Rev. Mat. Iberoamericana **19** (2003), 385–392

Nonassociative Algebras: Some Applications

Santos González and Consuelo Martínez

Abstract

Nonassociative algebras can be applied, either directly or using their particular methods, to many other branches of Mathematics and other Sciences. Here emphasis will be given to two concrete applications of nonassociative algebras. In the first one, an application to group theory in the line of the Restricted Burnside Problem will be considered. The second one opens a door to some applications of non-associative algebras to Error correcting Codes and Cryptography.

1. Introduction

It has been known, long ago, that some non-associative algebras, for instance Lie algebras, have important applications in Physics. In fact, many important classes of non-associative algebras, as Jordan algebras, have been originated in a Physics frame or have had a big development due to their applications in Physics. This is the case of Kac-Moody algebras (mainly affine algebras), vertex algebras or mutation algebras.

Some other non-associative algebras have been considered in relation to Differential Geometry (see [3]) or differential equations. For instance Lotka-Volterra algebras are associated to quadratic differential equations systems that appear in gas cinetic or populations dynamic (see [6] or [10]).

Genetic algebras appear in a Biological context, when one tries to formulate in an algebraic way the transmision of some characters in a random mate of populations (see [15]).

One of the most spectacular applications has been achieved with the use of non-associative algebras technics to solve problems in Group theory. The most significant example is the solution to the Restricted Burnside problem using ideas and results of Lie and Jordan algebras.

2000 Mathematics Subject Classification: Primary 17B60; Second. 20F40, 94A60, 94B60.
Keywords: Non-associative algebra, group, cryptography, Galois ring.

Let us remember that if F is a ground field of characteristic $\neq 2$, then a (linear) Jordan algebra is a vector space J with a binary bilinear operation $(x, y) \to xy$ satisfying the following identities:

(J1) $xy = yx$

(J2) $(x^2y)x = x^2(yx)$.

Relations between groups and non-associative algebras were already known and, indeed, as a consequence of a result by Jacobson relating groups and algebras, the construction made by Golod and Shafarevich in order to answer (in a negative way) to the ordinary Kurosh problem (a finitely generated nil ring is not necessarily nilpotent) gave also a counterexample to the ordinary Burnside problem (a finitely generated periodic group is not necessarily finite).

In this paper we want to explain two concrete applications of the non-associative algebras theory. The first one lies in the line of the restricted Burnside problem. So a group problem is translated into non-associative algebras terms, solved in this context and then translated back into group terms.

The second one is, by now, an attempt of application of non-associative algebras to Coding theory and Cryptography. The existence of a big number of "nonassociative examples" opens the door to the construction of new error correcting codes with "good properties" by using non-associative algebras instead of classical finite fields or to the generation of linear recursive sequences.

2. Grigorchuck groups in zero characteristic

As we have already mentioned, the example given by Golod and Shafarevich of a finitely generated nil ring in characteristic p (for any prime p) that is not nilpotent (counterexample to the Kurosh problem) allowed, thanks to the mentioned "bridge result" by Jacobson, the obtention of an example of a finitely generated group that is periodic (that is, all elements have finite order), but is not finite. In this way, the first counterexample to the Burnside problem was exhibited. Later Grigorchuck and Gupta and Sidki found new counterexamples. In both cases the corresponding groups are obtained as automorphisms groups acting on trees.

Grigorchuck groups have many interesting properties. They are infinite, finitely generated p-groups (all elements have order a power of p) for an arbitrary prime number p. They have intermediate growth, that is, striclty bigger than polynomial growth and strictly smaller than exponential one. So they give a negative answer to a conjecture by Milnor about the nonexistence of such groups.

Rozhkov and Bartholdi-Grigorchuck proved that all factors in the lower central series have order p or p^2. So these groups have finite width. What do we understand by finite width?

