ISRAEL JOURNAL OF MATHEMATICS 85 (1994), 391–405

BRAUER GROUPS, EMBEDDING PROBLEMS, AND NILPOTENT GROUPS AS GALOIS GROUPS*

BY

JACK SONN**

Technion—Israel Institute of Technology, Haifa, Israel
e-mail: mar16aa@technion.bitnet

ABSTRACT

Let $\mathbb{Q}_{ab}$ denote the maximal abelian extension of the rationals $\mathbb{Q}$, and let $\mathbb{Q}_{\mathrm{abnil}}$ denote the maximal nilpotent extension of $\mathbb{Q}_{ab}$. We prove that for every prime p, the free pro-p group on countably many generators is realizable as the Galois group of a regular extension of $\mathbb{Q}_{\mathrm{abnil}}(t)$. We also prove that $\mathbb{Q}_{\mathrm{abnil}}$ is not PAC (pseudo-algebraically closed).

Introduction

Let k be a field, G a profinite group. We will say that G is regular over k if there exists a Galois extension K of the rational function field $k(t)$ which is regular over k such that $G(K/k(t)) \cong G$. Let $\mathbb{Q}_{ab}$ denote the maximal abelian extension of the rationals $\mathbb{Q}$, and let $\mathbb{Q}_{\mathrm{abnil}}$ denote the maximal nilpotent extension of $\mathbb{Q}_{ab}$. We prove that for every prime p, the free pro-p group on countably many generators is regular over $\mathbb{Q}_{\mathrm{abnil}}$. This in particular implies that every finite nilpotent group is regular over $\mathbb{Q}_{\mathrm{abnil}}$, and that the same results hold with $\mathbb{Q}_{\mathrm{abnil}}$ replaced by any algebraic extension k of $\mathbb{Q}_{\mathrm{abnil}}$; in particular, every finite nilpotent group is regular over $\mathbb{Q}_{\mathrm{sol}}$, where $\mathbb{Q}_{\mathrm{sol}}$ is the maximal solvable extension of $\mathbb{Q}$. To put this result in perspective, it is known that every finite abelian group is regular over

* This paper was inspired by the author's participation in a special year on the arithmetic of fields at the Institute for Advanced Studies at the Hebrew University of Jerusalem. I would like to express my appreciation to the Institute for its hospitality, and to the organizers, especially Moshe Jarden.

** Partially supported by the Fund for the Promotion of Research at the Technion and by the Technion VPR Fund–Japan Technion Society Research Fund.

Received February 19, 1992 and in revised form January 26, 1993

$\mathbb{Q}$ (see e.g. [M, p.224] or [FJ, Lemma 24.46]), but it is not known if every finite nilpotent group is regular over $\mathbb{Q}$ [Sel, p. 16]. On the other hand, Fried and Völklein [FV] have recently proved that every finite group is regular over k if k is PAC (pseudo-algebraically closed) of characteristic zero. A field k is PAC iff every absolutely irreducible variety defined over k has a k-rational point. It is an open question [FJ, p. 136] whether or not $\mathbb{Q}_{\mathrm{sol}}$ is PAC, but we will prove below that $\mathbb{Q}_{\mathrm{abnil}}$ is not PAC.

The proof parallels the classical method of realizing finite p-groups over number fields, by means of a local-global principle for embedding problems. The role of the classical theorem of Albert—Hasse—Brauer—Noether on the Brauer group of a number field is played here by Theorem 1.1 concerning the injectivity of the canonical map from the Brauer group of a rational function field in one variable to the direct product of the Brauer groups of the completions at the geometric primes.

In this paper we will use the following notations. If F is a field, $\tilde{F}$ will denote the algebraic closure of F, F_s the separable closure of F, $G_F = G(F_s/F)$ the absolute Galois group of F, $\mathrm{Br}(F)$ the Brauer group of F. If A is an abelian group and p is a prime, A_p will denote the p-primary component of A, i.e. the subgroup of A consisting of all elements of p-power order.

