PARAMETERIZING SOLUTIONS TO ANY GALOIS EMBEDDING PROBLEM OVER $\mathbb{Z}/p^n\mathbb{Z}$ WITH ELEMENTARY $p$-ABELIAN KERNEL

ANDREW SCHULTZ

ABSTRACT. In this paper we use the Galois module structure for the classical parameterizing spaces for elementary $p$-abelian extensions of a field $K$ to give necessary and sufficient conditions for the solvability of any embedding problem which is an extension of $\mathbb{Z}/p^n\mathbb{Z}$ with elementary $p$-abelian kernel. This allows us to count the total number of solutions to a given embedding problem when the appropriate modules are finite, and leads to some nontrivial automatic realization and realization multiplicity results for Galois groups.

1. Introduction

One of the fundamental problems in Galois theory is to determine conditions on a field $F$ which are necessary and sufficient for the appearance of a group $G$ as a Galois group over $F$; i.e., to determine when there exists an extension $K/F$ with $\text{Gal}(K/F) \simeq G$. The relative version of this question is the so-called embedding problem. For a given surjection of groups

$$\hat{G} \xrightarrow{\varphi} G \longrightarrow 1$$

and a given isomorphism $\psi_K : \text{Gal}(K/F) \rightarrow G$, the embedding problem for $(\hat{G}, \varphi, \psi_K)$ over $K/F$ asks whether there is a field extension $L/F$ containing $K$ and an isomorphism $\psi_L : \text{Gal}(L/F) \rightarrow \hat{G}$ such that the natural surjection from Galois theory makes the following diagram commute:

$$\begin{array}{ccc}
\text{Gal}(L/F) & \longrightarrow & \text{Gal}(K/F) \\
\downarrow & & \downarrow \\
\hat{G} & \xrightarrow{\varphi} & G \\
\end{array} \quad \psi_L \quad \psi_K \quad 1$$

One can ask for a weaker solution to this embedding problem by only insisting that $\psi_L$ be a surjection; in this case, $L$ is said to be a weak solution to the embedding problem.

There are a number of results in the literature which explore embedding problems for $p$-groups, particularly embedding problems whose kernel is $\mathbb{Z}/p\mathbb{Z}$:

$$1 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \hat{G} \xrightarrow{\varphi} G \longrightarrow 1 \quad (1)$$

These trace back to Dedekind’s work on the embedding problem $Q_8 \longrightarrow \mathbb{Z}/2 \oplus \mathbb{Z}/2 \longrightarrow 1$ in [6]. The interested reader can also find a bounty of results concerning the realizability of small 2-groups as Galois groups (often by studying embedding problems) in articles such as [4, 5, 8, 9, 10, 11, 21, 23, 24], as well as a number of papers on the realizability of small $p$-groups as Galois groups (again, often via embedding problems) in [19, 20, 22, 30].
Away from characteristic $p$, the conventional method for approaching these problems is to assume $K$ contains the appropriate roots of unity and then consider the element $c \in H^2(G, \mathbb{Z}/p\mathbb{Z})$ that corresponds to this extension of groups, with $\mathbb{Z}/p\mathbb{Z}$ identified with the trivial $G$-module $\mu_p$ of $p$th roots of unity in $K$. The existence of an extension $L/F$ which solves the given embedding problem is then translated in terms of the image of this class $c$ within $\text{Br}(K)$ under the map $H^2(G, \mathbb{Z}/p\mathbb{Z}) \to H^2(G, K^\times)$ which is induced by $\mu_p \hookrightarrow K^\times$; often this involves determining a specific algebra that represents this element within $\text{Br}(K)$, and typically this is quite difficult. When one doesn’t have the necessary roots of unity, one approach is to solve the corresponding question in the extension of fields given by adjoining the necessary roots of unity, and then attempt to descend. In characteristic $p$, one hopes to use the power of Witt’s famous result from [33], concerning the realizability of $p$-group as Galois groups in characteristic $p$; for instance, in [15, App. A], Jensen, Ledet and Yau use a technique similar to Witt’s to show the embedding problem (1) is solvable in characteristic $p$ provided it is central (i.e., $\text{ker}(\varphi) \subseteq Z(\hat{G})$) and nonsplit.

In this paper, we will give a parameterization for the set of solutions to any embedding problem $\hat{G} \longrightarrow G \longrightarrow 1$ over an extension $K/F$ when $G \simeq \mathbb{Z}/p^n\mathbb{Z}$ and the kernel is an elementary $p$-abelian group $A$ with a prescribed $G$-action. Though it has the same spirit as many of the embedding problems in the literature, we will develop our results without explicitly delving into 2-cohomology. Our parametrization involves studying the $\text{Gal}(K/F)$-module structure of the parameterizing $\mathbb{F}_p$-space for elementary $p$-abelian extensions over $K$, which we denote $J(K)$; for instance, when $K$ contains a primitive $p$th root of unity, we will study the $\mathbb{F}_p[\text{Gal}(K/F)]$-structure of $J(K) = K^\times/K^{\times p}$. This study was initiated by Waterhouse in [31], and sections 3 and 4 from this paper can be thought of as a completion of the ideas that Waterhouse presents there.

The question of studying embedding problems with elementary $p$-abelian kernel was also recently considered by Mináč and Swallow in [26]. In this paper, the authors consider embedding problems where the corresponding factor group $\text{Gal}(K/F)$ is $\mathbb{Z}/p\mathbb{Z}$ and the kernel is a cyclic $\mathbb{F}_p[\text{Gal}(K/F)]$-module. Our paper generalizes these results by allowing $\text{Gal}(K/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$ for any $n \in \mathbb{N}$, and removes the condition of cyclicity (as a module) for the kernel. Shirbisheh also considers non-cyclic kernels in [29], where he studies embedding problems over the field $\mathbb{Q}(\xi_p^r)/\mathbb{Q}(\xi_p)$. Aside from the fact that we have no restriction on the fields we consider, our approach differs in that we give explicit descriptions for all possible extensions of $\mathbb{Z}/p^n\mathbb{Z}$ by a finite $\mathbb{F}_p[G]$-module $A$, and then we find a parameterizing set for each such group within $J(K)$. We are also more constructive in our approach to finding modules within $J(K)$ that solve a given embedding problem, giving a recipe for how one might build such a module first in terms of a fixed submodule and then through generators “over” this fixed subspace.

To accomplish our goal, we will first classify all solutions to the “group-theoretic embedding problem”

$$\hat{G} \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 1$$

(subject to a prescribed kernel $A$ with a prescribed $\mathbb{Z}/p^n\mathbb{Z}$-action). For example, one of these extensions will be the group $A \rtimes \mathbb{Z}/p^n\mathbb{Z}$. Once we have enumerated the possible group structures for $\hat{G}$, we then determine the necessary and sufficient conditions for finding solutions to the given field-theoretic embedding problems over $K/F$. Solutions to an
embedding problem will corresponds to a particular class of modules within \( J(K) \), and this allows us to count the number of solutions to a given embedding problem explicitly provided we know the module structure of \( J(K) \) (together with an additional field-theoretic invariant which we will discuss later).

To give the reader a sample of the results we are able to prove, we recall a definition from \[27\]. For a field extension \( K/F \) with \( \text{Gal}(K/F) \simeq \mathbb{Z}/p^n\mathbb{Z} \), let \( K_i \) denote the intermediate field of degree \( p^i \) over \( F \). If the embedding problem
\[
\mathbb{Z}/p^{n+1} \longrightarrow \mathbb{Z}/p^n \mathbb{Z} \longrightarrow 1
\]
for \( K/F \) has a solution, then define \( i(K/F) = -\infty \). Otherwise, let \( s \) be the minimum value such that the embedding problem
\[
\mathbb{Z}/p^{n-s+1} \longrightarrow \mathbb{Z}/p^{n-s} \mathbb{Z} \longrightarrow 1
\]
for \( K/K_s \) has a solution, and define \( i(K/F) = s - 1 \). Notice that we have \( i(K/F) \in \{ -\infty, 0, \ldots, n - 1 \} \) provided \( K \neq F \).

We also remind the reader that \((\binom{n}{m})_p\) is the \( p \)-binomial coefficient, which we define in section \[3\].

**Theorem 1.1.** Let \( G = \langle \sigma \rangle \simeq \mathbb{Z}/p^n\mathbb{Z} \), where \( p \) is a prime and \( n > 1 \) when \( p = 2 \), and suppose that \( K/F \) is an extension of fields so that \( \text{Gal}(K/F) \simeq G \) and \( \xi_p \in K \). Suppose that \( A \simeq \bigoplus_{i=1}^{p^n} \bigoplus_{d \in \mathbb{F}_p[G]} \mathbb{F}_p[G]/(\sigma - 1)^i \) as an \( \mathbb{F}_p[G] \)-module, and write \( \Delta(A_{(i)}) = \sum_{j \geq 1} d_j \). For \( 1 \leq i \leq p^n \) let
\[
\mathcal{O}_{(i)} = \text{dim}_{\mathbb{F}_p} \left( \frac{N_{K \cap \log_p(i)}/F(K^{\log_p(i)})}{K^{\times p}} \right).
\]
Then the embedding problem \( A \times G \longrightarrow G \longrightarrow 1 \) has a solution over \( K/F \) if and only if \( \Delta(A_{(i)}) \leq \mathcal{O}_{(i)} \).

If \( F^{\times}/K^{\times p} \) is infinite and the embedding problem \( A \times G \longrightarrow G \longrightarrow 1 \) is solvable, then there are infinitely many solutions to this embedding problem over \( K/F \). If \( F^{\times}/K^{\times p} \) is finite and the embedding problem \( A \times G \longrightarrow G \longrightarrow 1 \) is solvable, then the number of solutions to this embedding problem over \( K/F \) is
\[
\prod_{i=1}^{p^n} \left( \mathcal{O}_{(i)} - \Delta(A_{(i+1)}) - 1_{i=p(K/F)+1} \right) p^{d_i \left( \sum_{j<i} \mathcal{O}_{(j)} - \Delta(A_{(j)}) - 1_{j=p(K/F)+1} \right)}.
\]

Though this result is expressed only for fields containing a primitive \( p \)th root of unity, we’ll see later that this result holds for any extension of fields \( K/F \) with \( \text{Gal}(K/F) \simeq \mathbb{Z}/p^n\mathbb{Z} \) (after an appropriate translation of the constants \( \mathcal{O}_{(i)} \) and the space \( F^{\times}/K^{\times p} \)).

Our parameterization also allows us to make a number of statements about how the appearance of one group as a Galois group over \( F \) influences the existence of other groups as Galois groups over \( F \). To preview some results of this flavor, we introduce the following definition. For a given group \( G \) and field \( F \), we say that an extension \( K/F \) is a \( G \)-extension of \( F \) if \( \text{Gal}(K/F) \simeq G \); we will write \( \mathfrak{F}(G) \) for the set of all fields \( F \) which admit a \( G \)-extension. If \( F \in \mathfrak{F}(G) \) implies \( F \in \mathfrak{F}(Q) \), then we say that \( G \) automatically realizes \( Q \);
the automatic realization result is said to be trivial when \( Q \) is a quotient of \( G \). A classic example was given by Whaples showed in [32], where he showed that \( \mathbb{Z}/p\mathbb{Z} \) automatically realizes \( \mathbb{Z}/p^n\mathbb{Z} \) when \( p \) is an odd prime and \( n \geq 2 \), as well as showing \( \mathbb{Z}/4\mathbb{Z} \) automatically realizes \( \mathbb{Z}/2^n\mathbb{Z} \) for all \( n \geq 3 \). Jensen has written a number of excellent articles on automatic realizations, including [12, 13, 14], and there are other automatic realizations considered in [3, 8, 18, 20, 32].

**Theorem 1.2.** Suppose that \( \text{Gal}(K/F) = \langle \sigma \rangle \cong \mathbb{Z}/p^n\mathbb{Z} \) and that \( K \) contains a primitive \( p \)-th root of unity. Suppose that \( A \cong \bigoplus_{i=1}^{p^n} \oplus_{d_i} \mathbb{F}_p[G]/(\sigma - 1)^i \) as an \( \mathbb{F}_p[G] \)-module. Define

\[
[A] = \bigoplus_{i=1}^{p^n} \oplus_{d_i} \mathbb{F}_p[G]/(\sigma - 1)^{p^{\lceil \log_p(i) \rceil}}.
\]

If \( F \in \mathfrak{F}(A \rtimes G) \), then \( f \in \mathfrak{F}([A] \rtimes G) \).

This result is the natural generalization of the main result from [28]; more general automatic realization results for non-split groups will also be discussed in Theorem 6.5.

To take advantage of the fact that we have precise counts on the number of solutions to a given embedding problem, we also state some results concerning realization multiplicity. Let \( \nu(G, F) \) denote the number of distinct \( G \)-extensions of \( F \) within a fixed algebraic closure of \( F \), and

\[
\nu(G) = \min_{F \in \mathfrak{F}(G)} \nu(G, F).
\]

This latter quantity is called the realization multiplicity of \( G \). Jensen has explored realization multiplicities in [16, 17]. We have a generalization of the main result from [1].

**Theorem 1.3.** Let \( G = \langle \sigma \rangle \cong \mathbb{Z}/p^n\mathbb{Z} \), with \( n > 1 \) when \( p = 2 \). Suppose that \( A \) is an \( \mathbb{F}_p[G] \)-module which is not isomorphic to

\[
\mathbb{F}_p[G]/(\sigma - 1)^{p^j+1} \bigoplus_{i=0}^{p^n} \oplus_{d_i} \mathbb{F}_p[G]/(\sigma - 1)^{p^i}
\]

for any choice of \( j \in \{-\infty, 0, \cdots, n-1\} \) and \( d_i \in \mathbb{Z} \). If \( \hat{G} \) is any extension of \( G \) by \( A \), and if \( A \) contains elements \( a_1, \cdots, a_k \) which are \( \mathbb{F}_p[G] \)-independent, then \( \nu(\hat{G}) \geq p^k \).

This paper proceeds as follows. In the next section we remind the reader of some results about \( \mathbb{F}_p[G] \)-modules, and we classify all extensions of \( G \) by \( \mathbb{F}_p[G] \)-modules in section 3. In section 4, we consider the parameterizing space of elementary \( p \)-abelian extensions over \( K \) — denoted \( J(K) \) — and some of the known bijections between cyclic submodules of \( J(K) \) and extensions of \( G \); we extend these results to include the case of characteristic \( p \), and we then describe the collection of submodules in \( J(K) \) that correspond to fields that solve any given embedding problem \( \hat{G} \longrightarrow G \longrightarrow 1 \) for \( K/F \). This allows us to give a precise count for the number of such solutions, which we do in section 5. In section 6, we recall some of the known results about the module structure of \( J(K) \) when \( \text{char}(F) \neq p \), and we extend these results to include \( \text{char}(F) = p \) as well. We then use these to make statements about realization multiplicities and automatic realizations.
2. Notation and $\mathbb{F}_p[G]$-decompositions

Throughout the paper $p$ will denote a prime number, and we will use $K/F$ to denote an extension such that $\text{Gal}(K/F) = \langle \sigma \rangle \simeq \mathbb{Z}/p^n\mathbb{Z} := G$ with $n \in \mathbb{N}$. We use $1_S$ as the indicator function for a subset $S$ of the natural numbers; often we describe $S$ explicitly in terms of equalities or inequalities.

Our results will concern embedding problems $\hat{G} \xrightarrow{\varphi} G \xrightarrow{\psi} 1$ over $K/F$, where $\hat{G}$ is an extension of $G$ by a given $\mathbb{F}_p[G]$-module $A$. We will suppress the explicit isomorphism $\psi_K : \langle \sigma \rangle \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ when considering these embedding problems. To emphasize the Galois-theoretic motivation of our work, we will call the extensions of $G$ by $A$ “group-theoretic embedding problems.” We say that two group-theoretic embedding problems $(\hat{G}_1, \varphi_1)$ and $(\hat{G}_2, \varphi_2)$ are isomorphic if there exists an isomorphism of groups $\psi : \hat{G}_1 \rightarrow \hat{G}_2$ that makes the following diagram commute:

$$
\begin{array}{ccc}
\hat{G}_1 & \xrightarrow{\varphi_1} & G \\
\downarrow \psi & & \downarrow \\
\hat{G}_2 & \xrightarrow{\varphi_2} & G \\
\end{array}
$$

If we wish to assemble all embedding problems over $G$ into a reasonable category, the morphisms of interest will be surjections: we’ll be searching for solutions that come from Galois theory, and the only interesting morphisms of fields are injections.

