TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 333, Number 2, October 1992

GALOIS GROUPS OF MAXIMAL p-EXTENSIONS

ROGER WARE

ABSTRACT. Let p be an odd prime and F a field of characteristic different from p containing a primitive pth root of unity. Assume that the Galois group G of the maximal p-extension of F has a finite normal series with abelian factor groups. Then the commutator subgroup of G is abelian. Moreover, G has a normal abelian subgroup with pro-cyclic factor group. If, in addition, F contains a primitive p^2th root of unity then G has generators $\{x, y_i\}_{i\in I}$ with relations $y_iy_j = y_jy_i$ and $xy_ix^{-1} = y_i^{q+1}$ where $q = 0$ or $q = p^n$ for some $n \geq 1$. This is used to calculate the cohomology ring of G, when G has finite rank. The field F is characterized in terms of the behavior of cyclic algebras (of degree p) over finite p-extensions.

In what follows p will be a fixed odd prime and F will be a field of characteristic different from p containing a primitive pth root of unity ω. Let $F(p)$ denote the maximal Galois extension of F whose Galois group $G_F(p) = \mathrm{Gal}(F(p)/F)$ is a pro-p-group. An extension K/F is called a p-extension if $K \subseteq F(p)$. Note that if K/F is a p-extension with $[K : F] = p$ then K/F is Galois and $K = F(\sqrt[p]{d})$, for some $d \in F$.

The cyclic algebra (or "symbol algebra") generated over F by elements u, v, subject to relations $u^p = a$, $v^p = b$, and $uv = \omega vu$, will be denoted $(a, b)_F$ or simply (a, b) when no confusion is possible. Recall that $(a, b) = 0$ in the Brauer group, $\mathrm{Br}(F)$, if and only if b is a norm from $F(\sqrt[p]{a})$; in particular, since p is odd, $(a^i, a^j) = 0$ in $B_r(F)$, for all $a \in F = F\backslash\{0\}$ and all i, j.

If G is a pro-p-group we set $H^i(G) = H^i(G, \mathbb{Z}/p\mathbb{Z})$. From Merkurjev and Suslin's work [MS], an element of order p in the Brauer group is a product of cyclic algebras so is, in particular, split by $F(p)$. Hence, from Galois cohomology we have a commutative diagram

$$\begin{array}{ccc} F/F^p \times F/F^p & \xrightarrow{(\ ,\ )_F} & \mathrm{Br}_p(F) \\ \cong\downarrow & & \downarrow\cong \\ H^1(G_F(p)) \times H^1(G_F(p)) & \xrightarrow{\ \smile\ } & H^2(G_F(p)) \end{array}$$

where $\mathrm{Br}_p F$ denotes the subgroup of the Brauer group consisting of elements of order p. Moreover, if $K = F(\sqrt[p]{d})$, $G = G_F(p)$, $H = G_K(p)$, and $\overline{G} = G/H$ then the cohomology sequence $0 \to H^1(\overline{G}) \to H^1(G) \overset{\mathrm{res}}{\to} H^1(H)$ corresponds to

Received by the editors February 6, 1990 and, in revised form, July 9, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 12F10, 20E18.
This work was supported in part by NSA research grant no. MDA 904-88-H-2018.

the sequence $1 \to \langle a\rangle_p \to F/F^p \to K/K^p$ induced by $F \subseteq K$, where $\langle a\rangle_p$ is the cyclic subgroup of F/F^p generated by aF^p.

All groups considered here are profinite, homomorphisms are continuous, subgroups are closed, and generating set means topological generating set.

It should be mentioned that when $p = 2$ results analogous to those in this paper can be deduced from [JW, Theorems 2.1, 2.3, and Lemma 4.1] and [W, Theorems 4.1, 4.5, and Corollary 4.6]. For other related results the reader is referred to Geyer's paper [G], when G is a "solvable" subgroup of the absolute Galois group of the field of rational numbers, and to Becker's paper [B], in the case that G is the absolute Galois group of a formally real field.

