CONSTRUCTION AND CLASSIFICATION OF SOME GALOIS MODULES

JÁN MINÁČ*† AND JOHN SWALLOW‡

Abstract. In our previous paper we describe the Galois module structures of pth-power class groups $K^\times/K^{\times p}$, where K/F is a cyclic extension of degree p over a field F containing a primitive pth root of unity. Our description relies upon arithmetic invariants associated with K/F. Here we construct field extensions K/F with prescribed arithmetic invariants, thus completing our classification of Galois modules $K^\times/K^{\times p}$.

Let F be a field of characteristic not p containing a primitive pth root of unity ξ_p. For a cyclic field extension K/F with Galois group $\mathrm{Gal}(K/F)$ of order p, let $J = K^\times/K^{\times p}$, and let N denote the norm map from K to F.

In [MS], we proved that the structure of the $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module J is determined by the following three arithmetic invariants:

- $d = d(K/F) := \dim_{\mathbb{F}_p} F^\times/N(K^\times)$,
- $e = e(K/F) := \dim_{\mathbb{F}_p} N(K^\times)/F^{\times p}$, and
- $\Upsilon(K/F) := 1$ or 0 according to whether $\xi_p \in N(K^\times)$ or not.

Now if $G = \mathbb{Z}/p\mathbb{Z}$, then J may be considered an $\mathbb{F}_p[G]$-module via any isomorphism $G \cong \mathrm{Gal}(K/F)$, and the module structure of J is independent of the choice of isomorphism. It is a fundamental problem to classify the isomorphism classes of modules J for all K/F in our context. This problem is solved in Theorem 1 below. Corollaries 1 and 2 of Theorem 1 describe all modules J in an explicit way.

Date: April 8, 2003.

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

†Supported by the Mathematical Sciences Research Institute, Berkeley.

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

In the following theorem we determine the sets of invariants (d, e, Υ) which may be realized by an extension K/F and in so doing classify all $\mathbb{F}_p[G]$-modules $J = J(K/F)$ up to isomorphism.

Theorem 1. *Let p be a prime number. For arbitrary cardinal numbers d, e, and for $\Upsilon \in \{0, 1\}$, there exists a cyclic field extension K/F of degree p containing a primitive pth root of unity with invariants (d, e, Υ) if and only if*

- *if $\Upsilon = 0$, then $1 \le d$,*
- *if $p > 2$ then $1 \le e$, and*
- *if $p = 2$ and $\Upsilon = 1$ then $1 \le e$.*

From the theorem above and from [MS, Theorem 3 and Corollary 2] we immediately obtain the following corollaries. We denote by $M_{i,j}$ the jth cyclic module $\mathbb{F}_p[G]$ such that $\dim_{\mathbb{F}_p} M_{i,j} = i$, where j is a suitable index.

Corollary 1. *Let $p > 2$ be a prime number, and let G be a cyclic group of order p. Then an $\mathbb{F}_p[G]$-module J is realizable as an $\mathbb{F}_p[\mathrm{Gal}(K/F)]$-module $K^\times/K^{\times p}$ for some cyclic G-extension K/F such that F contains a primitive pth root of unity if and only if there exist cardinal numbers d, e, and $\Upsilon \in \{0, 1\}$ such that*

(i) *If $\Upsilon = 0$, then $1 \le d$;*
(ii) *$1 \le e$; and*
(iii)

$$J = \left(\bigoplus_{j \in \mathfrak{K}_1} M_{1,j}\right) \bigoplus \left(\bigoplus_{j \in \mathfrak{K}_2} M_{2,j}\right) \bigoplus \left(\bigoplus_{j \in \mathfrak{K}_p} M_{p,j}\right),$$

where

(1) *$|\mathfrak{K}_1| + 1 = 2\Upsilon + d$,*
(2) *$|\mathfrak{K}_2| = 1 - \Upsilon$, and*
(p) *$|\mathfrak{K}_p| + 1 = e$.*

The invariants d, e, and Υ determine the module J uniquely.

For $p = 2$ using [MS, Theorem 3 and Corollary 3], along with our theorem above, we obtain the next corollary.

Corollary 2. *Now let G be a cyclic group of order 2. Then an $\mathbb{F}_2[G]$-module J is realizable as an $\mathbb{F}_2[\mathrm{Gal}(K/F)]$-module $K^\times/K^{\times 2}$ for some* *quadratic extension* K/F *with its arithmetic invariants* $d(K/F)$*,* $e(K/F)$*, and* $\Upsilon(K/F)$ *coinciding with* d*,* e*, and* $\Upsilon \in \{0,1\}$*, respectively, if and only if* d*,* e*, and* Υ *satisfy the conditions below.*

- *if* $\Upsilon = 0$*, then* $1 \leq d$*,*
- *if* $\Upsilon = 1$*, then* $1 \leq e$*.*

In this case

$$J = \left(\bigoplus_{j\in\mathfrak{K}_1} M_{1,j}\right) \bigoplus \left(\bigoplus_{j\in\mathfrak{K}_2} M_{2,j}\right)$$

where

(1) $|\mathfrak{K}_1| + 1 = 2\Upsilon + d$ *and*
(2) $|\mathfrak{K}_2| + \Upsilon = e$*.*

Moreover, such a module J *is determined uniquely by the invariants* $2\Upsilon + d$ *and by* $e - \Upsilon$ *if* e *is finite and by* e *alone if* e *is infinite.*

If $p > 2$ then two $\mathbb{F}_p[G]$-modules are isomorphic if and only if their invariants d, e, and Υ are the same, by [MS, Corollary 2]. Thus we see in particular that if $p > 2$, then the arithmetic invariants of J depend only upon the isomorphism type of the $\mathbb{F}_p[G]$-module J.

In the case $p = 2$, we see from [MS, Corollary 2] again that the arithmetic invariants d, e, and Υ determine our module $\mathbb{F}_2[G]$, but two isomorphic $\mathbb{F}_2[G]$-modules may have different arithmetic invariants; see [MS, Corollary 3]. Here is a very simple, concrete example illustrating this possibility. Let K_1/F_1 be a quadratic extension of finite fields of characteristic not 2, $F_2 = \mathbb{R}((t))$ be a field of power series with coefficients in real numbers $\mathbb{R}$, and $K_2 = F_2(\sqrt{-1})$. Then both modules $K_1^\times/K_1^{\times 2}$ and $K_2^\times/K_2^{\times 2}$ are isomorphic to a trivial $\mathbb{F}_2[G]$-module $\mathbb{F}_2$, but their arithmetic invariants (d_i, e_i, Υ_i) are $(0,1,1)$ for $i = 1$ and $(2,0,0)$ for $i = 2$.

