TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 353, Number 6, Pages 2347–2370
S 0002-9947(00)02625-8
Article electronically published on October 11, 2000

RELATIVE EMBEDDING PROBLEMS

ELENA V. BLACK AND JOHN R. SWALLOW

ABSTRACT. We consider Galois embedding problems $G \twoheadrightarrow H \cong \mathrm{Gal}(X/Z)$ such that a Galois embedding problem $G \twoheadrightarrow \mathrm{Gal}(Y/Z)$ is solvable, where Y/Z is a Galois subextension of X/Z. For such embedding problems with abelian kernel, we prove a reduction theorem, first in the general case of commutative k-algebras, then in the more specialized field case. We demonstrate with examples of dihedral embedding problems that the reduced embedding problem is frequently of smaller order. We then apply these results to the theory of obstructions to central embedding problems, considering a notion of quotients of central embedding problems, and classify the infinite towers of metacyclic p-groups to which the reduction theorem applies.

INTRODUCTION

A classical question of Galois theory is the embedding problem: whether a given Galois extension may be embedded into a larger Galois extension with specified group. Embedding problems, considered variously over number fields and geometric fields, offer approaches both to the inverse Galois problem and to the determination of number-theoretic consequences implied by a particular Galois group. When solving embedding problems, it is often productive to determine relationships between the embedding problem at hand and related embedding problems, so that both the solvability conditions and the field solutions, if any, of one embedding problem may be used to advantage in the other.

In this paper we follow such an approach, considering embedding problems with the additional information that a related embedding problem has a solution. Given a Galois extension E_B/K with Galois group H and a surjection of groups $G \twoheadrightarrow H$, we ask if E_B/K embeds into a G-Galois extension of K, with the added knowledge that some Galois subextension of E_B, say K_1/K with Galois group $\bar{H}$, embeds in a Galois extension over K with Galois group G. We call these *relative embedding problems* and study such problems in detail when the kernel of the surjection $G \twoheadrightarrow \bar{H}$ is abelian. Our results on relative embedding problems, culminating in Theorem 3.1 in the context of fields, reduce the question of solvability of certain embedding problems with abelian kernel to the question of solvability of reduced embedding problems. These reduced embedding problems are of smaller order when the centralizers of the abelian kernels are larger than the kernels themselves.

Received by the editors January 4, 1999 and, in revised form, August 20, 1999.
2000 *Mathematics Subject Classification.* Primary 12F12, 13B05; Secondary 12F10.
The first author gratefully acknowledges a University of Oklahoma Junior Faculty Research Grant. The second author gratefully acknowledges support under National Science Foundation Grant No. DMS-9501366 and a Davidson College MacArthur Faculty Study and Research Grant.

The primary motivation for our work on this problem is derived from the case of dihedral groups of 2-power order. (For a survey of work on similar embedding problems see [GSS]; for later work, see [Cr] and [Le].) Suppose that K is a field and that $G = D_{2^d}$ is a dihedral group of order 2^{d+1}. The group $G = D_{2^d}$ naturally appears in a tower $\{G_i = D_{2^i}\}$ of central C_2-extensions

$$G = G_d \longrightarrow G_{d-1} \longrightarrow \cdots \longrightarrow G_1 = C_2 \times C_2 \longrightarrow G_0 = C_2.$$

Suppose further that M_1/K is a $C_2 \times C_2$-Galois extension which has a solvable embedding problem for G, with solution M_d/K. Let M_0/K be the fixed field in M_d of the C_{2^d}-subgroup of G. Now for $2 \leq i \leq d$, consider M_i/K, the intermediate D_{2^i}-Galois subextension of M_d/K. Each field M_i is obtained by adjoining a square root of some element of $M_{i-1}^{\times}$, so that $M_i = M_{i-1}(\sqrt{\gamma_{i-1}})$, where $\gamma_{i-1} \in M_{i-1}^{\times}$. It is well-known (see [Bl, Lemma 4.1], for instance) that the other embeddings of M_{i-1}/K into G_i-Galois extensions differ only by a $K^{\times}$-constant r, *i.e.*, these other embeddings are given by fields $M_{i-1}(\sqrt{r\gamma_{i-1}})$. Using our Main Theorem we determine for which r the extensions $M_{i-1}(\sqrt{r\gamma_{i-1}})/K$ embed in Galois extensions with group G as well. We show in Theorem 3.3 that $M_{i-1}(\sqrt{r\gamma_{i-1}})/K$ embeds in a Galois extension with group G if and only if the extension $M_0(\sqrt{r})/K$ embeds in a Galois extension with group G_{d-i+1} cyclic over M_0.

In section 1 we introduce the machinery of the relative embedding problem and Baer products of group extensions and Galois extensions. We then develop in section 2 correspondences among relative embedding problems and related split and reduced embedding problems. In section 3 we present the main reduction theorem, with an immediate application to dihedral relative embedding problems. In section 4 we present implications for the structure of obstructions of central embedding problems, and in section 5 we determine towers, particularly infinite towers, of metacyclic p-group extensions to which our reduction theorem applies.

We are grateful to the host institution, the Mathematisches Forschungsinstitut Oberwolfach, and the organizers, D. Harbater, B. H. Matzat and Y. Ihara, of the conference "Galois Groups and Fundamental Groups," for a discussion which became the starting point for this paper. We also thank the Department of Mathematics at the University of Oklahoma for its hospitality provided to the second author during some of the collaboration.

1. Notation, Definitions, and Background

Let k be a field. Unless stated otherwise, throughout this paper a k-algebra denotes a commutative k-algebra, and an extension of algebras S/R, or an algebra extension, denotes an extension of commutative k-algebras. Below we introduce embedding problems and relative embedding problems in this context. For definitions and basic results in the Galois theory of commutative rings, see [CHR] or [DI]. It is important to note that, in contrast with the theory over fields, a Galois extension of k-algebras S/R does not uniquely determine the Galois group and its action; to make precise a Galois extension, one must specify the extension S/R of k-algebras, the group G, and an explicit isomorphism $\nu\colon G \xrightarrow{\simeq} \mathrm{Aut}(S/R)$ such that the subring of S fixed by $\nu(G)$ is R. Sometimes this extension is denoted by the pair $(S/R, \nu)$ and is called a G-Galois extension (of algebras). Each of the following definitions subsumes a corresponding definition in the Galois theory of fields.

Definition 1.1. Let $f\colon G \twoheadrightarrow H$ be a surjection of finite groups with kernel B, and let $(S_B/R, \nu)$ be an H-Galois extension. The *embedding problem* associated to $(S_B/R, \nu, f)$ is to determine if there exists a G-Galois extension $(S/R, \eta)$ such that $S_B \subset S$ and $h\eta = \nu f$, where h is the homomorphism $h\colon \eta(G) \to \nu(H)$ with kernel $\eta(B)$ of Galois theory:

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G/B \\ {\scriptstyle\eta}\big\downarrow & & {\scriptstyle\nu}\big\downarrow \\ \mathrm{Aut}(S/R) & \xrightarrow{\ h=\mathrm{Gal}\ } & \mathrm{Aut}(S_B/R) \end{array}$$

We call an embedding problem *abelian*, *central*, or *Frattini* if B is abelian, B lies in the center $Z(G)$ of G, or B lies in the Frattini subgroup $\Phi(G)$ of G, respectively.

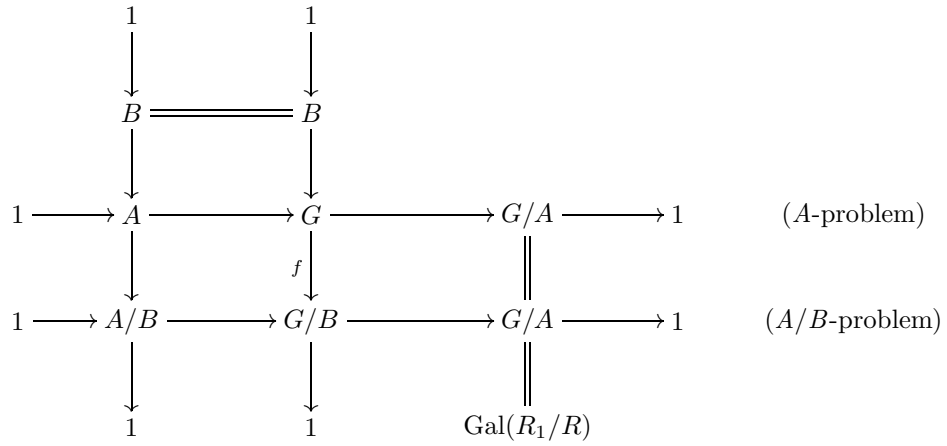
If the embedding problem associated to $(S_B/R, \nu, f)$ has an affirmative answer for an Galois extension S_B/R, we say that S_B/R has *solvable embedding problem* for ν and f. If the context is clear, we may omit ν and/or f and write that S_B/R has solvable embedding problem for G.

Definition 1.2. Suppose that we have two embedding problems, one associated to S_1/R, $\eta_1\colon H_1 \xrightarrow{\simeq} \mathrm{Aut}(S_1/R)$, and $f_1\colon G_1 \twoheadrightarrow H_1$, and one associated to S_2/R, $\eta_2\colon H_2 \xrightarrow{\simeq} \mathrm{Aut}(S_2/R)$, and $f_2\colon G_2 \twoheadrightarrow H_2$. We say that the embedding problems are *common over a Galois extension* R_1/R if R_1 lies in the intersection of S_1 and S_2. By Galois theory, then, there exist normal subgroups $A_1 \subset G_1$ and $A_2 \subset G_2$ such that $S_1^{\eta_1(A_1)} = S_2^{\eta_2(A_2)} = R_1$ and $G_1/A_1 \cong G_2/A_2$.

In the sequel the notation $\mathrm{Fix}(X)$ will denote the subgroup of the Galois group of the extension under consideration which fixes the subalgebra X.

Definition 1.3. A *relative embedding problem* consists of an embedding problem associated to S_B/R, $\nu\colon H \xrightarrow{\simeq} \mathrm{Aut}(S_B/R)$, and $f\colon G \twoheadrightarrow H$; a Galois subalgebra extension R_1/R with quotient action $\nu'\colon H/\mathrm{Fix}(R_1) \xrightarrow{\simeq} \mathrm{Aut}(R_1/R)$; and a solution $(T/R, \eta)$ to an embedding problem with group G associated to $(R_1/R, \nu')$ and the quotient surjection $f'\colon G \twoheadrightarrow H/\mathrm{Fix}(R_1)$, such that under η the subgroup in G corresponding to R_1 contains $\ker f$.

Informally, a relative embedding problem is a pair of embedding problems with group G, common over a Galois subalgebra extension R_1/R, such that one embedding problem is solvable. A relative embedding problem is then an embedding problem with additional information. The following commutative diagram helps connect the various embedding problems contained in the definition of a relative embedding problem. Let $B = \ker f$, so that $H = G/B$ and the subgroup of H corresponding to R_1/R is A/B.



Considered in this fashion, we are given in the definition of a relative embedding problem a solution $(S_B/R, \nu)$ of the A/B-embedding problem and a solution $(T/R, \eta)$ of the A-embedding problem, and we seek a solution of the B-embedding problem associated to the G/B-Galois extension $(S_B/R, \nu)$.

Under the further hypothesis that R_1/R corresponds to an *abelian* subgroup of G, *i.e.*, the subgroup A in the above diagram is abelian, we now define the principal object of study in this paper, the class of abelian relative embedding problems.

Definition 1.4. An *abelian relative embedding problem* is an embedding problem associated to S_B/R, $\nu\colon H \xrightarrow{\simeq} \mathrm{Aut}(S_B/R)$, and $f\colon G \twoheadrightarrow H$; a Galois subalgebra extension R_1/R with quotient action $\nu'\colon H/\operatorname{Fix}(R_1) \xrightarrow{\simeq} \mathrm{Aut}(R_1/R)$; and a solution $(T/R, \eta)$ to an embedding problem with group G associated to $(R_1/R, \nu')$ and the quotient surjection $f'\colon G \twoheadrightarrow H/\operatorname{Fix}(R_1)$, such that under η the subgroup in G corresponding to R_1 is abelian and contains $\ker f$. It follows that $\ker f$ is abelian and hence the embedding problem associated to S_B/R is abelian.

We note that several results of [ILF, §3.15] can be viewed as a treatment of abelian relative embedding problems in the case $S_B = R_1$.

We now recall from [ILF] definitions of Baer products of extensions (of groups and of Galois extensions).