When we work with an $\mathbb{F}_p[G]$-module, we will assume that the underlying vector space structure is written multiplicatively, and hence the $G$-action will be written exponentially, unless we say otherwise.

We now collect certain key facts about $\mathbb{F}_p[G]$-modules. A more detailed exposition can be found in [27]. Ideals in $\mathbb{F}_p[G]$ are simply $\{(\sigma - 1)^\ell : 1 \leq \ell \leq p^n - 1\}$, and hence any cyclic submodule with $\mathbb{F}_p$-dimension $\ell$ is isomorphic to $\mathbb{F}_p[G]/(\sigma - 1)^\ell$.

One can show that these are the only indecomposable $\mathbb{F}_p[G]$-modules, and moreover that any $\mathbb{F}_p[G]$-submodule $A$ can be decomposed as

$$
A \simeq \bigoplus_{i=1}^{p^n} \oplus d_i \mathbb{F}_p[G]/(\sigma - 1)^i.
$$

This decomposition is unique up to permutation of the summands. For a given element $\alpha \in A$, we will call $\text{dim}_{\mathbb{F}_p}(\alpha)$ the length of $\alpha$, which we write as $\ell(\alpha)$.

It will occasionally be helpful to know the number of various generators of an $\mathbb{F}_p[G]$-module $A$. Following the notation from the decomposition (2), we write

$$
\text{rk}(A) = \sum_{i=1}^{p^n} d_i, \quad \text{f-rk}(A) = d_{p^n} \quad \text{and} \quad \text{nf-rk}(A) = \sum_{i=1}^{p^n-1} d_i.
$$

We will call these quantities the rank, free rank and non-free rank, respectively.
The following proposition gives us a way to build an $\mathbb{F}_p[G]$-module from its fixed submodule.

**Proposition 2.1.** Suppose that $V$ is an $\mathbb{F}_p[G]$-module and consider the filtration of $\mathbb{F}_p[G]$-subspaces $V^G = V_1 \supseteq V_2 \supseteq \cdots \supseteq V_{[p^n]} \supseteq V_{[p^n+1]} = \{1\}$, where

$$V_{(i)} = \operatorname{im} \left( V \xrightarrow{\sigma^{-1}i^{-1}} V \right) \cap V^G.$$ 

Let $\mathcal{I}_i$ be chosen so that $\bigcup_{i \geq j} \mathcal{I}_i$ is a basis for $V_{(i)}$, and for each $x \in \mathcal{I}_i$ let $v_x \in V$ be given so that $v_x^{(\sigma^{-1}i^{-1})} = x$. Then $V = \bigoplus_{i=1}^{[p^n]} \bigoplus_{x \in \mathcal{I}_i} \langle v_x \rangle$.

**Proof.** Each of the submodules are independent by [27, Lm. 2], and so the stated sum is direct. The containment "$\supseteq$" is obvious. For the opposite containment, we prove that each $\alpha \in V$ is contained in $\tilde{V} := \bigoplus_{i=1}^{[p^n]} \bigoplus_{x \in \mathcal{I}_i} \langle v_x \rangle$ by induction on the length of $\alpha$. If $\ell(\alpha) = 1$ then $\alpha \in \tilde{V}$ since $V_{(1)} = V^G$. Now suppose $\tilde{V}$ contains all elements of length at most $\ell - 1$, and suppose $\ell(\alpha) = \ell$. Then $\alpha^{(\sigma^{-1})^{\ell-1}} \in \tilde{V}_{(\ell)}$, and hence there exists constants $c_x \in \mathbb{F}_p$ such that

$$\alpha^{(\sigma^{-1})^{\ell-1}} = \prod_{i \geq \ell} \prod_{x \in \mathcal{I}_i} x^{c_x} = \prod_{i \geq \ell} v_x^{c_{x}(\sigma^{-1})^{i-1}} = \prod_{i \geq \ell} \left( v_x^{c_{x}(\sigma^{-1})^{i-1}} \right)^{(\sigma^{-1})^{\ell-1}}.$$ 

Hence the element $\prod v_x^{c_{x}(\sigma^{-1})^{i-1}} / \alpha$ has length less than $\ell$, and is therefore contained in $\tilde{V}$. Since each of the $v_x \in \tilde{V}$ as well, this forces $\alpha \in \tilde{V}$, as desired. \hfill $\square$

3. Classifying groups

We are interested in classifying extensions $\hat{G} \longrightarrow G \longrightarrow 1$ for which the kernel is elementary $p$-abelian. In order to be slightly more precise, start with the data of the group $G$ and a $G$-module $A$ which is elementary $p$-abelian as a group. We say that $\hat{G} \longrightarrow G \longrightarrow 1$ is an embedding problem with kernel $A$ if in the short exact sequence

$$1 \longrightarrow A \xrightarrow{k} \hat{G} \xrightarrow{\varphi} G \longrightarrow 1$$ 

satisfies the condition that the action of $G$ on $A$ by conjugation is compatible with the $G$-action on $A$: for every $\tau \in G$ and $a \in A$, and for any $\hat{\tau} \in \hat{G}$ satisfying $\varphi(\hat{\tau}) = \tau$, we have

$$\hat{\tau}^{-1} k(a) \hat{\tau} = k(a^\tau).$$ 

Throughout the balance of the paper, we will be interested in studying the extensions of $G \simeq \mathbb{Z}/p^n\mathbb{Z}$ by a given $\mathbb{F}_p[G]$-module $A$.

Such an extension $\hat{G}$ is generated by $\mathbb{F}_p[G]$-generators $\{\alpha_i\}_{i=1}^{\operatorname{rk}(A)}$ for $A$ together with a lift $\hat{\sigma} \in \hat{G}$ of $\sigma \in G$. Clearly the relations satisfied by $A$ appear in the relations for such an extension of groups; hence if $A = \bigoplus_{i=1}^{\operatorname{rk}(A)} \langle \alpha_i \rangle$ then we have

1. $\alpha_i \alpha_j = \alpha_j \alpha_i$ for $1 \leq i, j \leq \operatorname{rk}(A)$;
2. $\hat{\sigma} \alpha_i \hat{\sigma}^{-1} = \alpha_i^\sigma$ for $1 \leq i \leq \operatorname{rk}(A)$; and
3. $\alpha_i^{(\sigma^{-1})^{\ell(\alpha_i)}} = 1$ for $1 \leq i \leq \operatorname{rk}(A)$. 


The last data that determines the structure of such an extension is the value of $\hat{\sigma}^{p^n}$. This element must lie in $A$ since it has trivial image in $G$, and it must be fixed by the action of $\sigma$ as well. Since the fixed submodule of $A$ is generated by $\{\alpha_{\ell(i)}^{(\sigma-1)\hat{i}(\alpha_i)^-1}\}$, this means that for some $c^i \in \mathbb{F}_p$, we have

$$(4) \quad \hat{\sigma}^{p^n} = \prod_{i=1}^{\text{rk}(A)} \alpha_i^{c_i(\sigma-1)\hat{i}(\alpha)}.$$ 

**Definition 3.1.** Let $A = \oplus_{i=1}^{\text{rk}(A)} \langle \alpha_i \rangle$, and let $\vec{c} \in \mathbb{F}_p^{\text{rk}(A)}$ be given. We define $\mathfrak{G}(A, \vec{c})$ to be the group generated by $\{\alpha_{\ell(i)}^{\text{rk}(A)} \cup \{\hat{\sigma}\}\}$ and subject to the relations

1. $\alpha_i \alpha_j = \alpha_j \alpha_i,$
2. $\hat{\sigma} \alpha_i \hat{\sigma}^{-1} = \alpha_i^\sigma,$
3. $\alpha_i^{(\sigma-1)^{\hat{i}(\alpha)}} = 1,$ and
4. $\hat{\sigma}^{p^n} = \prod_{i=1}^{\text{rk}(A)} \alpha_i^{c_i(\sigma-1)^{\hat{i}(\alpha)}}.$

The group-theoretic embedding problem for $\mathfrak{G}(A, \vec{c})$ over $G$ is then

$$\mathfrak{G}(A, \vec{c}) \xrightarrow{\varphi} G \rightarrow 1,$$

where $\varphi$ is defined by $\varphi(\alpha_i) = 1$ and $\varphi(\hat{\sigma}) = \sigma$; we will often abuse notation and speak of the embedding problem $\mathfrak{G}(A, \vec{c})$ without referring to either $G$ or $\varphi$.

The previous discussion provides the justification for the following

**Proposition 3.2.** If $\hat{G} \rightarrow G \rightarrow 1$ is a group-theoretic embedding problem with kernel given by the $\mathbb{F}_p[G]$-module $A$, where $A = \oplus_{i=1}^{\text{rk}(A)} \langle \alpha_i \rangle$, then there exists some $\vec{c} \in \mathbb{F}_p^{\text{rk}(A)}$ such that $\hat{G} \rightarrow G \rightarrow 1$ is isomorphic to the embedding problem $\mathfrak{G}(A, \vec{c})$.

It is worth noting that the relations on $\mathfrak{G}(A, \vec{0})$ are clearly the same as those for $A \rtimes G$, and hence these two groups (and group-theoretic embedding problems) are identical.

As a first step towards determining when embedding problems of this form are isomorphic, we have the following

**Lemma 3.3.** Suppose that $A = \oplus_{i=1}^{\text{rk}(A)} \langle \alpha_i \rangle$, and let $\vec{c} \in \mathbb{F}_p^{\text{rk}(A)}$ be given. If $\vec{d}$ is the vector such that

$$d_i = \begin{cases} 0, & \text{if } \ell(\alpha_i) = p^n \\ c_i, & \text{otherwise}, \end{cases}$$

then $\mathfrak{G}(A, \vec{c})$ and $\mathfrak{G}(A, \vec{d})$ are isomorphic as group-theoretic embedding problems.

**Proof.** Consider the lift of $\sigma$ given by $\hat{\sigma} = \left( \prod_{\ell(i)=p^n} \alpha_i^{-c_i} \right) \hat{\sigma}$. Applying relations (1)-(3) inductively, one can show that

$$\hat{\sigma}^{p^n} = \left( \prod_{\ell(i)=p^n} \alpha_i^{-c_i} \hat{\sigma} \right)^{p^n} = \prod_{\ell(i)=p^n} \alpha_i^{-c_i(1+\sigma+\ldots+\sigma^{-1})} \hat{\sigma}^{p^n}$$
Since \( \sum_{i=1}^{p^n} \sigma^i = (\sigma - 1)^{p^n-1} \mod p \), we therefore have
\[
\tilde{\sigma}^{p^n} = \prod_{\ell(i) = p^n} \alpha_i^{c_i(\sigma - 1)^{p^n-1}} \prod_{i=1}^{\text{rk}(A)} \alpha_i^{c_i(\sigma - 1)^{\ell(i) - 1}} = \prod_{\ell(\alpha_i) \neq p^n} \alpha_i^{c_i(\sigma - 1)^{\ell(\alpha_i) - 1}}.
\]
Because \( \mathfrak{G}(A, \tilde{e}) \) can be generated by \( \tilde{\sigma}, \alpha_1, \ldots, \alpha_s \) so that the relations for \( \mathfrak{G}(A, \tilde{e}) \) are satisfied, it must be that these two groups are isomorphic. Since the projections of these groups onto \( G \) are compatible, these two group-theoretic embedding problems are isomorphic. \( \square \)

**Lemma 3.4.** Suppose that \( A = \bigoplus_{i=1}^{\text{rk}(A)} \langle \alpha_i \rangle \), and let \( \tilde{e} \in F_p^{\text{rk}(A)} \) be given. Suppose that one can choose \( 1 \leq i \leq \text{rk}(A) \) so that \( \ell(\alpha_i) \) is minimal subject to the condition that \( c_i \neq 0 \) and \( \ell(\alpha_i) < p^n \). Let \( e_{i}^j \) be the \( i \)th standard basis vector. Then \( \mathfrak{G}(A, \tilde{e}) \simeq \mathfrak{G}(A, e_i^j) \) as group-theoretic embedding problems over \( G \). On the other hand, if no such \( i \) exists, then \( \mathfrak{G}(A, \tilde{e}) \simeq \mathfrak{G}(A, \tilde{0}) \) as group-theoretic embedding problems over \( G \).

**Proof.** We have already seen that we can assume \( \tilde{e} \) to have 0 coordinate in those positions \( j \) corresponding to \( \ell(\alpha_j) = p^n \). If no such \( i \) exists as in the statement of the theorem, then we appeal to the previous lemma to conclude that \( \mathfrak{G}(A, \tilde{e}) \simeq \mathfrak{G}(A, \tilde{0}) \) as group-theoretic embedding problems.

Now suppose that \( i \) is chosen as in the statement of the theorem, and that \( c_j = 0 \) when \( \ell(\alpha_j) = p^n \). Define \( \beta_j = \alpha_j \) for every \( j \neq i \), and let
\[
\beta_i = \alpha_i^{c_i} \prod_{c_j \neq 0} \alpha_j^{c_j(\sigma - 1)^{\ell(\alpha_j) - \ell(\alpha_i)}}.
\]
Then one can easily check that \( \{\beta_i\}_{i=1}^{\text{rk}(A)} \) generates the same \( F_p[G] \)-module as \( \{\alpha_i\}_{i=1}^{\text{rk}(A)} \), that \( \ell(\beta_i) = \ell(\alpha_i) \), and that
\[
\beta_i^{(\sigma - 1)^{\ell(i) - 1}} = \left( \prod_{c_j \neq 0} \alpha_j^{c_j(\sigma - 1)^{\ell(i) - \ell(\alpha_i)}} \right)^{(\sigma - 1)^{\ell(i) - 1}} = \tilde{\sigma}^{p^n}.
\]
Hence \( \mathfrak{G}(A, \tilde{e}) \) satisfies the relations defining \( \mathfrak{G}(A, e_i^j) \). Since the projections of these two groups onto \( G \) are compatible, they are isomorphic as group-theoretic embedding problems. \( \square \)

In light of the previous theorem, we see that the defining characteristics for an extension of \( G \) by an \( F_p[G] \)-module \( A \) are the isomorphism type of the \( F_p[G] \)-module \( A \), together with the smallest length for a generator of \( A \) which appears in relation (4) from Definition 3.1. Hence we introduce a new (and simpler) notation to keep track of the extensions of \( G \) by \( A \).

**Definition 3.5.** Suppose that \( A = \bigoplus_{i=1}^{\text{rk}(A)} \langle \alpha_i \rangle \), and let \( 1 \leq \lambda < p^n \) be given so that there exists some \( 1 \leq i \leq \text{rk}(A) \) with \( \ell(\alpha_i) = \lambda \). Then we define \( A \cdot_{\lambda} G \) to be the group \( \mathfrak{G}(A, e_i^\lambda) \).

The group $\mathcal{G}(A, \overrightarrow{0})$ will most often be expressed as $A \rtimes G$, though when we wish to fit this group within the context of the other embedding problems with kernel $A$ we will refer to it as $A \bullet_p G$ — even when $A$ contains no summand of length $p^n$.

**Remark.** Our definition for $A \bullet_{\lambda} G$ isn’t well-defined since the definition of $\mathcal{G}(A, \overrightarrow{c})$ requires us to name generators for $A$. This amounts to choosing an isomorphism $A \simeq \bigoplus_{i=1}^{\text{rk}(A)} \mathbb{F}_p[G]/(\sigma - 1)^{\ell_i}$, so when it becomes important we will name generators for $A$ explicitly.