Definition. An element a in $F\backslash F^p$ is *p-rigid* if $(a, b) = 0$ in $\mathrm{Br}(F)$ implies $b \in a^iF^p$ for some $i \geq 0$. The field F is called *p-rigid* if every element in $F\backslash F^p$ is p-rigid and F is *hereditarily p-rigid* if every p-extension is p-rigid. Note that F is hereditarily p-rigid iff every *finite* p-extension is p-rigid.

Example. If F is a local field with residue field of characteristic not equal to p then F is hereditarily p-rigid. Further examples are given in the Corollary and Example following the proof of Theorem 3.

Theorem 1. *For the field F the following statements are equivalent*:

(a) *F is hereditarily p-rigid.*

(b) *There is an exact sequence $1 \to \mathbb{Z}_p^I \to G_F(p) \to \mathbb{Z}_p \to 1$, for some index set I, where $\mathbb{Z}_p$ denotes the infinite procyclic p-group.*

(c) *The commutator subgroup of $G_F(p)$ is abelian.*

The proof of Theorem 1 requires several lemmas:

Lemma 1. *Let $\mu(p)$ be the group of all p-power roots of unity inside $F(p)$. If $\mu(p) \not\subset F$ then* $\mathrm{Gal}(F(\mu(p))/F) \cong \mathbb{Z}_p$.

Proof. We fix, inside $F(p)$, a system of primitive roots of unity $\omega_1 = \omega$, $\omega_2, \omega_3, \ldots$ chosen so that $\omega_i^p = \omega_{i-1}$ for all i. Then $F(\mu(p)) = F(\omega_i | i = 1, 2, \ldots)$. Choose $i \geq 1$ so that $\omega_i \in F$ and $\omega_{i+1} \notin F$. Define x on $F(\mu(p))$ by $x(\omega_{i+m}) = \omega_{i+m}^{p^i+1}$. Then restricted to $F(\omega_{i+m})$, x has order p^m and hence $\mathrm{Gal}(F(\mu(p))/F)$ is generated by x.

For any field K and $a \in \dot{K}$ we set $[a] = a\dot{K}^p$. Recall that $\langle a\rangle_p$ denotes the cyclic subgroup of K/K^p generated by $[a]$.

Lemma 2. *Let K/F be a cyclic extension of degree p with generator σ. For $\beta \in K$, $K(\sqrt[p]{\beta})$ is Galois over F if and only if $[\sigma\beta] = [\beta]$.*

Proof. First assume $K(\sqrt[p]{\beta})/F$ is a Galois extension. Then $\sqrt[p]{\sigma\beta} \in K(\sqrt[p]{\beta})$ so $[\sigma\beta] \in \langle\beta\rangle_p$ (by Kummer theory). If $[\sigma\beta] = [\beta]^i$ with $1 < i < p$ then in $\dot{K}/\dot{K}^p$, $[N(\beta)] = [\beta]^{1+i+i^2+\cdots+i^{p-1}}$ where $N\colon K \to F$ is the norm. Since $i^{p-1}+i^{p-2}+\cdots+i^2+i+1 \equiv 1 \pmod{p}$, $[N(\beta)] = [\beta]$ and, because $N(\beta) \in F$, this implies $[\sigma\beta] = [\beta]$.

Conversely, if $[\sigma\beta] = [\beta]$ then $K(\sqrt[p]{\beta}) = K(\sqrt[p]{\sigma\beta})$ and $K(\sqrt[p]{\beta})/F$ is a Galois extension.

Lemma 3. *Let $K = F(\sqrt[p]{d})$, $d \notin F^p$, and let $\overline{G} = \mathrm{Gal}(K/F)$. If $\overline{G}$ acts trivially on K/K^p then $K/K^p = \langle\sqrt[p]{d}\rangle_p \times \varepsilon(F/F^p)$, where ε is the map induced by $F \subseteq K$.*

Proof. By Hochschild-Serre [S, I-15] there is an exact sequence

$$0 \to H^1(\overline{G}) \to H^1(G_F(p)) \xrightarrow{\text{res}} H^1(G_K(p))^{\overline{G}} \to H^2(\overline{G})$$

and since $H^2(\overline{G}) \cong \mathbb{Z}/p\mathbb{Z}$, either res is surjective or its image has index p in $H^1(G_K(p))^{\overline{G}}$. Since $(\dot{K}/\dot{K}^p)^{\overline{G}} = \dot{K}/\dot{K}^p$, this means the image of ε has index p or 1 in $\dot{K}/\dot{K}^p$. If $[\sqrt[p]{d}] \in \operatorname{Im}\varepsilon$ then $\sqrt[p]{d} = uy^p$ with $u \in F$, $y \in K$. Then $d = N(\sqrt[p]{d}) = (uN(y))^p \in F^p$, a contradiction. Hence $\dot{K}/\dot{K}^p = \langle\sqrt[p]{d}\rangle_p \times \varepsilon(F/F^p)$.

