ISRAEL JOURNAL OF MATHEMATICS **145** (2005), 93–112

GALOIS EMBEDDING PROBLEMS WITH CYCLIC QUOTIENT OF ORDER p

BY

JÁN MINÁČ*†

Department of Mathematics, Middlesex College, University of Western Ontario
London, Ontario N6A 5B7, Canada
e-mail: minac@uwo.ca
URL: http://www.math.uwo.ca/minac.html

AND

JOHN SWALLOW‡

Department of Mathematics, Davidson College
Box 7046, Davidson, NC 28035-7046, USA
e-mail: joswallow@davidson.edu
URL: http://www.davidson.edu/math/swallow/

ABSTRACT

Let K/F be a cyclic field extension of odd prime degree. We consider Galois embedding problems involving Galois groups with common quotient $\mathrm{Gal}(K/F)$ such that corresponding normal subgroups are indecomposable $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-modules. For these embedding problems we prove conditions on solvability, formulas for explicit construction, and results on automatic realizability.

* Research supported in part by the Natural Sciences and Engineering Research Council of Canada grant R0370A01, as well as by the special Dean of Science Fund at the University of Western Ontario.

† Supported by the Mathematical Sciences Research Institute, Berkeley.

‡ Research supported in part by National Security Agency grant MDA904-02-1-0061.

Received December 10, 2003 and in revised form April 6, 2004

Introduction

Let $p > 2$ be a prime, and suppose that K/F is a cyclic field extension of degree p. In this paper we consider Galois embedding problems involving Kummer extensions of K of degree p^n that are Galois over F, and we establish new automatic realizability results, whereby the solvability of one Galois embedding problem implies the solvability of another. (See e.g. [GSS, Section 5] for some automatic realizations of 2-groups as Galois groups.) We restrict ourselves to the case $p > 2$ because the case $p = 2$ is quite simple and does not lead to new results.

We focus particularly on the case when F contains a primitive pth root of unity. In fact, this paper is a continuation of [MS] wherein, under this hypothesis, we classified $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-modules $K^\times/K^{\times p}$ using arithmetic invariants attached to K/F, and the investigations there were motivated by the embedding problems solved in this paper. When F is not of this type, we employ a descent argument in the case $\mathrm{char}\, F \neq p$ and Witt's Theorem in the case $\mathrm{char}\, F = p$ to extend our results to arbitrary fields.

When F contains a primitive pth root of unity, we additionally provide explicit solutions of some Galois embedding problems, and we show that these formulas are natural and quite transparent consequences of our method. For most of these embedding problems, explicit solutions were not previously known. For others, such as the example of Section 1, our methods yield an explanation of explicit solutions determined previously via ad hoc methods.

In Section 1 we present a motivating example and our Main Theorem on automatic realizability and explicit solution. In Section 2 we introduce notation and results in preparation for Section 3, where we give conditions and explicit solutions for a class of embedding problems under the hypothesis that a primitive pth root of unity lies in the base field. In Section 4 we use a descent argument and Witt's Theorem to establish equivalent conditions for embedding problems over all fields, and in Section 5 we prove our Main Theorem. Although this paper uses ideas and results developed in [MS] and in [W], we decided to make our paper largely self-contained, and hence we make minimal references to results in [MS] and [W].

1. Example and Main Theorem

A simple example serves as a motivating introduction to Galois embedding problems of the type we will consider. Assume that F contains a primitive pth root of unity ξ_p and $K = F(\sqrt[p]{a})$ is a cyclic extension of degree p, and consider

Heisenberg's group E, a noncommutative group of order p^3 and exponent p. These conditions determine E up to isomorphism. The center of E is cyclic of order p, and we have the following short exact sequence:

$$1 \to \mathbb{Z}/p\mathbb{Z} \to E \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to 1. \tag{1}$$

Now let L/K be an extension Galois over F such that $\mathrm{Gal}(L/F) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then the exact sequence naturally gives rise to a Galois embedding problem, asking whether L embeds in a Galois extension $\tilde{L}/F$ with group E and such that the surjection in the exact sequence is the surjection of Galois theory.

The obstruction to the solvability of this embedding problem may be computed as follows. Assume that $K = F(\sqrt[p]{a})$ is contained in L. Fix a primitive root ξ_p. By Kummer theory there exist elements $\sigma, \tau \in \mathrm{Gal}(L/F)$ and $b \in F^\times$ such that $\sqrt[p]{a}^{\sigma-1} = \xi_p = \sqrt[p]{b}^{\tau-1}$ and $\sqrt[p]{b}^{\sigma-1} = 1 = \sqrt[p]{a}^{\tau-1}$. Then the lifts of σ and τ in E generate E. It is well-known that the Galois embedding problem admits a solution if and only if $b \in N(K^\times)$, where N denotes the norm map from K to F. (See, for instance, [JLY, page 161].)

Moreover, if we suppose that $\omega \in K$ satisfies $N(\omega) = b$, then it has been observed in [Ma, Cor. p. 523 & Thm. 3(A)] (see also [JLY, page 161]) that all field extensions $\tilde{L}/F$ solving the Galois embedding problem may be written $\tilde{L} = L(\sqrt[p]{f\alpha})$, where $f \in F^\times$ and $\alpha = \omega^{p-1}\sigma(\omega)^{p-2} \cdots \sigma^{p-2}(\omega)$.

In our Main Theorem we generalize and motivate both the condition on solvability and the form of the solution. The condition implies that a new automatic realizability result holds for fields containing ξ_p, and we extend the automatic realizability result to all fields F. Further generalizations and explicit solutions appear in Theorems 2, 3, and 4.

Observe that in the example above L and $\tilde{L}$ are Kummer extensions of K of pth-power degree that are Galois over F, and the Galois groups $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(\tilde{L}/K)$ are naturally acted upon by $\mathrm{Gal}(K/F)$. The appropriate context for our results turns out to be Kummer extensions L of K such that $\mathrm{Gal}(L/K)$ is an indecomposable $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module; as we show later in Proposition 2, any Kummer extension of K of degree p^n that is Galois over F decomposes into a compositum of extensions L/F of this type.

Let F be an arbitrary field, and suppose that K/F is a cyclic extension with Galois group $G = \mathrm{Gal}(K/F) \cong \mathbb{Z}/p\mathbb{Z}$, with generator σ. Let $A = \bigoplus_{j=0}^{p-1} \mathbb{F}_p \tau^j$ be a free $\mathbb{F}_p[G]$-module on the generator τ, where σ acts by multiplication by τ. Let A_i be the $\mathbb{F}_p[G]$-submodule generated by $(\tau - 1)^i$. (See Section 2 for details.)

Finally let $\mathcal{E}_i$, $1 < i \leq p$, denote the following Galois embedding problem:

$$\mathcal{E}_i: \quad 1 \to A_1/A_i \to (A/A_i) \rtimes G \to (A/A_1) \rtimes G = \mathrm{Gal}(L/F) \to 1.$$

Observe that $A/A_1 \cong \mathbb{F}_p$, a trivial $\mathbb{F}_p[G]$-module; hence

$$(A/A_1) \rtimes G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

We also assume that the projection of $(A/A_1) \rtimes G = \mathrm{Gal}(L/F)$ onto G coincides with the restriction map $\mathrm{Gal}(L/F) \longrightarrow G = \mathrm{Gal}(K/F)$. Assume now that $\mathrm{char}\, F \neq p$. Then $[L : F]$ and $[F(\xi_p) : F]$ are coprime. Therefore $\mathrm{Gal}(L/F)$ is naturally isomorphic to $\mathrm{Gal}(L(\xi_p)/F(\xi_p))$. After identifying these two Galois groups we set $F(\xi_p, \sqrt[p]{b})$ to be the fixed field of $1 \rtimes G$ in $L(\xi_p)$. (Here b is a suitable element in $F(\xi_p)^\times$.)

Further observe that in the case $i = 2$, $(A/A_2) \rtimes G \cong E$. Hence $\mathcal{E}_2$ is precisely the embedding problem in equation (1) above.

In the following theorem we consider the embedding problems $\mathcal{E}_i$ where $i = 2, \ldots, p$. We prove:

THEOREM 1 (Main Theorem):

(A) *Let F be an arbitrary field. Then the following are equivalent:*

(1) *Some $\mathcal{E}_i$ is solvable.*

(2) *Each $\mathcal{E}_i$ is solvable.*

Consequently, if $(A/A_2) \rtimes G$ occurs as a Galois group over F, then $(A/A_i) \rtimes G$ occurs as well, for all $2 \leq i \leq p$.

(B) *Now assume that $\mathrm{char}\, F \neq p$. Then (1) and (2) are also equivalent to*

(3) $b \in N_{K(\xi_p)/F(\xi_p)}(K(\xi_p)^\times)$.

