J. reine angew. Math. ▮▮ (2007), 1—17
DOI 10.1515/CRELLE.2007.▮▮▮

Journal für die reine und
angewandte Mathematik
© Walter de Gruyter
Berlin · New York 2007

Detecting pro-p-groups that are not absolute Galois groups

By *Dave Benson* at Aberdeen, *Nicole Lemire* and *Ján Mináč* at London, and *John Swallow* at Davidson

Let p be a prime. It is a fundamental problem to classify the absolute Galois groups G_F of fields F containing a primitive pth root of unity ξ_p. In this paper we present several constraints on such G_F, using restrictions on the cohomology of index p normal subgroups from [LMS]. In section 1 we classify all maximal p-elementary abelian-by-order p quotients of these G_F. In the case $p > 2$, each such quotient contains a unique closed index p elementary abelian subgroup. This seems to be the first case in which one can completely classify nontrivial quotients of absolute Galois groups by characteristic subgroups of normal subgroups. In section 2 we derive analogues of theorems of Artin-Schreier and Becker for order p elements of certain small quotients of G_F. Finally, in section 3 we construct a new family of pro-p-groups which are not absolute Galois groups over any field F.

As a consequence of our results, we prove the following limitations on relator shapes of pro-p absolute Galois groups. For elements σ and τ of a group Γ, let ${}^0[\sigma,\tau] = \tau$, ${}^1[\sigma,\tau] = \sigma\tau\sigma^{-1}\tau^{-1}$, and ${}^n[\sigma,\tau] = [\sigma, {}^{n-1}[\sigma,\tau]]$ for $n \geqq 2$. Similarly, for subsets Γ_1 and Γ_2 of Γ, let ${}^n[\Gamma_1,\Gamma_2]$ denote the closed subgroup generated by all elements of the form ${}^n[\gamma_1,\gamma_2]$ for $\gamma_i \in \Gamma_i$.

Theorem A.1. *Let p be an odd prime, Γ a pro-p-group with maximal closed subgroup Δ, and $\sigma \in \Gamma \backslash \Delta$.*

(1) *Suppose that for some $\tau \in \Delta$ and some $2 \leqq e \leqq p-2$*

$$ {}^e[\sigma,\tau] \notin {}^{p-1}[\sigma,\Delta]\Phi(\Delta) \quad \textit{and} \quad {}^{e+1}[\sigma,\tau] \in \Phi(\Delta). $$

Then Γ is not an absolute Galois group.

Nicole Lemire was supported in part by Natural Sciences and Engineering Research Council of Canada grant R3276A01. Ján Mináč was supported in part by Natural Sciences and Engineering Research Council of Canada grant R0370A01. John Swallow was supported in part by National Science Foundation grant DMS-0600122.

Moreover, if Γ *contains a normal subgroup* $\Lambda \subset \Delta$ *such that* $\Gamma/\Lambda \simeq \mathbb{Z}/p^2\mathbb{Z}$, *we may take* $1 \leqq e \leqq p-2$.

(2) *Suppose that for some* $\tau_1, \tau_2 \in \Delta$,

$$[\sigma, \tau_i] \notin {}^{p-1}[\sigma, \Delta]\Phi(\Delta), \quad {}^{2}[\sigma, \tau_i] \in \Phi(\Delta), \quad i = 1, 2,$$
$$\langle[\sigma, \tau_1]\rangle\Phi(\Delta) \neq \langle[\sigma, \tau_2]\rangle\Phi(\Delta).$$

Then Γ *is not an absolute Galois group.*

(3) *Suppose that*

$$\sigma^p \in {}^{2}[\sigma, \Delta]\Phi(\Delta).$$

Then Γ *is not an absolute Galois group.*

Here $\Phi(\Delta) = \Delta^p[\Delta, \Delta]$ denotes the Frattini subgroup of Δ.

Furthermore, pro-p-groups with single relations similar to those of Demuškin groups for odd primes cannot be absolute Galois groups.

Corollary. *Let* p *be an odd prime and* Γ *a pro-p-group minimally generated by* $\{\sigma_1, \sigma_2\} \cup \{\sigma_i\}_{i \in \mathscr{I}}$ *subject to a single relation*

$$\sigma_1^q \cdot {}^{f}[\sigma_1, \sigma_2] \cdot \prod_{(i,j) \in \mathscr{J}} [\sigma_i, \sigma_j] \cdot \prod_{k \in \mathscr{K}} [\sigma_1^p, \sigma_k]$$

for some $2 \leqq f \leqq p-1$, $q \in \mathbb{N} \cup \{0\}$ *with* $q = 0 \operatorname{mod}(p^2)$, *a finite ordered set of pairs* $\mathscr{J} \subset \mathscr{I} \times \mathscr{I}$, *and a finite ordered subset* $\mathscr{K}$ *of* $\mathscr{I}$. *Then* Γ *is not an absolute Galois group.*

The results in [LMS] may be used to establish further new results on possible V-groups of fields and metabelian quotients of absolute Galois pro-p-groups. (For the definition of the V-group V_F of a field F, see section 2.) Moreover, some of the results here hold in a greater generality than their formulations here. For instance, the examples here of pro-p non-absolute Galois groups are also examples of groups which are not maximal pro-p-quotients of absolute Galois groups, by [LMS], §6. Furthermore, pro-p-groups which are not absolute Galois groups are not p-Sylow subgroups of absolute Galois groups. We plan a systematic study of these concerns in [BMS].

We observe that because this paper is concerned only with degree 1 and degree 2 cohomology, the results cited from [LMS] rely only on the Merkurjev-Suslin Theorem [MeSu], Theorem 11.5, and not the full Bloch-Kato Conjecture. Furthermore, we note that while this paper is self-contained, an extended version is available [BLMS].

1. *T*-groups

A *T-group* is a nontrivial pro-p-group T with a maximal closed subgroup N that is abelian of exponent dividing p. Then N is a normal subgroup, and the factor group T/N

acts naturally on N: choose a lift $t \in T$ and act via $n \mapsto tnt^{-1}$. Given any profinite group Γ with a closed normal subgroup Δ of index p, the factor group $\Gamma/\Delta^p[\Delta, \Delta]$ is a T-group. Now suppose that E/F is a cyclic field extension of degree p. We define the *T-group of E/F* to be $T_{E/F} := G_F/G_E^p[G_E, G_E]$. In this section we classify those T-groups realizable as $T_{E/F}$ for fields F either with $\operatorname{char} F = p$ or $\xi_p \in F$.

We develop a complete set of invariants t_i, $i = 1, 2, \ldots, p$, and u of T-groups as follows. For a pro-p-group Γ, denote by $Z(\Gamma)$ its center, $Z(\Gamma)[p]$ the elements of $Z(\Gamma)$ of order dividing p, $\Gamma^{(n)}$ the nth group in the p-central series of Γ, and $\Gamma_{(n)}$ the nth group in the central series of Γ. For a T-group T we define

$$t_1 = \dim_{\mathbb{F}_p} H^1\left(\frac{Z(T)[p]}{Z(T) \cap T_{(2)}}, \mathbb{F}_p\right),$$

$$t_i = \dim_{\mathbb{F}_p} H^1\left(\frac{Z(T) \cap T_{(i)}}{Z(T) \cap T_{(i+1)}}, \mathbb{F}_p\right), \quad 2 \leqq i \leqq p,$$

$$u = \max\{i : 1 \leqq i \leqq p, T^p \subset T_{(i)}\}.$$

Proposition A.1. *For arbitrary cardinalities t_i, $i = 1, 2, \ldots, p$, and u with $1 \leqq u \leqq p$, the following are equivalent*:

(1) *The t_i and u are invariants of some T-group.*

(2) (a) *If $u < p$ then $t_u \geqq 1$, and*

(b) *if $u = p$ and $t_i = 0$ for all $2 \leqq i \leqq p$, then $t_1 \geqq 1$.*

Moreover, T-groups are uniquely determined up to isomorphism by these invariants.

Theorem A.2. *For p an odd prime, the following are equivalent*:

(1) *T is a T-group with invariants t_i and u satisfying*

(a) $u \in \{1, 2\}$,

(b) $t_2 = u - 1$, *and*

(c) $t_i = 0$ *for* $3 \leqq i < p$.

(2) *$T \simeq T_{E/F}$ for some cyclic extension E of degree p of a field F such that either* $\operatorname{char} F = p$ *or* $\xi_p \in F$.

Now suppose $p = 2$. Then each T-group is isomorphic to $T_{E/F}$ for some cyclic extension E/F of degree 2.

Let G be a cyclic group of order p and M_i, $i = 1, 2, \ldots, p$, denote the unique cyclic $\mathbb{F}_p G$-module of dimension i. Since the $\mathbb{F}_p G$-modules we consider will be multiplicative groups, we usually write the action of G exponentially. For a set $\mathcal{I}$, let $M_i^{\mathcal{I}}$ denote the product of $|\mathcal{I}|$ copies of M_i endowed with the product topology. We use the word *duality* exclusively to refer to Pontrjagin duality, between compact and discrete abelian groups and more generally between compact and discrete $\mathbb{F}_pG$-modules. We denote the dual of Γ by $\Gamma^\vee$.

