two positive integers. Suppose $[d(x^k), x^k]_n = 0$ for all $x \in I$. Then either $d = 0$ or R is commutative.

Many authors have studied generalized derivations in the context of prime and semiprime rings (see [3], [1, 4]). By a generalized derivation on R one usually means an additive map $g : R \to R$ such that, for any $x, y \in R$, $g(xy) = g(x)y + xd(y)$, for some derivation d in R. Obviously any derivation is a generalized derivation. Moreover, other basic examples of generalized derivations are the following: (i) $g(x) = ax + xb$, for $a, b \in R$; (ii) $g(x) = ax$, for some $a \in R$.

By motivating above results we shall prove the following theorem.
Theorem 1. . *Let R be a noncommutative prime ring with a nonzero ideal I. Let g be a generalized derivation of R such that $[g(x^k), x^k]_n = 0$ for all $x \in I$, where k, n are fixed positive integers. Then there exists $c \in U$, the Utumi quotient ring of R, such that $g(x) = xc$ and $I(c - \gamma) = 0$ for a suitable $\gamma \in C$. In particular $g(x) = \alpha x$, for all $x \in I$ and a suitable $\alpha \in C$.*

References

[1] B. Hvala, generalized derivationsin eings, Comm. Algebra 26(4)(1998), 1147-1166

[2] C. Lanski, An Engel condition with derivation for left ideals, Proc. Amer. Math. Soc., 125(2), (1997), 339-345.

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

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

[5] E. C. Posner, Derivations in prime rings, Proc. Amer. Math. Soc. 8(1957), 193-1100.

Ege University, Science Faculty, Department of Mathematics, 35100, Bornova, İzmir

email: emine.albas@ege.edu.tr

Dunwoody Parameters $(1, 0, c, d-2)$ and $(1, b, 0, d-2)$

Nurullah Ankaralıoğlu

We have shown in this paper that cyclically presented groups obtained by using the words w constituted as connected with Dunwoody parameters both $(1, 0, c, d-2)$ and $(1, b, 0, d-2)$ have the same cyclic presentations when b, c are odd positive integers and $d = 2a + b + c$.

The results presented in my talk have been obtained in collaboration with Hüseyin Aydın.

References

[1] Cavicchioli, A., Hegenbarth, F., Kim, A.C., A Geometric study of Sieradski Groups, Algebra Colloquim, 1998; 5: 203-217.

[2] Dunwoody, M.J.,. Cyclic Presentations and 3-Manifolds. In Proc. Inter Conf., Groups Korea'94, Walter De Gruyter, Berlin, New York, 1995; 47-55.

[3] Graselli, L., Mulazzani, M. Genus one 1-bridge knots and Dunwoody manifolds. Forum Math. Proc. Camb Philos. Soc. 1999;125: 5169-5206.

[4] Gultekin, I., Cyclic Presentations and Cyclically Presented Groups. Ph.D.Thesis, Ataturk University, 2002.

[5] Johnson, D.L., Presentations of Groups. Cambridge University Press,1990.

[6] Cavichioli, A., Ruini, B., Spaggiari,F., On a Conjecture of M. J. Dunwoody. Algebra colloq., 2001; 8: 169-218.

Atatürk Üniversitesi

email: ankarali@atauni.edu.tr

(m, r)-Rank of Finite Full Transformation Semigroups

Gonca Ayık

Let T_n be the full transformation semigroup, which is a semigroup of all self maps of the finite set $X_n = \{1, 2, \ldots, n\}$ and let $ST_n = T_n \setminus S_n$ be the semigroup of all singular self maps of the finite set X_n. In this talk we first introduce concept of (m, r)-path-cycle. By means of (m, r)-path-cycle, (m, r)-rank of ST_n is defined to be

$$\min\{|A| : \langle A\rangle = ST_n \text{ and } A \text{ consists of } (m, r)\text{-path-cycles }\}.$$

For $2 \leq r \leq n$, it is shown that (m, r)-rank of ST_n is $\frac{n(n-1)}{2}$. Thus the rank, idempotent rank and (m, r)-rank of ST_n are all the same.

Finally we turn our attention to the semigroup

$$O_n = \{\alpha \in ST_n : (\forall x, y \in X_n)x \leq y \Rightarrow x\alpha \leq y\alpha\}$$

of all order-preserving singular self maps X_n. O_n is generated by (m, m)-path--cycles if and only if $m \leq \frac{(n+2)}{2}$.

The results presented in my talk have been obtain in collaboration with Hayrullah Ayık, Yusuf Ünlü (Çukurova University) and John M. Howie (University of St Andrews).

Çukurova University

email: agonca@cu.edu.tr

web: http://math.cu.edu.tr/goncagungor/gonca.htm

Projective planes and finite semifields

Simeon Ball

A *projective plane* is a pair $(\mathcal{P}, \mathcal{L})$ where $\mathcal{P}$ is a set and $\mathcal{L}$ is a set of subsets of $\mathcal{P}$ with the property that for any two elements of $\mathcal{P}$ there is exactly one element of $\mathcal{L}$ containing both and for any two elements of $\mathcal{L}$ there is exactly one element of $\mathcal{P}$ belonging to both subsets.

If we ignore the degenerate example, $\mathcal{L} = \{\mathcal{P} \setminus \{x\}, \{x, y\} \mid y \in \mathcal{P} \setminus \{x\}\}$, then it is a simple consequence of the definition that a finite projective plane has an order n, where every element of $\mathcal{L}$ contains $n + 1$ elements, every element of $\mathcal{P}$ belongs to $n + 1$ elements of $\mathcal{L}$ and $|\mathcal{P}| = |\mathcal{L}| = n^2 + n + 1$.

Normally we talk about the elements of $\mathcal{P}$ as points and the elements of $\mathcal{L}$ as lines. The dual of a projective plane $(\mathcal{P}, \mathcal{L})$ of order n, where as points we take the elements of $\mathcal{L}$ and as lines we take, for each $x \in \mathcal{P}$, the subset of lines that contain x, is also a projective plane of order n.

Two projective planes are *isomorphic* if there is a bijection between the points which induces a bijection on the lines.

All known finite projective planes have prime power order. We can construct a projective plane of order q^h from any partition of the non-zero vectors of $\mathbb{F}_q^{2h}$. Projective planes constructed in this way are called *translation planes*. The dual of a translation plane is a translation plane if and only if the plane can be coordinatised by a finite pre-semifield.

A *finite pre-semifield* is a finite set S with two operations, addition $(+)$ and multiplication $(\circ)$, such that $(S, +)$ is an additive group, both distributive laws hold and

$$x \circ y = 0 \text{ implies } x = 0 \text{ or } y = 0.$$

A pre-semifield can be used to coordinatise a projective plane of order $|S|$ and we are interested in finding pre-semifields that produce non-isomorphic projective planes. Two pre-semifields are said to be *isotopic* if they coordinatise isomorphic planes. A *semifield* is a pre-semifield that has a multiplicative identity. There is always a semifield isotopic to any pre-semifield.

In this talk I shall present some different ways to construct semifields and survey all the known examples.

Universitat Politènica de Catalunya, Barcelona, Spain

email: simeon@mat.upc.es

web: http://www-ma4.upc.edu/~simeon/

A new setting for co-Galois theory

Şerban A. Basarab

The so called *co-Galois theory* is a more or less recent development [10, 5, 3, 4, 1] of the study of finite radical extensions, carried out by Besicovitch [9], Mordell [12], Siegel [14], Kneser [11] and Schinzel [13], among others. Roughly speaking, co-Galois theory investigates field extensions, finite or not, which possess a co-Galois correspondence. This theory is somewhat dual to the very classical *Galois theory* dealing with field extensions possessing a Galois correspondence.

A topological and group theoretical approach of co-Galois theory is initiated in the recent papers [7, 2]. Given a profinite group Γ and a quasi-cyclic discrete group A, on which Γ acts continuously, several classes of closed subgroups of Γ, and related classes of subgroups of the cocycle group $Z^1(\Gamma, A)$, called *radical, hereditarily radical, Kneser, hereditarily Kneser* and *co-Galois*, are defined and investigated.

The idea to involve the group $Z^1(\Gamma, A)$ in defining the abstract concepts mentioned above comes from the description due to Barrera-Mora, Rzedowski--Calderón, and Villa-Salvador [5], via Hilbert's Theorem 90, of the Cogalois group $\mathrm{Cog}(E/F)$ of an arbitrary Galois extension E/F as a group of cocycles. More precisely, $\mathrm{Cog}(E/F)$, the torsion subgroup of the multiplicative factor group E^*/F^*, is canonically isomorphic to the group $Z^1(\mathrm{Gal}(E/F), \mu(E))$ of all continues 1-cocycles of the profinite Galois group $\mathrm{Gal}(E/F)$ of the extension E/F with coefficients in the discrete quasi-cyclic group $\mu(E)$ of all roots of unity in E. A more general approach concerning regular (in von Neumann sense) commutative Galois algebras over fields is sketched in [6].

The above description of $\mathrm{Cog}(E/F)$ in terms of 1-cocycles naturally suggests to study the abstract setting of subgroups of groups of type $Z^1(\Gamma, A)$, with Γ an arbitrary profinite group and A any subgroup of $\mathbb{Q}/\mathbb{Z}$ such that Γ acts continuously on the discrete group A. Such a continuous action establishes through the evaluation map $\Gamma \times Z^1(\Gamma, A) \longrightarrow A$, $(\sigma, g) \mapsto g(\sigma)$, a Galois connection between the lattice $\mathbb{L}(Z^1(\Gamma, A))$ of all subgroups of $Z^1(\Gamma, A)$ and the lattice $\mathbb{L}(\Gamma)$ of all closed subgroups of Γ. As the lattices above are naturally equipped with spectral topologies on which the profinite group Γ acts continuously, this Galois connection relates them through canonical continuous Γ-equivariant maps.

On the other hand, the continuous action of Γ on A endows the dual group $Z^1(\Gamma, A)^\vee = \mathrm{Hom}(Z^1(\Gamma, A), \mathbb{Q}/\mathbb{Z})$ with a natural structure of topological Γ-module, related to Γ through a canonical continuous cocycle $\eta : \Gamma \longrightarrow Z^1(\Gamma, A)^\vee$ which plays a key role in the study of the classes of groups above. Moreover this cocycle is the starting point of a very recent project of the author concerning a still more general setting for co-Galois theory. In this more general approach, the main object of study is the natural Galois connection between the topological lattice of closed subgroups of a given profinite group Γ and the topological lattice of quotients of a profinite Γ operator group G, induced by a continuous cocycle $\eta : \Gamma \longrightarrow G$ with the property that the profinite group G is topologically generated by $\eta(\Gamma)$. In particular, we can take $G = \Omega_{\Gamma,\mathcal{C}}$, the universal pro-$\mathcal{C}$ Γ operator group generated by Γ, and $\eta = \omega_{\Gamma,\mathcal{C}}$, the corresponding universal cocycle, where $\mathcal{C}$ is an almost full class of finite groups. The work is in progress, and basic notions and partial results are contained in [8].

References

[1] T. Albu, "*Cogalois Theory*", A Series of Monographs and Textbooks, Vol. 252, Marcel Dekker, Inc., New York and Basel, 2002, 368 pp.

[2] T. Albu and Ş.A. Basarab, *An abstract Cogalois Theory for profinite groups*, J. Pure Appl. Algebra **200** (2005), 227-250.

[3] T. Albu and F. Nicolae, *Kneser field extensions with Cogalois correspondence*, J. Number Theory **52** (1995), 299-318.

[4] T. Albu and F. Nicolae, *Finite radical field extensions and crossed homomorphisms*, J. Number Theory **60** (1996), 291-309.

[5] F. Barrera-Mora, M. Rzedowski-Calderón, and G. Villa-Salvador, *On Cogalois extensions*, J. Pure Appl. Algebra **76** (1991), 1-11.

[6] Ş.A. Basarab, *Actions on Stone spaces and co-Galois groups*, Antalya Algebra Days V, 28 May-1 June 2003.

[7] Ş.A. Basarab, *Kneser and hereditarily Kneser subgroups of a profinite group*, Serdica Math. J. **30** (2004), 325-348.

[8] Ş.A. Basarab, *A new setting for co-Galois Theory, I: Universal cocycles and Kneser structures*, preprint 2006.

[9] A.S. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. **15** (1940), 3–6.

[10] C. Greither and Harrison, *A Galois correspondence for radical extensions of fields*, J. Pure Appl. Algebra **43**(1986), 257-2.

[11] M. Kneser, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. **26** (1975), 307-308.

[12] L.J. Mordell, *On the linear independence of algebraic numbers*, Pacific J. Math. **3** (1953), 625–630.

[13] A. Schinzel, *On linear dependence of roots*, Acta Arithmetica **28**(1975), 161-175.

[14] C.L. Siegel, *Algebraische Abhängigkeit von Wurzeln*, Acta Arithmetica **21**(1972), 59-64.

A simple proof for the limit of the Bezerra–Garcia–Stichtenoth tower over cubic finite fields

Alp Bassa

Let F be an algebraic function field of one variable with the finite field $\mathbb{F}_\ell$ as its full field of constants. Let g be the genus of F and denote by $N(F)$ the number of $\mathbb{F}_\ell$-rational places of F. The Hasse–Weil bound gives an upper bound for $N(F)$ in terms of g and ℓ. This bound is not optimal, when the genus is large compared to the cardinality of the finite field, see [6, 7]. To study the asymptotic behavior with increasing genus, let $N_\ell(g)$ be the maximal number of $\mathbb{F}_\ell$-rational places that a function field over $\mathbb{F}_\ell$ of genus g can have. It was shown by Drinfel'd and Vlăduţ [2], that

$$A(\ell) := \limsup_{g\to\infty} \frac{N_\ell(g)}{g} \leq \sqrt{\ell} - 1.$$

If ℓ is a square (an even power of a prime), then the above inequality is in fact an equality; i.e., $A(\ell) = \sqrt{\ell} - 1$, see [6, 10].

If ℓ is not a square, not much is known about the exact value of $A(\ell)$. Using class field towers, Serre [8, 9] showed that there exists a constant $c > 0$, which is independent of ℓ, such that $A(\ell) \geq c \cdot \log \ell > 0$ for all ℓ.

Using degenerations of Shimura modular surfaces, Zink [11] showed that

$$A(p^3) \geq \frac{2(p^2-1)}{p+2},$$

if p is a prime number.

In [5], van der Geer and van der Vlugt gave an *explicit* example of a tower $\mathcal{E} = (E_n)_{n\geq 0}$ over the finite field with eight elements, with limit

$$\lambda(\mathcal{E}) := \lim_{n\to\infty} \frac{N(E_n)}{g(E_n)} = \frac{3}{2},$$

which attains Zink's lower bound for $p = 2$.

Zink's lower bound was generalized by Bezerra, Garcia and Stichtenoth [1] to arbitrary cubic finite fields. This was done by providing an explicit tower of function fields $\mathcal{F} = (F_n)_{n\geq 0}$ over the finite field $\mathbb{F}_\ell$, where $\ell = q^3$ for an arbitrary prime power q, with limit

$$\lambda(\mathcal{F}) = \lim_{n\to\infty} \frac{N(F_n)}{g(F_n)} \geq \frac{2(q^2-1)}{q+2}.$$

This tower is recursively given as follows: $F_0 = \mathbb{F}_\ell(x_0)$ and $F_{i+1} = F_i(x_{i+1})$ for $i \geq 0$, where

$$\frac{1 - x_{i+1}}{x_{i+1}^q} = \frac{x_i^q + x_i - 1}{x_i}. \qquad (*)$$

We call the tower $\mathcal{F}$, which is defined by Equation $(*)$ the Bezerra–Garcia–Stichtenoth tower (BGS tower for short). The case $q = 2$ corresponds to the van

der Geer–van der Vlugt tower. The case $q > 2$ is substantially different. In this case the extensions F_{i+1}/F_i $(i \geq 0)$ are not even Galois.

Determining the limit of a tower usually involves a lot of technical computations. Recently, Garcia and Stichtenoth showed how these computations could be avoided in some Artin–Schreier towers and their Galois closures (see [3, 4]). Unfortunately, this method is not directly applicable to the Bezerra–Garcia–Stichtenoth tower over cubic finite fields, since in this tower the steps are not even Galois. In this talk, I will explain how their idea can still be used in this case to simplify the proof of the limit of the tower and to obtain the limit of the Galois closure of the tower.

