

CHARACTERISTIC POLYNOMIALS OF CENTRAL SIMPLE ALGEBRAS

Chia-Fu Yu

Abstract. We characterize characteristic polynomials of elements in a central simple algebra A . We also give an account for the theory of rational canonical forms for separable linear transformations over a central division algebra. A description of separable conjugacy classes of the multiplicative group A^\times of A is included.

1. INTRODUCTION

Consider a p -adic local field F (i.e. a finite field extension of \mathbb{Q}_p) and the connected reductive groups G and G' over F of multiplicative groups of the matrix algebra $\text{Mat}_n(F)$ and a central division algebra D over F of degree n . The local Jacquet-Langlands correspondence states that there is a one-to-one correspondence

$$E^2(G') \simeq E^2(G)$$

between the sets $E^2(G')$ and $E^2(G)$ of essentially square-integrable irreducible smooth representations of G' and G [1, p. 34]. The correspondence is characterized by the following character identity

$$(1.1) \quad \chi_{\pi'}(g') = (-1)^{n-1} \chi_\pi(g), \quad \forall \text{ conjugacy class } \{g\} \text{ corresponds to } \{g'\}$$

if the representation π corresponds to π' , where $\chi_{\pi'}$ (resp. χ_π) is the character of π' (resp. π), which is a locally constant central function defined at least on the dense open set $G'(F)^{\text{reg}}$ (resp. $G(F)^{\text{reg}}$) of regular semi-simple elements. The conjugacy class $\{g\}$ corresponding to the conjugacy class $\{g'\}$ means that they share the same characteristic polynomial. Clearly not every regular semi-simple conjugacy class in $G(F)$ corresponds to a class in $G'(F)$. Therefore, it is of interest to know which

Received March 26, 2012, accepted July 28, 2012.

Communicated by Wen-Ching Li.

2010 *Mathematics Subject Classification*: 11R52, 11R37, 15A21.

Key words and phrases: Characteristic polynomials, Central simple algebras, Rational canonical forms, Conjugacy classes.

characteristic polynomials of elements of $\mathrm{GL}_n(F)$ may be those of elements in D^\times . In this Note we consider the following basic question in full generality:

(Q) Let A be a finite-dimensional central simple algebra over an arbitrary field F . Which polynomials of degree $\deg(A)$ are the characteristic polynomials of elements in A ?

We recall some basic definitions for central simple algebras; see [5].

Definition 1. Let A be a (f.d.) central simple algebra over a field F .

(1) The *degree*, *capacity*, and *index* of A are defined as

$$\deg(A) := \sqrt{[A : F]}, \quad c(A) := n, \quad i(A) := \sqrt{[\Delta : F]},$$

respectively if $A \cong \mathrm{Mat}_n(\Delta)$, where Δ is a division algebra over F , which is uniquely determined by A up to isomorphism. The algebra Δ is also called the *division part* of A .

(2) For any element $x \in A = \mathrm{Mat}_n(\Delta)$, the *characteristic polynomial* of x is defined to be the characteristic polynomial of the image of x in $\mathrm{Mat}_{nd}(\bar{F})$ under a map

$$A \rightarrow A \otimes_F \bar{F} \xrightarrow{\rho} \mathrm{Mat}_{nd}(\bar{F}),$$

where \bar{F} is an algebraic closure of F and d is the degree of Δ . This polynomial is independent of the choice of the isomorphism ρ and it is defined over F . Denote by $f_x(t)$ the characteristic polynomial of x .

The question **(Q)** would become more interesting when one specializes F as a global field. When A is a quaternion algebra over a number field F , the answer is well-known. It is easier to treat the case when the polynomial $f(t) := t^2 + at + b$ factorizes in $F[t]$ (the answer is yes if and only if $f(t)$ has double roots or A splits). So we may consider the case when $f(t)$ is irreducible. Let K be a splitting field of $f(t)$, which is unique up to isomorphism. Then $f(t)$ is a characteristic polynomial of A if and only if there is an F -algebra embedding of K in A . Then one can check the latter condition easily by the local-global principle (cf. Prasad-Rapinchuk [4, Proposition A.1]) which asserts that this is equivalent to that whenever a place v of F ramified in A , the F_v -algebra $K_v := K \otimes_F F_v$ is a field, where F_v denotes the completion of F at the place v .