Recall that for an odd prime p there exist (up to isomorphism) only two nonabelian groups of order p^3, namely:

Type E_1: Generators x, y, t and relations $x^p = y^p = t^p = 1$, $xyx^{-1}y^{-1} = t$, $xt = tx$, $yt = ty$.

Type E_2: Generators x, y and relations $x^p = y^{p^2} = 1$, $xyx^{-1} = y^{p+1}$.

Lemma 4. (1) *F is p-rigid if and only if no group of type E_1 occurs as a Galois group over F.*

(2) *If F is p-rigid and contains a primitive p^2th root of unity then no group of type E_2 occurs as a Galois group over F; hence, in this case, every Galois extension of degree p^3 is abelian.*

Proof. This is an immediate consequence of [MN, Theorem 14].

Lemma 5. *Let P be a p-subgroup of the symmetric group S_{p^2}. If every subgroup of order p^3 in P is abelian then P is abelian.*

Proof. We may assume $|P| = p^n > p^3$. The proof proceeds by induction on n so we assume that every subgroup of P of order p^{n-1} is abelian.

We first show that every element in P has order $\leq p$. If not, then P contains an element y of order p^2. This element must be a p^2-cycle and hence its centralizer in P is the cyclic subgroup, $\langle y\rangle$, generated by y. Since $|P| \geq p^3$, the center of P, $Z(P)$, is properly contained in $\langle y\rangle$ and because P is a p-group it follows that $Z(P) = \langle y^p\rangle$.

Now let H be a normal subgroup of P of order $p^{n-2} > p$. Then, because H is normal in the p-group P, the usual argument shows that $|Z(P) \cap H| > 1$ and since $|Z(P)| = p$ we conclude that $Z(P) \leq H$. Moreover, H is abelian by the induction assumption.

Case 1. $y \in H$. Then $\langle y\rangle = H$ (because H is abelian and the centralizer of y is $\langle y\rangle$). Choose $z \in P\backslash H$. Then $zy \neq yz$ so $H\langle z\rangle$ is nonabelian. If $|z| = p$ then

$$|H\langle z\rangle| = \frac{|H|\,|z|}{|H \cap \langle z\rangle|} = p^{n-2}\cdot p = p^{n-1},$$

a contradiction. If $|z| = p^2$ then by the argument in the second paragraph of this proof (applied there to y of order p^2) we have $Z(P) = \langle z^p\rangle$, hence $z^p \in H$. Then $|H\langle z\rangle| = (p^{n-2}\cdot p^2)/p = p^{n-1}$, likewise a contradiction.

Case 2. $y \notin H$. Since $|H| > p$ there exists h in H with $hy \neq yh$. However, $H \cap \langle y\rangle = \langle y^p\rangle$ in this case, yielding $|H\langle y\rangle| = p^{n-1}$, once again contradicting the induction assumption. This completes the proof that every element in P has order $\leq p$.

Now suppose that P is nonabelian. We assert that in this case $Z(P)$ is the unique normal subgroup of P of order p^{n-2}. To see this, let H be a normal subgroup of P with $|H| = p^{n-2}$. If there exists z in $Z(P)\backslash H$ then (since z has order p) $|H\langle z\rangle| = p^{n-1}$ so there exists x in $P\backslash H\langle z\rangle$. Since H is normal in P, $H\langle x\rangle$ is a subgroup of order p^{n-1}, hence abelian. If $z \in H\langle x\rangle$ then $z = hx^i$, $1 \leq i < p$, which forces $x \in H\langle z\rangle$. Hence $z \notin H\langle x\rangle$ so $H\langle x\rangle\langle z\rangle$ is an abelian group of order p^n, contrary to the assumption that P is nonabelian. Hence $Z(P) \leq H$. On the other hand, if there exists h in $H\backslash Z(P)$ then there exists x in $P\backslash H$ such that $xh \neq hx$ (since H is abelian). But then $H\langle x\rangle$ is a nonabelian group of order p^{n-1}. Hence $H = Z(P)$, as asserted.

