A NOTE ON LOCAL COMMUTATORS IN DIVISION RINGS WITH INVOLUTION

Mai Hoang Bien

Abstract. In this paper, we consider a conjecture of I. N. Herstein for local commutators of symmetric elements and unitary elements of division rings. For example, we show that if $D$ is a finite dimensional division ring with involution $\star$ and if $a \in D^\ast = D\\backslash\{0\}$ such that local commutators $axa^{-1}x^{-1}$ at $a$ are radical over the center $F$ of $D$ for every $x \in D^\ast$ with $x^\ast = x$, then either $a \in F$ or $\dim_{F} D = 4$.

1. Introduction and main results

Let $R$ be a ring. A function $\star : R \to R, x \mapsto x^\star$, is called an involution if it is an anti-morphism of degree 2, that is, $(x + y)^\ast = x^\ast + y^\ast; (xy)^\ast = y^\ast x^\ast$; and $(x^\ast)^\ast = x$ for every $x, y \in R$. An element $x \in R$ is called symmetric (resp. skew symmetric and unitary) if $x^\ast = x$ (resp. $x^\ast = -x$ and $x^\ast x = xx^\ast = 1$). Put $S = \{x \in R \mid x^\ast = x\}, K = \{x \in R \mid x^\ast = -x\}$ and $N = \{x \in R \mid x^\ast x = xx^\ast = 1\}$, the set of symmetric elements, the set of skew symmetric elements and the set of unitary elements respectively. It is natural and interesting to ask that if a certain subset relating directly to the involution $\star$ (e.g. the set of symmetric elements) of the ring $R$ is subjected to a certain condition, then how does it effect to the whole ring $R$? In this paper, we focus on the case when $R$ is a division ring with a conjecture from Herstein. In 1978, Herstein posed the following conjecture.

Conjecture 1.1 ([16, Conjecture 2]). Let $D$ be a division ring with center $F$ and an element in the multiplicative group $D^\ast = D\\backslash\{0\}$ of $D$. If for every $x \in D^\ast$, the local commutator $axa^{-1}x^{-1}$ at $a$ is radical over $F$, that is, $(axa^{-1}x^{-1})^{n_x} \in F$ for some positive integer $n_x$, then $a \in F$.

The answer to Conjecture 1.1 is affirmative in the cases when $F$ is uncountable [5, Corollary 2] and when $D$ is a finite dimensional division ring, that is, $\dim_{F} D < \infty$ [3, Corollary 2.10]. In general, the conjecture is still open. There

Received May 17, 2018; Revised November 7, 2018; Accepted December 5, 2018.

2010 Mathematics Subject Classification. 16K20, 16R50.

Key words and phrases. division ring, involution, symmetric element, unitary element, local commutator.

©2019 Korean Mathematical Society
are several subjects relating to this conjecture (e.g. see [12,14,16,17,21]). For example, the subject on the existence of non-cyclic free subgroups in \( D^* \) is one of them if \( a \) and \( x \) generate a non-cyclic free subgroup of \( D^* \), then \( axa^{-1}x^{-1} \) is not radical over \( F \). These subjects have been then studied in division rings with involution (e.g. see [4,8,9,11,18]). In particular, [13] could be a good survey to see what is different between the existence of non-cyclic free subgroups in division rings and in division rings with involution.

The aim of this work is to show the symmetric version and unitary version for Conjecture 1.1 in case \( D \) is finite dimensional and in case \( F \) is uncountable. We first focus on the case when \( D \) is finite dimensional. In fact, we show the following result.

**Theorem 1.2.** Let \( D \) be a finite dimensional division ring with center \( F \), let * be an involution of \( D \), and let \( a \) be an element of \( D \). Denote by \( S \) and \( N \) respectively the set of symmetric elements and the set of unitary elements of \( D \). Assume that \( \dim_F D > 4 \).

1. If \( axa^{-1}x^{-1} \) is radical over \( F \) for every \( x \in S \setminus \{0\} \), then \( a \in F \).
2. If \( \text{char}(D) \neq 2 \) and \( axa^{-1}x^{-1} \) is radical over \( F \) for every \( x \in N \), then \( a \in F \).