(C) *Now assume further that $\xi_p \in F$. Suppose that (1)–(3) hold, and let $\omega \in K^\times$ satisfy $N(\omega) = b$. Suppose $i > 2$. Then a solution to $\mathcal{E}_i$ is given by*

$$\tilde{L} = K(\sqrt[p]{f\omega^{(\sigma-1)p^{-i}}}, \sqrt[p]{\omega^{(\sigma-1)p^{-i+1}}}, \ldots, \sqrt[p]{\omega^{(\sigma-1)p^{-2}}}),$$

$f \in F^\times$. If $i = 2$ then a solution to $\mathcal{E}_2$ is given by

$$\tilde{L} = K(\sqrt[p]{f\omega^{(\sigma-1)(p-2)}}).$$

Moreover, all solutions of $\mathcal{E}_i$ arise in this way.

In particular, we have the following automatic realization of Galois groups: **if $E = (A/A_2) \rtimes G$ is a Galois group over F, $\mathbb{F}_p[G] \rtimes G$ is a Galois group over F.**

The explicit construction result in the theorem says that in the case $\xi_p \in F$, solutions of $\mathcal{E}_i$ are parameterized by ω with $N(\omega) = b$ and $f \in F^\times$. Note that in $\mathbb{F}_p[G]$ we have the identity

$$(\sigma - 1)^{p-2} = (p-1) + (p-2)\sigma + \cdots + \sigma^{p-2},$$

so the construction of $\tilde{L}$ in the theorem above is equivalent to that of [JLY, page 161] in the case $i = 2$.

2. Preliminaries

In this Section and Section 3 we assume that F is a field containing a primitive pth root of unity ξ_p, $K = F(\sqrt[p]{a})$, and $G = \mathrm{Gal}(K/F) \cong \mathbb{Z}/p\mathbb{Z}$. We let σ denote the generator of G such that $\sqrt[p]{a}^{\sigma-1} = \xi_p$. Since $\sigma - 1$ is used frequently, we use the abbreviation $\rho := \sigma - 1$. All modules and Galois extensions will be acted upon on the left by their respective groups, even though we will use exponential notation to denote Galois action on fields. We denote by $F^\times$ the multiplicative group of a field F, and we write $N = N_{K/F}$ for the norm map from K to F. For a subset S of an $\mathbb{F}_p$-module V we denote by $\langle S \rangle$ the $\mathbb{F}_p$-span of S in V.

2.1. $\mathbb{F}_p[G]$-MODULES. Let $A = \bigoplus_{j=0}^{p-1} \mathbb{F}_p \tau^j$ be a free $\mathbb{F}_p[G]$-module on the generator τ, where σ acts by multiplication by τ. There are p quotient modules $A/A_i, i = 1, \ldots, p$ of A where for $i < p$,

$$A_i = \langle (\tau-1)^i, (\tau-1)^{i+1}, \ldots, (\tau-1)^{p-1} \rangle, \quad \text{and} \quad A_p = \{0\}.$$

These quotients are all cyclic and together form a complete set of indecomposable $\mathbb{F}_p[G]$-modules. Each A/A_i is of dimension i as a vector space over $\mathbb{F}_p$. We call this dimension the **length**, and denote the length of a cyclic $\mathbb{F}_p[G]$-module M by $l(M)$, because we have the following criterion for $l(M)$, where M is a cyclic $\mathbb{F}_p[G]$-module generated by m: $l(M) = i$ such that $\rho^i m = 0$, $\rho^{i-1} m \neq 0$. Moreover, such a cyclic module M of length l contains precisely one submodule of each length $1 \leq j \leq l$: $M_i = \langle \rho^{l-j} m, \ldots, \rho^{l-1} m \rangle$.

For each $i \in \{1, \ldots, p\}$ we pick a basis $\{1, \overline{\tau - 1}, \ldots, \overline{(\tau-1)}^{i-1}\}$ of A/A_i consisting of images of $1, \tau - 1, \ldots, (\tau-1)^{i-1}$. We define an $\mathbb{F}_p$-linear map λ: $A/A_i \longrightarrow \mathbb{F}_p$ by $\lambda(f_0 + f_1\overline{(\tau-1)} + \cdots + f_{i-1}\overline{(\tau-1)}^{i-1}) = f_{i-1}$, where $f_k \in \mathbb{F}_p, k = 0, \ldots, i-1$. Observe that $\ker(\lambda)$ contains no nonzero ideal of A/A_i. Then $B(a,b) := \lambda(ab)$ for each $a, b \in A/A_i$ defines a nonsingular, symmetric bilinear form B: $A/A_i \times A/A_i \longrightarrow \mathbb{F}_p$. Thus A/A_i is a symmetric algebra. (See [La, page 442].) Further we have $B(a^\sigma, b^{\sigma^{-1}}) = B(a,b)$ for each $a, b \in A/A_i$ and

our bilinear form B induces a G-equivariant isomorphism between A/A_i and its dual.

2.2. GROUPS. In this section we classify the groups of interest in this paper and the surjections among them. For $e \in \mathbb{F}_p$, let $B_{i,e}$ be the group extension of A/A_i by G with $\tilde{\sigma}^p = e(\widetilde{\tau - 1})^{i-1}$. Here $\tilde{\sigma}$ is a lift in $B_{i,e}$ of $\sigma \in G$. Note that for $e = 0$, $B_{i,0} = (A/A_i) \rtimes G$. First we consider the equivalence classes of these groups.

LEMMA 1 (see [W, Theorem 2]):

(1) *If H is a group with a normal subgroup isomorphic to A/A_i as a G-module, with quotient group G, then $H = B_{i,e}$ for some e.*
(2) *For fixed $1 \leq i < p$, all $B_{i,e}$, $e \neq 0$, are isomorphic, and these groups are not isomorphic to $B_{i,0} = (A/A_i) \rtimes G$.*
(3) *For $i = p$, all $B_{i,e}$ are isomorphic to $B_{p,0} \cong \mathbb{F}_p[G] \rtimes G$.*

The Galois embedding problems in this paper consist of embedding an extension L/F with group $B_{j,e'}$ in an extension with strictly larger group $B_{i,e}$. We are interested in all surjections $B_{i,e} \to B_{j,e'}$ for which the kernel lies in $A/A_i \subset B_{i,e}$ and which are induced by the projection of $B_{i,e}$ on its quotient. We call these G-surjections.

LEMMA 2: *The G-surjections in the set of groups $\{B_{i,e}\}_{i \geq 1}$ are precisely*

$$B_{i,e} \to B_{j,0}, \quad i > j \geq 1, \ e \in \mathbb{F}_p, \quad \text{with kernel } A_j/A_i.$$

Proof: Considering the dimensions of A/A_i and A/A_j, if $B_{i,e} \to B_{j,e'}$ is a G-surjection then $i > j$. Now a surjection of G-modules A/A_i to A/A_j must have as kernel an $\mathbb{F}_p[G]$-submodule of A/A_i of $\mathbb{F}_p$-rank $i - j$. But since A/A_i is cyclic, there is precisely one such submodule, namely A_j/A_i. Hence $(\widetilde{\tau - 1})^k$ lies in the kernel for all $j \leq k < i$. In particular, the kernel must contain $e(\tau - 1)^{i-1}$, which is $\tilde{\sigma}^p$ in $B_{i,e}$. Therefore $\tilde{\sigma} \in B_{i,e}$ is sent to some lift $\hat{\sigma} \in B_{j,e'}$ of $\sigma \in G$ and hence $\hat{\sigma}^p = 1$ in $B_{j,e'}$, or $e' = 0$. ∎

We list some characteristics of the groups $B_{i,e}$. Each $B_{i,e}$ has order p^{i+1}, nilpotent index i, and rank (the smallest number of generators) 2. The exponent of $B_{i,0}$ is p, and the exponent of $B_{i,e}, e \neq 0$ is p^2. The Frattini subgroup $\Phi(B_{i,e})$ of $B_{i,e}$ is $A_1/A_i \cong (\mathbb{Z}/p\mathbb{Z})^{i-1}$. Finally, we have presentations

$$B_{i,0} = \langle \sigma, \{\tau_j\}_{j=0}^{i-1} : \sigma^p = \tau_j^p = [\sigma, \tau_{i-1}] = 1; \text{ for } j < i-1, \ [\sigma, \tau_j] = \tau_{j+1} \rangle$$

and, for $e \not\equiv 0 \bmod p$,

$$B_{i,e} = \langle \sigma, \{\tau_j\}_{j=0}^{i-1} : \sigma^p = \tau_{i-1}^e; \tau_j^p = [\sigma, \tau_{i-1}] = 1; \text{ for } j < i-1, \ [\sigma, \tau_j] = \tau_{j+1} \rangle.$$

2.3. EXTENSIONS AND SUBMODULES, $\xi_p \in F$. Now let J denote the $\mathbb{F}_p[G]$-module $J := K^\times/K^{\times p}$. We denote elements of J by $[\gamma]$, $\gamma \in K^\times$. Let J_i be the kernel of the endomorphism $(\sigma - 1)^i$ and let M_γ be the cyclic submodule of J generated by $[\gamma]$. Then $[\gamma] \in J_i$ if and only if $l(M_\gamma) \leq i$.

