UNIQUENESS OF LINEAR PERIODS: THE CASE OF CENTRAL SIMPLE ALGEBRAS

HANG XUE

CONTENTS

1. The Theorem 1
2. The proof 2
References 7

1. The Theorem

The goal of this short note is to extend the uniqueness results of [Guo97, JR96] from the matrix algebras to the case of general central simple algebras. This is also the first step towards a conjecture Prasad and Takloo-Bighash [PTB11, Conjecture 1].

Let $F$ be a local nonarchimedean field, $E$ a quadratic field extension of $F$. Let $M$ be a central simple algebra over $F$ of degree $2n$ with a fixed embedding $E \to M$. Such an embedding is unique up to conjugation by the Noether–Skolem theorem. Let $R$ be the centralizer of $E$ in $A$. Let $G = M^\times$ and $H = R^\times$ be the group of invertible elements, viewed as algebraic groups over $F$.

Theorem 1.1. We have the following assertions.

1. $(G, H)$ is a Gelfand pair.
2. For any $g \in G$, we have $g^{-1} \in HgH$.

Standard argument shows that the second assertion implies the first one so we will only prove the second assertion. The argument is classical and follows largely that of [Guo97]. The only difference is that at various points, we need to do linear algebra over the division algebras which are noncommutative, so some care needs to be exercised.

The original motivation of this note is to obtain a systematic refinement and generalization of a conjecture of Guo and Jacquet [Guo96]. Suffices to say here is that this conjecture concerns the $GL_{n,E}$-period of an automorphic form on $GL_{2n,F}$. The conjecture in the case $n$ being odd is nice and clean while it is less satisfactory in the case of $n$ being even. In the proposed relative trace formula attack to this conjecture and in the search of suitable refinement in the case $n$ being even, we are led to the idea that instead of considering general linear groups only, one should consider all inner forms of the general linear groups. The local counterpart of the situation is the theorem above.
Acknowledgement. I thank W. Zhang for many helpful discussions. This work is partially supported by the AMS-Simons Travel Grant.

2. The proof

First we explain some structural results of $M$. Recall that there is an embedding $E \to M$.

**Lemma 2.1.** There is an element $\beta \in G$ and a positive integer $d_0$, such that $\beta^2 \in H$, $\beta^{2d_0} = \gamma \in F^\times$, $M = R \oplus R\beta$, conjugating by $\beta$ preserves $R$ and induces Galois conjugate on $E$.

**Proof.** Write $M = M_r(D)$ where $D$ is a division algebra over $F$ of rank $d$.

We distinguish two cases.

**Case 1:** $d$ is even.

In this situation, there is an embedding $E \to D$. There is a cyclic maximal subfield $L$ of $D$ containing $E$ and $D$ is isomorphic to a cyclic algebra:

$$D \simeq L \oplus L\beta \oplus \cdots \oplus L\beta^{d-1}, \quad \beta z = z^\sigma \beta, \quad z \in L, \quad \beta^d = \gamma \in F^\times,$$

where $\sigma$ is a generator of Gal($L/F$). Let $D_0$ be the centralizer of $E$, then $D_0 \simeq L \oplus L\beta^2 \oplus \cdots \oplus L\beta^{d-2}$. Thus $R \simeq M_r(D_0)$ and $M = M_r(D) = R \oplus R\beta$. Here in the last equality, $\beta$ is viewed as an element in $D$ embedded in $M_r(D)$ diagonally.

**Case 2:** $d$ is odd.

In this situation, there is no embedding $E \to D$ and $r$ is even. Choose a cyclic extension $L$ of $F$ in $D$ and write $D$ as a cyclic algebra:

$$D \simeq L \oplus L\beta_0 \oplus \cdots \oplus L\beta_0^{d-1}, \quad \beta_0 z = z^\tau \beta_0, \quad z \in L, \quad \beta_0^d = \gamma \in F^\times,$$

where $\tau$ is a generator of Gal($L/F$). Then $M = M_r(L) \oplus \cdots \oplus M_r(L)\beta_0^{d-1}$. Note that $r$ is even.

