MORE ON EMBEDDINGS OF LOCAL FIELDS IN SIMPLE ALGEBRAS

Ernst Wilhelm Zink

Reine Mathematik
Humboldt Universität
Unter den Linden 6
10099 Berlin

Germany

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn

Germany

MPI 96-155

MORE ON EMBEDDINGS OF LOCAL FIELDS IN SIMPLE ALGEBRAS

ERNST-WILHELM ZINK

Let $A|F$ be a central simple algebra over a p-field F of arbitrary characteristic. Then concretely A may be represented as a complete $m \times m$ matrix algebra $A = M_m(D_d)$, where $D_d = D$ denotes a central division algebra of index d over F. Thus the reduced degree of A over F is $N = dm$.[1]

We write $\mathfrak{o}_F$, respectively $\mathfrak{O}_D$, for the ring of integers of F, respectively D, and $\mathfrak{P}_F = \pi_F \mathfrak{o}_F$, respectively $\mathfrak{P}_D = \pi_D \mathfrak{O}_D$, for the maximal ideals of $\mathfrak{o}_F$, respectively $\mathfrak{O}_D$. We write k_F, respectively k_D, for the residual fields of F and D.

An $\mathfrak{o}_F$ *order* of A is any subring of A containing the identity element of A which is also a finitely generated $\mathfrak{o}_F$ submodule of A containing an F basis for A. Let $\mathfrak{A}$ denote an $\mathfrak{o}_F$ order of A. We call $\mathfrak{A}$ *hereditary* [R, p. 27] if every left ideal of $\mathfrak{A}$ is a projective left $\mathfrak{A}$ module. The order $\mathfrak{A}$ has a Jacobson radical $\mathfrak{P}_\mathfrak{A}$ [R, p. 77ff]; it is the minimal (two-sided) ideal of $\mathfrak{A}$ such that the quotient ring $\mathfrak{A}/\mathfrak{P}_\mathfrak{A}$ is semi-simple. If $\mathfrak{A}$ is hereditary, then $\mathfrak{A}/\mathfrak{P}_\mathfrak{A}$ is a direct product of complete matrix algebras with entries in k_D, and $\pi_F\mathfrak{A} = \mathfrak{P}_\mathfrak{A}^{rd}$ with a positive integer r, called the *period* of $\mathfrak{A}$.

Following Benz [B], Bushnell/Fröhlich [BF], and Fröhlich [F] we call $\mathfrak{A}$ *principal* if $\mathfrak{P}_\mathfrak{A}$ is a principal two-sided ideal of $\mathfrak{A}$, i. e. if there exists $t_\mathfrak{A} \in \mathfrak{A}$ such that $\mathfrak{P}_\mathfrak{A} = t_\mathfrak{A} \cdot \mathfrak{A} = \mathfrak{A} \cdot t_\mathfrak{A}$. If $\mathfrak{A}$ is principal, then $\mathfrak{A}$ is hereditary; more specifically, $\mathfrak{A}$ is principal if and only if the period r of $\mathfrak{A}$ divides m and $\mathfrak{A}/\mathfrak{P}_\mathfrak{A} \cong [M_s(k_D)]^r$, where $rs = m$.

The period of a principal order $\mathfrak{A}$ determines $\mathfrak{A}$ up to conjugacy. If $\mathfrak{A}$ is principal with period r, then $\mathfrak{A}$ is conjugate to the *standard* principal order $\mathfrak{A}_r \subset M_r(M_s(\mathfrak{O}_D))$ such that the $r \times r$ matrix $g = (g_{ij})$ belongs to $\mathfrak{A}_r$ if and only if $g_{ij} \in M_s(\mathfrak{P}_D)$ for $i > j$. Thus the set of standard principal orders $\mathfrak{A}_r$ of A and, hence the set of conjugacy classes of principal orders of A, corresponds bijectively to the set of factors r of m.

For $\mathfrak{A}$ principal write

$$\mathfrak{K} = \mathfrak{K}(\mathfrak{A}) = \{x \in A^\times \, : \, x\mathfrak{A}x^{-1} = \mathfrak{A}\}$$

for the normalizer of $\mathfrak{A}$. Then $\mathfrak{K}$ is concretely the semi-direct product

$$\mathfrak{K} = \langle t_\mathfrak{A} \rangle \ltimes \mathfrak{A}^\times,$$

where $t_\mathfrak{A}$, as before, is a generator of the Jacobson radical $\mathfrak{P}$ of $\mathfrak{A}$.

[1] We write $R^\times$ for the group of units of any (unital) subring R of A and (u, v) to denote the greatest common divisor of any pair of positive integers u, v.

Every maximal compact subgroup of $A^\times/F^\times$ is conjugate to $\mathfrak{K}(\mathfrak{A}_r)/F^\times$ for some factor r of m [BF, (1.3.2)(v)]. Every compact subgroup of $A^\times/F^\times$ is contained in some maximal compact subgroup of $A^\times/F^\times$.

