Chapter 5

Maximal subfields of a division algebra

Let F be a field. A ring is called a *central F-algebra* if its center is equal to F. A central F-algebra D is called a *division F-algebra* if the dimension of D, as a vector space over F, is finite and D has neither non-zero proper left ideals nor non-zero proper right ideals. In other words, D is a division ring with center F and $\dim_F D < \infty$. In some books and papers, such a D is also called *centrally finite* [29, Definition 14.1]. A *central simple F-algebra* is a ring which is isomorphic to $M_n(D)$ for some positive integer n and division F-algebra D. For any central simple F-algebra A, the integer $\sqrt{\dim_F A}$ is said to be the *degree* of A.

Let D be a division F-algebra. Let $(D, +)$ and D^* be the *additive group* and the *multiplicative group* of non-zero elements of D, respectively. Let $[D, D]$ be the additive subgroup of the additive group $(D, +)$ generated by all commutators $xy - yx$ where x, y range over D, and D' be the multiplicative subgroup of the multiplicative group D^* generated by all commutators $xyx^{-1}y^{-1}$ where x, y range over D^*. It is well known from the Kothe Theorem that there exists a maximal subfield K of D such that the extension of fields K/F is separable [29, Theorem 15.12]. In [1, Theorem 7], it was proved that for any separable extension of fields K/F in D, there exists an element $c \in [D, D]$ such that

$K = F(c)$ unless $\mathrm{Char}(F) = \dim_F K = 2$ and 4 does not divide the degree of D. Hence, if the degree D is different from 2 then there exists $c \in [D, D]$ such that $F(c)$ is a maximal subfield of D. In case the degree of D is equal to 2 then, by [29, Corollary 13.5], there exists $c \in [D, D]$ such that $F(c) \neq F$, which implies $F(c)$ is a maximal subfield of D. Therefore, in both cases, there exists $c \in [D, D]$ such that $F(c)$ is a maximal subfield of D. We answer the following natural question that appear in [32]. Is it true that there exists an additive commutator $ab - ba \in [D, D]$ such that $F(ab - ba)$ is a maximal subfield of D (see [32, Problem 28])? Similarly, for multiplicative structure, there exists an element $d \in D^*$ such that $K = F(d)$ is a maximal subfield of D [32, Theorem 2.26]. Do there exist $x, y \in D^*$ such that $F(xyx^{-1}y^{-1})$ is a maximal subfield of D [32, Problem 29]?

The goal of this Chapter is to answer both questions affirmatively. The main tools used in this paper are rational identities over a central simple algebra. In the first Section, we recall some notions of rational identities of a central simple algebra, and also a specific rational expression which works even over the maximal right ring of quotients of a prime ring.

5.1 Rational identities of central simple algebras

Rational expressions.

The notion of "rational identity" which is a generalization of polynomial identities were attended after Amitsur used it for solving some problems of algebra and geometry (see [3]). A *rational expression* over a central F-algebra R is an expression formed from a set $X = \{ x_i \mid i \in I \}$ of non-commutative indeteminates with coefficients in F by addition, subtraction, multiplication and division. A rational expression f over R 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* f. For instance.

Examples 5.1.1. 1. (Hua's identity) $(x^{-1} + (y^{-1} - x^{-1})^{-1})^{-1} - x + xyx$ is a rational identity of every algebra.

2. It is easy to check $(x+y)^{-1} - y^{-1}(x^{-1}+y^{-1})^{-1}x^{-1}$ is a rational identity of every algebra.

3. It is easy to check $[[x,[y,z]x[y,x]^{-1}]^3,z]$ vanishes on permissible substitutions of $M_3(F)$ for any field F.

A rational identity f of a central F-algebra R is called *non-trivial* if there exist a field K which contains all coefficients of f and a central K-algebra S such that f is not a rational identity over S. Otherwise, f is called *trivial*. In examples 5.1.1, (1) and (2) are trivial, and one can check that (3) is non-trivial.

We denote $\mathcal{I}(R)$ the set of all non-trivial rational identities of a central F-algebra R.

Theorem 5.1.2. [36, Theorem 8.2.11] *A division ring D with infinite center F is a division F-algebra if and only if $\mathcal{I}(D) \neq \emptyset$.*

Theorem 5.1.3. [3, Theorem 11] *Let F be an infinite field and A be a central simple F-algebra of degree n. Assume that L is an extension field of F. Then $\mathcal{I}(A) = \mathcal{I}(M_n(F)) = \mathcal{I}(M_n(L))$.*

From Theorem 5.1.3, over a division algebra, there exists a non-trivial rational identity. Next we consider a special rational identity which may be thought of as a generalisation of characteristic polynomials of matrices of degree n over a field.

A rational expression

We consider the following example of a rational expression which is important in this Chapter. Given an integer $n \geq 1$ and $n+1$ non-commutative indeterminates $x, y_1, \cdots, y_n$, put

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

where S_{n+1} is the symmetric group of $\{0, 1, \cdots, n\}$ and $\mathrm{sign}(\delta)$ is the sign of permutation δ. This is a rational expression defined in [5] to connect an algebraic element of degree n and a polynomial of $n+1$ indeterminates.

Remark 5.1.4. *If $f, f_1, f_2, \cdots, f_n$ are rational expressions, then so is $g_n(f, f_1, f_2, \cdots, f_n)$.*

Let R be a ring with center $Z = Z(R)$. Recall that an element a of R is called *algebraic of degree n* over Z if there exists a polynomial $f(x)$ of degree n over Z such that $f(a) = 0$ and there is no polynomial of degree less than n vanishing on a. In general, $f(x)$ is not irreducible even if Z is a field. For example, the matrix $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in M_2(F)$, where F is a field, satisfies polynomial $f(x) = (x-1)(x-2)$. Since $A \notin F$, the smallest degree of all the polynomials vanishing on A is 2.

