Journal of Algebra and Its Applications
(2023) 2350145 (13 pages)

DOI: 10.1142/S0219498823501451

Free symmetric pairs in the field of fractions of enveloping Lie algebras with involution

Jairo Z. Gonçalves
Department of Mathematics, University of São Paulo
São Paulo 05508-090, Brazil
jz.goncalves@usp.br

Received 8 May 2021
Revised 18 July 2021
Accepted 18 July 2021
Published 15 April 2022

Communicated by V. Futorny

Let D be a division ring with center k, $\operatorname{char} k = p \neq 2$, let * be an involution of D, and let $D^\dagger$ be the multiplicative group of D. A pair (u, v) is called *free symmetric*, if it is formed by symmetric elements, and it generates a free non-cyclic subgroup of $D^\dagger$. If $U(L)$ is the enveloping algebra of the non-abelian nilpotent Lie k-algebra L over the field k of characteristic $\neq 2$, and * is a k-involution of L extended to the field of fractions D of $U(L)$, we show that $D^\dagger$ contains free symmetric pairs. We also discuss the consequences of symmetric elements of a normal subgroup being torsion over the center.

Keywords: Division rings; involutions; free groups; free symmetric pairs; normal subgroups.

Mathematics Subject Classification 2020: Primary: 16K40; Secondary: 20E05, 12E15

1. Introduction

Let D be a division ring with center k, $\operatorname{char} k = p \neq 2$, and let * and involution of D. A longstanding conjecture due to Lichtman is as follows.

Conjecture 1.1 ([15]). *If D is a division ring with center k and multiplicative group $D^\dagger$, then $D^\dagger$ contains a free non-cyclic subgroup.*

This question led us to consider an analogue one, now for division rings with an involution. Since involutions do not behave well in characteristic 2, it appears reasonable to exclude this case. We state the following.

Conjecture 1.2. *Let D be a division ring with center k, $\operatorname{char} k \neq 2$, and let * be an involution of D. Then $D^\dagger$ contains free symmetric and unitary pairs.*

We proved this claim when $[D:k] < \infty$ and D is not a quaternion algebra (this special case is well known), see [12], and for some families of division rings: [5, 6, 9, 10].

In this work, we investigate the existence of free symmetric pairs in the field of fractions of the universal enveloping algebra of a nilpotent Lie algebra.

In [20, Theorem 1.2], Sanchez shows that if $U(L)$ is the enveloping algebra of the non-abelian nilpotent Lie k-algebra L over the field k of characteristic 0, and * is a k-involution of L extended to the field of fractions D of $U(L)$, then there exist a pair of symmetric elements $x, y \in D$ such that $k\langle x, y\rangle$ is isomorphic to the k-free group algebra of the free group of rank two.

If $\operatorname{char} k = p > 2$ the field of fractions D is finite dimensional over its center, and so it cannot contain free group algebras. Nevertheless, we show that D still contains free symmetric pairs.

We offer the following.

Theorem 1.1. *Let $U(L)$ be the enveloping algebra of the non-abelian nilpotent Lie k-algebra L over the field k of characteristic $\neq 2$, and let * be a k-involution of L extended to the field of fractions D of $U(L)$. Then $D^\dagger$ contains free symmetric pairs.*

It is also possible to obtain a weaker version of [2] in the form.

Theorem 1.2. *Let D be the field of fractions of the group ring kG, of the non-abelian torsion free nilpotent group G over the uncountable field k of characteristic* 0, *and let * be a k-involution of G extended linearly to kG, and to D. Then $D^\dagger$ contains free symmetric pairs.*

In [2], we proved that in $\mathbb{A}_1(\mathbb{Q}) = \mathbb{Q}\langle s, t \mid st - ts = 1\rangle$, with the involution $s^* = t$, $t^* = s$, $D_1^\dagger$ contains free symmetric pairs. Here we add to this result.

Theorem 1.3. *Let be $\mathbb{A}_1(\mathbb{Q})$ with one of the following involutions*:

(1) $s^* = s$, $t^* = -t$,
(2) $s^* = s$, $t^* = s - t$,

and let D_1 be its field of fractions. Then $D_1^\dagger$ contains free symmetric pairs.

The technique we develop here is the outcome of the investigation of the following question: what happens when $H \lhd D^\dagger$ has a non-central symmetric element whose square falls in the center?

As a consequence, we conclude that the presence of certain algebraic elements in N implies that it contains free symmetric pairs [11]. On the other hand if $N = D^\dagger$ and the set $S = \{s \in D \mid s^* = s\}$ is power central, Chacron [1] shows that D is commutative.

Since S being power central precludes it to contain free symmetric pairs, we can ask what would happen if we assume that the subset S, with $\emptyset \neq S = \{h \in H \mid h^* = h\} \subseteq H \lhd D^\dagger$, and H proper, is torsion over the center?