**Theorem 3.6.** For an $\mathbb{F}_p[G]$-module $A$, there are $\text{nf-rk}(A) + 1$ many isomorphism types for embedding problems over $G$ with kernel $A$: one is $A \times G$, and the others correspond to $A \bullet_{\lambda} G$ where $1 \leq \lambda < p^n$ ranges over the dimensions of non-free summands in an $\mathbb{F}_p[G]$-decomposition of $A$.

**Remark.** This theorem was shown in the case that $A = \langle \alpha \rangle$ is a cyclic submodule by Waterhouse in [31]. In the case where the cyclic submodule isn’t isomorphic to $\mathbb{F}_p[G]$, the two possibilities are given by the semi-direct product and another group. In our language, if write $\lambda = \ell(\alpha)$, then this other group is simply $\langle \alpha \rangle \bullet_{\lambda} G$.

**Proof.** As usual, write $A = \bigoplus_{i=1}^{\text{rk}(A)} \langle \alpha_i \rangle$. We have already shown that any such group-theoretic embedding problem is isomorphic to $\mathcal{G}(A, \overrightarrow{c})$ for some $\overrightarrow{c} \in \mathbb{F}_p^{\text{rk}(A)}$, and that this group is isomorphic to either $A \times G = A \bullet_{p^n} G$ or $A \bullet_{\lambda} G$ for some $1 \leq \lambda < p^n$ such that there exists $1 \leq i \leq \text{rk}(A)$ with $\lambda = \ell(\alpha_i)$. Now we must show that if $\lambda_1 \neq \lambda_2$, then $A \bullet_{\lambda_1} G$ and $A \bullet_{\lambda_2} G$ are not isomorphic as group-theoretic embedding problems.

First, consider the case $\lambda_1 = p^n$ and $\lambda_2 < p^n$; our strategy will be to count the number of elements of order greater than $p^n$ in both groups. If we take an arbitrary element’s $p^n$th power in either group, we find

$$
\left( \prod_i \alpha_i^{f_i(\sigma)} \hat{\sigma}^j \right)^{p^n} = \prod_i \alpha_i^{(1+\sigma+\ldots+(\sigma^{p^n-1})f_i(\sigma)} (\hat{\sigma}^j)^{p^n} = \prod_i \alpha_i^{(\sigma^j-1)p^n-1f_i(\sigma)} (\hat{\sigma}^j)^{p^n}.
$$

(3)

In either group, if $j = p^kh$ for some $k > 0$, then this element is trivial: certainly $(\hat{\sigma}^j)^{p^n}$ is trivial since $\hat{\sigma}$ has order at most $p^{n+1}$, and we also have

$$
\sum_{s=1}^{p^n-1} (\sigma^j)^s \equiv (\sigma^j - 1)^{p^n-1} \equiv (\sigma^h - 1)^{p^n+k-p^k} \equiv ((\sigma - 1)^{p^n} \subseteq \mathbb{F}_p[G].
$$

Now when $(j, p) = 1$, equation (3) becomes

$$
\left( \prod_i \alpha_i^{f_i(\sigma)} \hat{\sigma} \right)^{p^n} = \left( \prod_i \alpha_i^{(\sigma-1)p^n-1f_i(\sigma)} \right)^c (\hat{\sigma}^{p^n})^j = \left( \prod_i \alpha_i^{(\sigma-1)p^n-1f_i(\sigma)} \right)^c (\hat{\sigma}^{p^n})^j
$$

where $c$ is the multiplicative inverse of $j$ in $\mathbb{F}_p^\times$. In the group $A \bullet_{p^n} G$ the term $(\hat{\sigma}^{p^n})^j$ vanishes, and so the term is nonzero only when at least one $f_i(\sigma) \not\in ((\sigma - 1)) \subseteq \mathbb{F}_p[G]$. In $A \bullet_{\lambda_2} G$, however, the term $(\hat{\sigma}^{p^n})^j$ is nonzero and independent from the terms in the product, and hence this element is nonzero for all $f_i(\sigma) \in ((\sigma - 1)) \subseteq \mathbb{F}_p[G]$. Hence $A \bullet_{\lambda_2} G$ has more elements of order $p^n$ than $A \bullet_{p^n} G$, so these two groups are not isomorphic.
With this case resolved, suppose without loss that \( \lambda_1 < \lambda_2 < p^n \). The defining relation for \( A \bullet_{\lambda_1} G \) is that we can find a lift \( \tilde{\sigma} \) and a generator \( \alpha_i \in A \) with \( \ell(\alpha_i) = \lambda_1 \) so that

\[
\tilde{\sigma}^{p^n} = \alpha_i^{(\sigma-1)^{\ell(\lambda_1)}-1}.
\]

Note that this same equation holds true if we quotient by the normal subgroup

\[ \langle \alpha_j \rangle_{j \neq i}, \]

and hence we have a surjection of group-theoretic embedding problems:

\[
A \bullet_{\lambda_1} G \twoheadrightarrow G \twoheadrightarrow 1
\]

\[
\mathbb{F}_p[G]/(\sigma - 1)^{\lambda_1} \bullet_{\lambda_1} G \twoheadrightarrow G \twoheadrightarrow 1.
\]

On the other hand, consider the group \( A \bullet_{\lambda_2} G \); the defining relation for this group tells us we can choose a lift \( \tilde{\sigma} \) for \( \sigma \) and a generator \( \alpha_j \) of \( A \) with \( \ell(\alpha_j) = \lambda_2 \) and so that

\[
\tilde{\sigma}^{p^n} = \alpha_j^{(\sigma-1)^{\lambda_2}-1}.
\]

Now suppose we have a surjection of group-theoretic embedding problems of the form

\[
A \bullet_{\lambda_2} G \twoheadrightarrow G \twoheadrightarrow 1
\]

\[
\mathbb{F}_p[G]/(\sigma - 1)^{\lambda_1} \bullet_{\mu} G \twoheadrightarrow G \twoheadrightarrow 1,
\]

where \( \mu \in \{\lambda_1, p^n\} \). (I.e., any group-theoretic embedding problem over \( G \) whose kernel is the module \( \mathbb{F}_p[G]/(\sigma - 1)^{\lambda_1} \).) The five lemma tells us that these arise from quotients of \( A \) isomorphic to \( \mathbb{F}_p[G]/(\sigma - 1)^{\lambda_1} \), which in turn correspond to submodules \( S \) of \( A \) so that \( A/S \cong \mathbb{F}_p[G]/(\sigma - 1)^{\lambda_1} \). Notice that for any such \( S \) we have \( \alpha_j^{(\sigma-1)^{\lambda_2}-1} \in S \), since otherwise \( A/S \) would contain a cyclic submodule generated by \( \alpha_j \) that has length at least \( \lambda_2 > \lambda_1 \).

Now notice that \( \psi(\tilde{\sigma}) \) is a lift of \( \sigma \) in \( \mathbb{F}_p[G]/(\sigma - 1)^{\lambda_1} \bullet_{\mu} G \). Because

\[
\tilde{\sigma}^{p^n} = \alpha_j^{(\sigma-1)^{\ell(\alpha_j)}-1}
\]

within \( A \bullet_{\lambda_2} G \), we therefore have \( \psi(\tilde{\sigma})^{p^n} - 1 \in A/S \). Hence it follows that \( \mu = p^n \). Since \( \mathbb{F}_p[G]/(\sigma - 1)^{\lambda_1} \bullet_{\lambda_1} G \not\cong \mathbb{F}_p[G]/(\sigma - 1)^{\lambda_1} \bullet_{p^n} G \), the result follows.

**Proposition 3.7.** If \( A \not\cong M \) as \( \mathbb{F}_p[G] \)-modules, then any group-theoretic embedding problem \( \hat{G}_M \twoheadrightarrow G \twoheadrightarrow 1 \) with kernel \( M \) is not isomorphic to any group-theoretic embedding problem \( \hat{G}_A \twoheadrightarrow G \twoheadrightarrow 1 \) with kernel \( A \).

**Proof.** Let \( j \) be the largest number such that \( |M_{(j)}| \neq |A_{(j)}| \), and assume that \( |A_{(j)}| \) is larger. Then \( A \twoheadrightarrow (\mathbb{F}_p[G]/(\sigma - 1)^j)^{D_j} \) where \( D_j = \text{dim}_{\mathbb{F}_p}(A_{(j)}) \), but \( M \) has no such
surjection. Hence we have a surjection of embedding problems

\[ \hat{G}_A \rightarrow G \rightarrow 1 \]

\[ (\mathbb{F}_p[G]_{(\sigma-1)^r})^D \cdot G \rightarrow G \rightarrow 1 \]

but no such surjection for \( \hat{G}_M \). □

4. Elementary \( p \)-abelian extensions of fields

If we are interested in computing \( \text{Gal}(L/F) \) when \( L/K \) is an elementary \( p \)-abelian extension which is additionally Galois over \( F \), then the preceding section tells us that we need to understand the module structure of \( \text{Gal}(L/K) \) together with a value for \( \hat{\sigma}^p^n \), where \( \hat{\sigma} \in \text{Gal}(L/F) \) is a lift of \( \sigma \in \text{Gal}(K/F) \). In this section we will consider how to determine these properties in terms of the classic parameterizing spaces for elementary \( p \)-abelian extensions.

4.1. Classifying elementary \( p \)-abelian extensions. Parametrizing spaces for elementary \( p \)-abelian extensions of fields have been known for quite some time. When \( \text{char}(K) \neq p \), let \( \hat{K} = K(\xi_p) \) and \( \hat{F} = F(\xi_p) \). Note that \( ([\hat{K} : \hat{F}], p) = 1 \), and hence \( \text{Gal}(\hat{K}/\hat{F}) \simeq G \). The Galois group of \( \hat{F}/F \) is cyclic, and for a generator \( \epsilon \) we write \( \epsilon(\xi_p) = \xi_p^t \). Relative Kummer theory tells us that the \( \oplus k\mathbb{Z}/p\mathbb{Z} \)-extensions of \( \hat{K} \) correspond to \( k \)-dimensional \( \mathbb{F}_p \)-subspaces of \( \hat{K}^\times/\hat{K}^{\times p} \) which are in the \( t \)-eigenspace of \( \epsilon \); we can then recover \( \oplus k\mathbb{Z}/p\mathbb{Z} \)-extensions of \( K \) via descent. The correspondence between a module \( M \) and an extension \( L/K \) is given explicitly by

\[ M \mapsto \text{the maximal } p\text{-extension of } K \text{ in } \hat{K} \left( \sqrt[t]{m} : m \in M \right) \]

\[ L \mapsto \frac{L(\xi_p)^{\times p} \cap \hat{K}^\times}{K^{\times p}} \bigg|_{\epsilon = t} \]

In the case where \( \text{char}(K) = p \), the parametrizing space is given to us by Artin-Schreier theory, which says that elementary \( p \)-abelian extensions of \( K \) are given by \( \mathbb{F}_p \)-subspaces of \( K/\varphi(K) \), where \( \varphi(K) = \{ k^p - k : k \in K \} \). For \( k \in K \) we write \( \rho(k) \) to denote a root of the equation \( x^p - x - k \). Using this notation, the correspondence is given by

\[ M \mapsto K(\rho(m) : m \in M) \]

\[ L \mapsto \frac{\varphi(L) \cap K}{\varphi(K)} \]

Regardless of the field \( F \) under consideration, we will write \( J(K) \) for the corresponding parametrizing space of elementary \( p \)-abelian extensions. When we consider \( J(K) \) as an \( \mathbb{F}_p[G] \)-module and don’t specify the characteristic of \( K \), we will write the group operation on \( J(K) \) multiplicatively and the \( \mathbb{F}_p[G] \)-action exponentially.
By putting additional structure on $J(K)$, one can make $J(K)$ a classifying space for a broader range of groups. In particular, we will focus on the $\mathbb{F}_p[G]$-structure of $J(K)$ and ask what it tells us about the Galois-ness of the extension $L/F$. The primordial result in this vein is that an elementary $p$-abelian extension $L/K$ is Galois over $F$ if and only if the corresponding subspace of $J(K)$ is an $\mathbb{F}_p[G]$-module; this was mentioned in [31] when $\text{char}(K) \neq p$, and the proof is straightforward in the $\text{char}(K) = p$ case as well.

For an $\mathbb{F}_p[G]$-module $A = \oplus_{i=1}^{\text{rk}(A)} \langle \alpha_i \rangle$ and a number $\lambda$ such that there exists $1 \leq i \leq \text{rk}(A)$ with $\lambda = \ell(\alpha_i)$, our ultimate goal is to show that one can parameterize all solutions to the embedding problem $A \cdot \lambda G \longrightarrow G \longrightarrow 1$ by a particular collection of submodules of $J(K)$.

4.2. Computations for cyclic modules. When $L/K$ is an elementary $p$-abelian extension that corresponds to a cyclic submodule in $J(K)$, Waterhouse was able to compute the structure of $\text{Gal}(L/F)$. The key ingredient in his analysis is to note that if $L$ is a particular elementary $p$-abelian extension of $K$ and $M$ is the corresponding $\mathbb{F}_p$-space in $J(K)$, then there is a $G$-equivariant perfect pairing $\text{Gal}(L/K) \times M \rightarrow \mathbb{F}_p$

which exhibits a duality between these two groups. Since we know from Galois theory that the Galois groups fit into a short exact sequence $1 \longrightarrow \text{Gal}(L/K) \longrightarrow \text{Gal}(L/F) \longrightarrow \text{Gal}(K/F) \longrightarrow 1$,

we have that $\text{Gal}(L/F)$ is an extension of $\text{Gal}(K/F)$ by $\text{Gal}(L/K)$. But since $\text{Gal}(L/K) \simeq \hat{M}$, and since all $\mathbb{F}_p[G]$-modules are self-dual (see [28, Sec. 1]), one can interpret $\text{Gal}(L/F)$ as an extension of $\text{Gal}(K/F)$ by $M$. All one needs to determine then is the value of $\hat{\sigma}^n$, which Waterhouse accomplishes using a particular field-theoretic computation on a generator for $M$.

Fortunately, the proofs carry over into the characteristic $p$ setting almost entirely unchanged, since they depend only on having a parametrizing space for elementary $p$-abelian extensions whose $\mathbb{F}_p[G]$-module theory encodes the property of being Galois over $F$, together with the $G$-equivariant Kummer pairing. In the characteristic $p$ setting, the Kummer pairing is replaced with the analogous Artin-Schreier pairing, defined as follows. Note that any two roots of $x^p - x - k$ differ by an element of $\mathbb{F}_p$. Furthermore, an element $\tau \in \text{Gal}(L/K)$ acts by permuting roots of $x^p - x - k$, and hence we can define $\langle \tau, m \rangle := \tau(\rho(m)) - \rho(m)$.

(Note that we have written the $\mathbb{F}_p[G]$-action additively since we are in characteristic $p$ and the underlying $\mathbb{F}_p$-structure for Artin-Schreier theory is on the additive group $K$.)

**Proposition 4.1.** [1, Lemma 3.1] Suppose that $\text{char}(K) = p$. If $L/K$ is an elementary $p$-abelian extension and $M \subseteq J$ the corresponding submodule, then the Artin-Schreier pairing is $G$-equivariant and perfect.

With the module structure of $\text{Gal}(L/K)$ determined by the module structure of the corresponding submodule $M \subseteq J(K)$, we only need to determine a value for a lift of $\sigma$ within $\text{Gal}(L/F)$. 

Definition. Let \( \alpha \in J(K) \) be given so that \( \ell(\alpha) < p^n \). If \( \text{char}(K) \neq p \) then the index of \( \alpha \) is defined by

\[
\xi^{e(\alpha)}_p = \sqrt[p]{N_{K/F}(\alpha)^{\ell}}.
\]

If instead \( \text{char}(K) = p \), then the index of \( \alpha \) is defined to be

\[
e(\alpha) = (\sigma - 1) \left( \rho \left( Tr_{K/F}(\alpha) \right) \right) .
\]

An element is said to have trivial index if it’s index is 0.