Still assuming P is nonabelian, let $x, y \in P$ map onto the basis of $P/Z(P) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Then $P = Z(P)\langle x\rangle\langle y\rangle$ and $xy \neq yx$. However, $xy = zyx$ for some $z \in Z(P)$ which forces $|\langle x, y\rangle| \leq p^3$ (as $|x| = |y| = |z| = p$). But then $\langle x, y\rangle$ is abelian by hypothesis.

Lemma 6. *Suppose F is hereditarily p-rigid. Let L be a p-extension of F containing a primitive p^2th root of unity.*

(1) *Every p-extension of L of degree p^2 is a Galois extension.*

(2) *If $K = L(\sqrt[p]{d})$, $d \notin L^p$, then $K/K^p = \langle\sqrt[p]{d}\rangle_p \times \varepsilon(L/L^p)$.*

(3) *If K is a finite p-extension of L then there exist $a_1, \dots, a_r$ in L such that*

$$K \subseteq L(\sqrt[p^{n_1}]{a_1}, \dots, \sqrt[p^{n_r}]{a_r}).$$

Proof. (1) Let M/L be a p-extension of degree p^2, let $G = G_L(p)$, and $H = G_M(p)$. Then $(G : H) = p^2$ so there exists a homomorphism $f : G \to S_{p^2}$ with $\operatorname{Ker} f \subseteq H$ and whose image P is a p-subgroup of S_{p^2}. Then there exists a Galois p-extension E/L containing M such that $\operatorname{Gal}(E/L) \cong P$. By Lemma 4(2), every subgroup of P of order p^3 (if any) is abelian and by Lemma 5, P is abelian. In particular, $H/\operatorname{Ker} f$ is a normal subgroup of $P = G/\operatorname{Ker} f$, whence $H \triangleleft G$.

By (1) and Lemma 2, $\operatorname{Gal}(K/L)$ acts trivially on K/K^p so (2) follows from Lemma 3.

To prove (3), we induct on $[K : L]$. Thus we can write $K = M(\sqrt[p]{d})$, with

$$d \in M \subseteq L(\sqrt[p^{m_1}]{a_1}, \dots, \sqrt[p^{m_s}]{a_s}), \qquad a_i \in L, \ m_i \geq 0.$$

By (2) we may assume $d = u\sqrt[p^{m_s}]{a_s}$ with $u \in L(\sqrt[p^{m_1}]{a_1}, \dots, \sqrt[p^{m_s-1}]{a_s})$ and by the induction assumption

$$L(\sqrt[p^{m_1}]{a_1}, \dots, \sqrt[p^{m_s-1}]{a_s})(\sqrt[p]{u}) \subseteq L(\sqrt[p^{k_1}]{b_1}, \dots, \sqrt[p^{k_t}]{b_t}), \qquad b_i \in L.$$

Hence $K \subseteq L(\sqrt[p^{m_1}]{a_1}, \dots, \sqrt[p^{m_s}]{a_s}, \sqrt[p^{k_1}]{b_1}, \dots, \sqrt[p^{k_t}]{b_t})$.

Lemma 7. *Assume $|F/F^p| = p^2$. Then either $G_F(p)$ is a free pro-p-group (of* rank 2) *or $G_F(p)$ has generators x, y and relation $xyx^{-1} = y^{q+1}$, where $q = 0$ or $q = p^m$, $m \geq 1$.*

Proof. Choose generators $[a], [b]$ for F/F^p. If $(a, b) = 0$ then $(u, v) = 0$ for all u, v in F and by the Merkurjev-Suslin theorem [MS], $H^2(G_F(p)) = 0$. Hence $G_F(p)$ is a free pro-p-group in this case [S, I-37].