We will show that if there is a bound for these orders, then there are free symmetric and unitary pairs outside the normal subgroup H.

Let us recall that an element $u \in D^\dagger$ is unitary if $u^* = u^{-1}$, and a pair (u, v) is free unitary if its elements are unitary, and generates freely a free subgroup.

More precisely, we obtain the following.

Theorem 1.4. *Assume that* $\emptyset \neq S = \{h \in H \mid h^* = h\} \subseteq H \lhd D^\dagger$, *that D is not a quaternion algebra, k is infinite and that* $\operatorname{char} p \neq 2$. *If there exists an integer $N > 1$ such that S^N is central, then $D^\dagger$ contains free symmetric and unitary pairs.*

Corollary 1.1. *If* $4 < [D : k] < \infty$, $\emptyset \neq S = \{h \in H \mid h^* = h\} \subseteq H \lhd D^\dagger$, *and if for every $s \in S$ there exists a positive integer $n(s) > 1$, such that $s^{n(s)} \in k$, then D contains free symmetric and unitary pairs.*

Finally, in the last section, we consider two pathological cases. They occur when $p = 2$ and $[D : k] = 4$, that is, our division algebra is the quaternion algebra.

In the first situation the set of symmetric elements modulo the center is 2-elementary abelian, and in the second, the multiplicative group $D^\dagger$ contains a free symmetric pair.

Let us recall that an involution * of D is of the *first kind* if k is fixed elementwise by *. Otherwise, we say that * is of the *second kind.*

2. Auxiliary Results

Theorem 2.1. *Let K be a non-absolute field and let $L = K(\alpha)$ be a finite separable extension of degree n. Then there are infinitely many pairs (ν_i, ω_i), $i \in \mathbb{N}$, where the ν_i's are discrete non-equivalent archimedean valuations of K, each one with n distinct prolongations to L, $\omega_i \in K$, and $\nu_i(\omega_i - \alpha) > 0 \ \forall\, i \in \mathbb{N}$.*

Proof. See [19]. □

Let $B = \{e_1, \ldots, e_n\}$ be a basis for an algebra $\mathfrak{A}$ over a field F. Then every $a \in \mathfrak{A}$ can be written uniquely as $\sum_{i=1}^{n} \alpha_i e_i$, with $\alpha_i \in F$, and we call the α_i the *B-coefficients* of a. If all such B-coefficients are nonzero, then we say that a has *full support* with respect to B.

We note that the elements α or β below, but of course not both, are allowed to be 1.

Lemma 2.1. *Let $\mathfrak{A} = k(X)$ be the rational function field in the indeterminate X over the field k of characteristic $\neq 2$. Let $n \geq 1$ be a fixed integer and set $y = X^n$ and $F = k(y) = k(X^n)$. Then $\mathfrak{A}$ is a finite-dimensional algebra over F with basis $B = \{1, X, \ldots, X^{n-1}\}$. Now let α and β be distinct non-negative powers of y, with $\alpha \neq \beta^{n+1} y$ and $\beta \neq \alpha^{n+1} y$, and set $w = (1 - \alpha X)(1 - \beta X)^{-1} \in \mathfrak{A}$.*

(1) *The elements w, w^2, w^{-1} and w^{-2} all have full support with respect to B.*

(2) *Let* $\alpha = y^a$, $\beta = y^b$ *and* $c = \max\{a, b\}$. *Then all the* B*-coefficients of* w *and* w^{-1} *in* $k(y)$ *have numerator and denominator degrees at most* $cn+1$. *Furthermore, the* B*-coefficients of* w^2 *and* w^{-2} *in* $k(y)$ *have numerator and denominator degrees at most* $2(cn+1)$.

(3) *If* * *is the* k*-involution defined on* $\mathfrak{A}$ *by* $X^* = X^{-1}$, *then* * *inverts* y, α *and* β. *It follows that* $w^* = (\beta\alpha^{-1})w$, *so* w^*, $(w^*)^{-1}$, ww^* *and* $(ww^*)^{-1}$ *all have full support with respect to* B.

Proof. See [10, Lemma 4.1]. □

One of our main tools to produce free groups is the following.

Proposition 2.1. *Let* ν *be a non-archimedean valuation defined on a field* F, *let* $m \geq 2$ *be an integer, and let* $u, v \in F^{m\times m}$ *be invertible* $m \times m$ *matrices. Assume that*

(1) u *is a diagonal matrix, and its diagonal has a unique entry with maximal* ν*-value, and a unique entry with minimal* ν*-value.*

(2) *All the entries of* v *and* v^{-1} *have zero* ν*-values, and in particular are not* 0.