Proposition 4.2. Suppose that \( m \in J(K) \), and let \( L \) be the extension corresponding to \( \langle \alpha \rangle \). Then

- if \( \ell = p^n \) or \( e(\alpha) = 0 \), then \( \text{Gal}(L/K) \cong \mathbb{F}_p[G]/(\sigma - 1)^{\ell} \rtimes G \); and
- if \( \ell < p^n \) and \( e(\alpha) \neq 0 \), then \( \text{Gal}(L/K) \cong \mathbb{F}_p[G]/(\sigma - 1)^{\ell} \rtimes \rho \cdot G \).

Proof. The result is precisely [27, Prop. 2] when \( \text{char}(K) \neq p \). The proof in this case only relies on a \( G \)-equivariant, perfect pairing between \( \text{Gal}(L/K) \) and \( \langle \alpha \rangle \), and since such a pairing is provided when \( \text{char}(K) = p \) above, the result also follows. For the sake of concreteness, though, we show the reader how one goes about verifying this identity more directly in the case \( \text{char}(K) = p \); of course, this same idea also applies when \( \text{char}(K) \neq p \) after minor notational changes.

Suppose that \( \text{char}(K) = p \) and consider \( \langle \alpha \rangle \subseteq J(K) \); let \( L/F \) be the corresponding extension of fields. Recall that there is only one extension of \( G \) by \( \mathbb{F}_p[G] \), and hence if \( \ell(\alpha) = p^n \) then we have \( \text{Gal}(L/K) \cong \langle \alpha \rangle \cong \mathbb{F}_p[G] \) and \( \text{Gal}(L/F) \cong \mathbb{F}_p[G] \rtimes G \).

Suppose, then, that \( \ell(\alpha) < p^n \). If \( \hat{\sigma} \in \text{Gal}(L/F) \) is a lift of \( \sigma \in \text{Gal}(K/F) \), then we need to determine whether or not \( \hat{\sigma}^{p^n} \) is trivial. Recall that \( \hat{\sigma}^{p^n} \in \text{Gal}(L/K) \) is in the submodule of elements fixed by the action of \( \sigma \). The generator of the fixed module in \( \text{Gal}(L/K) \) is dual to the element \( \alpha \), and so we simply need to know whether \( \hat{\sigma}^{p^n} \) acts trivially on \( \rho(\alpha) \) or not; i.e., we need to compute \( \langle \hat{\sigma}^{p^n}, \alpha \rangle \). Since \( (\sum_{i=1}^{p^n} \hat{\sigma}^i) \rho(\alpha) \) and \( \rho(Tr_{K/F}(\alpha)) \) are both roots for the same polynomial, they have the same image under \( \hat{\sigma} - 1 \); hence we have

\[
\langle \hat{\sigma}^{p^n}, \alpha \rangle = \hat{\sigma}^{p^n} (\rho(\alpha)) - \rho(\alpha)
= (\hat{\sigma}^{p^n} - 1) \rho(\alpha)
= (\hat{\sigma} - 1) \left( \sum_{i=0}^{p^n-1} \hat{\sigma}^i \right) \rho(\alpha)
= (\hat{\sigma} - 1) \left( \rho(Tr_{K/F}(\alpha)) \right).
\]

Since \( \ell(\alpha) < p^n \) it follows that \( Tr_{K/F}(\alpha) = (\sigma - 1)^{p^n-1} \alpha \in \varphi(K) \), and so \( \rho(Tr_{K/F}(\alpha)) \in K \). Hence the action of \( \hat{\sigma} \) on this element is identical to the action of \( \sigma \), and so

\[
\langle \hat{\sigma}^{p^n}, \alpha \rangle = (\sigma - 1) \left( \rho(Tr_{K/F}(\alpha)) \right) = e(\alpha).
\]

Hence \( \hat{\sigma}^{p^n} \) is trivial if and only if \( e(\alpha) = 0 \). \( \square \)
4.3. Moving beyond cyclic modules. Now that we have a description of Galois groups that arise from cyclic submodules of \(J(K)\), we can determine the Galois structure of a generic extension of \(G\) by a finite \(\mathbb{F}_p[G]\)-module in terms of its module structure and the index.

**Definition 4.3.** Suppose that \(A \subseteq J(K)\). If there exists an element \(\alpha \in A\) with \(\ell(\alpha) < p^n\) such that \(e(\alpha) \neq 0\), then we define

\[
\lambda(A) = \min_{\alpha \in A} \{ \ell(\alpha) : \ell(\alpha) < p^n \text{ and } e(\alpha) \neq 0 \}.
\]

Otherwise, we define \(\lambda(A) = p^n\).

**Theorem 4.4.** Suppose that \(A \subseteq J(K)\) is an \(\mathbb{F}_p[G]\)-module and \(L/F\) is the corresponding extension. Then \(L\) solves the embedding problem \(M \cdot \mu \to G \to 1\) over \(K/F\) if and only if \(A \simeq M\) and \(\mu = \lambda(A)\).

**Proof.** Theorem 3.6 tells us that the embedding problem \(\text{Gal}(L/F) \to \text{Gal}(K/F) \to 1\) is given by \(A \bullet A \to G \to 1\) for some \(1 \leq \lambda \leq p^n\). Our goal is to show that \(\lambda = \lambda(A)\). Once we have done this, Proposition 3.7 tells us that this is the only embedding problem that \(L\) solves over \(K/F\).

First, if \(\lambda(A) = p^n\), then there are no elements of length less than \(p^n\) with nontrivial index in \(A\). We claim then that \(\text{Gal}(L/F) \simeq A \times G\). To see this is true, let \(A = \bigoplus \langle \alpha_i \rangle\), and define \(L_i\) to be the field corresponding to \(\langle \alpha_i \rangle\); let \(\tau_i \in \text{Gal}(L/F)\) be chosen so that \(\tau_i\) restricts to the trivial automorphism on all extensions \(L_j/K\) for \(j \neq i\), and which restricts to an \(\mathbb{F}_p[G]\)-generator of \(\text{Gal}(L_i/K)\). By Proposition 4.2 we know that \(\text{Gal}(L_i/F) \simeq \langle \tau_i \rangle \times G\) since either \(e(\alpha_i) = 0\) or \(\ell(\alpha_i) = p^n\). We also have a surjection of embedding problems that comes from Galois theory, and which corresponds to quotienting by the subgroup \(\langle \{\tau_j\}_{j \neq i} \rangle\):

\[
\begin{array}{ccc}
A \bullet A & \longrightarrow & G \\
\psi \downarrow & & 1 \\
\langle \tau_i \rangle \times G & \longrightarrow & G \\
& & 1.
\end{array}
\]

Now if \(\hat{\sigma} \in A \bullet A\) is a lift of \(\sigma\), then \(\psi(\hat{\sigma}) \in \langle \tau_i \rangle \times G\) is a lift of \(\sigma\), and we know that \(\psi(\hat{\sigma})^{p^n} = 1\) if \(\ell(\alpha_i) < p^n\). Hence we have

\[
\hat{\sigma}^{p^n} = \prod_{\ell(\alpha_i) = p^n} \tau_i^{c_i(\sigma-1)^{p^n-1}},
\]

and it follows that \(\text{Gal}(L/F) \simeq A \times G\).

Suppose, then, that \(\lambda(A) < p^n\). We begin by choosing a decomposition \(A = \bigoplus_{i=1}^{\text{rk}(A)} \langle \alpha_i \rangle\) satisfying

\[
\begin{cases}
    e(\alpha_i) \neq 0 \text{ and } \ell(\alpha_i) = \lambda(A) \\
    e(\alpha_i) = 0 \text{ for all } i > 1 \text{ and } \ell(\alpha_i) < p^n.
\end{cases}
\]

To see this is possible, note that if we have any decomposition \(A = \bigoplus_{i=1}^{\text{rk}(A)} \langle \beta_i \rangle\), then we choose \(j\) such that \(\ell(\beta_j)\) is minimal amongst all elements with \(e(\beta_j) \neq 0\). For convenience we can assume that \(j = 1\) and also that \(e(\beta_1) = 1\). We then define \(\alpha_i = \beta_i\) if either \(i = 1\)
or \( \ell(\beta_i) = p^n \), and for \( i > 1 \) with \( \ell(\beta_i) < p^n \) we set \( \alpha_i = \beta_i^{-e(\alpha_i)} \alpha_i \). It is easy to check that \( \langle \alpha_i \rangle = \langle \beta_i \rangle \), and that \( \lambda(A) = \ell(\alpha_1) \).

Let \( L_i \) be the extension corresponding to \( \langle \alpha_i \rangle \); as before, let \( \tau_i \in \text{Gal}(L/F) \) be chosen so that \( \tau_i \) restricts to the trivial automorphism on all extensions \( L_j/K \) for \( j \neq i \), and which restricts to an \( \mathbb{F}_p[G] \)-generator of \( \text{Gal}(L_i/K) \). We know that \( \text{Gal}(L_i/K) \) solves the embedding problem \( \langle \tau_i \rangle \cdot \Lambda_i G \) over \( K/F \), with \( \lambda_1 = \lambda(A) \) and \( \lambda_i = p^n \) for \( i > 1 \). For each \( 1 \leq i \leq \text{rk}(A) \) we have a surjection of embedding problems that arises by quotienting by the subgroup generated by \( \{ \tau_j \}_{j \neq i} \):

\[
\begin{array}{c}
A \cdot \Lambda G \\
\langle \tau_i \rangle \cdot \Lambda_i G
\end{array} \longrightarrow
\begin{array}{c}
G \\
G
\end{array} \longrightarrow 1.
\]

If \( \hat{\sigma} \in A \cdot \Lambda G \) is a lift of \( \sigma \), then \( \psi_i(\hat{\sigma}) \in \text{Gal}(L_i/F) \) is a lift for \( \sigma \). Because we know the group structure of \( \text{Gal}(L_i/K) \), we can say that

\[
\psi_i(\hat{\sigma})^{p^n} = \begin{cases} 
\alpha_1^{c_1(\sigma-1)^{\ell(\alpha_1)-1}}, & \text{if } i = 1 \\
1, & \text{if } i > 1 \text{ and } \ell(\alpha_i) < p^n \\
\alpha_i^{c_i(\sigma-1)^{p^n-1}}, & \text{if } \ell(\alpha_i) = p^n.
\end{cases}
\]

for some \( c_1 \in \mathbb{F}_p^\times \) and \( c_i \in \mathbb{F}_p \). Hence we have

\[
\hat{\sigma}^{p^n} = \tau_1^{c_1(\sigma-1)^{\ell(\alpha_1)-1}} \prod_{\ell(\alpha_i) = p^n} \tau_i^{c_i(\sigma-1)^{p^n-1}},
\]

and it follows that \( \text{Gal}(L/F) \simeq A \cdot \Lambda(A) G \), as desired. \( \square \)

5. Counting solutions to one embedding problem within another

Now that we’ve seen how particular submodules of \( J(K) \) can be used to parametrize the appearance of extensions of \( G \) by an \( \mathbb{F}_p[G] \)-module \( A \) as a Galois group over \( K/F \), we can simply count the appearances of a particular module type within \( J(K) \) to account for the solutions to particular embedding problems \( A \cdot \Lambda G \longrightarrow G \longrightarrow 1 \). Since it requires no more work and ensures finiteness of the associated modules, we will actually answer this question in a slightly different setting: for a given \( A \subseteq J(K) \) corresponding to a finite extension \( E/F \) and a group-theoretic embedding problem \( M \cdot \mu G \longrightarrow G \longrightarrow 1 \), we will count the number of fields \( L \) within \( E/K \) that solve the embedding problem \( M \cdot \mu G \longrightarrow G \longrightarrow 1 \) over \( K/F \). Instead of simply looking for submodules \( U \subseteq J(K) \) with \( U \simeq M \) and \( \lambda(U) = \mu \), in this case we need to satisfy the additional condition that \( U \subseteq A \).

To begin, note that if \( \mu < \lambda \) then no such submodule \( M \) exists since \( A \) contains no elements of length \( \mu \) with non-trivial index. So we will only consider those cases where \( \mu \geq \lambda \).

Our strategy for counting the number of submodules of a particular type is to provide a recipe for building them from the ground up. By this we mean that we provide a way for counting the total number of possibilities for the fixed part of such a submodule, then we
count the number of ways to construct a module with the desired properties and a given fixed part.

Before counting these submodules explicitly, we offer some preparatory lemmas. In the next lemma, the term \( \binom{n}{m}_p \) is a \( p \)-binomial coefficient, defined for \( n \in \mathbb{N} \) and satisfying

\[
\binom{n}{m}_p = \begin{cases} 
0, & \text{if } m < 0 \text{ or } m > n \\
\frac{(p^{n-1})\ldots(p^{n-m+1}-1)}{(p^{m-1})\ldots(p-1)}, & \text{if } 0 \leq m \leq n.
\end{cases}
\]

We also frequently use \( \Delta(V) \) to stand for \( \dim_{\mathbb{F}_p}(V) \) when \( V \) is an \( \mathbb{F}_p \)-vector space.

**Lemma 5.1.** Suppose that \( V = V_1 \supseteq V_2 \supseteq \cdots \supseteq V_{p^n} \supseteq V_{p^n+1} = \{1\} \) is a flag of \( \mathbb{F}_p \)-spaces. If \( \{d_i\} \) is a collection of integers, then the number of flags \( W = W_1 \supseteq W_2 \supseteq \cdots \supseteq W_{p^n} \supseteq W_{p^n+1} = 1 \) satisfying \( d_i = \dim_{\mathbb{F}_p}(W_i) \) and \( W_i \subseteq V_i \) is given by

\[
\prod_i \binom{\Delta(V_i) - d_{i+1}}{d_i - d_{i+1}}_p.
\]

**Proof.** First, observe that if \( W_i \subseteq V_i \) then we have \( d_i \leq \Delta(V_i) \). Hence \( d_i > \Delta(V_i) \) implies there is no collection of nested subspaces with the desired properties. In this case, we also have that the corresponding \( p \)-binomial coefficient \( \binom{\Delta(V_i) - d_{i+1}}{d_i - d_{i+1}}_p = 0 \), and so the identity holds. The same vanishing happens if the terms \( \{d_i\} \) are not a decreasing sequence.

Suppose, then, that \( d_i \leq \Delta(V_i) \) and that \( d_1 \geq d_2 \geq \cdots \). The number of \( \mathbb{F}_p \)-subspaces of \( V_{p^n} \) of dimension \( d_{p^n} \) is \( \binom{\Delta(V_{p^n})}{d_{p^n}}_p \). Now suppose we have shown that the number of choices for nested subspaces \( W_\ell \supseteq \cdots \supseteq W_{p^n} \) is

\[
\prod_{i \geq \ell} \binom{\Delta(V_i) - d_{i+1}}{d_i - d_{i+1}}_p.
\]

For convenience, suppose we have \( \mathbb{F}_p \)-independent collections \( I_i \) such that \( \cup_{i \geq k} I_i \) is a basis for \( W_k \).