Definition 1 *Given a group G and its lower central series*

$$G = G_1 \geq G_2 \geq G_3 \geq \cdots, \;\; G_i = (G, G_{i-1}), \; i \geq 2$$

where the bracket is used to denote the commutator, then

(a) A residually p-group G is called of finite width if all factors G_i/G_{i+1} are finite groups and the orders $|G_i/G_{i+1}|$ are uniformly bounded from above.

(b) If G is a residually-(nilpotent torsion free) group, G has finite width if the numbers $b_i = \dim_Q(G_i/G_{i+1} \otimes_Z Q)$ are uniformly bounded.

Let's consider the associated graded Lie algebra: $L = \oplus_{i\geq 1} L_i$, with $L_i = G_i/G_{i+1} \otimes_Z K$ and bracket $[a_i G_{i+1}, b_j G_{j+1}] = (a_i, b_j) G_{i+j+1}$, where K denotes Z/pZ in case (a) and Q in case (b) and $(a_i, b_j) = a_i^{-1} b_j^{-1} a_i b_j$ is the commutator of the elements a_i, b_j.

If G has finite width, the dimensions of the homogeneous components L_i are uniformly bounded. In particular, $GK - \dim(L) \leq 1$.

The structure of finitely generated associative or Jordan algebras of Gelfand-Kirillov dimension one is known. The situation for Lie algebras is not the same. Not only the structure of such algebras is not known, but there are no hopes of getting similar results to those proved in the associative and Jordan cases. Indeed, if L is the Lie algebra associated to a Grigorchuck group, according to the previous process, then L is finitely generated, every element a of L is ad-nilpotent, that is, the adjoint operator $ad(a) : L \to L, \; x \to [x, a]$, is nilpotent, but L is not nilpotent. This situation, as we have said, can not appear in the associative and Jordan cases. It can be proved that it is also impossible in Lie algebras of zero characteristic.

Theorem 2 ([12]) *If $L = \oplus_{\alpha\in\Gamma} L_\alpha$ is a Lie algebra over a field K, $\operatorname{ch} K = 0$, Γ-graded, where Γ is an abelian group and satisfying:*

i) There is $d > 0$ such that $\dim_K L_\alpha \leq d$ for every $\alpha \in \Gamma$,

ii) Every homogenous element $a \in L_\alpha$ is ad-nilpotent.

Then the Lie algebra L is locally nilpotent.

Let's consider V a K-vector space that is a G-module. We say that the action of G is unipotent if for any $g \in G$ there is a natural number $n = n(g)$ such that $V(1-g)^n = (0)$.

A G–module V is called residually finite if there is a family of G–submodules $\mathcal{P}$ such that every $V' \in \mathcal{P}$ has finite codimension in V and $\cap_{V' \in \mathcal{P}} V' = (0)$.

Theorem 3 *([12]) Let G be a group and let's assume that all numbers $\dim_Q(G_i/G_{i+1} \otimes_Z Q)$, $i \geq 1$ are uniformly bounded. Then every finitely generated, residually finite and unipotent G-module is finite dimensional.*

The proof of Theorem 2 involves Jordan-algebras and non-associative algebras technics. Here we will just indicate the general lines of the proof of Theorem 3 and the way in which Theorem 2 is used.

Firstly the filtration given by the lower central series is substituted by a new filtration of the group

$$G = G'_1 \geq G'_2 \geq G'_3 \geq \cdots$$

with $(G'_i, G'_j) \subseteq G'_{i+j}$ and all factors G'_i/G'_{i+1} being torsion free. Using this filtration, we can construct the graded Lie ring $L = \oplus_{i \geq 1} G'_i/G'_{i+1}$ that has no additive torsion.

If $g \in G'_i - G'_{i+1}$ satisfies $V(1-g)^m = (0)$, then it is proved that $Lad(gG'_{i+1})^{2m-1} = (0)$.

