Ján MINÁČ, Andrew SCHULTZ et John SWALLOW

Automatic realizations of Galois groups with cyclic quotient of order $p^n$

<http://jtnb.cedram.org/item?id=JTNB_2008__20_2_419_0>
Automatic realizations of Galois groups with cyclic quotient of order $p^n$

par Ján MINÁČ, Andrew SCHULTZ et John SWALLOW


Abstract. We establish automatic realizations of Galois groups among groups $M \rtimes G$, where $G$ is a cyclic group of order $p^n$ for a prime $p$ and $M$ is a quotient of the group ring $\mathbb{F}_p[G]$.

1. Introduction

The fundamental problem in inverse Galois theory is to determine, for a given field $F$ and a given profinite group $G$, whether there exists a Galois extension $K/F$ such that $\text{Gal}(K/F)$ is isomorphic to $G$. A natural sort of reduction theorem for this problem takes the form of a pair $(A, B)$ of profinite groups with the property that, for all fields $F$, the existence of $A$ as a Galois group over $F$ implies the existence of $B$ as a Galois group over $F$. We call such a pair an automatic realization of Galois groups and denote it $A \Rightarrow B$. The trivial automatic realizations are those given by quotients of Galois groups; by Galois theory, if $G$ is realizable over $F$ then so is every quotient $H$. It is a nontrivial fact, however, that there exist nontrivial automatic realizations. (See [4, 5, 6] for a good overview of the theory of automatic realizations. Some interesting automatic realizations of groups of order 16 are obtained in [2], and these and other automatic realizations of finite 2-groups are collected in [3]. For comprehensive treatments of related Galois embedding problems, see [7] and [9].)

The usual techniques for obtaining automatic realizations of Galois groups involve an analysis of Galois embedding problems. In this paper we offer a new approach based on the structure of natural Galois modules: we use equivariant Kummer theory to reformulate realization problems in terms of Galois modules, and then we solve Galois module problems. We
take this approach in proving Theorem 1.1, which establishes automatic realizations for a useful family of finite metacyclic $p$-groups. Our methods extend those of [10], [11] and [12]. It is interesting to observe that, although not visible here, the essential fact underpinning our results is Hilbert 90. Indeed, the structural results in [12] rely crucially on the repeated application of Hilbert 90, using combinatorial and Galois-theoretic arguments to draw out the consequences.

Let $p$ be a prime, $n \in \mathbb{N}$, and $G$ a cyclic group of order $p^n$ with generator $\sigma$. For the group ring $\mathbb{F}_p[G]$, there exist precisely $p^n$ nonzero ring quotients, namely $M_j := \mathbb{F}_p[G]/(\sigma - 1)^j$ for $j = 1, 2, \ldots, p^n$. Multiplication in $\mathbb{F}_p[G]$ induces an $\mathbb{F}_p[G]$-action on each $M_j$. In particular, each $M_j$ is a $G$-module. Let $M_j \rtimes G$ denote the semidirect product.

Theorem 1.1. We have the following automatic realizations of Galois groups:

$$M_{p^i+c} \rtimes G \implies M_{p^{i+1}} \rtimes G, \quad 0 \leq i < n, \quad 1 \leq c < p^{i+1} - p^i.$$

In Section 2 we recall some facts about the set of quotients $M_j$ and the semidirect products $M_j \rtimes G$. In Sections 3 through 5 we consider the case $\text{char } F \neq p$. Following Waterhouse [15], we recall in Section 3 a generalized Kummer correspondence over $K$, where $K$ is a cyclic extension of $F$ of degree $p^n$, and in Section 4 we establish a proposition detecting when such extensions are Galois over $F$. In Section 5 we decompose $J_\epsilon$, the crucial Kummer submodule of the module $K(\xi_p)^{x}/K(\xi_p)^{xp}$, as an $\mathbb{F}_p[\text{Gal}(K(\xi_p)/F(\xi_p))]$-module, where $\xi_p$ is a primitive $p$th root of unity. In Section 6 we prove Theorem 1.1, using Sections 3 through 5 in the case $\text{char } F \neq p$ and Witt’s Theorem in the case $\text{char } F = p$. The case $i = 0$ was previously considered by two of the authors [11, Theorem 1(A)].

2. Groups and $\mathbb{F}_p[G]$-modules

Let $p$ be a prime and $G = \langle \sigma \rangle$ an abstract group of order $p^n$. We recall some facts concerning $R$-modules, where $R$ is the group ring $\mathbb{F}_p[G]$. Because we frequently view $R$ as a module over $R$, to prevent confusion we write the module $R$ as

$$R = \bigoplus_{j=0}^{p^n-1} \mathbb{F}_p \tau^j,$$

where $\sigma$ acts by multiplication by $\tau$. For convenience we set $\rho := \sigma - 1$.