Lemma A.1. *Suppose T is a T-group with invariants t_i, $i = 1, 2, \dots, p$ and u, and N is a maximal closed subgroup of T that is abelian of exponent dividing p. Let $\sigma \in T \setminus N$ and set $\bar{\sigma}$ to be the image of σ in $G := T/N$. Then N is a topological $\mathbb{F}_pG$-module and we have*:

(1) *For any $\mathbb{F}_pG$-submodule M of N and $i \geqq 0$, ${}^i[T, M] = M^{(\bar{\sigma}-1)^i}$.*

(2) *For $i \geqq 2$, $T_{(i)} = N^{(\bar{\sigma}-1)^{i-1}}$.*

(3) *There exist sets $\mathscr{I}_i$, $i = 1, 2, \dots, p$, such that N decomposes into indecomposable $\mathbb{F}_pG$-modules as $N = M_1^{\mathscr{I}_1} \times M_2^{\mathscr{I}_2} \times \cdots \times M_p^{\mathscr{I}_p}$, endowed with the product topology. Moreover, for $i \geqq 2$, $t_i = |\mathscr{I}_i|$, and*

$$t_1 = \begin{cases} 1 + |\mathscr{I}_1|, & T \textit{ is abelian of exponent } p, \\ |\mathscr{I}_1|, & \textit{otherwise.} \end{cases}$$

(4) $T^p = \langle \sigma^p \rangle \cdot T_{(p)}$.

(5) *If $u < p$ then u is the minimal v with $1 \leqq v \leqq p - 1$ such that there is a commutative diagram of pro-p-groups*

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] \arrow[d, two heads] & T \arrow[r] \arrow[d, two heads] & G \arrow[r] \arrow[d, "="] & 1 \\ 1 \arrow[r] & M_v \arrow[r] & H \arrow[r] & G \arrow[r] & 1 \end{tikzcd} \tag{1}$$

with a lift of $\bar{\sigma}$ in H of order p^2. If $u = p$ then no such diagram exists for $1 \leqq v \leqq p - 1$.

Proof. (1) Suppose that $\tau \in T$ is arbitrary, and write $\tau = n\sigma^i$ for $n \in N$ and $i \in \mathbb{N} \cup \{0\}$. The action of T factors through G. Hence $[\tau, M] = M^{(\bar{\sigma}^i - 1)}$ and so $[T, M] = M^{(\bar{\sigma}-1)}$. The result follows by induction. (Moreover, we observe that if p does not divide i, then $[\tau, M] = [M, \tau] = [T, M] = [M, T]$.)

(2) Observe that $[T, T] = [T, N]$. Then use (1).

(3) Because $\mathbb{F}_pG$ is an Artinian principal ideal ring, every $\mathbb{F}_pG$-module U decomposes into a direct sum of cyclic $\mathbb{F}_pG$-modules. Every cyclic $\mathbb{F}_pG$-module is indecomposable and self-dual. Applying these results to $U = N^\vee$ and using duality (see [RZ], Lemma 2.9.4 and Theorem 2.9.6), we obtain the decomposition.

Using (2) together with $M_j^G = M_j^{(\bar{\sigma}-1)^{j-1}}$ for all $1 \leqq j \leqq p$, we calculate

$$Z(T) \cap N = (M_1)^{\mathscr{I}_i} \times (M_2^{(\bar{\sigma}-1)})^{\mathscr{I}_2} \times \cdots \times (M_p^{(\bar{\sigma}-1)^{p-1}})^{\mathscr{I}_p},$$

$$Z(T) \cap T_{(i)} = (M_i^{(\bar{\sigma}-1)^{i-1}})^{\mathscr{I}_i} \times \cdots \times (M_p^{(\bar{\sigma}-1)^{p-1}})^{\mathscr{I}_p}, \quad 2 \leqq i \leqq p,$$

and

$$Z(T) \cap T_{(i)} = \{1\} \quad \text{for } i > p.$$

We deduce that $t_i = |\mathscr{I}_i|$, $2 \leqq i \leqq p$.

For the case $i = 1$, suppose first that T is abelian of exponent p. Then $Z(T) = Z(T)[p] = T$ and $T_{(2)} = \{1\}$. By (2), $N^{(\bar\sigma-1)} = \{1\}$, whence $|\mathscr{I}_i| = 0$ for $i \geqq 2$. Therefore $t_1 = 1 + |\mathscr{I}_1|$. Next suppose that T is nonabelian. Then $Z(T) \subset N$. We obtain $Z(T)[p] = Z(T) \cap N$ and so $t_1 = \dim_{\mathbb{F}_p} H^1\big((Z(T) \cap N)/(Z(T) \cap T_{(2)}), \mathbb{F}_p\big) = |\mathscr{I}_1|$. Finally, assume that T is abelian and not of exponent p. Then $N = Z(T)[p]$ and $t_1 = \dim_{\mathbb{F}_p} H^1(N, \mathbb{F}_p) = |\mathscr{I}_1|$.

(4) For $\delta \in N$ we have $(\delta\sigma)^2 = [\sigma, \delta]\delta^2\sigma^2$ and, by induction,

$$(\delta\sigma)^i = \underbrace{[\sigma, [\sigma, \dots, [\sigma}_{i-1 \text{ times}}, \delta] \cdots]]^{\binom{i}{i}} \cdots [\sigma, [\sigma, \delta]]^{\binom{i}{3}} [\sigma, \delta]^{\binom{i}{2}} \delta^i \sigma^i.$$

Then $(N\sigma)^p = (\sigma^p) \cdot {}^{p-1}[\sigma, N]$, which by (1) and (2) may be written $\sigma^p \cdot T_{(p)}$. Replacing σ with σ^v for $(v, p) = 1$, we conclude $T^p = \langle \sigma^p \rangle \cdot T_{(p)}$.

(5) Suppose that for some $v < u$ there is a commutative diagram (1) with a lift of $\bar\sigma$ in H of order p^2. Then $T \twoheadrightarrow H$ factors through $T/N^{(\bar\sigma-1)^v}$. But by (2), $T_{(v+1)} = N^{(\bar\sigma-1)^v}$ and by definition of u, we have $T^p \subset T_{(u)} \subset T_{(v+1)}$. Hence every lift of $\bar\sigma$ into $T/N^{(\bar\sigma-1)^v}$ is of order p, and the same holds for H. We conclude that no commutative diagram as above with $\bar\sigma$ lifting to an element of order p^2 exists for $v < u$.

Now suppose that $u < p$ and consider σ^p. By (4), $T^p = \langle \sigma^p \rangle \cdot T_{(p)}$, and $T_{(p)} \subset T_{(u+1)}$. We have $T^p \subset T_{(u)}$ and $T^p \not\subset T_{(u+1)}$ and so $\sigma^p \in T_{(u)} \backslash T_{(u+1)}$. Now $\sigma^p \in N$. By (2), since $T_{(u)} = N^{(\sigma-1)^{u-1}}$ for $u \geqq 2$, we deduce $\sigma^p \in N^{(\sigma-1)^{u-1}} \backslash N^{(\sigma-1)^u}$. From $[\sigma, \sigma^p] = 1$ we obtain $\sigma^p \in N^G$. Therefore $\sigma^p \in (N^G \cap N^{(\sigma-1)^{u-1}}) \backslash (N^G \cap N^{(\sigma-1)^u})$. We claim that there exists an $\mathbb{F}_p G$-submodule M_u of N such that $M_u^G = \langle \sigma^p \rangle$ and $N = M_u \times \tilde N$ for some $\mathbb{F}_p G$-submodule $\tilde N$ of N. Assume a factorization of N into cyclic $\mathbb{F}_p G$-submodules as in (3). Consider $w \in N$ such that $w^{(\sigma-1)^{u-1}} = \sigma^p$ and all components of w lie in factors of dimension at least u. For at least one factor M_u, $\mathrm{proj}_{M_u} w$ generates M_u as an $\mathbb{F}_p G$-module. Write $N = M_u \times \tilde N$. We obtain the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & N \arrow[r] \arrow[d, two heads] & T \arrow[r] \arrow[d, two heads] & G \arrow[r] \arrow[d, "="] & 1 \\
1 \arrow[r] & M_u \arrow[r] & T/\tilde N \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

in which a lift of $\bar\sigma$ is of order p^2. □

The following lemma follows easily from the definitions.

Lemma A.2. *Let T be a T-group with invariants t_i, $i = 1, 2, \dots, p$, and u.*

(1) *T is abelian if and only if $t_i = 0$ for all $2 \leqq i \leqq p$.*

(2) *T is of exponent p if and only if $u = p$ and $t_u = 0$.*

(3) *If $u < p$ then $t_u \geqq 1$.*

(4) *If $t_i = 0$ for all $2 \leqq i \leqq p$, then $t_1 \geqq 1$.*

Proof of Proposition A.1. By Lemma A.2(3,4), (1) implies (2). Now suppose we are given cardinalities t_i, $i = 1, 2, \dots, p$, and u satisfying conditions (2).

