Localizability of the Embedding Problem with Symplectic Kernel

JACK SONN*

Department of Mathematics, Adelphi University, Garden City, Long Island, New York 11530

Communicated by O. Taussky Todd

Received March 23, 1971; revised February 4, 1972

In this paper we consider the question of how much information is supplied by local solutions to a global embedding problem for the special case in which the normal subgroup belonging to the given group extension is the projective symplectic group $\text{PSp}(2m, q)$. It is proved that for suitable Galois extensions $K$ of a given number field $k$ (which constitute part of the data of the embedding problem), the local solutions in a sense determine whether or not an extension $L \supset K$, Galois over $k$, with $G(L/K) \cong \text{PSp}(2m, q)$, represents a global solution to the embedding problem.

1. INTRODUCTION

Let $k$ be an algebraic number field, $K/k$ a finite Galois extension, $G(K/k) = \bar{G}$ the Galois group of $K/k$. Let

$$
\Sigma: \quad 1 \longrightarrow N \xrightarrow{i} E \xrightarrow{e} G \longrightarrow 1
$$

be a short exact sequence defining an extension of a finite group $N$ by a group $G$ which is isomorphic to $\bar{G}$, and let $\gamma: \bar{G} \rightarrow G$ be a fixed isomorphism.

**Definition.** The embedding problem $P = P(K/k, \Sigma, \gamma)$ is the problem of establishing the existence or non-existence of an extension $L/K$, such

*Current address: Department of Mathematics, Technion—Israel Institute of Technology, Haifa, Israel.

Copyright © 1974 by Academic Press, Inc. All rights of reproduction in any form reserved.
that $L/k$ is normal, $G(L/k)$ is isomorphic to $E$, and there exists an isomorphism $\beta: E \to E$ such that the diagram

$$
\begin{array}{ccc}
E & \longrightarrow & G \\
\beta \downarrow & & \gamma \downarrow \\
E & \longrightarrow & G
\end{array}
$$

commutes, where $\tilde{e}$ is the canonical mapping. The pair $(L, \beta)$ will be called a (proper) solution to $P$. If $G(L/k)$ is isomorphic to a proper subgroup of $E$, and $\beta$ is only a monomorphism, we call $(L, \beta)$ an improper solution to $P$.

Let $p$ be a prime ideal of the ring $\mathcal{O}_k$ of integers of $k$, and let $\mathfrak{P}$ be a divisor of $p$ in $K$. Let $\sigma_k$ be a fixed embedding of $k$ into the completion $k_p$, and let $\sigma_K$ be an embedding of $K$ into the completion $K_\mathfrak{P}$ such that $\sigma_K|k = \sigma_k$ where we assume that $k_p \subseteq K_\mathfrak{P}$.

From the general theory of local fields we know that $\sigma_k$ induces a monomorphism $\sigma_k^*$ of $G(K_\mathfrak{P}/k_p)$ into $\mathcal{G}$, whose image is $\mathcal{G}(\mathfrak{P})$, the decomposition group of $\mathfrak{P}$. There results a local embedding problem $P = P(K_\mathfrak{P}/k_p, \Sigma_\mathfrak{P}, \gamma_\mathfrak{P})$ with $\Sigma_\mathfrak{P}: 1 \to N \to E_\mathfrak{P} \to \epsilon_\mathfrak{P} G_\mathfrak{P} \to 1$, where $G_\mathfrak{P} = \gamma(G(\mathfrak{P}))$, $E_\mathfrak{P} = \epsilon^{-1}(G_\mathfrak{P})$, $\epsilon_\mathfrak{P} = \epsilon|E_\mathfrak{P}$, and $\gamma_\mathfrak{P} = \gamma \cdot \sigma_k^*$.

Suppose that a global embedding problem $P(K/k, \Sigma, \gamma)$ has a solution $(L, \beta)$. Then for each prime $\mathfrak{P}$ of $K$ there results an improper (in general) solution $(L_\mathfrak{P}, \beta_\mathfrak{P})$ to the local embedding problem $P_\mathfrak{P}$, where $L_\mathfrak{P}$ is the completion of $L$ with respect to a divisor $q$ of $\mathfrak{P}$ in $L$, $L_\mathfrak{P} \supset k_\mathfrak{P}$, and $\beta_\mathfrak{P} = \beta \cdot \sigma_L^*$, where $\sigma_L$ is an embedding of $L$ into the completion $L_q$ such that $\sigma_L|K = \sigma_K$, and $\sigma_L^*$ is the monomorphism of $G(L_q/k_p)$ into $\mathcal{G}$ induced by $\sigma_L$. (For details, see [3, p. 420].)

How much information about the Galois group $\mathcal{E}$, considered as an extension of $N$ by $G$, is obtained from the local solutions? To investigate this question, we introduce the following hypothesis.

**Definition.** By the localization hypothesis $\mathcal{L}(P) = \mathcal{L}(K/k, \Sigma, \gamma)$ we mean the following: Let an embedding problem $P = P(K/k, \Sigma, \gamma)$ be given, $k$ a number field. Let $S$ be a finite set of prime ideals of $k$, and let there be associated with each $p \in S$ a prime $\mathfrak{P}$ of $K$ dividing $p$ together with embeddings $\sigma_k, \sigma_K$ defined above. Let $P_\mathfrak{P}$ denote the local embedding problem induced by $P$ for each $p \in S$. Suppose that for each $p \in S$, the set $\mathcal{L}_p$ of improper solutions to $P_\mathfrak{P}$ is not empty. Now let there be chosen from each $\mathcal{L}_p$ an improper solution $(L_\mathfrak{P}, \beta_\mathfrak{P})$. Then there exists a finite Galois extension $L/k$, $L \supset K$, such that $G(L/K) \approx N$, and the following hold:
(i) for each \( p \in S \), there exists an extension \( \sigma_L \) of \( \sigma_K \) to \( L \) such that \( K_p \cdot \sigma_L(L) = L^\mathfrak{g} \), and

(ii) there is an isomorphism \( \alpha: \mathcal{N} \rightarrow N \) (where \( \mathcal{N} = G(L/K) \)) such that for each \( p \in S \), the diagram

\[
\begin{array}{ccc}
G(L^\mathfrak{g}/K_p) & \xrightarrow{\nu_L} & \mathcal{N}(q) \\
\downarrow \alpha^\mathfrak{g} & & \downarrow \alpha \\
N & \xrightarrow{\gamma} & N
\end{array}
\]

is commutative, where \( q \) is the prime ideal of \( L \) induced by \( \sigma_L \), \( \alpha^\mathfrak{g} = \gamma^{-1} \cdot \beta^\mathfrak{g} \cdot \text{Incl}_{L^\mathfrak{g}/K_p} \), and \( \mathcal{N}(q) \) is the decomposition group of \( q \) in \( \mathcal{N} \).

In effect, \( \mathcal{L}(P) \) states that there is a Galois extension \( L \) of \( k \) containing \( K \) such that \( G(L/K) \approx N \) and \( L \) "localizes" to each of the given solutions \( (L^\mathfrak{g}, \beta^\mathfrak{g}) \) as if it were a solution field to \( P \).

We call an embedding problem \textit{localizable} if there exists a choice of \( S \) and a corresponding set of \( (L^\mathfrak{g}, \beta^\mathfrak{g}) \) such that the field \( L \) yielded by \( \mathcal{L}(P) \) is a solution field to \( P \).

If the kernel \( N \) has trivial center, then the centralizer \( H \) of \( N \) (rather \( \mathcal{L}(N) \)) in \( E \) intersects \( N \) trivially, and if one replaces \( E \) by \( E' = E/H \), one obtains an "irreducible" embedding problem \( P' \), with the same \( N \), but where \( E' \) is isomorphic to a subgroup of the automorphism group \( \text{Aut} N \) of \( N \). It is proved in [3, p. 419], that \( P \) has a solution if and only if \( P' \) has a solution \( (L', \beta') \) in which \( L' \cap K = K' \), where \( K' \) is the fixed field of \( \gamma^{-1} \in H \subseteq \overline{G} \). Because of this reduction theorem, we strengthen the hypothesis \( \mathcal{L}(P) \) to the statement \( \mathcal{L}^*(P) \) which says the same thing as \( \mathcal{L}(P) \) with the additional condition that the field \( L \) yielded by \( \mathcal{L}(P) \) can be chosen so that it is linearly disjoint over \( K \) to a finite extension \( L' \) of \( K \) given in advance. This stronger hypothesis reduces the localizability of embedding problems \( P \) with \( N \) having trivial center, (relative to \( \mathcal{L}(P) \),) to the localizability of irreducible embedding problems \( P' \) (relative to the stronger hypothesis \( \mathcal{L}^*(P') \)).

This paper deals with the localizability of irreducible embedding problems in which \( N \approx PSp(2m, q) \), the projective symplectic group of degree \( 2m \) over \( GF(q) \), where \( m > 1 \), \( q = p_1 \cdots p_n \) a rational prime. (The case \( m = 1, N \approx PSL(2, q) \) will not be treated here.) It is well known that \( PSp(2m, q) \) is simple (except when \( m = 1 \) and \( q = 2 \) or 3). The embedding problem in this case is relevant to the problem of constructing extensions of \( k \) with prescribed Galois group having \( N \) as a principal factor. We prove here that when \( N = PSp(2m, q) \), there are embedding problems which are not localizable, but every embedding problem \( P(K/k, \Sigma, \gamma) \) in which certain conditions on the local behavior of \( K/k \) are imposed, is localizable.
2. A Counterexample

In this section an example similar to the one in [3, p. 430], is given, in which \( P \) is an irreducible embedding problem, which is not localizable, with \( N \cong PSp(2m, q) \).