1. Notation and Strategy

In all that follows F denotes a field, $F^\times = F \setminus \{0\}$ the multiplicative group of F, p a prime number, and $F^\times/F^{\times p}$ the group of pth-power classes of F. For each $f \in F^\times$ we denote by $[f]$ the class of f in $F^\times/F^{\times p}$. For each subset A of $F^\times$ we denote by $[A]$ the set of classes $\{[a] \mid a \in A\}$ and by $\langle [A] \rangle$ the subgroup of $F^\times/F^{\times p}$ generated by $[A]$.

We denote by ξ_p a primitive pth root of unity in F. (Some fields will be assumed to contain such a primitive pth root; for the other fields in this paper, we will prove that a primitive pth root is contained in the field.) Observe that our assumption that there exists a primitive pth root of unity implies that $\operatorname{char}(F) \neq p$.

For a Galois extension K/F, $\operatorname{Gal}(K/F)$ denotes the Galois group and $N_{K/F}$ denotes the norm map from K to F. We denote by F^s the separable closure of F and G_F the absolute Galois group $\operatorname{Gal}(F^s/F)$. As usual, $H^i(G_F, \mathbb{F}_p)$ are Galois cohomology groups of F with coefficients in $\mathbb{F}_p$. Since all absolute Galois groups will be pro-p-groups, all considered $\mathbb{F}_p$ modules are trivial. Finally, let $|B|$ be the cardinal number of a set B.

First observe that the conditions on d, e, and Υ listed in our theorem above are necessary:

(1) If $\Upsilon = 0$, then $\xi_p \notin N_{K/F}(K^\times)$ and hence
$$d = \dim_{\mathbb{F}_p} F^\times/N_{K/F}(K^\times) \geq 1;$$
(2) If $p > 2$ and $K = F(\sqrt[p]{a})$ for a suitable $a \in F^\times \setminus F^{\times p}$, then $a = N_{K/F}(\sqrt[p]{a})$ and hence
$$e = \dim_{\mathbb{F}_p} N_{K/F}(K^\times) > 0.$$
(3) If $p = 2$, $\Upsilon = 1$, and $K = F(\sqrt{a})$ for a suitable $a \in F^\times \setminus F^{\times 2}$, then $-1 \in N_{K/F}(K^\times)$ since $\Upsilon = 1$. Consequently $a \in N_{K/F}(K^\times)$, and thus $1 \leq e$.

Therefore in order to prove Theorem 1 when $p > 2$, it is sufficient to show, for each cardinal numbers d, e as above, for each $\Upsilon \in \{0, 1\}$, and for each prime number $p > 2$, the existence of a field F such that:

- F contains a primitive pth root ξ_p;
- $F^\times/F^{\times p}$ decomposes intro a direct sum of subgroups
$$F^\times/F^{\times p} = D \oplus \langle [a] \rangle \oplus E,$$
where $\dim_{\mathbb{F}_p}(\langle [a] \rangle \oplus E) = e$ and, setting $K = F(\sqrt[p]{a})$,
  (1) $[N_{K/F}(K^\times)] = \langle [a] \rangle \oplus E$;
  (2) $\dim_{\mathbb{F}_p}(F^\times/N_{K/F}(K^\times)) = \dim_{\mathbb{F}_p} D = d$; and
  (3) $\Upsilon = 0$ if and only if $\xi_p \notin N_{K/F}(K^\times)$.

In the case $p = 2$ and $\Upsilon = 1$ we use the same conditions as above, and if $p = 2$ and $\Upsilon = 0$ we require instead that $e = \dim_{\mathbb{F}_2} E$ and

$d = \dim_{\mathbb{F}_2}(D \oplus \langle [a] \rangle)$. The latter condition is imposed because $-1 \notin N_{F(\sqrt{a})/F}(F(\sqrt{a})^\times)$ if and only if $a \notin N_{F(\sqrt{a})/F}(F(\sqrt{a})^\times)$.

Our strategy is to interpret the required conditions on $F^\times/F^{\times p}$ above in terms of Galois cohomology. We then observe that these conditions are satisfied if G_F is a free product, in the category of pro-p-groups, of suitable pro-p-groups G_1 and G_2, and finally we use the very nice theorem proved by Efrat and Haran which guarantees the existence of a field with G_F above. This is one of the key results used in our paper.

Theorem 2. *(Efrat-Haran; see* [EH, Proposition 1.3]*) Let $F_1, \ldots, F_n$ be fields of equal characteristic such that $G_{F_1}, \ldots, G_{F_n}$ are pro-p-groups. Then there exists a field F of the same characteristic such that*

$$G_F \cong G_{F_1} \star \cdots \star G_{F_n},$$

where the product is free in the category of pro-p-groups.

In order to apply this theorem, we show the existence of the fields F_1 and F_2 such that G_{F_1} and G_{F_2} are prescribed Galois groups G_1 and G_2. We use the techniques of henselian valuations and formal power series to construct fields F_1 and F_2.

2. Lemmas

2.1. Valued fields F_1 with prescribed residue field F_0 and valuation group Γ.

Let v be a valuation on a field F_1, written additively. Then we denote by A_v the valuation ring $\{f \in F_1 \mid v(f) \geq 0\}$; by M_v the unique maximal ideal $\{f \in A_v \mid v(f) > 0\}$ of A_v; by F_v the residue field A_v/M_v of v; by Γ the valuation group $v(F_1^\times)$ of v; and by U the group $A_v \setminus M_v$ of units of v.

The following lemma is well known and we shall omit its straightforward proof.

Lemma 1. *Let F_1 be a valued field with valuation v, valuation group $\Gamma = v(F_1^\times)$, and group of units U. For each prime $p \neq \operatorname{char}(F_1)$ there exists an isomorphism*

$$\varphi : F_1^\times/F_1^{\times p} \longrightarrow U/U^p \oplus \Gamma/p\Gamma.$$

In particular

$$\dim_{\mathbb{F}_p} F_1^\times/F_1^{\times p} = \dim_{\mathbb{F}_p} U/U^p + \dim_{\mathbb{F}_p} \Gamma/p\Gamma.$$

It is well-known that for each field F_0 and for each totally ordered abelian group Γ, there exists a field F_1 with a valuation $v : F_1 \to \Gamma \cup \{\infty\}$ such that the residue field F_v is isomorphic to F_0 and the valuation group is Γ.