We denote by $M \leftrightarrow L_M$ the Kummer correspondence over K of subspaces M of the $\mathbb{F}_p$-vector space J and abelian exponent p extensions L_M of K:

$$M = (L_M^{\times p} \cap K^\times)/K^{\times p} \quad \leftrightarrow \quad L_M = K(\sqrt[p]{\gamma}\colon [\gamma] \in M).$$

Set $C = \mathrm{Gal}(L_M/K)$. Then M and C are dual G-modules and the canonical duality $\langle m, c\rangle := c(\sqrt[p]{m})/\sqrt[p]{m}$ of M and C is G-equivariant. (See [W, pages 134 and 135].) The following proposition rephrases the results in [W, page 135] in our notation.

PROPOSITION 1: *Under the Kummer correspondence above,*

(1) *L_M is Galois over F if and only if M is an $\mathbb{F}_p[G]$-submodule of J.*

(2) *The following are equivalent:*

  (a) *L_M is the Galois closure, over F, of $K(\sqrt[p]{\gamma})$ for some $\gamma \in K^\times$;*

  (b) *$M = M_\gamma$ for some $\gamma \in K^\times$;*

  (c) *$\mathrm{Gal}(L_M/K) \cong A/A_i$, as G-modules, for some i;*

  (d) *$\mathrm{Gal}(L_M/F) \cong B_{i,e}$, as G-extensions, for some i and e.*

If these conditions hold, then $i = l(M)$ and

$$L_M = K(\sqrt[p]{\gamma}, \sqrt[p]{\gamma^\rho}, \ldots, \sqrt[p]{\gamma^{\rho^{i-1}}}).$$

Proof: Because L_M is Galois if and only if each automorphism of K extends to an automorphism of L_M, item (1) and (a)$\Leftrightarrow$(b) follow. That (c)$\Leftrightarrow$(d) follows from Lemma 1.

Suppose (b) holds. Then $M \cong A/A_i$ for some $i \in \{1, \ldots, p\}$ and $\mathrm{Gal}(L_M/K)$ is a G-equivariant dual of M. Since M is a G-equivariant self-dual module, we see that $\mathrm{Gal}(L_M/K)$ and A/A_i are G-isomorphic and (c) follows.

Suppose now that (c) holds. Then again using the G-equivariant self-duality of A/A_i and Kummer theory, we see that M must be a cyclic module M_γ for some $\gamma \in K^\times$. Hence (b) follows.

The presentation of L_M follows from the fact that a cyclic $\mathbb{F}_p[G]$-module M generated by m is generated over $\mathbb{F}_p$ by $\{\rho^k(m)\}_{k=0}^{l(M)-1}$. ∎

We can now prove

PROPOSITION 2: *Let L/K be a finite Kummer extension of pth-power degree which is Galois over F. Then L is a compositum of finitely many Galois closures, over F, of extensions of the form $L_\gamma = K(\sqrt[p]{\gamma})$, $\gamma \in K^\times$.*

Proof: The extension L/K corresponds to an $\mathbb{F}_p[G]$-submodule M of J. Since M is finite, it is decomposable into a direct sum of finitely many indecomposable $\mathbb{F}_p[G]$-modules M_j. Each indecomposable $\mathbb{F}_p[G]$-module M_j is isomorphic to some A/A_i and is hence cyclic. By Proposition 1 (2), these submodules correspond to Galois closures over F of extensions $L_\gamma = K(\sqrt[p]{\gamma})$. The submodule of J generated by each of the indecomposables M_j then corresponds to the compositum of the L_γ, and we are done. ∎

2.4. THE INDEX. The following homomorphism appears in a somewhat different form in [W, Theorem 3]:

Definition: The **index** $e([\gamma]) \in \mathbb{F}_p$ for $[\gamma] \in J_{p-1}$ is defined by

$$\xi_p^{e([\gamma])} = (\sqrt[p]{N_{K/F}(\gamma)})^\rho.$$

The index is well-defined, as follows. First, since

$$1 + \sigma + \cdots + \sigma^{p-1} = (\sigma - 1)^{p-1} = \rho^{p-1} \tag{2}$$

in $\mathbb{F}_p[G]$, $[N(\gamma)] = [\gamma]^{\rho^{p-1}}$, which is the trivial class [1] by the assumption $[\gamma] \in J_{p-1}$, and as a result $\sqrt[p]{N(\gamma)}$ lies in K and is acted upon by σ. Observe further that $e([\gamma])$ depends neither on the representative γ of $[\gamma]$ nor on the particular pth root of $N(\gamma)$. Also the index function e above is a group homomorphism from J_{p-1} to $\mathbb{F}_p$. Therefore the restriction of e to any M_γ is either trivial or surjective.

We show that the index is trivial for any $[\gamma]$ in the image of ρ:

$$\xi_p^{e([\gamma]^\rho)} = (\sqrt[p]{N(\gamma^{\sigma-1})})^\rho = (\sqrt[p]{1})^\rho = 1,$$

or $e([\gamma]^\rho) = 0$.

LEMMA 3 (see [W, Theorem 2]): *Let $[\gamma] \in J$ and $M = M_\gamma$.*

(1) *If $l(M) < p$ and $e = e([\gamma])$ then $\mathrm{Gal}(L_M/F) \cong B_{i,e}$.*

(2) *If $l(M) = p$ then $\mathrm{Gal}(L_M/F) \cong B_{p,0}$.*

Proof: The second item follows from Proposition 1 and Lemma 1. The fact that $\mathrm{Gal}(L_M/F) \cong B_{i,e}$ for some $e \in \mathbb{F}_p$ follows in the same manner. Therefore it remains only to show that $\mathrm{Gal}(L_M/F) \cong B_{i,e([\gamma])}$ if $l(M) < p$.

Let $\tilde{\sigma}$ denote a pullback of $\sigma \in G$ to $\mathrm{Gal}(L_M/F)$. Then $\tilde{\sigma}^p$ lies in $Z(\mathrm{Gal}(L_M/F)) \cap \mathrm{Gal}(L_M/K)$. (Here $Z(\mathrm{Gal}(L_M/F))$ means the center of $\mathrm{Gal}(L_M/F)$.) Recall that using Kummer theory and the G-equivariant self-duality of A/A_i we may identify $\mathrm{Gal}(L_M/K)$ with A/A_i. Adopting this identification we pick a basis $\{1, \overline{\tau-1}, \ldots, (\overline{\tau-1})^{i-1}\}$ of the $\mathrm{Gal}(L_M/F)$ dual with $\{[\gamma]^{(\sigma-1)^{i-1}}, \ldots, [\gamma]^{\sigma-1}, [\gamma]\}$ with respect to Kummer pairing. Under our identification, $\tilde{\sigma}^p$ lies in the G-invariant submodule of A/A_i, which is $\langle(\overline{\tau-1})^{i-1}\rangle$. Observe that $(\overline{\tau-1})^{i-1}$ sends $\sqrt[p]{\gamma}$ to $\xi_p \sqrt[p]{\gamma}$. If $\tilde{\sigma}^p = e(\overline{\tau-1})^{i-1}$ then

$$(\sqrt[p]{\gamma})^{(\tilde{\sigma}^p-1)} = \xi_p^e.$$

Therefore

$$\sqrt[p]{\gamma}^{(\tilde{\sigma}^p-1)} = \sqrt[p]{\gamma}^{(1+\tilde{\sigma}+\ldots+\tilde{\sigma}^{p-1})(\tilde{\sigma}-1)} = (\sqrt[p]{N_{K/F}(\gamma)})^{(\tilde{\sigma}-1)} = \xi_p^{e([\gamma])}. \quad \blacksquare$$

We characterize elements of J fixed by σ and of trivial index with the following

LEMMA 4: *If $[\gamma] \in J_1$ and $e([\gamma]) = 0$ then there exists $f \in F^\times$ such that $[\gamma] = [f]$.*

Proof: By [MS, Remark 2], we have the following short exact sequence:

$$0 \to \langle[a]\rangle \xrightarrow{i} F^\times/F^{\times p} \xrightarrow{\epsilon} J_1 \xrightarrow{N} \langle[a]\rangle,$$

where $\langle[a]\rangle$ is the subgroup of $F^\times/F^{\times p}$ generated by $[a] \in F^\times/F^{\times p}$, i is the inclusion map, ϵ is the natural homomorphism induced by the inclusion map $F^\times \to K^\times$, and N is the map induced by the norm map from K to F. Now $e([\gamma]) = 0$ implies that $[\gamma]$ is in the kernel of the surjection N above, and we are done. $\blacksquare$

We will also need a lemma on the smallest lengths of cyclic submodules of J generated by an element $[\gamma]$ with nontrivial index. Let $\Upsilon = 1$ if $\xi_p \in N(K^\times)$ and $\Upsilon = 0$ otherwise. In the proof of the next lemma we refer to [A] only for the sake of convenience. One can use basic Kummer theory instead.

