JOURNAL OF ALGEBRA 154, 499–506 (1993)

On the Galois Embedding Problem for p-Extensions in Characteristic p

T. KAMBAYASHI

Department of Mathematical Sciences, Tokyo Denki University, Hatoyama-machi, Saitama, 350-03, Japan

Communicated by Richard G. Swan

Received April 29, 1991

The general Galois Embedding Problem asks whether or not a given finite Galois extension of fields K/k is embeddable in a tower of Galois extensions $k \subset K \subset L$ in such a manner that the corresponding extension of finite groups matches a pre-designated group extension. Since the 1930s there has been extensive research on the problem, particularly in the case of number fields. The reader is referred to Matzat's monograph [6] for references. What we deal with in the present note is quite a special case of the problem wherein the field characteristic is p and the group extension has kernel $\simeq \mathbb{Z}/p\mathbb{Z}$; otherwise, however, the fields appearing in our treatment are completely unrestricted. In Section 1 below we give as Theorem 1 a condition in order that a Galois extension followed by an Artin–Schreier extension be Galoisian. Our main result is Theorem 2, which gives a criterion for the Galois embeddability in the case at hand: The condition is that either the given group extension is *not* split, or the base field k contains elements *not* expressible as $u^p - u$ with $u \in K$.

Since the factor group $K/\mathscr{P}K$, $\mathscr{P}x := x^p - x$, emerges as a key player in our situation, we study this group rather closely in Section 2 and obtain Theorem 3 which gives an important special case where the group is always infinite. As an application we show as Corollary 1 to Theorem 3 that, in characteristic p, any p-group can be realized as a Galois group over any field finitely generated and of positive transcendency over another field. Also about p-groups, we retrieve the classical Witt theorem which determines exactly when a p-group can be a Galois group over a given field. (Compare Corollary 2 of Theorem 3 below with Witt [14]. Also, see closely related results of Reichhardt [8] and Scholz [9] for the case of number fields.)

The origin of the present paper is the author's study of Abhyankar's Conjecture [1] about unramified coverings of the affine line in positive

0021-8693/93 $5.00

characteristics [4; 5]. In that direction, lately there have been remarkable advances made by Abhyankar himself [2] and Serre [11].

In completing this work I greatly benefited from talking with Madhav Nori. When I showed him Theorems 1 and 2 it became apparent to me that he had more or less known or anticipated these results through his earlier thesis work [7] related to Shafarevich's theorem about unramified Galois extensions of algebraic function fields [12]. More specifically, he pointed out to me how to handle Galois embedding questions from the viewpoint of profinite groups and produced for me Example 2 in the text below. I am greatly indebted to him. I am also grateful to my young colleagues, Noriyuki Suwa and Shuji Yamagata, for useful pieces of advice and information.

1. Embedding Theorems

For any $\mathbb{F}_p$-algebra A, the Frobenius map $\mathscr{F}: A \to A$ is defined by $\mathscr{F}(a) := a^p$ for every $a \in A$, and the map $\mathscr{P}: A \to A$ by $\mathscr{P} := \mathscr{F} - 1$, $\mathscr{P}(a) = a^p - a$.

Let $1 \to \mathbb{Z}/p\mathbb{Z} \to E \to G \to 1$ be an extension of a finite group G by $\mathbb{Z}/p\mathbb{Z}$. Given a Galois extension K/k with Galois group G, one asks whether or not one may build a Galois extension L/K with Galois group $\mathbb{Z}/p\mathbb{Z}$ such that the Galois group of L over k is E. To answer this question one must first know the conditions in order for L/k to be a Galois extension. Since L/K is always an Artin–Schreier extension, it is not hard to prove the next

THEOREM 1. *Let k be a field of prime characteristic p, and let K be a finite Galois extension of k with Galois group $G = \mathrm{Gal}(K/k)$. Let $L = K(\theta)$ be an Artin–Schreier extension of K such that $\theta^p - \theta - u = 0$ with $u \in K$, $u \notin \mathscr{P}K$. Then, L is a Galois extension of k if and only if there exists a p-character $\chi: G \to (\mathbb{F}_p)^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ such that ${}^s u \equiv \chi(s)\, u \pmod{\mathscr{P}K}$ for all $s \in G$.*