For any choice of subspace \( W_{\ell-1} \supseteq W_\ell \) we can find a collection \( I_{\ell-1} \) which we can use to complete \( \cup_{i \geq \ell} I_i \) to a basis for \( W_{\ell-1} \); certainly \( |I_{\ell-1}| = d_{\ell-1} - d_\ell \). We will count the number of choices for \( I_{\ell-1} \) that lead to distinct spaces \( W_{\ell-1} \). The number of choices for \( d_{\ell-1} - d_\ell \) linearly independent elements from \( V_{\ell-1} \) that are additionally linearly independent from \( \cup_{i \geq \ell} I_i \) is

\[
(p^{\Delta(V_{\ell-1})} - p^{d_{\ell}})(p^{\Delta(V_{\ell-1})} - p^{d_{\ell+1}})\cdots(p^{\Delta(V_{\ell-1})} - p^{d_{\ell-1}}).
\]

Likewise, for any given choice of subspace \( W_{\ell-1} \) satisfying \( d_{\ell-1} = \Delta(W_{\ell-1}) \) and \( W_{\ell-1} \supseteq W_\ell \), the number of choices for \( d_{\ell-1} - d_\ell \) linearly independent elements from \( W_{\ell-1} \) that are also linearly independent from \( \cup_{i \geq \ell} I_i \) is

\[
(p^{d_{\ell-1}} - p^{d_\ell})(p^{d_{\ell-1}} - p^{d_{\ell+1}})\cdots(p^{d_{\ell-1}} - p^{d_{\ell-1}}).
\]
Hence the total number of ways to choose $I_{\ell-1}$ is
\[
\frac{(p^{\Delta(V_{\ell-1})} - p^{d_\ell})}{(p^{d_\ell} - p^{d_{\ell-1}})} \cdot \frac{(p^{\Delta(V_{\ell-1})} - p^{d_{\ell-1}+1})}{(p^{d_{\ell-1}} - p^{d_{\ell-1}+1})} \cdots \frac{(p^{\Delta(V_{\ell-1})} - p^{d_{\ell-1}-1})}{(p^{d_{\ell-1}} - p^{d_{\ell-1}-1})} = \frac{(p^{\Delta(V_{\ell-1})} - d_\ell - 1)}{(p^{d_{\ell-1}} - d_\ell - 1)} \cdots \frac{(p^{\Delta(V_{\ell-1})} - d_{\ell-1} + 1)}{(p - 1)}.
\]
\[
= \left( \Delta(V_{\ell-1}) - d_\ell \over d_{\ell-1} - d_\ell \right)_p.
\]

\[\square\]

Suppose that $V$ is an $\mathbb{F}_p[G]$-module, and consider the filtration
\[V^G = V_1 \supseteq V_2 \supseteq \cdots \supseteq V_p \supseteq V_{p+1} = 1.\]
If a submodule $U \subseteq V$ is isomorphic to a given $\mathbb{F}_p[G]$-module $B$, then of course $U_{(i)} \subseteq V_{(i)}$ and $\Delta(U_{(i)}) = \Delta(B_{(i)})$. Conversely, for any flag $W = W_1 \supseteq W_2 \supseteq \cdots \supseteq W_{p^n} \supseteq W_{p^n+1} = 1$ satisfying $W_i \subseteq V_{(i)}$ and $\Delta(W_i) = \Delta(B_{(i)})$, there exists an $\mathbb{F}_p[G]$-module $U \subseteq V$ such that $W_i = U_{(i)}$ and $U \cong B$. To see this, choose collections $I_{\ell}$ such that $\bigcup_{\ell} I_{\ell}$ is a basis for $W_{\ell}$, and let $I = \cup_{\ell} I_{\ell}$. For each $x \in B_{\ell}$, select an element $v_x \in V$ such that $x = v_x^{(\sigma-1)^{\ell-1}}$; such a selection is possible since $x \in V_{(i)}$. Proposition 2.1 then tells us that $\bigoplus_{x \in I} \langle v_x \rangle \cong B$.

The following lemma tells us how we can determine when two submodules constructed in this way are identical.

**Lemma 5.2.** Suppose that $V$ is an $\mathbb{F}_p[G]$-module and $I \subseteq V^G$ is a collection of $\mathbb{F}_p$-independent elements. For each $x \in I$, let $1 \leq \ell_x \leq p^n$ be given so that $x \in W_{(\ell_x)}$, and suppose that $\alpha_x, \beta_x \in V$ satisfy
\[\alpha_x^{(\sigma-1)^{\ell_x-1}} = x = \beta_x^{(\sigma-1)^{\ell_x-1}}.\]
Then $\bigoplus_{x \in I} \langle \alpha_x \rangle = \bigoplus_{x \in I} \langle \beta_x \rangle$ if and only if for every $y \in I$ we have $\beta_y \in \bigoplus_{x \in I} \langle \alpha_x \rangle$.

*Proof.* Certainly one direction is trivial. For the other, we show that $\bigoplus \langle \alpha_x \rangle \subseteq \bigoplus \langle \beta_x \rangle$ by induction on length. The elements of length 1 in both modules are simply the $\mathbb{F}_p$-span of the collection $I$. Suppose we know that any element of length $\ell - 1$ within $\bigoplus \langle \alpha_x \rangle$ is contained in $\bigoplus \langle \beta_x \rangle$, and let $\alpha \in \bigoplus \langle \alpha_i \rangle$ be given so that $\ell(\alpha) = \ell$. Hence
\[\alpha^{(\sigma-1)^{\ell-1}} = \prod_{\ell_x \geq \ell} x^{c_x} = \left( \prod_{\ell_x \geq \ell} \beta_x^{c_x (\sigma-1)^{\ell_x - \ell}} \right)^{(\sigma-1)^{\ell-1}}.\]
It follows that $\hat{\alpha} := \alpha / \prod \beta_x^{c_x (\sigma-1)^{\ell_x - \ell}}$ has length less than $\ell$, and since each $\beta_y \in \bigoplus \langle \alpha_x \rangle$ it also follows that $\hat{\alpha} \in \bigoplus \langle \alpha_x \rangle$. By induction, $\hat{\alpha} \in \bigoplus \langle \beta_x \rangle$, and hence so too $\alpha \in \bigoplus \langle \beta_x \rangle$. \[\square\]

Since our analysis will require us to be extremely careful about selecting elements based on their index, we introduce notation that allows us to distinguish those elements of trivial index.

**Definition 5.3.** For $A \subseteq J(K)$, we define
\[A^0 = \{ \alpha \in A : \ell(\alpha) < p^n \text{ and } e(\alpha) = 0 \}.\]
Lemma 5.4. For $A \subseteq J(K)$, if $i < p^n$ then $\Delta(A_{(i)}^0) = \Delta(A_{(i)}) - \mathbbm{1}_{i=\lambda(A)}$.

Remark. Notice that $A_{(i)}^0 = \text{im} \left( A^0 \xrightarrow{(\sigma-1)^{i-1}} A^0 \right) \cap (A^0)^G$, and not $A_{(i)} \cap \ker(e)$. In particular, this means that $A_{(p^n)}^0 = \{1\}$, since all elements of $A^0$ have length at most $p^n - 1$.

Proof. Suppose first that $\lambda(A) = p^n$, and let $x \in \Delta(A_{(i)})$ be given with $i < p^n$. Any solution $\alpha \in A$ to $x = \alpha(\sigma-1)^{i-1}$ must have $e(\alpha) = 0$, since otherwise $\lambda(A) \leq i$. Hence $x \in A_{(i)}^0$. The same argument shows that if $\lambda(A) < p^n$ and $i < \lambda(A)$, then $A_{(i)} \subseteq A_{(i)}^0$.

Suppose, then, that $\lambda(A) < p^n$ and $i \geq \lambda(A)$. Let $\chi \in A$ be given with $\ell(\chi) = \lambda(A)$ and $e(\chi) = 1$; let $x \in A_{(i)}$ be given. For any solution $\alpha \in A$ to $x = \alpha(\sigma-1)^{i-1}$ we have $e(\alpha \chi^{-e(\alpha)}) = 0$, and hence

$$x \chi^{-e(\alpha)(\sigma-1)^{i-1}} = (\alpha \chi^{-e(\alpha)})^{(\sigma-1)^{i-1}} \in A_{(i)}^0.$$ 

Now when $i > \lambda(A)$ the left side of this equation becomes $x$, and hence we have $x \in A_{(i)}^0$ as desired. When $i = \lambda(A)$, this equation shows that $A_{(\lambda(A))} = \langle \chi^{(\sigma-1)^{\lambda(A)-1}} \rangle \oplus A_{(\lambda(A))}^0$.

Lemma 5.5. Suppose that $A \subseteq J(K)$, and let $M$ be an $\mathbb{F}_p[G]$-module. A given filtration $W = W_1 \supseteq W_2 \supseteq \cdots \supseteq W_{p^n} \supseteq W_{p^n+1} = \{1\}$ within $A^G$ satisfies $W_i = U_{(i)}$ for some module $U \subseteq A$ with $U \simeq M$ and $\lambda(U) = p^n$ if and only if

$$\Delta(W_i) = \Delta(M_{(i)})$$

$$W_i \subseteq \begin{cases} A_{(i)}^0, & \text{if } i < p^n \\ A_{(p^n)}, & \text{if } i = p^n. \end{cases}$$

(4)

Proof. First, if $U \subseteq A$ with $U \simeq M$ and $\lambda(U) = p^n$, then consider the natural filtration $U = U_{(1)} \supseteq U_2 \supseteq \cdots \supseteq U_{(p^n)} \supseteq U_{(p^n+1)} = \{1\}$. The condition $U \simeq M$ implies that $\Delta(U_{(i)}) = \Delta(M_{(i)})$ for all $1 \leq i \leq p^n$. The condition $U_{(i)} \subseteq A_{(i)}$ comes from the inclusion $U \subseteq A$. The additional restriction that $\lambda(U) = p^n$ implies that $U_{(i)} \subseteq A_{(i)}^0$ for each $1 \leq i < p^n$; otherwise there would be some $1 \leq i < p^n$ and an element $x \in U_{(i)}$ such that any solution $u \in U$ to $x = u^{(\sigma-1)^{i-1}}$ would satisfy $e(U) \neq 0$, contradicting $\lambda(U) = p^n$.

Conversely, suppose that $W \subseteq A^G$ has a filtration that satisfies conditions [4]. Choose a basis $B_{p^n}$ for $W_{p^n}$, and for each $i < p^n$ select a basis $B_i$ for a complement of $W_{i+1}$ within $W_i$. For each $x \in B_i$ choose an element $\alpha_x$ so that $x = \alpha_x^{(\sigma-1)^{i-1}}$; when $i < p^n$ we may choose $\alpha_x$ such that $e(\alpha_x) = 0$ since $x \in A_{(i)}^0$. Then the module $U = \oplus_{x \in B} \langle \alpha_x \rangle$ satisfies the conditions $U \simeq M$ and $\lambda(U) = p^n$.

Theorem 5.6. Suppose that $E/F$ is a solution to the embedding problem $A \bullet \chi G \longrightarrow G \longrightarrow 1$. Suppose further that $M$ is an $\mathbb{F}_p[G]$-module. Then the number of solutions to the embedding problem $M \rtimes G \longrightarrow G \longrightarrow 1$ within the extension $E/F$ is

$$\prod_{i=1}^{p^n} \left( \frac{\Delta(A_{(i)}) - \Delta(M_{(i+1)}) - \mathbb{1}_{i=\lambda} \cdot \mathbb{1}_{i \neq p^n}}{\Delta(M_{(i)}) - \Delta(M_{(i+1)})} \right)_p \left( p \sum_{j<i} \Delta(A_{(j)}) - \Delta(M_{(j)}) - \mathbb{1}_{j=\lambda} \cdot \mathbb{1}_{i \neq p^n} \right) \Delta(M_{(i)}) - \Delta(M_{(i+1)}) \right).$$
Proof. By Theorem 4.4 we know that a solution to this embedding problem within $E/F$ corresponds to a submodule

$$U \subseteq A$$

so that $U \cong M$ and $\lambda(U) = p^n$. (5)

To count all such submodules, we’ll count the number of filtrations $W = W_1 \supseteq W_2 \supseteq \cdots \supseteq W_{p^n} \supseteq W_{p^n+1} = \{1\}$ within $A^G$ for which there exists a submodule $U \subseteq A$ with $U \cong M$, $\lambda(U) = 0$ and $U_{\{j\}} = W_j$. For each such filtration, we will then count the number of modules $U$ as above.

Lemma 5.5 characterizes the flags within $A^G$ that are the fixed part of a submodule $U$ satisfying (5). By Lemma 5.1, the number of such flags is

$$\left( \frac{\Delta(A_{i(p^n)})}{\Delta(M_{(p^n)})} \right) \prod_{i=1}^{p^n-1} \left( \frac{\Delta(A_{(i)}) - \Delta(M_{(i+1)})}{\Delta(M_{(i)}) - \Delta(M_{(i+1)})} \right).$$

So suppose we have chosen a flag $\{W_i\} \subseteq A^G$ satisfying (4), and let $B$ be a basis for $W$ as in the previous paragraph. A submodule $U \subseteq A$ satisfies $W = U^G$ and (5) if and only if $U = \oplus_{x \in B} \langle \alpha_x \rangle$ for elements $\{\alpha_x\} \subseteq A$ satisfying

$$\begin{cases} 
\alpha_{\langle x \rangle}^{(s-1)^{i-1}} = x, & \text{for all } x \in B_i \\
e(\alpha_x) = 0, & \text{for all } x \in B_i \text{ with } i < p^n.
\end{cases}$$

We need to count the number of choices of $\{\alpha_x\}$ satisfying (6) which yield distinct modules.

Suppose that $\{\alpha_x\}_{x \in B}$ is such a collection, and let $\{\tilde{\alpha}_x\}_{x \in B}$ be another such collection. Then for each $x \in B_i$ we have $\tilde{\alpha}_x = g_x \alpha_x$ for some $g_x \in A$ and $\ell(g_x) < i$, and when $i < p^n$ we also have $e(g_x) = 0$. Conversely, any choice of a collection $\{g_x\}_{x \in B}$ such that $\ell(g_x) < i$ for $x \in B_i$ and $e(g_x) = 0$ when $i < p^n$ gives rise to a collection $\{g_x \alpha_x\}$ that satisfies (6). For each given $x \in B_i$ with $i < p^n$, the total number of choices for a given $g_x$ is simply the number of elements of length less than $i$ contained within $A^0$, which is counted by

$$p^{\sum_{j<i} \Delta(A_{(j)})}.$$

For each $x \in B_{p^n}$, the total number of choices for a given $g_x$ is the number of elements of length less than $p^n$ within $A$, which is given by

$$p^{\sum_{j<p^n} \Delta(A_{(j)})}.$$

Hence the total number of choices for the collection $\{g_x\}$ — and therefore the total number of collections $\{\alpha_x\}$ satisfying (6) — is given by

$$\left( p^{\sum_{j<p^n} \Delta(A_{(j)})} \right) \prod_{i=1}^{p^n-1} \left( p^{\sum_{j<i} \Delta(A_{(j)})} \right) \Delta(M_{(i)}) - \Delta(M_{(i+1)}).$$

By Lemma 5.2 the choices $\{\alpha_x\}_{x \in B}$ and $\{\tilde{\alpha}_x\}_{x \in B}$ satisfy $\oplus \langle \alpha_x \rangle = \oplus \langle \tilde{\alpha}_x \rangle$ if and only if for each $y \in B$ we have $g_y \in \oplus \langle \alpha_x \rangle$. This occurs if and only if for each $y \in B_i$ we have that $g_y$ is an element of $\oplus \langle \alpha_x \rangle \cong M$ of length less than $i$, of which there are

$$p^{\sum_{j<i} \Delta(M_{(j)})}$$
choices. Hence we have overcounted by a factor of
\[
\prod_{i=1}^{p^n} \left( p^{\sum_{j<i} \Delta(M_{i+j})} \right)^{\Delta(M_{i+1}) - \Delta(M_{i+1})}.
\]

To reach the desired conclusion, we make the relevant substitutions from Lemma 5.4. □

**Lemma 5.7.** Suppose that \(A \subseteq J(K)\) has \(\lambda := \lambda(A) \neq p^n\), and let \(M\) be an \(\mathbb{F}_p[G]\)-module. A given filtration \(W = W_1 \supseteq W_2 \supseteq \cdots \supseteq W_{p^n} \supseteq W_{p^n+1} = \{1\}\) within \(A^G\) satisfies \(W_i = U_{\{i\}}\) for some module \(U \subseteq A\) with \(U \simeq M\) and \(\lambda(U) = \lambda\) if and only if
\[
\Delta(W_\ell) = \Delta(M_{\ell})
\]
\[
W_\ell \subseteq \begin{cases} A^0_{\{\ell\}}, & \text{if } \ell < \lambda; \\
A_{\{\ell\}}, & \text{if } \ell \geq \lambda.
\end{cases}
\]

(7)

**Proof.** To see that this is true, suppose that \(U \subseteq A\) satisfies \(U \simeq M\) and \(\lambda(U) = \lambda\), and consider the natural filtration given by the subspaces \(U_{\{i\}}\). The condition \(U \simeq M\) implies \(\Delta(U_{\{i\}}) = \Delta(M_{\{i\}})\) for all \(1 \leq i \leq p^n\). The inclusion \(U \subseteq A\) implies that \(U_{\{i\}} \subseteq A_{\{i\}}\) for all \(1 \leq i \leq p^n\). However, since \(\lambda(U) = \lambda\) we know there are no elements in \(U\) of length less than \(\lambda\) with non-trivial index, and hence for \(b \in U_{\{i\}}\) with \(i < \lambda\) we know that any solution to \(b = u^{(\sigma-1)^{-1}}\) with \(u \in U\) must have \(u \in U^0\). Hence \(U_{\{i\}} \subseteq A^0_{\{i\}}\) if \(i < \lambda\). For the final condition, suppose to the contrary that \(U_{\{i\}} \subseteq A^0_{\{i\}}\), and let \(u \in U\) be given so that \(e(u) \neq 0\) and \(\ell(u) = \lambda\). Now by assumption \(u^{(\sigma-1)^{-1}} = v^{(\sigma-1)^{-1}}\) for some \(v \in U^0\), and so \(u/v\) has \(\ell(u/v) < \lambda\) and \(e(u/v) \neq 0\). This contradicts the condition \(\lambda(U) = \lambda\), and so our assumption that \(U_{\{i\}} \subseteq A^0_{\{i\}}\) is false.