Fix a maximal extension field $L|F$ of F contained in A. In other words, assume that $F \subset L \subset A$ and that $[L:F] = N$. Write e for the ramification exponent and f for the inertial degree of $L|F$; then $N = ef$ too. In this context H. Benz [B, p. 31, see the second paragraph] and A. Fröhlich [F, Theorem 1][2] have proved:

0. Theorem. *There is one and only one principal order $\mathfrak{A}$ such that $L^\times \subset \mathfrak{K}(\mathfrak{A})$. The period of the order $\mathfrak{A}$ is*

$$r(\mathfrak{A}) = \frac{m}{(f,m)} = \frac{e}{(d,e)}.$$

Thus, $m = r(\mathfrak{A})s(\mathfrak{A})$, where $s(\mathfrak{A}) = (f,m)$.

Notation. *For any maximal subfield $L|F$ of A we write $\mathfrak{A}_{L|F}$ for the unique principal order the normalizer of which contains L; we also write $\mathfrak{K}_{L|F} = \mathfrak{K}(\mathfrak{A}_{L|F})$.*

The purpose of this paper is first to derive some consequences of this important theorem of Benz and Fröhlich and second to generalize the concept of "pure element" – introduced by Bushnell and Kutzko in the split case – to all central simple algebras. I would like to thank A.J.Silberger for reading the manuscript and making several improvements.

First we prove a technical result to be used later.

Notation. *For $E|F$ any subfield of A we write $n = n_E = [E:F]$ and $N_E = N/n_E$.*

1. Proposition. *Let $E|F$ be a subfield of A and let A_E denote the centralizer of E in A. Then $A_E|E$ is a central simple algebra which is isomorphic to a matrix algebra $M_{m'}(D')$, where $D'|E$ is a central division algebra of index $d' = d/(d,n)$ and $m' = (m, N_E)$.*

Remark. The equality $nN_E = dm$ $(= N)$ implies that $N_E/(m,N_E) = d/(d,n)$, i. e. that $d'm' = N_E$.

Proof. Since $A_E \otimes_E M_n(E)$ and $A \otimes_F E$ are isomorphic as central simple E–algebras (see, for instance, [K, 8.5]), the algebras A_E and $A \otimes_F E$ belong to the same Brauer class

$$[A_E] = [A \otimes_F E] \in \mathrm{Br}(E).$$

This class is the image of $[A] \in \mathrm{Br}(F)$ under the natural map (extension of scalars) $\mathrm{Br}(F) \to \mathrm{Br}(E)$. From local class field theory [S, chap. XIII, Prop. 7] we know that these Brauer groups are canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$, the isomorphism being given by the "invariant map". Since the diagram

$$\begin{array}{ccc} \mathrm{Br}(F) & \longrightarrow & \mathrm{Br}(E) \\ {\scriptstyle \mathrm{inv}}\downarrow & & {\scriptstyle \mathrm{inv}}\downarrow \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\;n\;} & \mathbb{Q}/\mathbb{Z} \end{array}$$

[2] Both [BF] and [F] restrict their treatment to the case of characteristic zero, but their results, at least so far as they concern the questions dealt with here, do not depend upon the characteristic zero assumption. Benz's results have a more general formulation. We follow Fröhlich's treatment more closely, as it is better focused toward our own goals.

is commutative, it follows that $\mathrm{inv}(A_E) = n \cdot \mathrm{inv}(A)$. Moreover, since $A_E = M_{m'}(D')$, where $D'|E$ is central,

$$\sqrt{[D' : E]} = \mathrm{index}(D'|E) = \mathrm{denom}(\mathrm{inv} D')\,;$$

in other words, the reduced degree of $D'|E$ is the denominator of the invariant $\mathrm{inv}(D') \in \mathrm{Br}(E)$. On the other hand,

$$\mathrm{inv}(D') = \mathrm{inv}(A_E) = \mathrm{inv}(A) \cdot n = \frac{a}{d} \cdot n,$$

where $(a, d) = 1$, so

$$\mathrm{denom}(\frac{a}{d} \cdot n) = \frac{d}{(d, n)} = d'. \quad \square$$

Let $E|F$ be a field such that $F \subseteq E \subseteq L$. Then $L|E$ is a maximal subfield of $A_E|E$ too, so it lies in the normalizer

$$\mathfrak{K}_{L|E} = \mathfrak{K}(\mathfrak{A}_{L|E}) = \{x \in A_E^\times\,;\, x\mathfrak{A}_{L|E}x^{-1} = \mathfrak{A}_{L|E}\}$$

of a unique principal order $\mathfrak{A}_{L|E} \subset A_E$.

2. Theorem. *Assume $F \subseteq E \subseteq L \subset A$ as above. Then:*

(i) $\mathfrak{A}_{L|F} \cap A_E = \mathfrak{A}_{L|E}$.

(ii) $\mathfrak{K}_{L|F} \cap A_E = \mathfrak{K}_{L|E}$.