The set of nonzero cyclic $R$-modules is identical to the set of nonzero indecomposable $R$-modules, and these are precisely the $p^n$ quotients $M_j := R/(\tau - 1)^j$, $1 \leq j \leq p^n$. Each $M_j$ is a local ring, with unique maximal ideal $\rho M_j$, and is annihilated by $\rho^j$ but not $\rho^{j-1}$.

Moreover, for each $j$ there exists a $G$-equivariant isomorphism from $M_j$ to its dual $M_j^*$, as follows. For each $i \in \{1, \ldots, p^n\}$ we choose the $\mathbb{F}_p$-basis...
of $M_j$ consisting of the images of $\{1, (\tau - 1), \ldots, (\tau - 1)^{j-1}\}$ and define an $\mathbb{F}_p$-linear map $\lambda : M_j \rightarrow \mathbb{F}_p$ by

$$\lambda \left( f_0 + f_1(\tau - 1) + \cdots + f_{j-1}(\tau - 1)^{j-1} \right) = f_{j-1},$$

where $f_k \in \mathbb{F}_p$, $k = 0, \ldots, j - 1$. Observe that $\ker \lambda$ contains no nonzero ideal of $M_j$. Then

$$Q : M_j \times M_j \rightarrow \mathbb{F}_p, \quad Q(a, b) := \lambda(ab), \ a, b \in M_j$$

is a nonsingular symmetric bilinear form. Thus $M_j$ is a symmetric algebra. (See [8, page 442].) Moreover, $Q$ induces a $G$-equivariant isomorphism $\psi : M_j \rightarrow M_j^*$ given by $(\psi(a))(b) = Q(a, b), \ a, b \in M_j$.

**Remark.** In order for $\psi$ to be $G$-equivariant, we must define the action on $M_j^*$ by $\sigma f(m) = f(\sigma m)$ for all $m \in M_j$, and since $G$ is commutative, this action is well-defined. It is worthwhile to observe, however, that $M_j^*$ is $\mathbb{F}_p[G]$-isomorphic to the module $\bar{M}_j^*$ on which the action of $G$ is defined by $\sigma f(m) = f(\sigma^{-1}m)$ for all $m \in M_j$. Indeed by the $G$-equivariant isomorphism between $M_j$ and $M_j^*$ it is sufficient to show that the $\mathbb{F}_p[G]$-module $\bar{M}_j$ obtained from $M_j$ by twisting the action of $G$ via the automorphism $\sigma \rightarrow \sigma^{-1}$ is naturally isomorphic to $M_j$. But this follows readily by extending the automorphism $\sigma \rightarrow \sigma^{-1}$ to the automorphism of the group ring $\mathbb{F}_p[G]$ and then inducing the required $\mathbb{F}_p[G]$-isomorphism between $M_j$ and $M_j^*$.

We also recall some facts about the semidirect products $H_j := M_j \rtimes G$, $j = 1, \ldots, n$. For each $j$, the group $H_j$ has order $p^{j+n}$; exponent $p^n$, except when $j = p^n$, in which case the exponent is $p^{n+1}$; nilpotent index $j$; rank (the smallest number of generators) 2; and Frattini subgroup $\Phi(H_j) = (\rho M_j) \rtimes G$. Finally, for $j < k$, $H_j$ is a quotient of $H_k$ by the normal subgroup $\rho^j M_k \rtimes 1$.

### 3. Kummer theory with operators

For Sections 3 through 5 we adopt the following hypotheses. Suppose that $G = \text{Gal}(K/F) = \langle \sigma \rangle$ for an extension $K/F$ of fields of characteristic not $p$. For any element $\tau \in G$ we denote the fixed subfield of $\tau$ as $\text{Fix}_K(\tau)$. We let $\xi_p$ be a primitive $p$th root of unity and set $\tilde{F} := F(\xi_p)$, $\hat{K} := K(\xi_p)$, and $J := \hat{K}^\times/\hat{K}^{\times p}$, where $\hat{K}^\times$ denotes the multiplicative group $\hat{K} \setminus \{0\}$. We write the elements of $J$ as $[\gamma]$, $\gamma \in \hat{K}^\times$, and we write the elements of $\tilde{F}^\times/\tilde{F}^{\times p}$ as $[\gamma]_p$, $\gamma \in \tilde{F}^\times$. We moreover let $\epsilon$ denote a generator of $\text{Gal}(\tilde{F}/F)$ and set $s = [\hat{F} : F]$. Since $p$ and $s$ are relatively prime, $\text{Gal}(\hat{K}/F) \simeq \text{Gal}(\tilde{F}/F) \times \text{Gal}(K/F)$. Therefore we may naturally extend $\epsilon$ and $\sigma$ to $\hat{K}$, and the two automorphisms commute in $\text{Gal}(\hat{K}/F)$.
Using the extension of $\sigma$ to $\hat{K}$, we write $G$ for $\text{Gal}(\hat{K}/\hat{F})$ as well. Then $J$ is an $\mathbb{F}_p[G]$-module. Finally, we let $t \in \mathbb{Z}$ such that $\epsilon(\xi_p) = \xi_p^t$. Then $t$ is relatively prime to $p$, and we let $J_\epsilon$ be the $t$-eigenspace of $J$ under the action of $\epsilon$: $J_\epsilon = \{ [\gamma] : \epsilon[\gamma] = [\gamma]^t \}$. 