The case $u < p$. Let G be a group of order p and $\mathscr{I}_i$, $i = 1, 2, \dots, p$ sets with cardinalities $|\mathscr{I}_i|$ satisfying $|\mathscr{I}_i| = t_i$ for $i \neq u$ and $1 + |\mathscr{I}_u| = t_u$. Set

$$N = X \times M_1^{\mathscr{I}_1} \times M_2^{\mathscr{I}_2} \times \cdots \times M_p^{\mathscr{I}_p},$$

where $X \simeq M_u$ and N is endowed with the product topology. Then N is a pseudocompact $\mathbb{F}_p G$-module. (See [Br], page 443.) Define an action of $\mathbb{Z}_p$ on N by letting a generator σ of $\mathbb{Z}_p$ act via a generator of G, and form $N \rtimes \mathbb{Z}_p$ in the category of pro-p-groups. Now choose an $\mathbb{F}_p G$-module generator x of X and define $x_i = x^{(\sigma-1)^i}$ for $0 \leqq i \leqq u$. Since $(\sigma - 1)$ is nilpotent of degree u on X we obtain $x_{u-1} \neq 1$ and $x_u = 1$. We set R to be the closed subgroup $\langle \sigma^p x_{u-1} \rangle \subset N \rtimes \mathbb{Z}_p$. Finally form $\Gamma = (N \rtimes \mathbb{Z}_p)/R$ and set Δ to be the image of $N \rtimes \{1\}$ in Γ. Since $\Delta \simeq N$ as pro-p-G operator groups, we identify them. By construction Δ is a maximal closed subgroup of Γ which is abelian of exponent p. Hence Γ is a T-group. Since the image of σ in Γ has order p^2, Γ is not of exponent p. From the decomposition of N, we obtain by Lemma A.1(3) that the invariants t_i are as desired. It remains only to show that u is as given. By Lemma A.1(4) we have $\Gamma^p = \langle x_{u-1} \rangle \cdot \Gamma_{(p)}$. From Lemma A.1(4) we calculate that $x_{u-1} \in \Gamma_{(u)}$ and $x_{u-1} \notin \Gamma_{(u+1)}$. Hence u is as desired.

The case $u = p$ follows analogously. Let G be a group of order p and $\mathscr{I}_i$ sets with cardinalities $|\mathscr{I}_i|$ satisfying $|\mathscr{I}_i| = t_i$, $2 \leqq i \leqq p$; $|\mathscr{I}_1| = t_1$ if some $t_j \neq 0$, $2 \leqq j \leqq p$; and $1 + |\mathscr{I}_1| = t_1$ if all $t_j = 0$, $2 \leqq j \leqq p$. Set $N = M_1^{\mathscr{I}_1} \times M_2^{\mathscr{I}_2} \times \cdots \times M_p^{\mathscr{I}_p}$, $\Gamma = N \rtimes G$, $\Delta = N \rtimes \{1\}$, let σ be a generator of G, and proceed as before.

Now we show that T-groups are uniquely determined up to isomorphism by the invariants t_i and u. Let T be an arbitrary T-group with invariants t_i, $i = 1, 2, \dots, p$, and u, N a maximal closed subgroup of T that is abelian of exponent dividing p, and $G = T/N$. From Lemma A.1(3) the structure of N as an $\mathbb{F}_p G$-module is determined up to isomorphism, and T is an extension of N by G. Let $\sigma \in T \backslash N$. We have $\sigma^p \in N^G$. It remains only to determine the isomorphism class of N as an $\mathbb{F}_p G$-module with a distinguished factor X such that $\sigma^p \in X^G$.

Suppose first that $u = p$, $t_1 \geqq 1$, and $t_i = 0$ for all $2 \leqq i \leqq p$. From Lemma A.2(1), T is abelian and so $T_{(2)} = \{1\}$. Since $u = p$, T has exponent p. Then $T \simeq M_1^{\mathscr{I}_1} \times G$ and $t_1 = |\mathscr{I}_1| + 1$. Thus T is determined by the invariants. Now suppose that $t_1 \geqq 1$, $t_i = 0$ for all $2 \leqq i \leqq p$, and $u = 1$. Again T is abelian. Since $u \neq p$, T has exponent p^2. Then $N = X \times \tilde{N}$, where σ^p generates an $\mathbb{F}_p G$-module X isomorphic to M_1 and $\tilde{N} \simeq M_1^{\mathscr{I}'}$ with $|\mathscr{I}'| + 1 = t_1$.

Finally suppose $t_i \neq 0$ for some i with $2 \leqq i \leqq p$. Then T is nonabelian, and by Lemma A.1(4), $T^p = \langle \sigma^p \rangle \cdot T_{(p)}$. From Lemma A.1(2) we obtain, for $u < p$,

$\sigma^p \in (N^G \cap N^{(\sigma-1)^{u-1}}) \backslash (N^G \cap N^{(\sigma-1)^u})$, while for $u = p$, we have $\sigma^p \in N^{(\sigma-1)^{p-1}}$. If $u < p$ then by Proposition A.1 we have $t_u \geqq 1$, and using the same argument as in the proof of Lemma A.1(5), N contains a distinguished direct factor $X \simeq M_u$ such that $X^G = \langle \sigma^p \rangle$. We deduce that $N = X \times \tilde{N}$ where $\tilde{N} \simeq M_u^{\mathscr{I}'} \times \prod_{i \neq u} M_i^{\mathscr{I}_i}$ for sets $\mathscr{I}_i$, $i \neq u$, and $\mathscr{I}'$ such that $|\mathscr{I}_i| = t_i$, $i \neq u$, and $1 + |\mathscr{I}'| = t_u$. If $u = p$, we claim that without loss of generality we may assume that $\sigma^p = 1$. Since $\sigma^p \in N^{(\sigma-1)^{p-1}}$, let $v \in N$ such that $\sigma^p = v^{(\sigma-1)^{p-1}}$ and set $\tau = \sigma v^{-1}$. Then $\tau \in T \backslash N$ and $\tau^p = \sigma^p (v^{-1})^{1+\sigma+\cdots+\sigma^{p-1}} = 1$. Hence $T = N \rtimes G$. □

Lemma A.3. *Suppose that Γ is a profinite group such that its maximal pro-p-quotient $\Gamma(p)$ is a free pro-p-group of (positive and possibly infinite) rank n, and let Δ be a normal subgroup of Γ of index p. Then the invariants of the T-group $\Gamma/\Delta^p[\Delta,\Delta]$ are $t_1 = 1$, $t_i = 0$ for $2 \leqq i < p$, $t_p = n - 1$ if $n < \infty$ and $t_p = n$ for n an infinite cardinal, and $u = 1$.*

Proof. Since $\Gamma/\Delta^p[\Delta,\Delta] = \Gamma(p)/\Phi(\Delta(p))$, we may assume without loss that Γ is a free pro-p-group. The result then follows from the analogue of the Kurosh subgroup theorem in the context of pro-p-groups. □

Lemma A.4. *Let S be a free pro-p-group. Then there exists a field F of characteristic* 0 *such that $G_F \simeq S$.*

Proof. First let F_0 be any algebraically closed field of characteristic 0 with cardinality greater than or equal to $d = \dim_{\mathbb{F}_p} H^1(S, \mathbb{F}_p)$. Set $F_1 := F_0(t)$. By [Do], G_{F_1} is a free profinite group, and let P denote a p-Sylow subgroup of G_{F_1}. By [RZ], Corollary 7.7.6, P is a free pro-p-group. Let F_2 be the fixed field of P. The classes in $F_1^\times/F_1^{\times p}$ of the set A of linear polynomials $t - c$, $c \in F_0$, are linearly independent over $\mathbb{F}_p$. Choose a subset of A of cardinality d, and let V be the vector subspace of $F_1^\times/F_1^{\times p}$ generated by the classes of the elements of A. Since $([F_2 : F_1], p) = 1$, V injects into $F_2^\times/F_2^{\times p}$. Let W denote this image. Now let F be a maximal algebraic field extension of F_2 such that W injects into $F^\times/F^{\times p}$. By maximality, the image $i(W)$ of W in $F^\times/F^{\times p}$ is in fact $F^\times/F^{\times p}$. The rank of G_F is then $\dim_{\mathbb{F}_p} H^1(G_F, \mathbb{F}_p) = \dim_{\mathbb{F}_p} V = d$. □

Proof of Theorem A.2. *The case $p = 2$.* Let $u \in \{1, 2\}$, t_1, and t_2 be invariants of a T-group T. By Proposition A.1, $t_1 \geqq 1$ if $u = 1$, and if $u = 2$ then either $t_1 \geqq 1$ or $t_2 \geqq 1$.

Case 1: T is not of exponent 2. By Lemma A.2(2), either $u = 1$ or $t_2 \geqq 1$. Let G be a group of order 2 and $N = M_1^{\mathscr{I}_1} \times M_2^{\mathscr{I}_2}$ for sets $\mathscr{I}_1$ and $\mathscr{I}_2$ satisfying $|\mathscr{I}_1| = t_1$ and $|\mathscr{I}_2| = t_2$, and let $M = N^\vee$. From [MSw], Corollary 2, there exists E/F with $\operatorname{char} F \neq 2$ and $\operatorname{Gal}(E/F) \simeq G$ such that $H^1(G_E, \mathbb{F}_2) \simeq E^\times/E^{\times 2} \simeq M$ as $\mathbb{F}_2 G$-modules if and only if there exist $\Upsilon \in \{0, 1\}$ and cardinalities d and e such that $t_1 + 1 = 2\Upsilon + d$; $t_2 + \Upsilon = e$; if $\Upsilon = 0$ then $d \geqq 1$; and if $\Upsilon = 1$ then $e \geqq 1$. Moreover, $-1 \in N_{E/F}(E^\times)$ if and only if $\Upsilon = 1$. Finally, by [MSw], proof of Theorem 1, we may choose E/F such that G_F is a pro-2-group.