Let \( m > 1 \), \( p_0 \) a rational prime, and \( v \) a positive prime integer prime to the order of \( N = PSp(2m, p_0^v) \); for example \( m = 2 \), \( p_0 = 3 \), \( v = 7 \). The number 7 is prime to the order of \( N \) since it is prime to the order of \( PGL(4, 3^v) \) which contains \( N \) as a subgroup. Next set \( E = \langle \Phi, N \rangle \), where \( \Phi \) denotes the automorphism of \( Sp(2m, q) \) induced by applying the Frobenius automorphism \( x \mapsto x^{p_0} \) to the coefficients of a matrix, and \( \Phi \) is the corresponding automorphism induced in \( PSp(2m, q) \). Thus \( E \) is the semidirect product of \( N \) with a cyclic group of order \( v \), so that \( G \) is cyclic of order \( v \).

Now construct an extension \( K/k \) in the same manner as in [3, p. 430]: Let \( k = Q(\zeta_e) \), where \( e \) is the order of \( E \), \( \zeta_e \) is a primitive \( eth \) root of unity, \( K = k(a^{1/n}) \), \( a \in k \), where by virtue of the approximation theorem of valuation theory, \( a \) is chosen to have the following properties:

1. \( a \) is congruent to 1 mod \( p \) for every divisor \( p \) of \( e \) in \( k \) which is prime to \( v \).
2. \( a \) is congruent to 1 mod \( p^v \) for every divisor \( p \) of \( v \) in \( k \), where \( t_p \) is chosen sufficiently large so that every \( t_p^v \)-unit of \( k_p \) is a \( v \)th power of an element of \( k_p \).
3. Let \( p_0 \) be any fixed prime of \( k \) different from all the primes \( p \) occurring in (1) and (2) above. Then \( a \) is chosen to be congruent mod \( p_0 \) to a root of unity in \( k_{p_0} \) which is not a \( v \)th power. (Clearly such a root of unity exists, since \( v \) divides the order of the multiplicative group of the residue class field of \( k_{p_0} \).)

Any \( a \) satisfying (1), (2), and (3) is a \( v \)th power in \( k_p \) for all \( p/e \) but not in \( k \) since it is not a \( v \)th power in \( k_{p_0} \). Hence all prime divisors of \( e \) in \( k \) split completely in \( K \). Finally, let \( \gamma \) be any isomorphism from \( G = G(K/k) \) to \( G \).

We show that the embedding problem \( P(K/k, \Sigma, \gamma) \) (where \( \Sigma' \) is the natural sequence associated with \( E \) as an extension of \( N \) by \( G \)) is not localizable.

Suppose \( S \) is any finite set of primes of \( k \). Any \( \mathfrak{p} \in S \) which divides \( e \) is of no use, since it splits completely in \( K \) and hence gives no information about the (group) extension \( \overline{E} \) of \( N \) by \( \overline{G} \). Hence we may assume that every \( \mathfrak{p} \) in \( S \) is prime to \( e \). But this implies that if \( (L^\mathfrak{p}, \beta^\mathfrak{p}) \) is any of the prescribed local improper solutions, then \( L^\mathfrak{p}/k_\mathfrak{p} \) is tamely ramified, so that \( G(L^\mathfrak{p}/k_\mathfrak{p}) \)
is metacyclic. In fact, since \( k \) contains the \( \phi \)th roots of unity, \( G(L^\phi/k_p) \) is abelian. For the action of one cyclic factor on the other is given by raising to the power (absolute norm) \( N(\phi) \) which in this case is congruent to 1 mod the order of the cyclic factor being acted upon.

Let \( \mathcal{S} \) denote the canonical sequence

\[
1 \rightarrow \mathcal{N} \rightarrow E \rightarrow \mathcal{G} \rightarrow 1
\]

associated with the tower \( k \subset K \subset L \), where \( L \) is the field yielded by \( \mathcal{L}(P) \). Now \( \mathcal{L}(P) \) says, in effect, that for each \( \mathfrak{p} \) (the prime of \( K \) corresponding to \( p \in S \)), there is a monomorphism \( \beta_{\mathfrak{p}} : E(q) \rightarrow E \), where \( q \) is a divisor of \( \mathfrak{p} \) in \( L \) and \( E(q) \) is its decomposition group, such that the diagram

\[
\begin{align*}
1 & \rightarrow \mathcal{N}(q) \rightarrow E(q) \rightarrow \mathcal{G}(\mathfrak{p}) \rightarrow 1 \\
1 & \rightarrow \mathcal{N} \rightarrow E \rightarrow \mathcal{G} \rightarrow 1
\end{align*}
\]

commutes (the subscript \( \mathfrak{p} \) is affixed wherever necessary to indicate restriction of the original mapping), where \( \alpha \) is a fixed isomorphism of \( \mathcal{N} \) onto \( \mathcal{N} \), and \( \beta_{\mathfrak{p}}(E(q)) = \beta_{\mathfrak{p}}(G(L^\phi/k_p)) \).

We show now that the above conditions imposed by \( \mathcal{L}(P) \) are fulfilled if \( E \) is isomorphic to the direct product \( C_v \times N \), where \( C_v \) is a cyclic group of order \( v \). This implies that \( P \) is not localizable.

Suppose \( E \cong C_v \times N \). Let \( U_{\mathfrak{p}} = \beta_{\mathfrak{p}}(G(L^\phi/k_p)) \) be any two-generator abelian subgroup of \( E \). We need of course only consider the nontrivial case \( U_{\mathfrak{p}} \not\cong N \), in which case \( U_{\mathfrak{p}}N \cong E \). Since \( \nu \) is prime to the order of \( N \), we may write \( U_{\mathfrak{p}} = C_v \times U_{\mathfrak{p}} \cap N \). Then it is easy to find a subgroup of \( E \) which we shall call \( E(q) \), and an isomorphism \( \beta_{\mathfrak{p}} : E(q) \rightarrow U_{\mathfrak{p}} \) such that (2.1) commutes; namely, let \( E(q) = \mathcal{C}_v \times \alpha^{-1}(U_{\mathfrak{p}} \cap N) \), where \( \mathcal{C}_v \) is the unique subgroup of \( E \) of order \( v \), and let \( \beta_{\mathfrak{p}} \) be the isomorphism of \( \mathcal{C}_v \times \alpha^{-1}(U_{\mathfrak{p}} \cap N) \) onto \( C_v \times U_{\mathfrak{p}} \cap N \) which is uniquely determined by \( \alpha_{\mathfrak{p}} \) and \( \gamma_{\mathfrak{p}} \), where \( \rho : G \rightarrow C_v \) is a representative map for the split sequence \( \mathcal{S} \), so that \( \epsilon_\mathcal{S} = \text{identity} \).

Remark. This example adapts itself to the case \( N = PSL(n, q) \) \( \text{mutatis mutandis} \), as an alternative to the example in [3, p. 430].

3. Localization of the Embedding Problem with Symplectic Kernel

We assume henceforth that \( N \cong PSp(2m, q) \), \( m > 1 \) and \( q \neq 2 \) if \( m = 2 \) (\( PSp(4, 2) \cong PSL(2, 9) \)). From the preceding section we know
that not every irreducible embedding problem with kernel $N$ is localizable, given $K/k$. However, if the local behavior of $K/k$ can be prescribed (in a sense to be made precise), then localizability is guaranteed.

Given $k$, let $K/k$ be a finite extension (Galois) with Galois group $G(K/k) \cong G$, a finite group. Let a finite set $S$ of primes of $k$ be given. For each $p$ in $S$, let $\Psi$ be a divisor of $p$ in $K$. Then the decomposition group $G(\Psi)$ is a subgroup of $G = G(K/k)$ and is the Galois group of the extension $K^p/k_p$. If we modify $K$, but not $k$, then we modify $\Psi$, and hence $K\Psi$ and $\tilde{G}(\Psi)$. Conversely, suppose $\psi$ is given and $G_p$ is a subgroup of $G$ which is isomorphic to the Galois group of an extension $K^p/k_p$. Then $G_p$ may occur as a decomposition group $\tilde{G}(\Psi)$ in some extension $K/k$ (via an isomorphism $\gamma: \tilde{G}(\Psi) \to G$). If we specify, for each $p \in S$, such a subgroup $G_p$ of $G$ and assume that in an embedding problem $P(K/k, \Sigma, \gamma)$ that $\gamma(\tilde{G}(\Psi)) = G_p$ for each $p \in S$, where $\Psi$ is a prime of $K$ dividing $p$, then we say that we are prescribing the local behavior of $K/k$ at (the primes of) $S$. We can now state the main theorem.

**Theorem.** Let $P = P(K/k, \Sigma, \gamma)$ be an irreducible embedding problem with $N \approx PSp(2m, q)$, $m > 1$ and $q \neq 2$ if $m = 2$. Then $P$ is localizable if the local behavior of $K/k$ at any finite set of primes of $k$ can be prescribed.