Observe that since $\epsilon$ and $\sigma$ commute, $J_\epsilon$ is an $\mathbb{F}_p[G]$-subspace of $J$. By [15, §5, Proposition], we have a Kummer correspondence over $K$ of finite subspaces $M$ of the $\mathbb{F}_p$-vector space $J_\epsilon$ and finite abelian exponent $p$ extensions $L$ of $K$:

$$M = ((\hat{K}L)^{\times p} \cap \hat{K}^{\times})/\hat{K}^{\times p} \leftrightarrow L = L_M = \text{maximal } p\text{-extension of } K \text{ in } \hat{L}_M := \hat{K}(\sqrt[p]{\gamma} : [\gamma] \in M).$$

As Waterhouse shows, for $M \subset J_\epsilon$, the automorphism $\epsilon \in \text{Gal}(\hat{K}/K)$ has a unique lift $\tilde{\epsilon}$ to $\text{Gal}(\hat{L}_M/K)$ of order $s$, and $L_M$ is the fixed field of $\tilde{\epsilon}$.

In the next proposition we provide some information about the corresponding Galois modules when $L_M/F$ is Galois. Recall that in the situation above, the Galois groups $\text{Gal}(L_M/K)$ and $\text{Gal}(\hat{L}_M/\hat{K})$ are naturally $G$-modules under the action induced by conjugations of lifts of the elements in $G$ to $\text{Gal}(L_M/F)$ and $\text{Gal}(\hat{L}_M/\hat{F})$. Furthermore, because the Galois groups $\text{Gal}(L_M/K)$ and $\text{Gal}(\hat{L}_M/\hat{K})$ have exponents dividing $p$, we see that $\text{Gal}(L_M/K)$ and $\text{Gal}(\hat{L}_M/\hat{K})$ are in fact $\mathbb{F}_p[G]$-modules.

**Proposition 3.1.** Suppose that $M$ is a finite $\mathbb{F}_p$-subspace of $J_\epsilon$. Then

1. $L_M$ is Galois over $F$ if and only if $M$ is an $\mathbb{F}_p[G]$-submodule of $J_\epsilon$.
2. If $L_M/F$ is Galois, then base extension $F \to \hat{F}$ induces a natural isomorphism $\text{Gal}(L_M/F) \simeq \text{Gal}(\hat{L}_M/\hat{F})$ compatible with our isomorphism $\text{Gal}(\hat{K}/\hat{F}) \simeq \text{Gal}(K/F) \simeq G$ under the restriction map.
3. If $L_M/F$ is Galois, then as $G$-modules,

$$\text{Gal}(L_M/K) \simeq \text{Gal}(\hat{L}_M/\hat{K}) \simeq M.$$

**Proof.** (1). Suppose first that $L_M/F$ is Galois. Then $\hat{L}_M = L\hat{K}/\hat{F}$ is Galois as well. Every automorphism of $\hat{K}$ extends to an automorphism of $\hat{L}_M$, and therefore $M$ is an $\mathbb{F}_p[G]$-submodule of $J_\epsilon$. From [15, §5, Proposition] we see that $M$ is an $\mathbb{F}_p[G]$-submodule of $J_\epsilon$.

Going the other way, suppose that $M$ is a finite $\mathbb{F}_p[G]$-submodule of $J_\epsilon$. By the correspondence above, $L_M/K$ is Galois. Then $M$ is also an $\mathbb{F}_p[\text{Gal}(\hat{K}/F)]$-submodule of $J_\epsilon$ and therefore $\hat{L}_M/F$ is Galois. Now since $\hat{K}/F$ is Galois, every automorphism of $\hat{L}_M$ sends $K$ to $K$. Moreover, since $L_M$ is the unique maximal $p$-extension of $K$ in $\hat{L}_M$, every automorphism of $\hat{L}_M$ sends $L_M$ to $L_M$. Therefore $L_M/F$ is Galois.

(2). Suppose $L_M/F$ is Galois. Since $\hat{F}/F$ and $L_M/F$ are of relatively prime degrees, we have $\text{Gal}(L_M\hat{F}/F) \simeq \text{Gal}(\hat{F}/F) \times \text{Gal}(L_M/F)$. Therefore
we have a natural isomorphism $G = \text{Gal}(K/F) \simeq \text{Gal}(\hat{K}/\hat{F})$, which is compatible with the natural isomorphism $\text{Gal}(\hat{L}_M/\hat{F}) \simeq \text{Gal}(L_M/F)$ under the usual restriction maps provided by Galois theory.