In order to construct such a field, set

$$F_1 = F_0((\Gamma)) := \{f : \Gamma \to F_0 \mid \operatorname{supp}(f) \text{ is well-ordered}\}.$$

Thus a typical element $f \in F_1$ can be written as a formal sum $f = \sum_{g\in\Gamma} a_g t^g$ such that the set $\operatorname{supp}(f) := \{g \in G \mid a_g \neq 0\}$ is a well-ordered subset of G. The valuation v on f is defined as: $v(0) = \infty$ and $v(f) = \min \operatorname{supp}(f)$ for $f \neq 0$. An important property of the valued field F_1 as above is the fact that it is henselian. (See for example [Rib, (1.3)].) In what follows we will identify F_v with F_0. We will also assume that char $F_0 \neq p$.

We will be particularly interested in controlling the pth-power classes of such a field. To do so, we choose particular groups Γ for our valuation groups. These groups will be direct sums of

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0; \text{ if } a \neq 0 \text{ then } (a, b) = 1, p \nmid b \right\}.$$

Observe that $\mathbb{Z}_{(p)}$ is the valuation ring of a p-adic valuation on $\mathbb{Q}$. Let I be any non-empty, well-ordered set. Then set

$$\Gamma = \mathbb{Z}_{(p)}^{(I)} := \left\{ \gamma : I \to \mathbb{Z}_{(p)} \;\middle|\; |\operatorname{supp}(\gamma)| < \infty \right\}.$$

Thus Γ is a direct sum of $|I|$ copies of $\mathbb{Z}_{(p)}$. Observe that $\mathbb{Z}_{(p)}$ carries a natural ordering induced from $\mathbb{Q}$, and then we may order Γ lexicographically, as follows. Let $\gamma_1 \neq \gamma_2 \in \Gamma$. Then $\gamma_1 < \gamma_2$ if and only if $\gamma_1(i) < \gamma_2(i)$ for the least element $i \in I$ such that $\gamma_1(i) \neq \gamma_2(i)$. Then Γ is a linearly ordered abelian group. Recall that each non-empty set can be well-ordered. (See [La, Appendix 2, Theorem 4.1].)

We choose Γ as above because $G_{F_0((\Gamma))}$ will be pro-p (see Lemma 3 below) and because we may control the pth-power classes with the following lemma. This well-known lemma follows from Lemma 1 and the fact that the valued field F_1 is henselian. It is also an immediate consequence of [W, Lemma 1.4]. Therefore we shall omit its proof.

Lemma 2. *Let $F_1 = F_0((\Gamma))$ as above. Then*

$$\begin{aligned}\dim_{\mathbb{F}_p} F_1^\times/F_1^{\times p} &= \dim_{\mathbb{F}_p} F_0^\times/F_0^{\times p} + \dim_{\mathbb{F}_p} \Gamma/p\Gamma \\ &= \dim_{\mathbb{F}_p} F_0^\times/F_0^{\times p} + |I|.\end{aligned}$$

Finally, we record a criterion for G_{F_1} being pro-p:

Lemma 3. *Let* $F_1 = F_0((\Gamma))$ *as above with* $\mathrm{char}(F_0) = 0$ *and* G_{F_0} *pro-p. Then* G_{F_1} *is pro-p as well.*

Proof. From basic valuation theory, nicely summarized in [K, pages 3 and 4], and the fact that F_1 above is henselian,

$$G_{F_1} \cong T \rtimes G_{F_0},$$

where the action of G_{F_0} on T is uniquely determined by the cyclotomic character mapping G_{F_0} into a group of automorphisms of a group of roots of unity contained in F_0^s, and $T \cong \mathbb{Z}_p^I$, the topological product of $|I|$ copies of $\mathbb{Z}_p$. In particular, if G_{F_0} is a pro-p-group, so is G_{F_1}. □

2.2. $H^2(G_{F_1}, \mathbb{F}_p)$ for henselian valued fields F_1.

Now we study $H^2(G_{F_1}, \mathbb{F}_p)$ for our henselian valued fields F_1. The next lemma, taken from [W], will be used in the proof of Theorem 1 to show that norm groups of cyclic p-extensions of F_1 are not too large.

Suppose that F_1 is a field endowed with a henselian valuation v with valuation group $\Gamma = v(F_1^\times)$. Let F_1^{nr} denote the maximal unramified extension of F_1 in its separable closure F_1^s. Then $G_{F_0} \cong G_{F_1}/\operatorname{Gal}(F_1^s/F_1^{nr})$. Therefore, after identifying these groups, we have the inflation map

$$\inf = \inf{}_{F_0}^{F_1} : H^*(G_{F_0}, \mathbb{F}_p) \longrightarrow H^*(G_{F_1}, \mathbb{F}_p).$$

(See [W, page 483].)

Moreover, from basic Kummer theory we have the canonical isomorphism

$$\varphi_F : F^\times/F^{\times p} \longrightarrow H^1(G_F, \mathbb{F}_p),$$

as well as the corresponding canonical isomorphisms φ_{F_i}, $i = 1, 2$. We will denote by $(f)_F$ or $(f_i)_{F_i}$ the images $\varphi_F([f])$ or $\varphi_{F_i}([f_i])$. If the context is clear we will omit the subscript.

Assume next that $\{\pi_j,\ j \in \mathcal{J}\}$ is a set of elements of $F_1^\times$ such that their images in $\Gamma/p\Gamma$ form a basis of $\Gamma/p\Gamma$ over $\mathbb{F}_p$. Then we have the following lemma, obtained as a special case of a theorem of Wadsworth.

Lemma 4. [W, Theorem 3.6, page 483]. *Let* F_1 *and* F_0 *be as above. Then*

$$H^2(G_{F_1}, \mathbb{F}_p) = \inf(H^2(G_{F_0}, \mathbb{F}_p)) \oplus_{j \in \mathcal{J}} \left(\inf(H^1(G_{F_0}, \mathbb{F}_p)) \cup (\pi_j)\right) \oplus_{\{j_1, j_2\} \subset \mathcal{J},\ j_1 \neq j_2} \left((\pi_{j_1}) \cup (\pi_{j_2})\right).$$

Moreover, for each $j \in \mathcal{J}$,

$$\inf(H^1(G_{F_0}, \mathbb{F}_p)) \cong \inf(H^1(G_{F_0}, \mathbb{F}_p)) \cup (\pi_j)$$

and for each $j_1, j_2 \in \mathcal{J}$ such that $j_1 \neq j_2$, we have $(\pi_{j_1}) \cup (\pi_{j_2}) \neq 0$.