References

[1] J. Bezerra, A. Garcia, H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound for $A(q^3)$*, J. Reine Angew. Math. **589**, pp. 159-199, 2005.

[2] V. G. Drinfel'd, S. G. Vlăduţ, *The number of points of an algebraic curve*, Func. Anal. **17**, pp. 53-54, 1983.

[3] A. Garcia, H. Stichtenoth, *Some Artin–Schreier towers are easy*, Mosc. Math. J., to appear.

[4] A. Garcia, H. Stichtenoth, *On the Galois closure of towers*, preprint 2005.

[5] G. van der Geer, M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34**, pp. 291-300, 2002.

[6] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28**, pp. 721-724, 1981.

[7] Y. I. Manin, *What is the maximum number of points on a curve over $\mathbb{F}_2$?* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28**, pp. 715-720, 1981.

[8] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris **296**, pp. 397-402, 1983.

[9] J.-P. Serre, *Rational points on curves over finite fields*, unpublished lecture notes by F. Q. Gouvêa, Harvard University, 1985.

[10] M. A. Tsfasman, S. G. Vlăduţ, T. Zink, *Modular Curves, Shimura curves, and Goppa codes, better than the Varshamov–Gilbert bound*, Math. Nachr. **109**, pp. 21-28, 1982.

[11] T. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, in Fundamentals of Computation Theory (L. Budach, ed.), Lecture Notes in Computer Science, Vol. **199**, Springer Verlag, Berlin, pp. 503-511, 1985.

Universität Duisburg-Essen

email: alp.bassa@uni-duisburg-essen.de

On the linear complexity of Sidel'nikov–Lempel–Cohn–Eastman Sequences over $\mathbb{F}_d$

Nina Brandstätter

(Joint work with W. Meidl)

For an odd prime power q let $\mathbb{F}_q$ be the finite field of order q and let d be a prime divisor of $q-1$. The *cyclotomic classes of order d* give a partition of $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ defined by

$$D_0 := \{\alpha^{dn} \ : \ 0 \le n \le (q-1)/d - 1\} \quad \text{and} \quad D_j := \alpha^j D_0, \ 1 \le j \le d-1,$$

for a primitive element α of $\mathbb{F}_q^*$.
In [5] Sidel'nikov introduced the $q-1$-periodic sequence $S = s_0, s_1, \ldots$ with terms in $\mathbb{F}_d$ defined by

$$\begin{aligned} s_n &= j \quad \Leftrightarrow \quad \alpha^n + 1 \in D_j, \quad n = 0, \ldots, q-2, n \neq (q-1)/2, \\ s_{(q-1)/2} &= 0, \quad \text{and} \\ s_{n+q-1} &= s_n, \quad n \ge 0. \end{aligned} \tag{$\dagger$}$$

S is called the Sidel'nikov–Lempel–Cohn–Eastman (SLCE-)sequence. It was independently introduced by Lempel, Cohn and Eastman [3] for the case $d = 2$.

We are going to investigate the linear complexity $L(S)$ of S, which provides information on the predictability of the sequence. A high linear complexity is a desirable feature for sequences used for cryptographic purposes.

We present a technique for determining the linear complexity of sequences of the form (†). Roughly speaking, we can determine the exact linear complexity whenever we know the value of certain cyclotomic numbers and the factorization of $X^{q-1} - 1$ over $\mathbb{F}_d$.

We deduce a good lower bound on the linear complexity of sequences of the form (†) for several classes of period length. Furthermore, we obtain exact results on the linear complexity of the ternary SLCE-sequences (d=3).

The case $d = 2$ (binary SLCE-sequences) was studied by Helleseth and Yang [1], Kyureghyan and Pott [2], and Meidl and Winterhof [4].

References

[1] T. Helleseth and K. Yang, On binary sequences with period $n = p^m - 1$ with optimal autocorrelation, In (T. Helleseth, P. Kumar, and K. Yang, eds.), Proceedings of SETA 01, (2002), 209–217.

[2] G. M. Kyureghyan and A. Pott, On the linear complexity of the Sidelnikov–Lempel–Cohn–Eastman sequences, Designs, Codes, and Cryptography 29 (2003), 149–164.

[3] A. Lempel, M. Cohn, and W. L. Eastman, A class of balanced binary sequences with optimal autocorrelation properties. IEEE Trans. Inf. Th. 23 (1977), 38–42.

[4] W. Meidl and A. Winterhof, Some notes on the linear complexity of Sid'elnikov–Lempel–Cohn–Eastman sequences, Designs, Codes, and Cryptography 38 (2006), 159–178.

[5] V. M. Sidel'nikov, Some k-valued pseudo-random sequences and nearly equidistant codes. Problems of Information Transmission 5 (1969), 12–16.; translated from Problemy Peredači Informacii 5 (1969), 16–22 (Russian).

Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences

email: nina.brandstaetter@oeaw.ac.at

web: http://www.ricam.oeaw.ac.at

Totally Weak Supplemented Modules over Dedekind Domains

Engin Büyükaşık

A module M is *supplemented*, if every submodule N of M has a *supplement*, i.e. a submodule K minimal with respect to $N+K=M$. K is a supplement of N in M if and only if $N+K=M$ and $N\cap K\ll K$. If $N+K=M$ and $N\cap K\ll M$, then K is called a *weak supplement* of N. M is a *weakly supplemented* module if every submodule of M has a weak supplement in M. M is called a *totally weak supplemented* module if every submodule of M is weakly supplemented.

Supplemented modules over Dedekind domains characterized by Zöschinger in [4 , Theorem 2.4 and Theorem 3.1]. A characterization of weakly supplemented modules over commutative noetherian rings with finite Krull dimension is given by Rudlof in [2, Theorem 3.5].

In this work we study totally weak supplemented modules over Dedekind domains. Let R be a Dedekind domain and M be an R-module.
If R is semilocal then M is totally weak supplemented if and only if M is weakly supplemented. If R is non-semilocal then M is totally weak supplemented if and only if M is supplemented.
For torsion R-modules the classes of supplemented, weakly supplemented and totally weak supplemented modules coincide.

References

[1] C. Lomp, On semilocal modules and rings, Communications in Algebra 27-4(1999), 1921-1935.

[2] P. Rudlof, On the structure of couniform and complemented modules, Journal of Pure and Applied Algebra, 74(1991), 281-305.

[3] P. Rudlof, On minimax and related modules, Can. J. Math, 44-1(1992), 154-166.

[4] H. Zöschinger, Komplementierte moduln über Dedekindringen, Journal of Algebra, 29(1974), 42-56.

[5] H. Zöschinger, Invarianten wesentlicher überdeckungen, Math. Annalen, 237(1978), 193-202.

[6] H. Zöschinger, Minimax-moduln, Journal of Algebra, 102(1986), 1-32.

Izmir Institute of Technology

email: enginbuyukasik@iyte.edu.tr

Singular Loci of Schubert and Other Varieties with a Torus Action

Jim Carrell

We will give a survey of the state of knowledge about the singular loci of Generalized Schubert varieties and certain other varieties in a algebraic homogeneous space G/P which are invariant under a maximal torus T in G (here G denotes a linear algebraic group over an algebraically closed field and P is a parabolic subgroup). In particular we will discuss some joint work with Jochen Kuttler motivated by the technique of using Peterson varieties to study the linear span of the reduced tangent cone to a Schubert variety at a fixed point of T.

University of British Columbia

email: carrell@math.ubc.ca

web: http://www.math.ubc.ca/~carrell/carrell.html

Minimal but inefficient presentations for semi-direct products of finite cyclic monoids

A. Sinan Çevik

Let A and K be arbitrary two monoids. For any connecting monoid homomorphism $\theta : A \longrightarrow End(K)$, let $M = K \rtimes_\theta A$ be the corresponding monoid semi-direct product. In [2], Cevik discussed necessary and sufficient conditions for the standard presentation of M to be efficient (or, equivalently, p-Cockcroft for any prime p or 0), and then, as an application of this, the author showed the efficiency for the presentation, say $\mathcal{P}_M$, of the semi-direct product of any two finite cyclic monoids.

As a main tool of this talk, I will give sufficient conditions for $\mathcal{P}_M$ to be *minimal* but not *efficient*. To do that the same method in [2] will be used.

References

[1] H. Ayık, C.M. Campbell, J.J. O'Connor and N. Ruškuc, *Minimal presentations and efficiency of semigroups*, Semigroup Forum, **60** (2000), 231-242.

[2] A.S. Çevik, *Minimal but inefficient presentations of the semi-direct products of some monoids*, Semigroup Forum, **66** (2003), 1-17.

[3] J.M. Howie, *Fundamentals of Semigroup Theory*, Oxford University press, 1995.

[4] M. Lustig, *Fox ideals, $\mathcal{N}$-torsion and applications to groups and 3-monifolds*, in *Two-dimensional homotopy and combinatorial group theory* (C. Hog-Angeloni, W. Metzler and A.J. Sieradski, editors), Cambridge University Press, 219-250 (1993).

[5] S.J. Pride, *Geometric methods in combinatorial semigroup theory*, Semigroups, Formal Languages and Groups, (J.Fountain editor), Kluwer Academic Publishers, 215-232 (1995).

[6] S.J. Pride, *Low-dimensional homotopy theory for monoids*, Int. J. Algebra and Comput., **5**(6) (1995), 631-649.

[7] N. Ruskuc, *Semigroup Presentations*, Ph.D Thesis, University of St. Andrews, 1996.

[8] C.C. Squier, *Word problems and a homological finiteness condition for monoids*, Journal of Pure and Appl. Algebra, **49** (1987), 201-216.

[9] J. Wang, *Finite derivation type for semi-direct products of monoids*, Theoretical Computer Science, (**191**) 1-2, (1998), 219-228.

Balikesir Universitesi, Fen-Edebiyat Fakultesi,
Cagis Kampusu, Matematik Bolumu, 10145 Balikesir/Turkey

web: `http://w3.balikesir.edu.tr/~scevik/`

email: `scevik@balikesir.edu.tr`

Existence theorems for generator polynomials over finite fields

Stephen D. Cohen

A *generator polynomial* is simply an irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ whose roots $\mathcal{R}_f = \{\gamma, \gamma^q, \ldots, \gamma^{q^{n-1}}\}$ generate the extension $\mathbb{F}_{q^n}$ in a natural way. These include:

- *irreducible polynomials* themselves: $\mathbb{F}_{q^n} = \mathbb{F}_q(\gamma)$;
- *primitive polynomials*: γ is a generator (*primitive element*) of the cyclic multiplicative group $\mathbb{F}_{q^n}^*$;
- *normal polynomials*: $\mathcal{R}_f$ is a basis (*normal basis*) of $\mathbb{F}_{q^n}/\mathbb{F}_q$.

A survey will be given of various recent existence theorems on generator polynomials with a stress on results that are complete and unconditional. These include:

- the existence of irreducible polynomials in residue classes (a type of *Dirichlet's theorem*);
- irreducible polynomials with a prescribed coefficient;
- the Primitive Normal Basis and Strong Primitive Normal Basis theorems;
- primitive normal polynomials with prescribed norm and trace;
- primitive polynomials with a prescribed coefficient.

The broad sweep of these results should be easily comprehensible. Throughout the course of the description, a brief account will also be given of some key features of the method used to tackle existence questions for primitive and/or normal polynomials. These include:

- character sum expressions and estimates;
- a sieving technique based on the *order* (additive or multiplicative) of $\gamma \in \mathbb{F}_{q^n}$;
- a p-adic method for specifying coefficients of a polynomial.

Glasgow and Bristol

email: sdc@maths.gla.ac.uk

On the modules for which every submodule has a unique closure relative to a torsion theory

Semra Doğruöz

This is joint work with Meral Arnavut (Department of Mathematics, University of Fredonia, SUNY). In this work we consider unital right modules over general associative rings with identity. A module M is called a *UC-module* if every submodule of M has a unique closure in M ("UC" for "unique closure"). In 1993, Patrick F.Smith [5] and in 1995 Zelmanowitz [6] gave necessary and sufficient conditions for a module to be a UC-module. For a hereditary torsion theory τ and a module M every submodule of M is τ-essential in a τ-closed submodule of M. As an analogue of UC-modules, we investigate τ-UC-modules here and give necessary and sufficient conditions for a module to be a τ-UC-module. A module M is called *τ-UC-module* if every submodule of M has a τ-closure in M and unique.

References

[1] Anderson, F.W., Fuller, K.R.: Rings and categories of modules, Springer-Verlag: New York, (1974).

[2] Doĝruöz, S.: Classes of extending modules associated with a torsion theory, submitted to Rocky Mountain Journal of Mathematics (2005).

[3] Dung, N.V., Huynh, D.V., Smith, P.F., Wisbauer, R.: Extending modules, Longman, Harlow, (1994).

[4] Goodearl, K.R.; Warfield, R.B.: An introduction to noncomutative Noetherian rings. London Math. Society Student Texts 16 (1989).

[5] Smith, P.F.: Modules for which every submodule has unique closure, in Ring Theory, Wold Scientific, Singapore (1993), 302-313.

[6] Zelmanowitz J.M.: A class of modules with semisimple behavior, A. Facchini and C.Menini (eds.), Abelian Groups and Modules, 491-500, (1995), Kluwer Academic Publishers.

Department of Mathematics, Afyon Kocatepe University

email: dogruoz@aku.edu.tr

Multi-dimensional Langlands Functoriality (after M. M. Kapranov)

K. Ilhan Ikeda

To motivate our talk, let K denote the imaginary quadratic number field $\mathbb{Q}(i) = \{\alpha+\beta i \in \mathbb{C} : \alpha, \beta \in \mathbb{Q}\}$. A well-known result of Gauß states that prime numbers p satisfying $p \equiv 1 \pmod 4$ splits completely in the ring of integers $O_K = \mathbb{Z}[i]$ of K. For example, the prime numbers 5 and 13 have the following splittings :

$$5 = (2+i)(2-i) \qquad 13 = (3+2i)(3-2i).$$

Thus, the arithmetic of the quadratic field K is completely determined by the residue classes modulo 4. This particular example indeed has a far-reaching generalization to abelian extensions of global fields; that is, finite extensions of $\mathbb{Q}$ or of $\mathbb{F}_q(T)$; called the *global class field theory*. Now, let F be a global field, and let K be an arbitrary finite Galois extension over F with abelian Galois group $\mathrm{Gal}(K/F)$. The theory, developed mainly by Artin, Chevalley, Hasse, and Takagi describes the arithmetic of the number field K in terms of the ground field F and in terms of the invariants attached to F. (There is a local version of class field theory as well, which is compatible with the global theory.)

Thus, it is fair to state that, the theory, at least for abelian extensions over a global/local field F is more or less complete. Now, at this point two questions arise naturally :

- Question 1 : How to generalize the theory for arbitrary Galois extensions of F ? That is, extend the theory for non-abelian extensions over F.
- Question 2 : How to generalize abelian class field theory for fields "coming from geometry" (for example, finitely generated fields F with $\mathrm{tr.deg}_{\mathbb{Q}}(F) = 1$ or $\mathrm{tr.deg}_{\mathbb{F}_p}(F) = 2$, or for the local version: n-local fields), instead of a global/local field F ?

The first question is in the content of the famous *functoriality principle* of Langlands [1], [4], which is still in a conjectural state. The second question is answered by the *K-theoretic class field theory* of K. Kato, Parshin, and S. Saito [3], [5]. So the above two questions have answers (modulo functoriality principle).

The natural question now is to unify the functoriality principle and K-theoretic class field theory. In this talk, we shall describe our understanding of the proposal of M. M. Kapranov [2] on this question.