It is obvious that the question **(Q)** should land in the content of linear algebra when one realizes $A = \mathrm{Mat}_n(\Delta)$ as the algebra of Δ -linear transformations on the (right) Δ -vector space Δ^n . There are several books (for example the famous book by Jacobson [2]) on linear algebra that deal with vector spaces over division rings. However, we could not find one that deals with some core topics such as eigenvalues,

eigenspaces, Jordan canonical forms and rational canonical forms over central division algebras. As these are seemingly missing in the literature, we give an account for the theory of rational canonical forms over a (f.d.) central division F -algebra Δ . However, our theory is explicit only for *separable* linear transformations. We call a Δ -linear transformation x on a (f.d.) Δ -vector space V *separable* if any irreducible factor of its characteristic polynomial $f_x(t)$ is over F is a separable polynomial. The restriction of this separability assumption here is due to our argument which uses a theorem of Cohen (cf. [3, Theorem 60, p. 205]) where the separability assumption is needed.

The main result of this Note (Theorem 4) determines which polynomial is a characteristic polynomial. After that we give an explicit description of separable conjugacy classes of the multiplicative group A^\times (Theorem 9).

From now on, we fix a finite-dimensional central simple algebra A over an arbitrary ground field F . Let $A = \text{End}_\Delta(V)$, where Δ is the division part of A and V is a right vector space over Δ of dimension n . Put $d := \text{deg}(\Delta)$.

2. MINIMAL POLYNOMIALS

Let x be an element of A . The *minimal polynomial of x* is the unique monic polynomial $m_x(t) \in F[t]$ of least degree such that $m_x(x) = 0$ in A . Let $F[x] \subset A$ be the F -subalgebra generated by the element x . One has $F[x] = F[t]/(m_x(t))$ and V is an $(F[x], \Delta)$ -bimodule. Since $A = \text{End}_\Delta(V)$, the space V is a faithful $F[x]$ -module. When the ground division algebra Δ is equal to F , the theory of rational canonical forms is nothing but the classification theorem for faithful $F[x]$ -modules of F -dimension n . Therefore, the classification theorem for $F[x]$ -faithful $(F[x], \Delta)$ -bimodules of Δ -dimension n is exactly the theory of rational canonical forms over Δ .

Lemma 2.

- (1) *Let $p(t) \in F[t]$ be an irreducible polynomial of positive degree. Then $p(t) | m_x(t)$ if and only if $p(t) | f_x(t)$.*
- (2) *If $m_x(t)$ is an irreducible polynomial $p(t)$, then $f_x(t) = p(t)^a$, where $a := \text{deg}(A) / \text{deg } p(t)$.*

Proof. (1) This is a basic result in linear algebra when A is a matrix algebra over F . Suppose $p(t) | f_x(t)$. Let $\alpha \in \bar{F}$ be a root of $p(t)$. Since $A \otimes \bar{F}$ is a matrix algebra over \bar{F} , the basic result shows that $(t - \alpha) | f_x(t)$ in $\bar{F}[t]$ if and only if $(t - \alpha) | m_x(t)$ in $\bar{F}[t]$. Therefore, $(t - \alpha) | m_x(t)$ in $\bar{F}[t]$ and hence $p(t) | m_x(t)$ in $F[x]$.

(2) This follows from (1). ■

We write the minimal polynomial $m_x(t) = \prod_{i=1}^s p_i(t)^{e_i}$ into the product of irreducible polynomials, where $p_i(t) \in F[t]$ is a monic irreducible polynomial, $p_i \neq p_j$ if

$i \neq j$, and e_i is a positive integer. Put $F_i := F[t]/(p_i(t))$ and $\tilde{F}_i := F[t]/(p_i(t)^{e_i})$. By the Chinese Remainder Theorem, one has