Proof. Let $k_{\mathrm{sep}} \supset K$ be a separable closure of k fixed once and for all. For any $s \in G$ let $\tilde{s} \in \mathrm{Gal}(k_{\mathrm{sep}}/k)$ be any one of the extensions of s. Now suppose that, for all $s \in G$, we have ${}^s u = \chi(s)\, u + w_s^p - w_s$ with $w_s \in K$. Then, since

$$ {}^{\tilde{s}}\theta^p - {}^{\tilde{s}}\theta - {}^s u = 0 \tag{1} $$

the conjugate ${}^{\tilde{s}}\theta$ must equal $\chi(s)\, \theta + w_s + j$ for some $j \in \mathbb{F}_p$, so that $K(\theta)$ is a Galois extension of k. Conversely, assume that $K(\theta)$ is Galoisian over k.

Then, ${}^{\tilde{s}}\theta$ must be a polynomial in θ of degree $< p$ with coefficients in K: ${}^{\tilde{s}}\theta = \sum_{i=0}^{p-1} b_i\theta^i$. Substitute this in (1) above and we get

$$\left(\sum_{i=0}^{p-1} b_i\theta^i\right)^p - \sum_{i=0}^{p-1} b_i\theta^i - {}^s u = \sum_{i=0}^{p-1} b_i^p(\theta+u)^i - \sum_{i=0}^{p-1} b_i\theta^i - {}^s u = 0. \quad (2)$$

As θ is of degree p over K, the last expression of (2) as a polynomial in θ must have all coefficients equal to 0. It follows then

$$b_p = b_{p-1} = \cdots = b_2 = 0 \qquad \text{and} \qquad b_1 \in \mathbb{F}_p. \quad (3)$$

Indeed, introducing $b_p := 0$, we argue by descending induction to prove that $b_p = \cdots = b_{j+1} = 0$ and $b_j \in \mathbb{F}_p$ for $j = p-1, ..., 1$. Firstly, in (2), (coefficient of $\theta^{p-1}) = b_{p-1}^p - b_{p-1} = 0$, so $b_{p-1} \in \mathbb{F}_p$, which takes care of the case $j = p-1$. Next suppose our claim to be true for one j as above. Then, the last equality in (2) becomes $\sum_{i=0}^{j} b_i^p(\theta+u)^i - \sum_{i=0}^{j} b_i\theta^i - {}^s u = 0$ with $b_j \in \mathbb{F}_p$. In this last, the coefficient of θ^{j-1} is $b_j^p \cdot ju + b_{j-1}^p - b_{j-1}$ which equals 0. So, $-jb_j u = b_{j-1}^p - b_{j-1}$ and, since u is not in $\mathscr{P}K$, we see that $b_j = 0$ and $b_{j-1} \in \mathbb{F}_p$. This proves (3). We have now established

$${}^s u = b_1 u + b_0^p - b_0, \qquad b_1 \in \mathbb{F}_p,\ b_0 \in K \text{ for all } s \in G. \quad (4)$$

It is easy to see that the b_1 in (4) depends only on s and *not* on $\tilde{s}$, and that the correspondence $s \mapsto b_1$ gives a homomorphism of G to $\mathbb{F}_p^*$. ∎

Remark. Theorem 1 is the counterpart in our case of Reichhardt's criterion [8, p. 3] in the case of Kummer extensions over number fields.