(iii) *Let $\mathfrak{P}_{L|F}$ and $\mathfrak{P}_{L|E}$ be the Jacobson radicals of $\mathfrak{A}_{L|F}$ and $\mathfrak{A}_{L|E}$, let*

$$\nu_0 = \nu_0(\mathfrak{P}_{L|F}|\mathfrak{P}_{L|E}) := (f_{E|F}, \frac{f}{s(\mathfrak{A}_{L|F})}),$$

and, for $i \in \mathbb{Z}$, set $(i/\nu_0)+ = \lfloor (i + \nu_0 - 1)/\nu_0 \rfloor$, the smallest integer which is at least as large as i/ν_0. Then, for all $i \in \mathbb{Z}$,

$$\mathfrak{P}^i_{L|F} \cap A_E = \mathfrak{P}^{(i/\nu_0)+}_{L|E}.$$

(iv) *Let $\nu_{\mathfrak{P}}$ denote the exponent of $\mathfrak{K}_{L|F}$ corresponding to $\mathfrak{P} = \mathfrak{P}_{L|F}$ and let $t_{L|E}$ be a generator of the principal ideal $\mathfrak{P}_{L|E}$ of $\mathfrak{A}_{L|E}$. Then $\nu_0 = \nu_{\mathfrak{P}}(t_{L|E})$.*

Remark. In the split case, i. e. $m = N$ and $D = F$, we find that $\nu_0 = 1$; in the division algebra case, i. e. $m = 1$ and $D = A$, we obtain $\nu_0 = f_{E|F}$.

Proof. We shall prove Theorem 2 via a sequence of eight lemmas. For the whole proof we shall employ the notations $\mathfrak{A} = \mathfrak{A}_{L|F}$, $\mathfrak{P} = \mathfrak{P}_{L|F}$, and $\mathfrak{K} = \mathfrak{K}_{L|F}$. We also write $\nu = \nu_{\mathfrak{P}}$ for the exponent on $\mathfrak{K}$ associated to $\mathfrak{P}$.

Lemma 1. *$\mathfrak{A} \cap A_E$ is an $\mathfrak{o}_F$ order in the F algebra A_E and an $\mathfrak{o}_E$ order in the E algebra A_E.*

Proof. Clearly, $\mathfrak{A} \cap A_E$ is an $\mathfrak{o}_F$ submodule of A_E and a ring containing the identity element of A_E. We must show that $\mathfrak{A} \cap A_E$ contains a basis for the F vector space A_E and that it is finitely generated as an $\mathfrak{o}_F$ module. Since $\mathfrak{A}$ is an $\mathfrak{o}_F$ order in A, we may choose an F vector space basis for A which is comprised of elements of $\mathfrak{A}$. Since any element of A_E may be expressed as a linear combination of these basis elements with coefficients in F, it follows that some $\mathfrak{o}_F$ multiple of any element of A_E lies in $\mathfrak{A}$, thus in $\mathfrak{A} \cap A_E$. This means that $\mathfrak{A} \cap A_E$ contains a generating set, and therefore also a basis, for A_E as a vector space over F. Moreover, since $\mathfrak{A} \cap A_E$ is an $\mathfrak{o}_F$ submodule of the $\mathfrak{o}_F$ order $\mathfrak{A}$ and since $\mathfrak{o}_F$ is a principal ideal ring, $\mathfrak{A} \cap A_E$ is a finitely generated $\mathfrak{o}_F$ module. This proves that $\mathfrak{A} \cap A_E$ is an $\mathfrak{o}_F$ order in the F algebra A_E. Clearly, A_E is also an E algebra and, since $E \subseteq L$, it is clear that $\mathfrak{A}$ and hence $\mathfrak{A} \cap A_E$ is an $\mathfrak{o}_E$ module. Being finitely generated as an $\mathfrak{o}_F$ module, $\mathfrak{A} \cap A_E$ is also finitely generated as an $\mathfrak{o}_E$ module. This implies that $\mathfrak{A} \cap A_E$ is an $\mathfrak{o}_E$ order too. $\square$

Lemma 2. $\mathfrak{K} \cap A_E = \mathfrak{K}_{L|E}$.

Proof. By Theorem 0 $L^\times \subset \mathfrak{K}_{L|E}$, where $\mathfrak{K}_{L|E}$ is maximal compact modulo center in $A_E^\times$. From the exact sequence

$$E^\times/F^\times \hookrightarrow \mathfrak{K}_{L|E}/F^\times \twoheadrightarrow \mathfrak{K}_{L|E}/E^\times$$

it follows that $\mathfrak{K}_{L|E}$ is compact mod center in $A^\times$ too. Thus,

$$L^\times \subset \mathfrak{K}_{L|E} \subset \tilde{\mathfrak{K}},$$

where $\tilde{\mathfrak{K}}$ is some maximal compact modulo center subgroup of $A^\times$. By [BF, Remark following (1.5.4)] it follows that $\tilde{\mathfrak{K}} = \mathfrak{K}(\tilde{\mathfrak{A}})$ for some principal order $\tilde{\mathfrak{A}}$; from Theorem 0 we may conclude that $\tilde{\mathfrak{A}} = \mathfrak{A}$, $\tilde{\mathfrak{K}} = \mathfrak{K}$, and therefore