$$(2.1) \quad F[x] \simeq \prod_{i=1}^s \tilde{F}_i.$$

Note that $F[x]$ is an Artinian ring. The decomposition (2.1) is nothing but the decomposition of $F[x]$ into the product of local Artinian rings. Since \tilde{F}_i is a local Artinian ring with residue field F_i , it is a complete local Noetherian F -algebra with residue field F_i . By Cohen's theorem [3, Theorem 60, p. 205], there is a ring monomorphism $s_i : F_i \rightarrow \tilde{F}_i$ such that $\pi \circ s_i = \text{id}_{F_i}$ for all i , where $\pi : \tilde{F}_i \rightarrow F_i$ is the natural projection. The cotangent space $\mathfrak{m}_{\tilde{F}_i} / \mathfrak{m}_{\tilde{F}_i}^2$ of \tilde{F}_i is of F -dimension $\deg p_i(t)$, and hence it is a one-dimensional F_i -vector space. Let $\varepsilon_i \in \tilde{F}_i$ be a generator of the maximal ideal $\mathfrak{m}_{\tilde{F}_i}$ of \tilde{F}_i , one yields $\tilde{F}_i = s_i(F_i)[\varepsilon_i]/(\varepsilon_i^{e_i})$.

3. RATIONAL CANONICAL FORMS

We now come to the $(F[x], \Delta)$ -bimodule structure on V , or equivalently, the (right) $\Delta \otimes_F F[x]$ -module structure on V . The decomposition (2.1) gives a decomposition of V into Δ -submodules V_i on which the F -algebra \tilde{F}_i acts faithfully:

$$(3.1) \quad V = \bigoplus_{i=1}^s V_i, \quad \dim_{\Delta} V_i =: n_i > 0, \quad \sum_{i=1}^s n_i = n.$$

We say an element y of A *separable* if its characteristic polynomial is the product of irreducible *separable* polynomials in $F[t]$. As $A = \text{End}_{\Delta}(V)$, a Δ -linear transformation on V is called *separable* if it is separable as an element in A . Assume that x is separable. Then one can choose s_i so that $F \subset s_i(F_i)$ by Cohen's theorem. Suppose that $\Delta \otimes_F s_i(F_i) = \text{Mat}_{c_i}(\Delta_i)$, where c_i (resp. Δ_i) is the capacity (resp. the division part) of the central simple algebra $\Delta \otimes_F s_i(F_i)$ over $s_i(F_i)$. Each V_i is a right $\Delta \otimes_F \tilde{F}_i$ -module. One has

$$\Delta \otimes_F \tilde{F}_i = [\Delta \otimes_F s_i(F_i)] \otimes_{s_i(F_i)} \tilde{F}_i = \text{Mat}_{c_i}(\tilde{\Delta}_i), \quad \tilde{\Delta}_i := \Delta_i \otimes_{s_i(F_i)} \tilde{F}_i = \Delta_i[\varepsilon_i]/(\varepsilon_i^{e_i}).$$

By the Morita equivalence, we have $V_i = W_i^{\oplus c_i}$, where each W_i is a $\tilde{\Delta}_i$ -module. Since $\Delta_i[\varepsilon_i]/(\varepsilon_i^{e_i})$ is a non-commutative PID, there is an isomorphism of $\tilde{\Delta}_i$ -modules

$$(3.2) \quad W_i \simeq \bigoplus_{j=1}^{t_i} \Delta_i[\varepsilon_i]/(\varepsilon_i^{m_j})$$

for some positive integers $1 \leq m_1 \leq \dots \leq m_{t_i} \leq e_i$. As \tilde{F}_i acts faithfully on W_i , one has $m_{t_i} = e_i$. The decomposition (3.1) is exactly the decomposition of V into

generalized eigenspaces in the classical case. Moreover, the decomposition (3.2) is exactly a decomposition of each generalized eigenspace into indecomposable invariant components. These give all information to make the rational canonical form for a suitable choice of basis as one does in linear algebra when $\Delta = F$ (so far our theory is explicit only for separable Δ -linear transformations). We leave the details to the reader.

Remark 3. One needs explicit information of Δ , F and F_i in order to compute the capacity c_i and the division part Δ_i of $\Delta \otimes_F s_i(F_i)$ (or of $\Delta \otimes_F F_i$). When F is a global field, these can be computed explicitly using Brauer groups over local fields [6] and the period-index relation [5, Theorem 32.19, p. 280]; see [7, Section 3] for details.