### 3.1. The Automorphism Group of $N$

The automorphism group $\text{Aut} \ N$ of $N$ is known (see [2]). Namely: let $Gp(2m, q)$ be the general symplectic group consisting of those nonsingular linear transformations $g$ for which $(gX, gY) = a_g(X, Y)$, where $a_g \in GF(q)$, $a_g \neq 0$, and $a_g$ is independent of $X$ and $Y$, and $(, )$ denotes a nondegenerate symplectic (skew-symmetric and bilinear) form over $GF(q)$ of rank $2m$. Let $PGp(2m, q)$ be the factor group $Gp(2m, q)/A$, $A$ the scalar subgroup. Since the mapping $g \to a_g$ is an epimorphism of $Gp(2m, q)$ onto the multiplicative group of $GF(q)$ with kernel $Sp(2m, q)$, the symplectic group, we have $[Gp(2m, q): Sp(2m, q)] = q - 1$. Furthermore,

$$[PGp(2m, q): PSp(2m, q)] = [Gp(2m, q): A \cdot Sp(2m, q)],$$

the latter index being equal to 1 if $p_0 = 2$, and to 2 if $p_0 \neq 2$.

For convenience we will treat $Gp(2m, q)$ as a group of matrices. Let us introduce the following notation. Denote by $e_{ij}^n$ the $n$ by $n$ matrix with 1 in the $i, j$ position, and zeros elsewhere. In addition, if for $i = 1, \ldots, r$, $A_i$ is a square matrix of degree $n_i$, then $\bigoplus\{A_i \mid i = 1, \ldots, r\}$ will denote the square matrix of degree $n_1 + \cdots + n_r$ with $A_1, \ldots, A_r$ in order down
the main diagonal, zeros, elsewhere. If all the $A_i$ are equal, then we will write simply $\bigoplus r A_i$.

Set $J = \bigoplus_m (e_{1,2}^{(1)} - e_{2,1}^{(2)}); \text{then } Sp(2m, q) = \{X \in GL(2m, q) \mid X^T J X = J\}$ and $Gp(2m, q) = \{X \in GL(2m, q) \mid X^T J X = a_x J \text{ for some } a_x \neq 0 \text{ in } GF(q)\}$. The matrix $Z = \bigoplus_m (\zeta e_{11}^{(1)} + e_{22}^{(2)})$ belongs to $Gp(2m, q)$ ($0 \neq \zeta \in GF(q))$ and $u_z = \zeta$. We assume henceforth that $\zeta$ is a primitive $q - 1$th root of unity in $GF(q)$. Set $Z = Z \mod A$.

Next let $\Phi$ be the automorphism of $Gp(2m, q)$ and by restriction, of $Sp(2m, q)$ as well) induced by applying the Frobenius automorphism $x \mapsto x^{q^m}$ to the coefficients of a matrix. Let $\Phi$ be the automorphism of $PGp(2m, q)$ (and of $PSp(2m, q)$) induced by $\Phi$. Then

$$\text{Aut } N = \text{Aut } PSp(2m, q) = \langle \Phi, PGp(2m, q) \rangle,$$

the semidirect product of $\langle \Phi \rangle$ and $PGp(2m, q)$. (Aut $N$ can be identified with the group of all semilinear transformations $g$ of the $2m$-dimensional symplectic $GF(q)$-space such that $(gX, gY) = a_g(X, Y)^s$, where $0 \neq a_g \in GF(q), s_g \in G(GF(q)/GF(p))$, modulo the scalar transformations $X \mapsto aX$.) It follows that $Out N$, the outer automorphism group of $N$, is a cyclic group of order $\nu$ if $p_0 = 2$, and is the direct product of a cyclic group of order $\nu$ with a group of order $2$ if $p_0$ is odd. We denote by $Z$, $\Phi$, the classes of $Z$, $\Phi$ respectively, in $Out N$, so that $Out N = \langle \Phi \rangle$ or $\langle \Phi, Z \rangle$ accordingly as $p_0 = 2$ or $p_0$ is odd. (The exceptional case $PSp(4, 2) = PSL(2, 9)$ is excluded.)

### 3.2. Reformulation of $\mathcal{P}(P)$

In order to make use of $\mathcal{P}(P)$, it is advantageous to reformulate it by identifying isomorphic groups. It is shown in [3, p. 424], that $\mathcal{P}(P)$ is equivalent to the following: Given a family $\mathcal{U}$ of subgroups $U$ of $E$ such that

(i) for each $U$ there is a prime $p = p_U$ of $k$ and a divisor $\Psi$ of $p$ in $K$ such that the local problem $P_{\Psi}$ has an improper solution with $\beta^\Psi G(L^\Psi/k_p) = U$, and

(ii) the correspondence $U \mapsto p_U$ is one-one;

Then there exists an extension (of groups)

$$\Sigma: 1 \longrightarrow N \longrightarrow E \longrightarrow G \longrightarrow 1$$

of $N$ by $G$ such that
(iii) for each $U \in \mathcal{U}$, there is a subgroup $\mathcal{U}$ of $\mathcal{E}$ and an isomorphism 

$$\delta = \delta_U : \mathcal{U} \to U$$

such that $\iota^{-1}(\mathcal{U} \cap \iota N) = \iota^{-1}(U \cap \iota N)$, and the diagram

\[
\begin{array}{ccc}
\iota^{-1}(\mathcal{U} \cap \iota N) & \to & \mathcal{U} \to G \\
\| & & \downarrow \delta \\
\iota^{-1}(U \cap \iota N) & \to & U \to G
\end{array}
\]

(3.1)

commutes, and

(iv) if $\Sigma$ and $\Sigma'$ are equivalent group extensions, or even if there is

an isomorphism $\beta : E \to E$ such that $\epsilon \beta = \epsilon$ (a weaker condition), then

the embedding problem $P$ has a solution.

In this reformulation, $\Sigma$ corresponds to the Galois group sequence,

$E = G(L/k)$, where $L$ is the field yielded by $\mathcal{L}(P)$. Also, we write $U = p''(G(L'/k_p))$. $U = 8_p$ is then the decomposition group $E(q)$ for some divisor $q$ of $p$ in $L$.

3.3. Proof of the Theorem, Part I

We show first that we can find a set $\mathcal{U}$ satisfying (i) and (ii) such that

the sequence $\Sigma$ yielded by $\mathcal{L}(P)$ (reformulated) has the property that $E$

is isomorphic to a subgroup of Aut $N$, i.e., the centralizer $Z_E(\iota N)$ of

$\iota N$ in $\mathcal{E}$ is trivial. In Part II of the proof we will expand $\mathcal{U}$ to a larger set

such that any $\Sigma$ yielded by $\mathcal{L}(P)$ relative to the larger $\mathcal{U}$ is equivalent to $\Sigma$.

Suppose $\mathcal{H} = Z_E(\iota N) \neq 1$. Then $\mathcal{H}$ is a normal subgroup of $G$, and

contains a minimal normal subgroup of $G$ which in turn contains a cyclic

subgroup $C$ of prime order. If we set $C = \mathcal{H} \cap \mathcal{H}^{-1}C \cong C$, then $E$ contains

$C \times \iota N$ as a subgroup. It therefore suffices to determine $\mathcal{U}$ such that for

every cyclic subgroup $C$ of $G$ of prime order, such that $C$ is contained in

a minimal normal subgroup of $G$, there is a $U \in \mathcal{U}$ such that

(a) $\epsilon U \supseteq C$, and

(b) if $U_1 = U \cap \epsilon^{-1}C$, there is no monomorphism of $U_1$ into

$C \times \iota N$ (or equivalently, $C \times N$) whose restriction to to $U_1 \cap \iota N$ is the

identity mapping (and which induces the identity mapping on $C$).

Case 1. $C = \langle \mathbb{Z} \rangle$ (See Section 3.1).

In this case $p_0 \neq 2$ and $C$ has order 2.

Subcase 1.1. $q \equiv 1$ (mod 4). Set

$$A = (\zeta e_{11} + e_{22}) \oplus (\oplus_{m=1}^{\infty} (\zeta e_{12} - e_{21})) \in Gp(2m, q),$$
where here and in what follows, \( e_{ij} = e_{ij}^{(q)} \), and \( \zeta \) is a primitive, \( q - 1 \)th root of unity in \( GF(q) \). Set \( A = A \mod \text{scalars}, \) and \( U = \langle A \rangle \). By \( \text{Chebotarev's density theorem} \) (given a finite Galois extension \( K/k, k \) a number field, and given a cyclic subgroup \( \overline{C} \) of \( \overline{G} = G(K/k) \), there exist infinitely many primes \( \mathfrak{P} \) of \( K \) such that the decomposition group \( \overline{G}(\mathfrak{P}) = \overline{C} \), there are infinitely many primes \( p \) for which \( (a) \) can be satisfied. For we can choose a \( p \) of \( k \) which has a divisor \( \mathfrak{P} \) in \( K \), unramified over \( p, \) such that \( \overline{G}(\mathfrak{P}) = \overline{C} \), and since \( U \) is cyclic, there is a solution \( (L_{\mathfrak{P}}, \beta_{\mathfrak{P}}) \) to the local problem \( P_{\mathfrak{P}}(K/k, \Sigma, \gamma_{i}, \mathfrak{P}) \) in which the extension group \( E_{i} \) is cyclic and \( K_{i}/k_{i} \) is unramified, has a (proper) solution \( (L_{1}, \beta_{1}) \) with \( L_{1}/k_{1} \) unramified (see e.g. [3, p. 434]).