$$\mathfrak{K}_{L|E} \subseteq \mathfrak{K} \cap A_E.$$

On the other hand, $(\mathfrak{K} \cap A_E)/F^\times \subseteq \mathfrak{K}/F^\times$ and $\mathfrak{K}/F^\times$ is compact, so the quotient group $(\mathfrak{K} \cap A_E)/E^\times$ is compact too. Therefore, since $\mathfrak{K} \cap A_E$ is a compact modulo center subgroup of $A_E^\times$ and $\mathfrak{K}_{L|E} = \mathfrak{K}(\mathfrak{A}_{L|E})$ is maximal compact mod center in $A_E^\times$, the inclusion mapping $\mathfrak{K}_{L|E} \subseteq \mathfrak{K} \cap A_E$ is a surjection. $\square$

Lemma 3. $\mathfrak{A}^\times \cap A_E = \mathfrak{A}_{L|E}^\times$.

Proof. For any principal order in A or A_E the group of units is the maximal compact subgroup of its normalizer. Thus Lemma 2 implies that, to prove Lemma 3, it is sufficient to show that $\mathfrak{A}^\times \cap A_E$ is maximal compact in $\mathfrak{K} \cap A_E$. However, this follows from the existence of the inclusion mapping

$$\mathfrak{K} \cap A_E/\mathfrak{A}^\times \cap A_E \hookrightarrow \mathfrak{K}/\mathfrak{A}^\times \cong \mathbb{Z},$$

since all subgroups of $\mathbb{Z}$ are infinite cyclic. $\square$

Lemma 4. $\mathfrak{A}^\times \cap A_E = (\mathfrak{A} \cap A_E)^\times$.

Proof. The inclusion $\supseteq$ is obvious. Conversely let be $a \in \mathfrak{A}^\times \cap A_E$. There exists $b \in \mathfrak{A}$ such that $ab = 1$ in A. Now because a commutes with all elements from E we conclude the same for $b = a^{-1}$. Hence $b \in \mathfrak{A} \cap A_E$ such that $a \in (\mathfrak{A} \cap A_E)^\times$. $\square$

Lemma 5. $\mathfrak{A} \cap A_E = \mathfrak{A}_{L|E}$.

Proof. It follows from Lemmas 3 and 4 that $(\mathfrak{A} \cap A_E)^\times = \mathfrak{A}_{L|E}^\times$. We know that $\mathfrak{A}_{L|E}$ is an $\mathfrak{o}_E$ order in A_E and, by Lemma 1, so is $\mathfrak{A} \cap A_E$. Applying [BF, (1.1.1)] with A_E in place of A, we find that, since $(\mathfrak{A} \cap A_E)^\times = \mathfrak{A}_{L|E}^\times$, the orders $\mathfrak{A} \cap A_E$ and $\mathfrak{A}_{L|E}$ have the same Jacobson radical $\mathfrak{P}_{L|E}$. Since $\mathfrak{A}_{L|E}$ is principal,

$$\mathfrak{A}_{L|E} = \{x \in A_E \,;\, \mathfrak{P}_{L|E} \cdot x \subseteq \mathfrak{P}_{L|E}\}.$$

Hence, inasmuch as $\mathfrak{P}_{L|E}$ is the Jacobson radical of $\mathfrak{A} \cap A_E$, we have the inclusion $\mathfrak{A} \cap A_E \subseteq \mathfrak{A}_{L|E}$. Let $\mathfrak{B}$ be the $\mathfrak{o}_E$ order in A_E which is spanned by $\mathfrak{A}_{L|E}^\times = (\mathfrak{A} \cap A_E)^\times$. Then

$$\mathfrak{B} \subseteq \mathfrak{A} \cap A_E \subseteq \mathfrak{A}_{L|E}\,.$$

If the second inclusion is proper, $\mathfrak{B} \neq \mathfrak{A}_{L|E}$ and, by [BF, (1.1.1)], $\mathfrak{A}_{L|E}/\mathfrak{P}_{L|E}$ has a direct factor isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$. But $\mathfrak{A}_{L|E}$ is a principal order in A_E and $A_E \cong M_{m'}(D')$, so, using the notation introduced in Proposition 1, we have

$$\mathfrak{A}_{L|E}/\mathfrak{P}_{L|E} \cong \left[M_{s'}(k_{D'})\right]^{r'},$$

a direct product of r' matrix algebras over the residual field $k_{D'}$, where $r's' = m'$. Therefore [BF, (1,1,1)] implies that, for a proper inclusion $\mathfrak{A} \cap A_E \subsetneq \mathfrak{A}_{L|E}$, we must have $s' = 1$, $r' = m' \geq 2$, and $k_{D'} = \mathbb{F}_2$. Since $[k_{D'} : k_E] = d'$, it follows that $D' = E$, $d' = 1$, $m' = N_E$, and $A_E \cong M_{N_E}(E)$. Applying Theorem 0 to the split algebra A_E, we find that