4. WHICH POLYNOMIAL IS CHARACTERISTIC?

Let $f(t) \in F[t]$ be a monic polynomial of degree nd . We will determine when $f(t) = f_x(t)$ for some element $x \in A$. We say that $f(t)$ is a *characteristic polynomial of A* if $f(t) = f_x(t)$ for some element $x \in A$. Our main result of this Note is the following:

Theorem 4. *Let $f(t) \in F[t]$ be a monic polynomial of degree nd and let $f(t) = \prod_{i=1}^s p_i(t)^{a_i}$ be the factorization into irreducible polynomials. Put $F_i := F[t]/(p_i(t))$. Then $f(t)$ is a characteristic polynomial of A if and only if for all $i = 1, \dots, s$, one has*

- (a) $a_i \deg p_i(t) = n_i d$ for some positive integer n_i , and
- (b) $[F_i : F] \mid n_i \cdot c(\Delta \otimes_F F_i)$.

Suppose $f(t) = f_x(t)$ for some $x \in A$. Then the minimal polynomial $m_x(t)$ of x is equal to $\prod_{i=1}^s p_i(t)^{e_i}$ for some positive integers e_i with $e_i \leq a_i$. Discussion in Section 3 shows that there is a decomposition of V into Δ -subspaces V_i say of Δ -dimension n_i on which the F -algebra \tilde{F}_i acts faithfully. Regarding the element $x \in A$ as a Δ -linear transformation $x : V \rightarrow V$ on V , let x_i be the restriction of the map x on the invariant subspace V_i . Then we have

$$(4.1) \quad f_{x_i}(t) = p_i(t)^{a_i}, \quad m_{x_i}(t) = p_i(t)^{e_i}, \quad \text{and} \quad a_i \deg(p_i(t)) = n_i d.$$

This shows the following proposition.

Proposition 5. *Let $f(t)$ be as in Theorem 4. Then $f(t)$ is a characteristic polynomial of A if and only if for all $i = 1, \dots, s$, one has $a_i \deg(p_i(t)) = n_i d$ for some $n_i \in \mathbb{N}$ and the polynomial $p_i(t)^{a_i}$ is a characteristic polynomial of $\text{Mat}_{n_i}(\Delta)$.*

Therefore, to prove Theorem 4 it suffices to consider the case where $f(t)$ is a power of an irreducible polynomial.

Lemma 6. *Let $p(t) \in F[t]$ be a monic irreducible polynomial and put $E := F[t]/(p(t))$. Then a polynomial $f(t)$ of the form $p(t)^a$ of degree nd is a characteristic polynomial of A if and only if there is an F -algebra embedding of E in A .*

Proof. Let \bar{t} be the image of t in E and suppose that there is an F -algebra embedding $\rho : E \rightarrow A$. Put $x := \rho(\bar{t})$. Then $m_x(t) = p(t)$ and $f_x(t) = p(t)^a$ by Lemma 2 (2). Conversely, suppose there is an element $x \in A$ such that $f(t) = f_x(t)$. Let

$$0 = V_0 \subset V_1 \subset \cdots \subset V_{l-1} \subset V_l = V$$

be a maximal chain of $F[x]$ -invariant Δ -subspaces. The minimal polynomial of x on each factor V_i/V_{i-1} is equal to $p(t)$. Choosing an Δ -linear isomorphism $\rho : \bigoplus_{i=1}^l V_i/V_{i-1} \simeq V$, we get an element $x^{ss} := \rho \circ x \circ \rho^{-1}$ (called a semi-simplification of x) in $\text{End}_\Delta(V)$ whose minimal polynomial is equal to $p(t)$. The map $\bar{t} \mapsto x^{ss}$ gives an F -embedding of E in A . ■

When F is a global field and the degree $[E : F] = \deg(A)$ is maximal, one can use the local-global principle to check the condition in Lemma 6 (cf. Prasad-Rapinchuk [4, Proposition A.1]). However, when the degree $[E : F]$ is not maximal, the local-global principle for embedding E in A over F fails in general; see constructions of counterexamples in [8, Section 4] and [7, Sections 4 and 5]. The following lemma provides an alternative method to check this condition.