THEOREM 2. *Let k be a field of prime characteristic p, and let K be a finite Galois extension field of k with Galois group $G = \mathrm{Gal}(K/k)$. Let $1 \to \mathbb{Z}/p\mathbb{Z} \to E \to G \to 1$ be a central extension of G by $\mathbb{Z}/p\mathbb{Z}$. Then, the extension K/k is embeddable in a Galois extension L/K such that* $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$ *and* $\mathrm{Gal}(L/k) \simeq E$ *if and only if* either (a) *the given group extension is NOT split*, or (b) *k is NOT contained in $\mathscr{P}K$.*

Proof. (If) To begin with, observe that the exact sequence of additive groups $0 \to \mathbb{F}_p^* \to K^+ \to K^+/\mathbb{F}_p^+ \to 0$, combined with the fact that $H^i(G, K^+) = 0$ for $i > 0$, gives the isomorphism of Galois cohomology groups $H^1(G, K^+/\mathbb{F}_p^+) \simeq H^2(G, \mathbb{F}_p^+)$. Also observe that, since G here acts trivially on $\mathbb{F}_p^+$, one may (and shall) identify $H^2(G, \mathbb{F}_p^+)$ with $H^2(G, \mathbb{Z}/p\mathbb{Z})$ (with a trivial G-action) that controls central extensions of G by $\mathbb{Z}/p\mathbb{Z}$. From now on in the current proof we just write P in place of $\mathbb{F}_p^+ = \mathbb{Z}/p\mathbb{Z}$ with a trivial G-action. Now let $\gamma \in H^2(G, P)$ be the given central group extension. Then, $\gamma = c(-,-) \bmod B^2(G, P)$ for some $c(-,-) \in Z^2(G, P)$, there is a unique $\beta \in H^1(G, K^+/P)$ that corresponds to γ under the isomorphism above, and one can write $\beta = \bar{b}(-) \bmod B^1(G, K^+/P)$, $\bar{b}(-) = b(-) \bmod P$ with $b(-) \in C^1(G, K^+)$. So, for all $s, t \in G$, we have $b(st) - b(s) - {}^s b(t) \in P$ and, by definition of the connecting homomorphism which is our isomorphism now, we have

$$c(s, t) \equiv b(st) - b(s) - {}^s b(t) \qquad (\text{mod } B^2(G, P)). \tag{5}$$

Let us now define $f(-) \in C^1(G, K^+)$ by setting $f(s) := b(s)^p - b(s) = \mathscr{P}b(s)$ for all $s \in G$. Then, $f(st) = b(st)^p - b(st) = (b(s) + {}^s b(t) + j(s, t))^p - (b(s) + {}^s b(t) + j(s, t))$ where $j(s, t) \in P$, which in turn is $= b(s)^p - b(s) + {}^s b(t)^p - {}^s b(t) = f(s) + {}^s f(t)$. Therefore, $f(-) \in Z^1(G, K^+)$. But, then, $f(-) \in B^1(G, K^+)$ because $H^1(G, K^+) = 0$, and this means that there exists some $u \in K^+$ such that $f(s) = {}^s u - u$ for all $s \in G$. We conclude that