Note that in the last summand of Lemma 4 the sum ranges over subsets $\{j_1, j_2\}, j_1 \neq j_2$ of $\mathcal{J}$ and a choice between $(\pi_{j_1}) \cup (\pi_{j_2})$ and $(\pi_{j_2}) \cup (\pi_{j_1})$ is arbitrary but fixed.

2.3. **Residue fields F_0 with prescribed absolute Galois group.**

In our construction of F we choose a residue field F_0 depending on Υ and p. If $\Upsilon = 1$ we will simply put $F_0 = \mathbb{C}$, but when $\Upsilon = 0$ we require some special properties of F_0. In particular, in order that our cyclic extension $K = F(\sqrt[p]{a})$ have the desired invariant $\Upsilon = 0$, we require that K does not embed in a cyclic Galois extension L over F with degree $[L : F] = p^2$, for this is equivalent to $\xi_p \notin N_{K/F}(K^\times)$ by [A, Theorem 3].

To ensure that this nonembeddability condition holds, as well as to ensure that a certain nonabelian group of order p^3 does not occur as a Galois group over the field, we choose residue fields F_0 with absolute Galois groups taking a special form, and it is also convenient to require that $|F_0^\times / F_0^{\times p}|$ is small. As it turns out, we may choose some suitable algebraic infinite extension of $\mathbb{Q}$. Finitely generated pro-p-absolute Galois groups over $\mathbb{Q}$ and more generally any global field, were nicely classified in [E2]. (See also [E1] and [JP] for related results and techniques.)

The extensions we will need for $p > 2$ are given in the following

Lemma 5. [E2, page 84] *For each prime $p > 2$ there exists an algebraic extension $F_{0,p}$ of $\mathbb{Q}$ such that*

$$G_{F_{0,p}} = \langle \sigma, \tau \mid \sigma\tau\sigma^{-1} = \tau^{p+1} \rangle_{\text{pro-}p}$$

where the presentation is in the category of pro-p-groups.

Observe that the maximal abelian extension $F_{0,p}^{ab}$ of $F_{0,p}$ has $G_{F_{0,p}}^{ab} := \mathrm{Gal}(F_{0,p}^{ab}/F_{0,p})$ equal to

$$G_{F_{0,p}}^{ab} \cong \langle \bar{\sigma}, \bar{\tau} \mid \bar{\tau}^p = 1 \rangle = \mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$$

for all primes $p > 2$.

2.4. **Field arithmetic and free pro-p products.**

In this section we collect lemmas giving information about a field F derived from the structure of G_F, especially when G_F is a free pro-p product of two pro-p groups G_{F_1} and G_{F_2}.

First we record a lemma detecting the presence of primitive pth roots of unity in a field F, based only on the structure of G_F.

Lemma 6. *Suppose that $p > 2$ and that F is a field with $\mathrm{char}(F) \neq p$ and G_F pro-p. Then $\xi_p \in F^\times$.*

Proof. Because $\mathrm{char}(F) \neq p$, there exists a primitive pth root ξ_p of unity in F^s. If $\xi_p \in F^s \setminus F$ then $F(\xi_p)/F$ is a nontrivial Galois extension of degree $[F(\xi_p) : F] < p$. Therefore G_F has a nontrivial finite quotient of order coprime with p. This contradicts our assumption that G_F is a pro-p-group. Hence $\xi_p \in F^\times$ as asserted. □

Now suppose that $G_F = G_{F_1} \star G_{F_2}$ for pro-p absolute Galois groups G_F, G_{F_1}, and G_{F_2}, where the free product is taken in the category of pro-p-groups. From [N, (4.3) Satz] we see that the restriction homomorphism

$$\mathrm{res} : H^1(G_F, \mathbb{F}_p) \longrightarrow H^1(G_{F_1}, \mathbb{F}_p) \oplus H^1(G_{F_2}, \mathbb{F}_p) \qquad (1)$$

is an isomorphism. Now given $(f)_F$ in $H^1(G_F, \mathbb{F}_p)$, we denote the image $\mathrm{res}(f)_F$ by

$$\mathrm{res}(f)_F = (f)_{G_{F_1}} \oplus (f)_{G_{F_2}}.$$

This notation distinguishes, then, between $(f)_{F_1}$, which denotes $\varphi_{F_1}(f)$ for $f \in F_1^\times$, and $(f)_{G_{F_1}}$, which denotes the projection of $\mathrm{res}\,\varphi_F(f)$ onto the first summand.

One way of interpreting this restriction map is with the following

Lemma 7. *Let $G_F = G_{F_1} \star G_{F_2}$ be pro-p absolute Galois groups of fields containing a pth root of unity, and suppose that we have the following sequence:*

$$G_F \xrightarrow{\mathrm{can}} G_{F_1} \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Here the canonical map can *is an identity on G_{F_1} and contains G_{F_2} in its kernel.*

Then the right-hand surjection and the composed surjection correspond to fields $K_1 = F_1(\sqrt[p]{a_1})$ and $K = F(\sqrt[p]{a})$, respectively, where $(a)_{G_{F_1}} = (a_1)_{F_1}$ and $(a)_{G_{F_2}} = 0$.

Proof. The surjections are continuous homomorphisms, hence elements of $H^1(G_{F_1}, \mathbb{F}_p)$ and $H^1(G_F, \mathbb{F}_p)$, respectively, and the right-hand surjection is clearly the restriction of the composed surjection. The remainder follows by Kummer theory. □

Lemma 8. *Let $G_F = G_{F_1} \star G_{F_2}$ be pro-p absolute Galois groups and suppose that $(a)_F$ and $(b)_F$ satisfy $(a)_{G_{F_1}} = (b)_{G_{F_2}} = 0$. Then*

$$(a)_F \cup (b)_F = 0 \in H^2(G_F, \mathbb{F}_p).$$

The lemma follows from [N, (4.1) Satz] and from [Ris, Prop. 7.3, page 191]. However, we prove our lemma by translating the cup products into obstructions to basic Galois embedding problems, yielding an interesting Galois-theoretic variant of the proof.

Proof. If $(a) = 0$ or $(b) = 0$, we are done. Otherwise, the conditions $(a)_{G_{F_1}} = (b)_{G_{F_2}} = 0$ imply that (a) and (b) are linearly independent in $H^1(G_F, \mathbb{F}_p)$.