A ring R is called *prime* if, for two-sided ideals I, J of R with $IJ = 0$, then $I = 0$ or $J = 0$.

Lemma 5.1.5. [5, Corollary 2.3.8] *Let R be a prime ring, $Q_{mr}(R)$ be the maximal ring of quotients of R as in Chapter 1 and $Z = Z(Q_{mr}(R))$ be the center of $Q_{mr}(R)$. For any element $a \in Q_{mr}(R)$, the following conditions are equivalent:*

1. *The element a is algebraic over Z of degree less than n.*
2. *$g_n(a, r_1, r_2, \cdots, r_n) = 0$ for any $r_1, r_2, \cdots, r_n \in Q_{mr}(R)$.*

Let A be a central simple algebra. Then A is semisimple, so that every A-module is injective [14, Therem 1.2]. In particular, for every right ideal I of A, there exists a right ideal J of A such that $I_A \oplus J_A = A_A$ as A-modules. It means, A has the unique dense right ideal A as Definitions in Chapter 1. Therefore, $Q_{mr}(A) = A$. We have a corollary of Lemma 5.1.5.

Corollary 5.1.6. *Let F be a field and A be a central simple F-algebra. For any element $a \in A$, the following conditions 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 $r_1, r_2, \cdots, r_n \in A$.*

5.2 An application

We can apply rational identities to study maximal subfields of a division algebra. The following Lemma is basic.

Lemma 5.2.1. *Let F be a field and D be a division F-algebra of degree n. Assume that K is a subfield of D containing F. Then $\dim_F K \leq n$. The equality holds if and only if K is a maximal subfield of D.*

PROOF. See [29, Corollary 15.6 and Proposition 15.7] ∎

Lemma 5.2.2. *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.*

PROOF. Put

$$A := \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } B := \begin{pmatrix} b_1 & 0 & \cdots & 0 & 0 \\ 0 & b_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & b_{n-1} & 0 \\ 0 & 0 & 0 & 0 & b_n \end{pmatrix}, \text{ where } b_j \neq 0.$$

One has $ABA^{-1}B^{-1} = \begin{pmatrix} b_n b_1^{-1} & 0 & \cdots & 0 & 0 \\ * & b_1 b_2^{-1} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ * & * & * & b_{n-2} b_{n-1}^{-1} & 0 \\ * & * & * & * & b_{n-1} b_n^{-1} \end{pmatrix}$.

If we choose $b_n b_1^{-1}, b_1 b_2^{-1}, \cdots, b_{n-1} b^{-1}$ 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 [32, Page 83].

Theorem 5.2.3. *Let F be a field and D be a division F-algebra. 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 $D = F$. There is nothing to prove. Suppose that F is infinite and D is of degree n over F. By Lemma 5.2.1, 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 Corollary 5.1.6,

$$g_\ell(rsr^{-1}s^{-1}, r_1, r_2, \cdots, r_\ell) = 0$$

for any $r_1, r_2, \cdots, r_\ell \in D$ and $r, s \in D^*$. Hence, $g_\ell(xyx^{-1}y^{-1}, y_1, y_2, \cdots, y_\ell)$ is a rational idenity of D, so that, by Theorem 5.1.3, $g_\ell(xyx^{-1}y^{-1}, y_1, y_2, \cdots, y_\ell)$ is also a rational idenity of $M_n(F)$. Since $g_\ell(ABA^{-1}B^{-1}, r_1, r_2, \cdots, r_\ell) = 0$, for any $r_i \in M_n(F)$ and A, B are chosen in Lemma 5.2.2. Therefore $n \leq \ell$ because $ABA^{-1}B^{-1}$ is an algebraic element of degree n and by Corollary 5.1.6. ∎

Lemma 5.2.4. *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

$$A := \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \text{ and } B := \begin{pmatrix} 0 & b_1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & b_2 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & b_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

One has $AB - BA = \begin{pmatrix} -b_1 & * & \cdots & * & * \\ 0 & b_1 - b_2 & \cdots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & b_{n-2} - b_{n-1} & * \\ 0 & 0 & \cdots & 0 & b_{n-1} \end{pmatrix}$. Since F is infinite, 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. ∎

Similar to the proof of Theorem 5.2.3, we have the following Theorem, which answers Problem 28 in [32, Page 83].

Theorem 5.2.5. *Let F be a field and D be a division F-algebra. 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 $D = F$. There is nothing to prove. Suppose that F is infinite and D is of degree n. By Lemma 5.2.1, it suffices to show that there exist $x, y \in D$ such that $\dim_F F(xy - yx) \geq n$. Indeed, if $n = 2$, by [29, 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 $\ell := \max\{ \dim_F F(xy - yx) \mid x, y \in D \}$. By Corollary 5.1.6,

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

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 rational idenity of D. From Theorem 5.1.3, $g_\ell(xy - yx, y_1, y_2, \cdots, y_\ell)$ is also a rational idenity of $M_n(F)$. But because there exist $A, B \in M_n(F)$ such that $AB - BA$ is algebraic of degree n (Lemma 5.2.4), one has

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

for any $r_i \in M_n(F)$. Therefore, by Corollary 5.1.6, $n \leq \ell$. ∎