Lemma 7. *Let E be as in Lemma 6. There is an F -algebra embedding of E in A if and only if $[E : F] \mid n \cdot c(\Delta \otimes_F E)$.*

Proof. This is a special case of [8, Theorem 2.9]. We provide a direct proof for the reader's convenience. Write $\Delta \otimes_F E = \text{Mat}_c(\Delta')$, where Δ' is the division part of the central simple algebra $\Delta \otimes_F E$ over E . An F -algebra embedding of E into $A = \text{Mat}_\Delta(V)$ exists if and only if V is an (E, Δ) -bimodule, or equivalently a right $E \otimes_F E = \text{Mat}_c(\Delta')$ -module. By the dimension counting, the vector space V is a $\text{Mat}_c(\Delta')$ -module if and only if

$$(4.2) \quad \frac{\dim_F V}{c[\Delta' : F]} \in \mathbb{N}.$$

Note that $[E : F][\Delta : F] = c^2[\Delta' : F]$. From this relation and that $\dim_F V = n[\Delta : F]$, the condition (4.2) can be written as $[E : F] \mid nc$. This proves the lemma. ■

By Proposition 5 and Lemmas 6 and 7, the proof of Theorem 4 is complete. ■

5. CONJUGACY CLASSES

Let $x \in A$ be an separable element as in Section 3. Suppose we have another element $x' \in A$ with the same characteristic polynomial $f_{x'}(t) = f_x(t) = \prod_{i=1}^s p_i(t)^{a_i}$

and same minimal polynomial $m_{x'}(t) = m_x(t) = \prod_{i=1}^s p_i(t)^{e_i}$. We may identify $F[x'] = F[t]/(m_x(t)) = F[x]$. The $(F[x'], \Delta)$ -bimodule structure on V gives a similar decomposition into Δ -submodules V'_i as (3.1)

$$(5.1) \quad V = \bigoplus_{i=1}^s V'_i, \quad \dim_{\Delta} V'_i =: n'_i > 0, \quad \sum_{i=1}^s n'_i = n.$$

Similarly, we also have $V'_i = (W'_i)^{\oplus c_i}$, where each W'_i is a $\tilde{\Delta}_i$ -module, and there is an isomorphism of $\tilde{\Delta}_i$ -modules

$$(5.2) \quad W'_i \simeq \bigoplus_{j=1}^{t'_i} \Delta_i[\varepsilon_i]/(\varepsilon_i^{m'_j}).$$

Note that $n_i = n'_i$ as $n_i d = a_i \deg p_i(t) = n'_i d$ (see (4.1)). The elements x and x' are conjugate by an element in A^\times if and only if the $(F[x], \Delta)$ -bimodule structure and $(F[x'], \Delta)$ -bimodule structure on V are equivalent. This is equivalent to that

$$(5.3) \quad t_i = t'_i, \quad \text{and} \quad (m_1, \dots, m_{t_i}) = (m'_1, \dots, m'_{t_i}), \quad \forall i = 1, \dots, s.$$

The tuple (m_1, \dots, m_{t_i}) is a partition of the integer $\dim_{\Delta_i}(W_i)$. This integer is given by the following proposition.

Proposition 8. *We have $\dim_{\Delta_i} W_i = n_i c_i / \deg p_i(t) = a_i / \deg(\Delta_i)$.*

Proof. Write $\Delta \otimes s_i(F_i) = \text{Mat}_{c_i}(\Delta_i) = \text{End}_{\Delta_i}(L_i)$ for a right Δ_i -vector space L_i . As $\Delta \subset \Delta \otimes_F s_i(F_i)$ and that L_i is a $\Delta \otimes s_i(F_i)$ -module, the vector space L_i is a Δ -module. It follows that $(\dim_F L_i) / [\Delta : F] \in \mathbb{N}$. Put $d_i = \deg(\Delta_i)$. We have $d = c_i d_i$ and (using $\dim_F L_i = c_i [\Delta_i : F]$)

$$(5.4) \quad c_i [\Delta_i : F] / [\Delta : F] = c_i d_i^2 \deg p_i / d^2 = \deg p_i / c_i \in \mathbb{N}.$$

Now we have

$$(5.5) \quad \dim_{\Delta_i} W_i = \frac{\dim_F V_i}{c_i [\Delta_i : F]} = \frac{[\Delta : F] \dim_{\Delta} V_i}{c_i [\Delta_i : F]} = \frac{n_i c_i}{\deg p_i} = \frac{d n_i c_i}{d \deg p_i} = \frac{a_i}{d_i}.$$

This proves the proposition. ■

Let S be the set of monic separable irreducible polynomials p of $F[t]$ with $p \neq t$. For each irreducible polynomial p in $F[t]$, let Δ_p be the division part of the central simple algebra $\Delta \otimes_F k(p)$ over $k(p)$, where $k(p)$ is the residue field at the prime (p) . A partition $\lambda = (\lambda_1, \dots, \lambda_t)$ is a finite sequence of non-decreasing positive integers, and we write $|\lambda| := \sum_{i=1}^t \lambda_i$. Put $|\lambda| = 0$ if $\lambda = \emptyset$.