Now let H_{p^3} be the Heisenberg group of order p^3:

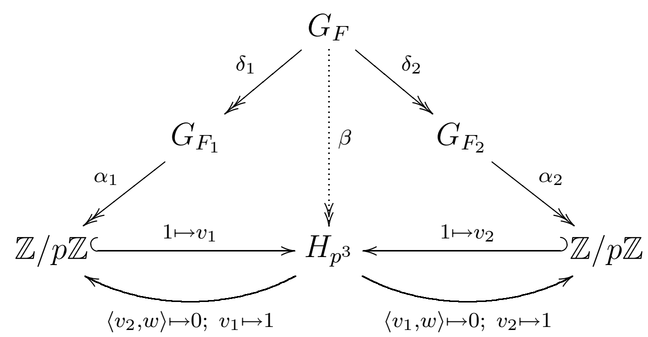
$$H_{p^3} = \langle v_1, v_2, w \mid v_1^p = v_2^p = w^p = 1, v_2 v_1 = w v_1 v_2, \\ [v_1, w] = [v_2, w] = 1 \rangle$$

In the case $p = 2$, H_8 is the familiar dihedral group D_4.

By [M, Corollary, page 523 and Theorem 3(A)], if (a) and (b) are linearly independent, then $(a) \cup (b) = 0$ if and only if H_{p^3} is the Galois group $\mathrm{Gal}(M/F)$ of a Galois extension M of F containing $F(\sqrt[p]{a}, \sqrt[p]{b})$ in such a way that

$$H_{p^3}/\langle v_1, w\rangle = \mathrm{Gal}(F(\sqrt[p]{a})/F) \text{ and } H_{p^3}/\langle v_2, w\rangle = \mathrm{Gal}(F(\sqrt[p]{b})/F).$$

Now consider the commutative diagram



Let $a_2 \in F_2^\times$ and $b_1 \in F_1^\times$ satisfy $(a_2)_{F_2} = (a)_{G_{F_2}}$ and $(b_1)_{F_1} = (b)_{G_{F_1}}$. Then set $K_1 = F_1(\sqrt[p]{b_1})$ and $K_2 = F_2(\sqrt[p]{a_2})$; these are $\mathbb{Z}/p\mathbb{Z}$-extensions of F_1 and F_2, respectively. We may then identify the left-hand $\mathbb{Z}/p\mathbb{Z}$ in the diagram with $\mathrm{Gal}(K_1/F_1)$ so that α_1 is the surjection of Galois theory. Similarly, the right-hand $\mathbb{Z}/p\mathbb{Z}$ may be identified with $\mathrm{Gal}(K_2/F_2)$ with α_2 the surjection of Galois theory. Finally, the topmost surjections δ_1 and δ_2 are canonical.

By Lemma 7, the surjections $\delta_1\alpha_1$ and $\delta_2\alpha_2$ correspond to fields $F(\sqrt[p]{b})$ and $F(\sqrt[p]{a})$, respectively. Now because $G_F = G_{F_1} \star G_{F_2}$, there exists a homomorphism $\beta : G_F \to H_{p^3}$, and because v_1 and v_2 generate H_{p^3}, β is a surjection.

Hence H_{p^3} is a Galois group over F corresponding to a normal subgroup H of G_F. Consider the smallest normal subgroup H_1 of G_F containing H and G_{F_2}. Then by the diagram, G_F/H_1 is the left-hand $\mathbb{Z}/p\mathbb{Z}$, which corresponds to $F(\sqrt[p]{b})$, and H_1/H is $\langle v_2, w\rangle$. Now consider the smallest normal subgroup H_2 of G_F containing H and G_{F_1}. Then by the diagram, G_F/H_2 is the right-hand $\mathbb{Z}/p\mathbb{Z}$, which corresponds to $F(\sqrt[p]{a})$, and H_2/H is $\langle v_1, w\rangle$.

Hence $(a) \cup (b) = 0$. □

Finally, we close with with a companion to Lemma 7. In Lemma 9 below, π denotes the canonical homomorphism of G to G_1 which is an identity on G_1, and is trivial on G_2.

Lemma 9. *Let $G = G_1 \star G_2$ be a free product of G_1 and G_2 in the category of pro-p-groups. Suppose that $A \cong \mathbb{Z}/p\mathbb{Z}$ is a factor group of G_1 such that the surjection $G_1 \to \mathbb{Z}/p\mathbb{Z}$ does not factor through $\mathbb{Z}/p^2\mathbb{Z}$. Then the following commutative diagram cannot occur:*

$$\begin{array}{ccc} G & \xrightarrow{\ \pi\ } & G_1 \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^2\mathbb{Z} & \longrightarrow & A. \end{array}$$

Proof. Suppose that contrary to our statement, such a diagram as the above exists. Then by passing to quotients by commutator subgroups we obtain

$$\begin{array}{ccc} G^{ab} & \xrightarrow{\pi^{ab}} & G_1^{ab} \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\gamma} \\ \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{\beta} & A. \end{array}$$

But $G^{ab} \cong G_1^{ab} \times G_2^{ab}$ and the canonical surjection onto G_1^{ab} is given by the projection map. Let δ be a splitting map of the projection map. Then $\gamma = \beta\alpha\delta$, contradicting the hypothesis. □

3. Proof of the Theorem

First we define fields F_0, F_1, F_2, and F using our given cardinal numbers d, e, and Υ, as well as the prime number p. Then we define the cyclic Galois extension K/F of degree p and check that the arithmetic invariants of K/F coincide with d, e, and Υ.

