Mehdi Aaghabali; Mai Hoang Bien

Certain simple maximal subfields in division rings

Czechoslovak Mathematical Journal, Vol. 69 (2019), No. 4, 1053–1060

Persistent URL: http://dml.cz/dmlcz/147913

Czechoslovak Mathematical Journal, 69 (144) (2019), 1053–1060

CERTAIN SIMPLE MAXIMAL SUBFIELDS IN DIVISION RINGS

Mehdi Aaghabali, Edinburgh, Tehran, Mai Hoang Bien, Ho Chi Minh City

Received January 22, 2018. Published online June 5, 2019.

Abstract. Let D be a division ring finite dimensional over its center F. The goal of this paper is to prove that for any positive integer n there exists $a \in D^{(n)}$, the nth multiplicative derived subgroup such that $F(a)$ is a maximal subfield of D. We also show that a single depth-n iterated additive commutator would generate a maximal subfield of D.

Keywords: division ring; rational identity; maximal subfield

MSC 2010: 16K20, 16R50, 17A35

1. Preliminary

Throughout this paper, D is a division ring with center F. An element $a \in D$ is called *algebraic* over F if there exists a nonzero polynomial $a_0 + a_1x + \ldots + a_nx^n$ over F such that $a_0 + a_1a + \ldots + a_na^n = 0$. If $a \in D$, then $F(a)$ denotes the subfield of D generated by F and $\{a\}$. For a (multiplicative) group G we denote by $(a, b) = aba^{-1}b^{-1}$ the multiplicative commutator of $a, b \in G$ and (G, G) the multiplicative commutator subgroup of G. We denote by $G \supseteq G' \supseteq \ldots \supseteq G^{(n)} \supseteq \ldots$ the derived series of G, that is, $G' = (G, G)$ and $G^{(n+1)} = (G^{(n)}, G^{(n)})$ for every $n \geqslant 1$. For a unital associative ring R we use $[a, b] = ab - ba$ to denote the additive commutator of $a, b \in R$ and $R_1 = [R, R]$ the additive commutator subgroup of R. We denote by $R \supseteq R_1 \supseteq \ldots \supseteq R_n \supseteq \ldots$ the additive derived series of R, that is, $R_1 = [R, R]$ and $R_{n+1} = [R_n, R_n]$ for every $n \geqslant 1$. For a given division ring D we call $D^{(n)}$ and D_n the nth multiplicative and additive derived groups of D, respectively. In the case of division ring D we simply use D' and $[D, D]$ to denote the multiplicative and additive group of commutators in D, respectively. If A is a subset of D, we use A^*

The research of the first author was supported by ERC grant number 320974. The second author was funded by Vietnam National University Ho Chi Minh City (VNU-HCM) under grant no. C2018-18-03.

DOI: 10.21136/CMJ.2019.0039-18

to denote $A \setminus \{0\}$. A subfield K of D is called a *maximal subfield* if K is its own centralizer in D^*. We denote by $\dim_F D$ the dimension of D over F. If $\dim_F D = n^2$, then n is called the *degree* of division ring D. By $M_n(K)$, $\mathrm{GL}_n(K)$ and $\mathrm{SL}_n(K)$ we mean all square matrices, all invertible matrices and all matrices of determinant one of order n with entries from K, respectively.

Mahdavi-Hezavehi in [10] investigates the algebraic properties of the multiplicative group of commutators in a division ring and shows that any subfield K of a division ring D which is separable over the center of D is generated over the center by a commutator subgroup of D'. Afterwards, Mahdavi-Hezavehi and his colleagues in [12] studied other generating properties of commutator subgroup and showed that each finite separable extension of the center of D could be considered as a simple extension $F(c)$, where c is an element in D'. Now, it is natural to consider similar questions in terms of some other elements coming from certain substructures of a division ring. In particular, one can pose the following questions:

Question 1.1 ([11], Problems 28, 29)**.** Let D be a division ring finite dimensional over its center F.