Theorem 9. *The association from x to its characteristic polynomial $f_x(t)$ and the partitions of the integers $\dim_{\Delta_i} W_i$ by (3.2) induces a bijection between the set of separable conjugacy classes of the multiplicative group A^\times and the set of partition-valued functions λ on S such that*

$$(5.6) \quad \sum_{p \in S} \deg(p) |\lambda(p)| \deg(\Delta_p) = \deg(A).$$

Proof. We have shown the injectivity (see (5.3)). We show the surjectivity. Let p_1, \dots, p_s be those with $|\lambda(p_i)| \neq 0$. Let $d_i := \deg(\Delta_{p_i})$ and $a_i := |\lambda(p_i)| d_i$. We need to show that the conditions (a) and (b) of Theorem 4 for the polynomial $\prod_{i=1}^s p_i^{a_i}$ are satisfied. But these conditions are satisfied due to

$$n_i c_i / \deg p_i = a_i / d_i = |\lambda(p_i)| \in \mathbb{N}$$

and (see (5.4))

$$a_i \deg p_i / d = (a_i / d_i) (\deg p_i / c_i) \in \mathbb{N}.$$

This proves the theorem. ■

When $A = \Delta$ is a division algebra, any minimal polynomial of Δ is irreducible. The same proof presented here shows that the set of all conjugacy classes of A^\times is parametrized by monic irreducible polynomials $p \neq t$ such that $\deg p \cdot \deg(\Delta_p) = \deg(\Delta)$.

When $\text{char } F = 0$, for example if F is a number field, Theorem 9 gives a complete description of conjugacy classes of the multiplicative group A^\times .

Naturally one would like to look for a description of full conjugacy classes that generalizes Theorem 9. This seems to be a subtle problem. Because we know that the Jordan decomposition for elements in a linear algebraic group exists only over the perfect closure of the ground field F but not over the field F itself in general. Note that Theorem 9 may be rephrased as the existence of the Jordan decomposition of separable elements over the ground field F .

ACKNOWLEDGMENTS

The author was partially supported by the grants NSC 97-2115-M-001-015-MY3, 100-2628-M-001-006-MY4 and AS-98-CDA-M01. He is grateful to Ming-Chang Kang for his interest and helpful comments.

REFERENCES

1. P. Deligne, D. Kazhdan and M.-F. Vignéras, Représentations des algèbres centrales simples p -adiques, *Representations of reductive groups over a local field*, 33-117, Travaux en Cours, Hermann, Paris, 1984.

2. N. Jacobson, *Lectures in Abstract Algebra II. Linear Algebra*. GTM, **31**, Springer-Verlag, 280 pp.
3. H. Matsumura, *Commutative algebra*. Second edition. Mathematics Lecture Note Series, 56, Benjamin/Cummings Publishing, 1980, pp. 313.
4. G. Prasad and A. Rapinchuk, Computation of the metaplectic kernel, *Inst. Hautes Études Sci. Publ. Math.* **84** (1996), 91-187.
5. I. Reiner, *Maximal orders*, London Mathematical Society Monographs, No. **5**. Academic Press, London-New York, 1975, pp. 395.
6. J.-P. Serre, *Local fields*. GTM **67**, Springer-Verlag, 1979.
7. Sheng-Chi Shih, Tse-Chung Yang and C.-F. Yu, Embeddings of fields in simple algebras over global fields, arXiv:1108.0830.
8. C.-F. Yu, Embeddings of fields into simple algebras: generalizations and applications, *J. Algebra*, **368** (2012), 1-20.

Chia-Fu Yu
Institute of Mathematics
Academia Sinica and NCTS (Taipei Office)
Astronomy Mathematics Building
No. 1, Roosevelt Road Sec. 4
Taipei 10617, Taiwan
E-mail: chiafu@math.sinica.edu.tw