If $u = 1$ then set $\Upsilon = 1$ and $e = t_2 + \Upsilon$. Since $t_1 \geqq 1$ we may choose $d \geqq 0$ such that $2\Upsilon + d = t_1 + 1$. Then $e \geqq 1$ and the conditions for E/F with $G_E/G_E^{(2)} \simeq M^\vee \simeq N$ are satisfied. Since $\Upsilon = 1$, $-1 \in N_{E/F}(E^\times)$, and by Albert's criterion [A], E/F embeds in a cyclic extension E'/F of degree 4. Let $\operatorname{Gal}(E/F) = \langle \bar{\sigma} \rangle$. We have the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & G_E/G_E^{(2)} \arrow[r] \arrow[d, two heads] & G_F/G_E^{(2)} \arrow[r] \arrow[d, two heads] & G \arrow[r] \arrow[d, "="] & 1 \\
1 \arrow[r] & M_1 \arrow[r] & H \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

in which $\bar{\sigma}$ lifts to an element of order 4. By Lemma A.1(5), $u = 1$ for $T_{E/F}$. By Lemma A.2(2), $T_{E/F}$ is not of exponent 2. Using Lemma A.1(3), because $G_E/G_E^{(2)} \simeq N \simeq M_1^{\mathscr{I}_1} \times M_2^{\mathscr{I}_2}$, the invariants t_1 and t_2 of $T_{E/F}$ match those of T. By Proposition A.1, $T \simeq T_{E/F}$.

If $u = 2$ then $t_2 \geqq 1$. We take $\Upsilon = 0$, $d = t_1 + 1 \geqq 1$, and $e = t_2$ and obtain an extension E/F as before. Since $\Upsilon = 0$, $-1 \notin N_{E/F}(E^\times)$ and so by [A], E/F does not embed in a cyclic extension E'/F of degree 4. Let $\mathrm{Gal}(E/F) = \langle \bar{\sigma} \rangle$. There is no commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & G_E/G_E^{(2)} \arrow[r] \arrow[d, two heads] & G_F/G_E^{(2)} \arrow[r] \arrow[d, two heads] & G \arrow[r] \arrow[d, "="] & 1 \\
1 \arrow[r] & M_1 \arrow[r] & H \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

in which $\bar{\sigma}$ lifts to an element of order 4. By Lemma A.1(5), $u = 2$ for $T_{E/F}$. Because $t_2 \geqq 1$, $G_E/G_E^{(2)}$ contains an $\mathbb{F}_2G$-submodule isomorphic to M_2 whence $T_{E/F}$ is nonabelian. By Lemma A.1(3) and the isomorphism $G_E/G_E^{(2)} \simeq N \simeq M_1^{\mathscr{I}_1} \times M_2^{\mathscr{I}_2}$ we deduce that the invariants t_1 and t_2 of $T_{E/F}$ match those of T. By Proposition A.1, $T \simeq T_{E/F}$.

Case 2: T has exponent 2. By Lemma A.2(2), $u = 2$ and $t_2 = 0$, and so $t_1 \geqq 1$. Let $N = M_1^{\mathscr{I}_1}$ for $\mathscr{I}_1$ satisfying $|\mathscr{I}_1| + 1 = t_1$. Set $\Upsilon = 0$, $d = t_1 + 1$, and $e = t_2 = 0$. Then $d \geqq 1$ and there exists E/F with $\mathrm{char}\, F \neq 2$ such that $H^1(G_E, \mathbb{F}_2) \simeq M$ and $-1 \notin N_{E/F}(E^\times)$. As before, $u = 2$ for $T_{E/F}$, and by Lemma A.1(3), $t_2 = 0$ for $T_{E/F}$. By Lemma A.2(2), $T_{E/F}$ has exponent 2, and by Lemma A.1(3), t_1 is the correct invariant for $T_{E/F}$. By Proposition A.1, $T \simeq T_{E/F}$.

The case $p > 2$. First we characterize those T-groups occurring as $T_{E/F}$ for fields F such that the maximal pro-p-quotient $G_F(p)$ of the absolute Galois group G_F is free pro-p. Lemma A.3 tells us that for such F and an E/F of degree p, the invariants of $T_{E/F}$ are $t_1 = 1$, $t_i = 0$ for $2 \leqq i < p$, and $u = 1$, and that the rank of $G_F(p)$ is one more than the invariant t_p. Now suppose that T is a T-group with invariants $t_1 = 1$, $t_i = 0$ for $2 \leqq i < p$, and $u = 1$. By Lemma A.4 there exists F such that G_F is a free pro-p-group of rank $t_p + 1$. Letting Δ be any maximal closed subgroup of G_F and $E = \mathrm{Fix}(\Delta)$, Lemma A.3 and Proposition A.1 give $T \simeq T_{E/F}$. Therefore the T-groups which occur as $T_{E/F}$ for fields F with free maximal pro-p-quotient $G_F(p)$ are precisely those for which $t_1 = 1$, $t_i = 0$ for $2 \leqq i < p$, and $u = 1$.

Now we characterize which of the remaining T-groups occur as $T_{E/F}$ for cyclic field extensions E/F of degree p for F a field such that either $\mathrm{char}\, F = p$ or $\xi_p \in F$. By Witt's Theorem, $\mathrm{char}\, F \neq p$. Hence we consider only fields F with $\mathrm{char}\, F \neq p$ and $\xi_p \in F$. For a cyclic extension E/F of degree p, consider the $\mathbb{F}_p \mathrm{Gal}(E/F)$-module $M_{E/F} := H^1(G_E, \mathbb{F}_p) \simeq E^\times/E^{\times p}$, and let G be an abstract group of order p. Since the particular isomorphism $G \simeq \mathrm{Gal}(E/F)$ does not alter the isomorphism class of $M_{E/F}$ as an

$\mathbb{F}_pG$-module, we may consider all such modules as $\mathbb{F}_pG$-modules. (See [MSw].) By [MSw], Corollary 1, $M \simeq M_{E/F}$ as $\mathbb{F}_pG$-modules for suitable E/F with $G \simeq \mathrm{Gal}(E/F)$ if and only if $M = M_1^{\mathscr{I}_1} \oplus M_2^{\mathscr{I}_2} \oplus M_p^{\mathscr{I}_p}$, where the cardinalities $j_1 = |\mathscr{I}_1|$, $j_2 = |\mathscr{I}_2|$, and $j_p = |\mathscr{I}_p|$ satisfy the following conditions: $j_1 + 1 = 2\Upsilon + d$, $j_2 = 1 - \Upsilon$, and $j_p + 1 = e$ for some cardinalities d, e and $\Upsilon \in \{0, 1\}$ where $d \geqq 1$ if $\Upsilon = 0$ and $e \geqq 1$. Moreover, $\Upsilon = 1$ if and only if $\xi_p \in N_{E/F}(E^\times)$. Finally, by [MSw], proof of Theorem 1, we may choose E/F such that G_F is a pro-p-group.

We observe that the constraints on j_1, j_2, and j_p are then $j_1 \geqq \Upsilon$ and $j_2 = 1 - \Upsilon$. Now by duality, $H^1(G_E, \mathbb{F}_p)^\vee \simeq G_E/G_E^{(2)}$, and since cyclic $\mathbb{F}_pG$-modules are self-dual, we may derive conditions on the topological $\mathbb{F}_pG$-module $G_E/G_E^{(2)}$ occurring as maximal closed subgroups of T-groups $G_F/G_E^{(2)}$, as follows. Set $G = G_F/G_E$.

First we relate Υ and the invariant u. We claim that for any T-group $G_F/G_E^{(2)}$, we have $u \leqq 2$. Write $E = F(\sqrt[p]{a})$ for some $a \in F^\times$. Let $[e] \in E^\times/E^{\times p}$ denote the class of $e \in E^\times$. Then $X = \langle [\sqrt[p]{a}], [\xi_p] \rangle$ is a cyclic $\mathbb{F}_pG$-submodule of M and is isomorphic to M_i for some $i \in \{1, 2\}$. By equivariant Kummer theory (see [W]), $L = E(\sqrt[p^2]{a}, \xi_{p^2})$ is a Galois extension of F. Moreover, G_F/G_L is a homomorphic image of $G_F/G_E^{(2)}$, since L/E is an elementary abelian extension. Then $L/F(\xi_{p^2})$ is Galois with group $\mathbb{Z}/p^2\mathbb{Z}$, and for any $\sigma \in G_F \backslash G_E$, the restriction $\sigma_L \in \mathrm{Gal}(L/F)$ restricts to a generator. Hence $1 \dotplus \sigma^p \in \mathrm{Gal}(L/E)$, and therefore $1 \dotplus \sigma^p \in G_E/G_E^{(2)}$. We have a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & G_E/G_E^{(2)} \arrow[r] \arrow[d, two heads] & G_F/G_E^{(2)} \arrow[r] \arrow[d, two heads] & G \arrow[r] \arrow[d, "="] & 1 \\
1 \arrow[r] & M_i \arrow[r] & G_F/G_L \arrow[r] & G \arrow[r] & 1
\end{tikzcd} \tag{2}$$

and so by Lemma A.1(5) we deduce that $u \leqq i \leqq 2$.

