Involutions in group algebras

by

Zsolt Balogh

University College NYIREGHYAZA, Hungary

Let FG be a group algebra of a group G over a field F. The F-linear extension of the anti-automorphism of G which sends each group element to its inverse is called canonical involution of FG. Evidently, the canonical involution always exists so FG is always an algebra with involution. The involutions play an important role in the study of the structure of group algebras and their group of units despite of the fact that we know very little about them.

We say that an involution $*$ of FG arises from the group G if $*$ is F-linear extension of an involutive anti-automorphism of G. We should also remark that the canonical involution is also arises form G. Denote by FG_*^+ and FG_*^- the set of symmetric and skew-symmetric elements in FG under involution $*$, respectively, that is $FG_*^+ = \{x \in FG \mid x^* = x\}$ and $FG_*^- = \{x \in FG \mid x^* = -x\}$. Let $U(FG)^+$ denote the set of symmetric units in the unit group $U(FG)$ of FG and let $U_*(FG) = \{x \in U(FG) \mid x^{-1} = x^*\}$ the $*$-unitary subgroup of $U(FG)$, with respect to the involution $*$.

We would like to talk about Lie identities on the set of symmetric and skew-symmetric elements of FG and some group identities on $U(FG)^+$ and the structure of $U_*(FG)$, with respect to an involution which arises from G.

====================

About codes defined over skew polynomials

by

Delphine Boucher

Université de Rennes, France

In 1985, E. Gabidulin introduced a new metric, the rank metric, for which he built optimal codes, the Gabidulin (linearized evaluation) codes. He defined them as evaluation codes of linearized polynomials over a finite field $\mathbb{F}_{q^m}$. He also introduced the notion of q-cyclic codes for which he gave both generator and test matrices.

In this talk, after presenting the Gabidulin codes with the skew polynomial ring $\mathbb{F}_{q^m}[X;\theta]$, I will introduce the notion of module skew codes which generalize the Gabidulin q-cyclic codes.

A generator matrix for the module skew codes is the same as Gabidulin q-cyclic codes generator matrix. However, the construction of a test matrix for module skew codes requires to split the family of module skew codes in two subfamilies, the family of θ-constacyclic codes, whose dual are θ-constacyclic codes and the family of shortened θ-constacyclic codes, whose dual are punctured θ-constacyclic codes.

Lastly, the construction of self-dual skew codes will be presented and their best Hamming minimal distances over $\mathbb{F}_4$ will be given for lengths up to 78.

====================

Codes quasi-cycliques et suites rcurrentes linaires

by

Ahmed CHERCHEM

Faculté de Mathématiques, USTHB, Algérie

Les codes quasi-cycliques constituent une généralisation des codes cycliques. On se propose de passer en revue différents points de vue pour la représentation de tels codes. On précisera en particulier le lien entre les codes quasi-cycliques et les suites récurrentes linéaires.

====================

Avenues of research for codes over rings

by

Steven DOUGHERTY

Scranton University PA, USA

We describe recent trends in codes over rings and describe some open questions and avenues of research.

====================

Krull-Schmidt Theorem: the case two

by

Alberto Facchini

Università di Padova, Italy

I will mainly present the content of a joint paper with Pavel Příhoda (The Krull-Schmidt Theorem in the case two, Algebr. Represent. Theory 14(3) (2011), 545–570), but also other results obtained jointly with A. Amini, B. Amini, Ş. Ecevit, M. T. Koşan and N. Perone. Essentially, the Krull-Schmidt-Azumaya Theorem says that if $M_1, \ldots, M_m, N_1, \ldots, N_n$ are R-modules with local endomorphism rings and $M_1 \oplus \cdots \oplus M_m \cong N_1 \oplus \cdots \oplus N_n$, then $n = m$ and there exists a permutation σ of $\{1, \ldots, n\}$ such that $M_i \cong N_{\sigma(i)}$ for every $i = 1, \ldots, n$. I will present what happens if the endomorphism rings of the modules M_i and N_j have two maximal ideals instead of only one.

====================

Two sequences of ideals associated to an infinite idempotent matrix

by

Dolors Herbera

Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona) Spain

e-mail:dolors@mat.uab.es

Let E be a column-finite idempotent matrix over a ring R. Thinking E by columns we associate to it an ascending chain of finitely generated left ideals and, thinking E by rows, we associate to E a descending chain of right ideals of R. We will show how the properties of these two sequences translate into properties of countably generated projective right R-modules.

Special attention will be paid to the case of semilocal rings. For noetherian semilocal rings we can nicely describe all possibilities that can occur for countably generated projective right R-modules. The case of general semilocal rings is still a challenge: we will give some partial results and formulate questions around it.

The results I will talk about are part of an on going joint project with P. Příhoda.