(i) For any noncentral normal subgroup N of D^*, does there exist an element $c \in N$ such that $F(c)$ is a maximal subfield in D?

(ii) For any noncentral subnormal subgroup N of D^*, does there exist an element $c \in N$ such that $F(c)$ is a maximal subfield in D?

In this note we rely on rational identities to show that some maximal subfields are generated by elements coming from $D^{(n)}$ and D_n, or the nth derived subgroup of D^* and the nth iterated group of additive commutators, for any positive integer n. These fall under a wider class of problems concerning the question of whether a noncentral subnormal subgroup of D^* cannot be "too small", and questions about the images of (noncommutative) polynomials evaluated on central simple algebras. For $n = 1$, both results have been proved by Chebotar et al. in [6], Theorem 3, Theorem 6, and recently again by the authors and Akbari in [1], Theorem 6, Theorem 7. Both [1], [6] and the current paper use rational polynomial identities for proving the aforementioned results. The idea is simple and clever: The key is a certain (noncommutative) polynomial $g_n(x, y_1, \ldots, y_n)$ that vanishes whenever an algebraic element of degree not more than n is substituted into x. One takes $n < \deg D$, substitutes a relevant rational expression into x and proves that the resulting expression cannot vanish on $D \otimes_F L$, where L is some splitting field of D. In [1] and [6], the expressions substituted into x are single additive, or multiplicative commutators on two variables, whereas here, iterated commutators are considered.

2. Rational identities

Let F be a field and $X = \{x_1, \ldots, x_m\}$ be m noncommuting indeterminates. Denote by $F\langle X\rangle$ and $F(X)$, respectively, the free algebra in X over F and the universal division ring of fractions of $F\langle X\rangle$. A *rational expression* over F is an element of $F(X)$. Let R be an F-algebra. A rational expression f over F is said to be a *rational identity* of R if it vanishes on all permissible substitutions from R. In this case, we say that R *satisfies the rational identity* $f = 0$.

Example 2.1.

(1) It is not hard to see that (Hua's identity) $(x^{-1}+(y^{-1}-x^{-1})^{-1})^{-1}-x+xyx = 0$ is a rational identity of every algebra over an arbitrary field F.
(2) One can easily verify that $(x+y)^{-1} - y^{-1}(x^{-1}+y^{-1})^{-1}x^{-1} = 0$ is a rational identity of every algebra over an arbitrary field F.
(3) It is easy to check that $((x,(y,z)x(y,x)^{-1})^3, z) = 0$ vanishes on permissible substitutions of $M_3(F)$ for any field F.

A rational identity f of an algebra R is called *nontrivial* if f is nonzero in $F(X)$, see [6]. In the special case when $R = D$ is a division ring, we have some further information: assume that $f = 0$ is a rational identity of D. Then f is nontrivial if and only if there exists a division ring L containing all coefficients of f and f is not a rational identity of L. One direction of the statement is trivial, to see the other direction, assume that f is nontrivial. Then it is well known that there exists a division ring L with infinite center, which contains F, and that L is infinite dimensional over its center. Hence by [7], $f = 0$ is not a rational identity of D. In the example, it is easily seen that (1) and (2) are trivial, however one can verify that (3) is nontrivial.

In this paper, our algebras R are central simple algebras over a field F. That is, $R \cong M_n(D)$, where D is a division ring which is finite dimensional over F. We denote by $\mathcal{I}(R)$ the set of all nontrivial rational identities of the algebra R. It is known that a division ring D with infinite center F is a finite dimensional vector space over its center if and only if $\mathcal{I}(D) \neq \emptyset$, see [7]. Therefore there are rings R with $\mathcal{I}(R) = \emptyset$. Moreover:

Theorem 2.2 ([3], Theorem 11)**.** *Let F be an infinite field and R be a central simple F-algebra with $\dim_F R = n^2$. Assume that L is a field extension of F. Then $\mathcal{I}(R) = \mathcal{I}(M_n(F)) = \mathcal{I}(M_n(L))$.*

We consider the following example of a rational expression which is important in this paper. Given a positive integer n and $n+1$ noncommutative indeterminates

$x, y_1, \ldots, y_n$, put

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

where S_{n+1} is the symmetric group of $\{0, \ldots, n\}$ and $\operatorname{sign}(\delta)$ is the sign of permutation δ. This is a rational expression defined in [5] as a mean to test whether an element is algebraic of degree n. This rational expression may be considered as a generalisation of the characteristic polynomials of matrices of degree n over a field.