It is also proved that $\dim_Q(G_i/G_{i+1} \otimes_Z Q) \leq d$ for every i. If $\rho : G \to GL(V)$ denotes the representation of G as automorphism group of V, then $\rho(G)$ is nilpotent. This is the point in which Theorem 2 is used. Indeed, the nilpotency of G follows from the nilpotency of the associated Lie algebra, what was proved in Theorem 2.

Now the finite dimension of V easily follows from the nilpotency of $\rho(G)$.

We can say, in a casual way, that there are no Grigorchuck groups in zero characteristic, understanding this according to the previous explanations.

3. Non-associative Galois rings

Associative Galois rings theory starts in a paper by Krull ([8]), being later developed by Janush [7] and Raghavendran [14]. Recently, Kuzmin and Nechaev have studied applications of these rings to Error correcting Codes (via the representation of non-linear codes over finite fields as linear codes over Galois rings [13]) and to Cryptography (via the generation of pseudo-random sequences based on linear recursive sequences over Galois rings [9]).

Hopefully, the development of a theory of non-associative Galois rings will open new applications in the mentioned areas. Let's remember that a finite associative ring S with unit element e is called Galois ring (GR) if the set $\Delta(S)$ of its one-side zero divisors (including the zero element) is equal to pS for some natural number p.

It can be proved that S is commutative, p is prime and $\operatorname{ch} S = p^n$ for some n. Furthermore, pS is the nilradical of S and $\bar{S} = S/pS$ is a finite field ($\bar{S} = GF(q)$ with $q = p^r$). Hence $|S| = p^{nr}$.

The theory of Galois rings reproduces, to a certain extent, the theory of finite fields. So, for every prime p and natural numbers n, r there is a unique, up to isomorphism) Galois ring S with $|S| = (p^r)^n$ and $\operatorname{ch} S = p^n$. Such ring is denoted $GR(q^n, p^n)$, where $q = p^r$.

Finite fields and integer residual rings are the first examples of Galois rings: $GF(q) = GR(q^1, p^1)$, $Z_{p^n} = GR(p^n, p^n)$ $(q = p)$.

Continuing with the similarities between finite fields and Galois rings, it is known that the automorphism group of the Galois ring $GR(q^n, p^n) = S$ is a cyclic group of order r $(q = p^r)$ and for every t divisor of r there is a unique subring R of S with $R \simeq GR((p^t)^n, p^n)$. Similarly, for every d there is an extension T of S with $T \simeq GR((q^d)^n, p^n)$.

We will define a generalized Galois ring (GGR) just by dropping the assumption of associativity. Now $S/\Delta(S)$ will be a semifield instead of a field.

Definition 4 *A ring D is a semifield if $D - \{0\}$ is closed with respect to the multiplication, there is a unit element e ($xe = ex = x$ $\forall x \in D$) and for every pair of elements $a, b \in D$, $a \neq 0$, there is a unique solution to the equations $ax = b$ and $xa = b$.*

If D is a finite semifield, then its characteristic is a prime number p and its associative center $Z(D)$ is a finite field ($GF(p^c)$ for some c). Furthermore, if D is not associative (that is, D is not a field) then $|D| = p^{cd}$, with $d \geq 3$.

So there are no proper semifields (i.e. not fields) of order p^2.

Constructions of semifields from finite fields were made by Dickson and Albert. A classification of finite semifields is not known. To illustrate difficulties, we want just mention that $GF(8)$ is the only semifield of order 8, the number of semifields of order 16 (up to isomorphism) is 24, while there are 2502 non-isomorphic semifields of order 32.

Definition 5 *A finite ring S with identity element e is called "generalized Galois ring" (GGR) if $\Delta(S) = \lambda S$ for some natural number λ.*

Remember that $\Delta(S)$ consists of zero and all one side zero divisors.

So, every finite semifield D is a GGR. If $\operatorname{ch} D = p$, then $\Delta(D) = pD = (0)$. The fact that $\Delta(S)$ is a two-side ideal implies that all nonzero elements in $\Delta(S)$ are two-side zero divisors and $S/\Delta(S)$ is a semifield.