Conversely, suppose that \(W \subseteq A^G\) has a filtration that satisfies conditions (7). Choose a basis \(B_{p^n}\) for \(W_{p^n}\), and for each \(i < p^n\) select a basis \(B_i\) for a complement of \(W_{i+1}\) within \(W_i\). For each \(x \in B_i\) choose an element \(\alpha_x\) so that \(x = \alpha_x^{(\sigma-1)^{-1}}\); when \(i < \lambda\) we may choose \(\alpha_x\) such that \(e(\alpha_x) = 0\) since \(x \in A^0_{\{i\}}\), and when \(i = \lambda\) we must have \(e(\alpha_x) \neq 0\) for some \(x\) since \(B_x \not\subseteq A^0_{\{\lambda\}}\). Then the module \(U = \oplus_{x \in B}(\alpha_x)\) satisfies the conditions \(U \simeq M\) and \(\lambda(U) = \lambda\). □

**Theorem 5.8.** Suppose that \(E/F\) is a solution to the embedding problem \(A \bullet \lambda G \longrightarrow G \longrightarrow 1\) with \(\lambda < p^n\). Suppose further that \(M\) is an \(\mathbb{F}_p[G]\)-module, and that \(M\) contains a summand of dimension \(\lambda\). Then the number of solutions to the embedding problem \(M \bullet \lambda G \longrightarrow G \longrightarrow 1\) within \(E/F\) is
\[
\left( \frac{\Delta(A_{\{\lambda\}})}{\Delta(M_{\{\lambda\}})} - \Delta(M_{\{\lambda+1\}}) \right)_p - \left( \frac{\Delta(A_{\{\lambda\}})}{\Delta(M_{\{\lambda\}})} - \Delta(M_{\{\lambda+1\}}) - 1 \right)_p \prod_{i \neq \lambda} \left( \frac{\Delta(A_{\{i\}})}{\Delta(M_{\{i\}})} - \Delta(M_{\{i+1\}}) \right)_p
\]
\[
\times \prod_{i=1}^{p^n} \left( p^{\sum_{j<i} \Delta(A_{\{j\}})} \right)^{\Delta(M_{\{i\}}) - \Delta(M_{\{i+1\}})}.
\]
Proof. We follow the same approach as in the proof of the previous theorem, enumerating the solutions to the embedding problem $M \bullet \lambda \overset{G}{\longrightarrow} G \overset{1}{\longrightarrow}$ by counting the number of submodules

$$U \subseteq A \text{ such that } U \cong M \text{ and } \lambda(U) = \lambda. \quad (8)$$

Also as before, we do this by first counting the number of filtrations $W \subseteq A^G$ that could arise as the fixed part of such a submodule, and then for each such filtration we count the number of submodules $U \subseteq A$ “above” this filtration satisfying (8).

By Lemma 5.1, a subspace $W \subseteq A^G$ is the fixed part of a module $U$ satisfying (8) if and only if $W$ satisfies (7). By a small variant of Lemma 5.1, the number of such subspaces is therefore

$$\prod_{\lambda \neq i} p^n \left( \frac{\Delta(A_{\{i\}}) - \Delta(M_{\{i+1\}})}{\Delta(M_{\{i\}}) - \Delta(M_{\{i+1\}})} \right) \Delta(A_{\{i\}}) - \Delta(M_{\{i+1\}}). \quad (9)$$

So suppose we have chosen a subspace $W \subseteq A^G$ satisfying (7), and let $B$ be a basis for $W$ as in the previous paragraph. A submodule $U \subseteq A$ satisfies $W = U^G$ and (8) if and only if $U = \oplus_{x \in B} \langle \alpha_x \rangle$ for elements $\{\alpha_x\} \subseteq A$ satisfying

$$\alpha_x^{(\sigma-1)^{-1}} = x, \quad \text{for all } x \in B_i \quad (9)$$

(Since our fixed submodule has $W_i \subseteq A^0_{\{i\}}$ for all $i < \lambda$ and $W_\lambda \not\subseteq A^0_{\{\lambda\}}$ by construction, any selection of $\alpha_x$ satisfying (9) will satisfy the necessary index conditions to ensure $\lambda(U) = \lambda.$) We need to count the number of different choices of $\{\alpha_x\}$ satisfying (9) which yield distinct modules.

Suppose, then, that $\{\alpha_x\}$ is one such collection satisfying (9), and let $\{\hat{\alpha}_x\}$ be another. Then for each $x \in B$, there exists an element $g_x \in A$ with $\hat{\alpha}_x = g_x \alpha_x$ and so that $\ell(g_x) < i.$ Conversely, any choice of a collection $\{g_x\}_{x \in B}$ such that $\ell(g_x) < i$ for $x \in B_i$ gives rise to a collection $\{g_x \alpha_x\}$ that satisfies (9). Since the total number of elements of length less than $i$ within $A$ is given by $p^{\sum_{j<i} \Delta(A_{\{j\}})}$, the total number of choices for collections $\{g_x\}$ and hence collections $\{\alpha_x\}$ satisfying (9) — is given by

$$\prod_{i=1}^n \left( p^{\sum_{j<i} \Delta(A_{\{j\}})} \Delta(M_{\{i\}}) - \Delta(M_{\{i+1\}}) \right).$$

Two collections $\{\alpha_x\}$ and $\{\hat{\alpha}_x\}$ satisfy $\oplus \langle \alpha_x \rangle = \oplus \langle \hat{\alpha}_x \rangle$ if and only if $g_x \in \oplus \langle \alpha_x \rangle$ for each $x \in B$ by Lemma 5.2. For each $x \in B$, the total number of possibilities for $g_x$ is therefore the total number of elements of length less than $i$ within $\oplus \langle \alpha_x \rangle \simeq M$:

$$p^{\sum_{j<i} \Delta(M_{\{j\}})}.$$

Hence we have overcounted by a factor of

$$\prod_{i=1}^n \left( p^{\sum_{j<i} \Delta(M_{\{j\}})} \Delta(M_{\{i\}}) - \Delta(M_{\{i+1\}}) \right).$$

Again, we reach the desired conclusion with relevant substitutions from Lemma 5.4. □
Lemma 5.9. Suppose that $A \subseteq J(K)$ has $\lambda := \lambda(A)$, and let $M$ be an $\mathbb{F}_p[G]$-module. Let $\mu < p^n$ be given with $\mu > \lambda$. A filtration $W = W_1 \supseteq W_2 \supseteq \cdots \supseteq W_{p^n} \supseteq W_{p^n+1} = \{1\}$ within $A^G$ satisfies $W_i = U_{(i)}$ for some module $U \subseteq A$ with $U \simeq M$ and $\lambda(U) = \mu$ if and only if
\[
\Delta(W_\ell) = \Delta(M_{(\ell)}) \quad W_\ell \subseteq \begin{cases} A_0^{(\ell)}, & \text{if } \ell < \mu, \\ A_{(\ell)}, & \text{if } \ell \geq \mu. \end{cases}
\] (10)

Proof. To see that this is true, suppose that $U \subseteq A$ satisfies $U \simeq M$ and $\lambda(U) = \mu$, and consider the natural filtration given by the subspaces $U_{(i)}$. The condition $U \simeq M$ implies $\Delta(U_{(i)}) = \Delta(M_{(i)})$ for all $1 \leq i \leq p^n$. The inclusion $U \subseteq A$ implies that $U_{(i)} \subseteq A_{(i)}$ for all $1 \leq i \leq p^n$. However, since $\lambda(U) = \mu$, we know there are no elements in $U$ of length less than $\mu$ with non-trivial index, and hence for any $b \in U_{(i)}$ with $i < \mu$, we know that any solution to $b = u^{(\sigma-1)^{i-1}}$ must have $u \in U_0$. Hence $U_{(i)} \subseteq A_0^{(i)}$ if $i < \mu$.

Conversely, suppose that $W \subseteq A^G$ has a filtration that satisfies conditions (10). Choose a basis $B_{p^n}$ for $W_{p^n}$, and for each $i < p^n$ select a basis $B_i$ for a complement of $W_{i+1}$ within $W_i$. For each $x \in B_i$, choose an element $\alpha_x$ so that $x = \alpha_x^{(\sigma-1)^{i-1}}$. When $i < \mu$, we may choose $\alpha_x$ such that $e(\alpha_x) = 0$ since $x \in A_0^{(i)}$. We may also select (at least) one $x \in B_\mu$ so that $e(\alpha_x) \neq 0$ since $\mu > \lambda$. With these choices made, the module $U = \bigoplus_{x \in B}(\alpha_x)$ satisfies the conditions of (11).

\[\square\]

Theorem 5.10. Suppose that $E/F$ is a solution to the embedding problem $A \bullet_\lambda G \longrightarrow G \longrightarrow 1$. Suppose further that $M$ is an $\mathbb{F}_p[G]$-module, and that $M$ contains a summand of dimension $\mu$ satisfying $\lambda < \mu < p^n$. Then the number of solutions to the embedding problem $M \bullet_\mu G \longrightarrow G \longrightarrow 1$ within $E/F$ is
\[
\prod_{i=1}^{p^n} \left( \frac{\Delta(A_{(i)}) - \Delta(M_{(i+1)}) - 1 = \lambda}{\Delta(M_{(i)}) - \Delta(M_{(i+1)})} \right) \times \prod_{i=1}^{p^n} \left( \frac{\Delta(M_{(i)})}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) \Delta\left(\frac{\Delta(A_{(i)}) - 1 = \lambda - 1 < \mu}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) \Delta\left(\frac{\Delta(M_{(i)})}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) - \prod_{i=1}^{p^n} \left( \frac{p^{\sum_{j<i} \Delta(A_{(j)}) - 1 = \lambda - 1 < \mu}}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) \Delta\left(\frac{\Delta(A_{(i)}) - 1 = \lambda - 1 < \mu}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) \Delta\left(\frac{\Delta(M_{(i)})}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) - \prod_{i=1}^{p^n} \left( \frac{p^{\sum_{j<i} \Delta(A_{(j)}) - 1 = \lambda - 1 < \mu}}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) \Delta\left(\frac{\Delta(M_{(i)})}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) - \prod_{i=1}^{p^n} \left( \frac{p^{\sum_{j<i} \Delta(A_{(j)}) - 1 = \lambda - 1 < \mu}}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) \Delta\left(\frac{\Delta(M_{(i)})}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) - \prod_{i=1}^{p^n} \left( \frac{p^{\sum_{j<i} \Delta(A_{(j)}) - 1 = \lambda - 1 < \mu}}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) \Delta\left(\frac{\Delta(M_{(i)})}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) - \prod_{i=1}^{p^n} \left( \frac{p^{\sum_{j<i} \Delta(A_{(j)}) - 1 = \lambda - 1 < \mu}}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) \Delta\left(\frac{\Delta(M_{(i)})}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) - \prod_{i=1}^{p^n} \left( \frac{p^{\sum_{j<i} \Delta(A_{(j)}) - 1 = \lambda - 1 < \mu}}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right) \Delta\left(\frac{\Delta(M_{(i)})}{p^{\sum_{j<i} \Delta(M_{(j)})}} \right)
\]

Proof. We follow the same strategy as in the previous two cases. This time we are interested in those submodules
\[
U \subseteq A \text{ such that } U \simeq M \text{ and } \lambda(U) = \mu.
\] (11)

We start by enumerating the number of filtrations $W \subseteq A^G$ that are the fixed part of such a submodule $U$, then for each such filtration we count the number of such submodules $U$ satisfying (11) that are “above” the filtration.

Lemma 5.9 tells us that the subspaces $W \subseteq A^G$ which are the fixed part of a module $U$ satisfying (11) are those which satisfy (10). By Lemma 5.1, the number of such subspaces
is
\[
\prod_{i=1}^{\mu-1} \left( \Delta(A_{(i)}^0) - \Delta(M_{(i+1)}) \right) \prod_{i=\mu}^{p} \left( \Delta(A_{(i)}) - \Delta(M_{(i+1)}) \right).
\]

So suppose we have chosen a subspace \( W \subseteq A^G \) with a filtration \( \{W_i\} \) satisfying (10), and let \( \mathcal{B} \) be a basis for \( W \) as in the previous paragraph. A submodule \( U \subseteq A \) satisfies \( W = U^G \) and (11) if and only if \( U = \oplus_{x \in \mathcal{B}} (\alpha_x) \) for elements \( \{\alpha_x\} \subseteq A \) satisfying
\[
\alpha_x^{(p-1)^{i-1}} = x, \quad \text{for all } x \in \mathcal{B}_i
\]
\[
e(\alpha_x) = 0 \quad \text{for all } x \in \mathcal{B}_i \text{ with } i < \mu
\]
\[
e(\alpha_x) \neq 0 \quad \text{for some } x \in \mathcal{B}_\mu.
\]  
(12)

We need to count the number of different choices of \( \{\alpha_x\} \) satisfying (12) which yield distinct modules.