References

[1] J. Arthur, *Automorphic representations and number theory*, 1980 Seminar on Harmonic Analysis (Montreal Quebec, 1980), CMS Conf. Proc. 1, Amer. Math. Soc., Providence RI, 1981, pp. 3-51

[2] M. M. Kapranov, *Analogies between the Langlands correspondence and topological quantum field theory*, Functional Analysis in the Eve of the 21^{st} Century (Vol. 1), Progr. Math. **131**, Birkhäuser, Boston MA, 1995, pp. 119-151

[3] K. Kato, S. Saito, *Global class field theory of arithmetic schemes*, Applications of Algebraic K-theory to Algebraic Geometry and Number Theory, Part I, II (Boulder, Colorado, 1983), Contemp. Math. **55**, AMS , Providence, Rhode Island, 1986, pp. 255-331.

[4] R. P. Langlands, *Problems in the theory of automorphic forms*, Lectures in Modern Analysis and Applications (Vol. III), Lecture Notes in Math. **170**, Springer-Verlag, Berlin, 1970, pp. 18-61

[5] A. N. Parshin, *On the arithmetic of two-dimensional schemes I : Distributions and residues*, Izv. Akad. Nauk. SSSR Ser. Mat. **40**, 1976, 736-773

Istanbul Bilgi University

email: ilhan@bilgi.edu.tr

Modular Forms

Özlem Imamoglu

In these two talks we will try to give a quick introduction to modular forms. We will start with the classical theta functions as the prime examples and through them we will try to motivate the study of these forms, their properties and some of the major open problems in the subject.

ETH, Zürich, Switzerland

email: ozlem@math.ethz.ch

Injectivity and Related Concepts in Incidence Algebras

Müge Kanuni

For R a commutative ring with identity and X a locally finite partially ordered set, we define $I(X,R)$, the incidence ring, to be the set of functions $f : X \times X \longrightarrow R$ such that $f(x,y) = 0$ unless $x \leq y$, with the following operations

$$(f+g)(x,y) = f(x,y) + g(x,y)$$

$$fg(x,y) = \sum_{x \leq z \leq y} f(x,z)g(z,y)$$

For all $f, g \in I(X,R)$ and $x, y \in X$.

In this survey, we consider $I(X,R)$ both as a module over itself and as an R-module and investigate the necessary and sufficient conditions for the incidence ring to be divisible, injective, or principally injective.

References

[1] T.Y. Lam: *Lectures on Modules and Rings*, Springer GTM 189,1999

[2] W.K. Nicholson, M.F. Yousif: *Quasi-Frobenius Rings*, Cambridge University Press, 2003

[3] J.J. Rotman: *An Introduction to Homological Algebra*, Academic Press, 1979

[4] E. Spiegel: *Classical Quotient Rings of Incidence Algebras*, Comm. in Algebra, 27(3) (1999), 999-1012

[5] E. Spiegel and C. J. O'Donnell: *Incidence Algebras*, Marcel Dekker,Inc., 1997

Boğaziçi University

email: muge.kanuni@boun.edu.tr

Irreducible polynomials by the polytope method over integral domains

Fatih Koyuncu

Ostrowski realized that there is a relation between the factorization of a multivariate polynomial over any field and the integral decomposition of the Newton polytope of this polynomial. Here, we extended this result to the multivariate polynomials over any integral domain. Moreover, we observed that this result is also valid for some special kind of multivariate polynomials over any ring.

References

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

[2] Gao S. *Decomposition of Polytopes and Polynomials*, Discrete and Computational Geometry **26** (2001), no. 1, 89-104.

[3] Ostrowski A.M. *On multiplication and factorization of polynomials, I. Lexicographic orderings and extreme aggregates of terms*, Aequationes Math. **13** (1975), 201-228.

Muğla Üniversitesi, Matematik Bölümü

email: fatih@mu.edu.tr

The Klein quartic: modular representation and reduction over finite fields

Gilles Lachaud

In his lost notebook, Ramanujan gave an algebraic relation between three theta functions, which leads to an isomorphism from the modular curve of order seven to the Klein quartic. In fact this isomorphism has already been obtained by Felix Klein. We show that this relation is a consequence of the automorphy properties with respect to the full modular group of the vector valued function made up from these these theta series. These identities lead to geometric interpretations of identities between modular forms of level 7. They are closely related to a Hecke L function associated to the quadratic field K of discriminant -7, which is as well the L function of the modular elliptic curve with complex multiplication by the ring of integers of K. With this identification, we shall give the structure of the Jacobian and the number of points of a remarkable form of the Klein quartic over finite fields.

Institut de Mathématiques de Luminy, Marseille

email: lachaud@iml.univ-mrs.fr

Growth of the intersection of the centralizer of an involution and its class of conjugated elements in finite simple groups

Vladimir M. Levchuk

As usual, we denote by $C_G(\tau)$, the centralizer of an element τ in a group G, and by τ^G, the class of all conjugate elements to τ.

The number of all finite simple groups with a preassigned centralizer of an involution is finite, by well-known R. Brauer's theorem. Since 90th V.P. Shunkov has developed the generalization of Brauer's theorem by using the following "parameter embedding of involution"

$$t(G,\tau) = \max_{g\in G} |gC_G(\tau) \cap (\tau^G\tau^G)|.$$

In 2001 V.P. Shunkov announced the theorem [1]:

The number of all periodical simple groups having an involution with a preassigned finite parameter of its embedding are finite and all such groups are finite.

Proof of this theorem isn't published still. Note that the theorem based on the assumption: *There exists only finite number of finite simple groups with a preassigned parameter of an involution embedding.* We investigate

Hypothesis 1. *There exists only finite number of finite simple groups G having an involution τ such that $|C_G(\tau) \cap \tau^G| \leq m$ for any preassigned positive integer m.*

Since $t(G,\tau) \geq |C_G(\tau) \cap \tau^G|$, so confirming of Hypothesis 1 should also mean that of Shunkov's assumption. It is proved

Theorem 2. *Let m be a positive integer and $G = S_n$, A_n or $PSL_n(q)$. If the order of $|G|$ is rather large, then $|C_G(\tau) \cap \tau^G| > m$ for any involution τ in G.*

Analogous strengthening of R. Brauer's theorem is proved for some another infinite families of finite Lie type groups. Thus, we may wait that Hypothesis 1 will be verified completely.

This research is supported by Russian fund of fundamental researches, grant No. 06-01-00824.

References

[1] V.P. Shunkov. Groups with involutions. – Proceed. Intern. Seminar on Groups Theory (Ekaterinburg, 17-21 December, 2001). Ekaterinburg: Inst. Matem. and Mech., 2001. – pp. 245-246.

Krasnoyarsk St. Univ., Russia

[The following speaker was not able to come to the meeting:]

Variants of the Cycle Class Map

James D. Lewis

The celebrated Hodge conjecture in its classical form, is a statement about the image of a particular cycle class map from an algebraic cycle group on a nonsingular complex projective variety to singular cohomology. We explain to the nonexpert what precisely this conjecture says. We then discuss a variant of this conjecture, called the Hodge-Deligne conjecture. Next, and motivated in part by constructions in algebraic K-theory, we consider twisted variants of this cycle class map construction, and explain the advantages of this construction over the original cycle class map.

University of Alberta

email: lewisjd@ualberta.ca

Non-singular coalgebras and copolyform modules

Christian Lomp

1. Motivation: One of the powerful tools in ring theory is the construction of certain rings of quotients, that allow to embed a ring into a "better" one. Our work was motivated by the desire to find similar tools for coalgebras in a dual sense, namely to construct a "better" coalgebra, that "covers" the given one.

2. Historical background: Passing from the integers to the rationals is one of our fundamental algebraic concepts. In the first issue of his book"Moderne Algebra" ([1]) from 1930, van der Waerden asked whether every non-commutative domain could be embedded into a divison ring. Shortly afterwards, Maltcev showed in [2] that this was not always possible and by that did not closed the subject, but rather raised the question as to when a domain could be embedded into a divison ring (or maybe into some other "good" ring). Two streams of research followed that I would like to sketch quickly. Already in 1931, Ore in [3], who wanted to develop determinants to solve systems of linear equations with non-commutative coefficients, had to find a condition that would allow him to embed a non-commutative domain D into a division ring. What he found is now called the *Ore condition* and says that any two non-zero elements have a common non-zero multiple, i.e. $\forall a, b \in D : aD \cap bD \neq 0$. In general Ore's localisation for non-commutative rings R aims at constructing an overing Q in which every non-zero divisor is invertible, such that every element of Q can be written as a product of an element of R and an inverse of a non-zero divisor. Q is nowadays called the (left/right) classical ring of quotients and denoted by $Q_{cl}(R)$. >From 1958 to 1960, following Ore's line, Goldie and Lesieur & Croisant (see [4], [5], [6]) gave necessary and sufficient condition for $Q_{cl}(R)$ to exist and to be a matrix ring over a division ring (resp. in a finite product of those matrix rings). Goldie's theorem, as it is called today, says that $Q_{cl}(R)$ exists and is a matrix ring over a division ring (resp. in a finite product Q of matrix rings over division rings) if and only if R is prime (resp. semiprime),

does not contain any infinite internal direct sum of left ideals and satisfies the ascending chain conditions on left annihilators. A ring satisfying the later two conditions is called a left Goldie ring.

A different way was taken by Asano, Johnson and Utumi. Going back to a construction of Asano from 1939 (see [7]), Johnson in 1951 (see [8]) and later Utumi in [9] defined an overing Q for any non-commutative ring R as follows: Call a left ideal D of R *dense* if for each $a, b \in R$ with $b \neq 0$ there exists $r \in R$ such that $ra \in D$ and $br \neq 0$. The set of dense left ideals is denoted by $\mathcal{D}$. Then define an equivalence relation on the set $\bigcup_{D\in\mathcal{D}} \mathrm{Hom}(D, R)$ as follows: for $D, E \in \mathcal{D}$ and $f \in \mathrm{Hom}D, R, g \in \mathrm{Hom}E, R$ set

$$f \sim g :\Leftrightarrow \exists F \in \mathcal{D} : f(x) = g(x) \forall x \in F$$

The *left maximal ring of quotients* of R is then defined as

$$Q_{max}(R) := \left(\bigcup_{D\in\mathcal{D}} \mathrm{Hom}(D, R) \right) / \sim$$

A ring R is called *left non-singular* if for any $0 \neq a \in R$ the left annihilator

$$l.ann_R(a) = \{b \in R \mid ba = 0\}$$

is not essential, i.e. there exists a left ideal I of R with $I \cap l.ann_R(a) = 0$. Obviously any domain is left non-singular. Johnson proved in [8] that a ring R is left non-singular if and only if $Q_{max}(R)$ is a von Neumann regular ring. Recall that a ring S is called von Neumann regular if for every element $a \in S$ there exists $b \in S$ such that $a = aba$. The element b can be regarded as some kind of pseudo inverse of a. Hence Johnson showed that although a domain might not be embeddable into a division ring, it can however be embedded into a von Neumann regular ring.

Shortly afterwards, in 1958, Findlay and Lambek in [10] gave a module theoretic definition of the maximal ring of quotients by using injective hulls. They called a submodule M of a module X *rational* provided $\mathrm{Hom}(L/N, X) = 0$ for all $N \subset L \subseteq X$. X is then called a rational extension of M. Using the injective hull of M they showed that there always exists a *maximal rational hull* $\overline{M}$, where maximality means here that for any other rational extension $\imath : M \subset X$ there exists a monomorphism $f : X \to \overline{M}$ such that $f \circ \imath_{|_M} = id_M$. The left maximal ring of quotients of R is then shown to be equal to the maximal rational hull of R as left R-module, i.e. $Q_{max}(R) = \overline{R}$.

The connection between the classical ring of quotients and the maximal ring of quotients is that any semiprime ring R with ascending chain condition of left annihilator is left non-singular. In particular any semiprime left Goldie ring R one has $Q_{max}(R) = Q_{cl}(R)$.

Gabriel showed in [11] that the set of dense ideals is a filter with some special properties. He showed that Utumi's construction of the maximal ring of quotients can be done analogously for any filter $\mathcal{F}$ with such special properties (those filters are now caled Gabriel filters). Any injective module Q defines a Gabriel filter by taking $\mathcal{F} = \{I \subseteq R \mid \mathrm{Hom}(R/I, Q) = 0\}$. Moreover given a

Gabriel filter $\mathcal{F}$ one defines a class of modules that are annihilated by some of the members of $\mathcal{F}$, i.e. $\tau = \{X \mid \exists I \in \mathrm{F} : IX = 0\}$. Taking for any R-module M the trace of τ in M, $\tau(M) = \sum\{\mathrm{Im}(f) \mid f : T \to M, T \in \tau\}$ defines a *torsion radical* with torsion class τ. On the other hand one can show that any torsion class corresponds to an injective module. Hence there exists a correspondence between Gabriel filters, torsion theories and injectiv modules. The filter of dense left ideals is precisely the filter associated to the injective hull of R and its torsion theory is called the Lambek torsion theory.

A module is called singular if every element is annihilated by some essential left ideal or equivalently if it is a quotient of a module by an essential submodule. The class of singular modules need not be closed under extensions and hence might not be a torsion class. However it makes sense to define a pretorsion radical associated to the class of singular modules, i.e. the singular submodule $Z(M)$ which is the sum of all singular submodules. Non-singular modules are then those that are "torsionfree" with respect to the class of singular modules.

Torsion theories and singular modules can be defined in more general module categories, like for instances in Wisbauer's category $\sigma[M]$ consisting of submodules of factor modules of direct sums of copies of M. Thus it makes sense to talk about non-singularity in $\sigma[M]$ and about the torsion theory cogenerated by the self-injective hull $\widehat{M}$ of M, i.e. the Lambek torsion theory in $\sigma[M]$. If M is non-singular in $\sigma[M]$, then the Lambek torsion class coincides with the class of singular modules. In particular one has that every essential submodule is rational. Zelmanowitz termed a module M *polyform* if every essential submodule is rational. He used it in [12] to generalize the Jacobson density theorem. Wisbauer in [13] showed that any not necessarily associative semiprime algebra A is polyform as a module over its multiplication algebra $M(A)$ and used module theory to construct the central closure of A. In [14] it is actually shown that a module M is polyform if and only if it is non-singular in $\sigma[M]$. Moreover Wisbauer showed a module theoretic version of Goldie's theorem by proving that $\mathrm{End}(\widehat{M}) = Q_{cl}(\mathrm{End}(M))$ is semisimple artinian if and only if M is polyform with finite uniform dimension and $\mathrm{End}(M)$ is semiprime, provided that $\mathrm{Hom}(M, N) \neq 0$ for all non-zero $N \subset M$.

3. Dualisation: As explained above, the construction of rings of quotients can be done in certain module categories. In this general settings we have all dual notions readily at hand by categorical dualisation.

Notions	and their Duals
Essential submodule $N \trianglelefteq M$	**small submodules** $N \ll M$
$\forall 0 \neq L \subseteq M : N \cap L \neq 0$	$\forall L \subset M : N + L \neq M$
Singular module N **in** $\sigma[M]$	**Small module** N **in** $\sigma[M]$
$N \simeq Z/Y$ where $Y \trianglelefteq Z \in \sigma[M]$	$N \simeq Y$ where $Y \ll Z \in \sigma[M]$
Non-singular module X **in** $\sigma[M]$	**Non-small module** X **in** $\sigma[M]$
$\mathrm{Hom}(S, X) = 0$ for all singular $S \in \sigma[M]$	$\mathrm{Hom}(X, S) = 0$ for all small $S \in \sigma[M]$
Rational extensions $\imath : M \hookrightarrow X$	**Co-rational covers** $\pi : X \twoheadrightarrow M$
$\mathrm{Hom}(U, X) = 0$ whenever $U \hookrightarrow \mathrm{Coke}(\imath)$	$\mathrm{Hom}(X, U) = 0$ whenever $\mathrm{Ker}(\pi) \twoheadrightarrow U$
Polyform module M	**Co-polyform module** M
$N \trianglelefteq M \Rightarrow N \hookrightarrow M$ is rational	$N \ll M \Rightarrow M \twoheadrightarrow M/N$ is co-rational

Co-rational covers had been defined already in 1966 by Courter (see [15]). Co-polyform modules had been studied by the author in 1997 in [16] and later by various authors [17],[18],[19],[20], [21]. A characterisation of co-polyform modules says that a module M is co-polyform if and only if

$$\nabla(M, M/N) = \{f : M \to M/N \mid \mathrm{Im}(f) \ll M/N\} = 0$$

for all $N \ll M$. The ∇-concept had been introduced by Beidar and Kasch in [22] where it was termed the *cosingular ideal* of M and M/N. For a self--projective module M, $\nabla(M, M)$ coincides with the Jacobson radical of the endomorphism ring of M and one has that M is co-polyform if and only if $\mathrm{Jac}(\mathrm{End}(M)) = 0$. Hence a ring R is co-polyform if and only if it is semiprimitive. On the other hand one easily verifies that a ring R is non-small in R-Mod if and only if it is a V-ring, i.e. there are no non-zero small R-modules. This shows that co-polyform modules need not be non-small. However for a (self-)injective (self-)cogenerator M one shows that these notions coincides and that $\nabla(M, M)$ equals $Z(\mathrm{End}(M))$, the singular right ideal of $\mathrm{End}(M)$. As a consequence we can characterize co-polyform self-injective self-cogenerators M as those whose endomorphism ring is right non-singular. We will show some more properties of co-polyform and non-small modules, in particular the construction of a maximal co-rational cover for modules with projective covers.