It can also be proved that $\lambda = p$ is a prime, $\operatorname{ch}(S/pS) = p$ and $\operatorname{ch} S = p^n$ for some n.

The following useful characterization of GGR can be given:

Theorem 6 *A finite ring S with identity element e is a GGR if and only if there is a prime p and a natural number n such that* $\operatorname{ch} S = p^n$ *and S/pS is a semifield.*

Some properties of GR related to the ideal structure can be recovered. In fact we have the following

Theorem 7 *Let $(S, +, \star)$ be a GGR with identity e, characteristic p^n and let S/pS be a finite semifield with $q = p^r$ elements. Then*

1. *$S - pS$ is $\star$-closed,*
2. *The ideal lattice of S is given by the chain*

$$S = \Delta^0 \geq \Delta^1 \geq \Delta^2 \geq \cdots \geq \Delta^{n-1} \geq \Delta^n = 0$$

   where Δ^t denotes the additive subgroup of $(S, +)$ generated by all powers of $s \geq t$ elements of $\Delta(S)$.
3. *$|S| = q^n$ and $|\Delta^t| = q^{n-t}$. Furthermore $|S - pS| = q^n - q^{n-1}$.*

If S is a GGR and $Z(S/\Delta(S)) = GF(p^c)$ and $d = \dim_{Z(S/\Delta)} S/\Delta$, then $|S| = q^n$ with $q = p^r$ and $r = cd$.

So we can associate to every GGR four parameters (p, c, d, n). Let's notice that S is a semifield if $n = 1$ and the generalized Galois ring is indeed a Galois ring if $r \leq 2$.

It seems natural to pose the following two questions:

1. Given a semifield D in characteristic p and a natural number n, is there a GGR S with $\operatorname{ch} S = p^n$ and $S/pS \simeq D$?
2. If S and S' are GGR with the same characteristic p^n and $S/pS \simeq S'/pS'$, does it follow that $S \simeq S'$?

In order to answer these questions we will consider a construction of generalized Galois rings with some "extra properties".

Let's notice that if S is a GGR and R is a subring of S, then R is not necessarily a GGR. If we consider the particular case in which S/pS is a field, then a subring R of S is a GGR if and only if $R \cap pS = pR$.

Definition 8 *Let S be a GGR with* $\operatorname{ch} S = p^n$ *and $D = S/pS$ the semifield. Then S is said to be a* **lifting** *of the semifield D by the Galois ring Z if $Z = Z(S)$ and $Z(D) \simeq Z/pZ$.*

Notice that a GGR S is a lifting of the semifield $D = S/pS$ if and only if the associative center of S, Z, is a GR and the associated field Z/pZ coincides with the center of the semifield D.

It can be proved that we can always construct a lifting of an arbitrary semifield D by and arbitrary Galois ring Z.

Theorem 9 *For every semifield D of characteristic p and for every natural number n, there is a lifting S of the semifield D by a GR of characteristic p^n.*

So the answer to the first question is affirmative, however the second one is given a negative answer. Indeed, there are examples of two non-isomorphic liftings of the same Dickson semifield with a fixed characteristic.

Remark. We will call "top-associative" to those generalized Galois rings in which S/pS is a field (not just a semifield). We can study if this class of GGR is interesting and has better properties that the general case. It has been proved that such rings become associative (that is, Galois rings) as soon as power-associativity is imposed on them. In a concret way, we have proved that if S is a power-associative GGR that is top-associative", $\operatorname{ch} S = p^n$, $p \neq 2$ and $Z(S/pS)$ has at least 6 elements, then S is a GR.

So it seems that, in order to get really new rings, the case in which the semifield S/pS is not a field is the one to be considered.