Then the pair $(u, v^{-1}uv)$ *generates a non-cyclic free subgroup.*

Proof. See [9, Lemma 6]. □

Recall that an element $u \in D^\dagger$ is unitary if $u^* = u^{-1}$. To construct unitary units satisfying the max–min condition, we need the following.

Lemma 2.2. *Let* ν *a non-archimedean valuation on a field* F *such that* $\nu(2) = 0$.

(1) *If* $\alpha \in F$, *then* $\nu(\frac{1-\alpha}{1+\alpha}) > 0$ *if and only if* $\nu(1-\alpha) > 0$.

(2) *Let* $\alpha, \beta \in F$ *be such that* $\alpha + \beta \neq 0$. *Then* $\nu(\frac{1-\alpha}{1+\alpha}) > 0$ *if and only if* $\overline{\alpha} = \overline{\beta}$ *in the residue field* $\overline{F}$.

Proof. See [12, Lemma 2.9]. □

Before we proceed, we need an important observation. *If* $[D : k] = n < \infty$, *and* * *is of the first kind, then* n *is a power of* 2.

This comes from the fact that the order of D in the *Brauer Group* of D is two, and so the index of D is a power or 2.

The next lemma is the involutorial version of [7, Proposition 3.6].

Lemma 2.3. *Assume that* $\operatorname{char} k = p > 2$, $[D : k] > 4$ *and that* a *is a symmetric non-central element of* D, *purely inseparable over* k. *Then* D *contains free symmetric and unitary pairs.*

Proof. Let us define the derivation $d_a(w) = wa - aw$. Since $d_a^{(p)}(w) \equiv 0$, there exists some integer $i > 1$ such that $x = d_a^{(i-1)}(w) = d_a(y) = ya - ay \neq 0$ but $xa - ax = 0$.

Since x commutes with a we can write $x = ta$, where t also commutes with a.

Therefore, since $x = ya - ay$, it follows that $ta = x = ya - ay$, which can be rewritten as

$$a = (t^{-1}y)a - a(t^{-1}y) = ua - au, \tag{1}$$

where $u = t^{-1}y$.

Applying * to (1) we obtain

$$a = au^* - u^*a. \tag{2}$$

Adding (2) to (1) we arrive at

$$a = \frac{(u - u^*)}{2}a - a\frac{(u - u^*)}{2}. \tag{3}$$

Setting $s = (u - u^*)/2$ we can write (3) as

$$a = sa - as \tag{4}$$

or

$$a^{-1}sa = 1 + s. \tag{5}$$

Set $\alpha = s(s+1)\cdots(s+p-1)$, and let $F = GF(p)(\alpha)$ be the field adjoining α to $GF(p)$.

The minimal polynomial of s over F is $f(T) = T^p - T - \alpha$.

Let now D_0 be the division ring generated by a and s over $F(a^p)$.

It is easy to check that D_0 has center $Z = F(a^p)$, is invariant under * and $[D_0 : Z] = p^2$.

We claim that $Z(s) = Z(s^2)$.

Indeed, since $[Z(s) : Z] = p$ is and odd prime, either $[Z(s^2) : Z] = p$, or $Z(s^2) = Z$.

This last possibility implies that $s^2 \in Z$, and from the fact that p is an odd prime, it follows that

$$s(s^2)^{(p-1)/2} - s - \alpha = 0$$

or

$$s\beta - s - \alpha = 0, \quad \text{with } \beta = (s^2)^{(p-1)/2} \in Z.$$

This implies that $s(\beta - 1) = \alpha$, and since $\beta \neq 1$, it follows that $s \in Z$, a contradiction.

The conclusion is that $Z(s) = Z(s^2)$.

Let $Z_0 = \{x \in Z \,|\, x^* = x\}$. Since * is of the second kind on D_0 it follows that $[Z : Z_0] = 2$, and since $p \neq 2$ there exists $\theta \in Z$, with $\theta^* = -\theta$, and $\theta^2 = \beta \in Z_0$.

Let us consider D_0 as a left vector space over $Z(s^2)$ with basis $\mathfrak{B} = \{1, a, \ldots, a^{p-1}\}$, and let $A = [s^2]_{\mathfrak{B}}$ be the matrix obtained from s^2 in the right regular representation, with respect to the basis $\mathfrak{B}$.

Going to a finite algebraic extension $\overline{Z}$ of Z, where the minimal polynomial of A has all its roots $\lambda_1, \ldots, \lambda_{p-1}$, we can write

$$A = \mathrm{diag}(\lambda_1, \ldots, \lambda_{p-1}).$$

Since $Z(s^2)$ is a finite, separable extension of Z_0 of degree $2p$, by Theorem 2.1 there exist elements $\epsilon, \delta \in Z_0$ and a non-archimedean valuation ν on $Z(s^2)$, such that

(1) $\nu(\epsilon - \lambda_1) > 0$, $\nu(\epsilon - \lambda_i) = 0, i = 2, \ldots, p$.
(2) $\nu(\delta - \lambda_1) = 0$, $\nu(\delta - \lambda_2) > 0$, $\nu(\delta - \lambda_i) = 0, \forall\, i = 3, \ldots, p$.
(3) For every finite subset $W \subseteq Z$ with $0 \notin W$, $\nu(w) = 0, \forall\, w \in W$.