(3). Suppose $L_M/F$ is Galois. By (2), it is enough to show that $\text{Gal}(\hat{L}_M/\hat{K}) \simeq M$ as $G$-modules. Under the standard Kummer correspondence over $\hat{K}$, finite subspaces of the $\mathbb{F}_p$-vector space $J$ correspond to finite abelian exponent $p$ extensions $\hat{L}_M$ of $\hat{K}$, and $M$ and $\text{Gal}(\hat{L}_M/\hat{K})$ are dual $G$-modules under a $G$-equivariant canonical duality $\langle m, g \rangle = g(\sqrt[p]{m})/\sqrt[p]{m}$. (See [15, pages 134 and 135] and [11, §2.3].) Because $M$ is finite, $M$ decomposes into a direct sum of indecomposable $\mathbb{F}_p[G]$-modules. From Section 2, all indecomposable $\mathbb{F}_p[G]$-modules are $G$-equivariant self-dual modules. Hence there is a $G$-equivariant isomorphism between $M$ and its dual $M^*$, and $\text{Gal}(\hat{L}_M/\hat{F}) \simeq M$ as $G$-modules. \hfill \Box

4. The index

We keep the same assumptions given at the beginning of Section 3. Set $A := \operatorname{ann}_J \rho^{p^n-1} = \{[\gamma] \in J : \rho^{p^n-1}[\gamma] = [1]\}$. The following homomorphism appears in a somewhat different form in [15, Theorem 3]:

**Definition.** The index $e(\gamma) \in \mathbb{F}_p$ for $[\gamma] \in A$ is defined by

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

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

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

in $\mathbb{F}_p[G]$, $[N_{\hat{K}/\hat{F}}(\gamma)] = [\gamma]^{\rho^{p^n-1}}$, which is the trivial class $[1]$ by the assumption $[\gamma] \in A$. As a result, $\sqrt[p]{N_{\hat{K}/\hat{F}}(\gamma)}$ lies in $\hat{K}$ and is acted upon by $\sigma$ and therefore $\rho$. Observe that $e(\gamma)$ depends neither on the representative $\gamma$ of $[\gamma]$ nor on the particular $p$th root of $N_{\hat{K}/\hat{F}}(\gamma)$.

The index function $e$ is a group homomorphism from $A$ to $\mathbb{F}_p$. Therefore the restriction of $e$ to any submodule of $A$ is either trivial or surjective. Moreover, the index is trivial for any $[\gamma]$ in the image of $\rho$:

$$\xi_p(e(\gamma)) = \sqrt[p]{N_{\hat{K}/\hat{F}}(\gamma)^\rho} = \sqrt[p]{1} = 1,$$

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

Following Waterhouse, we show how the index function permits the determination of $\text{Gal}(\hat{L}_M/\hat{F})$ as a $G$-extension.

For $1 \leq j \leq p^n$ and $e \in \mathbb{F}_p$, write $H_{j,e}$ for the group extension of $M_j$ by $G$ with $\bar{\sigma}^{p^n} = e(\tau - 1)^{j-1}$, where $\bar{\sigma}$ is a lift of $\sigma$. Observe that $H_{j,0} = H_j = M_j \rtimes G$.

Let $N_\gamma$ denote the cyclic $\mathbb{F}_p[G]$-submodule of $J$ generated by $[\gamma]$. 


Proposition 4.1. (See [15, Theorem 2].) Let $[\gamma] \in J_\epsilon$ and $M = N_\gamma$.

(1) If $M \simeq M_j$ for $1 \leq j < p^n$ and $e = e(\gamma)$, then $\mathrm{Gal}(L_M/F) \simeq H_{j,e}$ as $G$-extensions.

(2) If $M \simeq \mathbb{F}_p[G]$ then $\mathrm{Gal}(L_M/F) \simeq \mathbb{F}_p[G] \rtimes G$.

Before presenting the proof, we note that if $M \simeq M_j$ for $1 \leq j < p^n$ then we have

$$\rho^{p^n-1}[\gamma] = \rho^{p^n-1-j}(\rho^j[\gamma]) = \rho^{p^n-1-j}[1] = [1].$$

Hence $[\gamma] \in A$, and so $e(\gamma)$ is defined. Furthermore, Waterhouse tells us in this case that if $e \neq 0$, then $H_{j,e} \neq H_j$ (see [15, Theorem 2]). He also shows that if $j = p^n$ then there is a $G$-extension isomorphism $H_{p^n,e} \simeq H_{p^n}$ for every $e$. In particular, we may use Proposition 4.1 later to deduce that if $M \simeq M_j$ for $j < p^n$ and $\mathrm{Gal}(L_M/F) \simeq M_j \rtimes G$, then $e(\gamma) = 0$.