Our results except the case when \( \dim_F D \leq 4 \). In fact, every division ring whose dimension over its center is 1 is a field, so the theorem still holds and it is trivial. In the case when \( \dim_F D = 4 \), we give a counterexample. Let \( H = \mathbb{R} \oplus \mathbb{R} i \oplus \mathbb{R} j \oplus \mathbb{R} k \) be the real quaternion division ring. One has the center of \( H \) is \( \mathbb{R} \). If we define

\[
(a_1 + a_2 i + a_3 j + a_4 k)^* = a_1 - a_2 i - a_3 j - a_4 k
\]

for every element \( a_1 + a_2 i + a_3 j + a_4 k \in H \), then \( S \), the set of symmetric elements of \( H \), is \( \mathbb{R} \). Hence, \( axa^{-1}x^{-1} = 1 \) for every \( x \in S \setminus \{0\} \) and \( a \in H \). Now if we define

\[
(a_1 + a_2 i + a_3 j + a_4 k)^\# = a_1 + a_2 i + a_3 j - a_4 k
\]

for every element \( a_1 + a_2 i + a_3 j + a_4 k \in H \), then \# is also an involution of \( H \).

We can show that the set of unitary elements of \( H \) with respect to \# is

\[
N = \{ x \in H \mid x^\# x = xx^\# = 1 \} = \{ \cos \alpha + k \sin \alpha \mid \alpha \in [0, 2\pi) \}.
\]

Therefore, \( kxk^{-1}x^{-1} = 1 \) for every \( x \in N \) but \( k \not\in \mathbb{R} \). Moreover, with the unitary version, we additionally assume that \( \text{char}(D) \neq 2 \). The main reason we just consider the assumption \( \text{char}(D) \neq 2 \) is from the Cayley parametrization: with the assumption \( \text{char}(D) \neq 2 \), one has that if \( u \) is unitary, then \( u = (1 - k)(1 + k)^{-1} \) for some \( k \in K \); conversely, if \( k \in K \), then \( (1 - k)(1 + k)^{-1} \) is unitary. Hence, in this case, the set of unitary elements is “big enough”.

Observe that in 1979, P. M. Cohn introduced a division ring of characteristic 2 in which 1 is the only unitary element (see [6]).
Now we move to the case when the center $F$ is uncountable. We separate this case into two subcases: $\text{char}(D) = 0$ and $\text{char}(D) > 0$. When $\text{char}(D) = 0$, we receive an analogue of Theorem 1.2.

**Theorem 1.3.** Let $D$ be a division ring with uncountable center $F$ and $\text{char}(D) = 0$, let $\star$ be an involution of $D$ and let $a$ be an element of $D$. Denote by $S$ and $N$ respectively the set of symmetric elements and the set of unitary elements of $D$. Assume that one of following conditions holds:

1. Local commutators $axa^{-1}x^{-1}$ at $a$ are radical over $F$ for every $x \in S \setminus \{0\}$.
2. Local commutators $axa^{-1}x^{-1}$ at $a$ are radical over $F$ for every $x \in N$.

If $\dim_F D > 4$, then $a \in F$.

Unfortunately, we are unable to show an analogue of Theorems 1.2 and 1.3 in the case when $\text{char}(D) > 0$ and $F$ is uncountable. In following theorem, we additionally assume all commutators at $a$ are torsion.

**Theorem 1.4.** Let $D$ be a division ring with uncountable center $F$ and $\text{char}(D) > 0$, let $\star$ be an involution of $D$ and let $a$ be an element of $D$. Denote by $S$ and $N$ respectively the set of symmetric elements and the set of unitary elements of $D$. Assume that one of following conditions holds:

1. $axa^{-1}x^{-1}$ is torsion for every $x \in S \setminus \{0\}$.
2. $\text{char}(D) > 2$ and $axa^{-1}x^{-1}$ is torsion for every $x \in N$.

If $\dim_F D > 4$, then $a \in F$.