Set $\tau = a^p$ and let ζ and ρ be distinct non-negative powers of τ with $\zeta \neq \rho^{p+1}\tau$ and $\rho \neq \zeta^{p+1}\tau$.

Also set $v = (1 - \rho a)(1 - \zeta a)^{-1}$.

By Lemma 2.1 the elements v^2 and v^{-2} have full support with respect to $\mathfrak{B}$. We choose the set W of condition (3) above as being the union of the supports of v^2 and v^{-2}. This can always be done, since we have infinitely many ν's at our disposal.

Observe also that $u = (\epsilon - s^2)/(\delta - s^2)^{-1}$ is symmetric. So, by Proposition 2.1, (u, u^{v^2}) generates a free non-cyclic subgroup. Thus, we conclude that $(u^{v^{-1}}, u^v)$ is a free pair in which the generators are exchanged by *. This proves the first part of the lemma (See [9, Proposition 19]).

To obtain the free unitary pair, we act in the following way.

Define $b = \theta a$, $\theta^* = -\theta$, with $\theta^2 = \beta \in Z_0$. Then $b^* = -\theta a = -b$, with $b^p = \theta\beta^{(p-1)/2} a^p = \gamma$.

We consider the matrix $[s]_{\mathfrak{B}} = \mathrm{diag}(s, s+1, \ldots, s+p-1)$, with coefficients in $F(s)$. Let $\epsilon, \delta \in Z_0$, and let ν be a non-archimedean valuation of $Z(s)$, such that

(1) $\nu(\epsilon - s) > 0$, $\nu(\epsilon - (s+i)) = 0$, for $i = 2, \ldots, p-1$.
(2) $\nu(\delta - s) = 0$, $\nu(\delta - (s+1)) > 0$, $\nu(\epsilon - (s+i)) = 0$, for $i = 2, \ldots, p-1$.
(3) $\nu(a^p) = \nu(\beta) = \nu(\theta) = \nu(1-\gamma) = \nu(1+\gamma) = 0$.

Set $u = (\frac{\epsilon - s}{\epsilon + s})(\frac{\delta - s}{\delta + s})^{-1}$. Then $u^* = u^{-1}$ and

$$[u]_{\mathfrak{B}} = \mathrm{diag}\left(\left(\frac{\epsilon - (s+i)}{\epsilon + (s+i)}\right)\left(\frac{\delta - (s+i)}{\delta + (s+i)}\right)^{-1}\right), \quad i = 0, \ldots, p-1.$$

Then $[u]_{\mathfrak{B}}$ is ν max–min by Lemma 2.2.

Moreover $1 - b^p = 1 - \gamma = (1-b)^p = (1-b)(1 + b + \cdots + b^{p-1})$, and so

$$v = \frac{1+b}{1-b} = \frac{(1+\gamma) + 2\theta a + 2\beta a^2 + \cdots + 2\beta^{(p-1)/2} a^{p-1}}{1-\gamma}.$$

It is easy to check that $v^* = \frac{1-b}{1+b} = v^{-1}$ has an expression analogous to v, with some minus signs conveniently inserted.

From our reasoning, it follows that v is unitary, with both v and v^{-1} with full support, all these elements with ν valuation zero. By Proposition 2.1 (u, u^v) is a free unitary pair. □

The following unitary version of Brauer–Cartan–Hua Theorem, due to Herstein, will be useful.

Theorem 2.2. *Let D be a division ring with center k of characteristic $\neq 2$ and an involution *. Let A be a subdivision ring of D such that $uAu^{-1} \subseteq A$ for every unitary element u in D. Then*

(1) *If A is commutative and $[D : k] > 4$, then $A \subseteq k$.*
(2) *If A is not commutative and $[D : k] > 16$, then $A = D$.*

Proof. See [13]. □

Proposition 2.2. *Let G be a finitely generated linear group with center Z, and let $\bar{\ }: G \to G/Z$ be the canonical epimorphism. Then the set $\{m \in \mathbb{N} \mid \overline{g} \in \overline{G}, \overline{g}^m = \overline{1}\}$ is bounded by a positive integer N.*

Proof. Let K be a field, let $n > 1$ be an integer, and let $G \leq GL_n(K)$. Let A be the K linear span of G, namely $A = K[G]$. Then A is a finite-dimensional K-vector space and G/Z acts on it faithfully. So G/Z is also a linear group and by [18] 51.2.5 the claim follows. □