====================

On strongly prime modules ideals and radicals

by

Algirdas Kaučikas

M.Romeris university, Vilnius, Lithuania

Let R be an associative ring with unit. A nonzero left R-module M is called *strongly prime* if for any non-zero $x, y \in \mathsf{M}$, there exits a finite set of elements $\{a_1, ..., a_n\} \subseteq R$, $n = n(x, y)$, such that $Ann_R\{a_1x, ..., a_nx\} \subseteq Ann_R\{y\}$. Taking $\mathsf{M} = R$, the notion of the one sided strongly prime ring is obtained.(See [3]). When we look at the ring R as the R-bimodule taking into account left and right action of R on itself, this immediately leads to the notion of an $M(R)$-module, where $M(R)$ is the multiplication ring of the ring R. When R is strongly prime as the module over its multiplication ring $M(R)$ it is called a *strongly prime* ring. Correspondingly, a submodule $\mathcal{P} \subset \mathsf{M}$ is called strongly prime if the quotient module $\mathsf{M}/\mathcal{P}$ is strongly prime.

Various characterizations of these notions in terms of annihilators of the elements of the module will be given. It will be shown how to produce strongly prime ideals of the ring using multiplicative sets of the ring. New results on the related radicals will be discussed.

References

[1] S.Amitsur, *On rings of quotients*, Symp. Mathematica 8, 149-164, (1972).

[2] P.Jara, P.Verhaege, A.Verschoren, *On the left spectrum of a ring*, Comm. Algebra, 22(8), 2983-3002, (1994).

[3] D.Handelman, L.Lawrence, *Strongly prime rings*, TAMS, 211, 209-223, (1975).

[4] A.Kaučikas, On the left strongly prime modules, ideals and radicals, in: A.Dubickas, A.Laurinčikas, and E.Manstavičius (Eds.), *Analytic and Probabilistic Methods in Number Theory*, TEV, Vilnius (2002), pp 119-123.

[5] A.Kaučikas, R.Wisbauer, Noncommutative Hilbert rings, Journal of Algebra and its Applications, Vol.3, Nr4, 437–443, 2004.

[6] A.Kaučikas, R.Wisbauer, On strongly prime rings and ideals, *Comm. Algebra*, **28**, 5461-5473, (2000).

[7] A.Rosenberg, *Noncommutative Algebraic Geometry and Representations of Quantized Algebras*, Kluwer, Dordrecht, 1995.

====================

Jacobians of Modular Curves, Divisors and Twists

by

Ekin OZMAN

Max Planck Iinstitute Math. Bonn, Germany

In this talk we will try to give an overview of some topics in Number Theory. We will focus on modular curves, their twists and jacobians. These objects are arithmetically very rich and have interesting applications to many interesting problems in Number Theory. We will talk about these problems and if time permits we'll give the proofs of some of them.

====================

Généralisation des courbes de Huff et applications en cryptographie.

by

Djiby SOW

Université Cheikh Anta Diop, Dakar SENEGAL

Recently two kinds of Huff curves were introduced as elliptic curves models and their arithmetic was studied.It was also shown that they are suitable for cryptography use such as Montgomery curves or Koblitz curves (in Weierstrass form) and Edwards curves,. In this work, we introduce the new generalized Huff curves $ax(y^2-c)=by(x^2-d)$ with $abcd(a^2c-b^2d)\neq 0$, which contains the generalized Huff's model $ax(y^2-d)=by(x^2-d)$ with $abd(a^2-b^2)\neq 0$ of Joye-Tibouchi-Vergnaud and the generalized Huff curves $x(ay^2-1)=y(bx^2-1)$ with $ab(a-b)\neq 0$; of Wu-Feng as a special case. The addition law in projective coordinates is as fast as in the previous particular cases. More generally all good properties of the previous particular Huff curves, including completeness and independence of two of the four curve parameters, extend to the new generalized Huff curves. We have verified that the method of Joye-Tibouchi-Vergnaud for computing of pairings can be generalized over the new curve.

Keywords: Public key cryptosystem, , elliptic curves, hyperelliptic curves, Edwards curves, jacobian.

====================

Right Gaussian rings and skew power series rings.

by

Michal ZIEMBOWSKI

Warsaw University of Technology, Poland.

In this talk we introduce a class of rings we call right Gaussian rings, defined by the property that for any two polynomials f, g over the ring R, the right ideal of R generated by the coefficients of the product fg coincides with the product of the right ideals generated by the coefficients of f and that of g, respectively. Prüfer domains are precisely commutative domains belonging to this new class of rings. In this talk we adduce the connections between right Gaussian rings and the classes of Armendariz rings and rings whose right ideals form a distributive lattice. We characterize skew power series rings that are right Gaussian, extending

to the noncommutative case a well-known result by Anderson and Camillo. We also study quotient rings of right Gaussian rings. (This talk is based on joint work with Ryszard Mazurek.)