Definition 1.5. Let B be an abelian group. Let G_1 and G_2 be finite groups which are group extensions of a finite group H by a H-module B; hence we have exact sequences $1 \to B \to G_1 \xrightarrow{\phi_1} H \to 1$ and $1 \to B \to G_2 \xrightarrow{\phi_2} H \to 1$. Let $\tilde{G}$ be the product of G_1 and G_2 with amalgamated quotient group H, consisting of elements (g_1, g_2) such that $\phi_1(g_1) = \phi_2(g_2)$. Identify B with its image in each of G_1 and G_2. There is a natural surjection $\tilde{G} \twoheadrightarrow H$ with kernel $B \times B$, consisting of elements (b_1, b_2), $b_1 \in B \subset G_1$, $b_2 \in B \subset G_2$. Let $\tilde{B}$ consist of the elements (b_1, b_2) where $b_1 = b_2^{-1}$ under the identification of B. Then the *Baer product* (*of groups*) of G_1 and G_2 is the extension $\tilde{G}/\tilde{B}$, and we have an exact sequence

$$1 \longrightarrow B \longrightarrow \tilde{G}/\tilde{B} \longrightarrow H \longrightarrow 1,$$

where B is embedded in $\tilde{G}/\tilde{B}$ by means of the map $b \mapsto (b,1) \pmod{\tilde{B}}$.

Note that the Baer product of groups depends not only on the subgroups B in G_1 and G_2, but also on the particular injections of the groups B into the corresponding subgroups in G_1 and G_2.

Recall the notion of *equivalence of group extensions* of a group H by a H-module B. Let

$$1 \longrightarrow B \xrightarrow{i_1} G_1 \xrightarrow{\phi_1} H \longrightarrow 1$$

and

$$1 \longrightarrow B \xrightarrow{i_2} G_2 \xrightarrow{\phi_2} H \longrightarrow 1$$

describe two group extensions G_1, G_2 of H by a H-module B. Then (G_1, i_1, ϕ_1) and (G_2, i_2, ϕ_2) are defined to be *equivalent* if there exists an isomorphism $\theta\colon G_1 \xrightarrow{\simeq} G_2$ such that $\theta i_1 = i_2 \operatorname{id}_B$ and $\phi_2\theta = \operatorname{id}_H \phi_1$. The Baer product is then a composition law on the classes of equivalent group extensions, under which these classes form an abelian group isomorphic to $H^2(H,B)$ [ILF, Theorem 3.15.1]. Recall that the inverse class of G, an arbitrary extension of H by B, is given as follows. Define the group $\bar{G}$ as a set of elements $\bar{g}$, $g \in G$, with the multiplication $\overline{g_1} \cdot \overline{g_2} = \overline{g_2 g_1}$. Under the map $g \mapsto \bar{g}^{-1}$, G is abstractly isomorphic to $\bar{G}$. The group $\bar{G}$ is an extension of H by B, under the same action on B as before, and the Baer product of G and $\bar{G}$ is therefore the semidirect extension of H by B. Note that the map $g \mapsto \bar{g}^{-1}$ is the automorphism of B given by inversion.

Definition 1.6 ([ILF, §3.15])**.** Let G_1 and G_2 be finite groups which are group extensions of a finite group H by a H-module B, where the injections of B into G_1 and G_2 are fixed. Let $(S_1/R, \eta_1)$ be a G_1-Galois extension and $(S_2/R, \eta_2)$ be a G_2-Galois extension. Suppose that S_1/R and S_2/R share a subextension R_1/R which is the fixed subalgebra of $B_1 \subset G_1$ in S_1 and $B_2 \subset G_2$ in S_2. Identify B_1 and B_2 with B through the injections of B. Then let $\tilde{G}/\tilde{B}$ be the Baer product of groups G_1 and G_2 as defined above, and let $\tilde{S} = S_1 \otimes_{R_1} S_2$ with action $\eta_3\colon \tilde{G} \to \operatorname{Aut}(\tilde{S}/R)$ defined by $(\eta_3(g_1,g_2))(s_1 \otimes s_2) = \eta_1(g_1)(s_1) \otimes \eta_2(g_2)(s_2)$. For $(g_1,g_2) \in \tilde{G}$, we have $\nu_1(g_1) = \nu_2(g_2)$ when restricted to R_1, hence η_3 is well-defined. We emphasize this action on the tensor product by writing $\eta_1 \otimes \eta_2$ in place of η_3.

The *Baer product* (*of Galois extensions*) of $(S_1/R, \eta_1)$ and $(S_2/R, \eta_2)$ is the subalgebra U of $\tilde{S}$ fixed by $\tilde{B} \subset \tilde{G}$, with the quotient action derived from $\eta_1 \otimes \eta_2$ under the factorization. The (*Baer*) *inverse of a G-extension* $(S/R, \nu)$ is the $\bar{G}$-extension $(S/R, \nu i)$, where $i\colon \bar{G} \to G$ is the isomorphism from the (Baer group) inverse of G to G.

One immediately anticipates that the Baer product of Galois extensions gives a composition law on equivalence classes of Galois extensions $(S/R, \eta)$ which extend a given H-Galois extension $(S_B/R, \nu)$ by B-extensions S/S_B, where B is a fixed H-module. While there is a standard notion of equivalence of group extensions (given above), there are several choices for equivalence of Galois extensions. Observe that when a Galois extension $(S/R, \eta)$ is given, an implicit choice of a lifting of each element $h \in H$ has been made to an element $g_h \in G$ such that $\eta(g_h) = \nu(h)$ on S_B; these choices, in turn, determine a 2-cocycle $z \in Z^2(H,B)$. We do not want to distinguish between actions η which amount to no more than a different choice of liftings to the same automorphism group of S/R, which would correspond in the group setting to two elements of $Z^2(H,B)$ in the same class of $H^2(H,B)$.

Hence we wish to consider two Galois extensions $(S_1/R, G_1, \eta_1)$, $(S_2/R, G_2, \eta_2)$ which extend a given H-Galois extension $(S_B/R, \nu)$ by B-extensions, where B is a fixed H-module, (Galois extension-) equivalent if there exists an S_B-isomorphism of algebras $\theta\colon S_1 \to S_2$ such that, if an appropriate choice of lifts $\eta_1(g_{1,h})$, $\eta_2(g_{2,h})$ of $\nu(h)$ are made into $\eta_1(G_1)$ and $\eta_2(G_2)$, then $\theta(s^{\eta_1(g_{1,h})\eta_1(b)}) = \theta(s)^{\eta_2(g_{2,h})\eta_2(b)}$ for all $s \in S$, $h \in H$, $b \in B$. Such an equivalence implies that the map $\gamma\colon G_1 \to G_2$ given by $\gamma(g_{1,h}b) = g_{2,h}b$ satisfies $\theta(s^{\eta_1(g_1)}) = \theta(s)^{\eta_2(\gamma(g_1))}$ for $g_1 \in G$. The group law in G_1 is

$$(g_{1,h_1}b_1)(g_{1,h_2}b_2) = g_{1,h_1}g_{1,h_2}b_1^{h_2}b_2,$$

and since the analogous group law holds in G_2, the fact that

$$\gamma(g_{1,h_1}g_{1,h_2}b_1^{h_2}b_2) = g'_{1,h_1}g'_{1,h_2}b_1^{h_2}b_2$$

implies that γ is an isomorphism. Abstractly, then, G and G' are identical groups, and γ leaves fixed the specified injections of B into each group. We encapsulate this discussion in the following definition.

Definition 1.7 ([ILF, §3.15.2])**.** Let $f\colon G \twoheadrightarrow H$ be a surjection of finite groups and let $(S_B/R, \nu)$ be an H-Galois extension. Two solutions $(S_1/R, \eta_1)$, and $(S_2/R, \eta_2)$ of the embedding problem associated to $(S_B/R, \nu, f)$ are said to be *equivalent*, or, following [ILF], *equivalent in the broad sense*, if there exist an S_B-isomorphism $\theta\colon S_1 \to S_2$ and an automorphism $\gamma\colon G \to G$ trivial on $B = \ker f$ such that for all $s \in S_1$, $g \in G$,

$$\theta(s^{\eta_1(g)}) = \theta(s)^{(\eta_2\gamma)(g)}.$$

Remark 1.8. If S_1, S_2, and hence S_B and R, are fields, then S_1 and S_2 are equivalent in the broad sense if and only if $S_1 = S_2$ and $\eta_1^{-1}\eta_2$ is an automorphism of G trivial on B and identical on cosets G/B. Since θ is an S_B-isomorphism, the equivalence condition becomes $t^{\eta_1(g)} = t^{(\eta_2\gamma)(g)}$ for $t \in S_B$. Because $h\eta_1 = h\eta_2 = \nu f$, where h is the surjection $\mathrm{Gal}(S_i/R) \to \mathrm{Gal}(S_B/R)$, then we have $t^{(\nu f)(g)} = t^{(\nu f\gamma)(g)}$ for $t \in S_B$; hence $f\gamma = f$, or γ is identical on cosets $G/\ker f$.

Remark 1.9. The fact that the injection of B into G must be specified in the definitions of equivalence in the broad sense and the Baer product of Galois extensions raises the question of whether or not these definitions are unnecessarily restricted, *i.e.*, whether or not two Galois extensions $(S/R, \eta_1)$ and $(S/R, \eta_2)$, extending $(S_B/R, \nu)$, isomorphic under an S_B-algebra isomorphism $\theta\colon S \to S$ and a group automorphism $\gamma\colon G \to G$ *not* trivial on the injections of B, satisfying $\theta(s^{\eta_1(g)}) = \theta(s)^{\eta_2(\gamma(g))}$, are *also* isomorphic under θ' and γ', where γ' is trivial on B. When S is a field, this situation cannot occur: *any* S_B-automorphism $\theta'\colon S \to S$ is necessarily an element of the Galois group $\mathrm{Gal}(S/S_B)$, hence in B. Then the inner automorphism associated to θ' leaves B invariant.

When S is not a field, however, it is possible to find such elements (θ', γ'). Consider, for instance, the group $G = B = \langle\sigma\rangle \cong C_4$ and the completely splitting algebra (S, η), where $S = \bigoplus_{\sigma^i \in B} Re_{\sigma^i}$ and $\eta(\sigma^i)(e_b) = e_{b\sigma^i}$ for $b \in B$, and set $S_B = R$ so that $H = 1$. Define an R-automorphism $\theta\colon S \to S$ by $\theta(e_{\sigma^i}) = e_{\sigma^{-i}}$ and an automorphism $\gamma\colon B \to B$ by $\gamma(\sigma) = \sigma^{-1}$. Then γ is not trivial on B. Write

$s = \sum_{i=0}^{3} r_i e_{\sigma^i}$ for $s \in S$. Then

$$\begin{aligned}\theta(s^{\eta(b)}) =& \theta\left(\sum_{i=0}^{3} r_i e_{\sigma^i}^{\eta(b)}\right) = \theta\left(\sum_{i=0}^{3} r_i e_{\sigma^i b}\right) = \sum_{i=0}^{3} r_i e_{\sigma^{-i} b^{-1}} \\ &= \left(\sum_{i=0}^{3} r_i e_{\sigma^{-i}}\right)^{\eta(\gamma(b))} = \theta(s)^{\eta(\gamma(b))},\end{aligned}$$

while under $\theta' = \mathrm{id}_S$ and $\gamma' = \mathrm{id}_G$, we have the relation $\theta'(s^{\eta(b)}) = \theta'(s)^{\eta(\gamma'(b))}$ preserved, and γ' is trivial on B.

2. Baer Products and Descent for Relative Embedding Problems

From now on we restrict our attention to abelian relative embedding problems. Consider an embedding problem associated to S_B/R, $\eta_{S_B}\colon H \xrightarrow{\simeq} \mathrm{Aut}(S_B/R)$, and $f\colon G \twoheadrightarrow H$; a Galois subalgebra R_1/R with quotient action $\eta_{R_1}\colon H/\operatorname{Fix}(R_1) \xrightarrow{\simeq} \mathrm{Aut}(R_1/R)$; and a solution $(T/R, \eta_T)$ to an embedding problem with group G, associated to $(R_1/R, \eta_{R_1})$ and the quotient surjection $f'\colon G \twoheadrightarrow H/\operatorname{Fix}(R_1)$, such that under η_T the subgroup in G corresponding to R_1 is abelian and contains $\ker f$. We call the subalgebra R_1/R the *common* subalgebra of T/R and S_B/R.

Definition 2.1. The *A-embedding problem* associated to an abelian relative embedding problem is the embedding problem associated to R_1/R, $\eta_{R_1}\colon H/\operatorname{Fix}(R_1) \xrightarrow{\simeq} \mathrm{Aut}(R_1/R)$, and $f'\colon G \twoheadrightarrow H/\operatorname{Fix}(R_1)$. Denote $\ker f'$ by A. The A-embedding problem associated to an abelian relative embedding problem has a solution $(T/R, \eta_T)$. The split A-embedding problem is the embedding problem associated to $(R_1/R, \eta_{R_1}, A \rtimes G/A \xrightarrow{\mathrm{can}} G/A \cong H/\operatorname{Fix}(R_1))$.