LEMMA 5:

(1) *If $\Upsilon = 1$ then there exists $\delta \in K^\times$ such that $[\delta] \in J_1$ and $e([\delta]) \neq 0$. These are precisely the δ such that $K(\sqrt[p]{\delta})/F$ is a cyclic extension of degree p^2.*

(2) *If $\Upsilon = 0$ then $[\sqrt[p]{a}] \in J_2 \setminus J_1$, $e([\sqrt[p]{a}]) \neq 0$, and $e([\gamma]) = 0$ for all $[\gamma] \in J_1$.*

Proof: By [A, Theorem 3], $\Upsilon = 1$ if and only if K/F embeds in an extension $L = K(\sqrt[p]{\delta})$ Galois over F with group $\mathbb{Z}/p^2\mathbb{Z} \cong B_{1,e}$, $e \neq 0$. By Proposition 1

and Lemma 3, then, $\Upsilon = 1$ if and only if there exists $[\delta] \in J_1$ with $e([\delta]) \neq 0$. This proves the first statement.

Assume now that $\Upsilon = 0$. We have $[\sqrt[p]{a}] \in J_2$, since $[\sqrt[p]{a}]^\rho = [\xi_p] \in J_1$, and we calculate $e([\sqrt[p]{a}]) = 1$. Since $\Upsilon = 0$, $[\xi_p] \neq [1]$ in J_1 and therefore $[\sqrt[p]{a}] \notin J_1$. Now consider any $[\gamma] \in J_1$. Then $L = K(\sqrt[p]{\gamma})$ is Galois over F and since $\Upsilon = 0$ we see from [A, Theorem 3] that $\mathrm{Gal}(L/F)$ is $B_{1,0} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Hence $e([\gamma]) = 0$ and the second statement is proved. ∎

Finally, we introduce a variant of [MS, Lemma 1] for submodules generated by elements with trivial index. This is our key lemma:

LEMMA 6: *Let $[\gamma] \in J$. Suppose that $2 \leq l(M_\gamma) < p$ and $e([\gamma]) = 0$.*

Then there exists $[\gamma'] \in J$ such that

(1) $l(M_{\gamma'}) = l(M_\gamma) + 1$.

(2) $[\gamma']^{\rho^2} = [\gamma]^\rho$.

(3) *The fixed elements M_γ^G of M_γ under G coincide with $M_{\gamma'}^G$.*

(4) *If $l(M_\gamma) < p - 1$ then $e([\gamma'])$ is defined and has a value of 0.*

Proof: Let $c = N\gamma$. Since $l(M_\gamma) < p$, we have $[c] = [\gamma]^{\rho^{p-1}} = [1]$. Hence $c \in F^\times \cap K^{\times p}$. In fact, $c = a^s f^p$ for some $f \in F$ and $s \in \mathbb{Z}$, as follows. Since $c \in K^{\times p}$, $F(\sqrt[p]{c}) \subset K$. The Kummer extension $F(\sqrt[p]{c})$ is either F or K; if the former, then $c \in F^{\times p}$, while if the latter, then by Kummer theory c also has the desired form.

Thus $N\gamma = a^s f^p$ for some s and f. But $e([\gamma]) = 0$, so p divides s and we see that $N\gamma = f^p$ for some $f \in F^\times$. Since $N(\gamma/f) = 1$, by Hilbert's Theorem 90 there exists a $\omega \in K^\times$ such that $\omega^{\sigma-1} = \gamma/f$. Then $l(M_\omega) = l(M_\gamma) + 1$.

If $l(M_\gamma) < p - 1$ then let $t = e([\omega])$ and set $\gamma' = \omega/(a^{t/p})$; otherwise let $t = 0$ and set $\gamma' = \omega$.

We compute $[\gamma']^\rho = [\xi_p^{-t}\gamma/f]$ and, since ξ_p, $f \in F^\times$, $[\gamma']^{\rho^2} = [\gamma]^\rho$, which is nontrivial since $2 \leq l(M_\gamma)$. Hence (1) and (2) follow.

Now if $l(M_\gamma) < p - 1$ then $l(M_{\gamma'}) = l(M_\gamma) + 1 < p$ and so $\gamma' \in J_{p-1}$. Then $e([\gamma']) = e([\omega]) - t = 0$. Therefore (4) is valid.

Finally observe that M_γ^G is generated by $[\gamma]^{\rho^{l(M_\gamma)-1}}$ as well as $[\gamma']^{\rho^{l(M_{\gamma'})-1}}$, which in turn generates $M_{\gamma'}^G$. Hence $M_\gamma^G = M_{\gamma'}^G$ and therefore (3) follows from (2). ∎

3. Embedding problem conditions and solutions, $\xi_p \in F$

We consider all embedding problems involving groups $B_{i,e}$, based on the G-surjections determined in Lemma 2, defining the following embedding problems for $i > j \geq 1$:

$$\mathcal{E}_{i,j}(L)\colon 1 \to A_j/A_i \to B_{i,0} \to (A/A_j) \rtimes G = \mathrm{Gal}(L/F) \to 1,$$

and, for any $e \neq 0$,

$$\mathcal{E}'_{i,j}(L)\colon 1 \to A_j/A_i \to B_{i,e} \to (A/A_j) \rtimes G = \mathrm{Gal}(L/F) \to 1.$$

In each case we ask if there exists a Galois extension $\tilde{L}/F$ containing L such that $\mathrm{Gal}(\tilde{L}/F) \cong B_{i,0}$ or $\mathrm{Gal}(\tilde{L}/F) \cong B_{i,e}$, and under the identification of $\mathrm{Gal}(\tilde{L}/F)$ with $B_{i,0}$ (or $B_{i,e}$), the surjection $\mathrm{Gal}(\tilde{L}/F) \to \mathrm{Gal}(L/F)$ is identical to the surjection above.

Since $B_{p,0} \cong B_{p,e}$ as G-extensions for all e, the embedding problems $\mathcal{E}_{p,i}(L)$ and $\mathcal{E}'_{p,i}(L)$ are identical. Moreover, note $\mathcal{E}_{i,1}(L) = \mathcal{E}_i(L)$. (For the discussion of $\mathcal{E}_i$ see the text before Theorem 1 in the Introduction.)

For each of these problems, by Proposition 1, L is the Galois closure of $K(\sqrt[p]{\gamma})$ for some $\gamma \in K^\times$. Hence under the Kummer correspondence $M_\gamma \leftrightarrow L$, and by Proposition 1, $l(M_\gamma) = j$.

THEOREM 2: *Suppose that $\xi_p \in F$. Let $p \geq i > j \geq 1$ and L be the Galois closure of $K(\sqrt[p]{\gamma})$ over F.*

Then $\mathcal{E}_{i,j}(L)$ is solvable if and only if $[\gamma] = [\omega]^{\rho^{p-j}}$ for some $\omega \in K^\times$.

If so, then a solution $\tilde{L}$ to $\mathcal{E}_{i,j}(L)$, where $i > j+1$, is given by

$$\tilde{L} = L\left(\sqrt[p]{f\omega^{\rho^{p-i}}}, \sqrt[p]{\omega^{\rho^{p-i+1}}}, \ldots, \sqrt[p]{\omega^{\rho^{p-j-1}}}\right),$$

$f \in F^\times$.

In the case when $i = j+1$ a solution $\tilde{L}$ to $\mathcal{E}_{j+1,j}$ is given by $\tilde{L} = L(\sqrt[p]{f\omega^{\rho^{p-i}}})$, $f \in F^\times$.

Moreover, all solutions to $\mathcal{E}_{i,j}(L)$ arise in this way if one allows ω to vary over all elements of $K^\times$ with $[\omega]^{\rho^{p-j}} = [\gamma]$.

Proof: By Proposition 1, there exists a field $\tilde{L}$ with $\mathrm{Gal}(\tilde{L}/F) \cong B_{i,e}$ for some i and e if and only if there exists a cyclic submodule M_β of J of length i, and in this case we have $M_\beta \leftrightarrow \tilde{L}$ under the Kummer correspondence.

Furthermore, by Lemma 3, if $i < p$ then $\mathrm{Gal}(\tilde{L}/F) \cong B_{i,e}$, where $e = e([\beta])$, and if $i = p$ then $\mathrm{Gal}(\tilde{L}/F) \cong B_{p,0}$. Hence if $i < p$ then $\mathcal{E}_{i,j}(L)$ is solvable if

and only if there exists $\beta \in K^\times$ with $e([\beta]) = 0$, $l(M_\beta) = i$, and $M_\beta \supset M_\gamma$. If $i = p$ then $\mathcal{E}_{p,j}$ is solvable if and only if there exists $\beta \in K^\times$ with $l(M_\beta) = p$ and $M_\beta \supset M_\gamma$.