The ideas of proofs used in this paper are from the theory of group identities in algebras (e.g. from [7] and [10]) combining with that from [5].

Our notations in this paper are standard. In particular, for a division ring $D$, the center of $D$ is denoted by $Z(D)$ and if $S$ is a subset of $D$ and $K$ is a subfield of $Z(D)$, then $K(S)$ denotes the division subring of $D$ generated by $S$ over $K$.

2. Proofs

To show our main results, we borrow some lemmas.

**Lemma 2.1** ([3, Lemma 2.6]). Let $D$ be a finite dimensional division ring and $T$ a finite subset of $D$. If $P$ is the prime subfield of $D$ and $F_1$ is the center of the division subring $D_1$ of $D$ generated by $T$ (over the prime subfield $P$), then $F_1$ is finitely generated over $P$.

**Lemma 2.2** ([19, Lemma 3.1]). Let $D$ be a finite dimensional division ring whose center $F$ is finitely generated over its prime subfield. Then there exists a positive integer $n$ such that if $a \in D$ with $a^n(a) \in F$ for some positive integer $n(a)$, then $a^n \in F$.

Let $D' = [D^*, D^*]$ be the derived group of $D^*$, that is, $D'$ is the subgroup of $D^*$ generated by all commutators $aba^{-1}b^{-1}$ where $a, b$ range over $D^*$.
Lemma 2.3. Let $D$ be a finite dimensional division ring whose center $F$ is finitely generated over its prime subfield. Then there exists a positive integer $\ell$ such that if $a \in D'$ with $a^{n(a)} \in F$ for some positive integer $n(a)$, then $a^\ell = 1$.

Proof. Assume that $\dim_F D = m$. Then $D$ may consider as an $F$-subalgebra of $\operatorname{End}_F D \cong M_m(F)$ via the ring morphism $\Phi: D \to \operatorname{End}_F D, a \mapsto \Phi_a$ where $\Phi_a$ is defined by $\Phi_a(x) = ax$ for every $x \in D$. Now assume that $a \in D'$ such that $a^{n(a)} \in F$ for some positive integer $n(a)$. According to Lemma 2.2, there exists a positive integer $n$ such that $a^n = \alpha \in F$. Moreover, the images of $a$ and $\alpha$ are respectively $\Phi(a) = A \in SL_m(F)$ and $\Phi(\alpha) = \alpha I_m$ where $SL_m(F)$ is the special linear group over $F$. Hence, $A^n = \alpha I_m$. By taking the determinant of two sides, one has $1 = \alpha^m$. Therefore, if $\ell = mn$, then $a^\ell = (a^n)^m = \alpha^m = 1$.

The proof is complete. \[ \square \]

Let $D$ be a division ring and let $t$ be a central indeterminate over $D$. Denote by $D[t]$ the polynomial ring $D[t]$ in $t$ over $D$, by $D(t)$ the division ring of quotients of $D[t]$, and by $D((t))$ the Laurent series polynomial ring in $t$ over $D$. By [20, Example 1.6], $D((t))$ is a division ring and $D(t)$ is considered as a division subring of $D((t))$. For convenience, we always write an element $f(t)$ of $D((t))$ as $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots$ with increasing powers from left to right.

Lemma 2.4 ([2, Lemma 2.1]). For any $a, a_1, a_2, b \in D$, there exist $c, d \in D$ such that $(1 + at)^{-1} a_1 (1 + bt) a_2 = a_1 a_2 (1 + ct)(1 + dt)^{-1}$ in $D(t)$.

Lemma 2.5. Let $D$ be a division ring with center $F$ and let $f(t)$ be a polynomial of the polynomial ring $D[t]$ in a central indeterminate $t$ over $D$. If there are infinitely many elements $\alpha \in F$ such that $f(\alpha) = 0$, then $f(t)$ is identically zero.

Proof. The proof is the Vandermonde argument (or see [22, Propositions 2.3.26 and 2.3.27]). \[ \square \]

Now we are ready to show our main results.

Proof of Theorem 1.2. Let $P$ be the prime subfield of $D$.

