MAXIMAL SUBFIELDS OF A DIVISION ALGEBRA

MAI HOANG BIEN

ABSTRACT. Let $D$ be a division algebra over a field $F$. In this paper, we prove that there exist $a, b, x, y \in D^* = D\setminus \{0\}$ such that $F(ab - ba)$ and $F(xyx^{-1}y^{-1})$ are maximal subfields of $D$, which answers questions posted in [5].

1. Introduction

Let $F$ be a field. A ring $D$ is called a division algebra over $F$ if the center $Z(D) = \{a \in D \mid ab = ba, \forall b \in D\}$ of $D$ is equal to $F$, $D$ is a finite dimensional vector space over $F$ and $D$ has neither proper left ideal nor proper right ideal. In other words, $D$ is a division ring with the center $F$ and $\dim_F D < \infty$. In some books and papers, $D$ is also called centrally finite [4, Definition 14.1]. A central simple algebra over $F$ is an algebra isomorphic to $M_n(D)$ for some positive integer $n$ and division algebra $D$ over $F$. For any central simple algebra $A$ over $F$, $\sqrt{\dim_F A}$ is said to be degree of $A$.

For any division algebra $D$ over $F$, it is well known from Kothe’s Theorem that there exists a maximal subfield $K$ of $D$ such that the extension of fields $K/F$ is separable [4, Th. 15.12]. In [1, Theorem 7], authors proved that for any separable extension of fields $K/F$ in $D$, there exists an element $c \in [D, D]$, the group of additive commutators of $(D, +)$, such that $K = F(c)$ unless $\text{Char}(F) = [K : F] = 2$ and 4 does not divide the degree of $D$. Hence, if $K$ is a maximal subfield of $D$ which is separable over $F$, then there exists $c \in [D, D]$ such that $K = F(c)$. In particular, there exists a maximal subfield of $D$ such that it is of the form $F(c)$ for some element $c$ in $[D, D]$. We have a natural question: is it true that there exists a commutator $ab - ba \in [D, D]$ such that $F(ab - ba)$ is a maximal subfield of $D$ (see [5, Problem 28])? Almost similarly, if $K/F$ is a separable extension of fields in $D$ then there exists an element $d \in D' = [D^*, D^*]$, the group of multiplicative commutators of $D^* = D\setminus \{0\}$, such that $K = F(d)$ (see [5, Theorem 2.26]). Again, the author asked whether $F(xyx^{-1}y^{-1})$ is a maximal subfield of $D$ for some $x, y \in D^*$ (see [5, Problem 29]).

The goal of this paper is to answer in the affirmative for both questions. The main tools used in this paper are generalized rational identities over a central simple algebra. Readers can find their definitions and notions in detail in [2] and [6].

2. Results

Let $R$ be a ring. Recall that an element $a$ of $R$ is called algebraic of degree $n$ over a subring $S$ of $R$ if there exists a polynomial $f(x)$ of degree $n$ over $S$ such as

\begin{align*}
\text{Key words and phrases.} & \quad \text{Maximal subfield, division algebra, commutator, algebraic.} \\
\text{2010 Mathematics Subject Classification.} & \quad 12F05, 12F10, 12E15, 16K20. \\
\text{The author would like to thank his supervisor Prof. H.W. Lenstra for the comments.} \end{align*}
Lemma 2.3. The algebra of degree $m$ is basic.

Theorem 2.2. Assume that $K$ is a subfield of $D$ containing $F$. Then $\dim_F K \leq n$. The quality holds if and only if $K$ is a maximal subfield of $D$.

Proof. See [4, Corollary 15.6 and Proposition 15.7].

Lemma 2.4. Let $F$ be an infinite field and $n \geq 2$ be an integer. There exist two matrices $A, B \in M_n(F)$ such that the commutator $ABA^{-1}B^{-1}$ is an algebraic element of degree $n$ over $F$.
**Theorem 2.5.** Let $D$ be a central division algebra over a field $F$. There exist $x, y \in D^*$ such that $F(xyx^{-1}y^{-1})$ is a maximal subfield of $D$.

**Proof.** If $F$ is finite then $D$ is also finite, so that there is nothing to prove. Suppose that $F$ is infinite and $D$ is of degree $n$ over $F$. By Lemma 2.3, it suffices to show that there exist $x, y \in D^*$ such that $\dim_F F(xyx^{-1}y^{-1}) \geq n$. Indeed, put $\ell = \max\{ \dim_F F(xyx^{-1}y^{-1}) \mid x, y \in D^* \}$. Then from Lemma 2.3, 

$$g(t) = \sum_{i=0}^{\ell} a_i t^i$$

for any $a_i \in D$. Hence, $g(t)$ is a generalized rational identity for $D$, so that, by Lemma 2.3, $g(t)$ is a generalized rational identity for $M_n(F)$. Since $g(t)$ is an algebraic element of degree $n$ over $F$.