Lemma 2.3. *Let $R = M_n(D)$ be a central simple algebra over its center F. For any element $a \in R$, the following conditions are equivalent.*

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

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

P r o o f. It is just a corollary of [5], Corollary 2.3.8. □

3. Subfields generated by the elements in the nth multiplicative derived subgroup

Let n be a positive integer and let $x_1, \ldots, x_{2^n}$ be 2^n indeterminates. We will define a special rational polynomial $u_n(x_1, \ldots, x_{2^n})$ successively as follows: set $u_1(x_1, x_2) = (x_1, x_2) = x_1 x_2 x_1^{-1} x_2^{-1}$ and assume that $u_{n-1}(x_1, \ldots, x_{2^{n-1}})$ is defined. Then we put

$$u_n(x_1, \ldots, x_{2^n}) = u_1(u_{n-1}(x_1, \ldots, x_{2^{n-1}}), u_{n-1}(x_{2^{n-1}+1}, \ldots, x_{2^n})).$$

This polynomial relates to the solvability of a group: if G is a solvable group of length $\leqslant n$, that is $G^{(n)} = 1$, then $u_n(a_1, \ldots, a_{2^n}) = 1$ for every $a_1, \ldots, a_{2^n} \in G$. In fact, we show the following result.

Lemma 3.1. *Let u_n be as above. If G is a group with (multiplicative) derived series*

$$G \supseteq G' \supseteq \ldots \supseteq G^{(n)} \supseteq \ldots,$$

then $u_n(a_1, \ldots, a_{2^n}) \in G^{(n)}$ for $a_1, \ldots, a_{2^n} \in G$.

P r o o f. We prove the lemma by induction on n. Assume that G is a group and $a_1, a_2 \in G$. One has $a_1 a_2 a_1^{-1} a_2^{-1} \in G'$, which implies that $u_1(a_1, a_2) \in G'$. Hence, the lemma holds for u_1 and for the group G. Assume that for every group H, $u_{n-1}(a_1, \ldots, a_{2^{n-1}}) \in H^{(n-1)}$ for every $a_1, \ldots, a_{2^{n-1}} \in H$. We must prove that for every group G, $u_n(b_1, \ldots, b_{2^n}) \in G^{(n)}$ for every $b_1, \ldots, b_{2^n} \in G$. This follows immediately from the definitions of u_n and $G^{(n)}$ by induction on n. □

Lemma 3.2. *Let K be an infinite field and $m > 1$. For any positive integer n and every nonscalar matrix $C \in \mathrm{SL}_m(K)$ there exist nonscalar matrices $A_1, \ldots, A_{2^n} \in \mathrm{SL}_m(K)$ such that $C = u_n(A_1, \ldots, A_{2^n})$.*

P r o o f. We show the lemma by induction on n. Assume that $n = 1$. It is well-known that every nonscalar matrix in $\mathrm{SL}_m(K)$ is a single commutator, see [13]. Hence, there exist nonscalar matrices $A_1, A_2 \in \mathrm{SL}_m(K)$ such that $C = A_1 A_2 A_1^{-1} A_2^{-1}$. Thus, the statement holds for $n = 1$. Assume that the statement is true for $n-1$, that is, for every nonscalar matrix $C \in \mathrm{SL}_m(K)$ there exist nonscalar matrices $A_1, \ldots, A_{2^{n-1}} \in \mathrm{SL}_m(K)$ such that $C = u_{n-1}(A_1, \ldots, A_{2^{n-1}})$. Now by the induction hypothesis for every nonscalar matrix C there exist nonscalar matrices $B_1, B_2, A_1, \ldots, A_{2^n} \in \mathrm{SL}_m(K)$ such that $C = u_1(B_1, B_2), B_1 = u_{n-1}(A_1, \ldots, A_{2^{n-1}})$ and $B_2 = u_{n-1}(A_{2^{n-1}+1}, \ldots, A_{2^n})$. Therefore