Now suppose that $[\gamma] = [\omega]^{\rho^{p-j}}$ for some $\omega \in K^\times$. Then let $\beta = \omega^{\rho^{p-i}}$. Since $l(M_\gamma) = j$ and $[\gamma] = [\beta]^{\rho^{i-j}}$, $l(M_\beta) = i$. Now if $i = p$ then the condition of the previous paragraph is satisfied. If $i < p$ then β is in the image of the endomorphism ρ, therefore $e([\beta]) = 0$ and the condition of the previous paragraph is satisfied.

Going the other way, suppose that there exists $\beta \in K^\times$ with $l(M_\beta) = i$, $M_\beta \supset M_\gamma$, and, if $i < p$, $e([\beta]) = 0$. Since M_γ is the unique $\mathbb{F}_p[G]$-submodule of M_β of length j, $M_\gamma = M_{\beta^{\rho^{i-j}}}$. Further, since the linear map $M_\beta \to M_\gamma$ defined by $[\alpha] \mapsto [\alpha]^{\rho^{i-j}}$ is surjective, there is a $[\beta'] \in M_\beta$ such that we have $[\beta']^{\rho^{i-j}} = [\gamma]$. Moreover, $l(M_{\beta'}) = l(M_\beta)$ so $M_{\beta'} = M_\beta$. In the case of $i < p$, because e is trivial on $[\beta]$, then e is trivial on M_β and hence $e([\beta']) = 0$.

If $i = p$ then let $\omega = \beta'$. Otherwise, by repeated application of Lemma 6, we may find an $\omega \in K^\times$ such that $[\omega]^{\rho^{p-i+1}} = [\beta']^\rho$. Then $[\omega]^{\rho^{p-j}} = [\beta']^{\rho^{i-j}} = [\gamma]$.

We now treat the explicit construction of the solution fields. Let M_β be an $\mathbb{F}_p[G]$-module corresponding to a solution field to the embedding problem $\mathcal{E}_{i,j}(L)$. Let β' and ω be defined as above. Note that $[\omega]^{\rho^{p-i+y}} = [\beta']^{\rho^y}$ for all $y \geq 1$. Hence $\delta = \omega^{\rho^{p-i}}/\beta'$ satisfies $[\delta]^\rho = [1]$. Now $e([\delta]) = 0$, so by Lemma 4, $[\delta] = [f]$ for some $f \in F^\times$. If we have a solution $\tilde{L}$ to $\mathcal{E}_{i,j}(L)$ with $M_\beta \leftrightarrow \tilde{L}$, then $\tilde{L} = L(\sqrt[p]{\theta} : [\theta] \in M_\beta)$, or equivalently

$$\tilde{L} = L(\sqrt[p]{\beta}, \sqrt[p]{\beta^\rho}, \ldots, \sqrt[p]{\beta^{\rho^{i-j-1}}}),$$

by Proposition 1. Since $M_{\beta'} = M_\beta$, $[\omega]^{\rho^{p-i+y}} = [\beta']^{\rho^y}$ for all $y \geq 1$, and $[\beta'] = [\omega^{\rho^{p-i}}/f]$, we have

$$\tilde{L} = L(\sqrt[p]{f^{-1}\omega^{\rho^{p-i}}}, \sqrt[p]{\omega^{\rho^{p-i+1}}}, \ldots, \sqrt[p]{\omega^{\rho^{p-j-1}}})$$

in the case when $i > j + 1$ and $\tilde{L} = L(\sqrt[p]{f^{-1}\omega^{\rho^{p-i}}})$ if $i = j + 1$ again by Proposition 1.

Finally, observe that if we have a solution $\tilde{L}$ to $\mathcal{E}_{i,j}(L)$ with $M_\beta \leftrightarrow \tilde{L}$, then for each $f \in F^\times$ a module $M_{f\beta}$ also corresponds to a solution of $\mathcal{E}_{i,j}(L)$. Hence in our explicit formula for a solution field $\tilde{L}$, any $f \in F^\times$ is eligible. ∎

THEOREM 3: *Suppose $\xi_p \in F$. Let $p \geq i > j \geq 1$ and L be the Galois closure of $K(\sqrt[p]{\gamma})$ over F.*

(1) $\mathcal{E}'_{i,j}(L)$, $i > j+1-\Upsilon$ *or* $j = p-1$, *is solvable if and only if* $[\gamma] = [\omega]^{\rho^{p-j}}$ *for some* $\omega \in K^\times$. *If so, then a solution* $\tilde{L}$ *to* $\mathcal{E}'_{i,j}(L)$ *is given by*

$$\tilde{L} = L(\sqrt[p]{f\alpha\omega'^{\rho^{p-i}}}, \sqrt[p]{\omega'^{\rho^{p-i+1}}}, \ldots, \sqrt[p]{\omega'^{\rho^{p-j-1}}}),$$

$f \in F^\times$, *where in the case* $\Upsilon = 1$, α *is any element in* $K^\times$ *with* $K(\sqrt[p]{\alpha})/F$ *cyclic of degree* p^2, *and in the case* $\Upsilon = 0$, α *is* $\sqrt[p]{a}$. *Furthermore,* $\omega' = \omega^{c_0+c_1\rho+\cdots+c_{i-1}\rho^{i-1}}$ *for suitable* $c_k \in \mathbb{Z}$.

(2) $\mathcal{E}'_{j+1,j}(L)$, $\Upsilon = 0$, *is solvable if and only if* $[\gamma] = [\xi_p]^e[\omega]^{\rho^{p-j}}$ *for some* $\omega \in K^\times$ *and* $e \not\equiv 0 \bmod p$. *If so, then a solution* $\tilde{L}$ *to* $\mathcal{E}'_{i,j}(L)$ *is given by*

$$\tilde{L} = L(\sqrt[p]{fa^{e/p}\omega^{\rho^{p-j-1}}}), \quad f \in F^\times.$$

Moreover, all solutions to $\mathcal{E}'_{i,j}$ *arise in the way described above.*

Note that the two parts of the theorem overlap when $i = p$, $j = p-1$, and $\Upsilon = 0$.

Proof: We begin in the same manner as the previous proof: if $i < p$ then $\mathcal{E}'_{i,j}(L)$ is solvable if and only if there exists $\beta \in K^\times$ with $e([\beta]) \neq 0$, $l(M_\beta) = i$, and $M_\beta \supset M_\gamma$. If $i = p$ then $\mathcal{E}'_{p,j}$ is solvable if and only if there exists $\beta \in K^\times$ with $l(M_\beta) = p$ and $M_\beta \supset M_\gamma$.

We first treat the conditions on $[\gamma]$ that are equivalent to solvability. Then we consider the explicit presentations of the solution fields.

In the case $i = p$, since $\mathcal{E}'_{p,j} = \mathcal{E}_{p,j}$, the condition on $[\gamma]$ is the same as the condition on $[\gamma]$ for the solvability of $\mathcal{E}_{p,j}$ determined in the previous theorem. This gives us the condition in part 1. Now if additionally $j = p-1$, consider the condition of part 2: $[\gamma] = [\xi_p]^e[\omega']^{\rho^{p-j}} = [\xi_p]^e[\omega']^\rho$ for $e \not\equiv 0 \bmod p$. If this condition holds, $\omega = a^{-e/p}\omega'$ satisfies the condition $[\gamma] = [\omega]^{\rho^{p-j}} = [\omega]^\rho$ of part 1. Conversely, if the condition of part 1 holds, set $\omega' = a^{1/p}\omega$ and observe that the condition of part 2 holds with $e = 1$.

Now suppose $i < p$ and $\mathcal{E}'_{i,j}(L)$ is solvable with field $\tilde{L}$ such that $M_\beta \leftrightarrow \tilde{L}$. We show that the specified conditions on $[\gamma]$ must hold.

If $i > j+1$, then $M_{\beta^\rho} \leftrightarrow \bar{L}$, where, by Lemma 3, $\bar{L}$ is a solution to $\mathcal{E}_{i-1,j}(L)$. Then by the previous theorem the condition $[\gamma] = [\omega]^{\rho^{p-j}}$ is satisfied.