**Lemma 2.6.** Let $F$ be an infinite field and $n > 2$ be an integer. There exist two matrices $A, B \in M_n(F)$ such that $AB - BA$ is an algebraic element of degree $n$ over $F$.

**Proof.** Put

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{n-1} \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

and $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n-1} \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, where

$$a_i, b_j \neq 0.$$ One has $ABA^{-1}B^{-1} = \begin{pmatrix} b_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & b_{n-1} \\ b_1b_1^{-1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & b_{n-1}b_{n-1}^{-1} \end{pmatrix}$.

If we choose $b_1b_1^{-1}, b_1b_2^{-1}, \ldots, b_{n-1}b_{n-1}^{-1}$ all distinct (it is possible since $F$ is infinite), then the characteristic polynomial of $ABA^{-1}B^{-1}$ is a polynomial of smallest degree which vanishes on $ABA^{-1}B^{-1}$. That is, $ABA^{-1}B^{-1}$ is an algebraic element of degree $n$ over $F$. ■

The following theorem answers Problem 29 in [3] Page 83].
we can choose \( b_1, b_2, \cdots, b_{n-1} \in F \) such that \( b_1, b_1 - b_2, \cdots, b_{n-2} - b_{n-1}, b_{n-1} \) all distinct. Hence, the characteristic polynomial of \( AB - BA \) is a polynomial of smallest degree vanishing on \( AB - BA \). Therefore, \( AB - BA \) is an algebraic element of degree \( n \) over \( F \). \( \blacksquare \)

Almost similar to the proof of Theorem 2.5 we have the following theorem, which answers Problem 28 in [5, Page 83].

**Theorem 2.7.** Let \( D \) be a central division algebra over a field \( F \). There exist \( x, y \in D \) such that \( F(xy - yx) \) is a maximal subfield of \( D \).

**Proof.** If \( F \) is finite then \( D \) is also finite, so that there is nothing to prove. Suppose that \( F \) is infinite and \( D \) is of degree \( n \). By Lemma 2.3 it suffices to show that there exist \( x, y \in D \) such that \( \dim F(xy - yx) \geq n \). Indeed, if \( n = 2 \), by [4, Corollary 13.5], then there exist \( x, y \in D \) such that \( xy - yx \notin F \), which implies \( F(xy - yx) = 2 = n \). Assume that \( n > 2 \). Then put \( \ell = \max \{ \dim F(xy - yx) | x, y \in D \} \). By Lemma 2.1, 

\[
g_\ell(rs - sr, r_1, r_2, \cdots, r_\ell) = 0
\]

for any \( r_1, r_2, \cdots, r_\ell \in D \) and \( r, s \in D^* \). It follows \( g_\ell(xy - yx, y_1, y_2, \cdots, y_\ell) \) is a generalized rational identity of \( D \). From Lemma 2.2 \( g_\ell(xy - yx, y_1, y_2, \cdots, y_\ell) \) is also a generalized rational identity of \( M_n(F) \). But because there exist \( A, B \in M_n(F) \) such that \( AB - BA \) is algebraic of degree \( n \) (Lemma 2.4), one has 

\[
g_\ell(AB - BA, r_1, r_2, \cdots, r_\ell) = 0
\]

for any \( r_1 \in M_n(F) \). Therefore, by Lemma 2.1, \( n \leq \ell \). \( \blacksquare \)

**References**

[1] S. Akbari, M. Arian-Nejad, M. L. Mehrabadi, On additive commutator groups in division rings, *Results Math.*, 33 (1-2), 921, 1998.
[2] S. A. Amitsur, Rational identities and applications to algebra and geometry, *J. Algebra* 3, 304–359, 1966.
[3] K. I. Beidar, W. S. Martindale 3rd and A. V. Mikhalev, *Rings with Generalized Identities*, Marcel Dekker, Inc., New York- Basel-Hong Kong, 1996.
[4] T. Y. Lam, *A first course in noncommutative rings*, MGT 131, Springer, 1991.
[5] M. Mahdavi-Hezavehi, Commutators in division rings revisited. *Bull. Iranian Math. Soc.*, 26(3): 7–88, 2000.
[6] L. H. Rowen, *Polynomial identities in ring theory*, Academic Press, Inc., New York, 1980.

**Mathematisch Instituut, Leiden Universiteit, Niels Bohrweg 1,2333 CA Leiden, The Netherlands.**

**Current address:** Dipartimento di Matematica, Università degli Studi di Padova, Via Trieste 63, 35121 Padova, Italy.

**E-mail address:** maihoangbien012@yahoo.com