Proof. Suppose $M \simeq M_j$ for $1 \leq j \leq p^n$. By Proposition 3.1(3), $\mathrm{Gal}(L_M/K) \simeq M_j$ as $G$-modules. Hence $\mathrm{Gal}(L_M/F) \simeq H_{j,e}$ for some $e$. If $j = p^n$ then from the isomorphism $H_{p^n,e} \simeq H_{p^n}$ above we have the second item. By Proposition 3.1(2), it remains only to show that if $j < p^n$, $\mathrm{Gal}(\hat{L}_M/F) \simeq H_{j,e(\gamma)}$.

Let $\hat{\sigma}$ denote a pullback of $\sigma \in G$ to $\mathrm{Gal}(\hat{L}_M/F)$. Then $\hat{\sigma}p^n$ lies in $Z(\mathrm{Gal}(\hat{L}_M/F)) \cap \mathrm{Gal}(\hat{L}_M/\hat{K})$, where $Z(\mathrm{Gal}(\hat{L}_M/F))$ denotes the center of $\mathrm{Gal}(\hat{L}_M/F)$. Using the $G$-equivariant Kummer pairing

$$\langle \cdot, \cdot \rangle : \mathrm{Gal}(\hat{L}_M/\hat{K}) \times M \to \langle \xi_p \rangle \simeq \mathbb{F}_p$$

we see that $Z(\mathrm{Gal}(\hat{L}_M/\hat{K}))$ annihilates $\rho M$. Furthermore, since this pairing is nonsingular we deduce that $Z(\mathrm{Gal}(\hat{L}_M/\hat{K})) \simeq M/\rho M$ and we can choose a generator $\eta$ of $Z(\mathrm{Gal}(\hat{L}_M/\hat{K}))$ such that

$$\langle \eta, [\gamma] \rangle = \eta(\sqrt[p^n]{\gamma})/\sqrt[p^n]{\gamma} = \xi_p.$$

In particular, if $\hat{\sigma}p^n = \eta^e$ then

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

Therefore

$$\sqrt[p^n]{\gamma}^{(\hat{\sigma}p^n-1)} = \sqrt[p^n]{\gamma}^{(1 + \hat{\sigma} + \ldots + \hat{\sigma}p^n-1) - 1} = \left(\sqrt[p^n]{N_{\hat{K}/F}(\gamma)}\right)^{\rho} = \xi_p^{e(\gamma)}.$$

5. The $\mathbb{F}_p[G]$-module $J_\epsilon$

Again we keep the same assumptions given at the beginning of Section 3. In this section we develop the crucial technical results needed for Theorem 1.1: a decomposition of the $\mathbb{F}_p[G]$-module $J_\epsilon$ into cyclic direct summands, and a determination of the value of the index function $e$ on certain of the summands.
We first show that $J_\epsilon$ is indeed a summand of $J$. Then we combine a decomposition of $J$ into indecomposables, taken from [12, Theorem 2], with uniqueness of decompositions into indecomposables, to achieve important restrictions on the possible summands of $J_\epsilon$. Much of the remainder of the proof is devoted to establishing that we have an “exceptional summand” of dimension $p^r + 1$ on which the index function is nontrivial. In the argument we need [12, Proposition 7] in particular to derive a lower bound for the dimension of that summand.

**Theorem 5.1.** Suppose that $p > 2$ or $n > 1$. The $\mathbb{F}_p[G]$-module $J_\epsilon$ decomposes into a direct sum $J_\epsilon = U \oplus_{\alpha \in A} V_\alpha$, with $A$ possibly empty, with the following properties:

1. For each $\alpha \in A$ there exists $i \in \{0, \ldots, n\}$ such that $V_\alpha \simeq M_{p^i}$.
2. $U \simeq M_{p^{r+1}}$ for some $r \in \{-\infty, 0, 1, \ldots, n - 1\}$.
3. $e(U) = \mathbb{F}_p$.
4. If $V_\alpha \simeq M_{p^i}$ for $0 \leq i \leq r$, then $e(V_\alpha) = \{0\}$.

Here we observe the convention that $p^{-\infty} = 0$.

**Proof.** We show first that $J_\epsilon$ is a direct summand of $J$ by adapting an approach to descent from [13, page 258]. Recall that $[\hat{F} : F] = s$ and $\epsilon(\xi_p) = \xi_p^t$. Thus $s$ and $t$ are both relatively prime to $p$. Let $z \in \mathbb{Z}$ satisfy $zt^{s-1} \equiv 1 \pmod{p}$, and set

$$T = z \cdot \sum_{i=1}^{s} t^{s-i} e_{i-1} \in \mathbb{Z}[\text{Gal}(\hat{K}/F)].$$