$$r' = r(\mathfrak{A}_{L|E}) = e_{L|E} = m' = N_E,$$

which implies that $L|E$ is a fully ramified extension. However, since $k_E = \mathbb{F}_2$, the field extension $E|F$ is also fully ramified. Hence the maximal extension $L|F$ is fully ramified with $k_L = \mathbb{F}_2$. It suffices to show that $\mathfrak{A} \cap A_E$ is a principal order in order to show that $\mathfrak{A} \cap A_E = \mathfrak{A}_{L|E}$, because principal orders are uniquely determined by their Jacobson radicals and we already know that $\mathfrak{A} \cap A_E$ and $\mathfrak{A}_{L|E}$ have the same Jacobson radicals. In the case that $k_L = \mathbb{F}_2$ we may argue as in [F, (7.9)ff][3] to prove that $\mathfrak{A} \cap A_E$ is a principal order. To give Fröhlich's argument let us first recall that the field F is a p-field with residual field $\mathbb{F}_2$ and that $L \supset E \supset F$ is a tower of fully ramified extension fields. Taking $\alpha \in L$ such that $\alpha\mathfrak{o}_L = \mathfrak{P}_L$, we see that α is also a prime element of $\mathfrak{A}$, since $\mathrm{ord}_F(\alpha) = 1/N$. Since $\alpha \in L$, an overfield of E, we have $\alpha \in A_E \cap \mathfrak{A}$. Since $\mathfrak{A}$ is principal, every element $y \in A_E \cap \mathfrak{P}_{\mathfrak{A}}$ may be expressed as $y = \alpha x$ with $x \in \mathfrak{A}$. Since $y \in A_E$ and $\alpha^{-1} \in A_E$, it follows that $x \in \mathfrak{A} \cap A_E$; therefore, $\alpha^{-1}(\mathfrak{P}_{\mathfrak{A}} \cap A_E) = \mathfrak{A} \cap A_E$, i. e. $\mathfrak{A} \cap A_E$ is the set of all elements $x \in A_E$ such that $\alpha x \in \mathfrak{P}_{\mathfrak{A}} \cap A_E$, so $\mathfrak{A} \cap A_E$ is principal. We have proved that a proper inclusion $\mathfrak{A} \cap A_E \subsetneq \mathfrak{A}_{L|E}$ is impossible. $\square$

[3] The letters L and E interchange their meaning in Fröhlich's use of notation.

Lemma 6. *$\mathfrak{P}^i \cap A_E$ is a power of $\mathfrak{P}_{L|E}$ for all $i \in \mathbb{Z}$.*

Proof. Since $\mathfrak{A}_{L|E}$ is a principal order, it follows from [BF, Remark following (1.3.2)] that it is enough to show that $\mathfrak{P}^i \cap A_E$ is a fractional ideal in A_E with respect to $\mathfrak{A} \cap A_E = \mathfrak{A}_{L|E}$ which is normalized by $\mathfrak{K}_{L|E}$. By imitating the argument given in Lemma 1 for $\mathfrak{A} \cap A_E$ the reader can check that $\mathfrak{P}^i \cap A_E$ is an $\mathfrak{o}_E$ lattice in A_E. Moreover, $\mathfrak{P}^i$ being a fractional ideal of $\mathfrak{A}$, we see that $\mathfrak{P}^i \cap A_E$ is a fractional ideal of $\mathfrak{A} \cap A_E$. More precisely, since $\mathfrak{P}^i$ is an $\mathfrak{A}$ module, $(\mathfrak{A} \cap A_E)(\mathfrak{P}^i \cap A_E) \subseteq \mathfrak{P}^i \cap A_E$ and the other inclusion is even more obvious (see [BF, the definition following (1.1.3)].). Finally $\mathfrak{P}^i \cap A_E$ is $\mathfrak{K}_{L|E}$-invariant because $\mathfrak{K}_{L|E} = \mathfrak{K} \cap A_E$. □

Lemma 7. *Let $t = t_{L|E}$ be a generator of the principal ideal $\mathfrak{P}_{L|E}$ in $\mathfrak{A}_{L|E}$. Then $\mathfrak{P}^i \cap A_E = \mathfrak{P}^{(i/\nu_0)+}$, where $\nu_0 = \nu(t)$.*

Proof. By Lemma 6, $\mathfrak{P}^i \cap A_E = \mathfrak{P}^j_{L|E}$ for some $j \in \mathbb{Z}$. Clearly, $\mathfrak{P}^j_{L|E}$ is generated by t^j. Since $t \in \mathfrak{K}_{L|E} = \mathfrak{K} \cap A_E \subset \mathfrak{K}$, we have $\nu(t^j) = j\nu(t) = j\nu_0$, where $\mathfrak{P}^{j\nu_0} \cap A_E = \mathfrak{P}^j_{L|E}$, because $\mathfrak{P}^j_{L|E} \subseteq \mathfrak{P}^{j\nu_0} \cap A_E$ and $\mathfrak{P}^j_{L|E} \not\subseteq \mathfrak{P}^{j\nu_0+1} \cap A_E$. We conclude that $\mathfrak{P}^{j\nu_0+\ell} \cap A_E = \mathfrak{P}^{j+1}_{L|E}$ for all ℓ such that $1 \leq \ell \leq \nu_0$. □

Lemma 8. $\nu(t) = (f_{E|F}, f/s(\mathfrak{A}))$.