4. Applications to coalgebras: A coalgebra C over a field k has a comultiplication $\Delta : C \to C \otimes C$ and a counit $\epsilon : C \to k$ satisfying dual conditions of the usual associativity and unit condition for algebras. The vector space $C^* = \mathrm{Hom}(C, k)$ of linear forms becomes a k-algebra, called the dual algebra of C, under the *convolution product* which is defined as

$$f * g(c) = \sum_{i,j} f(c_i)g(d_j)$$

for $f, g \in C^*$, where $\Delta(c) = \sum_{i,j} c_i \otimes d_j$ is some representation of the comultiplication of $c \in C$. One also has a left C^*-module action on C by $f \cdot c := \sum_{i,j} f(d_j)c_i$. The lattice of left C^*-submodules equals the lattice of right subcomodules of C. Module theory enters into the study of comodules by the basic observation, that the category of right C-comodules equals $\sigma[{}_{C^*}C]$. Furthormore C is an injective cogenerator in $\sigma[{}_{C^*}C]$ and there exists an anti-isomorphism of k-algebras from $\mathrm{End}({}_{C^*}C)$ to C^*. See Brzezinski and Wisbauer's book [23] for further details

Applying our concept of co-polyform modules we have that the coalgebra C is co-polyform as right comodule if and only if C^* is left non-singular if and only if C is co-polyform as left comodule. Calling a coalgebra C non-singular if its dual algebra is left non-singular we also show that coalgebras whose category of right comodules has global dimension ≤ 1 (so-called hererditary coalgebras, see [24]) are non-singular. Path coalgebras are further examples of non-singular coalgebras (see [25]).

If time permits we talk also about covering coalgebras.

This is a joint work (see [26]) with Virgínia Rodrigues from the University of Santa Catarina, Florianopolis (Brasil) that spent six months at the University of Porto supported by the project "Interacções entre algebras e co-algebras"

(GRICES/CAPES). Moreover the author would like to thank the Fundação de Calouste Gulbenkian for a travel grant that allowed him to attend this conference.

References

[1] B.L. van der Waerden, *Moderne Algebra*, Grundlehren der mathematischen Wissenschaften 23, Springer Verlag (1930)

[2] A.Malcev, *On the immersion of an algebraic ring into a field*, Mathematical Annals 113 (1936), 686-691.

[3] O.Ore, *Linear equations in non-commutative fields*, Annals of Mathematics II, 32 (1931), 463-477

[4] A.Goldie, *The structure of prime rings under ascending chain conditions.* Proceedings of the London Mathematical Society III. Ser. 8 (1958), 589-608.

[5] L.Lesieur and R.Croisot, *Sur les anneaux premiers noethériens à gauche.* Annales Scientifiques de l'École Normale Supérieure, III. Sér. 76 (1959), 161-183.

[6] A.Goldie, *Semi- prime rings with maximum condition.*. Proceedings of the London Mathematical Society, III. Ser. 10 (1960), 201-220.

[7] K.Asano, *Arithmetische Idealtheorie in nichtkommutativen Ringen*, Japanese Journal of Mathematics 16 (1939),1-36

[8] R.E.Johnson, *The extended centralizer of a ring over a module*, Proceedings of the American Mathematical Society 2 (1951), 891-895

[9] Y.Utumi, *On quotient rings*, Osaka Mathematical Journal 8, No.1 (1956), 1-18

[10] G.D.Findlay and J.Lambek, *A generalized ring of quotients. I, II.*, Canadian Mathematical Bulletin 1 (1958), 77-85, 155-166

[11] P.Gabriel, *Des catégories abéliennes* Bulletin de la Société Mathématique de France 90 (1962), 323-448.

[12] J.Zelmanowitz, *Representation of rings with faithful polyform modules*, Communications in Algebra 14 (1986), 1141-1169

[13] R.Wisbauer, *Localization of modules and the central closure of rings.* Communications in Algebra 9, No.14 (1981), 1455-1493.

[14] R.Wisbauer, *Modules and algebras: bimodule structure and group actions on algebras*, Longman, Harlow, 1996

[15] R.C. Courter, *The maximal co-rational extension by a module*, Canadian Journal of Mathematics 18 (1966), 953-962.

[16] C.Lomp, *On dual Goldie dimension*, MSc Thesis, University of Glasgow (1997)

[17] Y.Talebi and N.Vanaja, *Copolyform modules.* Communications in Algebra 30 No. 3 (2002), 1461-1473.

[18] Y.Talebi and N.Vanaja, *Copolyform Σ-lifting modules.* Vietnam Journal of Mathematics 32, No.1 (2004), 49-64.

[19] G.Güngöroglu and D.Keskin Tütüncü, *Copolyform and lifting modules.* Far East Journal of Mathematical Sciences 9, No.2 (2003), 159-165

[20] G.Güngöroglu and A.Harmanci, *On some classes of modules.* Czechoslovak Mathematical Journal 50, No.4 (2000), 839-846

[21] G.Güngöroglu *Copolyform modules.* Communications de la Faculté des Sciences de l'Université d'Ankara, Série A1, Math. Stat. 49, No.1-2, 101-110 (2000).

[22] K.Beidar, and F.Kasch, *Good conditions for the total.*, in *International symposium on ring theory.*, Birkenmeier, Gary F. (ed.) et al., Birkhäuser. Trends in Mathematics. 43-65 (2001).

[23] Brzezinski, T. and Wisbauer, R., *Corings and Coalgebras*, London Mathematical Society Lecture Notes Series 309 (2003)

[24] C.Nastasescu, B.Torrecillas, and Y.H.Zhang, *Hereditary coalgebras.*, Communications in Algebra 24 No.4 (1996), 1521-1528

[25] W.Chin, *Hereditary and path coalgebras.*, Communications in Algebra 30 No. 4 (2002), 1829-1831

[26] C.Lomp and V.Rodrigues, *Covering coalgebras and non-singularity of modules*, preprint

University of Porto

email: clomp@fc.up.pt

web: http://www.fc.up.pt/mp/clomp/

[The following speaker did not come to the meeting:]

On the Projective S-acts

Ali Madanshekaf

Let S be a semigroup and $E(S)$ the set of all idempotents in S. We call a set M a *left S-act* if there exists an action $S \times M \longrightarrow M$ denoted by $(s, m) \mapsto sm$, satisfying $(st)m = s(tm)$ for all $s, t \in S$ and $m \in M$. We denote the category of all S-acts together with the obvious S-morphisms by S-bf Act. A comperhensive treatment of all aspects of acts is given in the Handbook [3]. In this talk some aspects of projective S-acts are studied and some fact about them are presented.

References

[1] Yuqun Chen, Projective S-acts and Exact Functors, Algebra Colloquium 7 (2000), 113-120.

[2] Yuqun Chen, K. P. Shum, Projective and Indecomposable S-acts, Science in China 42 (6) (1999) 593-599.

[3] M. Kilp, U. Knauer, A. Mikhalev, *Monoids, Acts and Categories*, Walter de Gruyter: Berlin, New York, 2000; 529 pp.

[4] A. Madanshekaf, J. Tavakoli, Tiny Object in the Category of M-sets, Ital. J. Pure Appl. Math. No. 10 (2001), 153-162.

Mathematics Department, Faculty of Science, Semnan University, Semnan, Iran

email: a.madanshekaf@yahoo.com

Generalized Marsaglia's lattice test and the linear complexity

Wilfried Meidl

Let $S = s_1, s_2, \ldots$ be a sequence with terms in the finite field $\mathbb{F}_q$, then we say that S passes the Λ-*dimensional* n-*lattice test* if the vectors $\{\mathbf{s}_j - \mathbf{s}_1 \mid 2 \le j \le n - \Lambda + 1\}$ span $\mathbb{F}_q^\Lambda$, where

$$\mathbf{s}_j = (s_j, s_{j+1}, \ldots, s_{j+\Lambda-1}), \quad 1 \le j \le n - \Lambda + 1.$$

If S passes the Λ-dimensional n-lattice test then it passes all Λ'-dimensional lattice tests with $\Lambda' \le \Lambda$, and if S fails the Λ-dimensional n-lattice test then it fails all Λ'-dimensional lattice tests with $\Lambda' \ge \Lambda$. The greatest Λ such that S passes the Λ-dimensional n-lattice test, denoted by $\Lambda_n(S)$, is called the *nth lattice level* of S. Additionally we define $\Lambda_0(S) = \Lambda_1(S) = 0$. The *lattice level* $\Lambda(S)$ of S is then defined to be

$$\Lambda(S) = \sup_{n \ge 0} \Lambda_n(S),$$

and we call the sequence $\langle \Lambda_n(S) \rangle_{n=0}^{\infty}$ the *lattice profile* of S (cf. [3], [4]). For a finite sequence of the length N we define the lattice profile to be the finite sequence $\langle \Lambda_n(S) \rangle_{n=0}^{N}$.
The above defined lattice test is a generalization of Marsaglia's lattice test [5], defined for periodic binary sequences.

For a sequence $S = s_1, s_2, \ldots$ with terms in the finite field $\mathbb{F}_q$ of length at least n, the *nth linear complexity* L_n of S, denoted by $L_n(S)$, is the length of the shortest linear recurrence relation over $\mathbb{F}_q$

$$a_{L_n} s_{j+L_n} + a_{L_n-1} s_{j+L_n-1} + \ldots + a_0 s_j = 0 \quad \text{for } j = 1, 2, \ldots, n - L_n$$

satisfied by the first n terms of S. If S starts with $n-1$ zeros and $s_n \neq 0$ then we define $L_i(S) = 0$ for $1 \le i \le n-1$, and $L_n(S) = n$. Additionally we can put $L_0(S) = 0$. The *linear complexity* $L(S)$ of S is defined as

$$L(S) = \sup_{n \ge 0} L_n(S),$$

and the sequence $\langle L_n(S) \rangle_{n=0}^{\infty}$ is called the *linear complexity profile* of S. Again for a finite sequence of the length N we can define the linear complexity profile to be the finite sequence $\langle L_n(S) \rangle_{n=0}^{N}$.

The linear complexity has mostly been considered in connection with cryptographic applications, while the lattice structure has mostly been considered with respect to applications in Quasi-Monte Carlo methods, but recently it turned out that these two complexity measures are strongly related. The investigations on the relations between linear complexity and lattice structure were originated by Niederreiter and Winterhof in the paper [8], which concentrates on q-periodic sequences over $\mathbb{F}_q$. In [1] the lattice test as defined above was introduced, and as the main result it was shown that the connection between nth linear complexity and nth lattice level of a sequence S is given by

$$\Lambda_n(S) = \min(L_n(S), n+1-L_n(S)) \text{ or } \Lambda_n(S) = \min(L_n(S), n+1-L_n(S)) - 1.$$

Moreover necessary and sufficient conditions for the occurence of both possible cases were given. As a consequence the lattice profile of a sequence S can completely be described via linear complexity methods.
In [3], the results of [1] were used to explicitly describe the nature of a lattice profile of a sequence S over a finite field $\mathbb{F}_q$: Roughly speaking, whenever the lattice profile starts to increase it steadily increases by 1 until it reaches the upper bound $n/2$.
Employing the strong relations between lattice structure and linear complexity, further results on the lattice structure can be obtained, which are accordant to well known results on the linear complexity:
In [4] the counting function for the number of sequences over a finite field $\mathbb{F}_q$ with fixed length n and fixed nth lattice level has been derived. Based on this result the expected nth lattice level and its variance have been calculated. Further enumeration results on the lattice profile can be found in [6]. In [7] the lattice profile of a sequence S over $\mathbb{F}_q$ has completely been described by the continued fraction expansion of the generating function corresponding to S.

References

[1] G. Dorfer, A. Winterhof, Lattice structure and linear complexity profile of nonlinear pseudorandom number generators, AAECC 13 (2003) 499–508.

[2] G. Dorfer, A. Winterhof, Lattice structure of nonlinear pseudorandom number generators in parts of the period, in: H. Niederreiter (Ed.), Monte Carlo and Quasi-Monte Carlo Methods 2002, Springer, Berlin, 2004, pp. 199–212.

[3] G. Dorfer, Lattice profile and linear complexity profile of pseudorandom number sequences, in: G.L. Mullen, A. Poli, H. Stichtenoth (Eds.), Proc. of the 7th International Conference on Finite Fields and Applications. Lecture Notes in Comput. Sci. 2948, Springer, Berlin, 2003, pp. 69–78.

[4] G. Dorfer, W. Meidl, A. Winterhof, Counting functions and expected values for the lattice profile at n, Finite Fields Appl. 10 (2004) 636–652.

[5] G. Marsaglia, The structure of linear congruential sequences, in: S.K. Zaremba (Ed.), Applications of Number Theory to Numerical Analysis, Academic Press, New York, 1972, pp. 249–285.

[6] W. Meidl, Enumeration results on linear complexity profiles and lattice profiles, J. Complexity 22 (2006), 275–286.

[7] W. Meidl, Continued fraction for formal Laurent series and the lattice structure of sequences, AAECC, to appear.

[8] H. Niederreiter, A. Winterhof, Lattice structure and linear complexity of nonlinear pseudorandom numbers, AAECC 13 (2002) 319–326.

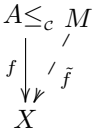
Sabanci University, Orhanli, Tuzla, 34956 Istanbul, Turkey email: `wmeidl@sabanciuniv.edu`

c-injective modules over Dedekind domains

Engin Mermut

We will approach to a *relative injectivity* problem for modules over Dedekind domains using *relative homological algebra*.

Let R be an associative ring with unity. Take R-modules to be *left* R-modules below. R-$\mathcal{M}od$ denotes the category of left R-modules.



Let X and M be R-modules. The module X is called M-*c-injective* if, for every *closed* submodule A of M, every homomorphism $f : A \longrightarrow X$ can be lifted to M, i.e. there exists a homomorphism $\tilde{f} : M \longrightarrow X$ such that $\tilde{f}|_A = f$:

A module M is called *self-c-injective* if M is M-c-injective. For a discussion of c-injectivity and related problems see [8], [11] and [9].

We say that an R-module X is ***c-injective*** if it is M-c-injective for every R-module M.

An R-module M is said to be a *homogenous* (*isotypic*) *semisimple* R-module if M is a semisimple R-module whose simple submodules are all isomorphic, that is, $M = \bigoplus_{\lambda\in\Lambda} S_\lambda$ for some index set Λ and simple submodules S_λ of M such that for some maximal left ideal P of R, $S_\lambda \cong R/P$ for every $\lambda \in \Lambda$.

[9, Theorem 6] shows that for a Dedekind domain W, every direct product of simple W-modules is self-c-injective. [9, after Theorem 6] has also noted that: for a Dedekind domain W, if M is a direct product of homogeneous semisimple W-modules, then M is self-c-injective and any simple W-module is M-c-injective.

We will see that all these mentioned self-c-injective modules over a Dedekind domain are c-injective and we are able to describe c-injective modules by the general theorems for *injectively generated proper classes* since for a Dedekind domain W, the *proper class* $\mathcal{C}ompl_{W\text{-}\mathcal{M}od}$ defined below is injectively generated by homogenous semisimple W-modules and c-injective modules are the same concept with $\mathcal{C}ompl_{W\text{-}\mathcal{M}od}$-injective modules.