(1) Assume $a \notin F$. We seek a contradiction. By [15, Theorem 2.1.6], $F(S) = D$. Since $a \notin F$, there exists $b \in S$ such that $ba \neq ab$. Let $D_1 = P(a, a^*, b)$ be the division subring of $D$ generated by $a, a^*$ and $b$ over $P$. Then it is obvious that $P \subseteq S$, so $D_1$ is invariant under $*$, that is, $x^* \in D_1$ for every $x \in D_1$. It implies that $*$ is an involution of $D_1$. Moreover, by Lemma 2.1, $D_1$ is finite dimensional over its center $F_1 = Z(D_1)$ and $F_1$ is finitely generated over the prime subfield $P$. According to Lemma 2.3, there exists a positive integer $n$ such that $(axa^{-1} x^{-1})^n = 1$ for every $x \in S_1 = S \cap D_1$. Let $t$ be a central indeterminate and consider the element $f_1(t) = (a(1+bt)a^{-1}(1+bt)^{-1})^n$ in $D_1(t)$. According to Lemma 2.4, $f_1(t) = g(t) h(t)^{-1}$ where $g(t), h(t)$ are polynomials in $D_1[t]$. Put $L_1 = \{x \in F_1 \mid x^* = x\}$ the fixed subfield of $F_1$. 

...
with respect to the involution $\star$. It is clear that $\dim_{L_1} F_1 \leq 2$, so $\dim_{L_1} D_1 = \dim_{L_1} F_1. \dim_{F_1} D_1 < \infty$. If $L_1$ is finite, then so is $D_1$, which implies that $D_1$ is commutative by Wedderburn’s little Theorem. As a corollary, $ab = ba$, a contradiction. Therefore, $D_1$ is commutative by Wedderburn’s little Theorem. As a corollary, $ab = ba$.

Moreover, as an element in the Laurent series division ring $D_1((t))$, the element $(1 + bt)^{-1}$ is written as $(1 + bt)^{-1} = 1 - bt + b^2t^2 + \cdots + (-1)^m b^m t^m + \cdots$. Hence,

$$a(1 + bt)a^{-1}(1 + bt)^{-1} = 1 + (a^{-1}ba - b)t + \cdots.$$ 

It implies that

(I) $$(1 + (a^{-1}ba - b)t + \cdots)^n = f_1(t) \equiv 1.$$

If $\text{char}(D_1) = 0$, then the left hand side of (I) is $1 + n(a^{-1}ba - b)t + \cdots$, so one has $a^{-1}ba - b = 0$, which contradicts to the hypothesis that $ab \neq ba$. If $\text{char}(D_1) = p > 0$, then we assume $n = p^m \ell$ with $(p, \ell) = 1$. In this case, the left hand side of (I) is

$$\begin{align*}
(1 + (a^{-1}ba - b)t + \cdots)^{p^m \ell} &= (1 + (a^{-1}ba - b)^{p^m \ell} + \cdots) \\
&= 1 + \ell(a^{-1}ba - b)^{p^m \ell} + \cdots.
\end{align*}$$

As a corollary, $\ell(a^{-1}ba - b)^{p^m} = 0$, equivalently, $aba^{-1} = b$. Again, this contradicts to the hypothesis. Both cases lead us to a contradiction. The first statement is complete.

(2) Assume $a \notin F$. Let $K$ be the set of skew elements of $D$. By [15, Theorem 2.1.10], $F(K) = D$, which implies that there exists $c \in K$ such that $ac \neq ca$. We repeat arguments as in the previous part with some modifications. Denote by $D_2 = P(a, a^*, c)$ the division subring of $D$ generated by $a, a^*$ and $c$. Then $D_2$ is a finite dimensional division ring whose center $F_2 = Z(D_2)$ is finitely generated over its prime subfield $P$. Put $K_2 = \{x \in D_2 \mid x^* = -x\} = K \cap D_2$, the set of all skew symmetric elements, and $N_2 = \{x \in D_2 \mid x^*x = 1\} = N \cap D_2$, the set of all unitary elements of $D_2$. According to Lemma 2.3, there exists a positive integer $n$ such that $(axa^{-1}x^{-1})^n = 1$ for every $x \in N_2$. Put $f_2(t) = (a(1 - ct)(1 + ct)^{-1}a^{-1}(1 + ct)(1 - ct)^{-1})^n$ in $D_2(t)$. Observe that $(1 - c\lambda)(1 + c\lambda)^{-1} \in N_2$ whenever $\lambda \in L_2 = \{x \in F_2 \mid x^* = x\}$, so using the same arguments as in the previous part, we have $f_2(t) \equiv 1$. Now as an element in the Laurent series division ring $D_2((t))$,