Now we claim that $\Upsilon = 1$ if and only if $u = 1$. We have that $\Upsilon = 1$ if and only if $\xi_p \in N_{E/F}(E^\times)$. By [A], $\Upsilon = 1$ if and only if E/F embeds in a cyclic extension of F of degree p^2, if and only if there exists a closed normal subgroup $\tilde{N} \subset G_E$ such that $G_F/\tilde{N} \simeq \mathbb{Z}/p^2\mathbb{Z}$. Any such closed normal subgroup must contain $G_E^{(2)}$. Hence we deduce that $\Upsilon = 1$ if and only if there exists a commutative diagram (2) with $i = 1$ in which nontrivial elements of G lift to elements of order p^2. By Lemma A.1(5), $\Upsilon = 1$ if and only if $u = 1$.

We have therefore shown that $u \leqq 2$ and $u = 2 - \Upsilon$. Translating the remaining conditions on j_1 and j_2, we see that $j_1 \geqq 2 - u$ and $j_2 = u - 1$. Now by Lemma A.1(3), $t_2 = j_2$, $t_i = 0$ for $3 \leqq i \leqq p - 1$, and $t_p = j_p$. Moreover, $t_1 = j_1$ if T is not abelian of exponent p. By Lemma A.2(2), T is of exponent p if and only if $u = p$. But we have shown that $u \leqq 2 < p$, whence T is not of exponent p and we have $t_1 = j_1$. By Proposition A.1, if $u = 1$ then $t_1 \geqq 1$, and since $t_2 = u - 1$ the conditions for applying [MSw], Corollary 1 are valid. Hence a T-group $T_{E/F}$ with prescribed invariants subject to condition (1) exists. □

Proof of Theorem A.1. Suppose Γ is a pro-p-group with maximal closed subgroup Δ, and let $T = \Gamma/\Delta^{(2)}$, $N = \Delta/\Delta^{(2)}$ and $G = \Gamma/\Delta$. Write $\bar{\sigma}$ and $\bar{\tau}$ for the images of σ and τ, respectively.

(1) Since Δ surjects onto N we have that $\bar{\sigma} \notin N$, $\bar{\tau} \in N$, ${}^{e}[\bar{\sigma}, \bar{\tau}] \notin {}^{p-1}[\bar{\sigma}, N]$, and ${}^{e+1}[\bar{\sigma}, \bar{\tau}] = 1$. By Lemma A.1(2,3) we have $1 \neq {}^{e}[\bar{\sigma}, \bar{\tau}] \in T_{(e+1)} \backslash T_{(p-1)}$. We deduce from ${}^{e+1}[\bar{\sigma}, \bar{\tau}] = 1$ that ${}^{e}[\bar{\sigma}, \bar{\tau}] \in Z(T)$. We obtain that some invariant $t_i \neq 0$ for $3 \leqq i < p$. Now if $\Gamma = G_F$ for some F, then setting $E = \mathrm{Fix}(\Delta)$ we obtain $T = T_{E/F}$, contradicting Theorem A.2. Now assume additionally that there exists a closed normal subgroup $\Lambda \subset \Delta$ of Γ such that $\Gamma/\Lambda \simeq \mathbb{Z}/p^2\mathbb{Z}$ and $e = 1$. Let $\tilde{\sigma}$ denote the image of σ in T. We have a commutative diagram (1) with $v = 1$ and an image of $\tilde{\sigma}$ in H of order p^2. By Lemma A.1(5), $u = 1$ for T is equal to 1. As before some $t_i \neq 0$, $2 \leqq i < p$. Again by Theorem A.2 we are done.

(2) We proceed as before, obtaining two elements $[\bar{\sigma}, \bar{\tau}_i]$, $i = 1, 2$, which generate distinct subgroups of $Z(T) \cap T_{(2)}$ with trivial intersection with $T_{(p)}$. We deduce that the sum of t_i, $2 \leqq i < p$, is at least two, and we apply Theorem A.2.

(3) We obtain $\bar{\sigma} \notin N$, $\bar{\tau} \in N$, and $\bar{\sigma}^p \in {}^{2}[\bar{\sigma}, N]$. By Lemma A.1(2,3) we have $\bar{\sigma}^p \subset T_{(3)}$, and from Lemma A.1(4) we deduce that $T^p \subset T_{(3)}$. Hence $u \geqq 3$, and we apply Theorem A.2. □

Proof of Corollary to Theorem A.1. Let Δ be the closed subgroup of Γ generated as a normal subgroup by σ_1^p, σ_2, and σ_i for $i \in \mathscr{I}$, and let Λ be the closed subgroup of Γ generated as a normal subgroup by $\sigma_1^{p^2}$, σ_2, and σ_i for $i \in \mathscr{I}$. Set also $T = \Gamma/\Delta^{(2)}$. Examining the quotient of Γ obtained by trivializing σ_2 and each σ_i, $i \in \mathscr{I}$, we see that Δ is maximal and $\Gamma/\Lambda \simeq \mathbb{Z}/p^2\mathbb{Z}$. Now let $e = f - 1$. By passing from Γ to T using bars for denoting images of elements of Γ in T, we see that ${}^{e}[\bar{\sigma}_1, \bar{\sigma}_2] \notin {}^{p-1}[\bar{\sigma}_1, \bar{\Delta}]$ in T. On the other hand, ${}^{e+1}[\sigma_1, \sigma_2] = {}^{f}[\sigma_1, \sigma_2] = 1$ in T. By Theorem A.1(1), Γ is not an absolute Galois group. □

It is a natural question to ask whether the maximal closed subgroup N in the definition of T-group is unique. Let H denote the Heisenberg group of order p^3 if $p > 2$ and the dihedral group of order 8 if $p = 2$. It is not difficult to show that if T is a T-group with a maximal closed subgroup N which is abelian of exponent dividing p, then unless T is either itself abelian of exponent p of order greater than p, or isomorphic to the direct product of H and (possibly zero) copies of $\mathbb{Z}/p\mathbb{Z}$, then N is unique in T. (From Pontrjagin duality we know that an abelian pro-p-group of exponent p is a topological product of cyclic groups of order p.) In particular, in these cases N is a characteristic subgroup of T. Since the exceptional T-groups have invariant $u = p$, we have by Theorem A.2 that for $p > 2$, each $T_{E/F}$ has a unique index p elementary abelian subgroup.

2. Analogues of theorems of Artin-Schreier and Becker

Recall that by Artin-Schreier there are no elements of order p in the absolute Galois groups of a field F, unless $p = 2$ and F is formally real. Becker proved that the same holds for maximal pro-p-quotients of absolute Galois groups [Be]. In this section we show that in certain small quotients of absolute Galois groups, there are no non-central elements of order p unless $p = 2$ and the base field F is formally real.

Let p be a prime and F a field with $\xi_p \in F$. We define the following fields associated to F:

- $F^{(2)}$: the compositum of all cyclic extensions of F of degree p.

- $F^{(3)}$: the compositum of all cyclic extensions of $F^{(2)}$ of degree p which are Galois over F.

- $F^{(2)^{(2)}}$: the compositum of all cyclic extensions of $F^{(2)}$ of degree p.

Then we set $W_F = \mathrm{Gal}(F^{(3)}/F)$ and $V_F = \mathrm{Gal}(F^{(2)^{(2)}}/F)$. Observe that for a cyclic extension E/F of degree p, $T_{E/F} = \mathrm{Gal}(E^{(2)}/F)$.

Theorem A.3. *Let p be prime and F a field with $\xi_p \in F$. The following are equivalent*:

(1) *There exists $\sigma \in V_F \backslash \Phi(V_F)$ of order p.*

(2) *There exists $\sigma \in W_F \backslash \Phi(W_F)$ of order p.*

(3) *There exists $\sigma \in V_F \backslash \Phi(V_F)$ such that for each cyclic E/F of degree p its image $\sigma_{E/F} \in T_{E/F}$ has order at most p.*

(4) *$p = 2$ and F is formally real.*

If these conditions hold, the elements whose square roots are fixed by σ form an ordering of F.

Proof of Theorem A.3. (1) ⇒ (2) and (1) ⇒ (3). Observe first that $F^{(3)} \subset F^{(2)^{(2)}}$. Hence we have a natural surjection $V_F \twoheadrightarrow W_F$. Assume that $\sigma \in V_F \backslash \Phi(V_F)$ has order p. Then its image in $W_F \backslash \Phi(W_F)$ also has order p. Moreover, for any cyclic extension E/F of degree p, the image $\sigma_{E/F}$ of σ in $T_{E/F}$ has order at most p, as follows. Since $E^{(2)}$ is contained in $F^{(2)^{(2)}}$ we see that $\sigma_{E/F}^p = 1$ in $T_{E/F}$.