To enumerate those collections \( \{\alpha_x\} \) satisfying (12), start by choosing elements \( \{\beta_x\}_{x \in \mathcal{B}} \) so that
\[
\beta_x^{(p-1)^{i-1}} = x \quad \text{for all } x \in \mathcal{B}_i
\]
\[
e(\beta_x) = 0 \quad \text{for all } x \in \mathcal{B}_i \text{ with } i < \mu
\]
If \( \{\alpha_x\} \) satisfies (12), then for each \( x \in \mathcal{B}_i \) there exists \( h_x \in A \) such that \( \alpha_x = h_x\beta_x \) and \( \ell(h_x) < i \). Note also that \( e(\alpha_x) = e(h_x) \) when \( i < p^n \). Hence to enumerate the number of choices of \( \{\alpha_x\} \) satisfying (12), we will count the total number of ways to choose \( \{h_x\} \subseteq A \) so that \( e(h_x) = 0 \) for all \( x \in \mathcal{B}_i \) with \( i < \mu \) and subtract the total number of ways to choose \( \{h_x\} \subseteq A \) so that \( e(h_x) = 0 \) for all \( x \in \mathcal{B}_i \) with \( i \leq \mu \). To do this, note that the number of elements of length less than \( i \) within \( A \) is \( p^{\sum_{j < i} \Delta(A_{(j)})} \), and the number of elements of length less than \( i \) within \( A \) that have trivial index is \( p^{\sum_{j < i} \Delta(A_{(j)})} \cdot 1_{j \leq \lambda} \). Therefore the total number of choices for \( \{h_x\} \) — and hence the total number of collections \( \{\alpha_x\} \) satisfying (12) — is given by
\[
\prod_{i=1}^{p^n} \left( p^{\sum_{j < i} \Delta(A_{(j)})} \cdot 1_{j = \lambda} \cdot 1_{i \leq \mu} \right) \Delta(M_{(i)}) - \Delta(M_{(i+1)}) - \prod_{i=1}^{p^n} \left( p^{\sum_{j < i} \Delta(A_{(j)})} \cdot 1_{j = \lambda} \cdot 1_{i \leq \mu} \right) \Delta(M_{(i)}) - \Delta(M_{(i+1)})\).
\]

Now suppose that \( \{\alpha_x\} \) and \( \{\hat{\alpha}_x\} \) are two collections satisfying (12); we examine when \( \oplus(\alpha_x) = \oplus(\hat{\alpha}_x) \). Note that for each \( x \in \mathcal{B}_i \) there exists \( g_x \in A \) so that \( \hat{\alpha}_x = g_x\alpha_x \), and that \( \ell(g_x) < i \). Notice also that \( e(g_x) = 0 \) for all \( x \in \mathcal{B}_i \) with \( i < \mu \), and that \( e(g_x\alpha_x) \neq 0 \) for some \( x \in \mathcal{B}_\mu \). On the other hand, Lemma 7.2 tells us that \( \oplus(\alpha_x) = \oplus(\hat{\alpha}_x) \) if and only if \( g_x \in \oplus(\alpha_x) \) for all \( x \in \mathcal{B} \). Hence we must count the number of collections \( \{g_x\} \subseteq \oplus(\alpha_x) \) satisfying
\[
\ell(g_x) < i, \quad \text{for all } x \in \mathcal{B}_i
\]
\[
e(g_x) = 0, \quad \text{for all } x \in \mathcal{B}_i \text{ where } i < \mu
\]
\[
e(g_x\alpha_x) \neq 0 \quad \text{for some } x \in \mathcal{B}_\mu.
\]  
(13)

Since \( \lambda(\oplus(\alpha_x)) = \mu \), if the first condition is satisfied then the second and third conditions are automatically satisfied. Hence we must only count the number of collections \( \{g_x\} \subseteq \oplus(\alpha_x) \) satisfying
\[
\ell(g_x) < i, \quad \text{for all } x \in \mathcal{B}_i
\]
\[
e(g_x) = 0, \quad \text{for all } x \in \mathcal{B}_i \text{ where } i < \mu
\]
\[
e(g_x\alpha_x) \neq 0 \quad \text{for some } x \in \mathcal{B}_\mu.
\]
⊕⟨αx⟩ satisfying ℓ(αx) < i for each x ∈ B_i. Since the number of elements of length i within ⊕⟨αx⟩ ≃ M is \( p^{\sum_{j<i} \Delta(M(j))} \), the number of such collections is
\[
\prod_{i=1}^p \left( p^{\sum_{j<i} \Delta(M(j))} \right)^{\Delta(M(i)) - \Delta(M(i+1))}.
\]

6. Embedding problems over a given K/F

We have already seen that a solution to the embedding problem \( A \bullet_\lambda G \twoheadrightarrow G \twoheadrightarrow 1 \) over \( K/F \) corresponds to a submodule \( U \subseteq J(K) \) with \( U \simeq A \) and \( \lambda(U) = \lambda \). If one knows the module structure of \( J(K) \) and a method for computing \( \lambda(J(K)) \) for a given extension \( K/F \) with Gal(\( K/F \)) ≃ \( \mathbb{Z}/p^n\mathbb{Z} \), then one knows everything about embedding problems over \( K/F \) with elementary \( p \)-abelian kernel. On the other hand, if one can make general statements about module structures of \( J(K) \) and \( \lambda(J(K)) \) across all fields \( K \), then one can make connections between a priori unrelated embedding problems. These goals will be the focus of this section.

We begin with a discussion of the module structure for \( J(K) \). The investigation into the module structure of \( J(K) \) began with Fadeev and Borevič's computations of \( J(K) \) when \( K \) is a local field (see [2, 7]). Miňáč and Swallow were able to compute the module structure of \( J(K) \) when Gal(\( K/F \)) ≃ \( \mathbb{Z}/p^n\mathbb{Z} \) and \( \xi_p \in K \) in [25]. In the case that char(\( K \)) ≠ \( p \) and Gal(\( K/F \)) ≃ \( \mathbb{Z}/p^n\mathbb{Z} \) with \( n \geq 1 \), the module structure for \( J(K) \) was computed in [27, Th. 2] and [28, Th. 2].

To state the decomposition, recall that for an extension \( K/F \) with Galois group \( G = \langle \sigma \rangle \simeq \mathbb{Z}/p^n\mathbb{Z} \), we write \( K_i \) for the intermediate field of degree \( p^i \) over \( F \). We let \( G_i = \text{Gal}(K_i/F) \). We also assign an invariant \( i(K/F) \in \{-\infty, 0, \cdots, n-1\} \) as in the paragraph preceding the statement of Theorem 1.1 in section 1. When char(\( K \)) ≠ \( p \), we write \( \hat{K} \) for the field \( K(\xi_p) \), and likewise denote \( \hat{K}_i = K_i(\xi_p) \). A generator for Gal(\( \hat{K}/\hat{K} \)) is denoted \( \epsilon \), and \( \epsilon(\xi_p) = \xi_p^t \). For a submodule \( A \subseteq J(K) \) we write \( A|_{\epsilon=t} \) for the \( t \)-eigenspace of \( \epsilon \) within \( A \).

**Proposition 6.1.** If char(\( K \)) ≠ \( p \) and Gal(\( K/F \)) ≃ \( \mathbb{Z}/p^n\mathbb{Z} \), with \( n > 1 \) when \( p = 2 \), then
\[
J(K) = \langle \chi \rangle \bigoplus_{i=0}^n Y_i,
\]
where

- \( \chi \in J(K) \) is an element of nontrivial index and length \( p^{i(K/F)} + 1 \)
- \( Y_i \simeq \bigoplus_{\mathfrak{d}} \mathbb{F}_p[G_i] \), and \( Y_i \subseteq J(K)^0 \) and \( \mathfrak{d}_i = \text{codim}_{\mathbb{F}_p} \left( \frac{N_{K_{i+1}/K_i}(\hat{K}_{i+1})}{K^{x_p}} \bigg|_{\epsilon=t} \right) \cdot \left( \frac{N_{K_{i+1}/K_i}(\hat{K}_{i+1})}{K^{x_p}} \bigg|_{\epsilon=t} \right) \).

We show that the module structure for \( J(K) \) when char(\( K \)) = \( p \) shares some of these same characteristics.
Suppose that 

Proof of Theorem 1.3. 

embedding problems, we showcase this fact by giving a proof of Theorem 1.3 

where

\[
\begin{align*}
\chi & \in J(K) \text{ is an element of nontrivial index and length } 1, \text{ and} \\
Y_n & \simeq \oplus \mathcal{O}_n \mathbb{F}_p[G] \text{ and } \mathcal{O}_n = \dim_{\mathbb{F}_p} \left( \frac{\text{Tr}_{K/F}(\ell)}{\varphi(K)} \right) = \dim_{\mathbb{F}_p} \left( \frac{F}{\varphi(K)} \right)
\end{align*}
\]

Proof. The embedding problem

\[
\begin{array}{ccc}
\mathbb{Z}/p^{n+1} \mathbb{Z} & \longrightarrow & \mathbb{Z}/p^n \mathbb{Z} \\
& & \longrightarrow 1
\end{array}
\]

is central and nonsplit, and hence has a solution by [15, App. A]. Let \( \chi \in \varphi(K)^G \) be the element which generates this extension, and for convenience let \( e(\chi) = 1 \). We will show that for any \( f \in \varphi(K)^G \) and any \( 1 \leq i \leq p^n \) there exists an element \( k_i \in \varphi(K) \) and a value \( c \in \mathbb{F}_p \) such that \( f = c\chi + (\sigma - 1)^{i-1}k_i \); furthermore, when \( i < p^n \) we may also insist that \( e(k_i) = 0 \). Notice that since \((\sigma - 1)^{n-1} = \sum_{i=0}^{p^n-1} \sigma^i = Tr_{K/F}\), this result tells us that \( f = c\chi + Tr_{K/F}(k_{p^n}) \). This gives the desired result.

First, let \( f \in \varphi(K)^G \) be given. If \( e(f) = c \), then the element \( k_1 = f - c\chi \) satisfies the necessary conditions. If \( k_1 = 0 \) then let \( k_{p^n} = 0 \); otherwise suppose \( 1 < i < p^n \), and we have a nonzero element \( k_i \in \varphi(K) \) with \( e(k_i) = 0 \) and \((\sigma - 1)^{i-1}k_i = f \). This means that we have a solution to the embedding problem

\[
\begin{array}{ccc}
\mathbb{F}_p[G]/(\sigma - 1)^i \times G & \longrightarrow & G \\
& & \longrightarrow 1
\end{array}
\]

Notice that we have a short exact sequence

\[
\begin{array}{ccc}
1 & \longrightarrow & \mathbb{F}_p \simeq (\langle (\sigma - 1)^i \rangle \times 1) \\
& & \longrightarrow \mathbb{F}_p[G]/(\sigma - 1)^{i+1} \times G \\
& & \longrightarrow \mathbb{F}_p[G]/(\sigma - 1)^i \times G \\
& & \longrightarrow 1
\end{array}
\]

Since the action of \( \sigma \) is trivial on the kernel, this is a central extension. Furthermore the sequence is nonsplit because \( \mathbb{F}_p[G]/(\sigma - 1)^{i+1} \) and \( \mathbb{F}_p[G]/(\sigma - 1)^i \) each have rank 2. Again applying [15, App. A], this embedding problem has a solution, and so there is an element \( k_{i+1} \in \varphi(K) \) with \((\sigma - 1)k_{i+1} = k_i \) and either \( e(k_{i+1}) = p^n \) or \( e(k_{i+1}) = 0 \). By induction, the desired result follows.

For any field \( K \), these results show us that the possibilities for the \( \mathbb{F}_p[G] \)-module structure for \( J(K) \) are quite limited. Before going into more technical results concerning general embedding problems, we showcase this fact by giving a proof of Theorem 1.3.

Proof of Theorem 1.3. Suppose that \( K/F \) admits a solution \( L \) to the embedding problem

\[
\begin{array}{ccc}
\mathbb{F}_p[G] & \longrightarrow & G \\
& & \longrightarrow 1
\end{array}
\]

where the kernel of this embedding problem is an \( \mathbb{F}_p[G] \)-module \( A \). The module structure for \( A \) tells us that \( A \subseteq J(K) \) and \( f \text{-rk}(A) \geq k \). Choose a decomposition \( A = \oplus_{i=1}^{\text{rk}(A)} \langle \alpha_i \rangle \) such that \( \ell(\alpha_i) = p^n \) for \( 1 \leq i \leq f \text{-rk}(A) \), and pick \( \beta \in J(K) \setminus A \) of minimal length. We claim that \( \langle c_{\beta(\sigma - 1)^{\ell(\beta) - 1}} \rangle \cap \prod_{i=1}^{f \text{-rk}(A)} \langle \alpha_i(\sigma - 1)^{p^n - 1} \rangle = \{1\} \). To see this is true, suppose to the contrary that \( \beta(\sigma - 1)^{\ell(\beta) - 1} = \prod_{i=1}^{f \text{-rk}(A)} \alpha_i^{d_i(\sigma - 1)^{p^n - 1}} \) for some collection \( d_i \), not all zero.
Then \( \beta / (\prod \alpha_i^d_i(\sigma-1)p^n-\ell(\beta)) \) would be an element of length at most \( \ell(\beta) - 1 \) which is not contained in \( A \), contradicting the minimality of \( \beta \).

For a vector \( \vec{c} \in \mathbb{F}_p^{f-rk(A)} \), define \( A^{\vec{c}} = \sum_{i=1}^{f-rk(A)} \langle \alpha_i \beta c_i \rangle + \sum_{i=f-rk(A)+1}^{rk(A)} \alpha_i \). If we can show that the elements \( \{ (\alpha_i \beta c_i)^{(\sigma-1)p^n-1} \} \) are \( \mathbb{F}_p \)-independent, then we will have \( A^{\vec{c}} = \bigoplus_{i=1}^{f-rk(A)} \langle \alpha_i \beta c_i \rangle \) and \( A^{\vec{c}} \cong A \); furthermore it will be clear that \( \lambda(A^{\vec{c}}) = \lambda(A) \), and hence each of these modules will solve the embedding problem \( A \circ \lambda(A) G \longrightarrow G \longrightarrow 1 \). Since the various \( A^{\vec{c}} \) are distinct, this will mean we have at least \( p^k \) many solutions to the embedding problem, and so \( \nu(A \circ \lambda(A) G) \geq p^k \).

Now if \( \ell(\beta) < p^n \) then the collection \( \{ (\beta c_i \alpha_i)^{(\sigma-1)p^n-1} \} \cup \{ \alpha_i^{(\sigma-1)p^n-1} \} \) is the collection \( \{ \alpha_i^{(\sigma-1)p^n-1} \} \), which is certainly \( \mathbb{F}_p \)-independent. Otherwise \( \ell(\beta) = p^n \) and \( \beta^{(\sigma-1)} \in A \) by minimality, so it must be the case that \( \beta^{(\sigma-1)p^n-1} \in A \setminus A_{(p^n-1)} \); by Proposition 21, we can insist that our decomposition \( A = \bigoplus_{i=1}^{rk(A)} \langle \alpha_i \rangle \) is chosen so that \( \alpha_i \in A \) satisfies \( \ell(\alpha_i) = p^n - 1 \) and \( \beta^{(\sigma-1)p^n-1} = \alpha_i^{(\sigma-1)p^n-2} \). If we have a dependence relation

\[
1 = \prod_{i=1}^{f-rk(A)} (\beta c_i \alpha_i)^{d_i(\sigma-1)p^n-1} \prod_{i=f-rk(A)+1}^{rk(A)} \alpha_i^{d_i(\sigma-1)p^n-1} \]

then it becomes the dependence relation

\[
1 = \left( \alpha_i^{(\sigma-1)p^n-1} \right)^{\sum_{j=1}^{f-rk(A)} c_j d_j} \prod_{i=1}^{f-rk(A)} \alpha_i^{d_i(\sigma-1)p^n-1} \]

Hence each \( d_i = 0 \) when \( i \neq f-rk(A) + 1 \). This means that \( \sum_{j=1}^{f-rk(A)} c_j d_j = 0 \), and so it also follows that \( d_{f-rk(A)+1} = 0 \) as desired. \( \square \)

We now give a characterization of fields \( K/F \) which admit a solution to a given embedding problem \( A \circ \lambda \longrightarrow G \longrightarrow 1 \). We will use the notation \( \lceil i \rceil_p \) to denote \( \lceil \log_p i \rceil \), and

\[
\mathcal{D}_i(K) = \begin{cases} \dim_{\mathbb{F}_p} \left( \frac{N_{K|\ell p}(K|\ell p)}{K \times p} \right), & \text{if } \text{char}(K) \neq p \\ \dim_{\mathbb{F}_p} \left( \frac{Tr_{K|\ell p}(K|\ell p)}{p(K)} \right), & \text{if } \text{char}(K) = p. \end{cases}
\]

The computed module structures for \( J(K) \) tell us that \( \Delta(J(K|\ell)) = \mathcal{D}_i + \mathbb{1}_{i=p^{(K/F)+1}} \).

**Theorem 6.3.** The embedding problem \( M \circ \mu \longrightarrow G \longrightarrow 1 \) has a solution over \( K/F \)

if and only if the following conditions hold:

\begin{enumerate}
\item \( \Delta(M_{\ell i}) \leq \mathcal{D}_i + \mathbb{1}_{i=p^{(K/F)+1}} \cdot \mathbb{1}_{p^{(K/F)+1}=\mu} \), and
\item \( \mu \geq p^{(K/F)+1} \).
\end{enumerate}
Proof. Since the smallest length for an element with non-trivial index in \( J(K) \) is \( p^i(K/F) + 1 \), any submodule \( U \subseteq J(K) \) must have \( \lambda(U) \geq p^i(K/F) + 1 \). Hence if the second condition fails, then there is no solution to the corresponding embedding problem.

