ON NORMAL SUBGROUPS OF D^* WHOSE ELEMENTS ARE PERIODIC MODULO THE CENTER OF D^* OF BOUNDED ORDER

Mai Hoang Bien

Dedicated to Professor Hendrik W. Lenstra for his 65th birthday

ABSTRACT. Let D be a division ring with the center $F = Z(D)$. Suppose that N is a normal subgroup of D^* which is radical over F, that is, for any element $x \in N$, there exists a positive integer n_x, such that $x^{n_x} \in F$. In [5], Herstein conjectured that N is contained in F. In this paper, we show that the conjecture is true if there exists a positive integer d such that $n_x \leq d$ for any $x \in N$.

Mathematics Subject Classification 2010: 16K20

Keywords: Division ring, normal subgroup, radical, central

1. Introduction

Let D be a division ring with the center $F = Z(D)$. For an element $x \in D$, if there exists a positive integer n_x such that $x^{n_x} \in F$ and $x^m \notin F$ for any positive integer $m < n_x$, then x is called n_x-*central*. If $n_x = 1$, x is said to be *central*. A subgroup N of the unit group D^* of D is called *radical* over F if for any element $x \in N$, there exists $n_x > 0$ such that x is n_x-central. Such a subgroup N is called *central* if $n_x = 1$ for any $x \in N$. In other words, N is central if and only if N is contained in F.

In 1978, Herstein [5] conjectured that if a subnormal subgroup N of D^* is radical over F then it is central. Two years later, he considered the conjecture again and proved that the assumption "subnormal" in this conjecture is equivalent to "normal" (see [6, Lemma 1]). That is, he asked whether a normal subgroup of D^* is central if it is radical over F. In [5], Herstein proved that the conjecture holds if N is torsion. As a consequence, one can see that the conjecture is also true if D is centrally finite. We notice that in [4], there is a different proof of this fact. Recall that a division ring D with the center F is called *centrally finite* if D is a finite dimensional vector space over F [8, Definition 14.1]. In [6], by using

the Pigeon-Hole Principle, Herstein also showed that the conjecture holds if F is uncountable.

Recently, there are some efforts to give the answer for this conjecture. In [3] and [2], we proved that the conjecture holds if D is either of type 2 or weakly locally finite. Actually, we get a more general result: if a normal subgroup of D^* is radical over a proper division subring K of D then it is central provided D is either of type 2 or weakly locally finite. Recall that a division ring D is of *type* 2 if $\dim_F F(x,y) < \infty$ for any $x, y \in D^*$. If $F(S)$ is a centrally finite division ring for any finite subset S of D then D is called *weakly locally finite*. Here, $F(S)$ denotes the division subring of D generated by $F \cup S$. In general, the conjecture remains still open.

In this paper, we give a positive answer for this conjecture in a particular case. In fact, we prove the following theorem.

Theorem 1.1. *Let D be a division ring and N be a normal subgroup of D^*. If there exists a positive integer d such that every element $x \in N$ is n_x-central for some positive integer $n_x \leq d$, then N is central.*

2. The proof of the Theorem

The technique we use in this paper is generalized rational expressions. For our further need, we recall some definitions and prove some lemmas.

First, basing on the structure of twisted Laurent series rings, we will construct a division ring which will be used for next lemmas. Let R be a ring and ϕ be a ring automorphism of R. We write $\mathcal{R} = R((t,\phi))$ for the ring of formal Laurent series $\sum_{i=n}^{\infty} a_i t^i$, where $n \in \mathbb{Z}, a_i \in R$, with the mutiplication defined by the twist equation $ta = \phi(a)t$ for every $a \in R$. In case $\phi(a) = a$ for any $a \in R$, we write $R((t)) = R((t,\phi))$. If $R = D$ is a division ring, then $\mathcal{D} = D((t,\phi))$ is also a division ring (see [8, Example 1.8]). Moreover, we have.