Definition 2.2. The *B-embedding problem* associated to an abelian relative embedding problem is the (original) embedding problem associated to S_B/R, $\eta_{S_B}\colon H \xrightarrow{\simeq} \mathrm{Aut}(S_B/R)$, and $f\colon G \twoheadrightarrow H$. Denote $\ker f$ by B. Solutions of the B-embedding problem associated to an abelian relative embedding problem are solutions of the relative embedding problem, and vice versa. All solutions of the B-embedding problem are also then solutions of the A-embedding problem.

Definition 2.3. The *A/B-embedding problem* associated to an abelian relative embedding problem is the embedding problem associated to R_1/R, $\eta_{R_1}\colon H/\operatorname{Fix}(R_1) \xrightarrow{\simeq} \mathrm{Aut}(R_1/R)$, and $f''\colon H \twoheadrightarrow H/\operatorname{Fix}(R_1)$. Keeping the same notation, the kernel of f'' is then A/B. The A/B-embedding problem associated to an abelian relative embedding problem has a solution S_B/R. The *split A/B-embedding problem* is the embedding problem associated to $(R_1/R, \eta_{R_1}, A/B \rtimes G/A \xrightarrow{\mathrm{can}} G/A \cong H/\operatorname{Fix}(R_1))$.

Let $C(A)$ denote the centralizer of A in G. In the following, note that since A is normal in G, $C(A)$ is also normal in G and therefore $C(A)/A$ is normal in G/A.

Definition 2.4. The *reduced embedding problems* associated to an abelian relative embedding problem are as follows, and all but the last are necessarily split. Let R_0 be the fixed subalgebra of $C(A)/A \subset G/A$ in R_1 and denote by $\eta_{R_0}\colon H/\operatorname{Fix}(R_0) \xrightarrow{\simeq} \mathrm{Aut}(R_0/R)$ the quotient action. The *reduced A-embedding problem* is the embedding problem associated to $(R_0/R, \eta_{R_0}, A \rtimes G/C(A) \xrightarrow{\mathrm{can}} G/C(A) \cong H/\operatorname{Fix}(R_0))$. The *reduced A/B-embedding problem* is the embedding problem associated to

$(R_0/R, \eta_{R_0}, A/B \rtimes G/C(A) \xrightarrow{\text{can}} G/C(A) \cong H/\mathrm{Fix}(R_0))$. Given a solution (U_0, η_{U_0}) of the reduced A/B-embedding problem, the *reduced B-embedding problem* is the embedding problem associated to $(U_0/R, \eta_{U_0}, A \rtimes G/C(A) \xrightarrow{\text{can}} A/B \rtimes G/C(A))$.

Proposition 2.5 ([ILF, §3.15])**.** *Fix the solution $(T/R, \eta_T)$ of the A-embedding problem. Then there exists a bijective correspondence between equivalence classes of solutions $(S/R, \eta_S)$ of the A-embedding problem and equivalence classes of solutions $(\tilde{U}/R, \eta_{\tilde{U}})$ of the split A-embedding problem.*

Proof ([ILF]). Let $(T/R, \eta_T)$ and $(S/R, \eta_S)$ be solutions of the A-embedding problem, hence G-Galois extensions. Let $i\colon \bar{G} \to G$ be the isomorphism carrying the Baer group inverse $\bar{G}$ of G to G. Then $(T/R, \eta_T i)$ is a $\bar{G}$-Galois extension. We form the Baer product of Galois extensions $(T/R, \eta_T i)$ and $(S/R, \eta_S)$ as follows. Let M be the k-algebra $T \otimes_{R_1} S$, with group the amalgamated product of $\bar{G}$ and G over H, and with action $\eta_M = \eta_T i \otimes \eta_S$. The Baer product is then the subalgebra $\tilde{U}$ of M fixed by $\eta_M(a, a^{-1})$, $a \in A$, which is the same as the subalgebra of elements of M fixed by $\eta_T(a) \otimes \eta_S(a)$, $a \in A$; the group is then the Baer product of $\bar{G}$ and G, namely the semidirect product $A \rtimes G/A$; and the action $\eta_{\tilde{U}}\colon A \rtimes G/A \xrightarrow{\simeq} \mathrm{Aut}(\tilde{U}/R)$ is derived from η_M. Since $(T/R, \eta_T)$ and $(S/R, \eta_S)$ both extend $(R_1/R, \eta_{R_1})$, the extension $\tilde{U}/R$ solves the embedding problem stated in the proposition.

Now let $(\tilde{U}/R, \eta_{\tilde{U}})$ be an $A \rtimes G/A$-Galois extension which extends $(R_1/R, \eta_{R_1})$, and let $(T/R, \eta_T)$ be a solution of the A-embedding problem. We form the Baer product of Galois extensions $(\tilde{U}/R, \eta_{\tilde{U}})$ and $(T/R, \eta_T)$ as follows. Let M be the k-algebra $\tilde{U} \otimes_{R_1} T$, with group the amalgamated product of $A \rtimes G/A$ and G over H, and with action $\eta_M = \eta_{\tilde{U}} \otimes \eta_T$. The Baer product is then the subalgebra S of M fixed by $\eta_M(a, a^{-1})$, $a \in A$, which is the set of elements of M fixed by $\eta_{\tilde{U}}(a) \otimes \eta_T(a^{-1})$, $a \in A$; the group is then the Baer product of $A \rtimes G/A$ and G, namely G; and the action $\eta_S\colon G \xrightarrow{\simeq} \mathrm{Aut}(S/R)$ is derived from η_M. Since $(\tilde{U}/R, \eta_{\tilde{U}})$ and $(T/R, \eta_T)$ both extend $(R_1/R, \eta_{R_1})$, the extension S/R solves the embedding problem stated in the proposition.

We now show that the correspondence is bijective. Having fixed T/R, we constructed a $\tilde{U}/R$ corresponding to any given S/R; we must show that the composition of this correspondence with the one which takes $\tilde{U}/R$ to a solution S'/R is the identity map. Consider the Galois extension

$$N = T \otimes_{R_1} S \otimes_{R_1} T$$

with group G_N, the amalgamated product of $\bar{G}$, G, and G over H, with action $\eta_N = \eta_T i \otimes \eta_S \otimes \eta_T$. The composition of the two mappings gives a certain Galois subextension S'/R inside the Galois extension N, namely that associated under η_N to the subgroup J of G_N generated by elements $(a, 1, a^{-1})$ and $(a, a^{-1}, 1)$, $a \in A$. Now set $\eta'_N = \eta_T \otimes \eta_S \otimes \eta_T$ and view η'_N as an action of $A \times A \times A$ on the Galois extension N/R_1. Then S'/R_1 is the subextension associated under η'_N to the subgroup J' of $A \times A \times A$ generated by elements $(a, 1, a)$ and $(a, a^{-1}, 1)$, $a \in A$.

We must now show that the fixed subextension S'/R, together with the quotient action given by η_N, is equivalent to (S, η_S). First we determine the subextension of $T \otimes_{R_1} T$ with action $\eta_T \otimes \eta_T$ fixed by elements (a, a). Following [ILF, lemma in Theorem 3.15.2], the algebra $T \otimes_{R_1} T$ with action $\eta_T \otimes \eta_T$ can be written as a sum $\bigoplus_{a \in A} T e_1$, where $e_1^{\eta_T(g) \otimes \eta_T(g)} = e_1$ for each $g \in G$; $e_a = e_1^{\eta_T(a) \otimes \eta_T(1)}$; and G acts on T via the first factor in $\eta_T \otimes \eta_T$. Since A is abelian, we have, moreover, that

$e_a^{\eta_T(b)\otimes\eta_T(b)} = e_a$ for each $b \in A$. With these relations one derives the fact that the subalgebra of $T \otimes_{R_1} T$ fixed by elements $\eta_T(a) \otimes \eta_T(a)$, $a \in A$, is $\bigoplus_{a\in A} R_1 e_a$; further, the action of A', the factor group of $A \times A$ by elements of the form (a, a), is via the same action $\eta_T \otimes \eta_T$, so that $a' \in A'$ acts as $(a', 1) \in A \times A$, or, equivalently, by permuting the summands,

$$\sum_{a\in A} r_a e_a \mapsto \sum_{a\in A} r_a e_{aa'}.$$

Then the subalgebra S' of N is the subalgebra of $(\bigoplus_{a\in A} R_1 e_a) \otimes_{R_1} S$ with action $((\eta_T \otimes \eta_T) \otimes \eta_S)$ fixed by elements $((a, 1), a^{-1})$, $a \in A$. This tensor product can be written $\bigoplus_{a\in A} S e_a$, and the fixed elements are those of the form $\sum_{a\in A} z^{\eta_S(a^{-1})} e_a$, $z \in S$. The group A, as a factor group of $A' \times A$ by elements (a, a^{-1}), then acts on S' as $((a, 1), 1)$ in $((\eta_T \otimes \eta_T) \otimes \eta_S)$, so that $a' \in A$ sends $\sum_{a\in A} z^{\eta_S(a^{-1})} e_a$ to

$$\sum_{a\in A} z^{\eta_S(a^{-1})} e_{aa'} = \sum_{a\in A} (z^{\eta_S(a')})^{\eta_S(a^{-1})} e_a.$$

This algebra is then clearly isomorphic, with the action of A, to S with action η_S, via $\sum_{a\in A} z^{a^{-1}} e_a \mapsto z$. □

Corollary 2.6. *Fix the solution $(T/R, \eta_T)$ of the A-embedding problem, and take the fixed subalgebra of T/R corresponding to B, with quotient action: (T_B, η_{T_B}). Then there exists a bijective correspondence between equivalence classes of solutions $(S_B/R, \eta_{S_B})$ of the A/B-embedding problem and equivalence classes of solutions $(U_1/R, \eta_{U_1})$ of the split A/B-embedding problem.*

Proof. Let (T, G, A) of the proposition refer to $(T_B, G/B, A/B)$; then the statement is the same, *mutatis mutandis*, as the proposition. □

Proposition 2.7. *Fix a relative embedding problem. Then there exists a bijective correspondence between equivalence classes of solutions $(S/R,\ \eta_S)$ of the B-embedding problem and equivalence classes of solutions $(\tilde{U}/R, \eta_{\tilde{U}})$ of the embedding problem associated to the surjection*

$$A \rtimes G/A \twoheadrightarrow A/B \rtimes G/A \cong \mathrm{Gal}(U_1/R).$$

Here the extension $(U_1/R, \eta_{U_1})$ corresponds to $(S_B/R, \eta_{S_B})$ under Corollary 2.6.

Proof. Solutions of the B-embedding problem are also solutions of the A-embedding problem, and hence we may invoke Proposition 2.5 to assert that solutions $(S/R, \eta_S)$ of the B-embedding problem correspond to solutions $(\tilde{U}, \eta_{\tilde{U}})$ of the split A-embedding problem. By Corollary 2.6, the extension S_B/R of the relative embedding problem corresponds to a solution $(U_1/R, \eta_{U_1})$ of the A/B-embedding problem. Since the correspondences are achieved in the same way and $(S/R, \eta_S)$ extends $(S_B/R, \eta_{S_B})$, $(\tilde{U}/R, \eta_{\tilde{U}})$ extends $(U_1/R, \eta_{U_1})$ and hence $(\tilde{U}/R, \eta_{\tilde{U}})$ is a solution of the embedding problem associated to $A \rtimes G/A \twoheadrightarrow A/B \rtimes G/A \cong \mathrm{Gal}(U_1/R)$.

Conversely, again by the identical process of the correspondences, we have that given a solution $(\tilde{U}/R, \eta_{\tilde{U}})$ of the embedding problem associated to $(U_1/R, \eta_{U_1})$ and surjection $A \rtimes G/A \twoheadrightarrow A/B \rtimes G/A$, which is then a solution of the split A-embedding problem, we have that by Proposition 2.5 $(\tilde{U}/R, \eta_{\tilde{U}})$ corresponds to a solution $(S/R, \eta_S)$ of the A-embedding problem, and, using Corollary 2.6, we find that this solution must extend the solution $(S_B/R, \eta_{S_B})$ corresponding to $(U_1/R, \eta_{U_1})$. □

Proposition 2.8. *Fix an abelian relative embedding problem. Then there exists a bijective correspondence between solutions* $(\tilde{U}/R, \eta_{\tilde{U}})$ *of the split* A*-embedding problem and solutions* $(U/R, \eta_U)$ *of the reduced* A*-embedding problem.*

Proof. Let $(\tilde{U}/R, \eta_{\tilde{U}})$ be a solution of the split A-embedding problem. The subgroup $C(A)$ is normal in G, hence $C(A)/A$ is normal in G/A. Therefore the subgroup $1 \rtimes C(A)/A$ of the semidirect product $A \rtimes G/A$ is normal. Taking the fixed ring of this subgroup under $\eta_{\tilde{U}}$ in $\tilde{U}$, we have a solution $(U/R, \eta_U)$ of the reduced A-embedding problem, where η_U is the quotient action from $\eta_{\tilde{U}}$.