If $i = j+1$ and $\Upsilon = 1$, then let $[\alpha] \in J_1$ with $e([\alpha]) \neq 0$. (See Lemma 5. Observe that $K(\sqrt[p]{\alpha})/F$ is cyclic of degree p^2.) Since $\mathcal{E}'_{j+1,j}(L)$ is solvable there exists $M_\beta \supset M_\gamma, l(M_\beta) = j+1$ and $e([\beta]) \neq 0$. Set $\beta' = \beta^{e([\alpha])}/\alpha^{e([\beta])}$. Then $e([\beta']) = 0$. Since $\alpha \in J_1$ we have $M_{(\beta')^\rho} = M_{\beta^\rho} = M_\gamma$. By Proposition 1

and Lemma 3, $M_{\beta'} \leftrightarrow \bar{L}$, where $\bar{L}$ is a solution to $\mathcal{E}_{j+1,j}(L)$. By the previous theorem, the condition $[\gamma] = [\omega]^{\rho^{p-j}}$ is satisfied.

Now consider the case $i = j+1$ and $\Upsilon = 0$. By choosing another generator $[\beta]$ of M_β if necessary, we may assume that $[\beta]^\rho = [\gamma]$. Consider $\beta' = \beta a^{-e([\beta])/p}$. Then $e([\beta']) = 0$. Now $[a^{-e([\beta])/p}]^\rho = [\xi_p^{-e([\beta])}]$, so $[\beta']^\rho = [\xi_p^{-e([\beta])}\gamma]$. Therefore, if $l(M_{\xi_p^{-e([\beta])}\gamma})$ is at least 1 there exists a solution to an embedding problem corresponding to $M_{\beta'}$ and $M_{\xi_p^{-e([\beta])}\gamma}$. By the previous theorem, the condition $[\xi_p]^{-e([\beta])}[\gamma] = [\omega]^{\rho^{p-j}}$ is satisfied. If $[\xi_p^{-e([\beta])}\gamma] = [1]$ then we can set $\omega = 1$ and again the condition $[\xi_p]^{-e([\beta])}[\gamma] = [\omega]^{\rho^{p-j}}$ is satisfied.

In all cases, then, we have shown that if $\mathcal{E}'_{i,j}(L)$ is solvable, the corresponding condition on $[\gamma]$ holds.

Now suppose that the condition of part 1 holds: $[\gamma] = [\omega]^{\rho^{p-j}}$ for some ω. Here we include the case $i = p$.

If $\Upsilon = 1$ then let $[\alpha] \in J_1$ with $e([\alpha]) \neq 0$. (See Lemma 5.) Consider $\beta = \alpha\omega^{\rho^{p-i}}$. If $i < p$, $e([\omega]^{\rho^{p-i}}) = 0$ and hence $e([\beta]) \neq 0$. Since $[\alpha] \in J_1$, $l(M_\beta) = l(M_{\omega^{\rho^{p-i}}}) = l(M_\gamma) + i - j = i$. Moreover, since $[\beta]^{\rho^{i-j}} = [\gamma]$, $M_\beta \supset M_\gamma$ and we have shown that $\mathcal{E}'_{i,j}(L)$ is solvable. In the case when $i = p$ and $\Upsilon = 1$ we observed above that $\mathcal{E}'_{p,j}(L)$ is equivalent with $\mathcal{E}_{p,j}(L)$ and also the solvability conditions are the same. Hence by Theorem 2 we see that $\mathcal{E}'_{p,j}(L)$ is solvable.

If $\Upsilon = 0$ and $i > j+1$, then let $\alpha = \sqrt[p]{a}$. Consider $\beta = \alpha\omega^{\rho^{p-i}}$. Again if $i < p$ then $e([\omega]^{\rho^{p-i}}) = 0$ and hence $e([\beta]) \neq 0$. Since $[\alpha] \in J_2$ (see Lemma 5) and $i > j+1$, $l(M_\beta) = l(M_{\omega^{\rho^{p-i}}}) = l(M_\gamma) + i - j = i$. Moreover, since $[\beta]^{\rho^{i-j}} = [\gamma]$, $M_\beta \supset M_\gamma$ and we have shown that $\mathcal{E}'_{i,j}(L)$ is solvable. (Observe that we employed the condition $i < p$ only to ensure that $e([\beta]) \neq 0$ in this case. If $i = p$ then $e([\beta])$ plays no role, and therefore we have covered this case in the construction above.)

Now suppose that the condition of part 2 holds: $[\gamma] = [\xi_p]^e[\omega]^{\rho^{p-j}}$ for some $\omega \in K^\times$ and $e \not\equiv 0 \bmod p$. Let $\beta = a^{e/p}\omega^{\rho^{p-j-1}}$. If $j+1 < p$ then, because $e([\omega]^{\rho^{p-j-1}}) = 0$, we have $e([\beta]) = e \not\equiv 0 \bmod p$. Moreover, $[\beta]^\rho = [\xi_p^e][\xi_p^{-e}][\gamma] = [\gamma]$, so $M_\beta \supset M_\gamma$ and we have shown that $\mathcal{E}'_{j+1,j}(L)$ is solvable. Finally, observe that if $j+1 = p$ we showed at the beginning of our proof that both embedding problems $\mathcal{E}'_{p,p-1}$ and $\mathcal{E}_{p,p-1}$ are the same, and that also the conditions in Theorem 2 and Theorem 3 for the existence of a solution of this problem are equivalent. Hence the existence of a solution in this case follows from Theorem 2.

Next we shall derive an explicit form of any solution field $\tilde{L}$ of our embedding problem.

Observe that for any $f \in F^\times$ and $J_{p-1} \supset M_\beta \supsetneq M_\gamma$, we have $l(M_{f\beta}) = l(M_\beta)$,

$M_{f\beta} \supset M_\gamma$, and $e([f\beta]) = e([\beta])$. Recall that in the case $\Upsilon = 1, \alpha$ is any element in $K^\times$ with $K(\sqrt[p]{\alpha})/F$ cyclic of degree p^2, and in the case $\Upsilon = 0, \alpha$ is $\sqrt[p]{\alpha}$. By Proposition 1, then,

$$\tilde{L} = L(\sqrt[p]{f\beta}, \sqrt[p]{\beta^\rho}, \ldots, \sqrt[p]{\beta^{\rho^{p-1}}})$$

is a solution to the appropriate embedding problem for $\beta = \alpha\omega^{\rho^{p-i}}$ in the case $i > j + 1 - \Upsilon$ or $j = p - 1$ and $\beta = a^{e/p}\omega^{\rho^{p-i}}$ in the case $i = j + 1$, $\Upsilon = 0$, as above.

To show that every solution field $\tilde{L}$ takes this form, suppose that $M_\beta \leftrightarrow \tilde{L}$ is a solution to $\mathcal{E}'_{i,j}(L)$. Hence $M_\beta \supset M_\gamma$. We consider first the case of part 1 when $\Upsilon = 1$. If $i < p$ then, by Lemma 3, $e([\beta]) \neq 0$; in this case we let $c \in \mathbb{Z}$ be such that $e([\beta^c]) = e([\alpha])$ and set $\beta' = \beta^c$ so that $e([\beta'/\alpha]) = 0$. If $i = p$ then let $\beta' = \beta$. Because $i > j \geq 1$ and $[\alpha] \in J_1$, $l(M_{\beta'/\alpha}) = l(M_{\beta'}) = i$. Observe that $[\beta'/\alpha]^\rho = [\beta^c]^\rho$, so $M_{\beta'/\alpha} \supset M_{(\beta'/\alpha)^\rho} = M_{\beta^\rho} \supset M_\gamma$, because M_γ is properly contained in M_β and M_{β^ρ} is the maximal proper $\mathbb{F}_p[G]$-submodule of M_β. Hence $M_{\beta'/\alpha} \leftrightarrow \bar{L}$, for $\bar{L}$ a solution to $\mathcal{E}_{i,j}(L)$.

By Kummer theory and Theorem 2,

$$M_{\beta'/\alpha} = \langle [f\omega^{\rho^{p-i}}], [\omega^{\rho^{p-i+1}}], \ldots, [\omega^{\rho^{p-1}}] \rangle$$

for some $f \in F^\times$ and $\omega \in K^\times$. Observe that hence $M_{\beta'/\alpha} = M_{f\omega^{\rho^{p-i}}}$. Because $[\beta'/\alpha]$ and $[f\omega^{\rho^{p-i}}]$ are both $\mathbb{F}_p[G]$-module generators of the same module of length i,

$$\beta'/\alpha = (f\omega^{\rho^{p-i}})^{c_0 + c_1\rho + \cdots + c_{i-1}\rho^{i-1}}$$

for some $c_k \in \mathbb{F}_p$. Let $f' = f^{c_0}$ and $\omega' = \omega^{c_0 + c_1\rho + \cdots + c_{i-1}\rho^{i-1}}$. Then $\beta'/\alpha = f'(\omega')^{\rho^{p-i}}$, or $\beta' = f'\alpha(\omega')^{\rho^{p-i}}$. Since $M_{\beta'} = M_\beta \leftrightarrow \tilde{L}$, $\tilde{L}$ takes the form

$$\tilde{L} = L(\sqrt[p]{f'\alpha(\omega')^{\rho^{p-i}}}, \sqrt[p]{(\omega')^{\rho^{p-i+1}}}, \ldots, \sqrt[p]{(\omega')^{\rho^{p-1}}})$$

by Proposition 1.