There is an embedding $E \to M_r(L)$ and $E$ embeds in $M$ via this embedding. Since $(L : F) = d$ is odd, $LE$ is again a cyclic field extension of $F$ of degree $2d$. We have that the centralizer of $E$ in $M_r(L)$ is isomorphic to $M_r/2(LE)$ and $M_r(L) = M_r/2(LE) \oplus M_r/2(LE)\theta$ where $\theta \in M_r(F)$ and $\theta^2 = 1$ and conjugating by $\theta$ is an automorphism of $M_r/2(LE)$. Note that $\theta$ and $\beta_0$ commute. So we have

$$M \simeq \bigoplus_{i=0,1}^{j=0,\ldots,d-1} M_{r/2}(LE)\theta^i\beta^j = M_{r/2}(LE) \oplus M_{r/2}(LE)\beta \oplus \cdots \oplus M_{r/2}(LE)\beta^{2d-1},$$

where $\beta = \theta\beta_0$. It is clear that $\beta^{2d} = \gamma \in F^\times$ and conjugating by $\beta$ induces Galois conjugate on $E$ since $\beta_0$ commutes with elements in $E$. \qed

From now on, we fix the following notation. Let $R = M_r(D)$ where $D$ is a division algebra over $E$ of degree $d$. We fix an element $\beta \in G$, such that $\beta^{2d} = \gamma \in F^\times$ and $M = R \oplus R\beta$ as in the above lemma. An element in $X \in M$ is then written as $A + B\beta$ with $A, B \in R$. For any $X \in R$, we put $X^\sigma = \beta X \beta^{-1}$. Note that conjugation by $\beta$ is an automorphism on $D$ and $\sigma$ acts on $R$ by
conjugation by $\beta$ on the entries of the matrices. So it indeed makes sense to talk about the action of $\sigma$ on matrices with entries in $D$ of any size.

Choose a $r \in F^x$ so that $E = F[\sqrt{r}]$ and put $\epsilon = \sqrt{r} \in R$. If $X = A + B\beta \in M$, then $\epsilon g \epsilon^{-1} = A - B\beta$. Thus $X \in R$ if and only if $\epsilon X \epsilon^{-1} = X$.

Let us put
\[
S = \{ g \in G \mid g \epsilon g \epsilon = \tau \} = \{ g \epsilon \epsilon^{-1} \mid g \in G \} \subset G.
\]

This is an algebraic variety over $F$. An element $g = A + B\beta \in G$ lies in $S$ if and only if
\[
A^2 = 1 + BB\beta^2, \quad AB = BA^\sigma.
\]

Indeed, it is straightforward to compute that
\[
geg \epsilon \tau = (A^2 - BB\beta^2 - (AB - BA^\sigma)\beta).
\]

The group $H$ acts on $S$ by conjugation. Define a morphism $\rho : G \to S$ by $\rho(g) = g \epsilon^{-1} \epsilon^{-1}$. Then $\rho$ induces an isomorphism of the $H$-varieties $H \setminus G$ and $S$.

In what follows, we are going to do linear algebra over $D$. We need to be careful as $D$ is not commutative. We always consider $D^r$ as an $r$ dimensional right $D$-module consisting of column vectors and matrix multiplication is from the left. With this understanding, $R \simeq \text{End}_D(D^r)$. We say that a matrix $g \in R$ is semisimple (resp. unipotent, resp. nilpotent) if it is so in $R(F)$ (under any fixed isomorphism $R(F) \simeq M_{rd}(F)$).

**Lemma 2.2.** Suppose that $g \in G$ and $\rho(g) = A + B\beta$ with $A^2 - 1$ being invertible. Then we have $g^{-1} \in HgH$.

**Proof.** Note that $1 + A$ and $1 + A^\sigma$ are invertible and $B(1 + A^\sigma)^{-1} = (1 + A)^{-1}B$. Also note that $B\beta$ and $A$ commute ($AB\beta = BA^\sigma\beta = B\beta A$). Put $C = (1 + A)^{-1}B$ and $g = 1 + C\beta$. Then
\[
1 - CC^\sigma \beta^2 = 1 - (1 + A)^{-1}B(1 + A^\sigma)^{-1}B^\sigma \beta^2 = 1 - (1 + A)^{-2}(A^2 - 1) = 2(1 + A)^{-1}.
\]