Conversely, note that subalgebra R_1/R of the abelian relative embedding problem is a G/A-extension with action η_{R_1} derived from the solution (T, η_T). Now let $(U/R, \eta_U)$ be a solution of the reduced A-embedding problem, and consider the k-algebra $N = U \otimes_{R_0} R_1$, where R_0 is the fixed subalgebra of $C(A)/A$ in R_1, with action $\eta_N = \eta_U \otimes \eta_{R_1}$. This k-algebra N is a Galois extension over R with group isomorphic to the product of $A \rtimes G/C(A)$ (under action η_U) and G/A (under action η_{R_1}) with amalgamated quotient group $G/C(A)$, under an action, say η_{R_0}, which is common to η_U and η_{R_1} by virtue of the definition of the reduced A-embedding problem. This amalgamation is a group $\tilde{H}$ which is a semidirect product of A with G/A, hence (N, η_N) is a solution of the split A-embedding problem. Set $(\tilde{U}, \eta_{\tilde{U}})$ equal to (N, η_N).

We now show that the correspondence is bijective. Given a solution $(U/R, \eta_U)$ of the reduced A-embedding problem, we see that the corresponding solution $(\tilde{U}/R, \eta_{\tilde{U}})$ has subalgebra U/R corresponding to $1 \rtimes C(A)/A$ under the action $\eta_{\tilde{U}}$. Hence the correspondence $\tilde{U} \mapsto U$ results in the same $(U/R, \eta_U)$. □

Corollary 2.9. *Fix an abelian relative embedding problem. Then there exists a bijective correspondence between solutions* $(U_1/R, \eta_{U_1})$ *of the split* A/B*-embedding problem and solutions* $(U_0/R, \eta_{U_0})$ *of the reduced* A/B*-embedding problem.*

Proof. Let (T_B, η_{T_B}) be the fixed subalgebra of the solution (T, η_T) of the A-embedding problem, under B and η_T; the quotient action is then η_{T_B}. Let (T, G, A) of the proposition refer to $(T_B, G/B, A/B)$; then the statement is the same, *mutatis mutandis*, as the proposition. □

Proposition 2.10. *Fix an abelian relative embedding problem. Then there exists a bijective correspondence between equivalence classes of solutions* $(S/R, \eta_S)$ *of the* B*-embedding problem and equivalence classes of solutions* $(U/R, \eta_U)$ *of the reduced* B*-embedding problem associated to the extension* $(U_0/R, \eta_{U_0})$ *corresponding to* $(S_B/R, \eta_{S_B})$ *under Corollary 2.9.*

Proof. By Proposition 2.7, solutions $(S/R, \eta_S)$ correspond to solutions $(\tilde{U}/R, \eta_{\tilde{U}})$, and by Proposition 2.8 this solution corresponds to a solution $(U/R, \eta_U)$. By Proposition 2.7 $(\tilde{U}/R, \eta_{\tilde{U}})$ extends $(U_1/R, \eta_{U_1})$, which corresponds in the same sense as Proposition 2.8 under Corollary 2.9 to $(U_0/R, \eta_{U_0})$. Hence $(U/R, \eta_U)$ extends $(U_0/R, \eta_{U_0})$ and solves the reduced A/B-embedding problem. The converse follows just as in the proof of Proposition 2.7. □

Proposition 2.11. *Assume that the* k*-algebras in the abelian relative embedding problem are fields and* S_B *and* T *are linearly disjoint over* R_1*. Then the correspondences in Propositions 2.5, 2.7, 2.8, and 2.10 and Corollaries 2.6 and 2.9 carry field solutions to field solutions as follows:*

(a) Proposition 2.5: solutions S linearly disjoint from T over R_1 $\longleftrightarrow$ solutions $\tilde{U}$ linearly disjoint from T over R_1;

(b) Corollary 2.6: solutions S_B linearly disjoint from T over R_1 $\longleftrightarrow$ solutions U_1 linearly disjoint from T over R_1;

(c) Proposition 2.7: solutions S linearly disjoint from T over R_1 $\longleftrightarrow$ solutions $\tilde{U}$ linearly disjoint from T over R_1;

(d) Proposition 2.8: solutions $\tilde{U}$ $\longleftrightarrow$ solutions U linearly disjoint from R_1 over R_0;

(e) Corollary 2.9: solutions U_1 $\longleftrightarrow$ solutions U_0 linearly disjoint from R_1 over R_0;

(f) Proposition 2.10: solutions S linearly disjoint from T over R_1 $\longleftrightarrow$ solutions U linearly disjoint from R_1 over R_0.

Proof. For (a), (b), and (c), observe that the Baer product of two Galois field extensions linearly disjoint over R_1 is again linearly disjoint over R_1 from either extension. In (d) and (e) one direction is given by taking a subfield and does not depend on the Baer product, while the other one is taken via the Baer product with R_1/R. The last is the combination of (a) through (e). □

3. Main Theorem and Applications to Dihedral Field Extensions

In this section we consider the abelian relative embedding problem in the setting of fields. We change notation for the field case and then specialize Proposition 2.10 to our Main Theorem.

Definition 3.0. The *abelian relative embedding problem for fields* is defined as follows. Let G be a finite group with a normal abelian subgroup A, and assume that B is a subgroup of A which is also normal in G. Let K be a field and L/K a G-Galois extension where we identify G with the Galois group of L/K. Suppose that E_B/K is a G/B-Galois extension such that $L \cap E_B = K_1$, where K_1/K is a Galois extension corresponding to $A \subset G$. Let $\dot{G}$ be an abstract group isomorphic to G, such that $\dot{G} \to G/B$ is the surjection corresponding to $G \to G/B$. The *abelian relative embedding problem* is to determine all $\dot{G}$-Galois extensions E/K which extend E_B/K.

In the following main theorem we connect the solutions of the relative abelian embedding problem for fields and the solutions of a reduced embedding problem for fields.

Theorem 3.1 (Main Theorem: Reduction)**.** *Consider an abelian relative embedding problem for fields as defined above. Let K_0 be the fixed field in L of the centralizer $C(A)$ of A in G, which is also the fixed field of $C(A)/A$ in K_1. Then*

(a) E_B/K corresponds uniquely to a solution F_0/K of the embedding problem associated to the split exact sequence

$$1 \longrightarrow A/B \longrightarrow A/B \rtimes G/C(A) \longrightarrow G/C(A) \cong \mathrm{Gal}(K_0/K) \longrightarrow 1.$$

Here $G/C(A)$ acts on A/B via the action of G on A; and

(b) the solutions E/K of the relative embedding problem which are linearly disjoint from L over K_1 are in bijective correspondence with the solutions F/K of the embedding problem associated to the exact sequence

$$1 \longrightarrow B \rtimes 1 \longrightarrow A \rtimes G/C(A) \longrightarrow A/B \rtimes G/C(A) \cong \mathrm{Gal}(F_0/K) \longrightarrow 1$$

which are linearly disjoint from K_1 over K_0.

Proof. With notation changed as in Definition 3.0 and attention paid to linear disjointness using Proposition 2.11, the theorem is a specialization of Proposition 2.10 to fields. □

Now we specialize our Main Theorem to a Dihedral Reduction Theorem for fields for the case in which G is a dihedral group. Let C_s denote the cyclic group of order s and $D_s \cong C_s \rtimes C_2$ the dihedral group of order $2s$. Let $1 < k \mid m \mid n$ be integers and set $G = D_n$.

We set up the abelian relative embedding problem and reinterpret Theorem 3.1 as follows. Let L/K be a Galois extension with $\mathrm{Gal}(L/K) \cong D_n$. Let E_B/K be a Galois extension with $\mathrm{Gal}(E_B/K) \cong D_m$, such that $E_B \cap L = K_1$ is Galois with $\mathrm{Gal}(K_1/K) \cong D_k$. Note that in this situation $A \cong C_{n/k}$, $B \cong C_{n/m}$, $C(A) \cong C_n$, and the fixed field of $C(A)$ in L is K_0.

Since L/K_0 is a cyclic Galois extension with a group C_n, there is a unique C_m-Galois subextension L_B/K_0 and it contains K_1. Furthermore, E_B and L_B are $C_{m/k}$-Galois extensions of K_1, thus corresponding to two distinct elements, α and β, respectively, of the cohomology group $H^1(K_1, C_{m/k})$. There exists a unique $C_{m/k}$-Galois extension of K_1 corresponding to the element $\alpha\beta^{-1} \in H^1(K_1, C_{m/k})$. We denote this extension of K_1 by F_1.

The thrust of Theorem 3.1(a) is that F_1/K_1 descends to a $C_{m/k}$-Galois extension F_0 of K_0 (so that, in particular, $F_1 = F_0 \otimes_{K_0} K_1$); further, F_0/K is a Galois extension with group $C_{m/k} \rtimes C_2$, with a quotient action derived from G: F_0/K is Galois with group $D_{m/k}$, cyclic over K_0. The content of Theorem 3.1(b) is then that E_B/K embeds in a D_n-extension of K cyclic over K_0 if and only if the extension F_0/K embeds in a D_m-extension of K cyclic over K_0. Note that if $m > 2$, then the cyclic over K_0 condition is automatically satisfied for a D_n-extension of K extending E_B/K, and if $m/k > 2$, then the cyclic over K_0 condition is automatically satisfied for a D_m-extension of K extending F_0/K.

Theorem 3.2 (Dihedral Reduction)**.** *Let k, m, n be integers as above and let all Galois extensions denote those of field extensions. Let L/K be a D_n-Galois extension and E_B/K a D_m-Galois extension such that $L \cap E_B = K_1$ is a Galois extension of K with group D_k.*

Then there exists a $D_{m/k}$-Galois extension F_0/K, cyclic over K_0, such that E_B/K embeds in a D_n-extension E/K cyclic over K_0 if and only if the $D_{m/k}$-Galois extension F_0/K embeds in a $D_{n/k}$-Galois extension of K cyclic over K_0.

Proof. Let L/K be a D_n-Galois extension with group presented as

$$\langle \sigma,\ \tau\ :\ \sigma^n = 1,\ \tau^2 = 1,\ \tau\sigma\tau = \sigma^{-1} \rangle,$$

and let E_B/K be D_m-Galois extension with group presented as

$$\langle \hat{\sigma},\ \hat{\tau}\ :\ \hat{\sigma}^m = 1,\ \hat{\tau}^2 = 1,\ \hat{\tau}\hat{\sigma}\hat{\tau} = \hat{\sigma}^{-1} \rangle,$$

such that $K_1 = E_B \cap L$ is a D_k-extension of K corresponding to the fixed fields of $\langle \sigma^k \rangle \subset D_n$ and $\langle \hat{\sigma}^k \rangle \subset D_m$, where σ and $\hat{\sigma}$ (respectively τ and $\hat{\tau}$) act identically on K_1. Let L_B be the fixed field of $\langle \sigma^m \rangle$ in L.

Let F_1 be the fixed field of the elements $(\sigma^{ki}, \hat{\sigma}^{ki})$ in the compositum $E_B L_B$ for $0 \le i < m/k$. Then F_1/K is the unique $C_{m/k}$-Galois extension of K_1 corresponding to the Baer product (of Galois extensions) of E_B/K and the inverse of L_B/K. The subgroup $\langle \sigma \rangle \subset \mathrm{Gal}(K_1/K)$ lifts to a normal subgroup of $\mathrm{Gal}(F_1/K)$, generated by $\sigma \in \mathrm{Gal}(K_1/K)$ extended to $\mathrm{Gal}(F_1/K_1)$ as $(\sigma, \hat{\sigma})$. Let F_0 be the fixed field in F_1 of

this subgroup; it is the unique extension described in Theorem 3.1(a). By Theorem 3.1(b), then, letting $A = \langle \sigma^k \rangle$ and $B = \langle \sigma^m \rangle$, we have that E_B/K embeds in a D_n-extension E/K cyclic over K_0, *i.e.*, in which $\hat{\tau}$ and $\hat{\sigma}\hat{\tau}$ are lifted to elements of order 2, if and only if the $D_{m/k}$-extension F_0 of K embeds in a $D_{n/k}$-extension of K cyclic over K_0, with group

$$\langle \tilde{\sigma},\ \tilde{\tau}\ :\ \tilde{\sigma}^{n/k} = 1,\ \tilde{\tau}^2 = 1,\ \tilde{\tau}\tilde{\sigma}\tilde{\tau} = \tilde{\sigma}^{-1} \rangle,$$

where τ lifts to $\tilde{\tau}$. □

Now we specialize even further to the case of dihedral groups of 2-power order and field K of characteristic not 2. Suppose L/K is a Galois extension with $\mathrm{Gal}(L/K) \cong D_{2^d}$ and let K_0/K be the unique quadratic subextension corresponding to the fixed field in L of the cyclic subgroup C_{2^d}. Denote a generator of C_{2^d} in Galois group $\mathrm{Gal}(L/K)$ by σ. Let L_i be the fixed field in L of $\langle \sigma^{(2^i)} \rangle$ for $i = 1, \ldots, d$. Thus the set $\{L_i/K\}$ may be viewed as a tower of dihedral Galois extensions, with $\mathrm{Gal}(L_i/K) \cong D_{2^i}$.