There are still many open problems in this area. The uniqueness of a GR with fixed parameters is not any longer true for GGR. But probably this is an advantage for applications, since we have a wide range of examples of GGR, even with the same set of parameters. But from a purely algebraic point of view, it seems natural to think of some additional assumptions so that a uniqueness result can be recovered. Now the question is: Which are the natural additional assumptions?

The exploration of the way in which non-associative rings can be applied to codes is an open and appealing challenge.

References

[1] Bartholdi, L. and Grigorchuck, R. I.: Lie methods in growth of groups of finite width. In *Computational and geometric aspects of modern algebra (Edinburgh, 1998)*, 1–27. London Math. Soc. Lecture Notes Ser. **275**. Cambridge Univ. Press, 2000.

[2] Elduque, A. and Myung, H. C.: *Mutations of Alternative Algebras*. Mathematics and its Applications **278**. Kluwer, Dordrecht, 1994.

[3] Elduque, A. and Myung, H. C.: The reductive pair (B_4, B_3) and affine connections on S^{15}. *J. Algebra* **227** (2000), no. 2, 504–531.

[4] González, S., Markov, V. T., Martínez, C., Nechaev, A. A. and Rúa, I. F.: *Nonassociative Galois rings. Discrete Math. Appl.* **12** (2002), 591–606.

[5] Grigorchuk, R. I.: On the Burnside problem for periodic groups. *Funct. Anal. Appl.* **14** (1980), 53–54.

[6] Hopkins, N. C.: Quadratic differential equations in graded algebras. In *Nonassociative Algebra and its Applications* (S. González ed.), 179–182. Math. Appl. **303**, Kluwer Acad. Publ., 1994.

[7] Janusz, G.J.: Separable algebras over commutative rings. *Trans. Amer. Math. Soc.* **122** (1966), 461–478.

[8] Krull, W.: Algebraische Theory der Ringe II. *Math. Ann.* **91** (1924), 1–46.

[9] Kuzmin, A. S. and Nechaev, A. S.: Linear recurring sequences over Galois Rings. *Algebra and Logic* **34** (1995), no. 2, 87–100.

[10] Markus, L.: Quadratic differential equations and nonassociative algebras. *Annals of Math. Stud.* **45** (1960), 185–213.

[11] Martínez, C. and Zelmanov, E.: Jordan algebras of Gelfand-Kirillov dimension 1. *J. Algebra* **180** (1996), no. 1, 211–238.

[12] Martínez, C. and Zelmanov, E.: Nil Algebras and Unipotent Groups of Finite Width. *Adv. Math.* **147** (1999), 328–344.

[13] Nechaev, A. A.: Kerdock's code in cyclic form. *Discrete Math. Appl.* **1** (1989), no. 4, 365–384.

[14] Raghavendran, R.: Finite associative rings. *Compositio Math.* **21** (1969), no. 2, 195–219.

[15] Reed, M. L.: Algebraic structures of genetic inheritance. *Bull. Amer. Math. Soc.* **34** (1997), 107–130.

[16] Small, L. W., Stafford, J. T. and Warfield Jr., R. B.: Affine algebras of Gelfand-Kirillov dimension 1 are PI. *Math. Proc. Cambridge Philos. Soc.* **97** (1985), 407–414.

[17] Zhevlakov, K. A., Slinko, A. M., Shestakov, I. P. and Shirshov, A. I.: *Rings that are nearly associative*. Academic Press, New York, 1982.

Recibido: 20 de febrero de 2002

Santos González
Department of Mathematics
University of Oviedo
C/ Calvo Sotelo s/n. 33007–Oviedo, Spain
santos@pinon.ccu.uniovi.es

Consuelo Martínez
Department of Mathematics
University of Oviedo
C/ Calvo Sotelo s/n. 33007–Oviedo, Spain
chelo@pinon.ccu.uniovi.es

Partially supported by PB97-1291-C03-01, FEDER IFD 97-0556.