(2) ⇒ (4). Suppose that $\sigma \in W_F \backslash \Phi(W_F)$ has order p. As in the proof of Theorem A.2, let $a \in F^\times \backslash F^{\times p}$ be arbitrary such that $F(\sqrt[p]{a}) \not\subset F(\xi_{p^2})$. Set $K_a := F(\sqrt[p]{a}, \xi_{p^2}) \subset F^{(2)}$. Then $[K_a : F(\xi_{p^2})] = p$ and $L_a := F(\sqrt[p^2]{a}, \xi_{p^2})$ is a cyclic extension of degree p^2 of $F(\xi_{p^2})$. Moreover, L_a/F is a Galois extension of F and $L_a \subset F^{(3)}$ since $\mathrm{Gal}(L_a/F)$ is a central extension of degree $\leqq p$ of $\mathrm{Gal}(K_a/F)$. Now if $\sigma(\sqrt[p]{a}) \neq \sqrt[p]{a}$ then σ has order p^2 in W_F. Hence σ fixes all $\sqrt[p]{a}$ for $a \in F^\times$ with $F \neq F(\sqrt[p]{a}) \not\subset F(\xi_{p^2})$. Since $\sigma \notin \Phi(W_F)$, there must exist a cyclic extension $E \subset F^{(2)}$ of F which is not fixed by σ. We deduce that $\xi_{p^2} \notin F$ and so $E = F(\xi_{p^2})$. If p is odd then $L := F(\xi_{p^3})$ is a cyclic extension of F of degree p^2 and σ restricts to a generator of $\mathrm{Gal}(L/F) \simeq \mathbb{Z}/p^2\mathbb{Z}$, again a contradiction, whence $p = 2$. Now let $s \in W_F \backslash \Phi(W_F)$ be an element of order 2. By [MSp1], proof of Theorem 2.7, the elements of F whose square roots are fixed by s form an ordering of F. Hence (2) ⇒ (4).

(4) ⇒ (1). Suppose that (4) holds. By [Be], Satz 3, there exists an ordering of F whose square roots are fixed by some element s of order 2 in $G_F(2)$. Then the restriction of s to $F^{(2)^{(2)}}$ is the required element $\sigma \in V_F \backslash \Phi(V_F)$ of order 2. Hence (4) ⇒ (1).

(3) ⇒ (2). Let $\sigma \in V_F \backslash \Phi(V_F)$ such that for each cyclic extension E/F of degree p the image $\sigma_{E/F}$ of σ in $T_{E/F}$ has order at most p. Let $E = F(\sqrt[p]{a})$ such that σ acts nontrivially on $\sqrt[p]{a}$ and $L_a = F(\sqrt[p^2]{a}, \xi_{p^2})$. As above, since the restriction of $\sigma_{E/F}$ to $L_a \subset E^{(2)}$ is not of order p^2, we deduce that $p = 2$ and $\sqrt{-1} \notin F$. Hence F is not quadratically closed. If F is real closed then there exists precisely one extension E/F of degree 2, namely $F^{(2)}$,

and $F^{(2)} = F^{(3)} = F^{(2)^{(2)}}$, whence $W_F = T_{E/F} = V_F$. Otherwise, $F^{(3)}$ is a compositum of extensions L/F such that $\mathrm{Gal}(L/F)$ is either a cyclic group of order 4 or a dihedral group of order 8. (See [MSp2], Corollary 2.18.) On the other hand, each such L lies in $E^{(2)}$ for a suitable quadratic extension E/F: each L may be obtained as a Galois closure of $E(\sqrt{\gamma})$ for some $[E:F] = 2$ and $\gamma \in E^\times$. Therefore the restrictions $\sigma_{L/F}$ of σ to the extensions L/F have order $\leqq 2$, and so the restriction of $\sigma_{F^{(3)}/F}$ of σ to $F^{(3)}/F$ has order 2. Hence (3) ⇒ (2). □

3. Pro-p-groups that are not absolute Galois groups

Theorem A.4. *Let $p > 3$ be prime. There exists a pro-p-$\mathbb{Z}_p$ operator group Ω such that no group of the form $\Gamma := \big((\Omega \star \Sigma) \rtimes \mathbb{Z}_p\big)/\mathscr{E}$, where Σ is any pro-p-group with trivial $\mathbb{Z}_p$-action, and $\mathscr{E}$ is any normal closed subgroup of $(\Omega \star \Sigma) \rtimes \mathbb{Z}_p$ such that $\mathscr{E} \subset \big((\Omega \star \Sigma) \rtimes p\mathbb{Z}_p\big)^{(3)}$, is an absolute Galois group.*

Here $\star$ denotes the free product in the category of pro-p-groups. (Recall that $R^{(n)}$ denotes the nth term of the p-descending series of a pro-p-group R; see section 1.)

The Ω of the theorem is that of the following proposition. Recall that for a pro-p-group Γ, the *decomposable subgroup* of $H^2(\Gamma, \mathbb{F}_p)$ is defined to be the subgroup generated by cup products of elements of $H^1(\Gamma, \mathbb{F}_p)$: $H^2(\Gamma, \mathbb{F}_p)^{\mathrm{dec}} = H^1(\Gamma, \mathbb{F}_p).H^1(\Gamma, \mathbb{F}_p)$. We say that $H^2(\Gamma, \mathbb{F}_p)$ is *decomposable* if $H^2(\Gamma, \mathbb{F}_p) = H^2(\Gamma, \mathbb{F}_p)^{\mathrm{dec}}$.

Proposition A.2. *Let $p > 3$ be prime and C be a cyclic group of order p. There exists a torsion-free pro-p-C operator group Ω such that as $\mathbb{F}_pC$-modules, $H^1(\Omega, \mathbb{F}_p) \simeq M_p$ and $H^2(\Omega, \mathbb{F}_p) = H^2(\Omega, \mathbb{F}_p)^{\mathrm{dec}} \simeq M_{p-1} \oplus \dfrac{(p-3)}{2} M_p$.*

Here we use M_i to denote the unique cyclic $\mathbb{F}_pC$-module of dimension i, and we write the action of $\mathbb{F}_pC$ multiplicatively.

Proof. Let $D = \langle g \mid g^p = 1 \rangle$ be a cyclic group of order p, and let $\mathbb{Z}_pD$ be the p-adic group ring, written multiplicatively as $\mathscr{G}$, where the element $\bar{g}_i$ of $\mathscr{G}$ corresponds to the element g^i of $\mathbb{Z}_pD$. We interpret the suffixes $\mathrm{mod}\, p$. Now let $C = \langle \sigma \mid \sigma^p = 1 \rangle$ be another group of order p, acting on $\mathscr{G}$ via $\sigma(\bar{g}_i) = \bar{g}_{i-1}$. In this way $\mathscr{G}$ and $H^1(\mathscr{G}, \mathbb{Z}_p)$ are free $\mathbb{Z}_pC$-modules, and $H^1(\mathscr{G}, \mathbb{Z}_p)$ has a topological generating set $y_0, y_1, \dots, y_{p-1}$ dual to $\bar{g}_0, \bar{g}_1, \dots, \bar{g}_{p-1}$. Observe that $\sigma(y_i) = y_{i+1}$. Next let $\mathscr{H} = \mathbb{Z}_p$ be a trivial $\mathbb{Z}_pC$-module with generator h, and let $z \in H^1(\mathscr{H}, \mathbb{Z}_p)$ be dual to h. We define a nonsplit central extension Ω of $\mathscr{H}$ by $\mathscr{G}$ as follows. The group $H^2(\mathscr{G}, \mathscr{H}) = \bigwedge^2 H^1(\mathscr{G}, \mathscr{H})$ is a free $\mathbb{Z}_pC$-module of rank $p(p-1)/2$ with free generators y_0y_j for $1 \leqq j \leqq (p-1)/2$. Consider the element

$$y := (1 + \sigma + \cdots + \sigma^{p-1})y_0y_1 = y_0y_1 + y_1y_2 + \cdots + y_{p-1}y_0.$$

Let Ω be the central extension of $\mathscr{H}$ by $\mathscr{G}$ corresponding to $y \in H^2(\mathscr{G}, \mathscr{H})$.

The group Ω is a torsion-free nilpotent pro-p-group of Hirsch length $p+1$. The standard correspondence of group extensions with H^2 gives us that for suitable representatives

$g_i \in \Omega$ with images $\bar{g}_i \in \mathscr{G}$, we have the relations $[g_i, g_j] = h$ for $j = i+1$; $[g_i, g_j] = 1$ for $j \neq i+1$ and $i \neq j+1$; and $[g_i, h] = 1$ for all i. The action of C on $\mathscr{G}$ may be extended to Ω by $\sigma(g_i) = g_{i-1}$, $0 \leqq i < p$, and $\sigma(h) = h$.

The E_2 page of the spectral sequence $H^s\big(\mathscr{G}, H^t(\mathscr{H}, \mathbb{F}_p)\big) \Rightarrow H^{s+t}(\Omega, \mathbb{F}_p)$ is generated by anticommuting elements $\bar{y}_i \in E_2^{1,0}$ and $\bar{z} \in E_2^{0,1}$, and we have $d_2^{0,1}(\bar{z}) = \bar{y}$, where $\bar{y}$ is the reduction mod p of y. Observe that $d_2^{0,1}$ is injective on $E^{0,1} = H^1(\mathscr{H}, \mathbb{F}_p)$. By the five-term exact sequence, $H^1(\Omega, \mathbb{F}_p) \simeq H^1(\mathscr{G}, \mathbb{F}_p)$ as $\mathbb{F}_pC$-modules and so $H^1(\Omega, \mathbb{F}_p) \simeq M_p$.