$$b(s)^p - b(s) = {}^s u - u \qquad \text{for all} \quad s \in G. \tag{6}$$

Our aim is to construct the field L by adjoining a root of $X^p - X - u = 0$. But, before doing that, we need to ensure that $u \notin \mathscr{P}K$. So, assume that $u = w^p - w$ for some $w \in K$. In that case, $b(s)^p - b(s) = {}^s(w^p - w) - ({}^s w - w)$ and, consequently, $(b(s) - ({}^s w - w))^p = b(s) - ({}^s w - w)$. Therefore, for all $s \in G$, $b(s) \equiv {}^s w - w$ (mod P), i.e., $b(-)$ is cohomologous to 0 modulo P, or $\bar{b}(-) \in B^1(G, K^+/P)$. This implies $\beta = 0$ so that $\gamma = 0$. It follows that the assumption of (a), $\gamma \neq 0$, guarantees $u \notin \mathscr{P}K$. If on the other hand the condition (b) $k \not\subset \mathscr{P}K$ is satisfied, then take $\alpha \in k$, $\alpha \notin \mathscr{P}K$. In case the initially chosen $u \in K$ is in $\mathscr{P}K$, replace u by $u + \alpha \notin \mathscr{P}K$. Then, ${}^s(u + \alpha) - (u + \alpha) = {}^s u - u = b(s)^p - b(s)$ for all $s \in G$, so (6) holds with $u + \alpha$ substituted for u. Now let θ be a root of $X^p - X - u = 0$ with $u \notin \mathscr{P}K$ and (6) sustained, and let $L := K(\theta)$. Then, L is a proper Artin–Schreier extension of K with Galois group $P = \mathbb{Z}/p\mathbb{Z}$, and L/k is indeed a Galois extension by virtue of (6) and Theorem 1. It remains to verify that $\text{Gal}(L/k) \simeq E$. To see that, let each $s \in G$ be extended to a k-automorphism of L. Since such an extended automorphism maps θ to $\theta + b(s) + i$ for $i = 0, 1, ..., p-1$ because of (6), let us choose for each $s \in G$ its standard extension $\tilde{s}$ defined by ${}^{\tilde{s}}\theta = \theta + b(s)$. Doing this amounts to choosing a section $G \to \text{Gal}(L/k)$, and one can now calculate the 2-cocycle corresponding to the extension $1 \to P \to \text{Gal}(L/k) \to G \to 1$ as follows: For any $s, t \in G$, $\tilde{s}\tilde{t}$: $\theta \mapsto \theta + b(t) \mapsto \theta + b(s) + {}^s b(t)$ and $(st)^\sim : \theta \mapsto \theta + b(st)$. So, the 2-cocycle $z(-,-)$ satisfying $\tilde{s}\tilde{t} = (st)^\sim \cdot z(s, t)$ is given by $z(s, t) = b(st) - b(s) - {}^s b(t)$ for all $s, t \in G$. By (5), then, $z(s, t) \equiv c(s, t)$ (mod $B^2(G, P)$), and this tells us that $1 \to P \to \text{Gal}(L/k) \to G \to 1$ is equivalent to the group extension originally given. In particular, $\text{Gal}(L/k) \simeq E$.

(Only If) Suppose that the given central extension is realized as Galois groups of the tower of Galois extensions $k \subset K \subset L$ with $\text{Gal}(L/k) \simeq E$. Then, $L = K(\theta)$ for some θ with $\theta^p - \theta - u = 0$, $u \in K$, $u \notin \mathscr{P}K$. Moreover, by

Theorem 1, for any $s \in G$ there is a $b(s) \in K$ such that ${}^s u - u = b(s)^p - b(s)$, and the choice of $b(s)$ is unique modulo P. Now, for any $s, t \in G$, $b(st)^p - b(st) = {}^{st}u - u = {}^s({}^t u - u) + {}^s u - u = {}^s(b(t)^p - b(t)) + b(s)^p - b(s) = (b(s) + {}^s b(t))^p - (b(s) + {}^s b(t))$, which shows that $b(st) - (b(s) + {}^s b(t)) \in P$ always. It follows that $b(-) \bmod P \in Z^1(G, K^+/P)$. By means of calculations just as in the (If) part above, the 2-cocycle in $Z^2(G, P)$ corresponding to our extension fields is easily found to be a $z(-,-)$ satisfying $z(s, t) = b(st) - b(s) - {}^s b(t)$ for all $s, t \in G$. Now, assume that $z(-,-) \in B^2(G, P)$, or equivalently that $b(-) \bmod P \in B^1(G, K^+/P)$. Then, there is $w \in K$ such that, for all $s \in G$, $b(s) = {}^s w - w + i(s)$ with $i(s) \in P$. When that is so, we have

$$\begin{aligned} {}^s u - u &= b(s)^p - b(s) \\ &= ({}^s w - w + i(s))^p - ({}^s w - w + i(s)) \\ &= {}^s(w^p - w) - (w^p - w), \end{aligned}$$

which then gives ${}^s(u - (w^p - w)) = u - (w^p - w)$ for all $s \in G$. Hence, $u = w^p - w + \alpha$ for some $\alpha \in k$. Since $u \notin \mathscr{P}K$, we see $\alpha \notin \mathscr{P}$.

This proves the (Only If) part, and hence the theorem. ∎

2. Examples and Corollaries

In this section we examine the conditions (a) and (b) of Theorem 2 to see which Galois extensions are p-embeddable.