Thus $1 - CC^\sigma \beta^2$ is invertible. It follows that
\[
g^{-1} = 2^{-1}(1 - C\beta)(1 + A) = 2^{-1} \epsilon \epsilon^{-1}(1 + A) \in HgH.
\]

Moreover
\[
geg \epsilon \epsilon^{-1} = 2^{-1}(1 + CC^\sigma \beta^2)(1 + A) + C\beta(1 + A),
\]
and
\[
1 + CC^\sigma \beta^2 = 1 + (1 + A)^{-2}(A^2 - 1) = 2A(1 + A)^{-1}, \quad C\beta = (1 + A)^{-1}B\beta = B\beta(1 + A)^{-1}.
\]

Thus $\rho(g) = g \epsilon^{-1} \epsilon^{-1} = A + B\beta$. This proves the lemma. \qed

We now need to look at the “Lie algebra” of the symmetric space $S$. The Lie algebra of $G$ is $M$ and the “Lie algebra” $\mathfrak{s}$ of $S$ is $R\beta$ on which $H$ acts by conjugation. It is also identified with $R$ where $H$ acts by twisted conjugation, i.e. $X^h = h^{-1}Xh^\sigma$. We say that an element $X \in R$ is $\sigma$-semisimple (resp. $\sigma$-nilpotent) if $X\beta \in M$ is semisimple (resp. nilpotent).
Lemma 2.3. Let $g \in G$ and $\rho(g) = s = A + B\beta$. Suppose that $A$ is unipotent (as an element in $G$). Then $g^{-1} \in H g H$.

Proof. We claim that $s = A + B\beta \in S$ is unipotent if and only if $A$ is unipotent. Indeed, straightforward computation gives $(s-1)^2 = 2(A-1)s$. Note also that $A$ commutes with $B\beta$, so $A$ commutes with $s$. As $s \in S$ is invertible, our claim follows.

Next we consider the Lie algebras. We denote by $\mathfrak{n} \subset \mathfrak{g} = M$ the set of nilpotent elements and $\mathcal{N} \subset G$ the set of unipotent elements. Recall that the exponential map $\mathfrak{n} \to \mathcal{N}$ is a bijection. We claim that $\mathcal{N} \cap S$ is precisely the image of $\mathfrak{n} \cap \mathfrak{s}$ under the usual exponential map. Suppose that $s = \exp(X)$ is unipotent. Then $s\epsilon s\epsilon = \tau \in F^\times$. This is equivalent to $s\epsilon^{-1}s\epsilon = 1$ and moreover equivalent to $\exp(\epsilon^{-1}X\epsilon) = \exp(-X)$ which in turn equivalent to $-X = \epsilon^{-1}X\epsilon$, which means that $X \in R\beta$. Running this argument backwards gives the reverse direction.

Now choose $s = \exp(X)$ unipotent, namely $X \in \mathfrak{n} \cap \mathfrak{s}$. Then $\rho(s) = \exp(2X) = s^2 \in \mathcal{N} \cap S$. Assume that $g \in G$ and $\rho(g) = s$. Put $u = \exp(X/2)$, then $\rho(g) = \rho(u) = s$. Thus $g = hu$ for some $h \in H$. Thus

$$g^{-1} = u^{-1}h^{-1} = \exp(-X/2)h^{-1} = \epsilon u\epsilon^{-1}h = \epsilon h^{-1}g\epsilon^{-1}h \in H g H.$$

This proves the lemma. \qed

Lemma 2.4. Let $g \in G$ and $\rho(g) = s = A + B\beta$. Suppose that $-A$ is unipotent. Then $g^{-1} \in H g H$.

Proof. Suppose that $\rho(g) = s = A + B\beta$ and $-A$ is unipotent. Then $\rho(g\beta) = g\beta\epsilon\beta^{-1}g^{-1}\epsilon^{-1} = -s$. Thus by our previous discussion, we have that $g\beta = h\exp(X)$ for some $h \in H$ and $X \in \mathfrak{n} \cap \mathfrak{s}$. Thus

$$g = h \exp(X)\beta^{-1}, \quad g^{-1} = \beta \exp(-X)h^{-1}.$$

We want to show that $g^{-1} \in H g H$, which is equivalent to $\beta \exp(-X) \in H \exp(X)\beta^{-1}H$. Note that $\beta^2 \in H$, thus $g^{-1} \in H g H$ is equivalent to

$$\exp(-\beta X\beta^{-1}) \in H \exp(X)\beta^{-1}H\beta^{-1} = H \exp(X)H.$$

Therefore it is enough to prove the next lemma. \qed

Lemma 2.5. For any $X \in R$, there is an $h \in H$ such that $X^\sigma = h^{-1}Xh^\sigma$.