So suppose that \( \mu \geq p^i(K/F) + 1 \). Lemmas 5.5, 5.7, and 5.9 give necessary and sufficient conditions (depending on the value of \( \mu \)) for a filtration \( W = W_1 \supseteq W_2 \supseteq \cdots \supseteq W_{p^n} \supseteq W_{p^n+1} = \{1\} \) within \( J(K)^G \) to be the fixed part of a module \( U \subseteq J(K) \) with \( U \cong M \) and \( \lambda(U) = \mu \). In each case, we need both \( \Delta(W_i) = \Delta(M_{(i)}) \) and

\[
W_i \subseteq \begin{cases} \langle J(K)_{(i)} \rangle, & \text{if } i < \mu; \\ J(K)_{(i)}, & \text{if } i \geq \mu; \end{cases}
\]

in the case that \( \mu = \lambda(J(K)) = p^j(E/F) + 1 \); it must also be the case that \( W_{p^i(K/F) + 1} \not\subseteq J(K)^0_{\{p^i(K/F) + 1\}} \). Since \( \Delta(J(K)_{(i)}) = \mathcal{D}_{i} + \mathbb{1}_{i=p^j(K/F) + 1} \), and furthermore \( J(K)^0_{(i)} = J(K)_{(i)} \) when \( i \neq p^j(K/F) + 1 \) and \( \text{codim}_F(J(K)^0_{\{p^j(E/F) + 1\}} : J(K)_{\{p^j(K/F) + 1\}}) = 1 \), we can find an appropriate filtration if and only if

\[
\Delta(M_{(i)}) \leq \mathcal{D}_{(i)} + \mathbb{1}_{i=p^j(K/F) + 1} \cdot \mathbb{1}_{p^j(K/F) + 1 = \mu}.
\]

Of course, this result is simply a more general version of Theorem 6.3.

**Proof of Theorem 6.3** The first part of Theorem 6.3 follows directly from Theorem 6.1. For the second part, suppose first that \( F^x/K^x \) is infinite, and let \( U = \oplus \langle \alpha_i \rangle \subseteq J(K) \) be given so that \( U \cong M \) and \( \lambda(U) = p^n \). Then for any \( f \in F^x/K^x \setminus U \), we can create a new module \( U_f := \oplus \langle f\alpha_i \rangle \) which has \( U \cong M \) and \( \lambda(U) = p^n \). Moreover, if \( f_2 \notin \langle f_1, U \rangle \), then \( U_{f_1} \neq U_{f_2} \). Hence there are infinitely many modules in \( J(K) \) which correspond to a solution to \( M \times G \longrightarrow G \longrightarrow 1 \).

So suppose that \( F^x/K^x \) is finite. This implies that \( J(K) \) is finite as well, and so we may apply Theorem 6.6.

Note that Theorem 6.3 gives a condition for solvability in terms of the values \( \mathcal{D}_{(i)} \) for all \( 1 \leq i \leq p^n \), even though the terms \( \mathcal{D}_{\{p^i + j\}} \) are equal for all \( 1 \leq j \leq p^{k+1} - p^k \). Hence we can give the slightly more general result

**Corollary 6.4.** The embedding problem \( M \bullet \mu \longrightarrow G \longrightarrow 1 \) has a solution over \( K/F \) if and only if the following conditions hold:

1. \( \Delta(M^G) \leq \mathcal{D}_{\{1\}} + \mathbb{1}_{i=\lambda(K/F)=-\infty} \cdot \mathbb{1}_{1=\mu} \)
2. \( \Delta(M_{\{p^k + 1\}}) \leq \mathcal{D}_{\{p^k + 1\}} + \mathbb{1}_{k=\lambda(K/F)} \cdot \mathbb{1}_{p^k(K/F) + 1 = \mu} \), and
3. \( \mu \geq p^i(K/F) + 1 \).

**Proof.** The only inequality that needs to be explained is \( \Delta(M_{\{p^i(K/F) + 2\}}) \leq \mathcal{D}_{\{p^i(K/F) + 1\}} \) when \( p^i(K/F) + 1 = \mu \). The above inequality gives us

\[
\Delta(M_{\{p^i(K/F) + 1\}}) \leq \mathcal{D}_{p^i(K/F) + 1} + 1.
\]
Now if \( U \subseteq J(K) \) satisfies \( U \simeq M \) and \( \lambda(U) = \mu \), then notice there is an element \( u \in U \) with \( \ell(u) = \mu \) and \( e(u) \neq 0 \). If \( u^{(\sigma-1)^{\mu-1}} = b^{(\sigma-1)^{\mu-1}} \) for some \( b \in U^0 \), then the term \( u/b \) would have \( \ell(u/b) < \mu \) and \( e(u/b) \neq 0 \). This would contradict \( \lambda(U) = \mu \), and therefore no such \( b \) exists. In particular, it must be that \( u \not\in U \{p_i(K/F) + 2\} \). Hence \( \Delta(U(p_i(K/F) + 1)) > \Delta(U(p_i(K/F) + 2)) \), and the result follows. \( \square \)

The previous corollary will be the foundation for a very general automatic realization result. Before stating the theorem, recall the definition of \( \ell \) with \( \lambda \) would have \( \lambda \) to be the\( n \) be the generator of \( G \) and \( \ell(\alpha_j) = \lambda \) and \( e(\alpha_j) \neq 0 \). We define \([A]\) to be the \( \mathbb{F}_p[G] \)-module with generators \( \{\beta_i\} \) subject to the conditions

\[
\ell(\beta_i) = \begin{cases} p^{\lceil\ell(\alpha_i)\rceil}, & \text{if } i \neq j \\ p^{|\log_p(\ell(\alpha_i))|} + 1, & \text{if } i = j. \end{cases}
\]

(Note: if \( \ell(\alpha_j) = 1 \), then we interpret \( p^{|\log_p(\ell(\alpha_j))|} + 1 \) as 1.)

**Theorem 6.5.** The group \( A \rtimes G \) automatically realizes the group \([A]\) \times G. Furthermore, if \( 1 \leq \lambda < p^n \), or if \( \lambda = p^n \) and \( A \) contains a summand isomorphic to \( \mathbb{F}_p[G] \), then \( A \rtimes G \) automatically realizes \([A] \rtimes \mathbb{F}_p[\lambda_{n+1} + 1] \).

**Proof.** Suppose first that \( F \in \mathcal{F}(A \rtimes G) \); let \( K \) be the fixed field of the subgroup \( A \rtimes G \). In order to show that there is a solution to the embedding problem \([A] \rtimes G \) over \( K/F \), Corollary 6.4 tells us that we must show that \( \Delta([A]_{(1)}) \leq \mathcal{D}_{(1)} \) and, for \( 0 \leq k \leq n-1 \), that \( \Delta([A]_{(p^{k+1})}) \leq \mathcal{D}_{(p^{k+1})} \). Now

\[
\Delta([A]_{(1)}) = \Delta([A]^G) = \Delta(A^G) = \Delta(A_{(1)}),
\]

and \( \Delta(A_{(1)}) \leq \mathcal{D}_{(1)} \) by Corollary 6.4 since \( A \rtimes G \) is solvable. For the second condition, notice that

\[
\Delta([A]_{(p^{k+1})}) = \Delta(A_{(p^{k+1})}) \leq \mathcal{D}_{(p^{k+1})},
\]

where the last inequality follows using Corollary 6.4 since \( A \rtimes G \) is solvable.

Now suppose that \( F \in \mathcal{F}(A \rtimes G) \); as before, let \( K \) be the fixed field of the subgroup generated by \( A \). By Corollary 6.4, we need to show that

1. \( \Delta([A]^G) \leq \mathcal{D}_{(1)} + \mathbb{I}_{i(K/F) = -\infty} \cdot \mathbb{I}_{1 = p^{|\log_p(\lambda-1)|} + 1} \)
2. \( \Delta([A]_{(p^{k+1})}) \leq \mathcal{D}_{(p^{k+1})} + \mathbb{I}_{k = i(K/F) \cdot p^{|(p(K/F) + 1) = p^{|\log_p(\lambda-1)|} + 1}} \)
3. \( p^{|\log_p(\lambda-1)|} + 1 \geq p^{|i(K/F)| + 1} \)

Now since \( A \rtimes G \) is realizable over \( K/F \) we know that \( \Delta(A^G) \leq \mathcal{D}_1 + \mathbb{I}_{i(K/F) = -\infty} \cdot \mathbb{I}_{1 = \lambda} \); since \( \Delta(A^G) = \Delta([A]^G) = \text{rk}(A) \) and \( \mathbb{I}_{1 = \lambda} = \mathbb{I}_{1 = p^{|\log_p(\lambda-1)|} + 1} \), the first property holds. For the second, note that \( \Delta([A]_{(p^{k+1})}) = \Delta(A_{(p^{k+1})}) \), and since \( A \rtimes G \) is solvable over \( K/F \) we have

\[
\Delta(A_{(p^{k+1})}) \leq \mathcal{D}_{p^{k+1}} + \mathbb{I}_{k = i(K/F) \cdot p^{|(p(K/F) + 1) = p^{|\log_p(\lambda-1)|} + 1}}.
\]

Finally, again using the solvability of \( A \rtimes G \) over \( K/F \), we have \( \lambda \geq p^{|i(K/F)| + 1} + 1 \). If \( \lambda = 1 \) then \( p^{|\log_p(\lambda-1)|} + 1 = 1 \geq p^{|i(K/F)| + 1} + 1 \). Otherwise write \( \lambda = p^k + j \) with \( 1 \leq j \leq p^{k+1} - p^k \).
Then
\[ k = \left\lfloor \log_p(\lambda - 1) \right\rfloor \geq \left\lfloor \log_p(p^{i(K/F)} + 1 - 1) \right\rfloor = i(K/F), \]
and so \( p^k + 1 \geq p^{i(K/F)} + 1 \). The third desired inequality therefore holds.

\[ \Box \]

The results we have presented here are certainly not the only conclusions one can draw, but give an indication of the results one can draw from the parameterization from Theorem 4.4 together with the computed module structures in Propositions 6.1 and 6.2.

References

[1] J. Berg, A. Schultz. \( p \)-groups have unbounded realization multiplicity. Preprint.
[2] Z. I. Borevič. The multiplicative group of cyclic \( p \)-extensions of a local field. Trudy Mat. Inst. Steklov 80 (1965) 16–29. English translation, Proc. Steklov Inst. Math. No. 80 (1965): Algebraic number theory and representations (ed D. K. Fadeev) (American Mathematical Society, Providence, RI, 1968), 15–30.
[3] G. Brattström. On \( p \)-groups as Galois groups. Math. Scandinavica 65 (1989), no. 2, 165–174.
[4] P. Damey, J. Martinet. Plongement d’une extension quadratique dans une extension quaternionienne. J. Reine Angew. Math. 262/263 (1973), 323–338.
[5] P. Damey, J.-J. Payan. Existance et construction des extensions Galoisiennes et non-abéliennes de degré 8 d’un corps de caractéristique différente de 2. J. Reine Angew. Math. 244 (1970), 37–54.
[6] R. Dedekind. Konstruktion von Quaternionkörpern. Gasammelte Mathematische Werke, Band 2, Vieweg, Braunschweig, 1931, 376–384.
[7] D. K. Fadeev. On the structure of the reduced multiplicative group of a cyclic extension of a local field. Izv. Akad. Nauk SSSR Ser. Math. 24 (1960), 145–152.
[8] H. Grundman, T. Smith. Automatic realizability of Galois groups of order 16. Proc. Amer. Math. Soc. 124 (1996), 2631–2640.
[9] H. Grundman, T. Smith. Realizability and automatic realizability of Galois groups of order 32. Cent. Eur. J. Math. 8 (2010), no. 2, 244–260.
[10] H. Grundman, T. Smith. Galois realizability of groups of order 64. Cent. Eur. J. Math. 8 (2010), no. 5, 846–854.
[11] H. Grundman, T. Smith, J. Swallow. Groups of order 16 as Galois groups. Expo. Math. 13 (1995), 289–319.
[12] C. U. Jensen, On the representations of a group as a Galois group over an arbitrary field. Théorie des nombres (Quebec, PQ, 1987), 441–458. Berlin: de Gruyter, 1989.
[13] C. U. Jensen. Finite groups as Galois groups over arbitrary fields. Proceedings of the International Conference on Algebra, Part 2 (Novosibirsk, 1989), 435–448. Contemp. Math. 131, Part 2. Providence, RI: American Mathematical Society, 1992.
[14] C. U. Jensen. Elementary questions in Galois theory. Advances in algebra and model theory (Essen, 1994; Dresden, 1995), 11–24. Algebra Logic Appl. 9. Amsterdam: Gordon and Breach, 1997.
[15] C. U. Jensen, A. Ledet, N. Yui. Generic polynomials: constructive aspects of the inverse Galois problem. Mathematical Sciences Research Institute Publications 45. Cambridge: Cambridge University Press, 2002.
[16] C. U. Jensen, A. Prestel. Unique realizability of finite abelian 2-groups as Galois groups. J. Number Theory 40 (1992), no. 1, 12–31.
[17] C. U. Jensen, A. Prestel. How often can a finite group be realized as a Galois group over a field? Manuscripta Math. 99 (1999), 223–247.
[18] A. Ledet. On 2-groups as Galois groups. Canad. J. Math. 47 (1995), no. 6, 1253–1273.
[19] R. Massy, T. Nguyen-Quang-Do. Plongement d’une extension de degré \( p^2 \) dans une surextension non abélienne de degré \( p^3 \): étude locale-globale. J. Reine Angew. Math. 291(1977), 149–161.
[20] I. Michailov. Four non-abelian groups of order \( p^4 \) as Galois groups. J. Alg. 307 (2007), 287–299.
[21] I. Michailov. Groups of order 32 as Galois groups. Serdica Math. J. 33 (2007), no. 1, 1–34.
[22] I. Michailov. Induced orthogonal representations of Galois groups. J. Alg. 322 (2009), 3713–3732.
[23] I. Michailov. On Galois cohomology and realizability of 2-groups as Galois groups. *Cent. Eur. J. Math.* 9 (2011), no. 2, 403–419.

[24] I. Michailov. On Galois cohomology and realizability of 2-groups as Galois groups II. *Cent. Eur. J. Math.* 9 (2011), no. 6, 1333–1343.

[25] J. Mináč, J. Swallow, Galois module structure of $p$th-power classes of extensions of degree $p$. Israel J. Math. 138 (2003), 29–42.

[26] J. Mináč, J. Swallow, Galois embedding problems with cyclic quotient of order $p$. Israel J. Math. 145 (2005), 93–112.

[27] J. Mináč, A. Schultz, J. Swallow, Galois module structure of the $p$th-power classes of cyclic extensions of degree $p^n$. Proc. London Math. Soc. 92 (2006), no. 2, 307–341.

[28] J. Mináč, A. Schultz, J. Swallow. Automatic realizations of Galois groups with cyclic quotient of order $p^n$. *J. Théor. Nombres Bordeaux* 20 (2008), 419–430.

[29] V. Shirbisheh. Galois embedding problems with abelian kernels of exponent $p$. VDM Verlag, 2009.

[30] J. Swallow. Central $p$-extensions of $(p, p, \cdots, p)$-type Galois groups. *J. Alg.* 186 (1996), 277–298.

[31] W. Waterhouse, The normal closures of certain Kummer extensions. Canad. Math. Bull. 37 (1994), no. 1, 133–139.

[32] G. Whaples, Algebraic extensions of arbitrary fields. *Duke Math. J.* 24 (1957), 201–204.

[33] E. Witt. Konstruktion von galoisschen Körpern der Charakteristik $p$ zu vorgegebener Gruppe der Ordnung $p^f$. *J. Reine Angew. Math.* 174 (1936), 237–245.