The relative homological algebra approach goes as follows:

We consider the *proper class* $\mathcal{C}ompl_{R\text{-}\mathcal{M}od}$ consisting of all short exact sequences

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \qquad (\ddagger)$$

of (*left*) R-modules and R-module homomorphisms such that $\mathrm{Im}(f)$ is a *complement* in B. Note that a submodule A of a module B is said to be a *complement* in B, denote by $A \leq_c B$, if there exits a submodule $K \leq B$ such that $K \cap A = 0$ and A is *maximal* with respect to this property; equivalently, A is *closed* in B which means that A has *no* proper essential extension in B (see [1, §1.10]).

$\mathcal{N}eat_{R\text{-}\mathcal{M}od}$ consists of all short exact sequences of R-modules and R-module homomorphisms with respect to which every simple R-module is projective (following [12, 9.6 in §9] and [13]), motivated by the concept of *neat subgroups* of abelian groups introduced by [4, pp. 42-43]. [2] gives more general definitions for

proper classes of complements related to another given proper class (motivated by the considerations in [3]).

For terminology and notation in *proper classes*, we shall follow [10] (see also [5, Ch. 12, §4] or [12]). Let $\mathcal{P}$ be a *proper class* of short exact sequences of R-modules. An R-module M is said to be $\mathcal{P}$-*projective* [$\mathcal{P}$-*injective*, $\mathcal{P}$-*flat*] if it is projective [resp. injective, flat] with respect to all short exact sequences in $\mathcal{P}$, that is, $\mathrm{Hom}(M,\mathbb{E})$ [resp. $\mathrm{Hom}(\mathbb{E},M)$, $M\otimes\mathbb{E}$] is exact for every $\mathbb{E}$ in $\mathcal{P}$. Denote all $\mathcal{P}$-projective [$\mathcal{P}$-injective, $\mathcal{P}$-flat] modules by $\pi(\mathcal{P})$ [resp. $\iota(\mathcal{P})$, $\tau(\mathcal{P})$]. For a given class $\mathcal{M}$ of modules, denote by $\pi^{-1}(\mathcal{M})$ [$\iota^{-1}(\mathcal{M})$, $\tau^{-1}(\mathcal{M})$], the class of all short exact sequences $\mathbb{E}$ of R-modules and R-module homomorphisms such that $\mathrm{Hom}(M,\mathbb{E})$ [resp. $\mathrm{Hom}(\mathbb{E},M)$, $M\otimes\mathbb{E}$] is exact for all $M\in\mathcal{M}$; this is the largest proper class $\mathcal{P}$ for which each $M\in\mathcal{M}$ is $\mathcal{P}$-projective [resp. $\mathcal{P}$-injective, $\mathcal{P}$-flat]; it is called the proper class *projectively generated* [resp. *injectively generated*, *flatly generated*] by $\mathcal{M}$. For the flatness part in these definitions to be meaningful for left-right module considerations consider just *commutative* rings.

An injective module is called *elementary* if it coincides with the injective envelope of some *cyclic* submodule. Such modules form a set and every injective module can be embedded in a direct product of elementary injective modules [10, Lemma 3.1]. A subclass $\mathcal{M}$ of a class $\overline{\mathcal{M}}$ of modules is called an *injective basis* for $\overline{\mathcal{M}}$ if every module in $\overline{\mathcal{M}}$ is a direct summand of a direct product of modules in $\mathcal{M}$ and of certain elementary injective modules. If $\mathcal{M}$ is a set, then for the proper class $\iota^{-1}(\mathcal{M})$, $\mathcal{M}$ is an injective basis for the class of all $\iota^{-1}(\mathcal{M})$-injective modules [10, Proposition 3.3].

When R is a Dedekind domain W, using the results in [7, Lemmas 4.4 and 5.2, and Theorem 5.1], we obtain that the proper class $\mathcal{C}ompl_{W\text{-}\mathcal{M}od}$ is both projectively generated, injectively generated and flatly generated:
Theorem. *$\mathcal{C}ompl_{W\text{-}\mathcal{M}od}$ equals the following for a Dedekind domain W:*

(i) $\mathcal{N}eat_{W\text{-}\mathcal{M}od} \overset{def.}{=} \pi^{-1}(\{W/P | P \text{ maximal ideal of } W\})$,

(ii) $\iota^{-1}(\{M | M\in W\text{-}\mathcal{M}od \text{ and } PM=0 \text{ for some maximal ideal } P \text{ of } W\})$,
$= \iota^{-1}(\{M | M \text{ is a homogenous semisimple } W\text{-module}\})$,

(iii) $\iota^{-1}(\{W/P | P \text{ maximal ideal of } W\})$,

(iv) $\tau^{-1}(\{W/P | P \text{ maximal ideal of } W\})$

(v) *The proper class of all short exact sequences of W-modules and W-module homomorphisms of the form (‡) such that*

$$A'\cap PB = PA', \qquad \text{where } A'=\mathrm{Im}(f),$$

for every maximal ideal P of W (or $A\cap PB=PA$ when A is identified with its image and f is taken as the inclusion homomorphism).

A c-injective module X is nothing but a $\mathcal{C}ompl_{R\text{-}\mathcal{M}od}$-injective, that is, X is injective with respect to every short exact sequence $\mathbb{E}$ in $\mathcal{C}ompl_{R\text{-}\mathcal{M}od}$, so:
Corollary. *Every* c*-injective-module is a direct summand of a direct product of homogeneous semisimple W-modules and of injective envelopes of cyclic W--modules.*

Acknowledgements.
These results are from my Ph.D. thesis [6]. My Ph.D. Thesis advisor is Rafail Alizade whom I wish to express my thanks once more (İzmir Institute of Technology, Turkey; e-mail: `rafailalizade@iyte.edu.tr`).
I would like to express my gratitude to TÜBİTAK (The Scientific and Technical Research Council of Turkey) for its support during my Ph.D. research.

References

[1] N. V. Dung, D.V. Huynh, P. F. Smith, and R. Wisbauer. *Extending Modules*. Number 313 in Putman Research Notes in Mathematics Series. Longman, Harlow, 1994.

[2] A. I. Generalov. On weak and w-high purity in the category of modules. *Math. USSR, Sb.*, 34:345–356, 1978. Translated from Russian from *Mat. Sb., N. Ser.* 105(147), 389-402 (1978).

[3] D.K. Harrison, J. M. Irwin, C. L. Peercy, and E. A. Walker. High extensions of abelian groups. *Acta Math. Acad. Sci. Hunger.*, 14:319–330, 1963.

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

[5] S. Maclane. *Homology*. Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

[6] E. Mermut. *Homological Approach to Complements and Supplements*. PhD thesis, Dokuz Eylül University, The Graduate School of Natural and Applied Sciences, İzmir/TURKEY, 2004. `http://www.fbe.deu.edu.tr/tez_arsivi/details.asp?yayin_no=403`.

[7] R. J. Nunke. Modules of extensions over dedekind rings. *Illunois J. of Math.*, 3:222–241, 1959.

[8] Catarina Santa-Clara and Patrick F. Smith. Modules which are self-injective relative to closed submodules. In *Algebra and its applications (Athens, OH, 1999)*, volume 259 of *Contemp. Math.*, pages 487–499. Amer. Math. Soc., Providence, RI, 2000.

[9] Catarina Santa-Clara and Patrick F. Smith. Direct products of simple modules over Dedekind domains. *Arch. Math. (Basel)*, 82(1):8–12, 2004.

[10] E. G. Sklyarenko. Relative homological algebra in categories of modules. *Russian Math. Surveys*, 33(3):97–137, 1978. Traslated from Russian from *Uspehi Mat. Nauk* 33, no. 3(201), 85-Ũ120 (1978).

[11] Patrick F. Smith. Commutative domains whose finitely generated projective modules have an injectivity property. In *Algebra and its applications (Athens, OH, 1999)*, volume 259 of *Contemp. Math.*, pages 529–546. Amer. Math. Soc., Providence, RI, 2000.

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

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

Dokuz Eylül University, İzmir/TURKEY

email: `engin.mermut@deu.edu.tr`

web: `http://kisi.deu.edu.tr/engin.mermut/`

Hilbert Functions of Gorenstein Monomial Curves

Pınar Mete

This is a joint work with Feza Arslan. The Hilbert function $H_R(n)$ of a graded k-algebra R is defined as $H_R(n) = dim_k R_n$, where R_n is the homogeneous piece consisting of elements of degree n. The behavior of the Hilbert function of a local ring (R, m) has remained as an important problem to be determined for a long time [9],[10]. For the literature, see [4],[9] and [10]. The importance of this problem comes from the fact that the Hilbert function is a very useful entity to investigate geometric and algebraic properties. Specifically, for the case of a local ring (R, m), it is a good measure of the singularity of (R, m) at m [7].

The purpose of this talk is to show the results of the above problem for a one-dimensional Gorenstein local ring of embedding dimension four associated to a Gorenstein monomial curve. Particularly, we show that the Hilbert function is non-decreasing for large families of these curves [2]. We used a procedure which employs the standard bases computations to obtain the generators of their tangent cones and checking the Cohen-Macaulayness of them [1],[3],[5], [6]. By using the lemma of Morales [8], we also give methods to construct large families of monomial curves satisfying our assumptions on the generators of the defining ideal with embedding dimension four and higher embedding dimensions.

References

[1] F. Arslan, *Cohen-Macaulayness of tangent cones*, Proc. Amer. Math. Soc. **128**, (2000), 2243-2251.

[2] F. Arslan, P. Mete, *Hilbert functions of Gorenstein Monomial Curves*, submitted.

[3] H. Bresinsky, *Symmetric semigroups of integers generated by four elements*, Manuscripta Math. **17**, (1975), 205-219.

[4] J. Elias, *The Conjecture of Sally on the Hilbert Function for Curve Singularities*, Journal of Algebra **160**, No.1 (1993), 42-49.

[5] G-M Greuel, G. Pfister, *A Singular Introduction to Commutative Algebra*, Springer-Verlag, 2002.

[6] E. Kunz, *The value-semigroup of a one-dimensional Gorenstein ring*, Proc. Amer. Math. Soc. **25**, (1970), 748-751.

[7] S. Molinelli, D. P. Patil, G. Tamone, *On the Cohen-Macaulayness of the associated graded ring of certain monomial curves*, Beiträge Algebra Geom., **39**, No. 2(1998), 443-446.

[8] M. Morales, *Syzgies of a monomial curve and a linear Diophantine problem of Frobenius*, Max-Planck-Institut für Mathematik, preprint, 1987.

[9] J. Sally, *Number of generators of ideals in local rings*, Lecture Notes in Pure and Appl. Math. **35**, Marcel Dekker, 1978.

[10] G. Valla, *Problems and results on Hilbert functions of graded algebras*, Six Lectures on Commutative Algebra, Progr. Math. vol. 66, Birkhäuser, Basel, 1998, pp. 293–344.

Balıkesir University

email: pinarm@balikesir.edu.tr

On truncated Fibonacci sequences

Engin Özkan

We have proved four original theorem concerning about the truncated Fibonacci sequences. We also have given four propositions concerning about Wall number of truncated Fibonacci sequence. Furthermore, we have given a computer verification of those propositions.

References

[1] D. Takahashi, A Fast Algorithm For Computing Large Fibonacci Numbers. Information Processing Letters, 75, 243-246 (2000) .

[2] E. Özkan, H. Aydın and R. Dikici.3-step Fibonacci series modulo . Applied Mathematics and Computation,143 (2003),165-172.

[3] Gyoung-Sik Choi, Suk-Geun Hwang, Ik-Pyo Kim and Bryan L. Shader, (1) Invariant sequences and truncated Fibonacci Sequences. Linear Algebra and its Applications 395 (2005)303-312.

[4] D.D. Wall, Fibonacci Series Modulo m. Amer. Math. Monthly, 67, 525- 532 (1960).

[5] H.J. Wilcox, Fibonacci Sequences of Period n in Groups. The Fibonacci Quarterly, 24, 356-361 (1986).

Atatürk Üniversitesi, Fen Edebiyat Fak., Matematik Böl., Erzurum, Turkey

email: eozkan@atauni.edu.tr

Thom polynomials via Schur functions

Özer Öztürk

Thom polynomials express invariants of singularities of a general map $f : X \to Y$ between complex analytic manifolds in terms of invariants of X and Y.

To be more precise let $k \geq 0$ be a fixed integer and $\bullet \in \mathbf{N}$. Let κ_1, κ_2 be two stable germs $(\mathbf{C}^\bullet, 0) \to (\mathbf{C}^{\bullet+k}, 0)$. They are said to be right-left equivalent if there exist $\phi \in \mathrm{Diff}(\mathbf{C}^n, 0)$ and $\psi \in \mathrm{Diff}(\mathbf{C}^{n+k}, 0)$ such that $\psi \circ \kappa_1 \circ \phi^{-1} = \kappa_2$. By a singularity we mean an equivalence class of the relation generated by right-left equivalence and suspension.

Let η be a singularity. By $V^\eta(f)$ denote the closure of the set

$$\{x \in X : \text{the singularity of } f \text{ at } x \text{ is } \eta\}.$$

$V^\eta(f)$ often becomes a submanifold and the problem is to find the Poincaré dual of (the cycle carried by) it.

By an early result of Thom for each singularity η there exists a universal polynomial $\mathcal{T}^\eta$, called the *Thom polynomial*, such that $\mathcal{T}^\eta(c_1, c_2, \ldots)$ gives the Poincaré dual of $V^\eta(f)$, after the substitution Chern classes c_i of the virtual bundle $TX - f^*TY$ (see [1]).

However computation of Thom polynomials is difficult in general. Different methods, such as desingularization, have been developed by many mathematicians (One can find a survey of the works of Porteous, Thom, Ronga, Menn, Sergeraert, Lascoux and Roberts in [2]). Recently a new method, the "method of restriction equations" (developed mainly by Rimanyi) converted the problem into an algebraic one (see [3]). Using this method, which is fine when k is small, Rimanyi computed Thom polynomials for some singularities when k is 0 or 1, which are not so easy to compute with the previous methods. Then he asked for formulas containing k as a parameter:

"However, another challenge is to find Thom polynomials containing k as a parameter." ([3], p.512)

To do this, in [4], Pragacz suggested to combine this method with the theory of *Schur functions* and obtained many new results including formulas for the Thom polynomials for the singularities $I_{2,2}$ and A_3 (for all k, as desired).

Currently, as a part of my PhD studies (supervised by Ö. Kişisel (METU) and P. Pragacz (IMPAN)), I am using this combination to study the Thom polynomials for the singularities $I_{2,3}$, $III_{2,3}$ and A_4. In this talk, after describing this combination (especially the role played by Schur functions) I will try to outline the results that I have obtained on the Thom polynomials for A_4 singularities.

References

[1] R. Thom, *Les singularités des applications différentiables,* Ann. Inst. Fourier **6** (1955–56), 43–87.

[2] S. Kleiman, *The enumerative theory of singularities,* in: "Real and complex singularities, Oslo 1976" (P. Holm ed.) (1978), 297–396.

[3] R. Rimanyi, *Thom polynomials, symmetries and incidences of singularities,* Inv. Math. **143** (2001), 499–521.

[4] P. Pragacz, *Thom polynomials and Schur functions I,* Preprint (August 2005), math.AG/0509234.

METU

email: ozero@metu.edu.tr

Relative one-relator groups

Stephen J Pride

The study of one-relator groups was begun by Wilhelm Magnus in the late 1920's and early 1930's (this study was suggested to Magnus by his PhD supervisor, Max Dehn). There is a good account of the basics of one-relator group theory in [1] and [2]. The class of one-relator groups has been intensely studied since Magnus' pioneering work. Nevertheless, there are still basic open questions concerning these groups [3]. In particular, the problem of when one-relator groups are residually finite is still open ([3], Questions OR1, OR6), as is the conjugacy problem ([3], Question O5).