Proof. We proceed in several steps.

Step 1. If $X$ is $\sigma$-semisimple or equivalently $X\beta$ is semisimple, then there is an $h \in H$ such that $h^{-1}Xh^\sigma$ is of the form

$$\begin{pmatrix} B \\ 0 \end{pmatrix}$$

where $B$ is invertible and semisimple (as an element in $\text{GL}_m(D)$ for some $m$).
Indeed, under the stated assumption, we can find a \( g \in G \) and an invertible semisimple matrix \( \Lambda \in \text{GL}_s(D) \) \((s \leq r)\) such that

\[
X\beta = g^{-1} \begin{pmatrix} \Lambda \\ 0 \end{pmatrix} g, \quad X = g^{-1} \begin{pmatrix} \Lambda \\ 0 \end{pmatrix} g^{\beta^{-1}}.
\]

It follows that

\[
XX^\sigma \cdots X^\sigma^i = g^{-1} \begin{pmatrix} \Lambda^i+1 \\ 0 \end{pmatrix} g^{\beta^{-i-1}}.
\]

Since \( \Lambda \) is semisimple and invertible, all \( XX^\sigma \cdots X^\sigma^i \) have the same (right column) rank. Moreover \( N = XX^\sigma \cdots X^\sigma^{2d-1} \) is semisimple since \( \beta^{2d} = \gamma \in F^\times \).

Put \( V = D^\sigma \) \((right D\text{-module})\) and \( R \) acts on \( V \) by \( left \) multiplication. Let \( V_0 \) and \( V_1 \) be the kernel and the image of \( N \) respectively. As \( N \) is semisimple (as an element of \( R \)) we have \( V = \text{Ker} N \oplus \text{Im} N \). It follows from the above discussion that \( \text{Ker} N = X^{\sigma^d-1} \) and \( \text{Im} N = X \). Put \( V_0 = \text{Ker} X \) and \( V_1 = \text{Im} X \). Then \( X^{\sigma^d-1} = V_0^{\sigma^{-1}} \) and

\[
V = V_0^{\sigma^{-1}} \oplus V_1 = V_0 \oplus V_1^\sigma.
\]

Let \( \{v_1, \ldots, v_d\} \) \((\text{resp. } \{v_{d+1}, \ldots, v_r\})\) a basis of \( V_0 \) \((\text{resp. } V_1^\sigma)\). Then form the matrices

\[
h = (v_1, \ldots, v_d, v_{d+1}, \ldots, v_r), \quad g = h^{-\sigma^{-1}}.
\]

We then have that

\[
g^\sigma(v_1, \ldots, v_r) = g(v_1^{\sigma^{-1}}, \ldots, v_r^{\sigma^{-1}}).
\]

This means in particular that \( g^\sigma V_0 = (g^\sigma V_0)^{\sigma^{-1}}, g^\sigma V_1^\sigma = gV_1 \), i.e. \( g^\sigma V_0 \) and \( gV_1 \) are both \( \sigma \) invariant. We may choose bases of them respectively, say \( w_1, \ldots, w_d \) and \( w_{d+1}, \ldots, w_r \) that are \( \sigma \) invariant.

Consider \( Y = gXg^{-\sigma} \). We \( \text{Ker} Y = g^\sigma V_0 \) and \( \text{Im} Y = gV_1 \). The same argument as for \( X \) shows that \( V = g^\sigma V_0 \oplus g^\sigma V_1^\sigma = g^\sigma V_0 \oplus gV_1 \). The second inequality makes uses of the fact that \( gV_1 \) is \( \sigma \) invariant. Form the matrix

\[
h = (w_1, \ldots, w_r).
\]

Then \( h \) is \( \sigma \) invariant and

\[
h^{-1} Y h = \begin{pmatrix} B \\ 0 \end{pmatrix}.
\]

where \( B \) is semisimple and invertible. This finishes the first step.