If $(a, b) \neq 0$ then the pairing $H^1(G) \times H^1(G) \to H^2(G)$, $G = G_F(p)$, is necessarily nondegenerate so, again using Merkurjev-Suslin, G is a Demushkin group of rank 2 and by Demushkin's theorem [D], G has the generators and relation described above.

Remark. Using Merkurjev and Suslin's result it is easy to show that the following statements are equivalent (giving a p-analogue of [S, Proposition 5, II-7], when F contains a primitive pth root of unity):

(a) $G_F(p)$ is a free pro-p-group.

(b) The p-primary part, $\mathrm{Br}(F)(p)$, of the Brauer group of F is trivial.

(c) $\mathrm{Br}(K)(p) = 0$ for every p-extension K of F.

(d) For every p-extension K of F and every p-extension L of K, $N_{L/K}\colon L \to K$ is surjective.

(e) For every cyclic extension K/F of degree p, $N_{K/F}\colon K \to F$ is surjective.

Proof of Theorem 1. (a) $\Rightarrow$ (b). Let $L = F(\mu(p))$ where, as before, $\mu(p)$ is the group of all p-power roots of unity. By Lemma 6, $F(p) = L(p) = L(\sqrt[p^{n_i}]{a_i} | i \in I,\ n_i \geq 0)$, where $\{[a_i]\}_{i\in I}$ is an $\mathbb{F}_p$-basis for L/L^p. Since all p-power roots of unity lie in L, $\mathrm{Gal}(F(p)/L) \cong \mathbb{Z}_p^I$ (direct product) and by Lemma 1, $\mathrm{Gal}(L/F) \cong \mathbb{Z}_p$ or $\{1\}$.

(b) $\Rightarrow$ (c). Given an exact sequence as in (b) the commutator subgroup of $G_F(p)$ must be contained in $\mathbb{Z}_p^I$.

(c) $\Rightarrow$ (a). Suppose K is a p-extension of F and a, b are elements of K with $(a, b) = 0$. If $[b] \notin \langle a\rangle_p$ then $[a], [b]$ are independent over $\mathbb{F}_p$. Let M be a maximal p-extension of K such that $[a], [b]$ remain linearly independent in M/M^p. We assert that $M/M^p = \langle a\rangle_p \times \langle b\rangle_p$. Indeed, if $c \in M\backslash M^p$ then $L = M(\sqrt[p]{c})$ is a larger extension so there exists i, j (not both $0 \bmod p$) such that $a^i b^j \in L^p$. Kummer theory implies that $[a]^i[b]^j = [c]^k$ in M/M^p with $0 < k < p$ and hence $[c] \in \langle a\rangle \times \langle b\rangle$. Thus the group $G_M(p)$ has rank 2. Since $(a, b) = 0$ the proof of Lemma 7 shows that $G_M(p)$ is a free pro-p-group. Let C be the commutator subgroup of $G_M(p)$. Since the factor group $G_M(p)/C$ is a free abelian pro-p-group of rank 2, C is a free pro-p-group of infinite rank [S, Proposition 22, Corollary 3, I-33, I-37]. Since C is contained in the commutator subgroup of $G_F(p)$ this contradicts (c).

A profinite group G is said to be *metabelian* if there is an exact sequence $1 \to A \to G \to B \to 1$ of profinite groups with A and B abelian. It is clear that G is metabelian iff its commutator subgroup is abelian.

Corollary 1. *For the group $G = G_F(p)$ the following statements are equivalent*:

(a) *G is not metabelian.*

(b) *G contains a free pro-p-subgroup of* rank 2.

(c) *G contains a free pro-p-subgroup of infinite rank.*

Proof. (a) $\Rightarrow$ (b). Let $L = F(\mu(p))$. If $G_L(p)$ is abelian then G is metabelian so we can choose x, y in $G_L(p)$ with $xy \neq yx$. If the pro-p-subgroup generated by x and y is not free then by Lemma 7 it is metabelian and hence by Theorem 1 ((c) $\Rightarrow$ (a) and the proof of (a) $\Rightarrow$ (b)) it is abelian.

(b) $\Rightarrow$ (c). As noted in the proof of Theorem 1 (c) $\Rightarrow$ (a), the commutator subgroup of a free pro-p-group of rank 2 is a free pro-p-group of infinite rank.