Proposition 2.3. *Let R be an Ore domain with a discrete valuation ν, and let $R\langle t\rangle$ be the group ring of the infinite cyclic group $\langle t\rangle$ over R. Then*

(1) *The valuation ν can be extended to $R\langle t\rangle$ such that $\nu(t) = 1$.*
(2) *Let $T = \{x \in R\langle t\rangle \mid \nu(x) \geq 0\}$ and $T_0 = \{x \in R\langle t\rangle \mid \nu(x) > 0\}$. Then the quotient ring T/T_0 is isomorphic to the graded ring $gr(R)$ associated to the filtration defined by ν. Further, the extended valuation becomes a t-adic valuation on T defined by the powers of the ideal $T_0 = tT$.*
(3) *The graded ring $gr(R)$ is an Ore domain, and if D and Δ are, respectively, the division ring of fractions of T and $gr(R)$, then there exists a local subring $S \subseteq D$, such that $S/J(S) \cong \Delta$.*

Proof. See [17, Propositions 16 and 18]. □

Lemma 2.4. *Let D be a division ring with an uncountable center k, let n be a positive integer and let $R = M_n(D)$. Let t be a commutative indeterminate and suppose that $R(t)$ contains a free pair $(u(t), v(t))$. Then R contains a free pair of the form $(u(\lambda)), v(\lambda))$, for some $\lambda \in k$.*

Moreover, if R has an involution * extended to $R(t)$ by the formula $t^* = t$, and $(u(t), v(t))$ is a free symmetric pair under the induced involution, then we can find infinitely many $\lambda \in k$ such that the free pair $(u(\lambda)), v(\lambda))$ is symmetric.

Proof. See [2, Lemma 5.3]. □

3. Nilpotent Lie Algebras with Involutions

We start this section borrowing some definitions and results from Sanchez [20].

Let k be a field and let L be Lie k-algebra. A k-linear map $^* : L \to L$ is a k-*involution* if for all $x, y \in L$ we have $[x, y]^* = [y^*, x^*]$ and $x^{**} = x$. The natural involution in L, which is called the *principal involution*, is defined as $x^* = -x$ for all $x \in L$.

The *Heisenberg Lie k-algebra* is the Lie k-algebra with presentation

$$H = \langle x, y, z \mid [y, x] = z \neq 0, [y, z] = [x, z] = 0\rangle.$$

We need.

Lemma 3.1 ([20]). *Let k be a field of characteristic $\neq 2$ and let H be the Heisenberg Lie k-algebra. Then any k-involution of H is equivalent to $^*\colon H \to H$, where*

(1) $x^* = x, y^* = -y, z^* = z$, *or*
(2) $x^* = x, y^* = y, z^* = -z$, *or*
(2) $x^* = -x, y^* = -y, z^* = -z$.

Let $U(H)$ be the universal enveloping algebra of the Heisenberg algebra, let D be its Ore field of fractions, and let * be any of the involutions of H extended to D. We can state the following.

Proposition 3.1. *Let * be any of the involutions of Lemma* 3.1 *induced to D. Then, we have the following possibilities*:

(1) *If* $\operatorname{char} k > 2$ *then $D^\dagger$ contains free symmetric and unitary pairs.*
(2) *If* $\operatorname{char} k = 0$ *then $D^\dagger$ contains free symmetric pairs.*

Proof. (1) Let $\operatorname{char} k = p > 2$. The generators of D satisfy the relations $yx = z + xy$, $yz = zy$ and $xz = zx$.

From these, we obtain, by induction on $n \in \mathbb{N}\backslash\{0\}$, that $y^n x = ny^{n-1}z + xy^n$, and $x^n y = yx^n - nx^{n-1}z$. Therefore, $x^p, y^p \in Z$, the center of D, and D is finite-dimensional over Z. In any case either x or x^2 is symmetric and totally inseparable over Z, and so by Lemma 2.3 $D^\dagger$ contains free symmetric and unitary pairs.

(2) Let $\operatorname{char} k = 0$ and let us denote by D the field of fractions of the skew polynomial ring $R = \mathbb{Z}_{(p)}[z, x][y; yx = z + xy]$, where $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at any odd prime p, and where the polynomials in y have coefficients in $\mathbb{Z}_{(p)}[z, x]$ on the left.