To prove \( (b) \), suppose that such a monomorphism existed. Then there would exist \( B \in Sp(2m, q) \) such that \( B^2 = bA^2 \ (0 \neq b \in GF(q)) \). Now

\[
A^2 = (\zeta^2 e_{11} + e_{22}) \oplus (\bigoplus_{m-1}(-\zeta e_{11} - \zeta e_{22}))
\]

where \( I_r \) denotes the \( r \) by \( r \) identity matrix. Since \( B \) commutes with \( A^2 \) and \( \in Sp(2m, q), \) and \( \xi \neq \xi^{-1} \neq -1, B = (ae_{11} + a^{-1}e_{22}) \oplus B', 0 \neq a \in GF(q), \)

\( B' \in Sp(2m - 2, q), a^2 = b^2, a^{-2} = b \) hence \( a^4 = \zeta^2, \) contradiction.

**Subcase 1.2.** \( q \equiv 3 \pmod{4} \). Let \( R \) be a representation of \( GF(q^2) \) in the algebra \( M_2(GF(q)) \) of 2 by 2 matrices over \( GF(q), \) let \( u \) be a primitive \( q^2 - 1 \)th root of unity in \( GF(q^2) \), \( A_1 = R(u) \). Set

\[
A = A_1 \oplus (\bigoplus_{m-1}(\zeta e_{11} + e_{22})),
\]

where we may assume \( \det A_1 = \zeta \). It follows that \( A \in Sp(2m, q), a_A = \zeta \) (see Section 3.1 above for definition of \( a_A \)). Set \( U = \langle A \rangle, (a) \) is satisfied by the same argument as in subcase 1.1 above, and denial of \( (b) \) leads to an element \( B \) of \( Sp(2m, q) \) satisfying \( B^2 = bA^2 \ (0 \neq b \in GF(q)) \). Since \( u^2 \notin GF(q), \) the commutativity of \( B \) with \( A^2 \) implies that \( B = B_1 \oplus B_2, B_1 \in SL(2, q) \), hence \( B_1 \) and \( A_1 \) commute, which implies \( B_1 = R(v) \) for some \( v \in GF(q^2) \), \( v^{q+1} = 1 \). \( B_1^2 = bA_1^2 \) implies \( u^2 = bu^2 \) which implies \( u^2 = b^{-2}v^2 \). But \( (v^2b^{-2}) \) to the power \( (q + 1)/2 \) has odd order, and \( u^2 \) to the same power has even order, contradiction.

**Case 2.**

**Subcase 2.1.** \( v \) odd. Then \( C \subseteq \langle \Phi \rangle \). Let \( G = \langle \Phi, Z \rangle, 0 < i < v, \)

\( 0 \leq j < 2 \) (in this case \( G \) is of this form); we may assume \( i \mid v \). Let
\[ U = \langle \Phi^i, A \rangle, \] where \( A = (\zeta_p e_{11} + \zeta_p^{-1} e_{22}) + I_{2m-2}, \) \( \zeta_p \) is a \( p \)th root of unity \( \neq 1 \) in \( GF(q) \), \( p \) a rational prime dividing \( q - 1 \) but not \( p^r - 1 \) for \( 0 < r < v \). The existence of \( p \) follows from a lemma of Artin [1, p. 358]. Note \( p \neq 2 \).

Let \( p \) be a prime of \( k \) dividing \( p \). We prescribe the local behavior of \( K/k \) at \( p \) by making \( p \) unramified in \( K/k \), and assuming that the decomposition group \( G(\mathfrak{p}) \) of a divisor \( \mathfrak{p} \) of \( p \) in \( K \) is equal to \( \gamma^{-1} \langle \Phi \rangle \). It follows from the following theorem that there is a local solution \((L^\mathfrak{p}, \beta^\mathfrak{p})\) to \( P_\mathfrak{p} \) such that \( \beta^\mathfrak{p} G(L^\mathfrak{p}/k_p) = U \).

**Theorem.** Let \( k \) be a local \( p \)-adic field, \( K/k \) a tamely ramified Galois extension of degree \( e \), where \( e = e(K/k), f = f(K/k) \) are the ramification index and residue class degree, respectively, \( \gamma: G(K/k) \to G \) an isomorphism \((G \text{ an abstract group}), N \) a cyclic group of order \( p \), where \( p \) is the characteristic of the residue class field of \( k \). Let \( \Sigma \) be an extension of \( N \) by \( G: 1 \to N \to E \to G \to 1 \) such that the subgroup of \( G \) corresponding under \( \gamma \) to the inertia group of \( G(K/k) \) acts trivially on \( N \); i.e., if \( G_1 \) is the inertia group of \( G = G(K/k) \), then \( G_1 = \gamma(G_1) \) acts trivially on \( N \).

Then the embedding problem \( P = P(K/k, \Sigma, \gamma) \) has a proper solution.

**Proof.** Postponed until Section 5 for the sake of continuity.

We resume the proof of Subcase 2.1. Assertion (a) is valid for the group \( U = \langle \Phi^i, A \rangle \), hence we must now verify (b). Denial of (b) leads to an element \( B \in Sp(2m, q) \) such that \( B^{-1}AB = bA^{p_0} \) \((0 \neq b \in GF(q))\). Since \( p \neq 2 \), comparison of eigenvalues yields \( b = 1 \), which implies \( \zeta_p \) is either a \( p_0 \)-th root of unity or a \( p_0^4 \)-th root of unity. The first is impossible, and the second implies that \( \zeta_p \) is a \( p_0^2 \)-th root of unity, \( 2l = m, m \) even, contrary to the present hypothesis. This completes Subcase 2.1.

**Subcase 2.2. \( m \) even.** Then either \( p_0 = 2 \) or \( q \equiv 1 \pmod{4} \). Let \( A = A_1 \oplus I_{2m-2}, \) where \( A_1 = R(u_p), u_p \) a \( p \)th root of unity \( \neq 1 \) in \( GF(q^2), \) where this time \( p \) (by virtue of Artin’s lemma) is a prime dividing \( q^2 - 1 \) but not \( p_0^r - 1 \) for \( 0 < r < 2v \). \((R \text{ is the same as in Subcase 1.2, a representation of } GF(q^2) \text{ in } M_{2}(GF(q^2)).)\)

There exists \( W_1 \in GL(2, q) \) such that \( \Phi W_1 \) transforms \( R(u) \) into \( R(u)^{p_0} \) for every \( u \in GF(q^2) \). For if \( u \) is a primitive \( q^2 - 1 \)th root of unity in \( GF(q^2) \) and \( f(t) \) is the minimal polynomial of \( R(u) \) over \( GF(p_0) \), then \( f(t)^{p_0} \) is the minimal polynomial of \( R(u)^{p_0} \) and also of \( R(u^{p_0}) = R(u)^{p_0} \), so that \( R(u)^{p_0} \) is similar to \( R(u)^{p_0}, R(u^{p_0}) = R(u)^{p_0} \) for some \( W_1 \in GL(2, q). \) \((f(t)^{p_0} \) is obtained from \( f(t) \) by applying the Frobenius automorphism to the coefficients of \( f(t) \).\)

Set \( \Phi_a = \Phi \cdot (\oplus_m W_1). \) We may modify \( W_1 \) by an element of \( R(GF(q^2)) \)
so that $\Phi_2 = \Phi$, where $\Phi_2$ denotes the class of $\Phi$ modulo the inner automorphism group $\text{Inn} \; \text{PSp}(2m, q)$ of $\text{PSp}(2m, q)$.

If $p_0 = 2$, then $C \subseteq \langle \Phi^i \rangle$; set $U = \langle \Phi^i, A \rangle$, where $\Phi_2 = \Phi_2$ mod scalars. If $p_0 \neq 2$, and $G$ is cyclic ($G \neq \langle \Phi^i \rangle$), then $G = \langle \Phi^i \rangle$. If $G$ is not cyclic, then $G = \langle \Phi^i, \mathbb{Z} \rangle$. In the first case, set $U = \langle \Phi^i, A \rangle$.

In the latter three cases, set $B = \oplus_{m=1}^{B_1}$, where $B_1 = R(v)$, $v$ an element of $GF(q^2)$ of maximal 2-power order. If $G = \langle \Phi^i, \mathbb{Z} \rangle$, set $U = \langle \Phi^i B, A \rangle$; if $G = \langle \Phi^i, \mathbb{Z} \rangle$, set $U = \langle \Phi^i, B, A \rangle$. Note that $B \in \text{Sp}(2m, q)$, $B \neq \text{Sp}(2m, q)$, and $B^a = 1$, $(B = B$ mod scalars) since $q \equiv 1 \pmod{4}$, and $B$ commutes with both $\Phi_2$ and $A$.