Proof. Write $\mathfrak{Q} = \mathfrak{P}_{L|E}$ for the Jacobson radical of $\mathfrak{A}_{L|E}$ and $\nu_{\mathfrak{Q}}$ for the corresponding exponent on $\mathfrak{K}_{L|E}$. Since $t^{\nu_{\mathfrak{Q}}(\pi_F)}$ is equivalent to π_F,

$$\nu(\pi_F) = \nu(t) \cdot \nu_{\mathfrak{Q}}(\pi_F).$$

Since $\mathfrak{A}$ has the period $r = r(\mathfrak{A})$, we have $\nu(\pi_F) = dr$, where d is the index of the division algebra $D_d|F$. Similarly, since $A_E = M_{m'}(D')$, where $D'|E$ is a central division algebra of index d', we have $\nu_{\mathfrak{Q}}(\pi_E) = d'r'$; thus $\nu_{\mathfrak{Q}}(\pi_F) = d'e_{E|F}r'$, with $r' = r(\mathfrak{A}_{L|E})$, which implies that $\nu(t) = dr/d'e_{E|F}r'$. From Proposition 1 we have $d' = d/(d,n)$, so we obtain the result

$$\nu(t) = \frac{(d,n)r}{e_{E|F}r'}. \tag{1}$$

By Theorem 0, $r = e/(d,e)$ and $r' = e_{L|E}/(d', e_{L|E})$, so

$$\frac{r}{e_{E|F}r'} = \frac{(d', e_{L|E})}{(d,e)}.$$

Substituting this into (1), we find that

$$\nu(t) = \frac{(d,n)(d', e_{L|E})}{(d,e)}.$$

In the numerator we use the relation $a(b,c) = (ab, ac)$ together with the fact that $(d,n)d' = d$ to obtain

$$\nu(t) = \frac{(d, (d,n)e_{L|E})}{(d,e)}.$$

Since

$$(d,(d,n)e_{L|E}) = (d,(de_{L|E}, e_{L|E}n)) = (d, e_{L|E}n) = (d, ef_{E|F}),$$

it follows that

$$\nu(t) = \frac{(d, ef_{E|F})}{(d,e)} = (\frac{d}{(d,e)}, \frac{e}{(d,e)} f_{E|F}) = (\frac{d}{(d,e)}, f_{E|F}) = (\frac{f}{(f,m)}, f_{E|F}),$$

where Theorem 0 gives the equality $d/(d,e) = f/(f,m)$. To complete the proof recall that $(f,m) = s(\mathfrak{A})$. $\square$

Lemmas 5, 2, 7, and 8 state and prove parts (i) through (iv) of Theorem 2, respectively, so the proof of Theorem 2 is complete. $\square$

3. Corollary.

(i) *The invariants r' and s' of $\mathfrak{A}_{L|E} = \mathfrak{A}_{L|F} \cap A_E$ are*

$$s' = (f_{L|E}, m') = (f_{L|E}, m, N_E) = (f_{L|E}, m)$$

and

$$r' = \frac{e_{L|E}}{(d', e_{L|E})} = \frac{m'}{(f_{L|E}, m')} = \frac{(m, N_E)}{(f_{L|E}, m)}.$$

In particular, if $L|E$ is fully ramified, $s' = 1$ and $r' = m'$.

(ii) *Conversely if $\mathfrak{B}$ is a given principal order of A_E, then there is precisely one principal order $\mathfrak{A}$ of A such that*

$$\mathfrak{B} = \mathfrak{A} \cap A_E, \qquad \mathfrak{K}(\mathfrak{B}) = \mathfrak{K}(\mathfrak{A}) \cap A_E,$$

where $\mathfrak{K}(\mathfrak{B})$, $\mathfrak{K}(\mathfrak{A})$ are the normalizers of $\mathfrak{B}$ in $A_E^\times$ and of $\mathfrak{A}$ in $A^\times$ resp., and we have: $s(\mathfrak{A}) = (s(\mathfrak{B})f_{E|F}, m)$.