By [8, Proposition 19], we can construct a specialization $S \supseteq R$, with a maximal ideal M such that $M \cap R = pR$. It is clear that the quotient map preserves *, and since the center of S/M has characteristic p, it follows that both $\overline{x}$ and $\overline{y}$ are. Purely inseparable over the corresponding center. We are under the same conditions as in (1). Let $(\overline{u}, \overline{v})$ be a free pair in the quotient. Then (uu^*, vv^*) is a free symmetric pair in D (See [9, Proposition 19]). $\square$

Proof of Theorem 1.1. Let L be a non-abelian nilpotent Lie k-algebra over a field k of characteristic $\neq 2$, with a k involution.* By [20, Proposition 3.4], L contains a * invariant Heisenberg Lie k-algebra H, such that the restriction of * to H is one of the involutions of Lemma 3.1. The conclusion follows by Proposition 3.1. $\square$

4. Nilpotent Group Algebras with Involution

Proposition 4.1. *Let G be a non-abelian torsion free nilpotent group with an involution *. Then G contains a Heisenberg subgroup $\Gamma = \langle x, y, \lambda \,|\, (y,x) = \lambda \neq 1, (x,\lambda) = (y,\lambda) = 1\rangle$, invariant by *, such that either*

(1) $x^* = x, y^* = y, \lambda^* = \lambda^{-1}$, *or*
(2) $x^* = x^{-1}, y^* = y^{-1}, \lambda^* = \lambda^{-1}$, *or*
(3) $x^* = x, y^* = y^{-1}, \lambda^* = \lambda$.

Proof. See [4, Proposition 2.4]. $\square$

Lemma 4.1. *Let * be one of the involutions above of Γ, let D be the field of fractions of $k\Gamma$, the group algebra of Γ over the uncountable field k of characteristic 0, and let us still denote by * the extension of the involution of Γ to D. Then $D^\dagger$ contains free symmetric pairs.*

Proof. Let L be the Lie k-algebra of Γ as defined in [14], and let $U(L)$ be its enveloping algebra. Let us recall that if Γ is a residually torsion free nilpotent group, and if $\gamma_i(\Gamma), i \geq 1$ is its descending central series, we can construct a *Lie Algebra* associated to Γ, where the product of Γ becomes the addition and the commutator becomes the *Lie bracket*.

The powers of the augmentation ideal define a valuation ν of $k\Gamma$, and the graded ring associated with this valuation is isomorphic to $U(L)$, by [16, Theorem 2.1].

Here we need to observe that if * is one of the involutions of Γ above, then this involution can be induced to the graded ring, since the augmentation ideal of $R = k\Gamma$ and all its powers are invariant by $*$. Moreover, since L is the nilpotent algebra with generators u and v and relations $[u,v] = z$, $[u,z] = [v,z] = 0$, when * is induced to L, then * is one of the involutions described in Lemma 3.1.

We now consider the Laurent polynomial ring $R[t, t^{-1}]$, with the extended involution $t^* = t$, and extended valuation ν with $\nu(t) = 1$.

Let T be the valuation ring of $R[t, t^{-1}]$ and $T_0 = tT$. By Proposition 2.3 T/T_0 is isomorphic to $gr(k\Gamma)$, and more precisely, the images of the elements $(x-1)/t$ and $(y-1)/t$ generate L and $U(L)$.

Let Δ_1 be the field of fractions of $U(L)$ and Δ be the field of fractions of T. By Theorem 1.1 Δ_1 contains a free symmetric pair $(u(t)_1, v_1(t))$, and by Proposition 2.3 Δ contains a local subring S such that $S/J(S) \cong \Delta_1$.

Let $(u(t), v(t))$ be a free symmetric pair in Δ. By Lemma 2.4 there exists $\mu \in k$ such that $(u(\mu), v(\mu))$ is a free symmetric pair in $D^\dagger$. □

Proof of Theorem 1.2. By Proposition 4.1 G contains a Heisenberg subgroup Γ, invariant by *, where the involution is one of those described by the proposition. By Lemma 4.1 the result follows. □

Proof of Theorem 1.3. We argue as in the proof of Proposition 3.1(2). We obtain as the quotient the division ring generated by s and t over $GF(p)$, the field with p elements, subject to the relation $st = 1 + ts$. Therefore s^p is purely inseparable over the center, and since $s^* = s$ the result follows lifting the free symmetric pair to $\mathbb{A}_1(\mathbb{Q})$. □

5. Symmetric Elements Torsion over the Center

Proof of Theorem 1.4 and Corollary 1.1. We start observing that we may assume that $H^* = H$.

Indeed, since H^* is also a normal, non-central subgroup of $D^\dagger$, and $H \cap H^* \supseteq S$ is normal, the claim follows.

Next, we can also assume that S is not abelian.

Otherwise, if $u \in D$ is unitary $uSu^{-1} \subseteq S$, and if we denote by $A = [S]$ the subdivision ring of D generated by the elements of S, A is commutative. But A is invariant by conjugation by unitary elements of D, and by Theorem 2.2 we have $A \subseteq k$, a contradiction.

So, we can assume that A is not abelian.

Also, if $\operatorname{char} k = p > 2$, we can assume that p does not divide N, otherwise by Lemma 2.3 D contains free symmetric and unitary pairs.