Now consider $H^2(\Omega, \mathbb{F}_p)$. We claim first that $d_2^{1,1}$ is injective. It is enough to show that $d_2^{1,1}(\bar{x}.\bar{z}) = 0$ implies that $\bar{x} = 0$ for $\bar{x} \in H^1(\mathscr{G}, \mathbb{F}_p)$. Write $\bar{x} = \sum_{i=0}^{p-1} c_i \bar{y}_i$, $c_i \in \mathbb{F}_p$. Since $p > 3$, the set of elements $\bar{y}_i.\bar{y}_{i+2}.\bar{y}_{i+3}$, $0 \leqq i < p$, is $\mathbb{F}_p$-independent and may be expanded to an $\mathbb{F}_p$-basis of $E_2^{3,0} = H^3(\mathscr{G}, \mathbb{F}_p)$ consisting of products $\bar{y}_i.\bar{y}_j.\bar{y}_k$, $0 \leqq i < j < k \leqq p-1$. Consider the coefficient β_i of $\bar{y}_i.\bar{y}_{i+2}.\bar{y}_{i+3}$ in an expansion of $d_2^{1,1}(\bar{x}.\bar{z})$. Since $p > 3$, the only consecutive pair of indices in $\bar{y}_i.\bar{y}_{i+2}.\bar{y}_{i+3}$ is $\{i+2, i+3\}$. Hence $\beta_i = c_i$. If all $\beta_i = 0$, then each $c_i = 0$ and therefore $d_2^{1,1}$ is injective. Now since $d_2^{1,1}$ is injective, $E_3^{1,1} = E_\infty^{1,1} = 0$, and because $E_2^{0,2} = 0$ we have $E_\infty^{0,2} = 0$. Next observe that $\bar{y} = (\sigma - 1)^{p-1}\bar{y}_0.\bar{y}_1$ and so $\bar{y} \in H^2(\mathscr{G}, \mathbb{F}_p)^C$. Since $E^{2,0} = H^2(\mathscr{G}, \mathbb{F}_p)$ is the direct sum of free $\mathbb{F}_pC$-modules $M(0,i) \simeq M_p$ on generators $\bar{y}_0.\bar{y}_i$, $1 \leqq i \leqq (p-1)/2$, we deduce that

$$E_\infty^{2,0} = E_3^{2,0} = \big(M(0,1)/M(0,1)^C\big) \oplus \frac{(p-3)}{2} M(0,i).$$

Thus $H^2(\Omega, \mathbb{F}_p) \simeq M_{p-1} \oplus \frac{(p-3)}{2} M_p$. Finally, since $H^1(\Omega, \mathbb{F}_p) \simeq H^1(\mathscr{G}, \mathbb{F}_p)$ and $H^2(\Omega, \mathbb{F}_p)$ is a quotient of $E_2^{2,0} = H^2(\mathscr{G}, \mathbb{F}_p) = \bigwedge^2 H^1(\mathscr{G}, \mathbb{F}_p)$, $H^2(\Omega, \mathbb{F}_p)$ is decomposable as well. □

Given a free pro-p-group V and a pro-p-group Δ, we say that a surjection $V \twoheadrightarrow \Delta$ is a *minimal presentation* of Δ if $\inf : H^1(\Delta, \mathbb{F}_p) \to H^1(V, \mathbb{F}_p)$ is an isomorphism.

Proposition A.3. *Let Δ be a pro-p-group, V a free pro-p-group, and $1 \to R \to V \to \Delta \to 1$ a minimal presentation of Δ. Then we have natural maps*

(1) $H^2(\Delta, \mathbb{F}_p) \simeq \big(R/(R^p[R, V])\big)^\vee$,

(2) $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}} \simeq \big(R/(R \cap V^{(3)})\big)^\vee$.

Proof. Set $\Delta^{[2]} := \Delta/\Delta^{(2)}$ and $V^{[3]} := V/V^{(3)}$. Because the presentation is minimal, $\Delta^{[2]} \simeq V/V^{(2)}$. We then have the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] & R \arrow[r] \arrow[d] & V \arrow[r] \arrow[d] & \Delta \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \frac{V^{(2)}}{V^{(3)}} \arrow[r] & V^{[3]} \arrow[r] & \Delta^{[2]} \arrow[r] & 1.
\end{tikzcd}$$

Passing to the natural maps induced by the Hochschild-Serre-Lyndon spectral sequence with coefficients in $\mathbb{F}_p$, we obtain the commutative diagram

$$\begin{tikzcd}
H^1(\Delta^{[2]}) \arrow[r, "\mathrm{inf}"] \arrow[d] & H^1(V^{[3]}) \arrow[r, "\mathrm{res}"] \arrow[d] & H^1\left(\dfrac{V^{(2)}}{V^{(3)}}\right)^{\Delta^{[2]}} \arrow[r, "\mathrm{tra}"] \arrow[d] & H^2(\Delta^{[2]}) \arrow[r] \arrow[d] & \cdots \\
H^1(\Delta) \arrow[r, "\mathrm{inf}"] & H^1(V) \arrow[r, "\mathrm{res}"] & H^1(R)^{\Delta} \arrow[r, "\mathrm{tra}"] & H^2(\Delta) \arrow[r] & 0.
\end{tikzcd}$$

Since the extension $1 \to V^{(2)}/V^{(3)} \to V^{[3]} \to \Delta^{(2)} \to 1$ is central,

$$H^1(V^{(2)}/V^{(3)}, \mathbb{F}_p)^{\Delta^{[2]}} = H^1(V^{(2)}/V^{(3)}, \mathbb{F}_p).$$

Additionally using the fact that the inflation map on the first cohomology group in each row of the previous diagram is an isomorphism, we may extract the following commutative square, with the rightmost transgression map an isomorphism:

$$\begin{tikzcd}
H^1\left(\dfrac{V^{(2)}}{V^{(3)}}, \mathbb{F}_p\right) \arrow[r] \arrow[d, "\mathrm{tra}"] & H^1(R, \mathbb{F}_p)^{\Delta} \arrow[d, "\mathrm{tra}", "\simeq"'] \\
H^2(\Delta^{[2]}, \mathbb{F}_p) \arrow[r] & H^2(\Delta, \mathbb{F}_p).
\end{tikzcd}$$

Since $H^1(R, \mathbb{F}_p)^{\Delta} \simeq (R/R^p[R, V])^{\vee}$, we have (1).

The leftmost transgression map, however, is also an isomorphism by [Ho], 1.1 and proof. Now consider the natural map $R/R^p[R, V] \to V^{(2)}/V^{(3)}$ of abelian topological groups of exponent p. The image of the natural map $H^1(V^{(2)}/V^{(3)}, \mathbb{F}_p) \to H^1(R, \mathbb{F}_p)^{\Delta}$ is $H^1(RV^{(3)}/V^{(3)}, \mathbb{F}_p)$. We then factor the horizontal maps of the commutative square into homomorphisms followed by injections:

$$\begin{tikzcd}
H^1\left(\dfrac{V^{(2)}}{V^{(3)}}, \mathbb{F}_p\right) \arrow[r] \arrow[d, "\mathrm{tra}", "\simeq"'] & H^1\left(\dfrac{RV^{(3)}}{V^{(3)}}, \mathbb{F}_p\right) \arrow[r, hook] & H^1(R, \mathbb{F}_p)^{\Delta} \arrow[d, "\mathrm{tra}", "\simeq"'] \\
H^2(\Delta^{[2]}, \mathbb{F}_p) \arrow[r] & H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}} \arrow[r, hook] & H^2(\Delta, \mathbb{F}_p).
\end{tikzcd}$$

We obtain isomorphisms

$$H^1\bigl(R/(R \cap V^{(3)}), \mathbb{F}_p\bigr) \simeq H^1(RV^{(3)}/V^{(3)}, \mathbb{F}_p) \simeq H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}}.$$

Hence $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}} \simeq \bigl(R/(R \cap V^{(3)})\bigr)^{\vee}$, and we have proved (2). □

Proposition A.4. *Let* Γ *and* H *be pro-p-groups with maximal closed subgroups* Δ *and* N, *respectively, and* $\alpha : \Gamma \to H$ *a surjection with* $\alpha(\Delta) = N$ *and* $\ker \alpha \subset \Delta^{(3)}$. *Write* G *for* $\Gamma/\Delta \simeq H/N$. *Then as* $\mathbb{F}_p G$*-modules,* $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}} \simeq H^2(N, \mathbb{F}_p)^{\mathrm{dec}}$.