(b) $\Rightarrow$ (a). Choose H free of rank 2, $H \leq G$. Then the commutator subgroup of H is contained in the commutator subgroup of G so the latter cannot be abelian.

Corollary 2. *Assume* $G = G_F(p)$ *has finite* $\operatorname{rank} r$.

(1) *If* $\operatorname{rank} H \leq r$ *for all subgroups* H *then* $G_F(p)$ *is metabelian.*

(2) *If* G *is metabelian and* F *contains a primitive* p^2*th root of unity then* $\operatorname{rank} H \leq r$ *for all subgroups* H.

Proof. (1) follows from Corollary 1.

(2) We first show that the rank of H equals r, whenever $(G : H)$ is finite. By induction it suffices to assume that $(G : H) = p$. Then the result follows from Theorem 1, (c) $\Rightarrow$ (a), and Lemma 6(2).

For the general case, suppose $\operatorname{rank} H > r$. Then there exist $r+1$ $\mathbb{F}_p$-linearly independent elements $[a_1], \dots, [a_{r+1}]$ in L/L^p, where L is the fixed field of H. If $K = F(a_1, \dots, a_{r+1})$ then $G_K(p)$ has finite index in G and $\operatorname{rank} G_K(p) \geq r+1$.

Corollary 3. *If* $G_F(p)$ *is metabelian and* $\operatorname{rank} G_F(p) = r$ *then*

$$\dim_{\mathbb{F}_p} \operatorname{Br}_p(F) = \frac{r(r-1)}{2}.$$

Proof. By the Merkurjev-Suslin theorem it suffices to show that if $[a_1], \dots, [a_t]$ are linearly independent in F/F^p then $\{(a_i, a_j)\}_{i<j}$ is a linearly independent subset of $\operatorname{Br}(F)$. If not, among all hereditarily p-rigid fields where this fails choose one, F, with t minimal. Then there is a relation $\sum_{i<j} n_{ij}(a_i, a_j) = 0$ with $n_{ij} \in \mathbb{F}_p$, not all zero. Let $K = F(\sqrt[p]{a_t})$. Then $[a_1], \dots, [a_{t-1}]$ remain linearly independent in K/K^p so by the minimality of t, the set $\{(a_i, a_j)\}$, $1 \leq i < j < t$, is linearly independent in $\operatorname{Br}(K)$. This forces $n_{ij} = 0$ for $1 \leq i < j < t$ and we are left with $\sum_{i<t} n_{it}(a_i, a_t) = 0$ in $\operatorname{Br}(F)$; i.e., $(a_1^{n_{1t}} \cdots a_{t-1}^{n_{t-1,t}}, a_t) = 0$. Since F is p-rigid this implies $[a_1^{n_{1t}} \cdots a_{t-1}^{n_{t-1,t}}] \in \langle a_t \rangle_p$ contrary to the linear independence of $[a_1], \dots, [a_t]$.

Remark. In Theorem 4, this corollary will be generalized under the additional assumption that F contains a primitive p^2th root of unity.

Theorem 2. *Assume* $G_F(p)$ *is a metabelian pro-p-group. If* F *contains a primitive* p^2*th root of unity then* $G_F(p)$ *has generators* $\{y_i, x\}_{i\in I}$ *with relations* $y_i y_j = y_j y_i$ *and* $x y_i x^{-1} = y_i^{q+1}$ *where* $q = 0$, *if* f *contains all p-power roots of unity, or* $q = p^n$, *where* n *is the largest integer such that* F *contains a primitive* p^n*th root of unity.*

Proof. If F contains all p^mth roots of unity, $m > 0$, this follows as in the proof of Theorem 1, (a) $\Rightarrow$ (b). Otherwise, by Lemma 6(3), $F(p) = F(\omega_{n+j}, \sqrt[p^{m_i}]{a_i} \mid j = 1, 2, \dots, i \in I,\ m_i > 0)$ where $\{[\omega_n], [a_i]\}_{i\in I}$ is an $\mathbb{F}_p$-basis for F/F^p and the ω_k are chosen so that $\omega_1 = \omega$ and $\omega_k^p = \omega_{k-1}$ (as in the proof of Lemma 1). Thus we can define a set of generators $\{y_i, x_i\}_{i\in I}$ for $G_F(p)$ as follows:

$$x(\omega_{n+j}) = \omega_{n+j}^{q+1}, \qquad q = p^n,\ j \geq 1; \qquad x(\sqrt[p^m]{a_i}) = \sqrt[p^m]{a_i},$$
$$y_i(\sqrt[p^m]{a_i}) = \omega_m \sqrt[p^m]{a_i}, \quad y_i(\sqrt[p^m]{a_k}) = \sqrt[p^m]{a_k} \quad \text{if } k \neq i,$$
$$y_i(\omega_m) = \omega_m \quad \text{for all } m \geq 1.$$

It is readily verified that the set $\{y_i, x\}_{i\in I}$ satisfies the given relations.

Remark. One should be able to remove the assumption on the existence of a p^2th root of unity. However the use of Lemma 6(3) seems to be crucial for the above proof.

A profinite group G is *solvable* if there exists a chain of (closed) subgroups $\{1\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = G$ with $H_i \lhd H_{i+1}$ and H_{i+1}/H_i abelian.

Theorem 3. *The following statements are equivalent*:

(a) $G_F(p)$ *is solvable.*

(b) $G_F(p)$ *is metabelian.*

(c) $G_F(p)$ *does not contain a free, nonabelian subgroup.*

Proof. The equivalence of (b) and (c) is contained in Corollary 1 to Theorem 1. It remains to prove (a) $\Rightarrow$ (b). Assume $G = G_F(p)$ is solvable. By induction we may assume G has subgroups H_1, H_2 such that $H_1 \lhd H_2$, $H_2 \lhd G$ and H_1, H_2/H_1, G/H_2 are abelian. By Theorem 1, the fixed field F_2 of H_2 is hereditarily p-rigid. Let $L = F(\mu(p))$ and let $L_2 = F_2 L$. Then L_2 is hereditarily p-rigid so (because $\mu(p) \subseteq L_2$) $G_{L_2}(p)$ is abelian. Moreover, there exists an injective homomorphism $G_L(p)/G_{L_2}(p) \hookrightarrow G_F(p)/G_{F_2}(p) = G/H_2$. Hence $G_L(p)$ is metabelian and L is hereditarily p-rigid. Since $\mu(p) \subseteq L$, $G_L(p)$ is abelian, whence $G_F(p)$ is metabelian.

Let $\Gamma = \mathbb{Z}^{(I)}$ (direct sum) to be totally ordered group obtained by totally ordering the set I and then using the usual lexicographic ordering. Let $F((\Gamma)) = \{f\colon \Gamma \to F \mid \operatorname{supp}(f) \text{ is well ordered}\}$ be the (henselian) generalized formal power series field. If $|I| = n$ then $F((\Gamma))$ can be identified with the field of iterated power series $F((x_1))\cdots((x_n))$.

Corollary. F *satisfies the conditions of Theorem* 1 *if and only if* $F((\Gamma))$ *does.*

Proof. Let $K = F((\Gamma))$. From valuation theory there is an exact sequence

$$1 \to \mathbb{Z}_p^I \to G_K(p) \to G_F(p) \to 1$$

where $\mathbb{Z}_p^I$ is identified with $G_{K_{nr}}(p)$, where K_{nr} is the maximal nonramified extension of K inside $K(p)$. Hence $G_K(p)$ metabelian implies $G_F(p)$ metabelian. On the other hand, if $G_F(p)$ is metabelian then $G_K(p)$ is solvable and Theorem 3 applies.

Example. Given any pro-p-group G with generators and relations as described in Theorem 2, there is a field F with $G_F(p) \cong G$:

Let r be a prime with $r \equiv 1 \pmod p$, let $K = \mathbb{F}_r(\omega_n)$ where ω_n is a primitive p^nth root of unity (resp., $K = \mathbb{F}_r(p)$) and let $F = K((\Gamma))$, $\Gamma = \mathbb{Z}^{(I)}$.

Theorem 4. *Assume* $G = G_F(p)$ *is solvable and* F *contains a primitive* p^2*th root of unity. If* $\operatorname{rank} G = n$ *then for* $k \geq 0$, $\dim_{\mathbb{F}_p} H^k(G) = \binom{n}{k}$ (*where* $\binom{n}{k} = 0$ *if* $k > n$).