Let $p$ be a prime of $k$ dividing $p$. In the cyclic cases, we prescribe the behavior of $p$ in $K/k$ so that $p$ is unramified in $K/k$ and $\overline{\gamma}(\mathbb{F}) = \gamma^{-1}U \cdot iN$ (where $\mathbb{F}/p$). In the noncyclic case, we prescribe the local behavior of $p$ in $K/k$ so that $p$ is tamely ramified in $K/k$, $\gamma^{-1} \langle \mathbb{Z} \rangle$ is the inertia group of $\mathbb{F}/p$. We apply the theorem of Subcase 2.1 (in the same manner) so that (a) is fulfilled. It remains to verify (b). Denial would yield a matrix $D \in \text{Sp}(2m, q)$, satisfying $A' = bA'p^i$ (assuming $C = \langle \Phi^i \rangle$ or $\langle \Phi^i \mathbb{Z} \rangle$ without loss of generality), $0 \neq b \in GF(q)$. Comparing eigenvalues of both sides of this equation, we conclude $b = 1$, $A' = A'p^i$, $u_p = u_{p^i}$ or $u_p = u_{p^i}q$, implying that $u_p$ is either a $p_0^i$ - 1th root of unity or a $p_0^{i+v}$ - 1th root of unity, hence $2v \mid i$ or $2v \mid i + v$, both impossible since $i > v$. This completes Subcase 2.2 and hence Part I of the proof of the main theorem.

### 3.4. Proof of the Theorem, Part II

By virtue of Part I, we assume that the field $L$ yielded by the localization hypothesis $L^\ast(P)$ has the property that the centralizer $Z_G(iN)$ of $iN$ in $E$ is equal to one. However, it is now necessary to augment the set of primes $p$ used in Part I to make further restrictions on $L$.

The isomorphism $\alpha: \overline{N} \rightarrow N$ yielded by $L^\ast(P)$ induces an isomorphism $\alpha^* = \alpha i^{-1}$ of $iN$ onto $iN$; we assume for convenience that $E \subseteq \text{Aut} \; N$. Then $\alpha^*$ induces a monomorphism $\beta': \overline{E} \rightarrow \text{Aut} \; N$ in the natural way: $\beta'(x) = \gamma \in \text{Aut} \; N$ iff $n^\gamma = \alpha^{-1}(x-i(n)x)$ for $n \in N$. Set $E' = \beta' \overline{E}$. In turn $\beta'$ induces a monomorphism $\gamma': \overline{G} \rightarrow \text{Out} \; N$. (Here $N$ is identified with $\text{Inn} \; N$; this is valid since $iN$ is the unique minimal normal subgroup of $E$.) Set $G' = \gamma' \overline{G}$, $\gamma'' = \gamma^{-1}: G' \rightarrow G$.

Let $p$ be a prime of $k$, $q$ the prime of $L$ induced by the embedding $\sigma_L$ of $L$ into the algebraic closure $\overline{k}_p$ of $k_p$. (See Section 1 above.) Let $\mathbb{F}$ be the prime of $K$ divisible by $q$, $\beta^\mathbb{F}: G(L^\mathbb{F}/k_p) \rightarrow E$ the (prescribed) local solution monomorphism, $\sigma^\ast_L: G(L^\mathbb{F}/k_p) \rightarrow \overline{E}(q)$ the isomorphism induced
by $\sigma_L$. Then the monomorphism $\beta^\Psi \sigma_L^{x-1}: E(q) \to E$ is coherent with $\alpha$ and $\gamma$, i.e., the diagram

$$
\begin{array}{c}
I \overset{\iota}{\longrightarrow} N(q) \overset{\iota}{\longrightarrow} E(q) \overset{\iota-}{\longrightarrow} G(\Psi) \overset{\iota}{\longrightarrow} I \\
\downarrow{\alpha} \hspace{1cm} \downarrow{\beta^\Psi \sigma_L^{x-1}} \hspace{1cm} \downarrow{\gamma} \\
I \overset{\iota}{\longrightarrow} N \overset{\iota}{\longrightarrow} E \overset{\iota}{\longrightarrow} G \overset{\iota}{\longrightarrow} I
\end{array}
$$

is commutative. (Here $\iota$, $\iota$ denote their restrictions to the given subgroups.)

On the other hand, $\beta'$ restricted to $E(q)$ is a monomorphism of $E(q)$ into $E'$. Set $U_{\Psi} = \beta^\Psi G(L_{\Psi}/k_{\Psi})$; then $U_{\Psi}$ also is $\beta^\Psi \sigma_L^{x-1}E(q)$. Set $U_{\Psi}' = \beta'^E(q)$. Finally, set $\beta_{\Psi}' = \beta^\Psi \sigma_L^{x-1} \beta'^{-1}: U_{\Psi}' \to U$. By construction, the restriction of $\beta_{\Psi}'$ to $\iota N \cap U_{\Psi}'$ is the identity mapping; moreover, the diagram

$$
U_{\Psi}'/\iota N \cap U_{\Psi}' \overset{\gamma_{\Psi}}{\longrightarrow} U_{\Psi}/\iota N \cap U_{\Psi} \quad \downarrow \gamma'' \quad \downarrow \\
G' \quad \gamma' \quad G
$$

with canonical vertical arrows, and $\gamma_{\Psi}$ induced by $\beta_{\Psi}'$, is commutative. In other words, $\beta_{\Psi}'$ is the identity mapping in $\iota N$ and agrees with $\gamma''$ mod $\iota N$.

In order that $(L, \beta')$ be a solution to $P$ it is necessary and sufficient that $E = E'$ and $\gamma''$ be the identity mapping, by definition of $\beta'$ and $\gamma''$.

We now augment the set of primes $p$ used in Part I so that $(L, \beta')$ is a solution, as follows:

(i) We fix a system of generators of $G$.

(ii) For each generator $g$ of $G$ given in (i), we produce subgroups $U$ of $E$ with the following properties:

1. $g \in \iota U$.

2. If for each $U$ there is a monomorphism $\delta: U \to E'$ such that $\delta$ leaves $U \cap \iota N$ elementwise fixed and $\delta$ agrees with $\gamma''^{-1}$ mod $\iota N$, then $\gamma''^{-1}(g) = g$.

3. There is a local solution $(L_{\Psi}, \beta_{\Psi})$ to $P$ such that $U = U_{\Psi}$.

4. The prime $p$ of $k$ under $\Psi$ has not been used elsewhere. If (1)–(4) can be fulfilled, then $P$ is localizable.

To fix a system of generators of $G$ in (i), we observe that any subgroup of $\text{Out } N$ can be generated by a set of the form $\{Z\}$, $\{\Phi^i\}$, $\{\Phi^i Z\}$, or $\{\Phi^i, Z\}$, where $i | \nu$. (See Section 3.1.)
Case 1. $G = \langle \zeta \rangle$. Set $U = \langle A \rangle$, where $A = \sum_{m} (\xi_{e_{11} + e_{22}})$. Let $\xi$ a primitive $q-1$th root of unity in $GF(q)$, so that (1) is satisfied. Suppose $\delta: U \to E'$ is a monomorphism such that $\delta / U \cap N$ is the identity mapping and agrees with $\gamma^{r-i}$ mod $U \cap iN$. Then $\delta(A) = \Phi^{i}C$, $C \in Gp(2m, q)$, and $A^2 = \delta(A)^2 = (\Phi^{i}C)^2$, since $A \in N$. If $i = 0$, then since $C = \gamma^{r-i}(A) \neq 1$ and $\xi$ has order 2, we must have $C = \xi Z$ so we are done. If $i \neq 0$, then $(\Phi^{i}C)^2 = bA^2$, $0 \neq b \in GF(q)$, hence $\Phi^{i}C$ commutes with $A^2$. $(\Phi^{i})^{c-1} = (A^2)^{c-1} = A^{2p^0}$, hence $A^2$ and $A^{2p^0}$ are similar, so that $\xi^2 = \xi^{2p^0}$, $\xi^{2p^0 - a} = 1$, $\xi \in GF(p^0)$. But $i \equiv 0 \pmod{v}$, hence if $i < v$, $i = v/2$, and we have $\xi^2 \in GF(p^{2v})$ which is impossible by choice of $\xi$. Thus (2) is verified. There are, by Cebotarev's density theorem (see Section 3.3), infinitely many unramified primes $\Psi$ of $K$ whose decomposition groups $G(\Psi)$ are equal to any prescribed cyclic subgroup of $G$, in particular, to $G$ itself in this case. Since $U$ is cyclic, we can find (as in Section 3.3) a local solution $(L^{p}, B)$ to $P$ with $L^{p}/K_{p}$ unramified and $U_{Q} = U$, hence (3) is verified. (4) can be satisfied since infinitely many such $\Psi$ exist. This completes Case 1.

Case 2. $G = \langle \Phi^{i}Z \rangle$, $i | v$, $0 \leq j < 2$. We claim first that the local restrictions already imposed in Part I of the proof imply that $\gamma^{r-i}(\Phi^{i}Z) = \Phi^{i}Z^*$ for some $s$, $0 \leq s < 2$.