Lemma 2.1. *Let $R = D$ be a division ring, $\mathcal{D} = D((t,\phi))$ be as above, $F = Z(D)$ be the center of D, and $L = \{a \in D \mid \phi(a) = a\}$ be the fixed division ring of ϕ in D. If the center $k = Z(L)$ of L is contained in F, then the center of $\mathcal{D}$ is*

$$Z(\mathcal{D}) = \begin{cases} k & \text{if } \phi \text{ has infinite order,} \\ k((t^s)) & \text{if } \phi \text{ has an order } s. \end{cases}$$

Proof. The proof is similar to [8, Proposition 14.2]. It suffices to prove that $Z(D) \subseteq k$ if ϕ has infinite order, and $Z(\mathcal{D}) \subseteq k((t^s))$ in case f has an order s since it is easy to check that $k((t^s)) \subseteq Z(\mathcal{D})$ if f has an order s. Let

$\alpha = \sum\limits_{i=n}^{\infty} a_i t^i$ be in $Z(\mathcal{D})$. We first prove that $a_i \in k$ for every $i \geq n$. One

has $\sum\limits_{i=n}^{\infty} a_i t^{i+1} = (\sum\limits_{i=n}^{\infty} a_i t^i)t = t \sum\limits_{i=n}^{\infty} a_i t^i = \sum\limits_{i=n}^{\infty} \phi(a_i) t^{i+1}$. Hence, $\phi(a_i) = a_i$ for

every $i \geq n$. It means $a_i \in L$ for every $i \geq n$. Moreover, for any $a \in L$,

$\sum\limits_{i=n}^{\infty} a a_i t^i = (\sum\limits_{i=n}^{\infty} a_i t^i)a = \sum\limits_{i=n}^{\infty} a_i \phi(a) t^i = \sum\limits_{i=n}^{\infty} a_i a t^i$. Therefore, $a a_i = a_i a$ for ev-

ery $i \geq n$. It implies, $a_i \in k$ for every $i \geq n$. Now for any $b \in D$, $\sum\limits_{i=n}^{\infty} b a_i t^i =$

$(\sum\limits_{i=n}^{\infty} a_i t^i)b = \sum\limits_{i=n}^{\infty} a_i \phi^i(b) t^i = \sum\limits_{i=n}^{\infty} \phi^i(b) a_i t^i$, so that $b a_i = \phi^i(b) a_i$ for every $i \geq n$.

Case 1. The automorphism ϕ has infinite order. For some $i \neq 0$, from the fact that $(b - \phi^i(b))a_i = 0$, one has $a_i = 0$, which implies $\alpha = a_0 \in k$.

Case 2. The automorphism Φ has an order s. For any i which is not divided by n, since $(b - \phi^i(b))a_i = 0$, so that $a_i = 0$. Therefore, $\alpha = \sum\limits_{i=m}^{\infty} a_{si} t^{si} \in k((t^s))$. $\qquad\square$

Let $\{\, t_i \mid i \in \mathbb{Z} \,\}$ be a countable set of indeterminates and D be a division ring. We construct a family of division rings by the following way. Set

$$D_0 = D((t_0)), D_1 = D_0((t_1)),$$

$$D_{-1} = D_1((t_{-1})), D_2 = D_{-1}((t_2)),$$

for any $n > 1$,

$$D_{-n} = D_n((t_{-n})), D_{n+1} = D_{-n}((t_{n+1})).$$

Now put $D_\infty = \bigcup\limits_{n=-\infty}^{+\infty} D_n$. Then D_∞ is a division ring. Assume that F is the center of D. By Lemma 2.1, it is elementary to prove by induction on $n \geq 0$ that the center of D_0 is $F_0 = F((t_0))$, the center of D_{n+1} is $F_{n+1} = F_{-n}((t_{n+1}))$ and the center of D_{-n} is $F_{-(n+1)} = F_{n+1}((t_{-(n+1)}))$. In particular, F is contained in $Z(D_\infty)$. Consider an automorphism f on D_∞ defined by $f(a) = a$ for any a in D and $f(t_i) = t_{i+1}$ for every $i \in \mathbb{Z}$.