The case when $\Upsilon = 0$ can be treated as above with slight modifications. First in this case instead of $[\alpha] \in J_1$ we take $[\sqrt[p]{a}]$. We use our hypothesis $i > j + 1$ to make sure as above that $l(M_{\beta'/\sqrt[p]{a}}) = l(M_{\beta'})$. Next observe that

$$M_{\beta'/\sqrt[p]{a}} \supset M_{(\beta'/\sqrt[p]{a})^{\rho^2}} = M_{\beta^{\rho^2}} \supset M_\gamma$$

as the $\mathbb{F}_p[G]$-submodules of M_β are linearly ordered by inclusion and $l(M_\beta) - l(M_\gamma) \geq 2$. The rest of the argument for case (1) when $\Upsilon = 0$ faithfully follows the argument for case (1) when $\Upsilon = 1$ as above.

In order to show that every solution field $\tilde{L}$ in part 2 takes the specified form, observe that A_j/A_{j+1} is in the center of $B_{j+1,e}$. Therefore, since we have one solution of the embedding problem $\mathcal{E}'_{j+1,j}$ of the form $L' = L(\sqrt[p]{a^{e/p}\omega^{\rho^{p-j-1}}})$, by the well-known theorem on solutions of central embedding problems (see [JLY, Lemma A.1.1]), any other solution $\tilde{L}$ of the embedding problem $\mathcal{E}'_{j+1,j}$ takes the form

$$\tilde{L} = L(\sqrt[p]{fa^{e/p}\omega^{\rho^{p-j-1}}}), \quad f \in F^\times,$$

as required. ∎

Remark: Lemma 2 implies that among our embedding problems, only Galois extensions L/F with $\mathrm{Gal}(L/F) \cong B_{j,0}$ may be solved. This result agrees with our Theorems 2 and 3, as follows. Suppose that L is the Galois closure of $K(\sqrt[p]{\gamma})$, $\gamma \in K^\times$, and $l(M_\gamma) = j$. From our solvability conditions we see that if L can be embedded in some extension $\tilde{L}$ such that $\mathrm{Gal}(\tilde{L}/F) \cong B_{i,e}$ and $p \geq i > j \geq 1, e \in \mathbb{F}_p$, then necessarily $e([\gamma]) = 0$.

4. Arbitrary fields

4.1. CHARACTERISTIC NOT p. We now suppose that K_0/F_0 is a cyclic extension of degree p of fields of characteristic not p. Set $F = F_0(\xi_p)$, $K = K_0(\xi_p)$, and $s = [F : F_0]$. Let ϵ denote a generator of $\mathrm{Gal}(F/F_0)$ and σ a generator of $G = \mathrm{Gal}(K_0/F_0)$. Since p and s are relatively prime, $\mathrm{Gal}(K/F_0) \cong \mathrm{Gal}(F/F_0) \times \mathrm{Gal}(K_0/F_0)$. Therefore we may naturally extend ϵ and σ to K, and they commute in $\mathrm{Gal}(K/F_0)$. Using the extension of σ to K, we write G for $\mathrm{Gal}(K/F)$ as well.

Let $t \in \mathbb{Z}$ such that $\epsilon(\xi_p) = \xi_p^t$. Then t is relatively prime to p. Let J^ϵ be the t-eigenspace of $J = K^\times/K^{\times p}$ under the action of ϵ. Observe that since ϵ and σ commute, J^ϵ is an $\mathbb{F}_p[G]$-subspace of J. By [W, §5, Prop.], we have a Kummer correspondence over K_0 of subspaces M^ϵ of the $\mathbb{F}_p$-vector space J^ϵ and abelian exponent p extensions L_0 of K_0:

$$M^\epsilon = ((KL_0)^{\times p} \cap K^\times)/K^{\times p} \quad \leftrightarrow$$
$$L_0 = \text{maximal } p\text{-extension of } K_0 \text{ in } L_{M^\epsilon} = K(\sqrt[p]{\gamma} : [\gamma] \in M_\epsilon).$$

As Waterhouse shows, for $M^\epsilon \subset J^\epsilon$, $\epsilon \in \mathrm{Gal}(K/K_0)$ has a unique lift $\tilde{\epsilon}$ to $\mathrm{Gal}(L_{M^\epsilon}/K_0)$ of order s, and L_0 is the fixed field of $\tilde{\epsilon}$.

We first prove a lemma on the decomposition of J:

LEMMA 7: *$J = J^\epsilon \oplus J^\nu$, where J^ν is an $\mathbb{F}_p[G]$-submodule of J, and e is trivial on $J^\nu \cap J_{p-1}$.*

Proof: We adapt an approach to descent from [Sa, page 258]. Let $z \in \mathbb{Z}$ satisfy $zst^{s-1} \equiv 1 \bmod p$, and set

$$T = z \cdot \sum_{i=1}^{s} t^{s-i}\epsilon^{i-1} \in \mathbb{Z}[\mathrm{Gal}(K/F_0)].$$

We calculate that $(t-\epsilon)T \equiv 0 \bmod p$, and hence the image of T on J lies in J^ϵ. Moreover, on J^ϵ, ϵ acts by multiplication by t, and hence T acts as the identity on J^ϵ. Finally, since ϵ and σ commute, T and $I-T$ commute with σ. Hence J decomposes into a direct sum $J^\epsilon \oplus J^\nu$, with associated projections T and $I-T$.

Let $a \in F^\times$ satisfy $K = F(\sqrt[p]{a})$, and consider $[a]_F \in F^\times/F^{\times p}$. By [W, §5, Prop.], $\epsilon([a]_F) = [a]_F^t$. Suppose $\gamma \in K^\times$ satisfies $[\gamma] \in J_{p-1}$. Then, since ϵ and σ commute,

$$[N(\epsilon(\gamma))]_F = [\epsilon(N(\gamma))]_F = \epsilon([N(\gamma)]_F) = [N(\gamma)]_F^t.$$

Hence $e(\epsilon([\gamma])) = t \cdot e([\gamma])$, and we then calculate that $e([T\gamma]) = e([\gamma])$. Therefore $e((I-T)[\gamma]) = 0$. ∎

Now we establish that the Galois structure of L_{M^ϵ}/F is equivalent to that of L_0/F_0.

PROPOSITION 3: *Under the Kummer correspondence above, L_0 is Galois over F_0 if and only if M^ϵ is an $\mathbb{F}_p[G]$-submodule of J^ϵ. In this case the base extension $F_0 \to F$ induces a natural isomorphism of G-extensions* $\mathrm{Gal}(L_0/F_0) \cong \mathrm{Gal}(L/F)$.

Proof: If L_0/F_0 is Galois, then $L_{M^\epsilon} = L_0K/F$ is Galois as well, and by Proposition 1 (1), L^ϵ is an $\mathbb{F}_p[G]$-submodule of J.

Going the other way, suppose that M^ϵ is an $\mathbb{F}_p[G]$-submodule of J^ϵ. By the correspondence, L_{M^ϵ}/K_0 is Galois. Then M^ϵ is also an $\mathbb{F}_p[\mathrm{Gal}(K/F_0)]$-submodule of J^ϵ and therefore L_{M^ϵ}/F_0 is Galois.

Now since K_0/F_0 is Galois, every automorphism of L_{M^ϵ} sends K_0 to K_0. Moreover, since L_0 is the unique maximal p-extension of K_0 in L_{M^ϵ}, every automorphism of L_{M^ϵ} sends L_0 to L_0. Therefore L_0/F_0 is Galois.

Finally, we show that base field extension $F_0 \to F$ induces a natural isomorphism of G-extensions $\mathrm{Gal}(L_0/F_0) \to \mathrm{Gal}(L/F)$. Now F/F_0 and L_0/F_0 are of relatively prime degrees, and hence $\mathrm{Gal}(L_0F/F_0) \cong \mathrm{Gal}(F/F_0) \times \mathrm{Gal}(L_0/F_0)$.

Moreover, we deduce that we have the natural isomorphism $G = \mathrm{Gal}(K_0/F_0) \cong \mathrm{Gal}(K/F)$, and that the natural isomorphism $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(L_0/F_0)$ is a G-extension isomorphism. ∎

Now we make the connection between embedding problems over F_0 and embedding problems over F. For $p \geq i > j \geq 1$, denote by $\mathcal{E}_{i,j}(L_0)$ and $\mathcal{E}'_{i,j}(L_0)$ the embedding problems

$$\mathcal{E}_{i,j}(L_0): \quad 1 \to A_j/A_i \to B_{i,0} \to (A/A_j) \rtimes G = \mathrm{Gal}(L_0/F_0) \to 1$$

and, for any $e \neq 0$,

$$\mathcal{E}'_{i,j}(L_0): \quad 1 \to A_j/A_i \to B_{i,e} \to (A/A_j) \rtimes G = \mathrm{Gal}(L_0/F_0) \to 1.$$

WARNING. In order to avoid possible confusion, let us recall that by $[\delta]^\epsilon$ we mean the projection of $[\delta]$ into the summand J^ϵ of J. Similarly, $[\delta]^\nu$ means the projection of $[\delta]$ into the summand J^ν of J.