Proof. The proof of (i) is immediate from Theorem 0 and Proposition 1. As to (ii) we choose a maximal field extension $L|E$ in A_E such that $f_{L|E} = s(\mathfrak{B})$. By Theorem 0 we conclude $s(\mathfrak{A}_{L|E}) = (f_{L|E}, m') = s(\mathfrak{B})$ because $s(\mathfrak{B})$ divides $m' = m(A_E|E)$. Therefore up to conjugating L we may assume $\mathfrak{A}_{L|E} = \mathfrak{B}$, i.e. $L^\times \subset \mathfrak{K}(\mathfrak{B})$. Now $\mathfrak{K}(\mathfrak{B}) \subset \mathfrak{K}(\mathfrak{A})$ implies $\mathfrak{A} = \mathfrak{A}_{L|F}$ and $s(\mathfrak{A}) = (f_{L|F}, m) = (s(\mathfrak{B})f_{E|F}, m)$. $\square$

We note that the first part of (ii) is Corollary 3 of Theorem 1 in [F].

Next we wish to generalize the concept of "pure element", a notion introduced by Bushnell and Kutzko in the split case [BK (1.5.5)]:

4. Definition. Let $\mathfrak{A}$ be a principal order of A and let e and f be natural numbers such that $ef = dm = N$. We call an element $x \in A$ an *(e,f)-pure element* with respect to $\mathfrak{A}$ if there is a subfield $L|F$ of A which contains x such that:

(i) $e_{L|F} = e$ and $f_{L|F} = f$;
(ii) $L^\times$ normalizes $\mathfrak{A}$.

Notation. *We write $A(e,f,\mathfrak{A})$ for the set of all (e,f)-pure elements with respect to $\mathfrak{A}$.*

From (i) we see that $L|F$ is a maximal subfield of A and from Theorem 0 that the set $A(e,f,\mathfrak{A}) = \emptyset$ unless

$$(*) \qquad \frac{m}{(f,m)} = \frac{e}{(d,e)} = r(\mathfrak{A}).$$

Equation (*) is a necessary and sufficient condition for (ii) in the Definition. Note that the field L occurring in the definition is not fixed; several different L's may contain the same $x \in \mathfrak{A}$. Assume that the numerical condition (*) is fulfilled. Then $0 \in A(e,f,\mathfrak{A})$; obviously, $A(e,f,\mathfrak{A}) \subseteq \mathfrak{K}(\mathfrak{A}) \cup \{0\}$ and $A(e,f,\mathfrak{A})$ is stable under conjugation by $\mathfrak{K}(\mathfrak{A})$.

5. Definition. For any pair of natural numbers e and f let $F[T]_{e,f}$ be the set of all irreducible monic polynomials $f(T) \in F[T]$ such that $F[T]/\big(f(T)\big)$ as a field extension of F has ramification exponent dividing e and inertial degree dividing f.

As another consequence of Theorem 0 let us prove the following weak form of "intertwining of strata implies conjugacy" (see [BK (2.6.1)] and [Z, 1.4]):

6. Proposition. *Let $\mathfrak{A}$ be a principal order in A with normalizer $\mathfrak{K} = \mathfrak{K}(\mathfrak{A})$, let e and f be natural numbers such that $ef = N$, and assume that $A(e,f,\mathfrak{A}) \neq \emptyset$. Then there is a natural bijection*

$$Ad\,\mathfrak{K}\backslash A(e,f,\mathfrak{A}) \longrightarrow F[T]_{e,f}$$

from the set of $\mathfrak{K}$-conjugacy classes contained in $A(e,f,\mathfrak{A})$ to the set $F[T]_{e,f}$ which assigns to each conjugacy class in $A(e,f,\mathfrak{A})$ its corresponding minimal polynomial over F. Especially this means that the natural map $Ad\,\mathfrak{K}\backslash A(e,f,\mathfrak{A}) \to Ad\,A^\times\backslash A$ is injective.

Proof. We begin by showing that the map is surjective, i. e. we choose $f(T) \in F[T]_{e,f}$ and show that $f(T) = 0$ has a solution in $A(e,f,\mathfrak{A})$. Since $\deg f(T) \mid N$, there exists a solution $x \in A$. Let $E = F[x] \subset A$ and let A_E be the centralizer of E in A. A maximal field extension $L|E$ in A_E has degree

$$[L:E] = \frac{N}{\deg f(T)} = \frac{e}{e_{E|F}} \cdot \frac{f}{f_{E|F}}.$$

By assumption $e_{E|F} \mid e$ and $f_{E|F} \mid f$. Therefore there exists $L|E$ such that $e_{L|E} = e/e_{E|F}$ and $f_{L|E} = f/f_{E|F}$. Consider the principal order $\mathfrak{A}_{L|F}$. Since $e_{L|F} = e$ and $f_{L|F} = f$, Theorem 0 implies that $r(\mathfrak{A}_{L|F}) = m/(f,m) = e/(d,e) = r(\mathfrak{A})$. This means that $\mathfrak{A}_{L|F}$ and $\mathfrak{A}$ are conjugate principal orders of A. Choosing $y \in A^\times$ such that $y\mathfrak{A}_{L|F}y^{-1} = \mathfrak{A}$, we find a solution $yxy^{-1} \in yLy^{-1}$ of $f(T)$ such that $(yLy^{-1})^\times$ normalizes $\mathfrak{A}$. Thus, $yxy^{-1} \in A(e,f,\mathfrak{A})$, as required.