Let $a, u \in S$, with $(a, u) \neq 1$, $\alpha = u^r \in k$, and let $\lambda^* = \lambda, \lambda \in k$ be such that $\lambda^r \alpha \neq 1$. Then

$$(1 - \lambda u)^{-1} = \frac{1 + \lambda u + \cdots + \lambda^{r-1} u^{r-1}}{1 - \lambda^r \alpha}.$$

Set

$$t = a(1 - \lambda u)a^{-1}(1 - \lambda u)^{-1} \in H$$

and

$$t^* = (1 - \lambda u)^{-1} a^{-1} (1 - \lambda u) a \in H.$$

Then $tt^* = a(1-\lambda u)a^{-1}(1-\lambda u)^{-2}a^{-1}(1-\lambda u)a \in H$ is symmetric, and since

$$(1-\lambda u)^{-2} = \frac{1+2\lambda u + \cdots + \lambda^{2(r-1)}u^{2(r-1)}}{(1-\lambda^r\alpha)^2}$$

and $(tt^*)^N \in k$, it follows that $(tt^*)^N$ as a rational function of λ is

$$(1+N(-aua^{-1}+2u-a^{-1}ua)\lambda + \cdots + (\cdots)\lambda^{2rN})((1-\lambda^r\alpha)^2)^{-1},$$

and belongs to k, for all $\lambda^* = \lambda \in k$. Since k is infinite, by the principle of identity of polynomials and from the fact the p does not divide N, we conclude that

$$-aua^{-1} + 2u - a^{-1}ua = 0. \tag{6}$$

Or, equivalently

$$ua^2 - 2aua + a^2u = 0. \tag{7}$$

Define $d_a(x) = xa - ax, x \in D$.

From (7) it follows that $d_a^{(2)}(u) = 0$.

Call $y = d_a(u) \neq 0$ (since $(a,u) \neq 1$).

Then, setting $y = at$, it follows that t commutes with a, and therefore we can rewrite $y = ua - au$ as

$$a = (t^{-1}u)a - a(t^{-1}u). \tag{8}$$

Let us denote $s = t^{-1}u$. Then we can rewrite Eq. (8) as

$$a^{-1}sa = 1 + s. \tag{9}$$

Finally, since $a^N \in k$, it follows that

$$a^{-N}sa^N = N + s = s$$

and so $N = 0$, the final contradiction for the proof of Theorem 1.4.

The proof of Corollary 1.1 is almost immediate. First, observe that since D is finite-dimensional over k, by [3, Lemma 2.3], we can assume that the center k of D is finitely-generated over the prime field $GF(p)$. Hence we can see $D^\dagger$ as a finitely generated linear group over k, and by Proposition 2.2 the order of elements of $D^\dagger$ over k are bounded. The conclusion follows from Theorem 1.4. □

6. Remarks

Usually, involutions do not behave well in characteristic 2. So, we present below two extreme cases. One does not have free symmetric pairs, and the other does. Both lie in quaternion division algebras.

Let $F = GF(2)(a,b)$ be the field of fractions of the polynomial ring $GF(2)[a,b]$, in the independent commutative indeterminates a and b over the field of two elements $GF(2)$, and let $\mathfrak{A} = F\langle \mathbf{i}, \mathbf{j} \,|\, \mathbf{i}^2 + \mathbf{i} + a = 0, \mathbf{j}^2 = b, \mathbf{ji} = (\mathbf{i}+1)\mathbf{j}\}$ be the quaternion division ring over F.

In this quaternion algebra, we can define two involutions, in which the symmetric elements have a quite distinct behavior.

(1) Set $\mathbf{i}^* = \mathbf{i}+1, \mathbf{j}^* = \mathbf{j}$ and $\alpha^* = \alpha, \forall\, \alpha \in F$. By [11] we have $S^2 \subseteq F$, and so there are no free symmetric pairs in S.
(2) If $u = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$, define $u^* = u + \delta$. Then * is an F-involution of $\mathfrak{A}$, and $S = \{\alpha+\beta\mathbf{i}+\gamma\mathbf{j} \mid \alpha, \beta, \gamma \in F\}$. By [8, Theorem 3], we have $\langle 1+\mathbf{i}, 1+\mathbf{j}\rangle/center \cong \mathbb{Z} * \mathbb{Z}_2$, proving the existence of free symmetric pairs in S.

The reader may wonder how is it possible to produce free symmetric pairs in a division ring of characteristic 2. In this direction, we may offer a lame version of Lemma 2.3, this time with the lack of free unitary pairs.

Proposition 6.1. *Let D be a division ring with center k of characteristic* 2, *with an involution* *, *and let $a \in D$ be a symmetric element such that $a^2 \in k$. Then D contains a free symmetric pair.*

Proof. Let S be the set of symmetric elements of D. Since S generates D, defining the derivation $d_a(x) = xa - ax$, there exists $b \in S$ such that $y = d_a(b) \neq 0$, but $d_y = 0$.