$$a(1 - ct)(1 + ct)^{-1}a^{-1}(1 + ct)(1 - ct)^{-1} = 1 + 2(c - aca^{-1})t + \cdots,$$

which implies that

(II) $$(1 + 2(c - aca^{-1})t + \cdots)^n = f_2(t) \equiv 1.$$
Proof of Theorem 1.3. Put $L = \{x \in F \mid x^* = x\}$. Because $\dim_L F \leq 2$ and $F$ is uncountable, $L$ is also uncountable.

(1) Assume that $axa^{-1}x^{-1}$ is radical over $F$ for every $x \in S \setminus \{0\}$. We show that $a \in F$. We first claim that $a^{-1}ba - b \in F$ for every $b \in S$. Indeed, let $b \in S$. Then, for each $\alpha \in L$, one has

\[
(a(1 + ba)a^{-1}(1 + ba)^{-1})^n(\alpha) \in F
\]

for some $n(\alpha) > 0$. Hence, since $L$ is uncountable, there exists a positive $n$ such that $(a(1 + ba)a^{-1}(1 + ba)^{-1})^n \in F$ for infinitely many elements $\alpha \in F$. Let $t$ be a central indeterminate and consider the element

\[
f(t) = (a(1 + bt)a^{-1}(1 + bt)^{-1})^n
\]

in $D(t)$. According to Lemma 2.4, $f(t) = g(t)v(t)^{-1}$ where $g(t)$, $v(t)$ are polynomials in $D[t]$. Since $f(\alpha) \in F$ for infinitely many element $\alpha \in F$, by [21, Lemma 1], $g(t)v(t)^{-1} = f(t) \in F(t)$, that is, all coefficients of $g(t)$ and $v(t)$ belong to $F$. Moreover, if we write $f(t)$ as an element in $D(\{t\})$, then $f(t) = a_0 + a_1t + \cdots$ where $a_i \in F$. On the other hand,

\[
(a(1 + ba)a^{-1}(1 + ba)^{-1})^n = (1 + (a^{-1}ba - b)t + \cdots)^n
\]

\[
= 1 + n(a^{-1}ba - b)t + \cdots.
\]

Hence, $a^{-1}ba - b \in F$. The claim is shown. Therefore,

\[
(a^{-1}ba - b)c - c(a^{-1}ba - b) = 0
\]

for every $b, c \in S$. Now suppose that $a \notin F$. Then $S$ satisfies a generalized polynomial identity $g(a^{-1}xa - x)y - g(a^{-1}xa - x) = 0$. By [1, Corollary 6.2.5], $D$ also satisfies a generalized polynomial identity. It is well known that every division ring satisfying a generalized polynomial identity is finite dimensional over its center (e.g. see [1, Theorem 6.1.9]), so $D$ is finite dimensional over $F$. In the view of Theorem 1.2, one has $\dim_F D \leq 4$, which contradicts to the hypothesis. Thus, $a \in F$.