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

We claim that $e((I - T)A) = \{0\}$. Since $\xi_p \in \hat{F}$, the fixed field $\text{Fix}_{\hat{K}}(\sigma^p)$ may be written $\hat{F}(\sqrt[p]{a})$ for a suitable $a \in \hat{F}^\times$. By [15, §5, Proposition], $e([a]_{\hat{F}}) = [a]_{\hat{F}}^t$. Suppose $\gamma \in \hat{K}^\times$ satisfies $[\gamma] \in A$. Then, since $\epsilon$ and $\sigma$ commute,

$$[N_{\hat{K}/\hat{F}}(\epsilon(\gamma))]_{\hat{F}} = [\epsilon(N_{\hat{K}/\hat{F}}(\gamma))]_{\hat{F}} = \epsilon([N_{\hat{K}/\hat{F}}(\gamma)]_{\hat{F}}) = [N_{\hat{K}/\hat{F}}(\gamma)]^t_{\hat{F}}.$$

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

Now since $\mathbb{F}_p[G]$ is an Artinian principal ideal ring, every $\mathbb{F}_p[G]$-module decomposes into a direct sum of cyclic $\mathbb{F}_p[G]$-modules [14, Theorem 6.7]. Since cyclic $\mathbb{F}_p[G]$-modules are indecomposable, we have a decomposition of $J = J_\epsilon \oplus J_\nu$ as a direct sum of indecomposables. From Section 2 we know that each of these indecomposable modules are self-dual and local,
and therefore they have local endomorphism rings. By the Krull-Schmidt-Azumaya Theorem (see [1, Theorem 12.6]), all decompositions of $J$ into indecomposables are equivalent. (In our special case one can check this fact directly.)

On the other hand, we know by [12] several properties of $J$, including its decomposition as a direct sum of indecomposable $\mathbb{F}_p[G]$-modules, as follows. By [12, Theorem 2],

$$J = X \oplus \bigoplus_{i=0}^{n} Y_i,$$

where each $Y_i$ is a direct sum, possibly zero, of $\mathbb{F}_p[G]$-modules isomorphic to $M_{p^i}$, and $X = N_\chi$ for some $\chi \in \hat{K}^\times$ such that $N_{\hat{K}/\hat{F}}(\chi) \in a^w \hat{F}^{\times p}$ for some $w$ relatively prime to $p$. Moreover, $X \simeq M_{p^{r+1}}$ for some $r \in \{-\infty, 0, \ldots, n-1\}$. We deduce that $e(\chi) \neq 0$ and that $e$ is surjective on $X$. Furthermore, considering each $Y_i$ as a direct sum of indecomposable modules $M_{p^i}$, we have a decomposition of $J$ into a direct sum of indecomposable modules.

We deduce that every indecomposable $\mathbb{F}_p[G]$-submodule appearing as a direct summand in $J_\epsilon$ is isomorphic to $M_{p^i}$ for some $i \in \{0, \ldots, n\}$, except possibly for one summand isomorphic to $M_{p^{r+1}}$. Moreover, we find that $e$ is nontrivial on $J_\epsilon$, as follows. From the hypothesis that either $p > 2$ or $n > 1$ we deduce that $p^r + 1 < p^n$. Therefore since $N_\chi \simeq M_{p^{r+1}}$ we have $[\chi] \in A$. Let $\theta, \omega \in \hat{K}^\times$ satisfy $[\theta] = T[\chi] \in J_\epsilon$ and $[\omega] = (I - T)[\chi]$. From $e((I - T)A) = \{0\}$ we obtain $e(\omega) = 0$. Therefore $e(\theta) \neq 0$. Observe that $\rho e(p^{r+1} \theta) = [1]$.

We next claim that $e$ is trivial on any $\mathbb{F}_p[G]$-submodule $M$ of $J_\epsilon$ such that $M \simeq M_j$ for $j < p^r + 1$. Suppose not: $M$ is an $\mathbb{F}_p[G]$-submodule of $J_\epsilon$ isomorphic to $M_j$ for some $j < p^r + 1$ and $e(M) \neq \{0\}$. Then $M = N_\gamma$ for some $\gamma \in \hat{K}^\times$. Since $e$ is an $\mathbb{F}_p[G]$-homomorphism and $M$ is generated by $[\gamma]$, we have $e(\gamma) \neq 0$. But [12, Proposition 7 and Theorem 2] tells us that $c = p^r + 1$ is the minimal value of $c$ such that $\rho^c[\beta] = [1]$ for $\beta \in \hat{K}$ with $N_{\hat{K}/\hat{F}}(\beta) \not\in \hat{F}^{\times p}$. Hence we have a contradiction.