Since $y = ab + ba$, and a and b are symmetric, y is also symmetric. Moreover, since y commutes with a, setting $y = ta$, we have that t is symmetric, and

$$ab + ba = y = ta,$$

can be rewritten as

$$a(t^{-1}b) + (t^{-1}b)a = a.$$

Calling $u = t^{-1}b$, we obtain the relation

$$aua^{-1} = u + 1. \tag{10}$$

Let D_0 be the division ring generated by u and a over $GF(2)$, and let Z_0 be its center. From the relation (10) we have that $\alpha = u(u+1)$ and a^2 both belong to Z_0, u is a root of $f(T) = T^2 + T + \alpha$, and that a is transcendental over $GF(2)$. Therefore $F = GF(2)(a^2, \alpha)$ is a non-absolute field, and by Theorem 2.1 there exist a non-archimedean valuation ν in $F(u)$ and an element $\omega \in F$, such that $\nu(a^2) = 0$, $\nu(\omega - u) > 0$ and $\nu(\omega - (u+1)) = 0$. By Proposition 2.1 $(\omega - u, (\omega - u)^{1+a})$ is a free symmetric pair. $\square$

Acknowledgments

The author was supported by Fapesp-Brazil, Projeto Tematico 2015/09162-9, and by Grant CNPq 301.205/2015-9.

References

[1] M. Chacron, A generalization of a theorem of Kaplansky and rings with involutions, *Mich. Math. J.* **20**(1) (1973) 45–54.

[2] V. O. Ferreira and J. Z. Goncalves, Free symmetric and unitary pairs in division rings infinite-dimensional over theirs centers, *Israel J. Math.* **210** (2015) 297–321.

[3] V. O. Ferreira, J. Z. Goncalves and A. Mandel, Free symmetric and unitary pairs in division rings with involution, *Int. J. Algebra Comput.* **15**(1) (2005) 15–36.

[4] V. O. Ferreira, J. Z. Goncalves and J. Sanchez, Free symmetric and unitary pairs in the field of fractions of torsion free nilpotent group algebras, *Algebra Represent. Theory* **23**(3) (2020) 605–619.

[5] J. Z. Goncalves, Constructing free groups in a normal subgroup of the multiplicative group of division rings, *J. Group Theory* **18**(5) (2015) 829–843.

[6] J. Z. Goncalves, Free groups in a normal subgroup of the field of fractions of a skew polynomial ring, *Commun. Algebra* **45**(13) (2017) 5193–5201.

[7] J. Z. Goncalves and A. Mandel, Are there free groups in division rings? *Israel J. Math.* **53**(1) (1986) 69–80.

[8] J. Z. Goncalves, A. Mandel and M. Shirvani, Free products of units in algebras I: Quaternion algebra, *J. Algebra* **214** (1999) 301–316.

[9] J. Z. Goncalves, A. Mandel and M. Shirvani, Free products of units in algebras: Crossed products, *J. Algebra* **233** (2000) 567–593.

[10] J. Z. Goncalves and D. S. Passman, Free pairs of symmetric elements in normal subgroups of division rings, *J. Algebra* **550** (2020) 154–185.

[11] J. Z. Goncalves and P. R. Oliveira, Free symmetric pairs in normal subgroups of division rings, Preprint.

[12] J. Z. Goncalves and M. Shirvani, Free symmetric and unitary pairs in central simple algebras with involution, *Contemp. Math.* **420** (2006) 121–139.

[13] I. N. Herstein, A unitary version of Brauer–Cartan–Hua theorem, *J. Algebra* **32** (1974) 555–560.

[14] M. Lazard, Sur les groups nilpotents et les aneaux de Lie, *Ann. Sci. Ecole. Norm. Sup.* **71**(2) (1954) 101–190.

[15] A. I. Lichtman, On subgroups of the multiplicative group of skewfields, *Proc. Amer. Math. Soc.* **63** (1977) 15–16.

[16] A. I. Lichtman, Matrix rings and linear groups over field of fractions of enveloping algebras and group ring I, *J. Algebra* **88** (1984) 1–37.

[17] A. I. Lichtman, Free subalgebras in division rings generated by universal enveloping algebras, *Algebra Colloq.* **6**(2) (1999) 145–153.

[18] Y. I. Merzljakov, *Rational Groups*, Contemporary Algebra (Moscow, 1980) (in Russian, Nauka).

[19] M. Nagata, T. Nakayama and T. Tuzuku, On an existence lemma in valuation theory, *Nagoya Math. J.* **6** (1953) 59–61.

[20] J. Sanchez, Free group algebras in division rings with valuation II, *Canadian J. Math* **72**(6) (2020) 1463–1504.