PROPOSITION 4:

(1) *$\mathcal{E}_{i,j}(L_0)$ is solvable if and only if $\mathcal{E}_{i,j}(L)$ is solvable.*

(2) *$\mathcal{E}'_{i,j}(L_0)$ is solvable if and only if $\mathcal{E}'_{i,j}(L)$ is solvable.*

Proof: Let $\tilde{L}_0$ be a solution to $\mathcal{E}_{i,j}(L_0)$. Then by Proposition 3, $\tilde{L} := \tilde{L}_0 F$ is a solution to $\mathcal{E}_{i,j}(L)$.

Going the other way, let $\tilde{L}$ be a solution to $\mathcal{E}_{i,j}(L)$. Kummer theory gives correspondences $M^\epsilon \leftrightarrow L_0$ over K_0, as well as $M^\epsilon \leftrightarrow L$ and $\tilde{M} \leftrightarrow \tilde{L}$ over K. By Proposition 1 (2), $\tilde{M} = M_\delta$ and $M^\epsilon = M_\gamma$ for some $\delta, \gamma \in K^\times$, with $[\gamma] \in J^\epsilon$. By Lemma 7, we may write $[\delta] = [\delta]^\epsilon + [\delta]^\nu \in J^\epsilon \oplus J^\nu$, with $e([\delta]^\epsilon) = e([\delta])$ if $[\delta] \in J_{p-1}$. Moreover, since $[\delta]^{\rho^{i-j}} = [\gamma]$ and J^ν is a $\mathbb{F}_p[G]$-submodule, $([\delta]^\epsilon)^{\rho^{i-j}} = [\gamma]$. Let $\tilde{M}^\epsilon = M_{\delta^e}$. Then $M^\epsilon \subset \tilde{M}^\epsilon$. By the Kummer correspondence over K_0, there exists a field $\tilde{L}_0$ such that $\tilde{M}^\epsilon \leftrightarrow \tilde{L}_0$ and $L_0 \subset \tilde{L}_0$. By Lemma 3 and Proposition 3, $\tilde{L}_0$ is a solution to $\mathcal{E}_{i,j}(L_0)$.

The case of $\mathcal{E}'_{i,j}$ follows analogously. ∎

4.2. EMBEDDING PROBLEM CONDITIONS, ARBITRARY FIELDS. To state the general result, we alter our notation to let F take the place of F_0. If $\mathrm{char}\, F \neq p$, then J now denotes $K(\xi_p)^\times / K(\xi_p)^{\times p}$.

THEOREM 4: *Let F be an arbitrary field.*

(1) *If $\mathrm{char}\, F = p$, then $\mathcal{E}_{i,j}(L)$ and $\mathcal{E}'_{i,j}(L)$ are solvable.*

(2) *If $\mathrm{char}\, F \neq p$, let $\gamma \in F(\xi_p)^\times$ satisfy $K(\xi_p) = F(\xi_p)(\sqrt[p]{\gamma})$, and set $\Upsilon = 1$ if $\xi_p \in N_{K(\xi_p)/F(\xi_p)}(K(\xi_p)^\times)$ and $\Upsilon = 0$ otherwise. Then*

(a) $\mathcal{E}_{i,j}(L)$ *is solvable if and only if* $[\gamma] = [\omega]^{\rho^{p-j}}$ *in* J *for some* $\omega \in K(\xi_p)^\times$.

(b) $\mathcal{E}'_{i,j}(L)$, $i > j+1-\Upsilon$ *or* $j = p-1$, *is solvable if and only if* $[\gamma] = [\omega]^{\rho^{p-j}}$ *in* J *for some* $\omega \in K(\xi_p)^\times$.

(c) $\mathcal{E}'_{j+1,j}(L)$, $\Upsilon = 0$, *is solvable if and only if* $[\gamma] = [\xi_p]^e[\omega]^{\rho^{p-j}}$ *in* J *for some* $\omega \in K(\xi_p)^\times$ *and* $e \not\equiv 0 \bmod p$.

Proof: If $\operatorname{char} F = p$, then by Witt's theorem all central non-split embedding problems with kernel $\mathbb{F}_p$ are solvable. (See [JLY, Appendix A].) Since $B_{i,e}$ and $B_{j,0}$ have the same minimal number of generators for all $1 \leq i, j$ and e, Witt's theorem gives that $\mathcal{E}_{i,j}(L)$ and $\mathcal{E}'_{i,j}(L)$ are solvable. Indeed, one can successively solve a chain of suitable central non-split embedding problems with kernel $\mathbb{F}_p$ leading to solutions of $\mathcal{E}_{i,j}(L)$ and $\mathcal{E}'_{i,j}(L)$.

If $\operatorname{char} F \neq p$, then the statements follow from Theorems 2 and 3 using Proposition 4. ∎

5. Proof of Main Theorem

Proof: Observe that $\mathcal{E}_i = \mathcal{E}_{i,1}$. The equivalence of (1) and (2) follows from Theorem 4.

Now assume that $\operatorname{char} F \neq p$. By Proposition 4, $\mathcal{E}_{i,1}(L)$ is solvable if and only if $\mathcal{E}_{i,1}(L(\xi_p))$ is solvable. The condition on b implies that $M_b \leftrightarrow L(\xi_p)/K(\xi_p)$ under the Kummer correspondence. To show (3), by Theorem 2 we need only show that there exists $\alpha \in K(\xi_p)^\times$ with $[b] = [\alpha]^{\rho^{p-1}}$ if and only if there exists ω with $N_{K(\xi_p)/F(\xi_p)}(\omega) = b$. Let N denote $N_{K(\xi_p)/F(\xi_p)}$.

By equation (2) of Section 2.4,

$$[\omega]^{\rho^{p-1}} = [\omega]^{1+\sigma+\cdots+\sigma^{p-1}} = [\omega^{1+\sigma+\cdots+\sigma^{p-1}}] = [N(\omega)] = [b],$$

so if ω exists satisfying $N(\omega) = b$, then $\alpha = \omega$ satisfies $[b] = [\alpha]^{\rho^{p-1}}$.

Going the other way, suppose that $[b] = [\alpha]^{\rho^{p-1}}$ for some α. By equation (2) again, $[b] = [N(\alpha)]$. Then $N(\alpha) = k^p b$ for some $k \in K(\xi_p)^\times$. Hence $N(\alpha)/b \in F(\xi_p)^\times \cap K(\xi_p)^{\times p}$. Let $a \in K(\xi_p)^\times$ satisfy $K(\xi_p) = F(\xi_p)(\sqrt[p]{a})$. Then by Kummer theory $k^p = a^s f^p$ for some $s \in \mathbb{Z}$. Choosing $\omega = \alpha/(a^{s/p} f)$ we obtain $N(\omega) = b$.

Finally, the explicit solution of solution fields in the case $\xi_p \in F$ follows directly from Theorem 2. ∎

ACKNOWLEDGEMENT: It is clear from the content of our paper that we are strongly influenced by the beautiful paper of Waterhouse cited in the references, and we gratefully acknowledge this crucial influence on our work. We are also grateful to Adrian Wadsworth for some helpful discussions concerning this work. Finally, we thank an anonymous referee for suggesting that our results would likely extend from the case of fields with a primitive pth root of unity to the arbitrary field case, using Albert's descent technique.

References

[A] A. Albert, *On cyclic fields*, Transactions of the American Mathematical Society **37** (1935), 454–462.

[GSS] H. G. Grundman, T. L. Smith and J. R. Swallow, *Groups of order* 16 *as Galois groups*, Expositiones Mathematicae **13** (1995), 289–319.

[JLY] C. Jensen, A. Ledet and N. Yui, *Generic polynomials: constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications 45, Cambridge University Press, Cambridge, 2002.

[La] T.-Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics 189, Springer-Verlag, New York, 1999.

[Ma] R. Massy, *Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p*, Journal of Algebra **109** (1987), 508–535.

[MS] J. Mináč and J. Swallow, *Galois module structure of pth-power classes of extensions of degree p*, Israel Journal of Mathematics **138** (2003), 29–42.

[Sa] D. Saltman, *Generic Galois extensions and problems in field theory*, Advances in Mathematics **43** (1982), 250–283.

[W] W. Waterhouse, *The normal closures of certain Kummer extensions*, Canadian Mathematical Bulletin **37** (1994), 133–139.