$$\begin{aligned} C = u_1(B_1, B_2) &= u_1(u_{n-1}(A_1, \ldots, A_{2^{n-1}}), u_{n-1}(A_{2^{n-1}+1}, \ldots, A_{2^n})) \\ &= u_n(A_1, \ldots, A_{2^n}). \end{aligned}$$

This implies that the statement is true for n. □

Before showing the main result of this section, we recall the following well-known lemma.

Lemma 3.3 ([9], page 242)**.** *Let D be a division ring with center F and K be a subfield of D containing F. If $\dim_F D = m^2$, then $\dim_F K \leqslant m$. The equality holds if and only if K is a maximal subfield of D.*

Theorem 3.4. *Let D be a division ring finite dimensional over a its center F. For any positive integer n there exists $a \in D^{(n)}$, the nth multiplicative derived subgroup, such that $F(a)$ is a maximal subfield of D.*

P r o o f. If F is finite, then D is also finite and we have nothing to prove. Suppose that F is infinite and $\dim_F D = m^2$. By Lemma 3.3, it suffices to show that there exists $a \in D^{(n)}$ such that $\dim_F F(a) \geqslant m$. Indeed, put

$$l = \max\{\dim_F F(u_n(a_1, \ldots, a_{2^n}))\colon\ a_1, \ldots, a_{2^n} \in D^*\}.$$

Applying Lemma 2.3 we see that $g_l(u_n(a_1, \ldots, a_{2^n}), r_1, \ldots, r_l) = 0$ for any $r_1, \ldots, r_l \in D$ and $a_1, \ldots, a_{2^n} \in D^*$. In other words,

$$g_l(u_n(x_1, \ldots, x_{2^n}), y_1, \ldots, y_l) = 0$$

is a rational identity of D. It is not hard to verify that $g_l(u_n(x_1, \ldots, x_{2^n}), y_1, \ldots, y_l)$ is a nonzero element of $F(x_1, \ldots, x_{2^n}, y_1, \ldots, y_l)$ (see [8], Theorem 3.4). Hence, by Theorem 2.2 it is also a rational identity of $M_n(F)$. This yields that

$$g_l(u_n(A_1, \ldots, A_{2^n}), B_1, \ldots, B_l) = 0$$

for all matrices $A_i \in \mathrm{GL}_m(F)$ and $B_i \in M_m(F)$. In view of Lemma 2.3, $u_n(A_1, \ldots, A_{2^n})$ is algebraic over F of degree not more than l for every $A_1, \ldots, A_{2^n} \in M_m(F)$. Now consider the $(m \times m)$-matrix $T = (t_{ij})_{1 \leqslant i,j \leqslant m}$ as follows: if $j = i$ or $j = i + 1$, then $t_{ij} = 1$, otherwise $t_{ij} = 0$. It is easy to see that $T \in \mathrm{SL}_m(F)$ and T is algebraic of degree m over F. By Lemma 3.2, one can find matrices $A_1, \ldots, A_{2^n} \in \mathrm{SL}_m(F)$ such that $u_n(A_1, \ldots, A_{2^n}) = T$. Hence, $l \geqslant m$. This completes the proof. □

4. Subfields generated by the elements in the nth additive derived subgroup

Let n be a positive integer and let $x_1, \ldots, x_{2^n}$ be 2^n indeterminates. We define a polynomial $v_n(x_1, \ldots, x_{2^n})$ successively as follows: set $v_1(x_1, x_2) = [x_1, x_2] = x_1x_2 - x_2x_1$. Assume that $v_{n-1}(x_1, \ldots, x_{2^{n-1}})$ is defined. Then we put

$$v_n(x_1, \ldots, x_{2^n}) = v_1(v_{n-1}(x_1, \ldots, x_{2^{n-1}}), v_{n-1}(x_{2^{n-1}+1}, \ldots, x_{2^n})).$$