Example 1. Let L/K be a Galois extension of *finite* fields with $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/p\mathbb{Z}$. Since $\mathscr{P}K$ is of index p in K^+ and L contains an element u such that $\mathscr{P}u \in K^+ \setminus \mathscr{P}K$, we have $\mathscr{P}L \cap K^+ = K^+$, or $\mathscr{P}L \supset K$. It follows by Theorem 2 that the only extension $0 \to \mathbb{Z}/p\mathbb{Z} \to E \to \mathbb{Z}/p\mathbb{Z} \to 0$ in which L/K is embeddable is a non-split one, i.e., a cyclic extension. Arguing by induction and observing that the only non-split extension of a cyclic group by $\mathbb{Z}/p\mathbb{Z}$ is cyclic, one retrieves the well-known fact that all Galois p-extensions (indeed *any* Galois extensions) of a finite field are cyclic.

Next we consider finitely generated extension fields as our ground field. In preparation we give a lemma found in [3, Sect. 64.5, pp. 225ff] where, though, the assumption on G appears to be needlessly restrictive. We rehash:

Lemma 1. *Let L/K be a finite Galois extension whose Galois group G is a p-group. Let $A(L/K) := \{u \in L: \mathscr{P}u = u^p - u \in K\}$. Then, there is a natural isomorphism* $\mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}) \simeq A(L/K)/K^+ \simeq (\mathscr{P}L \cap K^+)/\mathscr{P}K$ *of additive groups.*

Proof. Given $\chi \in \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{F}_p)$, one can regard χ as an element of 1-cocycle group $Z^1(G, L^+)$ in Galois cohomology because the action of G on $\mathbb{F}_p \subset L^+$ is trivial. So, there exists $u \in L$ such that $\chi(s) = {}^s u - u$ for all $s \in G$ by the nullity of $H^1(G, L^+)$, and $({}^s u - u)^p = {}^s u - u$. It follows that $u^p - u \in K$. Clearly, for a given χ, such u is uniquely determined modulo K^+. Conversely, for any $u \in A(L/K)$ one just puts $\chi(s) := {}^s u - u$ to define a $\chi \in \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$. Finally, $A(L/K)/K^+ \simeq (A(L/K)/\mathbb{F}_p^+)/(K^+/\mathbb{F}_p^+) \simeq (\mathscr{P}L \cap K)/\mathscr{P}K$ because $\mathrm{Ker}(\mathscr{P}) = \mathbb{F}_p^+$. ∎

We now prove the main result of this section:

THEOREM 3. *Let $K = k(x_1, ..., x_n)$ be a finitely generated extension field of positive transcendence-degree over a field k of characteristic $p > 0$. Then, the index $[K^+ : \mathscr{P}K] = +\infty$.*

Proof. We break up the proof in several steps:

(3.1) If R is a normal domain of characteristic p and $K := \mathscr{Q}(R)$ is the field of quotients of R, then $[R^+ : \mathscr{P}R] = +\infty$ implies $[K^+ : \mathscr{P}K] = +\infty$.

Let $u_1, ..., u_n, ...$ be an infinite sequence of elements of R that are mutually distinct modulo $\mathscr{P}R$. Suppose for a moment that $u_i - u_j$ for some $i \neq j$ belonged to $\mathscr{P}K$, or $u_i - u_j = w^p - w$ for $w \in K$. Since R is integrally closed in K, this means $w \in R$, or $u_i \equiv u_j \pmod{\mathscr{P}R}$, which is a contradiction.

(3.2) For $K = k(t_1, ..., t_n) =$ a purely transcendental extension of a field k, we have $[K^+ : \mathscr{P}K] = +\infty$.

We consider K as the field of quotients of $k(t_2, ..., t_n)[t_1]$ and make use of (3.1). So, we only need to show $[k[t] : \mathscr{P}k[t]] = +\infty$ where $k[t]$ denotes the polynomial ring over k. But it is immediately clear that the elements of the set $\{t^j \mid j > 0 \text{ not divisible by } p\}$ are mutually distinct modulo $\mathscr{P}k[t]$.