To prove injectivity we take non-zero elements $x_1, x_2 \in A(e,f,\mathfrak{A})$ with the same minimal polynomial over F. The Skolem/Noether Theorem implies that x_1 and x_2 are conjugate in $A^\times$; we have to show that they are also conjugate in $\mathfrak{K}$. Assume that $x_1 \in L_1^\times \subset \mathfrak{K}$ and $x_2 \in L_2^\times \subset \mathfrak{K}$ and assume that the maximal subfields $L_i|F$ both satisfy the two conditions in the definition of (e,f)-pure elements with respect to $\mathfrak{A}$. Choose $g \in A^\times$ such that $x_2 = gx_1g^{-1}$. Then

$$x_2 \in L_2^\times \subset \mathfrak{K} \cap A_{x_2} \qquad \text{and} \qquad x_2 \in gL_1^\times g^{-1} \subset g\mathfrak{K}g^{-1} \cap A_{x_2},$$

where A_{x_2} denotes the centralizer of x_2 in A. Both $L_2|F(x_2)$ and $gL_1g^{-1}|F(x_2)$ are maximal subfields of A_{x_2}, so we have principal orders

$$\mathfrak{A}_{L_2|F(x_2)} = \mathfrak{A} \cap A_{x_2} \qquad \text{and} \qquad \mathfrak{A}_{gL_1g^{-1}|F(x_2)} = \mathfrak{A}_{gL_1g^{-1}|F} \cap A_{x_2} = g\mathfrak{A}g^{-1} \cap A_{x_2}.$$

Since $L_2|F(x_2)$ and $gL_1g^{-1}|F(x_2)$ have the same ramification exponents and inertial degrees, Theorem 0 implies that $r(\mathfrak{A}_{L_2|F(x_2)}) = r(\mathfrak{A}_{gL_1g^{-1}|F(x_2)})$. Therefore these orders are conjugate in A_{x_2}. For any $h \in A_{x_2}^\times$ such that

$$h(g\mathfrak{A}g^{-1} \cap A_{x_2})h^{-1} = \mathfrak{A} \cap A_{x_2} \qquad \text{and} \qquad h(g\mathfrak{K}g^{-1} \cap A_{x_2})h^{-1} = \mathfrak{K} \cap A_{x_2},$$

we have

$$hg\mathfrak{K}g^{-1}h^{-1} \cap A_{x_2} = \mathfrak{K} \cap A_{x_2}.$$

Since $L_2^\times \subset \mathfrak{K} \cap A_{x_2}$, it follows that $L_2^\times \subset hg\mathfrak{K}g^{-1}h^{-1}$. Therefore the maximal field extension $L_2|F$ of A normalizes both $hg\mathfrak{A}g^{-1}h^{-1}$ and $\mathfrak{A}$. In this case, Theorem 0 implies that these two principal orders satisfy

$$hg\mathfrak{A}g^{-1}h^{-1} = \mathfrak{A} = \mathfrak{A}_{L_2|F},$$

so $hg \in \mathfrak{K}$. Since h commutes with x_2, the equality $x_2 = gx_1g^{-1}$ implies also that $x_2 = hgx_1(hg)^{-1}$. Thus x_1 and x_2 lie in the same $\mathfrak{K}$ conjugacy class, as required. □

References

[B] H. Benz, *Untersuchungen zur Arithmetik in lokalen einfachen Algebren, insbesondere über maximalen Teilkörpern. I*, J. reine angew. Math. **225** (1967), 30–75.

[BF] C. Bushnell, A. Fröhlich, *Non abelian congruence Gauss sums and p-adic simple algebras*, Proc. London Math. Soc. **(3) 50** (1985), 207–264.

[BK] C. Bushnell, P. Kutzko, *The Admissible Dual of GL(N) via Compact Open Subgroups*, Annals of Math. Studies 129, Princeton U. Press, Princeton, N. J., 1993.

[F] A. Fröhlich, *Principal orders and embedding of local fields in algebras*, Proc. London Math. Soc. **(3) 54** (1987), 247–266.

[K] I. Kersten, *Brauergruppen von Körpern*, Aspekte der Mathematik, Band D6, Braunschweig, 1990.

[R] I. Reiner, *Maximal Orders*, Academic Press, New York, 1975.

[S] J. P. Serre, *Corps locaux*, 2. éd., Hermann, Paris, 1968.

[Z] E.-W. Zink, *Comparison of GL_N and Division Algebra Representations – Some Remarks on the Local Case*, Math. Nachr. **159** (1992), 47–72.

Ernst-Wilhelm Zink
Humboldt-Universität
Reine Mathematik
Unter den Linden 6
10099 Berlin
e-mail: zink@mathematik.hu-berlin.de