Proposition 2.2. *Let D, D_∞ and f be as above. Then $\mathcal{D} = D_\infty((t, f))$ is a division ring whose center coincides with the center F of D.*

Proof. We have D is the fixed division ring of f in D_∞. Since the center F of D is contained in the center of D_∞, f has infinite order and by Lemma 2.1, $Z(\mathcal{D}) = F$. $\qquad\square$

Recall that a *generalized rational expression* of a division ring D is an expression constructed from D and a set of noncommutative indeterminates using addition, subtraction, multiplication and division. A generalized rational expression over D

is called a *generalized rational identity* if it vanishes on all permissible substitutions from D. A generalized rational expression f of D is called nontrivial if there exists an extension division ring D_1 of D such that f is not a generalized rational identity of D_1. The details of generalized rational identities can be found in [9].

Given a positive integer n and $n+1$ noncommutative indeterminates $x, y_1, \cdots, y_n$, put

$$g_n(x, y_1, y_2, \cdots, y_n) = \sum_{\delta \in S_{n+1}} \text{sign}(\delta).x^{\delta(0)} y_1 x^{\delta(1)} y_2 x^{\delta(2)} \ldots y_n x^{\delta(n)},$$

where S_{n+1} is the symmetric group of $\{0, 1, \cdots, n\}$ and $\text{sign}(\delta)$ is the sign of permutation δ. This is the generalized rational expression defined in [1] to connect an algebraic element of degree n and a polynomial. We have the first property of this generalized rational expression.

Lemma 2.3. *Let D be a division ring with the center F. For any element $a \in D$, the following are equivalent:*

(1) *The element a is algebraic over F of degree less than n.*

(2) *$g_n(a, r_1, r_2, \cdots, r_n) = 0$ for any $r_1, r_2, \cdots, r_n \in D$.*

Proof. See [1, Corollary 2.3.8]. $\qquad\qquad\square$

Let D be a division ring with center F and a be an element of D. Then, by definition, $g_n(axa^{-1}x^{-1}, y_1, y_2, \cdots, y_n)$ is also a generalized rational expressions of D. Notice that, in general, the expression $g_n(x, y_1, \cdots, y_n)$ is a polynomial but $g_n(axa^{-1}x^{-1}, y_1, y_2, \cdots, y_n)$ is not necessary a polynomial. If a is algebraic of degree less than n over F then $g_n(a, y_1, y_2, \cdots, y_n)$ is a trivial generalized rational expression according to Lemma 2.3. However, the following lemma shows that $g_n(axa^{-1}x^{-1}, y_1, y_2, \cdots, y_n)$ is always nontrivial if a is not in F.

Lemma 2.4. *Let D be a division ring with center F. If $a \in D \backslash F$, then the generalized rational expression $g_n(axa^{-1}x^{-1}, y_1, y_2, \cdots, y_n)$ is nontrivial.*

Proof. Let D_∞, $\mathcal{D} = D_\infty((t, f))$ and F be as in Proposition 2.2. Since $a \notin F$, there exists $c \in D$ such that $c = aba^{-1}b^{-1} \neq 1$. Because a, b, c commute with t,

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

If $a(b + t)a^{-1}(b + t)^{-1}$ is algebraic over F, then so is $(c - 1)(1 + b^{-1}t)^{-1}$. Hence, $(c - 1)^{-1} + b^{-1}(c - 1)^{-1}t = ((c - 1)(1 + b^{-1}t)^{-1})^{-1}$ is algebraic over F. Let $p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$, with $m > 0$, be the minimal polynomial

of $(c-1)^{-1} + b^{-1}(c-1)^{-1}t$ over F. It means

$$0 = ((c-1)^{-1} + b^{-1}(c-1)^{-1}t)^m + \cdots + a_1((c-1)^{-1} + b^{-1}(c-1)^{-1}t) + a_0.$$