3.1. Constructing F_0, F_1, F_2, and F.

If $\Upsilon = 1$ then let $F_0 = \mathbb{C}$. If $\Upsilon = 0$ and $p = 2$, let $F_0 = \mathbb{R}$. (See Proposition 1 for alternative choices in these two cases.) If $\Upsilon = 0$ and $p > 2$ then let $F_{0,p}$ be the algebraic extension of $\mathbb{Q}$ of Lemma 5. In the first two cases we see trivially that $\xi_p \in F_0$, and in the last case $\xi_p \in F_0$ by Lemma 6. Observe that

$$\dim_{\mathbb{F}_p} F_0^\times / F_0^{\times p} = \begin{cases} 0, \text{ if } \Upsilon = 1; \\ 1, \text{ if } \Upsilon = 0, \ p = 2; \\ 2, \text{ if } \Upsilon = 0, \ p > 2. \end{cases} \tag{2}$$

We next construct the field F_1. Because $\Upsilon = 0$ implies $1 \le d$, for either choice of $\Upsilon \in \{0, 1\}$ there exists a well-ordered set I_1 such that $|I_1| + 1 = d + 2\Upsilon$. Let $\Gamma_1 = \mathbb{Z}_{(p)}^{(I_1)}$ be a direct sum of $|I_1|$ copies of $\mathbb{Z}_{(p)}$. Then Γ_1 is a linearly ordered abelian group. Finally set $F_1 := F_0((\Gamma_1))$. From Lemmas 2 and 3 it follows that G_{F_1} is a pro-p-group and

$$\dim_{\mathbb{F}_p} F_1^\times / F_1^{\times p} = \dim_{\mathbb{F}_p} F_0^\times / F_0^{\times p} + |I_1|.$$

Hence

$$\dim_{\mathbb{F}_p} F_1^\times / F_1^{\times p} = \begin{cases} d + 1, & \text{if } \Upsilon = 1; \\ d, & \text{if } \Upsilon = 0, \ p = 2; \\ d + 1, & \text{if } \Upsilon = 0, \ p > 2. \end{cases} \tag{3}$$

Similarly, we construct F_2 as follows. Because $p > 2$ and also $p = 2$ and $\Upsilon = 1$ implies $e > 0$, there exists a well-ordered set I_2 such that $1 + |I_2| = e$ in either of the cases $p > 2$ or $\Upsilon = 1$, $p = 2$, and $|I_2| = e$ in the case $\Upsilon = 0$, $p = 2$. Then again $\Gamma_2 = \mathbb{Z}_{(p)}^{(I_2)}$ is a linearly ordered abelian group. We set $F_2 := \mathbb{C}((\Gamma_2))$. Then from [K, pages 3 and 4] it follows that $G_{F_2} \cong \mathbb{Z}_p^{I_2}$, the topological product of $|I_2|$ copies of $\mathbb{Z}_p$. In particular

$$e = \begin{cases} \dim_{\mathbb{F}_p} F_2^\times / F_2^{\times p} + 1, & \text{if } p > 2 \text{ or } p = 2 \text{ and } \Upsilon = 1; \\ \dim_{\mathbb{F}_p} F_2^\times / F_2^{\times p}, & \text{if } p = 2,\ \Upsilon = 0. \end{cases} \tag{4}$$

From Theorem 2 we see that there exists a field F of characteristic zero, such that $G_F = G_{F_1} \star G_{F_2}$ is a free product of G_{F_1} and G_{F_2} in the category of pro-p-groups. In particular G_F is again a pro-p-group, and from Lemma 6 we see that F contains a primitive pth root of unity.

3.2. **Constructing K/F.**

We define the cyclic extension K/F of degree p as $K = F(\sqrt[p]{a})$ where $[a] \in F^\times / F^{\times p}$ is chosen via the isomorphism (1).

If $\Upsilon = 1$ then let $(a_1)_{F_1}$ be any nontrivial element in $H^1(G_{F_1}, \mathbb{F}_p)$, which is possible since $1 \leq \dim_{\mathbb{F}_p} H^1(G_{F_1}, \mathbb{F}_p) = d + 1$. Let $(a_2)_{F_2} = 0$ in $H^2(G_{F_2}, \mathbb{F}_p)$.

Now suppose $\Upsilon = 0$ and $p > 2$. We denote the fixed field of the factor $\mathbb{Z}_p$ in $G_{F_0}^{ab} \cong \mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$ acting on a maximal abelian extension F_0^{ab} of F_0 as $K_0 := F_0(\sqrt[p]{b})$. (See the discussion following Lemma 5.) Because $F_0^\times / F_0^{\times p}$ is naturally isomorphic to a subgroup of $F_1^\times / F_1^{\times p}$, we may set $(a_1)_{F_1} = \inf(b)_{F_0} \neq 0$ in $H^1(G_{F_1}, \mathbb{F}_p)$ and $(a_2)_{F_2} = 0$ in $H^2(G_{F_2}, \mathbb{F}_p)$.

Finally assume that $\Upsilon = 0$ and $p = 2$. We set $(a_1)_{F_1} = (-1)_{F_1} \neq 0$ in $H^1(G_{F_1}, \mathbb{F}_2)$ and $(a_2)_{F_2} = 0$ in $H^2(G_{F_2}, \mathbb{F}_2)$.

Now by (1) there exists $a \in F^\times$ such that $(a)_F \neq 0$ and $(a)_{G_{F_i}} = (a_i)_{F_i}$, $i = 1, 2$. Since we have already determined that $\xi_p \in F^\times$, we see that $K = F(\sqrt[p]{a})$ is a cyclic extension of degree p. Hence it remains to show that the arithmetic invariants $d(K/F)$, $e(K/F)$, and $\Upsilon(K/F)$ coincide with the prescribed cardinal numbers d, e, and Υ respectively.

3.3. **Determining $d(K/F)$ and $e(K/F)$ via annihilators.**

We first observe some relationships among cup products of elements in $H^1(G_F, \mathbb{F}_p)$. Recall that Lemma 8 tells us that if $c_1, c_2 \in F^\times$ with $(c_1)_{G_{F_1}} = (c_2)_{G_{F_2}} = 0$ then

$$(c_1)_F \cup (c_2)_F = 0 \in H^2(G_F, \mathbb{F}_p). \tag{5}$$

Moreover, recall that by [N, Satz 4.1]

$$H^2(G_F, \mathbb{F}_p) \cong H^2(G_{F_1}, \mathbb{F}_p) \times H^2(G_{F_2}, \mathbb{F}_p),$$

where the isomorphism is induced by the restriction maps

$$\mathrm{res}_i : H^2(G_F, \mathbb{F}_p) \to H^2(G_{F_i}, \mathbb{F}_p), i = 1, 2.$$

Because these restriction maps commute with cup product maps ([Ris, Proposition 7.3, page 191]), we see that if $c_1, c_2 \in F^\times$ such that $(c_1)_{G_{F_2}} = (c_2)_{G_{F_2}} = 0$ in $H^2(G_{F_2}, \mathbb{F}_p)$ then

$$(c_1)_F \cup (c_2)_F \neq 0 \quad \text{iff} \quad (c_1)_{G_{F_1}} \cup (c_2)_{G_{F_1}} \neq 0, \tag{6}$$

where the first cup product lies in $H^1(G_F, \mathbb{F}_p)$ and the second cup product lies in $H^1(G_{F_1}, \mathbb{F}_p)$. By symmetry the analogous statement with F_1 and F_2 exchanged holds as well.