By definition, a one-relator group is defined by a presentation $\mathcal{P} = \langle \mathbf{x}; R \rangle$ where $\mathbf{x}$ is the generating set and R is a word on $\mathbf{x}$ which is the single defining relator. A more general situation is to consider *relative* one-relator groups . These are given by a *relative* one-relator presentation $\mathcal{P} = \langle \mathbf{x}, H; R \rangle$. Here H is a group (to be thought of as a "coefficient group"), and R is a word on the alphabet $\mathbf{x}$ and the elements of H. The group $G(\mathcal{P})$ defined by $\mathcal{P}$ is the quotient of the free product $F(\mathbf{x}) * H$ (where $F(\mathbf{x})$ is the free group on $\mathbf{x}$), by the normal closure of R. One would hope that the properties of $G(\mathcal{P})$ should be governed by the "shape" of the "$\mathbf{x}$-skeleton" (the word on $\mathbf{x}$ obtained from R by deleting all terms from H), and the algebraic properties of the coefficient group H.

Here I will introduce the "unique max-min property" for the shape. It turns out then that $G(\mathcal{P})$ is residually finite if and only if H is residually finite. This theorem can then be used to get some corollaries concerning ordinary one-relator groups. Further results (including results concerning the conjugacy problem) are also obtained [4].

References

[1] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*, Dover Publications, (1976).

[2] R.C. Lyndon and P.E. Schupp *Combinatorial Group Theory*, Springer , (1977).

[3] G. Baumslag, A. Miasnikov and V. Shpilrain, *Open problems in combinatorial and geometric group theory*,,http://zebra.sci.ccny.cuny.edu/web/nygtc/problems/

[4] S.J. Pride, *On the residual finiteness and other properties of (relative) one-relator groups*, preprint (2006).

University of Glasgow

email: sjp@maths.gla.ac.uk

Some New Results on Goldie Dimension of Modules and Modular Lattices

Edmund R.Puczyłowski

It is well known that the concept of Goldie dimension can be extended from modules to modular lattices with zero element. Some constructions, which can be applied in this more general context, allow to express many properties of Goldie dimension more clearly, compare it with some other dimensions of modular lattices (e.g., the Kurosh-Ore dimension and the length). This can be applied in studies of modules (e.g., applying the results on Goldie dimension of lattices to the lattice of submodules or to the dual lattice one gets uniformly some results on Goldie and dual Goldie dimension of the module). In the talk some new results obtained in this area will be surveyed. They in particular concern so called dimension modules, i.e., modules M such that for arbitrary submodules N, K, $u(N+K)+u(N\cap K) = uN+uK$, where u stands for the Goldie dimension. This concept can be in obvious way generalized to modular lattices. Some results concerning dimension lattices and their applications to modules will be presented.

Institute of Mathematics, University of Warsaw

email: edmundp@mimuw.edu.pl

Modules over Prüfer Domains which Satisfy the Radical Formula

Dilek Pusat-Yılmaz

Let M be a module over a ring R and N be a submodule of M with $N \neq M$. The *prime radical of N in M*, $rad_M(N)$, is defined to be the intersection of all prime submodules of M containing N. If there is no prime submodule containing N, then $rad_M(N) = M$. In particular $rad_M(M) = M$.

Let M be an R-module and N a submodule of M. The *envelope of N in M* which is denoted by $E_M(N)$ is defined to be the set

$$\{rm : r \in R, m \in M \text{ such that } r^n m \in N \text{ for some } n \in \mathbb{Z}^+\}.$$

We say that a module M satisfies the radical formula (M s.t.r.f.), if for every submodule N of M, the prime radical of N is the submodule generated by its envelope, that is, $rad_M(N) = \langle E_M(N)\rangle$. A ring R s.t.r.f. provided that for every R-module M, M s.t.r.f..

The question of what kind of rings and modules s.t.r.f. has drawn the attention of many authors. In [1], Jenkins and Smith proved that Dedekind domains s.t.r.f.. In [2], Leung and Man proved that the only Noetherian rings which s.t.r.f. are of at most dimension one and they gave a complete characterization of Noetherian rings which s.t.r.f. Now we are looking for non-Noetherian rings which s.t.r.f. For that reason we investigated whether modules over Prüfer domains s.t.r.f.. We proved that if R is a Prüfer domain, then the R-module $R \oplus R$ s.t.r.f..

References

[1] J.Jenkins and P. F. Smith, On the prime radical of a module over a commutative ring, *Comm. Algebra* **20**(1992), 3593-3602.

[2] Ka Hin Leung and S. H. Man, On Commutative Noetherian Rings which Satisfy the Radical Formula, *Glasgow Math.J.*, **39** (1997), 285-293

[3] S.H. Man, One dimensional domains which satisfy the radical formula are Dedekind domains, *Arch. Math.*, **66**(1996), 276-279.

[4] R. L. McCasland and M. E. Moore, On radicals of submodules of finitely generated modules, *Canad. Math. Bull.* **29**(1), 1986, 37-39.

[5] R. L. McCasland and M. E. Moore, On Radicals of Submodules, *Comm. Algebra*, **19**(5) (1991), 1327-1341.

Izmir Institute of Technology

email: dilekyilmaz@iyte.edu.tr

Artin's conjecture on primitive roots in historical perspective

Peter Roquette

In any algebra course we teach (hopefully) our students that the multiplicative group of any finite field is cyclic. This fact was observed and proved by Gauss 1801; his proof is still the best and shortest. Any element which generates the multiplicative group of $\mathbb{Z}/p$ is called a *primitive root* modulo p. Again, it was Gauss who described a method how to compute a primitive root for a given prime number p. The knowledge of a primitive root t is relevant for computations within $\mathbb{Z}/p$ since every non-zero element can be represented by its "logarithm" with respect to t which permits to reduce *multiplication* within $\mathbb{Z}/p$ to *addition* in $\mathbb{Z}$ modulo $p-1$. This is important in today's programs for coding and cryptography where one has to deal with very large primes p.

Artin has raised the question whether a given integer t can be used as a primitive root for infinitely many primes p (with the exception of those cases where one can trivially see this is not so). Artin conjectured that this is indeed the case, and he even conjectured the relative density of those primes (compared to the set of all primes). His conjectured value of the density was

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.373955\ldots$$

which is now called "Artin's constant". Artin never published this conjecture or any paper dealing with this topic. But we know precisely the date when he uttered this conjecture for the first time: this was September 13, 1927 when Artin had visited Hasse. In his mathematical diary of that day Hasse had noted down Artin's conjecture.

We shall report how Hasse had taken up Artin's conjecture. There were two doctor students of Hasse who (unsuccessfully) tried to solve this problem. Erdös as a young mathematician tried to solve it too but in vain. It was Emma Lehmer who first tried to check this conjecture by computer computations (in the days when computers were still quite slow) but she found that already $a = 5$ did not seem to blend with the numerical value Artin had given. In a correspondence with Emma Lehmer in December 1957 Artin had to modify his conjectured relative density in certain cases, e.g., if t is prime and $\equiv 1 \bmod 4$. We shall report about the present status of Artin's conjecture which has been "almost" proved (with the modified conjectural densities). If time permits then we will also report about our correspondence with Gunduz Ikeda on the Artin conjecture.

University of Heidelberg, Germany

email: roquette@uni-hd.de

web: roquette.uni-hd.de

Noether-Lefschetz locus for Beilinson-Hodge cycles on open complete intersections

S. Saito

The infinitesimal method in Hodge theory is fruitful in various aspects of algebraic geometry. The idea originates from Griffiths work [Gri] where the Poincaré residue representation of cohomology of a hypersurface played a crucial role in proving the infinitesimal Torelli theorem for hypersurfaces. Since then many important applications of the idea have been made in different geometric problems such as the generic Torelli problem and the Noether-Lefschetz theorem for Hodge cycles and the study of algebraic cycles (see [G1], Lectures 7 and 8). In this lecture we explain that the method can be applied to study an analog of the Noether-Lefschetz theorem in the context of Beilinson's Hodge conjecture.

Let $X \subset \mathbb{P}^n$ be a smooth projective variety over $\mathbb{C}$. Recall that the Hodge conjecture for X predicts that the space of Hodge cycles in codimension q on X is generated by cohomology classes of algebraic subvarieties on X, namely the cycle class map from the the Chow group to the singular cohomology of X:

$$CH^q(X) \otimes \mathbb{Q} \to H^{2q}(X, \mathbb{Q}(q)) \cap F^q H^{2q}(X, \mathbb{C})$$

is surjective, where $\mathbb{Q}(q) = (2\pi\sqrt{-1})^q\mathbb{Q} \subset \mathbb{C}$ and F^* denotes the Hodge filtration. Let

$$H^{2q}(X, \mathbb{Q}(q))_{triv} \subset H^{2q}(X, \mathbb{Q}(q)) \cap F^q H^{2q}(X, \mathbb{C}),$$

be the (one-dimensional) $\mathbb{Q}$-subspace generated by the class of the section on X of a linear subspace of codimension q in $\mathbb{P}^n$. It is called the space of trivial cycles.

Now let S be a non-singular quasi-projective variety over $\mathbb{C}$ and assume that we are given $\mathcal{X} \hookrightarrow \mathbb{P}^n_S$, an algebraic family over S of smooth projective varieties. Let X_t be the fiber of $\mathcal{X}$ over $t \in S$. Then the Noether-Lefschetz locus for Hodge cycles in codimension q on $\mathcal{X}/S$ is defined to be

$$S^q_{NL} = \{t \in S |\ F^q H^{2q}(X_t, \mathbb{C}) \cap H^{2q}(X_t, \mathbb{Q}(q)) \neq H^{2q}(X_t, \mathbb{Q}(q))_{triv}\}.$$

It is the locus of such $t \in S$ that there exist non-trivial Hodge cycles in codimension q on X_t and hence that the Hodge conjecture is non-trivial for X_t. One can prove S^q_{NL} is the union of countable number of (not necessarily proper) closed algebraic subsets of S.

Now we take S to be the moduli space of smooth hypersurfaces of degree d in $\mathbb{P}^3$ and $\mathcal{X}/S$ to be the universal family of hypersurfaces. Let S_{NL} denote S^q_{NL} for $q = 1$. It is the locus of those surfaces that possess curves which are not complete intersections of the given surface with another surface. The celebrated theorem of Noether-Lefschetz affirms that every component of S_{NL} has positive codimension in S when $d \geq 4$. M. Green and C. Voisin have refined it to show the following striking theorem:

Theorem 3. *([G2], [G3], [V]) For every irreducible component T of S_{NL},* $\mathrm{codim}(T) \geq d - 3$. *If $d \geq 5$, the only irreducible component of S_{NL} having codimension $d - 3$ is the family of surfaces of degree d containing a line.*

Let U be a (non-complete) smooth variety over $\mathbb{C}$. Beilinson's Hodge conjecture for U predicts the surjectivity of the regulator maps:

$$reg^q_{U_t} \ : \ CH^q(U,q)\otimes\mathbb{Q} \to H^q(U,\mathbb{Q}(q))\cap F^qH^q(U,\mathbb{C}),$$

where $CH^q(U,q)$ denotes Bloch's higher Chow group and $H^q(U,\mathbb{C})$ is endowed with the mixed Hodge structure defined by Deligne (see [J] for the definitions). Taking a smooth compactification $U\subset X$ with $Z=X\setminus U$, a simple normal crossing divisor on X, we have the following formula for the values of $reg^q_{U_t}$ on decomposable elements in $CH^q(U,q)$;

$$reg^q_{U_t}(\{g_1,\dots,g_q\}) = \frac{dg_1}{g_1}\wedge\cdots\wedge\frac{dg_q}{g_q} \in H^0(X,\Omega^q_X(\log Z)) = F^qH^q(U,\mathbb{C}),$$

where $\{g_1,\dots,g_q\}\in CH^q(U,q)$ is the products of $g_j\in CH^1(U,1)=\Gamma(U,\mathcal{O}^*_{Zar})$. Such elements of $CH^q(U,q)$ is called *decomposable* and we let

$$CH^q(U,q)_{dec}\subset CH^q(U,q)\otimes\mathbb{Q}$$

denote the subspace generated by decomposable elements. The description of $reg^q_{U_t}$ on non-decomposable elements are rather complicate. We put

$$H^q(U,\mathbb{Q}(q))_{triv} := reg^q_{U_t}(CH^q(U,q)_{dec}) \subset H^q(U,\mathbb{Q}(q))\cap F^qH^q(U,\mathbb{C}).$$

Now let S be a non-singular quasi-projective variety over $\mathbb{C}$ and assume given $\mathcal{U}\to S$, an algebraic family over S of non-complete smooth varieties. Let U_t be the fiber of $\mathcal{U}$ over $t\in S$. Then the Noether-Lefschetz locus for Beilinson-Hodge cycles on $\mathcal{U}/S$ is defined as

$$S^q_{NL} = \{t\in S|\ H^q(U_t,\mathbb{Q}(q))\cap F^qH^q(U_t,\mathbb{C}) \neq H^q(U_t,\mathbb{Q}(q))_{triv}\}.$$

In this lecture we explain some results on Noether-Lefschetz locus for Beilinson-Hodge cycles that are analogous to 3 obtained by the joint works with M. Asakura ([AS1] and [AS2]).

References

[AS1] M. Asakura and S. Saito, *Beilinson's Hodge conjecture for open complete intersections*, Math. Zeit. **252** (2006), 251–273

[AS2] M. Asakura and S. Saito, *Beilinson's Hodge conjecture for open complete intersections, II*, preprint

[G1] M. Green *Infinitesimal methods in Hodge theory*, Lecture Notes in Math., **1594** (1993), 1-92 Springer-Verlag

[G2] M. Green, *A new proof of the explicit Noether-Lefschetz theorem*, J. Differential Geometry, **27** (1988), 155-159

[G3] M. Green, *Components of maximal dimension in the Noether-Lefschetz locus*, J. Differential Geometry, **29** (1989), 295-302

[Gri] P. Griffiths *Periods of certain rational integrals:I and II*, Ann. of Math., **90** (1969), 460-541

[J] U.Jannsen, *Mixed motives and Algebraic K-Theory*, Lecture Notes in Math., **1400** (1980), Springer-Verlag

[V] C. Voisin, *Une précision concernant le théorem de Noether*, Math. Ann., **280** (1988), 605-611

Graduate School of Mathematical Sciences, University of Tokyo, 3-8-1 Komaba, Tokyo, 153-8914 JAPAN

email: sshuji@msb.biglobe.ne.jp

Generalized Fesenko Reciprocity Map : Non-abelian Local Class Field Theory

Erol Serbest

This talk describes our recent joint work with K. I. Ikeda [12], which has been announced in the XVIII. National Mathematics Symposium during the period September 5-8, 2005.

In [1, 2, 3], Fesenko has defined the non-abelian local reciprocity maps, in the sense of Koch, for every totally-ramified arithmetically profinite Galois extension (APF-extension) of a given local field K by extending the works of Hazewinkel and Iwasawa-Neukirch. The theory of Fesenko extends the previous non-abelian generalizations of local class field theory by Koch-de Shalit [15] and by Gurevich [7]. In this talk, we construct the non-abelian local reciprocity maps for every Galois extension of K by generalizing the local Fesenko reciprocity maps, and build the non-abelian local class field theory in the sense of Koch philosophy. In order to do so, we first review the APF-extensions over the local field K and their corresponding fields of norms introduced by Fontaine and Wintenberger, and the theory of p-adic Lie extensions over K developed by Fontaine and Wintenberger in the equi-characteristic case and by S. Sen in the non-equi-characteristic case respectively, and prove that certain Galois extensions $\Gamma_d^{(n)}/K$ defined for each $1 \leq n, d \in \mathbb{Z}$ are APF, and are the building blocks of the extension K^{sep}/K, as

$$K^{sep} = \bigcup_{1 \leq n \in \mathbb{Z}} \bigcup_{1 \leq d \in \mathbb{Z}} \Gamma_d^{(n)}.$$

For each $1 \leq n, d \in \mathbb{Z}$, the definition of $\Gamma_d^{(n)}$ involves a fixed Lubin-Tate splitting φ over the local field K, and is defined to be the maximal n-abelian extension in the fixed field K_{ϕ^d} of ϕ^d. In case $n = d = 1$, this theorem is a special case of the well-known fact in Fontaine-Wintenberger theory that *any* totally-ramified abelian extension over K is APF, which follows from theorems of S. Sen (non-equi-characteristic case), and of J.-P. Wintenberger (equi-characteristic case) on p-adic Lie extensions of local fields (cf. [19] and [25]). Next, we review the construction of the local Fesenko reciprocity map $\phi_{L/K}^{(\varphi)}$ defined for any totally-ramified and APF-Galois extension L over K and use the functorial properties of the local Fesenko reciprocity maps defined for totally-ramified and APF-Galois extensions over K to construct the generalized local Fesenko reciprocity map

$\Phi_K^{(\varphi)}$ for the absolute Galois extension K^{sep}/K as a projective limit of local Fesenko reciprocity maps $\phi^{(\varphi)}_{\Gamma_d^{(n)}/K}$ for the totally-ramified and APF-Galois extensions $\Gamma_d^{(n)}/K$ for every $1 \leq n, d \in \mathbb{Z}$. Finally, we investigate the functorial and ramification-theoretic properties of the generalized local Fesenko reciprocity map $\Phi_K^{(\varphi)}$ for the absolute Galois extension K^{sep}/K and build the non-abelian local class field theory in the sense of Koch.