(2) Assume that local commutator $axa^{-1}x^{-1}$ at $a$ is radical over $F$ for every $x \in N$. Let $K = \{x \in D \mid x^* = -x\}$ be the set of all skew symmetric elements of $D$. Similarly, we claim that $a^{-1}ca - c \in F$ for every $c \in K$. Indeed, assume that $c \in K$. Clearly, $(1 + c\lambda)(1 - c\lambda)^{-1}$ is unitary whenever $\lambda \in L$. We consider the element

\[
g(t) = (a(1 - ct)(1 + ct)^{-1}a^{-1}(1 + ct)(1 - ct)^{-1})^n
\]

in $D(t)$. Using the same arguments as in the previous, we have $g(t) \in F(t)$. On the other hand, as an element in the Laurent series division ring $D(\{t\})$,

\[
a(1 - ct)(1 + ct)^{-1}a^{-1}(1 + ct)(1 - ct)^{-1} = 1 + 2(c - ca^{-1})t + \cdots,
\]
which implies that $1 + 2n(c - ac a^{-1})t + \cdots = (1 + 2(c - ac a^{-1})t + \cdots)^n = g(t) \in F[[t]]$. Therefore $a^{-1}ca - c \in F$. The claim is shown. If $a \notin F$, then $K$ satisfies a generalized polynomial identity $(a^{-1}xa - x)y - y(a^{-1}xa - x) = 0$. In the view of [1, Corollary 6.2.5], $D$ also satisfies a generalized polynomial identity. Using [1, Theorem 6.1.9] again, $\dim_F D < \infty$. By Theorem 1.2, $\dim_F D \leq 4$. Contradiction.

Proof of Theorem 1.4. Put $p = \text{char}(D)$ and $L = \{x \in F \mid x^p = x\}$. One has $L$ is uncountable since $\dim_FL \leq 2$.

(1) Assume that $axa^{-1}x^{-1}$ is torsion and $\dim_F D > 4$. Then, by [15, Theorem 2.1.6], $F(S) = D$, so there exists $b \in S$ such that $ab \neq ba$. For each $\alpha \in L$, one has

$$(a(1 + ba)a^{-1}(1 + ba)^{-1})^n(\alpha) = 1$$

for some $n(\alpha) > 0$. Hence, since $L$ is uncountable, there exists a positive $n$ such that $(a(1 + ba)a^{-1}(1 + ba)^{-1})^n = 1$ for infinitely many elements $\alpha \in L$. Let $t$ be a central indeterminate and consider the element

$$f(t) = (a(1 + bt)a^{-1}(1 + bt)^{-1})^n$$

in $D(t)$. Using the same arguments as in Theorem 1.2, $f(t) \equiv 1$ in $D(t)$. Moreover, $f(t) = (a(1 + bt)a^{-1}(1 + bt)^{-1})^n = (1 + (a^{-1}ba - b)t + \cdots)^n$ in $D(t(t))$. We assume $n = p^m\ell$ with $(p, \ell) = 1$. One has

$$(1 + (a^{-1}ba - b)t + \cdots)^{p^m\ell} = (1 + (a^{-1}ba - b)p^{m\ell} + \cdots)^\ell = 1 + \ell(ab^{-1} - b)p^{m\ell} + \cdots.$$ 

As a corollary, $\ell(ab^{-1} - b)p^{m\ell} = 0$, which implies that $aba^{-1} = b$, equivalently, $ab = ba$. This contradicts the hypothesis.

(2) Let $K$ be the set of skew symmetric elements of $D$. Assume that $a \notin F$. Then, by [15, Theorem 2.1.10], $F(K) = D$, so there exists $c \in K$ such that $ac \neq ca$. It is similar to the previous part and Theorem 1.2(2), by replacing $1 + bt$ by $(1 - bt)(1 + bt)^{-1}$ in the arguments, we conclude that $a^{-1}ba - b = 0$, equivalently, $ab = ba$. A contradiction! □

Acknowledgements. The author would like to thank the referee for carefully reading the paper. His/Her comments have improved the presentation of this paper. This research was funded by Vietnam National University HoChiMinh City (VNU-HCM) under grant number C2018-18-03.

References


Mai Hoang Bien
Faculty of Mathematics and Computer Science
University of Science-VNUHCM
227 Nguyen Van Cu Str., Dist. 5, HCM-City, Vietnam
Email address: mhbien@hcmus.edu.vn, maihoangbien012@yahoo.com