Now we calculate $e(K/F)$. We adopt the following notation for an annihilator of $\phi \in H^1(G_F, \mathbb{F}_p)$:

$$\mathrm{ann}_{F_1} \phi := \{\eta \in H^1(G_F, \mathbb{F}_p) \mid \eta \cup \phi = 0\}.$$

For $x \in F^\times$ we have $x \in N_{K/F}(K^\times)$ if and only if $(x)_F \cup (a)_F = 0$ in $H^2(G_F, \mathbb{F}_p)$. Therefore, using (5) and (6) with the fact that in every case $(a)_{G_{F_2}} = 0$,

$$\begin{aligned} e(K/F) &= \dim_{\mathbb{F}_p} N(K^\times)/F^{\times p} \\ &= \dim_{\mathbb{F}_p} \{(x)_F \in H^1(G_F, \mathbb{F}_p) \mid (a)_F \cup (x)_F = 0\} \\ &= \dim_{\mathbb{F}_p} \{(y)_{F_1} \in H^1(G_{F_1}, \mathbb{F}_p) \mid (a)_{G_{F_1}} \cup (y)_{F_1} = 0\} \\ &\quad + \dim_{\mathbb{F}_p} H^1(G_{F_2}, \mathbb{F}_p) \\ &= \dim_{\mathbb{F}_p} \mathrm{ann}_{F_1} (a)_{G_{F_1}} + \dim_{\mathbb{F}_p} F_2^\times / F_2^{\times p}. \end{aligned}$$

If $\Upsilon = 1$ then $H^1(G_{F_0}, \mathbb{F}_p) = 0$, and so by Lemma 4 we have $\dim_{\mathbb{F}_p} \mathrm{ann}_{F_1} (a)_{G_{F_1}} = 1$.

If $p > 2$ and $\Upsilon = 0$ then by Lemma 4,

$$\dim_{\mathbb{F}_p} \mathrm{ann}_{F_1} (a)_{G_{F_1}} = \dim_{\mathbb{F}_p} \mathrm{ann}_{F_0} (b)_{F_0},$$

where b was chosen so that $K_0 = F_0(\sqrt[p]{b})$ was the fixed field of the factor $\mathbb{Z}_p$ in $G_{F_0}^{ab}$. Now because $(b)_{F_0} \cup (b)_{F_0} = 0$ as an identity in $H^2(G_F, \mathbb{F}_p)$ for $p > 2$,

$$1 \leq \dim_{\mathbb{F}_p} \operatorname{ann}_{F_0}(b)_{F_0} \leq 2.$$

On the other hand, let $c \in F^\times \setminus F^{\times p}$ be defined so that $F_0(\sqrt[p]{c})$ is contained in the fixed field of the factor $\mathbb{Z}/p\mathbb{Z}$ in $G_{F_0}^{ab}$. Then by (2), $\{(b)_{F_0}, (c)_{F_0}\}$ spans $H^1(G_{F_0}, \mathbb{F}_p)$. Furthermore, since by Lemma 5, H_{p^3} is not a quotient of $G_{F_0,p}$, $(b)_{F_0} \cup (c)_{F_0} \neq 0$ by [M, Corollary, page 523 and Theorem 3(A)]. We conclude that $\dim_{\mathbb{F}_p} \operatorname{ann}_{F_0}(b)_{F_0} = 1$.

Finally, if $p = 2$ and $\Upsilon = 0$ then again by Lemma 4

$$\dim_{\mathbb{F}_2} \operatorname{ann}_{F_1}(a)_{G_{F_1}} = \dim_{\mathbb{F}_2} \operatorname{ann}_{F_0}(-1)_{F_0}.$$

As $F_0 = \mathbb{R}$, $\dim_{\mathbb{F}_2} F_0^\times / F_0^{\times 2} = 1$ and $(-1)_{\mathbb{R}} \cup (-1)_{\mathbb{R}} \neq 0$, yielding $\dim_{\mathbb{F}_2} \operatorname{ann}_{F_1}(a)_{G_{F_1}} = 0$.

Combining our results with (4), we have that $e(K/F) = e$.

Now we turn to a similar calculation of $d(K/F)$. Again using (5) and (6) with the fact that in every case $(a)_{G_{F_2}} = 0$,

$$\begin{aligned} d(K/F) &= \dim_{\mathbb{F}_p}(H^1(G_F, \mathbb{F}_p)/\operatorname{ann}_F(a)_F) \\ &= \dim_{\mathbb{F}_p}(H^1(G_{F_1}, \mathbb{F}_p)/\operatorname{ann}_{F_1}(a)_{G_{F_1}}) \\ &= d. \end{aligned}$$

For this last equality we use (3) together with calculations of the dimension of $\operatorname{ann}_{F_1}(a)_{G_{F_1}}$ already achieved. Hence $d(K/F) = d$ in all cases.

3.4. **Determining Υ via quotients of G_F.**

It remains to show that $\Upsilon(K/F) = \Upsilon$. First consider the case $\Upsilon = 1$. Since $F_0 = \mathbb{C}$, ξ_p is a pth power in F_1, and $F_1(\sqrt[p]{a})$ embeds in a $\mathbb{Z}/p^2\mathbb{Z}$-extension $F_1(\sqrt[p^2]{a})$ of F_1. Then the surjection $G_{F_1} \to \operatorname{Gal}(K_1/F_1)$ factors through $\mathbb{Z}/p^2\mathbb{Z}$. Following the surjection with the canonical surjection $G_F \to G_{F_1}$, we see that $\mathbb{Z}/p^2\mathbb{Z}$ is a factor group of G_F. Moreover, by Lemma 7, the surjection $G_F \to \mathbb{Z}/p\mathbb{Z}$ corresponds to K. Hence K/F embeds in a $\mathbb{Z}/p^2\mathbb{Z}$-extension of F. By [A, Theorem 3], $\xi_p \in N_{K/F}(K^\times)$. Therefore $\Upsilon(K/F) = 1 = \Upsilon$.