Lemma 4.1. *Let R be an algebra with additive derived series*

$$R \supseteq R_1 \supseteq \ldots \supseteq R_n \supseteq \ldots.$$

If v_n is defined as above, then $v_n(a_1, \ldots, a_{2^n}) \in R_n$ for $a_1, \ldots, a_{2^n} \in R$.

Proof. The proof is similar to that of Lemma 3.1. □

Lemma 4.2. *Let K be a field and $m > 1$ such that $\mathrm{char}\, K \nmid m$. For any positive integer n and every matrix $C \in M_m(K)$ with zero-trace there exist matrices $A_1, \ldots, A_{2^n} \in M_m(K)$ whose trace is zero and $C = v_n(A_1, \ldots, A_{2^n})$.*

Proof. The idea of the proof is similar to that of Lemma 3.2. We prove the lemma by induction on n. Assume that $n = 1$. In view of [2], which states that every matrix in $M_n(K)$ with zero-trace is a single additive commutator, there exist $A_1, A_2 \in M_m(K)$ such that $C = A_1A_2 - A_2A_1$. Set $B_1 = A_1 - (\mathrm{tr}(A_1)/m)I_m$ and $B_2 = A_2 - (\mathrm{tr}(A_2)/m)I_m$, where by $\mathrm{tr}(A)$ we mean the trace of A. We have $C = B_1B_2 - B_2B_1 = v_1(B_1, B_2)$ and $\mathrm{tr}(B_1) = \mathrm{tr}(B_2) = 0$. Hence, the statement holds for $n = 1$. The general case follows by induction on n, similarly to the proof of Lemma 3.2. □

The following result is the goal of this section. Note that the same result as Theorem 3.4, however, follows from the case where $n = 1$, proved in [1] and [6], since by a theorem of Amitsur and Rowen, $D_1 = D_2 = D_3 = \ldots$, see [4]. However, the proof yields a slightly stronger claim that a single depth-n iterated additive commutator would generate a maximal subfield, which does not follow from $D_1 = D_2 = D_3 = \ldots$

Theorem 4.3. *Let D be a division ring finite dimensional over its center F of characteristic either zero or a prime p such that $p \nmid \dim_F D$. For any positive integer n there exists a depth-n iterated additive commutator which generates a maximal subfield of D.*

P r o o f. First note that if $\operatorname{char} F = 0$, then by a result due to Amitsur and Rowen in [4] we have $D_1 = D_2 = \ldots$ Hence, in this case the result follows from [1], Theorem 7. In case of $\operatorname{char} F = p > 0$, the proof is similar to the one of Theorem 3.4. We assume that F is infinite since if F is finite, then D is also finite and there is nothing to prove. Suppose $\dim_F D = m^2$. In view of Lemma 3.3, it suffices to show that there exists $a \in D_n$ such that $\dim_F F(a) \geqslant m$. Indeed, put

$$l = \max\{\dim_F F(v_n(a_1, \ldots, a_{2^n})) \colon\ a_1, \ldots, a_{2^n} \in D^*\}.$$

According to Lemma 2.3 we see that $g_l(v_n(a_1, \ldots, a_{2^n}), r_1, \ldots, r_l) = 0$ for any $r_1, \ldots, r_l \in D$ and $a_1, \ldots, a_{2^n} \in D^*$. In other words,

$$g_l(v_n(x_1, \ldots, x_{2^n}), y_1, \ldots, y_l) = 0$$

is a polynomial identity of D, so it is also a rational identity of $M_n(F)$ (Lemma 2.2). Note that it is easily seen that $g_l(v_n(x_1, \ldots, x_{2^n}), y_1, \ldots, y_l)$ is a nonzero element of $F(x_1, \ldots, x_{2^n}, y_1, \ldots, y_l)$ (see [8], Theorem 3.4). This yields that