Proof. We proceed by induction on n. By Theorem 2 there is an abelian subgroup N of rank $n-1$ such that $G/N \cong \mathbb{Z}_p$. The Lyndon-Hochschild-Serre spectral sequence satisfies

$$E_2^{r,s} = H^r(G/N, H^s(N)) \Rightarrow H^{r+s}(G).$$

Since $G/N \cong \mathbb{Z}_p$, $E_2^{r,s} = 0$ for $r \neq 0, 1$. Hence as in [R], third quadrant version of Lemma 11.36, p. 349, there is an exact sequence

$$0 \to E_2^{1,k-1} \to H^k(G) \to E_2^{0,k} \to 0.$$

We assert that G/N acts trivially on $H^1(N)$ (and hence on $H^m(N)$ for any $m \geq 1$). The action of G/N on $H^1(N) = \operatorname{Hom}(N, \mathbb{Z}/p\mathbb{Z})$ is given by $(\overline{\sigma} \cdot f)(\tau) = f(\sigma^{-1}\tau\sigma)$, for $\sigma \in G$, $\tau \in N$. By Theorem 2, $\sigma^{-1}\tau\sigma = \tau^{q+1}$, where either $q = 0$ or $q = p^t$ for some t. Thus $f(\sigma^{-1}\tau\sigma) = f(\tau^{q+1}) = (q+1)f(\tau) = f(\tau)$, proving the assertion.

Hence, $E_2^{0,k} = H^0(G/N, H^k(N)) = H^k(N)$ and

$$E_2^{1,k-1} = \operatorname{Hom}(G/N, H^{k-1}(N)) \cong \operatorname{Hom}(\mathbb{Z}_p, H^{k-1}(N)) \cong H^{k-1}(N).$$

Therefore the above sequence becomes

$$0 \to H^{k-1}(N) \to H^k(G) \to H^k(N) \to 0.$$

By the induction assumption (and the previous example), $\dim_{\mathbb{F}_p} H^m(N) = \binom{n-1}{m}$. Hence

$$\dim_{\mathbb{F}_p} H^k(G) = \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}.$$

Corollary. *With the assumptions in Theorem 4, the cohomology ring* $H^*(G) = \coprod_{k \geq 0} H^k(G)$ *is isomorphic to the exterior algebra over* $\mathbb{F}_p$ *with generators* $x_1, \ldots, x_n$.

Remark. If $p = 2$ the foregoing argument, together with [JW, Theorem 2.3, and Lemma 4.1], shows that $H^*(G)$ is isomorphic to the (commutative) polynomial ring $\mathbb{F}_2[x_1, \ldots, x_n]$ modulo the ideal generated by $x_1^2, \ldots, x_n^2$.

References

[B] E. Becker, *Formal-reele Körper mit streng-auflösbarer absoluter Galoisgruppe*, Math. Ann. **238** (1978), 203–206.

[D] S. Demushkin, *On the maximal p-extension of a local field*, Izv. Akad. Nauk SSR Ser. Math. **25** (1961), 329–346.

[G] W.-F. Geyer, *Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschrankter Stufe ist*, J. Number Theory **1** (1969), 346–374.

[JW] B. Jacob and R. Ware, *A recursive description of the maximal pro-2 Galois group via Witt rings*, Math. Z. **200** (1989), 379–396.

[MN] R. Massy and T. Nguyen-Quang-Do, *Plongement d'une extension de degree p^2 dans une surextension non abelienne de degre' p^3: étude locale-globale*, J. Reine Angew. Math. **291** (1977), 149–161.

[MS] A. Merkurjev and A. A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR Ser. Mat. **46** (1982), 1011–1046; English transl., Math. USSR Izv. **21** (1983), no. 2, 307–340.

[R] J. J. Rotman, *An introduction to homological algebra*, Academic Press, 1979.

[S] J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math., vol. 5, Springer-Verlag, 1965.

[W] R. Ware, *Quadratic forms and profinite 2-groups*, J. Algebra **58** (1979), 227–237.

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802

E-mail address: ware@math.psu.edu