Because $J_\epsilon$ decomposes into a direct sum of cyclic $\mathbb{F}_p[G]$-modules, we may write $\theta$ as an $\mathbb{F}_p[G]$-linear combination of generators of such $\mathbb{F}_p[G]$-modules, and we will use this combination and the fact that $e(\theta) \neq 0$ to prove that there exists a summand isomorphic to $M_{p^{r+1}}$ on which $e$ is nontrivial. Let $M = N_\delta$ be an arbitrary summand of $J_\epsilon$. Then $M \simeq M_j$ for some $j$. Let $[\theta_\delta]$ be the projection of $[\theta]$ on $M$. Since $\rho^{p^{r+1}}[\theta] = [1]$, we deduce that $\rho^{p^{r+1}}[\theta_\delta] = [1]$. Now if $j > p^r + 1$ then $[\theta_\delta]$ lies in a proper submodule of $M$. Because $\rho M$ is the unique maximal ideal of $M$ and $e$ is an $\mathbb{F}_p[G]$-module homomorphism, $e(\theta_\delta) = 0$. On the other hand, if $j < p^r + 1$ then we have already observed that $e(M) = \{0\}$. From $e(\theta) \neq 0$ we deduce that there
must exist a summand isomorphic to $M_{p^r+1}$ and on which $e$ is nontrivial. Let $U$ denote such a summand.

Now let $\{V_{\alpha}\}$, $\alpha \in A$, be the collection of summands of $J_\epsilon$ apart from $U$. Hence $J_\epsilon = U \oplus_{\alpha \in A} V_{\alpha}$. Since every summand of $J_\epsilon$ is isomorphic to $M_{p^i}$ where $i \in \{0,1,\ldots,n\}$, except possibly for one summand isomorphic to $M_{p^r+1}$, we have (1). From the last paragraph, we have (2) and (3). Finally, since $e$ is trivial on $F_p[G]$-submodules isomorphic to $M_j$ with $j < p^r + 1$, we have (4).

\[ \square \]

6. Proof of Theorem 1.1

Proof. We first consider the case $\text{char } F \neq p$.

Suppose that $L/F$ is a Galois extension with group $M_{p^i+c} \rtimes G$, where $0 \leq i < n$ and $1 \leq c < p^{i+1} - p^i$. Let $K = \text{Fix}_L(M_{p^i+c})$ and identify $G$ with $\text{Gal}(K/F)$. Define $\hat{F}$, $\hat{K}$, $J$, $J_\epsilon$, and $A$ as in Sections 3 through 5. By the Kummer correspondence of Section 3 and Proposition 3.1, $L = L_M$ for some $F_p[G]$-submodule $M$ of $J_\epsilon$ such that $M \simeq \text{Gal}(L/K) \simeq M_{p^i+c}$ as $F_p[G]$-modules. Let $\gamma \in \hat{K}^\times$ be such that $M = N_\gamma$. Since $p^i + c < p^n$, we see that $M \subset A$ and so $e$ is defined on $M$. By Proposition 4.1 and the discussion following it, from $\text{Gal}(L/F) \simeq M_{p^i+c} \rtimes G$ we deduce $e(\gamma) = 0$.

Observe that if $p = 2$ then from $p^i + c < p^{i+1}$ and $1 \leq c$ we see that $i > 0$ and hence $n > 1$. By Theorem 5.1, $J_\epsilon$ has a decomposition into indecomposable $F_p[G]$-modules

\[ J_\epsilon = U \oplus \bigoplus_{\alpha \in A} V_{\alpha} \]

such that each indecomposable $V_{\alpha}$ is isomorphic to $M_{p^j}$ for some $j \in \{0,\ldots,n\}$, $U \simeq M_{p^r+1}$ for some $r \in \{-\infty,0,\ldots,n-1\}$, $e(U) = F_p$, and $e(V_{\alpha}) = \{0\}$ for all $V_{\alpha} \simeq M_{p^i}$ with $0 \leq i \leq r$. Let $U = N_\chi$ for some $\chi \in \hat{K}^\times$. Then $e(\chi) \neq 0$.

Because $\rho^{p^i+c-1}M \neq \{0\}$ we know that $J_\epsilon$ is not annihilated by $\rho^{p^i+c-1}$. Therefore either $\rho^{p^i+c-1}$ does not annihilate $U \simeq M_{p^r+1}$, whence $p^r + 1 \geq p^i + c$, or $p^r + 1 < p^i + c$ and there exists an indecomposable summand isomorphic to $M_{p^j}$ for some $j > i$.

Suppose first that $p^r + 1 < p^i + c$ and $J_\epsilon$ contains an indecomposable summand $V$ isomorphic to $M_{p^j}$ for some $j > i$. If $j = n$ then by Proposition 3.1
there exists a Galois extension $L_V/F$ such that $\text{Gal}(L_V/K) \simeq M_{p^n} \simeq \mathbb{F}_p[G]$. By Proposition 4.1(2), we have $\text{Gal}(L_V/F) \simeq \mathbb{F}_p[G] \rtimes G$. Since $M_{p^{i+1}} \rtimes G$ is a quotient of $\mathbb{F}_p[G] \rtimes G$, we deduce that $M_{p^{i+1}} \rtimes G$ is a Galois group over $F$.