$$g_l(v_n(A_1, \ldots, A_{2^n}), B_1, \ldots, B_l) = 0$$

for all matrices $A_i, B_i \in M_m(F)$. According to Lemma 2.3, $v_n(A_1, \ldots, A_{2^n})$ is algebraic over F of degree not more than l for every $A_1, \ldots, A_{2^n} \in M_m(F)$. Now consider the $(m \times m)$-matrix $T = (t_{ij})_{1 \leqslant i,j \leqslant m}$ defined by $t_{i(i+1)} = 1$ and $t_{ij} = 0$ if $j \neq i + 1$. We can show that $\operatorname{tr}(T) = 0$ and T is algebraic of degree m over F. By Lemma 4.2, there exist matrices $A_1, \ldots, A_{2^n} \in M_m(F)$ such that $v_n(A_1, \ldots, A_{2^n}) = T$. Hence, $l \geqslant m$ and this completes the proof. □

References

[1] *M. Aaghabali, S. Akbari, M. H. Bien*: Division algebras with left algebraic commutators. Algebr. Represent. Theory *21* (2018), 807–816. zbl MR doi

[2] *A. A. Albert, B. Muckenhoupt*: On matrices of trace zeros. Mich. Math. J. *4* (1957), 1–3. zbl MR doi

[3] *S. A. Amitsur*: Rational identities and applications to algebra and geometry. J. Algebra *3* (1966), 304–359. zbl MR doi

[4] *S. A. Amitsur, L. H. Rowen*: Elements of reduced trace 0. Isr. J. Math. *87* (1994), 161–179. zbl MR doi

[5] *K. I. Beidar, W. S. Martindale, III, A. V. Mikhalev*: Rings with Generalized Identities. Pure and Applied Mathematics 196, Marcel Dekker, New York, 1996. zbl MR

[6] *M. A. Chebotar, Y. Fong, P.-H. Lee*: On division rings with algebraic commutators of bounded degree. Manuscr. Math. *113* (2004), 153–164. zbl MR doi

[7] *K. Chiba*: Generalized rational identities of subnormal subgroups of skew fields. Proc. Am. Math. Soc. *124* (1996), 1649–1653. zbl MR doi

[8] *B. X. Hai, T. H. Dung, M. H. Bien*: Almost subnormal subgroups in division rings with generalized algebraic rational identities. Available at `https://arxiv.org/abs/1709.04774`.

[9] *T. Y. Lam*: A First Course in Noncommutative Rings. Graduate Texts in Mathematics 131, Springer, New York, 2001. zbl MR doi

[10] *M. Mahdavi-Hezavehi*: Extension of valuations on derived groups of division rings. Commun. Algebra *23* (1995), 913–926. zbl MR doi

[11] *M. Mahdavi-Hezavehi*: Commutators in division rings revisited. Bull. Iran. Math. Soc. *26* (2000), 7–88. zbl MR

[12] *M. Mahdavi-Hezavehi, S. Akbari-Feyzaabaadi, M. Mehraabaadi, H. Hajie-Abolhassan*: On derived groups of division rings. II. Commun. Algebra *23* (1995), 2881–2887. zbl MR doi

[13] *R. C. Thompson*: Commutators in the special and general linear groups. Trans. Am. Math. Soc. *101* (1961), 16–33. zbl MR doi

Authors' addresses: Mehdi Aaghabali (corresponding author), School of Mathematics, University of Edinburgh, Edinburgh EH9 3JZ, Scotland; School of Mathematics, Statistics and Computer Science, University of Tehran, Tehran, Iran, e-mail: `maghabali@gmail.com`; Mai Hoang Bien, Faculty of Mathematics and Computer Science, University of Science, VNU-HCM, 227 Nguyen Van Cu Str., Dist. 5, Ho Chi Minh City, Vietnam, e-mail: `mhbien@hcmus.edu.vn`.