Proof of Claim. For $v$ odd, we may assume that $j = 0$. The group $U$ of Part I is $\langle \Phi^{i}, A \rangle$, where $A = (\xi_{p}e_{11} + \xi_{p}^{-1}e_{22}) \oplus I_{2m-2}$, $\xi_{p}$ a p'th root of unity $\neq 1$ in $GF(q)$, $p$ prime, $p | q - 1$ but $p \neq p^{0} - 1$ for $0 < r < v$. Let $\delta: U \to E'$ be a monomorphism leaving $U \cap iN$ pointwise fixed and agreeing with $\gamma^{r-i}$ mod $N$. If $\delta(\Phi^{i}) = \Phi^{i}B$ $(0 \leq r < v)$, it follows that $A^{\sigma B} = bA^{\sigma}$, $0 \neq b \in GF(q)$, $A^{\sigma B}A^{\sigma B^{-1}} = bA = A$ to the power $\Phi^{i}B^{\sigma_{-1}}$, implying $bA$ is similar to $A^{\sigma B^{\sigma_{-1}}}$. Comparing eigenvalues, we get $b = 1$, $\xi_{p} = \xi_{p}^{2t_{r}} - 1$. By choice of $p$ ($p | q - 1$, $p \neq p^{0} - 1$ for $r < v$), $-p^{0} - i$ is impossible for $r \neq i \pmod{v}$ and $-p^{0} - i$ is impossible for $v$ odd and $r \neq i \pmod{v}$.

For $v$ even, the group $U$ of Part I is contained in $\langle \Phi^{i}, A, B \rangle$ (see Part I, Subcase 2.2 above for definition of $\Phi^{i}, A, B$). The crucial relation is between $\Phi^{i}A$ or $\Phi^{i}B$, respectively, according as $j = 0$ or 1, and $A$. Suppose $\delta(\Phi^{i})$ (or $\delta(\Phi^{i}B$ respectively) $= \Phi^{i}C$. Then $A^{\Phi^{i}B} = bA^{\Phi^{i}C}$.

Comparison of element orders yields $b = 1$, and as before, $A^{\sigma_{-1}}$ is similar to $A$, implying that $A^{\sigma B^{\sigma_{-1}}}$ is similar to $A_{1}$, hence there exists $u \neq 1$ in $GF(q^{2})$ such that $u^{p} = 1$, $p | p^{0} - 1$ but not $p^{0} - 1$ for $0 < s < 2v$, and (the set) $\{ u, u^{*} \} = \{ u^{p_{0}^{s - r}}, u^{p_{0}^{s - r + v}} \}$. $u$ is distinct from all its conjugates over $GF(p_{0})$, hence $u$ equals one of the two latter powers of $u$ if and only if
\( r - i \equiv 0 \pmod{2\nu} \) or \( r - i + \nu \equiv 0 \pmod{2\nu} \), in particular, \( r \equiv i \pmod{\nu} \) as desired. The claim is proved.

We now resume the proof of Case 2. Suppose first that \( \nu/i \) is odd. Then \( (\Phi^i Z)^{2^k} = \Phi^i \) where \( 2^k \equiv 1 \pmod{\nu/i} \), hence \( \Phi^i \in G \), whence \( Z^i \in G \). But then \( G = \langle \Phi^i, Z^i \rangle \). By Case 1 we may assume \( \gamma^{s-1}(Z^i) = Z^i \). By the above claim, \( \gamma^{s-1}(\Phi^i) = \Phi^i Z^s \) \( (0 \leq s < 2) \). \( \Phi^i \) has odd order \( \nu/i \), and \( \Phi^i Z \) has even order \( 2\nu/i \), hence since \( \gamma^{s-1} \) is an isomorphism, \( s = 0 \), which means that \( \gamma^{s-1} \) is the identity mapping.

We now assume \( \nu/i \) is even. We may also assume \( p_0 \neq 2 \), since if \( p_0 = 2 \), then \( Z = 1 \) and there is nothing further to prove.

For the remainder of the proof of Case 2, we need the following two lemmas, the proofs of which are deferred until Section 4 below.

Let \( L/K \) be a finite extension of a finite field \( K \), \( G(L/K) = \langle \theta \rangle \). Let \( A \in GL(n, L) \). We denote by \( N_0 A \) the product \( A^0 A^{-1} \cdots A^0 A \), where \( r \) is the order of \( \theta \), and \( A^0 \) is the matrix obtained from \( A \) by applying \( \theta \) to the coefficients of \( A \).

**Lemma 1.** Given \( a \in L^* \) (the multiplicative group of \( L \)) there exists \( A \in GL(n, L) \), such that \( \det A = ab^{1-\theta} \) for some \( b \in L^* \), and \( N_0 A \) is an irreducible companion matrix in \( GL(n, K) \).

**Lemma 2.** Let \( N_0(AX) = bN_0 A \), where \( b \in L^* \), \( A \) and \( X \) are in \( GL(n, L) \), and \( B = N_0 A \) is a companion matrix in \( GL(n, K) \). Then \( X = cY^\theta Y^{-1} \) for some \( c \in L^* \), \( Y \in GL(n, L) \).

Now by Lemma 1, there exists a matrix \( A_1 \in GL(2, q) \) such that
\[
\det A_1 = \xi^b b^{1-p_0^i} \text{ for some } b \in GF(q)^* \text{ (where } \xi \text{ is the primitive } q-1 \text{th root of unity appearing in the matrix } Z), \text{ and } N_{\phi}(A_1) \text{ is an irreducible companion matrix in } GL(2, p_0^i). \text{ Since } 1 - p_0^i \text{ is even, we may write } \\
\det A_1 = \xi^c c, \text{ } c \in GF(q)^*. \text{ Set } A = A_1 \oplus (\oplus_{m-1}(\det A_1) e_{11} + e_{22}), \text{ and } \\
U = \langle \Phi^i A \rangle. \text{ Clearly } (1) \text{ is satisfied. Denial of (2) yields a matrix } C \text{ such that } (\Phi^i C)^{\nu/i} = (\Phi^i A)^{\nu/i}, \text{ } C \in Gp(2m, q), \text{ hence } \Phi^i C \text{ commutes with } (\Phi^i A)^{\nu/i} = N_{\phi}(A), \text{ the latter having coefficients in } GF(p_0^i), \text{ hence } C \text{ commutes with } N_{\phi}(A) = \text{ the direct sum of } N_{\phi}(A_1) \text{ with the direct sum of } m-1 \text{ copies of } (\det A_1) e_{11} + e_{22} \text{ raised to the power } (q-1)/(p_0^i - 1). \text{ It follows that } C = C_1 \oplus C_2, \text{ } C_1 \in GL(2, q), \text{ hence } N_{\phi}(C_1) = dN_{\phi}(A_1), \text{ } d \in GF(q)^*. \text{ It follows from Lemma 2 that } A_1^{-1} C_1 = d_1 Y_1^{\theta} Y_1^{-1} \text{ for some } Y_1 \in GL(2, q), \text{ } d_1 \in GF(q)^*, \text{ hence } \det C_1 = (\det A_1)(d_1^2)(\det Y_1)^{p_0^i - 1}; \text{ in particular, } \det C_1 \text{ and } \det A_1 \text{ are equal up to a square multiple in } GF(q). \text{ This implies that the multipliers } a_A \text{ and } a_C \text{ differ by a square multiplier, hence } C = A = Z^i, \text{ proving (2). (3) and (4) follow exactly as in the previous case, since } U \text{ is cyclic.} \)
Case 3. $G = \langle \Phi^i, Z \rangle$. Follows immediately from Cases 1 and 2. The proof is complete.

4. ON THE NORM FUNCTION $N_\theta$

**Lemma.** Let $K$ be a finite field, $L/K$ a finite extension with $G(L/K) = \langle \theta \rangle$, $\theta$ having order $r$. Let $n$ be a positive integer. Then every $B \in GL(n, k)$ is the norm $N_\theta A$ of some $A \in GL(n, L)$, where $N_\theta A = A^{\theta r-1} A^{\theta r-2} \cdots A^0 A$.

**Remark.** The author is indebted to the referee for pointing out that this lemma is a special case of a more general result. Namely, a field $K$ is said to have dimension $\leq 1$ if all its finite extension fields have trivial Brauer groups (finite fields have dimension $\leq 1$). Let $K$ have dimension $\leq 1$. Then for every finite commutative algebra $R/K$ and every cyclic field $L/K$, the norm $N_{L/K} : (L \otimes_K R)^* \to R^*$ is surjective. This result comes out of the theory of the Brauer group of a commutative ring which has been developed by Azumaya (On maximally central algebras, *Nagoya Math. J.* — (1951), 119–150) and Auslander and Goldman (The Brauer group of a commutative ring, *Trans. A.M.S.* — (1960), 367–409). We prove here only the lemma stated above.

**Proof of Lemma.** We first observe that $B$ is a norm if and only if every similar matrix $B^C$, $C \in GL(n, L)$, is also a norm. To see this, form the semidirect product $\langle \theta \rangle GL(n, L)$ and note that $N_\theta X = (\theta X)^r$, $X \in GL(n, L)$. Then if $B = N_\theta X$, $B^C = (N_\theta X)^C = (\theta X)^C = (\theta X)^{cr} = (\theta^C X^C)^r = (\theta C^{-r} \theta^C X^C)^r = (\theta C^{-r} \theta^C X^C)^r = N_\theta (C^{-r} \theta^C X^C)$. Hence without loss of generality, we may assume that $B$ is in rational normal form over $K$. Then $B$ is a direct sum of companion matrices to prime power polynomials, hence we may assume that $B$ is a companion matrix of $f(t)^m$, where $f(t)$ is a polynomial of degree $s$ in $K[t]$, irreducible over $K$, and $m$ is a positive integer.