If instead $j < n$, then let $\gamma \in \hat{K}^\times$ such that $V = N_\gamma$. Because $e$ is surjective on $U$ we may find $\beta \in \hat{K}^\times$ such that $[\beta] \in U$ and $e(\beta) = e(\gamma)$. Now set $\delta := \gamma/\beta$. Then $e(\delta) = 0$ and we consider $N_\delta$. From $p^j > p^i + c > p^r + 1$ and $\rho^{p^r+1}[\delta] = [1]$ we deduce that $\rho^{p^j-1}[\beta] = [1]$. Then $\rho^{p^i}(\delta) = [1]$ while $\rho^{p^j-1}(\delta) \neq [1]$, so $N_\delta \simeq M_{p^j}$. Let $W = N_\delta$. By Propositions 3.1 and 4.1 we obtain a Galois field extension with $\text{Gal}(L_W/F) \simeq M_{p^j} \rtimes G$. Since $M_{p^{i+1}} \rtimes G$ is a quotient of $M_{p^j} \rtimes G$, we deduce that $M_{p^{i+1}} \rtimes G$ is a Galois group over $F$.

Suppose now that for every $j > i$ there does not exist an indecomposable summand isomorphic to $M_{p^j}$. We claim that $r > i$. Suppose not. Then from $p^r + 1 \geq p^i + c$ we obtain $r = i$ and $c = 1$. Moreover, $U$ is the only summand of $J_\epsilon$ not annihilated by $\rho^{p^i}$. Let $\theta \in \hat{K}^\times$ such that $[\theta] = \text{proj}_U \gamma$. If $[\theta] \in \rho U$, then $\rho^\theta[\gamma] = [1]$, whence $\rho^\theta M = \{0\}$, a contradiction. Since $[\theta] \in U \setminus \rho U$ and $\rho U$ is the unique maximal ideal of $U$, we obtain that $U = N_\theta$. Since $e(U) = \mathbb{F}_p$, we deduce that $e(\theta) \neq 0$. Now if $V_\alpha \simeq M_{p^j}$ for $j \leq r$ then $e(V_\alpha) = \{0\}$. Hence $e(V_\alpha) = \{0\}$ for all $\alpha \in A$. We deduce that $e(\gamma) \neq 0$, a contradiction. Therefore $r \geq i + 1$.

Let $\omega = \rho \chi$ and consider $N_{\omega} = \rho N_{\chi} = \rho U$. We obtain that $e(\omega) = 0$ and $N_{\omega} \simeq M_{p^r}$. By Propositions 3.1 and 4.1, we have that $\text{Gal}(L_W/F) \simeq M_{p^r} \rtimes G$ for some suitable cyclic submodule $W$ of $J_\epsilon$. Since $M_{p^{i+1}} \rtimes G$ is a quotient of $M_{p^r} \rtimes G$, we deduce that $M_{p^{i+1}} \rtimes G$ is a Galois group over $F$.

Finally we turn to the case char $F = p$. Recall that we denote $M_j \rtimes G$, $j = 1, \ldots, p^n$, by $H_j$. We have short exact sequences

$$1 \to \mathbb{F}_p \simeq \rho^{p^i+c+k} M_{p^i+c+k+1} \rtimes 1 \to H_{p^i+c+k+1} \to H_{p^i+c+k} \to 1$$

for all $1 \leq i < n$, $1 \leq c < p^{i+1} - p^i$, and $0 \leq k < p^{i+1} - p^i - c$. For all of these, the kernels are central, and the groups $H_{p^i+c+k+1}$ and $H_{p^i+c+k}$ have the same rank, so the sequences are nonsplit. By Witt’s Theorem, all central nonsplit Galois embedding problems with kernel $\mathbb{F}_p$ are solvable. (See [7, Appendix A].) Hence if $H_{p^i+c}$ is a Galois group over $F$, one may successively solve a chain of suitable central nonsplit embedding problems with kernel $\mathbb{F}_p$ to obtain $H_{p^{i+1}}$ as a Galois group over $F$.

7. Acknowledgements

Andrew Schultz thanks Ravi Vakil for his encouragement and direction in this and all other projects. John Swallow thanks Université Bordeaux I for its hospitality during 2005–2006.
Automatic realizations of Galois groups

References


Ján Mináč
Department of Mathematics
Middlesex College
University of Western Ontario
London, Ontario
N6A 5B7
CANADA
E-mail: minac@uwo.ca
URL: http://www.math.uwo.ca/~minac/minac.html

Andrew Schultz
Department of Mathematics
University of Illinois at Urbana-Champaign
1409 W. Green Street
Urbana, IL
61801
USA
E-mail: acs@math.uiuc.edu
URL: http://www.math.uiuc.edu/~acs/

John Swallow
Department of Mathematics
Davidson College
Box 7046 Davidson, North Carolina
28035-7046
USA
E-mail: joswallow@davidson.edu
URL: http://www.davidson.edu/math/swallow/