It is well-known that all embeddings of L_i/K into $D_{2^{i+1}}$-Galois extensions of K cyclic over K_0 "differ" from L_{i+1} by a square root of an element in $K^\times$ (see for example [Bl, Lemma 4.1]); more precisely, if $L_{i+1} = L_i(\sqrt{\gamma_i})$ for some $\gamma_i \in L_i$, then all embeddings of L_i/K into $D_{2^{i+1}}$-Galois extensions cyclic over K_0 are of the form $L_i(\sqrt{r\gamma_i})$ for $r \in K^\times$, and any $L_i(\sqrt{r\gamma_i})$ is such an embedding. In the following theorem we determine the condition on r permitting such alternate $D_{2^{i+1}}$-Galois extensions to embed into $D_{2^{i+j}}$-Galois extensions cyclic over K_0; the condition is the solvability of a reduced embedding problem, which can be thought of as a quotient of the embedding problems extending L_{i+1} and $L_i(\sqrt{r\gamma_i})$, in the sense of our section 4. As stated above, if $i > 1$, then the cyclic over K_0 condition is automatically satisfied.

Theorem 3.3 (Dihedral 2-Group Reduction)**.** *Assume that the characteristic of the field K is different from 2. Let L/K be a D_{2^d}-Galois extension of fields, with L_i defined as above. Let $K_0 = K(\sqrt{ab})$ and $L_1 = K_0(\sqrt{a})$ for $a, b \in K^\times$. Choose $\gamma_i \in L_i$ such that $L_{i+1} = L_i(\sqrt{\gamma_i})$ for $i = 1, \ldots, d-1$. Let $r \in K^\times \smallsetminus {K^\times}^2$ such that r, a, b, and ab are independent in $K^\times/{K^\times}^2$.*

Then for $j = 1, \ldots, d-i$, the D_{2^i}-Galois field extension L_i embeds in a $D_{2^{i+j}}$-Galois field extension which extends $L_i(\sqrt{r\gamma_i})$ and is cyclic over K_0 if and only if the D_2-Galois field extension $K_0(\sqrt{r})/K$ embeds in a D_{2^j}-Galois field extension cyclic over K_0.

Proof. We apply Theorem 3.2 with $n = 2^{i+j}$, $m = 2^{i+1}$, $k = 2^i$; we must only determine F_0/K. We have that $E_B = L_i(\sqrt{r\gamma_i})$ and $L_B = L_{i+1} = L_i(\sqrt{\gamma_i})$. The compositum $E_B L_B$ is then $L_i(\sqrt{\gamma_i}, \sqrt{r})$, and the Baer product of E_B and the inverse of L_B over L_i is then $L_i(\sqrt{r})$, which is then F_1. Now F_0/K is a D_2-Galois extension extending $K_0/K = K(\sqrt{ab})/K$ inside F_1/K. Because $F_1 = L_i \otimes_K K(\sqrt{r})$, we have that $\mathrm{Gal}(F_1/K) \cong D_{2^i} \times C_2$, and the D_2-Galois subextensions are the $C_2 \times C_2$-Galois subextensions of the $C_2 \times C_2 \times C_2$-Galois subextension $K(\sqrt{a}, \sqrt{b}, \sqrt{r})$. By the discussion above Theorem 3.2 we know that $F_1 = F_0 \otimes_{K_0} L_i$, and since L_i contains the subextension $K(\sqrt{a}, \sqrt{b})$, we must have that F_0 is $K_0(\sqrt{rs}) = K_0(\sqrt{rsab})$ for $s = 1$ or a. But since F_1/L_i descends to F_0/K_0, we have that $s = 1$, *i.e.*, $F_0 = K_0(\sqrt{r}) = K(\sqrt{r}, \sqrt{ab})$. □

Examples 3.4: Explicit 2-Power Dihedral Extensions. For embedding problems consisting of small 2-power dihedral groups, the obstructions to their solution (see section 4) and some formulas for the explicit construction of their solution fields are well-known. We use these obstructions and our reduction theorems to describe some explicit 2-power dihedral extensions over fields K of characteristic not 2.

Examples 3.4.1 ($D_{2^v} \to D_4$)**.** It is known (from [GSS, Proposition 3.10], for instance) that any D_4-Galois extension W of such a field K is of the form $W = K(\sqrt{x+y\sqrt{a}}, \sqrt{b})$, where a and b are independent in $K^\times/K^{\times 2}$ and there exists $z \in K^\times$ such that $x^2 - ay^2 = bz^2$. The extension W/K is then cyclic over $K(\sqrt{ab})$.

Let $E_B = K(\sqrt{r(x+y\sqrt{a})}, \sqrt{b})$ for $r \in K^\times \smallsetminus K^{\times 2}$ an element such that r, a, b, and ab are independent in $K^\times/K^{\times 2}$. Now suppose that W embeds in a D_{2^v}-extension L of K. Then by Theorem 3.3, E_B embeds in a D_{2^v}-extension E of K if and only if $N = K(\sqrt{r}, \sqrt{ab})$ embeds in a $D_{2^{v-1}}$-extension of K cyclic over $K(\sqrt{ab})$.

Example 3.4.2 ($D_{16} \to D_8$)**.** First we describe all *admissible* D_8-extensions in the sense of [Sw1], applying the transformation described after [GSS, Theorem 4.5.2] correctly; note that this corrects an error in [GSS, Theorem 4.5.3] and describes all D_8-extensions over fields $K = \mathbb{Q}$ and $K = \mathbb{Q}(t)$.

Let $L_B = K(\chi, \sqrt{b})$, where

$$\chi = \sqrt{s\left(\tilde{z} + \frac{y}{2}\sqrt{a}\right)\left(2x + 2\left(c + \frac{aey^2}{4} - \frac{exy}{4}\sqrt{a}\right)\sqrt{x+y\sqrt{a}}\right)}.$$

Here a and b are independent mod $K^{\times 2}$; $s \in K^\times$; x, y, and z satisfy $x^2 - ay^2 = bz^2$ as above; $\tilde{z}, w \in K$ are such that $\tilde{z}^2 - 2w^2 = ay^2/4$; $c, e \in K$ are such that $c^2 + (aby^2\tilde{z}^2/16)e^2 = x/2$; $z \neq 0$; $w \neq 0$; $z \neq w$; and $z \neq ay^2/(2x)$. Then L_B is a D_8-extension of K extending W, and all D_8-extensions of $\mathbb{Q}$ or $\mathbb{Q}(t)$ may be so described for suitable W.

Second, we describe an E_B resulting from a solvable embedding problem in Example 3.4.1. Let r be such that the embedding problem for $K(\sqrt{r}, \sqrt{ab})$ and $D_4 \to D_2$ is solvable with a solution field cyclic over $K(\sqrt{ab})$, as in Example 3.4.1. Then, by [GSS, Proposition 3.10], the quaternion algebra $(r, -ab)_K$ must be split. Applying [GSS, Theorem 4.5.3] to L_B/K, the quaternion algebra $(2x, -ab)_K$ is split. Viewing the quaternion algebras as Hilbert symbols, we have $(r, -ab)(2x, -ab) \sim (2xr, -ab) \sim (rx/2, -ab)$. Hence there exist $c', e' \in K$ satisfying

$$c'^2 + (ab(ry)^2(rz)^2/16)e'^2 = rx/2.$$

The D_8-extensions E_B/K which solve the problem of Example 3.4.1 are then described with $x' = rx$, $y' = ry$, $z' = rz$, $\tilde{z}' = r\tilde{z}$, $w' = rw$, and $E_B = K(\sqrt{\chi'}, \sqrt{b})$, where

$$\chi' = \sqrt{s'\left(\tilde{z}' + \frac{y'}{2}\sqrt{a}\right)\left(2x' + 2\left(c' + \frac{ae'y'^2}{4} - \frac{e'x'y'}{4}\sqrt{a}\right)\sqrt{x'+y'\sqrt{a}}\right)},$$

$s' \in K^\times$. Let $\hat{\sigma}$ be a generator of the C_8-subgroup of $\mathrm{Gal}(E_B/K)$, and let $\hat{\tau} \in \mathrm{Gal}(E_B/K)$ leave χ' invariant.

Now suppose that L_B embeds in a D_{16}-extension of K. One shows, using the relations for admissible dihedral extensions in [Sw1], that the element

$$\nu = \chi\chi' + \chi^{\sigma}\chi'^{\hat{\sigma}} + \chi^{\sigma^2}\chi'^{\hat{\sigma}^2} + \chi^{\sigma^3}\chi'^{\hat{\sigma}^3}$$

lies in F_0 and has square

$$32ss'r^2x^2\tilde{z}^2 + q'\sqrt{r}$$

for $q' \in K$. Therefore the element $\omega = \nu/(4rx\tilde{z}) \in N$ has square $2ss' + q\sqrt{r}$ for $q \in K$. Then we have that

$$F_0 = K\left(\sqrt{2ss' + q\sqrt{r}}, \sqrt{ab}\right)$$

for $q \in K^{\times}$ and we have found the F_0 such that *E_B embeds in a D_{16}-extension of K if and only if F_0 embeds in a D_8-extension of K.*

4. Applications to Obstructions to Central C_p-Embedding Problems

When the embedding problem under consideration is central with kernel isomorphic to C_p over the field k containing p-th roots of unity, one associates to the problem an element of p-torsion component of the Brauer group, known as the *obstruction*. This element often determines the precise solvability conditions of the associated embedding problem; see Remark 4.2 below. In this section we explore some of the implications of our Main Theorem in the theory of obstructions.

From our Main Theorem we deduce that the condition determining the solvability of an abelian relative embedding problem is identical to the condition determining the solvability of a reduced embedding problem. In the following Theorem 4.3 we make this statement precise in the context of central Galois embedding problems with kernel C_p over a k-algebra containing the p-th roots of unity, proving that the reduced embedding problem can be viewed as a quotient of two embedding problems, and, moreover, that the obstruction of the reduced embedding problem is the quotient of the obstructions to the two associated embedding problems. Thus, even when it is not known that one of the embedding problems is solvable, we have that the reduced embedding problem expresses the condition by which the two embedding problems differ. Then, in Theorem 4.6, we show how a phenomenon related to this connection gives information about the structure of the obstructions, particularly when the obstructions can be expressed as tensor products of p-cyclic algebras. In what follows, we denote the Brauer group of a ring R by $\mathrm{Br}(R)$.

Definition 4.1. Let p be a prime and k a field of characteristic not p containing the full group μ_p of p-th roots of unity. Let $(S_B/R, \eta_{S_B})$ be an H-Galois extension of k-algebras. Let $f\colon G \twoheadrightarrow H$ be a surjection of groups where $B = \ker f$ is central and isomorphic to C_p. Then *the obstruction $O_{S_B/R} = O_{S_B/R,\eta_{S_B},f}$ of the embedding problem* $(S_B/R, \eta_{S_B}, f)$ is the class $[(S_B/R, \eta_{S_B}, \overline{c_f})] \in \mathrm{Br}(R)$ of the crossed product $(S_B/R, \eta_{S_B}, \overline{c_f})$, where $\overline{c_f} \in H^2(H, \mu_p \cong B)$ is a 2-cocycle describing the C_p-extension G of H.

Remark 4.2. If R is a field K, then in some situations the obstruction is a "proper" obstruction, *i.e.*, the embedding problem has a (proper) solution if and only if the obstruction vanishes in $\mathrm{Br}(K)$, which means that the class of the crossed product is trivial. One situation is when the embedding problem is Frattini. Another is when the field K is Hilbertian, by a result of Ikeda [Ik]. The obstruction is also

useful in constructing the solutions of the embedding problem: given an explicit isomorphism from a matrix ring over K to a representative of the Brauer class, one has a method explicitly to construct all of the solution fields [Sw2].