For convenience, we introduce the tensor product notation for matrices. If $X$ and $Y$ and square matrices of degree $m$ and $n$ respectively over a field, then $X \otimes Y$ denotes the square matrix of degree $mn$, which when looked at as a block matrix of degree $n$ with $m$ by $m$ components, its $i, j$th block is the product of $X$ with the $i, j$th component of $Y$.

$B$ can be transformed into $A \otimes I_m + I_s \otimes N_m$, where $N_m$ denotes the standard nilpotent matrix $e_{12} + e_{23} + \cdots + e_{m-1,m}$ of degree $m$ (here $e_{ij}$ has degree $m$), and $A$ is a companion matrix of $f(t)$. (See e.g. [5, Theorem 6, p. 115].)

We may therefore transform $B$ into $A \otimes (I_m + N_m)$, by transforming the normal form $A \otimes I_m + I_s \otimes N_m$ by the matrix $I_s \otimes e_{11} + A \otimes e_{28} +$
It is easy to verify that the norm distributes over the tensor product that is, \( \mathcal{N}_\rho(X \otimes Y) = \mathcal{N}_\rho(X) \otimes \mathcal{N}_\rho(Y) \) for any square matrices \( X, Y \) over \( L \). Therefore it suffices to prove that \( B \) is a norm in the following two special cases.

**Case 1.**

\( B \) is a companion matrix of a polynomial \( f(t) \in K[t] \), irreducible in \( K[t] \).

**Case 2.** \( B = I \) + \( N_m \).

We treat first Case 1. Let \( n \) now denote the degree of \( f(t) \). Let \( f(t) = f_1(t) \cdots f_s(t) \) be the complete factorization of \( f(t) \) in \( L[t] \). We may assume \( f_i(t) = f_i(t)^{p^{s_i}} \), \( i = 1, \ldots, s \). We have \( s = \text{gcd}(n, r) \). Transform \( B \) into \( B_1 \otimes e_{11} + B_2 \otimes e_{22} + \cdots + B_s \otimes e_{ss} \), where the \( e_{ii} \) have degree \( s \) and \( B_i \) is a companion matrix of \( f_i(t) \), \( i = 1, \ldots, s \). (This is possible since \( \text{gcd}(f_i(t), f_j(t)) = 1 \) for \( i \neq j \).)

Let \( M \) be the splitting field of \( f(t) \) over \( K \). We then have \([L \cap M : K] = s, [M : L \cap M] = n/s, [L : L \cap M] = r/s, \) and \( B_i \in GL(n/s, L \cap M) \). We show first that \( B_i \) is a norm from \( L \) into \( L \cap M \); i.e., \( B_i = \mathcal{N}_\rho(A_i) \) for some \( A_i \in GL(n/s, L) \). Let \( u_1, \ldots, u_{n/s} \) be a basis of \( M \) over \( L \cap M \). Then \( u_1, \ldots, u_{n/s} \) is also a basis of \( LM \) over \( L \). We may extend \( \theta^s \) to an automorphism \( (\theta^s)^* \) of \( LM \) such that \( (\theta^s)^* \) leaves \( M \) pointwise fixed. Let \( R \) be the regular representation of \( LM \) over \( L \) with respect to the basis \( u_1, \ldots, u_{n/s} \). Then we may assume \( B_1 = R(b), b \in M \). We know \( b = N_{(\theta^s)^*}(a) \) for some \( a \in LM \). Let \( A_1 = R(a) \). Then \( N_{\theta^s}(A_1) = N_{\theta^s}(R(a)) = R(a)^{p^{(r/s)-1}} \cdots R(a)^{p^{r/s}} R(a) \). This last is equal to \( R(a^{(\theta^s)^*}((r/s)-1) \cdots R(a^{(\theta^s)^*}) R(a) \) since if \( au_i = \Sigma_j a_iu_j \), then

\[
(a^{(\theta^s)^*}u_i = (au_i)^{\theta^e^*} = \left( \sum_j a_{ij}u_j \right)^{\theta^e^*} = \sum_j a_{ij}^{\theta^e^*}u_j = \sum_j a_{ij}^e u_j.
\]

Hence the norm expression becomes \( R(N_{(\theta^s)^*}(a)) = R(b) = B_1 \).

Now let \( X = A_1 \otimes e_{11} + I_{n/s} \otimes e_{22} + \cdots + I_{n/s} \otimes e_{ss} \) \( (\rho GL(n, L)), \)
\( P = I_{n/s} \otimes (e_{12} + e_{20} + \cdots + e_{s-1,s} + e_{ss}) \) \( (\rho GL(n, L)), \)
\( A = PX \). We claim \( N_{\rho^s}(A) = N_{\rho^s}(PX) = (\theta^s)^{(r/s)} \). \( (\theta^s)^{(r/s)} \) \( X^{\theta^e^s-1}X^{\theta^e^s-2} \cdots X^{\theta^e}X \). Hence

\[
(\theta^s)^{(r/s)} = (\theta^e \cdot X^{\theta^e^s-1}X^{\theta^e^s-2} \cdots X^{\theta^e}X)^{(r/s)}
\]

\[
= N_{\rho}(X^{\theta^e^s-1}X^{\theta^e^s-2} \cdots X^{\theta^e}X)
\]

\[
= N_{\rho}(X^{\theta^e^s-1})N_{\rho}(X^{\theta^e^s-2}) \cdots N_{\rho}(X^{\theta^e})N_{\rho}(X) = B.
\]

This completes the proof of Case 1. We now prove Case 2.
Let \( a \in L \), \( S_\theta(a) = 1 \), where \( S_\theta \) denotes the trace function. Let \( A_1 = I_m + aN_m \). We observe that \( A_1^\theta = I_m + a^\theta N_m \in L[N_m], \) \( i = 1, \ldots, r \).

\[
N_\theta(A_1) = \prod \{ A_1^\theta r^{-1} \mid 1 \leq i \leq r \} = \prod \{ I_m + a^\theta r^{-1} N_m \mid 1 \leq i \leq r \}
\]

\[= I_m + N_m \text{ (modulo } N_m^2).\]

Suppose inductively that \( N_\theta(A_i) = I_m + N_m \) (modulo \( N_m^{i+1} \)), \( i \geq 1 \).
Let \( A_{i+1} = A_i + bN_{m+1} \), \( b \in L \) to be determined.

\[
N_\theta(A_{i+1}) = N_\theta(A_i) + S_\theta(b) N_m^{i+1} \text{ (modulo } N_m^{i+2}).
\]

Since \( N_\theta(A_i) \) is fixed by \( \theta \), \( N_\theta(A_i) = I_m + N_m + cN_m^{i+1} \) (modulo \( N_m^{i+2} \)), \( c \in K \). Hence \( N_\theta(A_{i+1}) = I_m + N_m + cN_m^{i+1} + S_\theta(b) N_m^{i+1} \) (modulo \( N_m^{i+2} \)).

We therefore choose \( b \) so that \( S_\theta(b) = -c \). When \( i = m - 1 \), \( N_{m+1} = N_m^m = 0 \), hence setting \( A = A_{m-1} \), we have \( N_\theta(A) = I_m + N_m \), completing the proof.

Remark. A theorem of Specht [4] states that if \( L/K \) is any separable cyclic extension of a field \( K \), then for \( X, Y \in GL(n, L) \), \( N_{\theta}X \) is conjugate to \( N_{\theta}Y \) if and only if \( X \) and \( Y \) are \( \theta \)-equivalent,” i.e., there exists \( \gamma \in GL(n, L) \) such that \( Y = \gamma^{-\theta}X\gamma \), or what is the same thing, \( \gamma Y = Z^{\theta}XZ \). In particular, let \( X = I_n \). Then, if \( N_{\theta}(Y) = I_n \) we have \( Y = Z^{\theta}Z \). Conversely, \( N_{\theta}(Z^{\theta}Z) = (\theta Z^{\theta}Z)^r = (\theta^{r-1}Z^{-1}\theta Z)^r = (Z^{-1}\theta Z)^r = I_n \). Thus the statement about elements of \( L^* \) with norm \( =1 \) also generalizes to \( GL(n, L) \).

Lemma 1 of Section 3.4. Given \( a \in L^* \), there exists \( A \in GL(n, L) \) such that \( \det A = ab^{1-\theta} \) for some \( b \in L^* \), and \( N_{\theta}A \) is an irreducible companion matrix in \( GL(n, K) \).

Proof. Let \( B \) be an irreducible companion matrix in \( GL(n, K) \) such that \( \det B = N_{\theta}a \) (ordinary norm). By the preceding lemma, \( B = N_{\theta}A \) for some \( A \in GL(n, L) \). Furthermore, \( N_{\theta}(\det A) = \det N_\theta A = \det B = N_\theta a \), hence \( \det A = ab^{1-\theta} \) for some \( b \in L^* \).

Lemma 2 of Section 3.4. Let \( N_{\theta}(AX) = bN_{\theta}A \), where \( b \in L^* \), \( A \) and \( X \) are in \( GL(n, L) \), and \( B = N_{\theta}A \) is a companion matrix in \( GL(n, K) \). Then \( X = cY^\theta Y^{-1} \) for some \( c \in L^* \), \( Y \in GL(n, L) \).