A similar theory have been announced by F. Laubie [16] in Journées Arithmétiques XXIV during the period July 4-8 2005 as well. The relationship of these two theories will be investigated elsewhere in the near future.

References

[1] I. B. Fesenko, *Noncommutative local reciprocity maps*, Class Field Theory - Its Centenary and Prospect (Ed. K. Miyake), Advanced Studies in Pure Math. **30**, 2001, 63-78

[2] I. B. Fesenko, *On the image of noncommutative local reciprocity map*, Homology, Homotopy and Appl. **7**, 2005, 53-62.

[3] I. B. Fesenko, *Local reciprocity cycles*, Invitation to Higher Local Fields (Ed. I. B. Fesenko, M. Kurihara), Geometry & Topology Monographs **3**, Warwick, 2000, 293-298

[4] I. B. Fesenko, S. V. Vostokov, *Local Fields and Their Extensions: A Constructive Approach*, AMS Translations of Mathematical Monographs **121**, AMS, Providence, Rhode Island, 1993

[5] J.-M. Fontaine, J.-P. Wintenberger, *Le "corps des normes" de certaines extensions algébriques de corps locaux*, C. R. Acad. Sci. Paris Sér. A Math. **288**, 1979, 367-370

[6] J.-M. Fontaine, J.-P. Wintenberger, *Extensions algébriques et corps des normes des extensions APF des corps locaux*, C. R. Acad. Sci. Paris Sér. A Math. **288**, 1979, 441-444

[7] A. Gurevich, *Ph.D. Thesis*, Humboldt Univ., Berlin, 1997

[8] M. Hazewinkel, *Local class field theory is easy*, Adv. Math. **18**, 148-181.

[9] K. I. Ikeda, *On the metabelian local Artin map I: Galois conjugation law*, Tr. J. of Math. **24**, 2000, 25-58

[10] K. I. Ikeda, *On the metabelian local Artin map II: Metabelian transfer law* (preprint)

[11] K. I. Ikeda and M. Ikeda, *Two lemmas on formal power series*, Tr. J. of Math. **23**, 1999, 435-440

[12] K. I. Ikeda and E. Serbest, *Generalized Fesenko reciprocity map : Non-abelian local class field theory* (preprint)

[13] K. Iwasawa, *Local Class Field Theory*, Oxford Univ. Press and Clarendon Press, Oxford and New York, 1986.

[14] K. Iwasawa, *local Class Field Theory*, Iwanami-Shoten, Tokyo, 1980.

[15] H. Koch and E. de Shalit, *Metabelian local class field theory*, J. reine angew. Math. **478**, 1996, 85-106

[16] F. Laubie, *Une théorie du corps de classes local non abélien* (preprint)

[17] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math. IHES **26**, 1965, 389-603

[18] J. Neukirch, *Class Field Theory*, Springer-Verlag, Berlin and Heidelberg, 1986.

[19] S. Sen, *Ramification in p-adic Lie extensions*, Invent. Math. **17**, 1972, 44-50

[20] J.-P. Serre, *Sur les groupes de Galois attachés aux groupes p-divisibles*, Proc. of Conf. on Local Fields, Driebergen, 1966, Springer-Verlag, Berlin, Heidelberg, New York, 1967, pp. 118-131

[21] J.-P. Serre, *Abelian ℓ-adic Representations and Elliptic Curves*, Benjamin, New York, 1968

[22] J.-P. Serre, *Corps Locaux*, 2^e éd., Publications de l'Institut de Mathématique de l'Université de Nancago, Actualités Sci. Indust. **1296**, Hermann, Paris, 1968

[23] J.-P. Serre, *Lie Algebras and Lie Groups*, 2^{nd} Ed., Lecture Notes in Math. **1500**, Springer-Verlag, Berlin, Heidelberg, New York, 1992

[24] J.-P. Wintenberger, *Le corps des normes de certaines extensions infinies de corps locaux; applications*, Ann. sci. Éc. Norm. Sup. **46**, 1983, 59-89

[25] J.-P. Wintenberger, *Extensions de Lie et groupes d'automorphismes des corps locaux de charactéristique p*, C. R. Acad Sci. Paris Sér. A Math. **288**, 1979, 477-479

Atılım University

email: eserbest@atilim.edu.tr

On K3 surfaces and lattices

Ali Sinan Sertöz

A K3 surface X is a simply connected compact complex surface with a nowhere vanishing holomorphic 2-form ω. The second integral cohomology of a K3 surface is an integral lattice which is isomorphic to the so called K3 lattice $\Lambda = U^3 \oplus E_8(-1)^2$. When this K3 surface accepts a fixed point free involution, the quotient space under this involution is an Enriques surface. It has no nonzero holomorphic form on it and the free part of its second integral cohomology is isomorphic to the lattice $E = U \oplus E_8(-1)$. A common reference for surfaces is [1].

This talk will mainly be expository in nature to explain how these lattices Λ, E and the 2-form ω together reveal so much of the geometry associated to the K3 and the Enriques surfaces. Building on this I will report briefly on a joint work with Caner Koca on the irreduciblity of some Heegner divisors in the moduli space of Enriques surfaces, see [3].

For the interplay between K3 and Enriques surfaces we can quote [2, 6, 8]. For the role of ω, we can refer to [5]. The generic references for matters of lattices are [4, 7].

References

[1] Barth et al, *Compact Complex Surfaces*, Second enlarged edition, Springer Verlag, 2004.

[2] Keum, J. H.; Every algebraic Kummer surface is the K3 cover of an Enriques surface, Nagoya Math J 118 (1990) 99-100.

[3] Koca, C., Sertöz, A. S., Orbits in the anti invariant sublattice of the K3 lattice, *preprint*.

[4] Milnor, J., Husemoller, D., *Symmetric Bilinear Forms*, Springer Verlag, 1973.

[5] Pjatečkiĭ-Šhapiro, I. Z., Šafarevič, I. R., A Torelli theorem for algebraic surfaces of type K3, Math USSR Izv., 5 (1971), 547-588.

[6] Namikawa, Y., Periods of Enriques surfaces, Math. Ann., 270 (1985), 201-222.

[7] Nikulin, V. V., Integral symmetric bilinear forms and some of their applications, Math. USSR Izv., 14 (1980), 103-167.

[8] Sertöz, A. S., Which singular K3 surfaces cover an Enriques surface, Proc. AMS, 133 (2005), 43-50.

Bilkent University, Ankara

email: `sertoz@bilkent.edu.tr`

web: `http://www.bilkent.edu.tr/~sertoz`

Compressible and Related Modules

Patrick F. Smith

Let R be a ring. A non-zero R-module is called compressible provided M embeds in each of its non-zero submodules. Every compressible module M is prime in the sense that M is non-zero and M and N have the same annihilator in R for every non-zero submodule N of M. Compressible modules are described for rings R which satisfy certain chain and other conditions. The class of compressible R-modules is clearly closed under taking submodules but not under taking direct sums (coproducts). This leads to the investigation of larger classes of modules which will also be discussed.

University of Glasgow

email: `pfs@maths.gla.ac.uk`

Four applications of $\mathbb{Z}_4-$codes

Patrick Solé

We survey the four main applications of $\mathbb{Z}_4-$codes in the nineties: low correlation sequences [5], nonlinear binary codes [4], lattices [1, 2], combinatorial designs [3]. The results include but are not limited to

- the first quaternary sequence meeting the Sidelnikov bound
- the formal duality of Kerdock and Praparata Codes
- the simplest construction of the Leech lattice known to date

- new 5-designs on 24 points besides the Witt designs

We give pointers to more recent trends like OFDM and space time codes.

References

[1] A. Bonnecaze, C. Bachoc,P. Solé, B. Mourrain Type II Codes over $\mathbb{Z}_4$, *IEEE Trans. on Information Theory*, **43** (1997) 969-976.

[2] A. Bonnecaze, P. Solé, A.R. Calderbank, Quaternary Construction of Unimodular Lattices, *IEEE Trans. on Information Theory* , **41** , (1995) 366-377.

[3] A. Bonnecaze, E.M. Rains,P. Solé, 3-Colored 5-Designs and $\mathbb{Z}_4$-Codes , *J. Statistical Plan. Inf.*, **86** (2000) 349-368.

[4] R. Hammons, V.P. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock Preparata Goethals and related codes, *IEEE Trans. of Information Theory* , **40**, (1994) 301–319.

[5] P. Solé, A quaternary cyclic code, and a family of quadriphase sequences with low correlation properties, *Springer Lect. Not. Comp. Sc. 388*, 1988, 193–201.

CNRS-I3S, ESSI, route des Colles, 06903 Sophia Antipolis, France

email: sole@essi.fr

Exceptional Groups

T. A. Springer

In the classification of simple Lie groups and simple algebraic groups five "exceptional" types appear, named G_2, F_4, E_6, E_7, E_8. The problem to understand these groups over an arbitrary base field has only been solved for the first two types.

In the talk I will review a number of known facts. If time permits I will discuss results of the paper [1] about certain forms of E_7, appearing as invariance groups of quartic forms in 56 dimensions.

References

[1] T. A. Springer, Some groups of type E_7, to appear in Nagoya Math. J.

University of Utrecht

email: springer@math.uu.nl

Amply Cofinitely Supplemented Lattices

S. Eylem Toksoy

L will mean a modular lattice with greatest element 1. L is called *supplemented* if every element a of L has a supplement, i.e. an element b minimal with respect to $a \vee b = 1$. An element b is a supplement of a in L if and only if $a \vee b = 1$ and $a \wedge b \ll b/0$. An element a of a complete lattice L is called *compact* if for every subset X of L with $a \leq \bigvee X$ there exists a finite subset F of X such that $a \leq \bigvee F$. A lattice L with greatest element 1 is said to be *a compact lattice* if 1 is compact. An element a of a lattice L is called *cofinite* in L if the quotient sublattice $1/a$ is compact. A lattice L is called *cofinitely supplemented* if every cofinite element of L has a supplement in L. An element a of a lattice L has *ample supplements* in L if for every element b of L with $a \vee b = 1$, $b/0$ contains a supplement of a in L. A lattice L is called *amply supplemented* if every element of L has ample supplements, moreover L is called *amply cofinitely supplemented* if every cofinite element of L has ample supplements.

Lemma 4. *If a lattice L is amply cofinitely supplemented then the quotient sublattice $1/a$ is amply cofinitely supplemented for every element a of L.*

Definition. A lattice L is called *local* if the set of elements different from 1 has a largest element.

Lemma 5. *Let $\{l_i/0\}_{i\in I}$, where $I = \{1, ..., m\}$ be a finite collection of local sublattices of a lattice L and a be an element of L such that $a \vee (\bigvee_{i\in I} l_i)$ has a supplement b in L. Then there exists a subset J of I such that $b \vee (\bigvee_{i\in J} l_i)$ is a supplement of a in L.*

Definition. A lattice L is called *semilocal* if $1 = \bigvee_{i=1}^{n} l_i$, where $l_i/0$ is local.

Theorem 6. *A lattice L is amply cofinitely supplemented if and only if for every cofinite element a and an element b of L with $a \vee b = 1$ there exists an element c with $c/0$ a semilocal sublattice of $b/0$ such that $a \vee c = 1$.*

Joint work with: Rafail Alizade, İzmir Institute of Technology

email: rafailalizade@iyte.edu.tr

References

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

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

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

İzmir Institute of Technology

email: eylemtoksoy@iyte.edu.tr

web: www.iyte.edu.tr/~eylemtoksoy/

A generalization of the Weierstrass semigroup

Nesrin Tutaş

This talk will be a presentation of a joint work with Peter Beelen(Danish Technical University).

Let $\mathcal{C}$ be a nonsingular algebraic curve defined over a finite field $\mathbb{F}$. Throughout, the field $\mathbb{F}$ should be finite of cardinality $|\mathbb{F}| > n$. Let P be a rational point on the curve $\mathcal{C}$. The Weierstrass semigroup $H(P)$ is defined as the set of integers k such that there exists a function on $\mathcal{C}$ having pole divisor exactly kP. From this description of $H(P)$ it is clear that one could generalize the Weierstrass semigroup to $n-$tuples of rational points $P_1, \ldots, P_n$. Especially for small n, this semigroup and its gaps have been studied extensively.

In this work we will state a different generalization of Weierstrass semigroup to n-tuples. In particular, we will give more detail results for $n = 2$, and we will illustrate the theory by calculating semigroups for the Hermitian and Suzuki curves.

References

[1] Garcia A. and Viana P., Weierstrass points on certain non-classical curves, Arch. Math., 46, 315–322, 1986.

[2] Graham R.L. Knuth D.E. and Patashnik O. Concrete Mathematics, Second Edition, Reading, Massachusetts: Addison-Wesley, 1994.

[3] Hansen J.P. and Stichtenoth H., Group codes on certain algebraic curves with many rational points, Applicable Algebra in Engineering, Commnication and Computing, 1, 67–77, 1990.

[4] Homma M., The Weierstrass semigroup of a pair of points on a curve, Arch. Math., 63, 337–348, 1996.

[5] Ishii N., Weierstrass gap sets for quadruples of points on compact Riemann surfaces, Journal of Algebra, 250, 44–66, 2002.

[6] Kim S.J., On the index of the Weierstrass semigroup of a pair of points on a curve, Arch. Math., 62, 73–82, 1994.

[7] Matthews G., Weierstrass Pairs and Minimum Distance of Goppa Codes, Design, Codes and Cryptography, 22, 107–121, 2001.

[8] Matthews G., Codes from the Suzuki function field, G. L. Matthews, IEEE Transactions on Information Theory, 50,12,2398–3302,2004.

[9] Stichtenoth H, Algebraic function Fields and codes, Springer-Verlag,1993.

[10] Tsfasman M.A. and Vladut G., Algebraic-geometric codes, Kluwer, Dordrecht, 1991.

Akdeniz University, Antalya

email: ntutas@akdeniz.edu.tr

A-solvable groups

Bill Wickless

Let A be a fixed abelian group (or R-module). Then B is called A-projective if $(*) : B \oplus B' \cong A^k$. One tool used by group and module theorists is that studying A-projective groups is equivalent to studying finitely generated projective right E-modules, where E is the endomorphism ring of A. The reason for this is that from $(*)$ we obtain a direct sum decomposition of right E-modules: $Hom(A,B) \oplus Hom(A,B') \cong E^k$. Here the abelian group $Hom(A,B)$ becomes an E-module in the natural way: for $f \in Hom(A,B)$ and $\lambda \in E$, the map $(f\lambda) : A \to B$ is given by $(f\lambda)(a) = f(\lambda a)$. Conversely, if $M \oplus M' \cong E^k$ is a decomposition of right E-modules, then tensoring with the left module ${}_EA$ gives us the abelian group decomposition $(M \otimes_E A) \oplus (M' \otimes_E A) \cong E^k \otimes_E A \cong A^k$. What makes this work (makes this be a category equivalence) is that, if B is A-projective, then the evaluation map $e_B : Hom(A,B) \otimes_E A \to B$ is an isomorphism.