Now consider the case $\Upsilon = 0$ and $p > 2$. Because $K_0 = F_0(\sqrt[p]{b})$ does not embed in a $\mathbb{Z}/p^2\mathbb{Z}$-extension of F_0, $\xi_p \notin N_{K_0/F_0}(K_0^\times)$. (See 3.2 for the definition of K_0.) Hence $(b)_{F_0} \cup (\xi_p)_{F_0} \neq 0$ in $H^1(G_{F_0}, \mathbb{F}_p)$, and, by Lemma 4, $(\inf(b)) \cup (\xi_p)_{F_1} \neq 0$ in $H^1(G_{F_1}, \mathbb{F}_p)$ as well. Choose $b_1 \in F_1^\times$ so that $(b_1)_{F_1} = \inf(b)_{F_0}$ and set $K_1 = F_1(\sqrt[p]{b_1})$. Then $\xi_p \notin N_{K_1/F_1}(K_1^\times)$ and by [A, Theorem 3] the field extension K_1/F_1 does not embed in a $\mathbb{Z}/p^2\mathbb{Z}$-extension of F_1. Therefore the surjection $G_{F_1} \to \mathrm{Gal}(F_1(\sqrt[p]{b})/F_1)$ does not factor through $\mathbb{Z}/p^2\mathbb{Z}$. From Lemmas 7 and 9 we see that surjection $G_F \to \mathrm{Gal}(K/F)$ does not factor through $\mathbb{Z}/p^2\mathbb{Z}$. Again by [A, Theorem 3] we conclude that $\xi_p \notin N_{K/F}(K^\times)$ and therefore $\Upsilon(K/F) = 0 = \Upsilon$.

Finally consider the case $\Upsilon = 0$ and $p = 2$. Because $-1 \notin N_{\mathbb{C}/\mathbb{R}}(\mathbb{C})$ from Lemma 4 we conclude that $-1 \notin N_{K_1/F_1}(K_1^\times)$. By [A, Theorem 3] the surjection $G_{F_1} \to \mathrm{Gal}(K_1/F_1)$ does not factor through $\mathbb{Z}/4\mathbb{Z}$. As in the previous case, by Lemmas 7 and 9 we see that K/F does not embed in a $\mathbb{Z}/4\mathbb{Z}$-extension of F. Again by [A, Theorem 3] we see that $-1 \notin N_{K/F}(K^\times)$ and therefore $\Upsilon(K/F) = 0 = \Upsilon$.

Hence we have checked in all cases that $\Upsilon(K/F) = \Upsilon$, and our proof of Theorem 1 is now complete. □

Remark. In [EH, Lemma 1.2 and Proposition 1.3] Efrat and Haran construct some fields with prescribed absolute Galois groups together with some bounds on the transcendence degrees of these fields. These bounds, together with the replacement of $\mathbb{C}$ by an algebraic closure of $\mathbb{Q}$ and of $\mathbb{R}$ by a real-closed algebraic number field R in the case when $p = 2$ and $\Upsilon = 0$ in our proof above, yield the following proposition.

Proposition 1. *Suppose that p is a prime number, and let d, e, and $\Upsilon \in \{0, 1\}$ be cardinal numbers such that if $\Upsilon = 0$ then $1 \leq d$, if $p > 2$ then $1 \leq e$, and if $p = 2$ and $\Upsilon = 1$ then $1 \leq e$. Then there exists a field F containing $\mathbb{Q}(\xi_p)$ and a cyclic Galois extension K of degree p over F such that*

$$e(K/F) = e, \quad d(K/F) = d, \quad \text{and} \quad \Upsilon(K/F) = \Upsilon.$$

Moreover

$$\mathrm{tr.deg}(F/\mathbb{Q}) \leq 1 + \max\{e, d + 1\}.$$

In particular if $d, e \in \mathbb{N} \cup \{0\}$, there exists a Galois cyclic extension K/F of degree p with prescribed invariants d, e, and Υ of finite transcendence degree over its prime field $\mathbb{Q}$.

4. Acknowledgements

We would like to thank the organizers of the MSRI programs on Galois theory and the MSRI staff for giving us the opportunity to meet and to begin our collaboration in the Fall of 1999. We are also grateful to A. Wadsworth for stimulating conversations. The first author is very appreciative of the kind assistance of Ron Hemphill, manager of Ivest Properties Limited (London, Canada), for having provided excellent working conditions.

References

[A] A. Albert. *On cyclic fields.* Trans. Amer. Math. Soc. **37** (1935), 454–462.

[AT] E. Artin and J. Tate. *Class field theory.* Second edition. Redwood City, CA: Addison-Wesley Advanced Book Program, 1990.

[E1] I. Efrat. *Pro-p-Galois groups of algebraic extensions of* $\mathbb{Q}$. J. Number Theory **64** (1997), 84–99.

[E2] ______. *Finitely generated pro-p-absolute Galois groups over global fields.* J. Number Theory **77** (1999), 83–96.

[EH] I. Efrat and D. Haran. *On Galois groups over pythagorean and semi-real closed fields.* Israel J. Math. **85** (1994), no. 1-3, 57–78.

[JP] C. U. Jensen and A. Prestel. *Realization of finitely generated profinite groups by maximal abelian extensions of fields.* J. reine angew. Math. **447** (1994), 201–218.

[K] J. Koenigsmann. *Solvable absolute Galois groups are metabelian.* Invent. Math. **144** (2001), 1–22.

[La] S. Lang. *Algebra.* Revised third edition. Graduate Texts in Mathematics **211**. New York: Springer-Verlag, 2002.

[M] R. Massy. *Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p.* J. Algebra **109** (1987), no. 2, 508–535.

[MS] J. Mináč and J. Swallow. *Galois module structure of pth-power classes of extensions of degree p.* To appear, Israel J. Math.

[N] J. Neukirch. *Freie Produkte pro-endlicher Gruppen und ihre Kohomologie.* Arch. Math. (Basel) **22** (1971), 337–357.

[Rib] P. Ribenboim. *Some examples of valued fields.* J. of Algebra **173** (1995), 668–678.

[Ris] L. Ribes. *Introduction to profinite groups and Galois cohomology.* Queen's Papers in Pure and Applied Mathematics **24**. Kingston, Canada: Queen's University, 1970.

[S] J.-P. Serre. *Local Fields.* Trans. Marvin Jay Greenberg. Graduate Texts in Mathematics **67**. New York-Berlin: Springer-Verlag, 1979.

[W] A. Wadsworth. *p-Henselian fields: K-theory, Galois cohomology, and graded Witt rings.* Pacific J. Math. **105** (1983), 473–496.

Department of Mathematics, Middlesex College, University of Western Ontario, London, Ontario N6A 5B7 CANADA

E-mail address: minac@uwo.ca

Department of Mathematics, Davidson College, Box 7046, Davidson, North Carolina 28035-7046 USA

E-mail address: joswallow@davidson.edu