Proof. We have \((\theta AX)^r = b(\theta A)^r\), so that \( \theta AX \) commutes with \( bB \) hence with \( B \). \( B \in GL(n, K) \), \( B^\theta = B \), hence both \( A \) and \( X \) are contained in the commutative ring \( L[B] \); hence \( AX =XA \). It follows that \( N_{\theta}(AX) = N_{\theta}A \cdot N_{\theta}X = bN_{\theta}A \) whence \( N_{\theta}X = bI \). In particular, \( b^\theta = b \),
localizability of embedding problem

5. a local embedding problem

Theorem. (See Section 3.3 above.) Let k be a local $\wp$-adic field, $K/k$ a tamely ramified Galois extension of degree ef, where $e = e(K/k)$, $f = f(K/k)$ are the ramification index and residue class degree, respectively, $\gamma: G(K/k) \rightarrow G$ an isomorphism, $N$ a cyclic group of order $p$, where $p$ is the characteristic of the residue class field of $k$. Let $\Sigma$ be an extension of $N$ by $G$: $1 \rightarrow N \rightarrow E \rightarrow G \rightarrow 1$ such that the subgroup of $G$ corresponding under $\gamma$ to the inertia group of $G(K/k)$ acts trivially on $N$; i.e., if $G_1$ is the inertia group of $G = G(K/k)$, then $G_1 = \gamma(G_1)$ acts trivially on $N$.

Then the embedding problem $P = P(K/k, \Sigma, \gamma)$ has a proper solution.

Proof. $e - \text{order of } G_1$, is prime to $p$ hence the centralizer of $iN$ in $E$ contains a subgroup $H_1 \approx G_1$ such that $eH_1 = G_1$, $H_1$ is normal in $E$, and $H_1 \cap iN = 1$. We factor off the subgroup $H_1$ and consider the resulting embedding problem $P' = P(K'/k, \Sigma', \gamma')$, where $K'$ is the inertia field of $K/k$, $\Sigma'$ is the extension $1 \rightarrow N \rightarrow E' \rightarrow G' \rightarrow 1$ obtained by factoring out $H_1 : E' = E/H_1, G' = G/G_1, G_1 = G(K'/k)$, $\gamma': G' \rightarrow G'$ induced by $\gamma$. By Theorem 3.1 of [3, p. 131], $P$ has a proper solution if and only if $P'$ has a proper solution $(L', \beta')$ satisfying $L' \cap K = K'$. We observe that any solution $L'$ to $P'$ will (automatically satisfy the condition $L' \cap K = K'$, since $e$ and $p$ are relatively prime. We now drop the prime symbol ('') and assume $P = P'$.

We next perform a further reduction to the case $\Sigma$ is a split extension. If $\Sigma$ is not a split extension, then let $U$ be a cyclic subgroup of $E$ such that $U \cdot iN = E$, $(G$ is now assumed to be cyclic) and construct the “splitting expansion” $E^*$, the semidirect product of $U$ with $N$, where the action of $U$ on $N$ is given by $u^n = u^{-1}(u^{-1}(u(n)) u)$ for $n \in N, u \in U$. Consider first the embedding problem $P_1 = P(K/k, \Sigma_1, \gamma)$ where $\Sigma_1$ is the sequence $1 \rightarrow iN \cup U \rightarrow U \rightarrow G \rightarrow 1$. Since $U$ is cyclic, and $K/k$ is now assumed to be unramified, $P_1$ has a proper solution $(L_1, \beta_1)$ with $L_1/k$ unramified. (See, e.g., [3, p. 434].)

We consider next the embedding problem $P_2 = P(L_2/k, \Sigma_2, \beta_2)$, where $\Sigma_2$ is the sequence $1 \rightarrow N \rightarrow E^* \rightarrow U \rightarrow 1$, where $i^*, e^*$ are the canonical mappings associated with the semidirect product. If $P_2$ has a proper solution $(L_2, \beta_2)$, then by Theorem 2.1 in [3, p. 415], the epimorphism of $E^*$ onto $E$ given by $(u, n) \mapsto un (n \in N, u \in U)$ yields a subfield.
L of \( L_2 \) which is a solution field to \( P \). We may therefore assume that \( \Sigma \) splits.

We identify \( \mathcal{G} \) with \( G(K/k) \), where \( K, k \) are the residue class fields of \( K, k \) respectively. The multiplicative group \( K^* \) of \( K \) can be written as

\[
K^* = \langle \pi \rangle \times W \times U^{(1)},
\]

where \( \pi \) is a prime element of \( k \), \( W \) is the group of roots of unity in \( K \) of order prime to \( p \), and \( U^{(1)} \) is the group of units of \( K \) congruent to \( 1 \) mod \( \pi^t \).

The isomorphism \( \sigma_0 \) of \( K^+ \) (additive group of \( K \)) onto \( U^{(1)}/U^{(2)} \) given by \( \sigma_0(a) = 1 + a\pi \) mod \( U^{(2)} \) is a \( \mathcal{G} \)-mapping. Prolong \( \sigma_0 \) to a \( \mathcal{G} \)-isomorphism

\[
\sigma : K^+ \rightarrow K^*/H'' ,
\]

where \( H'' = \langle \pi \rangle WU^{(2)} \), and \( \sigma \) is the composite of \( \sigma_0 \) and the canonical isomorphism from \( U^{(1)}/U^{(2)} \) to \( K^*/H'' \).

By local class field theory, \( H'' \) is the norm group of its class field \( L'' \supset K \), and the reciprocity map

\[
\tau : K^*/H'' \rightarrow \overline{N}^* = G(L/K)
\]

is a \( \mathcal{G} \)-isomorphism, since \( H'' \) is \( \mathcal{G} \)-invariant. By the normal basis theorem, \( K^+ \) is a \( \mathcal{G} \)-regular module, i.e.,

\[
K^+ = \oplus \{ A^g \mid g \in \mathcal{G} \} , \quad \text{where } A \approx K^+.
\]

It follows that \( \overline{N}^* \) is \( \mathcal{G} \)-regular so that the cohomology groups \( H^i(\mathcal{G}, \overline{N}^*) = 0 \) for all \( i \). In particular, \( \mathbb{E}^* = G(L^*/k) \) is (group-theoretically) a uniquely determined split extension of \( \overline{N}^* \) by \( \mathcal{G} \). Let \( J_0 \) be a subgroup of \( A \) with \( [A : J_0] = p \). Then \( J = \oplus \{ J_0^g \mid g \in \mathcal{G} \} \) is a \( \mathcal{G} \)-submodule of \( K^+ \).

Let \( H' \) be the subgroup of \( K^* \) corresponding to \( J \) under \( \sigma \), so that \( K^*/H' \) is \( \mathcal{G} \)-isomorphic to \( K^+/J \). Let \( L' \) be class field to \( H' \), \( \overline{N}' = G(L'/K) \), \( E' = G(L'/k) \). (\( L'/k \) is normal since \( H' \) is \( \mathcal{G} \)-invariant.) Since \( K^*/H' \) is \( \mathcal{G} \)-regular, \( E' \) is a uniquely determined split extension of \( \overline{N}' \) by \( \mathcal{G} \). We now produce a natural operator epimorphism \( \mu \) from \( \overline{N}' \) onto \( N \) which extends to an epimorphism \( \mu' \) of \( E' \) onto \( E \). \( \overline{N}' \) is the direct product \( \prod \{ B^g \mid g \in \mathcal{G} \} \), where \( B \) is cyclic of order \( p \), say \( B = \langle x \rangle \). Let \( N = \langle y \rangle \).

Define \( \mu(x^g) = y^{\gamma(g)} \) (\( g \in \mathcal{G} \)). It is easy to verify that \( \mu \) determines a \( \gamma \)-epimorphism of \( \overline{N}' \) onto \( N(\mu(z^g) = \mu(z)^{\gamma(g)} \), for all \( z \in \overline{N}' \), \( g \in \mathcal{G} \).

Write \( E' = \overline{U} \overline{N}' \), \( \overline{U} \cap \overline{N}' = 1 \), \( E = UN \), \( U \cap N = 1 \). For \( uz \in E' \),
u \in U, z \in \overline{N}', define \mu'(uz) = \gamma'(u) \mu(z), where \gamma': \overline{U} \to U is an isomorphism such that the diagram

\[
\begin{array}{ccc}
\overline{U} & \xrightarrow{\text{Res}} & \overline{G} \\
\gamma' \downarrow & & \downarrow \gamma \\
U & \xrightarrow{\mu} & G
\end{array}
\]

commutes. \mu and \mu' have the same kernel. Let \( L \) be the subfield of \( L' \) fixed by the kernel of \mu', \( E = G(L/k) \). Then \mu' factors naturally:

\[
E' \xrightarrow{\text{Res}} E \xrightarrow{\beta} E.
\]

\((L, \beta)\) is the desired solution to \( P \). Q.E.D.

Remark. This theorem also holds when \( N \) is an elementary abelian \( p \)-group of rank \( f(k/Q_n) = [k: \mathbb{Z}/p\mathbb{Z}] \); the proof is essentially the same.

REFERENCES