Proof. We prove that $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}} \simeq H^2(N, \mathbb{F}_p)^{\mathrm{dec}}$ under a natural isomorphism, and it will follow that the isomorphism is $\mathbb{F}_pG$-equivariant. Let $\theta : V \to \Delta$ be a minimal presentation of Δ with kernel R. We may choose a section $W \subset V^{(3)}$ of $\ker\alpha$ under the surjection θ. We obtain a minimal presentation of $N = \alpha(\Delta)$: $1 \to RW \to V \xrightarrow{\psi} N \to 1$, where $\psi = \alpha \circ \theta$. By Proposition A.3(2),

$$H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}} \simeq (RV^{(3)}/V^{(3)})^\vee \simeq (RWV^{(3)}/V^{(3)})^\vee \simeq H^2(N, \mathbb{F}_p)^{\mathrm{dec}}. \quad \square$$

Lemma A.5. *Let p be prime and Γ a nonfree pro-p-group which is the absolute Galois group of a field F. Then $\operatorname{char} F \neq p$ and $\xi_p \in F$.*

Proof. Since Γ is not free, then by Witt's Theorem, $\operatorname{char} F \neq p$. Since $\big([F(\xi_p) : F], p\big) = 1$, $\xi_p \in F$. $\square$

Proposition A.5. *Let $p > 3$ be prime. Suppose that Γ is a pro-p-group and Δ is a maximal closed subgroup of Γ. If the $\mathbb{F}_p(\Gamma/\Delta)$-module $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}}$ contains a cyclic summand of dimension i with $3 \leqq i < p$, then Γ is not an absolute Galois group. Moreover, if Γ contains a normal closed subgroup $\Lambda \subset \Delta$ with $\Gamma/\Lambda \simeq \mathbb{Z}/p^2$, then we may take $2 \leqq i < p$ in the same statement.*

Proof. Suppose that $\Gamma = G_F$ for some field F. Then $\Delta = G_E$ for some E/F of degree p. Since $H^2(\Delta, \mathbb{F}_p) \neq 0$, G_E is not a free pro-p-group and therefore neither is G_F [S], Corollary 3, §I.4.2. Lemma A.5 gives $\operatorname{char} F \neq p$ and $\xi_p \in F$. By [MeSu], Theorem 11.5, $H^2(\Delta, \mathbb{F}_p)$ is decomposable. Therefore by [LMS], Theorem 1, $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}}$ contains no cyclic $\mathbb{F}_p(\Gamma/\Delta)$-summand of dimension i with $3 \leqq i < p$, a contradiction. Moreover, if $\Lambda \subset N$ is a normal closed subgroup and $\Gamma/\Lambda \simeq \mathbb{Z}/p^2\mathbb{Z}$, then by [A], $\xi_p \in N_{E/F}(E)$. Letting $E = F(\sqrt[p]{a})$ for some $a \in F^\times$, we obtain in $H^2(\Gamma, \mathbb{F}_p)$ that $(a).(\xi_p) = 0$. By [LMS], Theorem 1, $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}}$ contains no cyclic $\mathbb{F}_p(\Gamma/\Delta)$-summand of dimension 2, again a contradiction. $\square$

Corollary A.5. *Let $p > 3$ be prime. Suppose that Γ and H are pro-p-groups with respective maximal subgroups Δ and N, and $\alpha : \Gamma \to H$ a surjection with $\alpha(\Delta) = N$ and $\ker\alpha \subset \Delta^{(3)}$. Write G for $\Gamma/\Delta \simeq H/N$. If either $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}}$ or $H^2(N, \mathbb{F}_p)^{\mathrm{dec}}$ contains a cyclic $\mathbb{F}_pG$-summand of dimension i with $3 \leqq i < p$, then neither Δ nor H is an absolute Galois group.*

Moreover, suppose additionally that H contains a normal closed subgroup $\Lambda \subset N$ with $H/\Lambda \simeq \mathbb{Z}/p^2\mathbb{Z}$. Then if either $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}}$ or $H^2(N, \mathbb{F}_p)^{\mathrm{dec}}$ contains a cyclic $\mathbb{F}_pG$-summand of dimension 2, then H is not an absolute Galois group.

Proof. By Proposition A.4 we have that $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}} \simeq H^2(N, \mathbb{F}_p)^{\mathrm{dec}}$ as $\mathbb{F}_pG$-modules. The remainder follows from Proposition A.5. $\square$

Proof of Theorem A.4. Let Ω be the group of Proposition A.2. Observe that $\Delta := \big((\Omega \star \Sigma) \times p\mathbb{Z}_p\big)/\mathscr{E}$ is a maximal closed subgroup of Γ of index p. Let $G = \Gamma/\Delta$ and note that the actions of G and C on Δ are identical. By Corollary A.5 it is enough to show that $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}}$ for $\mathscr{E} = 1$ contains a cyclic $\mathbb{F}_pG$-summand M_i with $3 \leqq i < p$. Assume then that $\mathscr{E} = 1$. By [NSW], Theorem 4.1.4, we have

$$H^1(\Delta, \mathbb{F}_p) \simeq H^1(\Omega, \mathbb{F}_p) \oplus H^1(\Sigma, \mathbb{F}_p) \oplus H^1(p\mathbb{Z}_p, \mathbb{F}_p)$$

and $H^2(\Delta, \mathbb{F}_p) \simeq H^2(\Omega, \mathbb{F}_p) \oplus H^2(\Sigma, \mathbb{F}_p) \oplus H^1(\Omega, \mathbb{F}_p) \oplus H^1(\Sigma, \mathbb{F}_p)$. By Proposition A.2, $H^2(\Omega, \mathbb{F}_p)$ is decomposable and so $H^2(\Omega, \mathbb{F}_p)$ is a direct summand of $H^2(\Delta, \mathbb{F}_p)^{\mathrm{dec}}$. From Proposition A.2, we obtain that $H^2(\Omega, \mathbb{F}_p)$ contains an $\mathbb{F}_pG$-summand M_i with $3 \leqq i \leqq p-1$. □

Remark. The proof excludes the groups Γ from the class of absolute Galois groups by using the $n = 2$ case of [LMS], Theorem 1. However, neither a direct application of the $n = 1$ case nor Theorem A.2 excludes the groups Γ. Observe also that the fact that $\Omega \rtimes \mathbb{Z}_p$ is not an absolute Galois group could be deduced from the main results in [Koe], using different methods. However, the fact that each $\big((\Omega \times \Sigma) \rtimes \mathbb{Z}_p\big)/\mathscr{E}$ is not an absolute Galois group does not follow from [Koe].

Acknowledgement

We thank the referee of [LMS] for suggesting that we illustrate [LMS], Theorem 1 by constructing examples of pro-p-groups which are not absolute Galois groups, for this appendix is the result. The third author would also like to thank Sunil Chebolu, Ajneet Dhillon and Vahid Shirbisheh for stimulating discussions related to this paper.

References

[A] *A. Albert*, On cyclic fields, Trans. Amer. Math. Soc. **37** (1935), no. 3, 454–462.

[Be] *E. Becker*, Euklidische Körper und euklidische Hüllen von Körpern, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II, J. reine angew. Math. **268/269** (1974), 41–52.

[BLMS] *D. Benson*, *N. Lemire*, *J. Mináč*, and *J. Swallow*, Detecting pro-p-groups that are not absolute Galois groups, expanded version, ArXiv: math.NT/0610632.

[BMS] *D. Benson*, *J. Mináč*, and *J. Swallow*, p-Sylow subgroups of absolute Galois groups, in preparation.

[Br] *A. Brumer*, Pseudocompact algebras, profinite groups and class formations, J. Algebra **4** (1966), 442–470.

[Do] *A. Douady*, Détermination d'un groupe de Galois, C. R. Acad. Sci. Paris **258** (1964), 5305–5308.

[Ho] *K. Hoechsmann*, Zum Einbettungsproblem, J. reine angew. Math. **229** (1968), 81–106.

[Koe] *J. Koenigsmann*, Solvable absolute Galois groups are metabelian, Invent. Math. **144** (2001), no. 1, 1–22.

[LMS] *N. Lemire*, *J. Mináč*, and *J. Swallow*, Galois module structure of Galois cohomology and partial Euler-Poincaré characteristics, J. reine angew. Math.

[MeSu] *A. S. Merkurjev* and *A. A. Suslin*, K-cohomology of Severi-Brauer varieties and the norm residue homomorphism, Math. USSR Izv. **21** (1983), 307–340, English translation of Russian original: Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), no. 5, 1011–1046, 1135–1136.

[MSp1] *J. Mináč* and *M. Spira*, Formally real fields, Pythagorean fields, C-fields and W-groups, Math. Z. **205** (1990), no. 4, 519–530.

[MSp2] *J. Mináč* and *M. Spira*, Witt rings and Galois groups, Ann. Math. (2) **144** (1996), no. 1, 35–60.

[MSw] *J. Mináč* and *J. Swallow*, Galois modules appearing as pth-power classes of units of extensions of degree p, Math. Z. **250** (2005), no. 4, 907–914.

[NSW] *J. Neukirch*, *A. Schmidt*, and *K. Wingberg*, Cohomology of number fields, Grundl. Math. Wiss. **323**, Springer-Verlag, Berlin 2000.

[RZ] *L. Ribes* and *P. Zalesskii*, Profinite groups, Ergebn. Math. Grenzgeb. (3) **40**, Springer-Verlag, Berlin 2000.

[S] *J.-P. Serre*, Galois cohomology, Springer Monogr. Math. Springer-Verlag, Berlin 2002.

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

Department of Mathematical Sciences, University of Aberdeen, Meston Building, King's College, Aberdeen
AB24 3UE, Scotland UK
e-mail: bensondj@maths.abdn.ac.uk

Department of Mathematics, Middlesex College, University of Western Ontario, London, Ontario N6A 5B7,
Canada
e-mail: nlemire@uwo.ca
e-mail: minac@uwo.ca

Department of Mathematics, Davidson College, Box 7046, Davidson, North Carolina 28035-7046, USA
e-mail: joswallow@davidson.edu

Eingegangen 24. Oktober 2006