For instance, $(b^{-1}(c-1)^{-1})^m = 0$, a contradiction! Therefore, $a(b+t)a^{-1}(b+t)^{-1}$ is not algebraic over F. Using Lemma 2.3, we have

$$g_n(a(b+t)a^{-1}(b+t)^{-1}, r_1, r_2, \cdots, r_n) \neq 0,$$

for some $r_1, r_2, \cdots, r_n \in \mathcal{D}$. This means $g_n(axa^{-1}x^{-1}, y_1, y_2, \cdots, y_n)$ is nontrivial.
□

A polynomial identity ring is a ring R with a non-zero polynomial P vanishing on all permissible substitutions from R. In this case, P is called *polynomial identity* of R or we say that R *satisfies* P. There is a well-known result: a division ring is a polynomial identity division ring if and only if it is centrally finite (see [7, Theorem 6.3.1]). We have a similar property for generalized rational identity division rings.

Lemma 2.5. *Let D be a division ring with the center F. If there exists a nontrivial generalized rational identity of D, then either D is centrally finite or F is finite.*

Proof. See [9, Theorem 8.2.15].   □

Now we are ready to prove our Theorem.

Proof of Theorem 1.1. Suppose that N is not contained in F. Then, there exists $a \in N\backslash F$. For any $d+1$ elements $r, r_1, r_2, \cdots, r_d$ of D with $r \neq 0$, since $ara^{-1}r^{-1} \in N$ is $n_{a,r}$-central element for some $0 < n_{a,r} \leq d$, by Lemma 2.3,

$$g_d(ara^{-1}r^{-1}, r_1, r_2, \cdots, r_d) = 0.$$

By Lemma 2.4, $g_d(axa^{-1}x^{-1}, y_1, y_2, \cdots, y_d)$ is a nontrivial generalized rational identity of D. Now, in view of Lemma 2.5, either D is centrally finite or F is finite. If D is centrally finite, then $N \subseteq F$ by [3, Theorem 3.1]. If F is finite, then N is torsion, so by [5, Theorem 8], $N \subseteq F$. Thus, in both cases we have $N \subseteq F$, a contradiction.   □

References

[1] K. I. Beidar, W. S. Martindale 3rd and A. V. Mikhalev, Rings with Generalized Identities, Marcel Dekker, Inc., New York-Basel-Hong Kong, 1996.

[2] B. X. Hai, M. H. Bien and T. T. Deo, *On linear groups over weakly locally finite division rings*, Algebra Colloq., in press.

[3] B. X. Hai, T. T. Deo and M. H. Bien, *On subgroups in division rings of type 2*, Studia Sci. Math. Hungar., 49(4) (2012), 549–557.

[4] B. X. Hai and L. K. Huynh, *On subgroups of the multiplicative group of a division ring*, Vietnam J. Math., 32 (2004), 21–24.

[5] I. N. Herstein, *Multiplicative commutators in division rings,* Israel J. Math., 31(2) (1978), 180–188.

[6] I. N. Herstein, *Multiplicative commutators in division rings II*, Rend. Circ. Mat. Palermo (2), 29(3) (1980), 485–489.

[7] I. N. Herstein, Noncommutative Rings, Cambridge University Press, 2005.

[8] T. Y. Lam, A First Course in Noncommutative Rings, MGT 131, Springer, 1991.

[9] L. H. Rowen, Polynomial Identities in Ring Theory, Academic Press, Inc., New York, 1980.

Mai Hoang Bien

Mathematisch Instituut

Leiden Universiteit, The Netherlands

and

Dipartimento di Matematica

Università degli Studi di Padova, Italy

e-mail: maihoangbien012@yahoo.com