**Step 2.** If \( X \) is \( \sigma \)-nilpotent, then there is an \( h \in H \) such that \( h^{-1} X h^\sigma \) is the Jordan canonical form. Here by the Jordan canonical form, we mean the diagonal blocked matrices (with entries in
where $B$ is semisimple and invertible. Then write $X'_n = \begin{pmatrix} X_1 & X_0 \\ X'_0 & X_2 \end{pmatrix}$ according to the block size of $X'_n$. Then we have $X_0 = 0$, $X'_0 = 0$ and $X_1 B \beta = B \beta X_1 \beta$. The last quality is equivalent to $X_1 B^\sigma = B X_1^\sigma$, i.e. $B^{-1} X_1 B^\sigma = X_1^\sigma$. It is easy to see that $X_2^\sigma$ is $\sigma$-nilpotent. So there is an $h$ such that $h^{-1} X_2 h^\sigma$ is in Jordan canonical form. Therefore $h^{-1} X_2 h^\sigma = h^{-\sigma} X_2^\sigma h^{\sigma^2}$. So $X_2^\sigma = (hh^{-\sigma})^{-1} X_2 (hh^{-\sigma})^\sigma$. We then have

$$\begin{pmatrix} B^\sigma + X_1^\sigma \\ X_2^\sigma \end{pmatrix} = \begin{pmatrix} B \\ hh^{-\sigma} \end{pmatrix}^{-1} \begin{pmatrix} B + X_1 \\ X_2 \end{pmatrix} \begin{pmatrix} B \\ hh^{-\sigma} \end{pmatrix}^\sigma.$$ 

This proves the lemma. \[\square\]

**Proof of Theorem 1.1.** Let $s = A + B \beta \in S$ with $A, B \in R$. First we observe that there is an $h \in H$ and $A_i \in M_{r_i}(D)$ where $r = r_1 + r_2 + r_3$,

$$A = h^{-1} \begin{pmatrix} A_1 & & \\ & A_2 \\ & & A_3 \end{pmatrix} h,$$

and $A_i^2 - 1$ is invertible, $A_2$ and $-A_3$ are unipotent. Indeed, we put $V_1 = \text{Im}(A^2 - 1)^r$, $V_2 = \text{Ker}(A - 1)^r$, $V_3 = \text{Ker}(A + 1)^r$. They are invariant under left multiplication by $A$ and $V = V_1 \oplus V_2 \oplus V_3$. Routine linear algebra arguments give what we want. We now write $h B h^{\sigma^{-1}}$ as block matrices as that of $h A h^{-1}$, say $h B h^{\sigma^{-1}} = (B_{ij})$ where $B_{ij} \in M_{r_i \times r_j}(D)$. The fact that $s \in S$ implies that $AB = BA^\sigma$ and this is equivalent to that $A_i B_{ij} = B_{ij} A_i^\sigma$. We conclude that $B_{ij} = 0$ if $i \neq j$. Indeed, we may consider $A_i B_{ij} = B_{ij} A_i^\sigma$ as an identity in $R(\overline{F})$ and fix an identification $R(\overline{F}) \simeq M_{rd}(\overline{F})$. It then follows that $B_{ij} = 0$ since the image of $A_i$ and $A_i^\sigma$ in $M_{rd}(\overline{F})$ have no
eigenvalue in common. In conclusion, we have shown that up to conjugation by elements in $H$, any element in $S$ can be written as

$$\begin{pmatrix} A_1 \\ A_2 \\ A_3 \end{pmatrix} + \begin{pmatrix} B_1 \\ B_2 \\ B_3 \end{pmatrix} \beta.$$ 

It is also easy to check that $A_i + B_i \beta$ satisfies analogous condition as that of $A + B \beta$, i.e.

$$A_i^2 = 1 + B_i B_i^\sigma \beta^2, \quad A_i B_i = B_i A_i^\sigma.$$ 

Now Theorem 1.1 follows from Lemma 2.2, Lemma 2.3 and Lemma 2.4. \qed

REFERENCES