(3.3) Let L/K be a finite algebraic extension of fields, and let $A := A(L/K) = \{u \in L \mid \mathscr{P}u \in K\}$. Then, $[\mathscr{P}A : \mathscr{P}K] < +\infty$.

Since A is contained in the separable closure of K within L, it suffices to prove the assertion in case L is separably algebraic over K. Further, we may clearly assume that L is Galoisian over K with $G := \mathrm{Gal}(L/K)$ a p-group. Then, by Lemma 1 above, $\mathscr{P}A/\mathscr{P}K \simeq \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$, which is of course finite.

Theorem 3 is now obvious from (3.1), (3.2), and (3.3) above. ∎

COROLLARY 1. *Let K be a finitely generated extension field of positive transcendence-degree over a field k of characteristic p. Then, for any given* *finite p-group G one can find a Galois extension L of K such that its Galois group* Gal(L/K) *is G.*

Proof. For any finite extension field $F \supset K$ we have $[\mathscr{P}A : \mathscr{P}K] < +\infty$ where $A := A(F/K) = \{u \in F \mid \mathscr{P}u \in K\}$ as in (3.3), while $[K : \mathscr{P}K] = +\infty$ by Theorem 3. This implies $[K : \mathscr{P}A] = +\infty$, so that any Galois extension of K is embeddable in any given extension of its Galois group by $\mathbb{Z}/p\mathbb{Z}$ by virtue of Theorem 2. ∎

In the same vein as Corollary 1 above, there is a classical result due to Witt [14] which we briefly discuss now. Before that, for any p-group G, let G^* be the subgroup generated by all commutators $[x, y] = xyx^{-1}y^{-1}$ and all pth powers z^p. Then G^* is normal, and every homomorphism $G \to$ (abelian group of exponent p) factors uniquely through $G \to G/G^*$. Further, a theorem due to Burnside states that if one writes the order $|G/G^*| = p^n$ then G can be generated by n elements, but never by fewer than n elements (cf. [14, Sect. 1]). Let us denote this number n by $n(G)$.

COROLLARY 2 (Witt's Theorem). *Let K be any field of characteristic p, and let* $[K^+ : \mathscr{P}K] = p^N$. *Let G be a p-group. Then, a Galois extension field L of K with* Gal$(L/K) = G$ *exists if and only if* $n(G) \leqslant N$.

Proof. (Only If) Let $n := n(G)$. Then, $\mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G/G^*, \mathbb{Z}/p\mathbb{Z}) \simeq \mathrm{Hom}((\mathbb{Z}/p\mathbb{Z})^n, \mathbb{Z}/p\mathbb{Z}) \simeq$ (dually) $(\mathbb{Z}/p\mathbb{Z})^n$. So, by Lemma 1, $[\mathscr{P}L \cap K : \mathscr{P}K] = p^n \leqslant [K^+ : \mathscr{P}K] = p^N$.

(If) Write $|G| = p^f$ and use induction on f, the case $f = 1$ being obvious. So, for $f > 1$, make out a central extension $1 \to \mathbb{Z}/p\mathbb{Z} \to G \to H \to 1$ and construct a Galois extension field $B \supset K$ with Gal$(B/K) = H$. Now, in case this group extension is not split, we are done because of Theorem 2. In case it is split, $G \simeq H \times \mathbb{Z}/p\mathbb{Z}$, so that $G^* \simeq H^* \times \{1\}$. This implies $n(H) = n(G) - 1 = n - 1$ and, therefore, $n(H) < N$. By looking at the inclusion $\mathscr{P}K \subset \mathscr{P}B \cap K^+ \subset K^+$ with $[\mathscr{P}B \cap K^+ : \mathscr{P}K] = p^{n(H)}$, we find at once that K^+ properly contains $\mathscr{P}B \cap K^+$. Applying our Theorem 2 to B and H, we establish our assertion. ∎

The above Example 1 and Corollary 1 give the two extreme cases of fields K: one in which *only cyclic* p-groups can occur and the other in which *any* p-group can occur—as Galois groups over K. Note that in these cases $[K : \mathscr{P}K]$ was p and $+\infty$, respectively. We then ask, can the index $[K : \mathscr{P}K]$ be anything else? The answer is yes and is provided by an example due to Madhav Nori as follows:

EXAMPLE 2 (M. Nori). We can construct a field K for which the group $K/\mathscr{P}K$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^m$ for any $m > 1$. It is sufficient to establish this for $m = 2$, as seen readily from what follows, so we stick to this case.