Theorem 4.3. *Let p be a prime and k a field of characteristic not p containing the full group μ_p of p-th roots of unity. Let G be a group with a normal abelian subgroup A containing a subgroup $B \cong C_p$ lying in the center of G. Let $H = G/B$, and let $(S_B/R, \eta_{S_B})$ and $(T_B/R, \eta_{T_B})$ be two H-Galois extensions (of algebras) which are common over $(R_1/R, \eta_{R_1})$, the fixed subalgebra with quotient action of $\eta_{S_B}(A/B)$ in S_B and of $\eta_{T_B}(A/B)$ in T_B.*

Then, as elements of $\mathrm{Br}(R)$,

$$O_{S_B,\eta_{S_B/R},G\longrightarrow G/B}O^{-1}_{T_B/R,\eta_{T_B},G\longrightarrow G/B} = O_{U_0/R,\eta_{U_0},A\rtimes G/C(A)\xrightarrow{\text{can}}A/B\rtimes G/C(A)},$$

where $(U_0/R, \eta_{U_0})$ is the fixed subalgebra with quotient action of $1 \rtimes C(A)/A$ in the $A/B \rtimes G/A$-Galois extension $(U_1/R, \eta_{U_1})$, which in turn is given by the Baer product of the Galois extension (S_B, η_{S_B}) and the inverse of the Galois extension (T_B, η_{T_B}).

Proof. Let $N = S_B \otimes_{R_1} T_B$, with group Γ, be the amalgamated product of H and $\bar{H}$ over G/A, and action $\eta_N = \eta_{S_B} \otimes \eta_{T_B} i$, where i is the isomorphism from the Baer inverse $\bar{H}$ of H over G/A to H. Then the Baer product $(U_1/R, \eta_{U_1})$ is the fixed subalgebra of N corresponding to the subgroup $(A/B)^{\sim}$ consisting of elements $(a, \overline{a}^{-1})$, $a \in A/B$, and is an $A/B \rtimes G/A$-Galois extension. Note that in this proof we emphasize elements of $\bar{H}$ by denoting them with a bar.

Let $f\colon G \twoheadrightarrow H = G/B$ denote the surjection of the embedding problems associated to S_B/R and T_B/R, and let $r\colon A \rtimes G/C(A) \twoheadrightarrow A/B \rtimes G/C(A)$ denote the surjection of the embedding problem associated to U_0/R. We consider $\inf_{N/S_B} c_f$, $\inf_{N/T_B} c_f^{-1}$, and $\inf_{N/U_0} c_r$ in the cohomology group $H^2(\eta_N(\Gamma), \mu_p)$, where $\eta_N(\Gamma)$ acts trivially on μ_p. Note that in order to make precise the inflation maps, we must specify the maps between actions which are to take place; these are the maps, respectively, $\eta_N(\Gamma) \to \eta_{S_B}(H)$, $\eta_N(\Gamma) \to (\eta_{T_B} i)(\bar{H})$, and $\eta_N(\Gamma) \to \eta_{U_1}(A/B \rtimes G/A) \to \eta_{U_0}(A/B \rtimes G/C(A))$, of Galois theory.

The inflation map $\inf_{N/S_B}$ corresponds to amalgamation with $(T_B/R, \eta_{T_B} i)$. More precisely, the map takes the class of an extension of the H-Galois extension $(S_B/R, \eta_{S_B})$ by an extension with group B and sends it to the class of the amalgamation of this extension with the H-Galois extension $(T_B/R, \eta_{T_B} i)$ over the common subextension $(R_1/R, \eta_{R_1})$. Hence $\inf_{N/S_B} c_f$ describes a group Γ_1 which is the amalgamation of G with the Baer inverse of G/B, over the common factor group G/A, where the kernel of $\Gamma_1 \twoheadrightarrow \Gamma$ commutes with elements in $A/B \subset (\eta_{T_B} i)(\bar{H})$. In 2-cocycle notation, this map is expressed as follows:

$$(\inf_{N/S_B} c_f)((h_1, \overline{h_2}), (h_3, \overline{h_4})) = c_f(h_1, h_3), \quad (h_1, \overline{h_2}), (h_3, \overline{h_4}) \in \Gamma.$$

Similarly, the inflation map $\inf_{N/T_B}$ corresponds to amalgamation with $(S_B/R, \eta_{S_B})$. Thus, $\inf_{N/T_B} c_f^{-1}$ describes a group Γ_2 which is the amalgamation of G/B with $\bar{G}$, over the common factor group G/A, where the kernel of $\Gamma_2 \twoheadrightarrow \Gamma$ commutes with elements in $A/B \subset \eta_{S_B}(H)$. In 2-cocycle notation, this map is expressed as follows:

$$(\inf_{N/T_B} c_f^{-1})((h_1, \overline{h_2}), (h_3, \overline{h_4})) = c_f^{-1}(i(\overline{h_2}), i(\overline{h_4})), \quad (h_1, \overline{h_2}), (h_3, \overline{h_4}) \in \Gamma.$$

By [ILF, Theorem 3.15.1], the multiplication of classes in $H^2(\eta_N(\Gamma), \mu_p)$ corresponds on one hand to function multiplication, and on the other to the Baer product of the group extensions corresponding to the classes, where the amalgamation occurs over Γ. Hence the quotient $(\inf_{N/S_B} c_f)(\inf_{N/T_B} c_f^{-1})$ describes the Baer product $\tilde{\Gamma}$ of Γ_1 and Γ_2 over Γ. Since Γ is the amalgamated product of H and $\bar{H}$ over G/A, and since Γ_1 is the amalgamation of G and $\bar{H}$ over G/A, and Γ_2 is the amalgamation of H and $\bar{G}$ over G/A, we have that $\tilde{\Gamma}$ is the quotient of the amalgamation of G and $\bar{G}$ over G/A by the set of elements $(b, \overline{b}^{-1})$, $b \in B$.

By the definition of the Baer product, we have a canonical surjection $p\colon \tilde{\Gamma} \twoheadrightarrow \Gamma$. Consider $p^{-1}((A/B)^{\check{}}) \subset \tilde{\Gamma}$. Let $(a_1, \overline{a_1}^{-1})$, $(a_2, \overline{a_2}^{-1}) \in (A/B)^{\check{}}$. By function multiplication of 2-cocycles in $Z^2(\eta_N(\Gamma), \mu_p)$ we have that

$$\begin{aligned}&\left(\inf_{N/S_B} c_f \cdot \inf_{N/T_B} c_f^{-1}\right)\left((a_1, \overline{a_1}^{-1}), (a_2, \overline{a_2}^{-1})\right)\\ &\quad = \left(c_f(a_1, a_2) \cdot c_f^{-1}(i(\overline{a_1}^{-1}), i(\overline{a_2}^{-1}))\right) = c_f(a_1, a_2) c_f^{-1}(a_1, a_2) = 1.\end{aligned}$$

Therefore, when restricted to $(A/B)^{\check{}}$, the group extension $\tilde{\Gamma}$ of Γ corresponds to $(A/B)^{\check{}} \times B$. Hence the subgroup $(A/B)^{\check{}} \times 1$ of $\tilde{\Gamma}$ is isomorphic to $(A/B)^{\check{}}$ and is a preimage of $(A/B)^{\check{}}$ under p. By abuse of notation we denote this subgroup $(A/B)^{\check{}} \subset \tilde{\Gamma}$.

We now consider the quotient of $\tilde{\Gamma}$ by $(A/B)^{\check{}}$. Because $\tilde{\Gamma}$ is the quotient of the amalgamated product of G and $\bar{G}$ over G/A by the elements $(b, \overline{b}^{-1})$, $b \in B$, and the elements in $(A/B)^{\check{}}$ are of the form $(a, \overline{a}^{-1})$, $a \in A/B$, we have that $\tilde{\Gamma}/(A/B)^{\check{}}$ is the quotient of the amalgamated product of G and $\bar{G}$ over G/A by the elements $(a, \overline{a}^{-1})$, $a \in A$, or, in other words, the Baer product of G and $\bar{G}$ over G/A, which is the semidirect product $A \rtimes G/A$. Furthermore, we may view $(A/B)^{\check{}}$ as the group of the Galois subextension $(N/U_1, \eta_N)$, so that $\Gamma/(A/B)^{\check{}}$ is the group of the Galois extension $(U_1/R, \eta_{U_1})$ and $\tilde{\Gamma}$ is the group extension of Γ given by the surjection $A \rtimes G/A \xrightarrow{\text{can}} A/B \rtimes G/A$. Indeed, the group $\tilde{\Gamma}$ appears by amalgamation of $\tilde{\Gamma}/(A/B)^{\check{}}$ with the Galois extension $(N/U_1, \eta_N)$.

On the other hand, r describes the group extension problem $A \rtimes G/C(A) \xrightarrow{\text{can}} A/B \rtimes G/C(A)$. Let R_0 be the fixed subalgebra of $C(A)/A$ in the G/A-Galois extension (R_1, η_{R_1}). Then $U_1 = U_0 \otimes_{R_0} R_1$ and $\eta_{U_1} = \eta_{U_0} \otimes \eta_{R_1}$. By the argument in Proposition 2.7 the inflation $c_r' = \inf_{U_1/U_0} c_r$ sends this group extension to the group extension $A \rtimes G/A \xrightarrow{\text{can}} A/B \rtimes G/A$. By the previous paragraph $\inf_{N/U_1} c_r'$ describes $\tilde{\Gamma}$, so we are done. □

Examples 4.4: Cyclic 2-Power Obstructions over Fields. In each of the following cases we set $B = C_2$ and consider central C_2-extensions over a field $R = K = k$ of characteristic not 2. We use the notation for fields established at the beginning of section 3.

Example 4.4.1 ($C_8 \to C_4$ over C_2)**.** Let $G = C_8 = \langle\sigma\rangle$, $A = \langle\sigma^2\rangle$, $B = \langle\sigma^4\rangle$. Then $H = G/B \cong C_4$. It is well-known that H-Galois extensions E_B/K and L_B/K common over the G/A-extension $K_1/K = K(\sqrt{d})/K$ are all of the form

$$K\left(\sqrt{rd + ry\sqrt{d}}\right),$$

$r \in K^\times$, where there exist $x, y \in K^\times$ such that $x^2 + y^2 = d \in K^\times \smallsetminus {K^\times}^2$ (see, for example, [GSS, Proposition 3.4]). Let

$$E_B/K = K\left(\sqrt{r_1 d + r_1 y\sqrt{d}}\right)/K$$

and

$$L_B/K = K\left(\sqrt{r_2 d + r_2 y\sqrt{d}}\right)/K,$$

where r_1, r_2, and d are necessarily independent in $K^\times/{K^\times}^2$. Then $F_0/K = K(\sqrt{r_1 r_2})/K$. By [Sc] we have that $O_{E_B/K} = (2,d)(-1,r_1)$, where the latter is the class of a tensor product of quaternion algebras over K; $O_{L_B/K} = (2,d)(-1,r_2)$; and $O_{F_0/K} = (-1, r_1 r_2)$. Then Theorem 4.3 gives us the following relation in $\mathrm{Br}(K)$:

$$\big((2,d)(-1,r_1)\big)\big((2,d)(-1,r_2)\big)^{-1} = (-1, r_1 r_2).$$

Example 4.4.2 ($C_{16} \to C_8$ over C_2 for $K = \mathbb{Q}$ or $\mathbb{Q}(t)$)**.** Let $G = C_{16} = \langle\sigma\rangle$, $A = \langle\sigma^2\rangle$, $B = \langle\sigma^8\rangle$. Then $H = G/B \cong C_8$. By [Sw1], all H-Galois extensions E_B/K and L_B/K common over the G/A-extension $K_1/K = K(\sqrt{d})/K$ which are admissible in the sense of [Sw1] are all of the form

$$K\left(\sqrt{s(z+\sqrt{d})(2rd + v\psi + u\psi^\sigma)}\right),$$

for $r, s \in K^\times$, where $\psi = (rd + ryd^{1/2})^{1/2}$; there exist $x, y \in K^\times$ such that $x^2 + y^2 = d \in K^\times \smallsetminus {K^\times}^2$; $z, w \in K$ such that $z^2 - 2w^2 = d$; and $t_1, t_2 \in K$ such that $t_1^2 + t_2^2 = r$; and $u = t_1 x - t_2 y - t_1 y - t_2 x$, $v = t_1 x - t_2 y + t_1 y + t_2 x$. Note that in our case the x, y, z, and w may be fixed for both E_B and L_B. By [Sc], all H-Galois extensions over $\mathbb{Q}$ and $\mathbb{Q}(t)$ are admissible.