We study A-solvable groups; that is, those groups B such that e_B is an isomorphism. The class $\mathcal{C}_A$ of A-solvable groups strictly contains the class of A-projective groups and $\mathcal{C}_A$ is a weak isomorphism invariant of A. Here are a few typical theorems:

(1) If A is a mixed abelian group in the class $\mathcal{G}$ (to be defined in the talk), every subgroup B of finite index is A-generated (e_B is onto) and every A-generated group is A-solvable. Neither of these claims holds for torsion-free finite rank (tffr) abelian groups.

(2) If $E(A)$ is a Dedekind domain, then A-generated groups are A-solvable.

References

[1] U. Albrecht; Modules with Morita-equivalent endomorphism rings, Houston J. Math. 28 (2002), 665-81.

[2] U. Albrecht and W. Wickless, Homological properties of quotient divisible groups, Comm. Alg. 32 (2004), 2407-23.

Dept. of Math., University of Connecticut, Storrs, CT, 06269, USA

email: `wickless@math.uconn.edu`

web: `www.math.uconn.edu/people`

Comparison of complexity measures for binary sequences

Arne Winterhof

(joint work with Nina Brandstätter)

Various complexity measures for the randomness of binary sequences are in use. We prove several relations between such complexity measures and focus on the following two comparisons:

1. Linear complexity and correlation measure

   A high linear complexity profile is a measure for the unpredictability of a sequence and thus a desirable feature of sequences used for cryptographical purposes. For a given binary sequence we estimate its linear complexity profile in terms of the correlation measure, which was introduced by Mauduit and Sárközy and is a measure for the independence of several shifts of the original sequence.

2. Nonlinearity of Binary Sequences with Small Autocorrelation

   Sequences and Boolean functions for cryptographic purposes have to fulfil several randomness properties as a low autocorrelation and a high nonlinearity, respectively. The autocorrelation is a measure for the independence of a sequence from a single shift of it and the nonlinearity is a measure for the distance of a Boolean function from linear functions. For a given periodic sequence we estimate the nonlinearity of a naturally associated Boolean function in terms of the maximal absolute value of the aperiodic autocorrelation of the sequence.

References

[1] N. Brandstätter and A. Winterhof, Linear complexity profile of binary sequences with small correlation measure, Periodica Mathematica Hungarica, to appear.

[2] N. Brandstätter and A. Winterhof, Nonlinearity of binary sequences with small autocorrelation, Proceedings of the 2nd International Workshop on Sequence Design and its Applications in Communications (IWSDA'05), 44–47.

Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Linz, Austria

email: `arne.winterhof`

web: `http://www.ricam.oeaw.ac.at/`

Polynomial decomposition

Michael Zieve

Consider the operation of *composition* on polynomials over a field K, namely $(f \circ g)(x) = f(g(x))$. A polynomial of degree at least 2 is called *indecomposable* if it cannot be written as the composition of polynomials of strictly lower degree. Every polynomial f of degree at least 2 can be written as the composition of indecomposable polynomials, but this decomposition need not be unique. However, if K has characteristic zero, then results of Ritt, Levi, Engstrom, and Schinzel provide a complete theory of decompositions of polynomials – for instance, any two decompositions of f must have the same length, and it is known how to produce all decompositions of f from any single decomposition.

After reviewing these classical results, and sketching the Galois-theoretic proofs, I will turn to the more complicated case of positive characteristic. I will present various theorems, examples, conjectures and questions.

Along the way I will discuss the difficult problem of computing the intersection of two subfields of $K(x)$, as well as results on reducibility of 'variables-separated' polynomials $f(x) - g(y)$.

Center for Communications Research – Princeton

email: zieve@idaccr.org

Poster

Rough Sets and Its Algebraic Applications

Hacı Aktaş and Filiz Erdoğan

The notion of rough sets has been introduced by Pawlak. In this paper, basic notions of the rough set theory will be given. The paper concerns a relationship between rough set and algebraic structures. Rough group was introduced by Bismas and Nanda with respect to a normal subgroup a group. The notion of rough ring proposed by Davvaz with respect to an ideal of a ring which is an extended notion of a subring in a ring. In this study, we shall define rough field by using a relation on the integral domain and give some properties of the lower and upper approximations in the field of quotients of an integral domain.

References

[1] B. Bismas and S.Nanda, Rough groups and rough subgroups, Bull. Polish Acad. Sci. Math. 42 (1994), 251-254.

[2] Z. Bonikowaski, Algebric structures of rough sets, Fuzzy Sets and Knowledge Discovery (1995), 242-247.

[3] B. Davvaz, Roughness in rings, Information Sciences 164 (2004), 147-163.

[4] J. B. Fraleigh, A First Course in Abstract Algebra, New York (1994).

[5] T. Iwinski, Algebric approach to rough sets, Bull. Polish Acad. Sci. Math. 35 (1987), 673-683.

[6] N. Kuroki, Rough ideals in semigroups, Inform. Sci. 100(1997), 139-163.

[7] N.Kuroki and P. P. Wang, The lower and upper approximations in fuzzy group, Inform. Sci. 90 (1996), 203-220.

[8] S. Nanda, Fuzzy fields and fuzzy linear spaces, Fuzzy Sets and Systems 19 (1986), 89-94.

[9] Z. Pawlak, Rough Sets, Int. J. Inf. Comp. Sci. 11 (1982), 341-356.

[10] Z. Pawlak, Rough sets: basic notions, ICS PAS Rep. 436 (1981).

[11] Z. Pawlak, Some remarks on rough sets, Bull. Pol. Ac. Tech. 33 (1985).

[12] A. Rosenfeld, Fuzzy groups, J. Math. Anal. Appl. 35 (1971), 512-517.

Department of Mathematics, Gaziosmanpasa University

email: haktas@gop.edu.tr,ferdogan@gop.edu.tr

6 Participants

Hüseyin Acan	acan@fen.bilkent.edu.tr
Esen Aksoy	eaksoy@su.sabanciuniv.edu
Hacı Aktaş	haktas@gop.edu.tr
Ersan Akyıldız	ersan@metu.edu.tr
Yılmaz Akyıldız	akyildiz@boun.edu.tr
Emine Albaş	emine.albas@ege.edu.tr
Selma Altınok	saltinok43@yahoo.com
Salim Ali Altuğ	geyikali@gmail.com
Murat Altunbulak	murat.altunbulak@gmail.com
Nurullah Ankaralıoğlu	ankarali@atauni.edu.tr
Nurcan Argaç	nurcan.argac@ege.edu.tr
Aykut Arslan	aykutmath@yahoo.com
Okan Arslan	oarslan@adu.edu.tr
Mesut Arslandok	mesutarslandok@mynet.com
Fırat Ateş	firat@balikesir.edu.tr
Gonca Ayık	agonca@cu.edu.tr
Hayrullah Ayık	hayik@cu.edu.tr
Simeon Ball	simeon@ma4.upc.edu
Şerban A. Basarab	Serban.Basarab@imar.ro
Alp Bassa	alp.bassa@uni-duisburg-essen.de
Oleg Belegradek	obelegradek@rambler.ru
M. Gökhan Benli	gokhan@metu.edu.tr
Ayşe Berkman	aberkman@metu.edu.tr
Mustafa Kemal Berktaş	m.k.berktas@gmail.com
Cansu Betin	cbetin@metu.edu.tr
Göksal Bilgici	gbilgici@gazi.edu.tr
Mehpare Bilhan	mehpare@metu.edu.tr
Hatice Boylan	boylan@fen.bilkent.edu.tr
Nina Brandstaetter	nina.brandstaetter@oeaw.ac.at
Dilek Buyruk	dilekbuyruk@yahoo.com
Engin Büyükaşık	enginbuyukasik@iyte.edu.tr
Vural Cam	cvural@metu.edu.tr
James B Carrell	carrell@math.ubc.ca
Stephen Cohen	sdc@maths.gla.ac.uk
Emrah Çakçak	cakcak@metu.edu.tr
Şermin Çam	sermincam5@yahoo.com
İlke Çanakçı	ilkecanakci@yahoo.com
Münevver Çelik	e127417@metu.edu.tr
Yasemin Çengellenmiş	ycengellenmis@yahoo.com
Ayça Çeşmelioğlu	cesmelioglu@su.sabanciuniv.edu
Ahmet Sinan Çevik	scevik@balikesir.edu.tr
Selçuk Demir	sdemir@bilgi.edu.tr
Musa Demirci	mdemirci@uludag.edu.tr
Yılmaz M Demirci	yilmazdemirci@iyte.edu.tr
Semra Doğruöz	dogruoz@aku.edu.tr
Askar Dzhumadil'daev	askar@math.kz
Şükrü Uğur Efem	ugurefem@gmail.com

Ali Bülent Ekin	A.Bulent.Ekin@science.ankara.edu.tr
Elçim Elgün	elcimelgun@yahoo.com
Filiz Erdoğan	ferdogan@mail.gop.edu.tr
Vahap Erdoğdu	erdogdu@itu.edu.tr
Bayram Ali Ersoy	ersoya@yildiz.edu.tr
Kıvanç Ersoy	kersoy@metu.edu.tr
Özgür Evren	oevren@bilgi.edu.tr
Meltem Finachine	meltemfinachine@yahoo.com
Öznur Gölbaşı	ogolbasi@cumhuriyet.edu.tr
Haydar Göral	hgoral@gmail.com
Seda Güllüoğlu	sedagulluoglu@hotmail.com
Cem Güneri	guneri@sabanciuniv.edu
Mustafa Hakan Güntürkün	ghakan@metu.edu.tr
A. Tuğba Güroğlu	tugba.guroglu@deu.edu.tr
Osman Can Hatipoğlu	can.hatipoglu@deu.edu.tr
İlhan İkeda	ilhan@bilgi.edu.tr
Sebahattin İkikardeş	sebahattinikikardes@gmail.com
Özlem İmamoğlu	ozlem@math.ethz.ch
Mustafa Devrim Kaba	e124469@metu.edu.tr
Müge Kanuni	muge.kanuni@boun.edu.tr
Fatih Karabacak	fatihkarabacak@anadolu.edu.tr
Ulaş Karadağ	ukaradag@bilgi.edu.tr
Erdal Karaduman	eduman@atauni.edu.tr
Yalçın Karataş	zykaratas@yahoo.com
Tolga Karayayla	tlgkryyl@yahoo.com
Özcan Kasal	ozcankasal@yahoo.com
Canan Kaşıkçı	canank@su.sabanciuniv.edu
Gülay Kaya	gukaya@gsu.edu.tr
Ruşen Kaya	krusen@metu.edu.tr
Barış Kendirli	bkendirli@fatih.edu.tr
Derya Keskin Tütüncü	keskin@hacettepe.edu.tr
Melek Kılıç	melek_kl@yahoo.com
Ömer Faruk Koç	farukoc@gmail.com
Emre Kolotoğlu	emkolot@yahoo.com
Fatih Koyuncu	fatih@mu.edu.tr
Feride Kuzucuoğlu	feridek@hacettepe.edu.tr
Mahmut Kuzucuoğlu	matmah@metu.edu.tr
Gilles Lachaud	lachaud@iml.univ-mrs.fr
Vladimir Levchuk	levchuk@lan.krasu.ru
James Lewis	lewisjd@ualberta.ca
Christian Lomp	clomp@fc.up.pt
Ali Madanshekaf	a_madanshekaf@yahoo.co.uk
Wilfried Meidl	wmeidl@sabanciuniv.edu
Engin Mermut	engin.mermut@deu.edu.tr
Pınar Mete	pinarm@balikesir.edu.tr
Ray Mines	mines@math.uconn.edu
Nedim Narman	nedimnarman@gmail.com
Ali Nesin	anesin@bilgi.edu.tr
Gabriela Rino Nesin	nesinster@gmail.com

Kürşat Hakan Oral	khoral993@gmail.com
Figen Öke	fospo@hotmail.com
Neslihan Ös	neslihanos@yahoo.com
Ferruh Özbudak	ozbudak@metu.edu.tr
A. Çiğdem Özcan	ozcan@hacettepe.edu.tr
Mehmet Özdemir	mehmetozdemir@su.sabanciuniv.edu
Selahattin Özdemir	salahattin.ozdemir@deu.edu.tr
Şafak Özden	sozden@su.sabanciuniv.edu
Özen Özer	ozenozer2002@yahoo.com
Engin Özkan	eozkan@atauni.edu.tr
Engin Özkan	enozkan@metu.edu.tr
Ekin Özman	ekinozman@yahoo.com
Özer Öztürk	ozero@metu.edu.tr
Erdal Özyurt	eozyurt@adu.edu.tr
Soner Pehlivan	spehlivan@adu.edu.tr
Ayten Pekin	aspekin@hotmail.com
David Pierce	dpierce@metu.edu.tr
Gottlieb Pirsic	gottlieb.pirsic@oeaw.ac.at
Stephen Pride	sjp@maths.gla.ac.uk
Edmund Puczylowski	edmundp@mimuw.edu.pl
Dilek Pusat Yılmaz	dilekyilmaz@iyte.edu.tr
Peter Roquette	roquette@uni-hd.de
Shuji Satio	sshuji@msb.biglobe.ne.jp
Erol Serbest	eserbest@atilim.edu.tr
Sinan Sertöz	sertoz@bilkent.edu.tr
Patrick Smith	pfs@maths.gla.ac.uk
Patrick Solé	ps@essi.fr
Gökhan Soydan	gsoydan@uludag.edu.tr
Tonny Springer	springer@math.uu.nl
Henning Stichtenoth	henning@sabanciuniv.edu
Murat Şahin	Murat.Sahin@science.ankara.edu.tr
Nil Şahin	nilsahin16@hotmail.com
Hatice Şahinoğlu	hatice@fen.bilkent.edu.tr
Fatma Şengüler	fatma_senguler@yahoo.com
Ünsal Tekir	utekir@marmara.edu.tr
Eylem Toksoy	eylemtoksoy@iyte.edu.tr
Vladimir Tolstykh	tvlaa@rambler.ru
Serpil Top	serpiltop@iyte.edu.tr
Mustafa Topkara	topkara@metu.edu.tr
Alev Topuzoğlu	alev@sabanciuniv.edu
Hakan Tor	htor@metu.edu.tr
Bülent Tosun	tbulent@metu.edu.tr
Demirhan R. Tunç	dtunc@nd.edu
Nesrin Tutaş	ntutas@akdeniz.edu.tr
Erkan Murat Türkan	erkanmurat@yahoo.com
İ. Utku Türkmen	turkmen@fen.bilkent.edu.tr
Pınar Uğurlu	pugurlu@yahoo.com
William Wickless	wickless@math.uconn.edu
Arne Winterhof	arne.winterhof@oeaw.ac.at

Hasret Yazarlı	hyazarli@cumhuriyet.edu.tr
Muhammet Yazıcı	ytuyazici@hotmail.com
Gökhan Yener	yenergokhan82@hotmail.com
Yunus Emre Yıldırır	yildirir@balikesir.edu.tr
Zahide Yıldız	zahideyildiz@yahoo.com
Nazlı Yıldız İkikardeş	nyildizikikardes@gmail.com
Mohammed Yousif	myousif@lima.ohio-state.edu
Ayberk Zeytin	ayberkz@gmail.com
Michael Zieve	zieve@math.usc.edu

Organizers

Ayşe Berkman, Cem Güneri, Ferruh Özbudak, David Pierce, Henning Stichtenoth, Alev Topuzoğlu (chair)

7 Timetable

Wednesday	Thursday	Friday	Saturday	Sunday
	9.00: Sh. Saito	T. Springer	S. Ball	8.45: S. Sertöz
9.30: opening S. Cohen	9.50: coffee		10.00: E. Puczyłowski	9.45: P. Solé
10.30: coffee	10:20: S. Pride	P. Smith	10.50: coffee	10.35: coffee
11.00: C. Lomp	11.20: M. Zieve	İ. İkeda		farewell
12.00: J. Carrell	12.10: lunch			lunch
12.50: lunch				
		14.00: excursion		
14.30: ‖ sessions			15.30: ‖ sessions	
16.00: coffee				
16.30: Ö. İmamoğlu (tutorial)	G. Lachaud		17.00: coffee	
	17.30: Ö. İmamoğlu		17.30: P. Roquette	
(tutorial)				
18.30: reception				

See p. 4 for the detailed schedule:
p. 6 for the parallel sessions, and p. 7 for the special sessions