For our purpose, though, it is necessary to draw on the theory of profinite p-groups as founded by Serre [10] (see Shatz [13] also) and to deal with infinite ground field extensions—something we have avoided up to now in order to make our constructions algorithmic. Let k be a field of characteristic p subject to $[k : \mathscr{P}k] = +\infty$. (For instance, $k := \mathbb{F}_p(t)$ will do, in view of Theorem 3.) Within a fixed separably algebraic closure of k take the union E of all Galois p-extensions of k. Then, E/k is an infinite Galois extension with a *free* profinite p-group Γ as its Galois group. It is known and is also easy to see from Lemma 1 that $H^1(\Gamma, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(\Gamma, \mathbb{Z}/p\mathbb{Z}) \simeq k/\mathscr{P}k$, so that Γ is of *infinite rank* (cf. [10, II-5, Sect. 2, Corollary 1; 13, Chap. 3, Sect. 3, Corollaries 1, 2, p. 72]). Let Δ be a free pro-p-subgroup of Γ of rank 2, and let K be the subfield of E consisting of elements fixed by Δ. Then, $\mathrm{Gal}(E/K) \simeq \Delta$, so that $K/\mathscr{P}K \simeq \mathrm{Hom}(\Delta, \mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$, as desired.

References

1. S. S. Abhyankar, Coverings of algebraic curves, *Amer. J. Math.* **79** (1957), 825–826.
2. S. S. Abhyankar, Galois theory on the line, *in* "Abstracts Amer. Math. Soc.," No. 855–14–07, Amer. Math. Soc., Providence, RI, 1990.
3. A. Babakhanian, "Cohomological Methods in Group Theory," Pure Appl. Math., Vol. 11, Dekker, New York, 1972.
4. T. Kambayashi and V. Srinivas, On etale coverings of the affine space, *in* "Algebraic Geometry—Proc. Ann Arbor Conf.," Lecture Notes in Math., Vol. 1008, Springer, Berlin/New York, 1983.
5. T. Kambayashi, Nori's construction of Galois coverings in positive characteristics, *in* "Algebraic and Topological Theories—To the Memory of Dr. Takehiko Miyata," Kinokuniya Bookstores, Ltd., Tokyo, 1985.
6. B. H. Matzat, "Konstruktive Galoistheorie," Lecture Notes in Math., Vol. 1284, Springer, Berlin/Heidelberg/New York, 1987.
7. M. Nori, The fundamental group-scheme, *Proc. Indian Acad. Sci. Math. Sci.* **91** (1982), 73–122.
8. H. Reichhardt, Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung, *J. Reine Angew. Math.* **177** (1937), 1–5.
9. A. Scholz, Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung, I, *Math. Z.* **42** (1937), 161–188.
10. J.-P. Serre, "Cohomologie Galoisienne," Lecture Notes in Math., Vol. 5, Springer, Berlin/Heidelberg/New York, 1965.
11. J.-P. Serre, Construction de revêtements étales de la droite affine en caractéristique p, *C.R. Acad. Sci. Paris Sér. I Math.* **311** (1990), 341–346.
12. I. Shafarevich, On p-extensions, *Mat. Sb.* **20**, No. 62 (1956); *Amer. Math. Soc. Transl. Ser.* 2 **4** (1956), 59–72.
13. S. S. Shatz, "Profinite Groups, Arithmetic, and Geometry," Annals of Math. Studies, Vol. 67, Princeton Univ. Press, Princeton/Tokyo, 1972.
14. E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, *J. Reine Angew. Math.* **174** (1936), 237–245.