Let

$$E_B/K = K\left(\sqrt{s_1(z+\sqrt{d})(2r_1 d + v_1\psi_1 + u_1\psi_1^\sigma)}\right)/K$$

and

$$L_B/K = K\left(\sqrt{s_2(z+\sqrt{d})(2r_2 d + v_2\psi_2 + u_2\psi_2^\sigma)}\right)/K,$$

where r_1, r_2, and d are necessarily independent in $K^\times/{K^\times}^2$; $r_1 = t_{1,1}^2 + t_{1,2}^2$; $r_2 = t_{2,1}^2 + t_{2,2}^2$; and u_1, u_2, v_1, and v_2 are defined analogously. Then one shows that

$$F_0/K = K\left(\sqrt{s_1 s_2 r_1 r_2 + s_1 s_2 (t_{1,1}t_{2,1} \pm t_{1,2}t_{2,2})\sqrt{r_1 r_2}}\right)/K.$$

Using [Sw1] for the computation of obstructions, we have that

$$O_{E_B/K} = (s_1(z-w), -1)(r_1 z(z-y), -2)(z(z-w), d),$$

where the latter is the class of a tensor product of three quaternion algebras over K;

$$O_{L_B/K} = (s_2(z-w), -1)(r_2 z(z-y), -2)(z(z-w), d);$$

and $O_{F_0/K} = (-1, s_1s_2)(2, r_1r_2)$. Then Theorem 4.3 gives us the following relation in $\mathrm{Br}(K)$:

$$\begin{aligned}&\big((s_1(z-w),-1)(r_1z(z-y),-2)(z(z-w),d)\big)\\&\quad\cdot\big((s_2(z-w),-1)(r_2z(z-y),-2)(z(z-w),d)\big)^{-1}\\&\quad=(-1,s_1s_2)(-2,r_1r_2)=(-1,s_1s_2)(2,r_1r_2).\end{aligned}$$

The last equality holds since

$$(-1,r_1)=(-1,r_2)=(-1,r_1r_2)=1.$$

We now introduce the concept of a relatively general pair of embedding problems and prove a structural statement about obstructions of relatively general pairs, followed by an example of this phenomenon.

Definition 4.5. Let p be a prime and k a field of characteristic not p containing the full group μ_p of p-th roots of unity. Let G be a finite group with normal abelian subgroup A, containing a normal subgroup $B \cong C_p$.

Suppose that $(S_B/R, \eta_{S_B})$ is a G/B-Galois extension and $(U_0/R, \eta_{U_0})$ is an $A/B \rtimes G/C(A)$-Galois extension, common over the $G/C(A)$-Galois extension $(R_0/R, \eta_{R_0})$, the fixed subalgebra with quotient action of $\eta_{S_B}(C(A)/B)$ in S_B and $\eta_{U_0}(A/B \rtimes 1)$ in U_0. Let the G/A-Galois extension $(R_1/R, \eta_{R_1})$ be the fixed subalgebra with quotient action of $\eta_{S_B}(A/B)$ in S_B. Let $(T_B/R, \eta_{T_B})$ denote the Baer product of $(S_B/R, \eta_{S_B})$ and $((U_0 \otimes_{R_0} R_1)/R, \eta_{U_0} \otimes \eta_{R_1})$ over $(R_1/R, \eta_{R_1})$.

Then $(S_B/R, \eta_{S_B})$ and $(U_0/R, \eta_{U_0})$ form a *relatively general pair* if there exists an injection $\alpha\colon R \to R$ and an R_1-isomorphism $\beta\colon S_B \otimes_\alpha R \to T_B$ such that $\beta(s^{\eta_{S_B}(g)}) = \beta(s)^{\eta_{T_B}(g)}$ for $s \in S_B$, $g \in G/B$.

Theorem 4.6. *Let $(S_B/R, \eta_{S_B})$ and $(U_0/R, \eta_{U_0})$ form a relatively general pair. Then*

$$\alpha\left(O_{S_B/R,\eta_{S_B},G\to G/B}\right)\ O^{-1}_{S_B/R,\eta_{S_B},G\to G/B} = O_{U_0/R,\eta_{U_0},A\rtimes G/C(A)\xrightarrow{\mathrm{can}}A/B\rtimes G/C(A)},$$

where α acts on the crossed product via $(\cdot \otimes_\alpha R)$ on S_B and $\mathrm{id}_{G/B}$ on G/B.

Proof. By Theorem 4.3 we need only show that the two crossed products

$$O_{T_B/R,\eta_{T_B},G\to G/B}, \qquad \alpha\left(O_{S_B/R,\eta_{S_B},G\to G/B}\right)$$

are R-isomorphic, and this isomorphism is given by extending the β of the definition of a relatively general pair by the identity on the elements of G/B in the crossed product. □

Example 4.7: $D_8 \to D_4$. Let k be a field of characteristic not 2. As in Example 3.4.1, it is well-known that D_4-extensions over a field K of characteristic not 2 are of the form $K(\sqrt{x+y\sqrt{a}}, \sqrt{b})/K$, for a choice of $a, b \in K$ such that a and b are independent in $K^\times/K^{\times 2}$, and there exist x, y, $z \in K$ such that $x^2 - ay^2 - bz^2 = 0$. Let

$$R = k[a,b,x,y,z,r](1/abrxyz)/\langle x^2 - ay^2 - bz^2\rangle.$$

Note that R is étale over a localized polynomial ring $k[a,b,x,y,z,r](1/abrxyz)$, and thus R is normal, *i.e.* integrally closed in its field of fractions. Next, let

$$S_B/R = R\left(\sqrt{x+y\sqrt{a}}, \sqrt{b}\right)/R.$$

Note that S_B is étale over R and thus is normal. Since the field extension corresponding to fields of fractions of S_B/R is a D_4-Galois extension, we have that S_B/R is a D_4-Galois extension. Let

$$G = D_8 = \langle \sigma,\ \tau\ :\ \sigma^8 = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} \rangle,$$

and let $A = \langle \sigma \rangle$, $B = \langle \sigma^2 \rangle$. Then the corresponding reduced embedding problem is that of $D_4 \to D_2$, and we choose the D_2-Galois extension $U_0/R = R\left(\sqrt{ab}, \sqrt{r}\right)/R$. One shows that

$$T_B/R = R\left(\sqrt{rx + ry\sqrt{a}}, \sqrt{b}\right)/R.$$

Let $\alpha\colon R \to R$ be given by $\alpha(a) = a$, $\alpha(b) = b$, $\alpha(r) = r$, $\alpha(x) = rx$, $\alpha(y) = ry$, $\alpha(z) = rz$; then α and $\beta = \mathrm{id}$ show that S_B/R and U_0/R are a relatively general pair. We have that

$$O_{S_B/R, \eta_{S_B}, D_8 \to D_4} = (a, 2)(2x, -ab),$$

where the latter denotes the tensor product of a pair of quaternion algebras, and

$$O_{U_0/R, \eta_{U_0}, D_4 \to D_2} = (r, -ab).$$

Applying Theorem 4.6, we recover

$$\big((a, 2)(2xr, -ab)\big)\big((a, 2)(2x, -ab)\big)^{-1} = (r, -ab).$$

5. Applications to p-Metacyclic Embedding Problems: Determining Towers

Constructing large dihedral extensions of a field remains a problem of interest, and if one uses the theory of embedding problems, one naturally seeks to "climb up" a tower of dihedral extensions, constructing them iteratively. The case of dihedral towers is a particularly attractive context for the theory of relative embedding problems since the existence of *infinite* towers of dihedral extensions implies that results such as Theorem 3.3 have a fairly general application. In order to find similarly general contexts, we are led to consider other infinite towers of groups for which our Main Theorem is applicable. In this section we classify, for all p, all towers which are analogous in a certain sense: given a fixed metacyclic nonabelian p-group G with normal cyclic subgroup A and cyclic quotient G/A, we determine all towers of metacyclic p-groups over G which extend the cyclic group A. We do not treat the case of abelian groups, since the many towers over a given abelian group which contain a nonabelian member are distinguished by their smallest nonabelian group. In determining the towers, we also specify the corresponding groups which occur in the reduced embedding problems.

We first recall a description of metacyclic p-groups which is particularly useful for our purposes, due to Liedahl [Li]. Let G be a metacyclic p-group of order p^N. Then G can be specified by a quintuple (c, n, m, t, s) with parameters limited to the following three types, where in every case $n + m = N$:

Case 1 ($c = 1$; p odd):

$$G \cong \langle x,\ y\ \mid\ x^{p^n} = 1,\ y^{p^m} = x^{p^s},\ yxy^{-1} = x^{(p+1)^{p^t}} \rangle,$$

$$t \in \{\max(0, n - m - 1), \cdots, n - 1\}, \quad s \in \{n - t - 1, \cdots, \min(n, m)\};$$

Case 2 ($c = 2$; $p = 2$):

$$G \cong \langle x,\ y \mid x^{2^n} = 1,\ y^{2^m} = x^{2^s},\ yxy^{-1} = x^{5^{2^t}} \rangle,$$

$$t \in \{\max(0, n-m-2), \cdots, n-2\}, \quad s \in \{n-t-2, \cdots, \min(n,m)\};$$

Case 3 ($c = 3$; $p = 2$):

$$G \cong \langle x,\ y \mid x^{2^n} = 1,\ y^{2^m} = x^{2^s},\ yxy^{-1} = x^{-5^{2^t}} \rangle, \quad 2 \le n \le N-1,$$

$$t \in \{\max(0, n-m-2), \cdots, n-2\}, \quad s \in \{n-1, \min(n, N-n+t+1)\}.$$

These descriptions are not unique: as [Li, Remark 2.4.3] points out, even discounting the many presentations of the above types for groups of order p and p^2, the metacyclic p-groups which are split by a cyclic subgroup may have multiple descriptions, and there are some groups which have presentations of both the second and third types. However, in the following proposition we insure that once we fix the normal subgroup $A = \langle x \rangle$, then there is a unique set of parameters (c, n, m, t, s) above.

Proposition 5.1. *Let G be a nonabelian metacyclic p-group with normal cyclic subgroup A and cyclic quotient group G/A. Then there exists one and exactly one presentation above for G in which $\langle x \rangle = A$.*

Proof. By [Li] we know that any nonabelian metacyclic p-group has a presentation listed above and that we may choose one such that $\langle x \rangle = A$. We must show then that if $\tilde{x}$ and $\tilde{y}$ are any two generators of G, with $\tilde{x} \in A$, then the resulting presentation of G as $\langle \tilde{x}, \tilde{y} \rangle$ is identical to the first.

First, note that for any presentation above with generators $\tilde{x}$ and $\tilde{y}$, the pair $\hat{x}$ and $\tilde{y}$, where $\hat{x}$ is any element such that $\langle \tilde{x} \rangle = \langle \hat{x} \rangle$, generate G with the same presentation as $\tilde{x}$ and $\tilde{y}$. Hence if G has another presentation $G = \langle \tilde{x}, \tilde{y} \rangle$ with $\langle \tilde{x} \rangle = A$ in addition to the first presentation $G = \langle x, y \rangle$, then we may assume without loss of generality that $x = \tilde{x}$. We then must show that for no other choice of $\tilde{y} \in G$ such that $G = \langle x, \tilde{y} \rangle$ does the pair x, $\tilde{y}$ satisfy a different presentation as above.

Depending on the case of the first presentation, we have that $yxy^{-1} = x^{(p+1)^{p^t}}$ (in case 1), or $yxy^{-1} = x^{\pm 5^{2^t}}$ (in cases 2 and 3). Consider a general element $\tilde{y} = x^i y^j \in G \smallsetminus A$ with $0 \le i < p^n$ and $0 < j < p^m$. The conjugation relation between x and $\tilde{y}$ becomes

$$\tilde{y}x\tilde{y}^{-1} = (x^i y^j)x(x^i y^j)^{-1} = x^{(p+1)^{jp^t}}$$

in case 1 and

$$\tilde{y}x\tilde{y}^{-1} = x^{(\pm 1)^j 5^{j 2^t}}$$

in cases 2 and 3. Now if $(j, p) \neq 1$, then

$$\tilde{y}^{p^{m-1}} = (x^i y^j)^{p^{m-1}} \in A,$$

whence $\langle x, \tilde{y} \rangle \subsetneq G$. Moreover, since the presentations above restrict the exponent of x in the conjugation relation to be a power of p, a power of 5, or the negative of a power of 5, we cannot have that $\tilde{y} = x^i y^j$ for some $j > 1$ with $(j, p) = 1$; hence no other choice of $\tilde{y}$ save $x^i y$ can serve as another possible generator with x.

We then invoke [Li, §2.1], which insures that no two of the presentations above describe the same group under an isomorphism $x \mapsto x,\ y \mapsto x^i y$. Hence the only $\tilde{y}$ such that $G = \langle x, \tilde{y} \rangle$ under a presentation above is $\tilde{y} = y$. Once the normal cyclic subgroup $A = \langle x \rangle$ is fixed, then, the presentation of G is unique. □

In the following theorem and corollary we describe the set of towers of metacyclic p-groups which have a given nonabelian group G as the smallest member and which only extend a fixed normal cyclic subgroup A. In the situation of Galois theory, then, if $G = \mathrm{Gal}(M/K)$ with $L = M^A$, then we show the possible Galois groups of Galois field extensions $\tilde{M}/K$ with degree p^N such that $\mathrm{Gal}(\tilde{M}/L)$ is cyclic, extending $A = \mathrm{Gal}(M/L)$.

Theorem 5.2 (Towers)**.** *Let G be a nonabelian metacyclic p-group with distinguished cyclic subgroup A, and let (c, n, m, t, s) be its unique parameters as in Proposition 5.1. Consider the set of metacyclic p-groups H such that there exists a surjection $f\colon H \twoheadrightarrow G$ which extends $\langle x \rangle$ in G,* i.e.*, we have $(x \in H) \mapsto (x \in G)$ and $\ker f = \langle x^{p^n} \rangle$. Then the parameters as above for the set of such groups H, together with the centralizers $C_H(\langle x \rangle)$ and the quotient groups $H/C_H(\langle x \rangle)$, are as follows:*

Case 1: If $s \neq n$, then $n' \in \{n+1, \cdots, \min(t+m+1, s+t+1)\}$; $m' = m$; $t' = t$; $s' = s$; $C_H(\langle x \rangle) = \langle x, y^{p^{n'-t-1}} \rangle$; and $H/C_H(\langle x \rangle) \cong C_{n'-t-1}$.

If $s = n$, then $n' \in \{n+1, \cdots, t+m+1\}$; $m' = m$; $t' = t$; $s' \in \{\max(n'-t-1, n), \cdots, \min(n', m)\}$; $C_H(\langle x \rangle) = \langle x, y^{p^{n'-t-1}} \rangle$; and $H/C_H(\langle x \rangle) \cong C_{n'-t-1}$.

Case 2: If $s \neq n$, then $n' \in \{n+1, \cdots, \min(t+m+2, s+t+2)\}$; $m' = m$; $t' = t$; $s' = s$; $C_H(\langle x \rangle) = \langle x, y^{2^{n'-t-2}} \rangle$; and $H/C_H(\langle x \rangle) \cong C_{n'-t-2}$.

If $s = n$, then $n' \in \{n+1, \cdots, t+m+2\}$; $m' = m$; $t' = t$; $s' \in \{\max(n'-t-2, n), \cdots, \min(n', m)\}$; $C_H(\langle x \rangle) = \langle x, y^{2^{n'-t-2}} \rangle$; and $H/C_H(\langle x \rangle) \cong C_{n'-t-2}$.

Case 3: If $s = n-1 \neq m+t+1$, then there are no such groups. If $s = n$ or $s = n-1 = m+t+1$, and $t < n-2$, then $n' \in \{n+1, \cdots, t+m+2\}$; $m' = m$; $t' = t$; $s' \in \{n'-1, \cdots, \min(n', m+t+1)\}$; $C_H(\langle x \rangle) = \langle x, y^{2^{n'-t-2}} \rangle$; and $H/C_H(\langle x \rangle) \cong C_{n'-t-2}$.

If $s = n$ and $t = n-2$, then $n' > n$; $m' = m$; $t' \in \{\max(n-2, n'-m-2), \cdots, n'-2\}$; $s' \in \{n'-1, \cdots, \min(n', m+t'+1)\}$; $C_H(\langle x \rangle) = \langle x, y^2 \rangle$; and $H/C_H(\langle x \rangle) \cong C_2$.

Corollary 5.3 (Infinite Towers)**.** *The infinite towers of nonabelian metacyclic p-groups extending a fixed normal cyclic subgroup $\langle x \rangle$ in the sense of Theorem 5.2 have as foundations the 2-groups of the following type:*

$$\langle x, y \mid x^{2^n} = 1, y^{2^m} = 1, yxy^{-1} = x^{-1} \rangle.$$

If A is a subgroup of $\langle x \rangle$, then $C(A) = \langle x, y^2 \rangle$ and $G/C(A) \cong C_2$.

Proof of Theorem 5.2. Let (c', n', m', t', s') be a description of a group H satisfying the conditions of the theorem. Then under the surjection f, the elements $x \in H$ and $y \in H$ are sent to generators $f(x)$, $f(y)$ of G, respectively, and these generators are associated to a presentation of G related to that of H, with description $(c'', n'', m'', t'', s'')$. We study this description of G; then, based on the uniqueness of the presentation of G, we deduce restrictions on the presentation of H. The descriptions of $C_H(\langle x \rangle)$ and $H/C_H(\langle x \rangle)$ in the statement of the theorem are easily calculated.

Assume that the presentation of H falls into one of the first two cases. Then G has a parametrization in the same case. First, $f(x)$ clearly has order p^n, so $n'' = n$. Second, since $f(y)$ must have the same order as y, $m'' = m'$. Depending on the case, we have in H the conjugation relation

$$yxy^{-1} = x^{(p+1)^{p^{t'}}}$$

in case 1, or

$$yxy^{-1} = x^{5^{2^{t'}}}$$

in case 2. Now the order of the automorphism $x \mapsto x^{p+1}$ is p^{n-1} in case 1, where p^n is the order of x; similarly, the order of the automorphism $x \mapsto x^5$ is 2^{n-2} in case 2. Hence if $t' \geq n-1$ in case 1 or $t' \geq n-2$ in case 2, then we have that G is abelian, which by hypothesis it is not, and otherwise we may take $t'' = t'$. Note that t'' lies within the appropriate bounds, because, in case 1, if $n' - m' - 1 \leq t'$, then since $n \leq n'$ and $m'' = m'$, we have $n'' - m'' - 1 \leq t''$, and the analysis is the same for case 2.

Again, depending on the case, we have that

$$y^{p^{m'}} = x^{p^{s'}}$$

in case 1, or

$$y^{2^{m'}} = x^{2^{s'}}$$

in case 2, so that if $s' \geq n$ in either case, we may take $s'' = n$, otherwise $s'' = s'$; hence $s'' = \min(s', n)$. Note that s'' lies within the appropriate bounds, for $s'' \leq m''$, since if $m'' < s''$, then $m' < s'$, which cannot occur in cases 1 and 2, and, just as with $t'' = t'$ and $n'' - m'' - 1$, s'' must be greater than $n'' - t'' - 1$ in case 1 and $n'' - t'' - 2$ in case 2.

Now assume that the presentation of H falls into the third case. Then G has a parametrization in the same case. First, $f(x)$ clearly has order p^n, so $n'' = n$. Second, since $f(y)$ must have the same order as y, $m'' = m'$. We have in H the conjugation relation

$$yxy^{-1} = x^{-5^{2^{t'}}}.$$

Now the order of the automorphism $x \mapsto x^5$ is 2^{n-2}, where 2^n is the order of x; therefore, if $t' \geq n-2$, then we may take $t'' = n-2$. Otherwise, the same conjugation relation holds in G, so that $t'' = t'$. Combining both possibilities, $t'' = \min(t', n-2)$.

We also have that in H, $y^{2^{m'}} = x^{2^{s'}}$, so that if $s' \geq n$, we may take $s'' = n$, and if not, $s'' = s'$. Combining both possibilities, we have that $s'' = \min(s', n)$. As before, the value of t'' lies in the appropriate bounds for case 3; we need only check the bounds for s''. Note that the parametrization for case 3 states that either $s \in \{n-1, n\}$ or $s = n-1$, according to whether or not $m + t + 1 \geq n$. Moreover, if $m + t + 1 = n - 1$, then [Li, §2.1] shows that while $f(x)$ and $f(y)$ may be generators of a parametrization with $s'' = n''$, the parametrization with $\tilde{x} = f(x)$, $\tilde{y} = f(x)^{-m''-t''-1} f(y)$ allows us to set $s'' = n'' - 1$, as required. If $s'' = n$, then $s'' = n''$; otherwise, $s'' = s' < n$, but then we must have that $s'' = s' = n' - 1 = n'' - 1$.

For all three cases, then, we have that $(c'', n'', m'', t'', s'')$ is one of the set of presentations of section 6.1, from [Li, §2.1]. By Proposition 5.1 the presentations

of G are unique, given a fixed $\langle x \rangle$; we then have that $n = n''$, $m = m''$, $t = t''$, and $s = s''$. Hence the set of H which admit a surjection of the type described to G must have certain parameters fixed: in cases 1 and 2, $m' = m$ and $t' = t$, while in case 3, we have only that $m' = m$. The remaining parameters may then vary. In case 1, since $t' \in \{\max(0, n' - m' - 1), n' - 1\}$, we must have that $n' - m - 1 \leq t$ or $n' \leq t + m + 1$. If $s = n \leq m$, then $n \leq s' \leq \min(m, n')$, and the range of such s' is nonempty for any $n' \leq t + m + 1$. If $s \neq n$, we have that $n' - t' - 1 \leq s'$ or that $n' \leq s + t + 1$, so that $n' \leq \min(t + m + 1, s + t + 1)$. Case 2 is similar: since $t' \in \{\max(0, n' - m' - 2), n' - 2\}$, we must have that $n' - m - 2 \leq t$ or $n' \leq t + m + 2$. If $s = n \leq m$, then $n \leq s' \leq \min(m, n')$, and the range of such s' is nonempty for any $n' \leq t + m + 2$. If $s \neq n$, we have that $n' - t' - 2 \leq s'$ or that $n' \leq s + t + 2$, so that $n' \leq \min(t + m + 2, s + t + 2)$.

For case 3, we have more choices, as follows. We have that $t = \min(t', n - 2)$ and $s = \min(s', n)$. Now if $t < n - 2$, then $t' = t$ and then $n' - m' - 2 \leq t' = t$ and hence $n' \leq t + m + 2$. If $t = n - 2$, however, t' may vary anywhere in $\{\max(n - 2, n' - m - 2), \cdots, n' - 2\}$. If $s = n$ or $s = m + t + 1 = n - 1$, then s' may vary to take any value in $\{n' - 1, \min(n', m + t' + 1)\}$, otherwise no surjection exists with $n' > n$. □

References

[Bl] E. Black, *Deformation of dihedral 2-group extensions of fields*, Trans. Amer. Math. Soc. **351** (1999), 3229–3241. MR **99m:**12004

[CHR] S. Chase, D. Harrison, and A. Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc., vol. 52, American Mathematical Society, Providence, RI, 1965; reprinted with corrections, 1968. MR **33:**4118

[Cr] T. Crespo, *Galois representations, embedding problems and modular forms*, Journées Arithmétiques (Barcelona, 1995), Collect. Math. **48** (1997), 63–83. MR **98j:**11101

[DI] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Mathematics, vol. 181, Springer-Verlag, Berlin, 1971. MR **43:**6199

[GSS] H. Grundman, T. Smith, and J. Swallow, *Groups of order 16 as Galois groups*, Exposition. Math. **13** (1995), 289–319. MR **96h:**12005

[Ho] K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106. MR **39:**5507

[Ik] M. Ikeda, *Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren*, Abh. math. Sem. Hamburg **24** (1960), 126–131. MR **22:**12103

[ILF] I. Ishkhanov, B. Lur'e, and D. Faddeev, *The embedding problem in Galois theory*, Translations of Mathematical Monographs, vol. 165, American Mathematical Society, Providence, RI, 1997. MR **98c:**12007

[Le] A. Ledet, *Embedding problems with cyclic kernel of order 4*, Israel J. Math. **106** (1998), 109–132. MR **99k:**12009

[Li] S. Liedahl, *Presentations of metacyclic p-groups with applications to K-admissibility questions*, J. Algebra **169** (1994), 965–983. MR **96a:**20043

[Sc] L. Schneps, *On cyclic field extensions of degree 8*, Math. Scand. **71** (1992), 24–30. MR **94d:**12004

[Sw1] J. Swallow, *Embedding problems and the $C_{16} \to C_8$ obstruction*, Contemporary Mathematics 186: Recent Developments in the Inverse Galois Problem, American Mathematical Society, Providence, RI, 1995, pp. 75–90. MR **96j:**12010

[Sw2] J. Swallow, *Solutions to central embedding problems are constructible*, J. Algebra **184** (1996), 1041–1051. MR **97e:**12007

Department of Mathematics, University of Oklahoma, Norman, Oklahoma 73019
Current address: 131 Salina Street, Lafayette, Colorado 80026
E-mail address: eblack@math.ou.edu

Department of Mathematics, Davidson College, Davidson, North Carolina 28036
E-mail address: joswallow@davidson.edu