1. Brauer groups of rational function fields

THEOREM 1.1: *Let p be a prime number, and let k be a field of characteristic $\neq p, K = k(t)$ a rational function field in one variable over k, $\mathcal{V}$ the set of finite primes of K trivial on k (corresponding to irreducible polynomials in $k[t]$), and K_v the completion of K at $v \in \mathcal{V}$. Then the map*

$$\prod_v \mathrm{res}_v \colon \mathrm{Br}(K)_p \longrightarrow \prod_{v\in\mathcal{V}} \mathrm{Br}(K_v)_p$$

is injective, where K_v denotes the completion of K at v, and $\mathrm{res}_v\colon \mathrm{Br}(K)_p \to \mathrm{Br}(K_v)_p$ the restriction map.

Remark: We are indebted to David Saltman for pointing out that Theorem 1.1 is essentially known, in the framework of the theory of Brauer groups of commutative rings. Indeed in the case $\mathrm{char}(k) = 0$, the injectivity of the map $\mathrm{Br}(K) \to \prod_v \mathrm{Br}(K_v)$ can easily be deduced from [AG, Prop. 7.4, Theorem 7.5, and Prop. 8.2]. Moreover, it is stated in [AG] that all the results in that paper can be proved with no added difficulty for p-primary components in characteristic $\neq p$, so that Theorem 1.1 can be also proved in the same way. Having said this, we will give a "self-contained" proof, which is based on the following lemma.

LEMMA 1.2: *Assume $p \neq \mathrm{char}(k)$. Let $\beta \in k_s$, $k' = k(\beta)$, $F = k'((t-\beta))$ (formal power series field), $E = k_s F$ (the maximal unramified extension of F). Then we have the following commutative diagram:*

$$\begin{array}{ccc} H^2(G_k, k_s(t)^*)_p & \xrightarrow[\text{inf}]{\sim} & H^2(G_{k(t)}, k(t)_s^*)_p = \mathrm{Br}(k(t))_p \\ \Big\downarrow \text{res} & & \Big\downarrow \text{res} \\ H^2(G_{k'}, E^*)_p & \xrightarrow[\text{inf}]{\sim} & H^2(G_F, F_s^*)_p = \mathrm{Br}(F)_p \end{array}$$

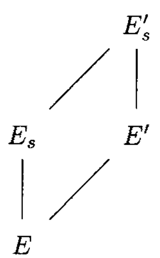
where the horizontal maps are canonical isomorphisms.

Proof: The diagram is commutative because it is induced by an inclusion diagram of fields. (Note that $F_s = k(t)_s F$ by Krasner's Lemma, so G_F can be identified with a subgroup of $G_{k(t)}$.) By the exact inflation-restriction sequence [Se, Prop. 6, p. 156], it suffices to show:

(1) $H^2(G_{k_s(t)}, k(t)_s^*)_p = 0$, and
(2) $H^2(G_E, F_s^*)_p = 0$.

(1) is [FS, Lemma 2, p. 51] (essentially Tsen's theorem).

(2) Observing that E is Henselian and that $E' = k_s((t-\beta))$ is the completion of E, we show first that $G_E \cong G_{E'}$. Consider the field diagram



By a corollary to Krasner's Lemma [Rib, Cor. 2, p. 190], $E_s \cap E' = E$, and by another corollary to Krasner's Lemma [J, Prop. 12.3], $E_s E' = E'_s$. It follows that $G_E \cong G_{E'}$. Let T' be the maximal tamely ramified extension of E'. Every finite subextension of T'/E' is of the form $E'(\pi^{1/n})$ with $\pi = u(t-\beta)$, u a unit in $k_s[[t-\beta]]$ [W, Theorem 3-4-3] since $\mathrm{char}(k) \neq p$. But $u^{1/n} \in E'$, hence $E'(\pi^{1/n}) =$

$E'((t-\beta)^{1/n})$. Since the nth roots of unity lie in E, $E'((t-\beta)^{1/n})/E'$ is a cyclic extension of degree n. It follows that $G(T'/E')$ is a procyclic group, hence $\mathrm{cd}_p G(T'/E') = 1$, where cd_p denotes the cohomological p-dimension. Further, $G(E'_s/T')$ is a pro-q-group, where $q = \mathrm{char}(k)$, so $\mathrm{cd}_p G(E'_s/T') = 0$. By [Ri, Prop. 2.6, p. 209] $\mathrm{cd}_p G_{E'} = 1$. Since $G_E \cong G_{E'}$, $\mathrm{cd}_p G_E \le 1$. It follows that $H^2(G_E, F_s^*)_p = 0$. ∎

Proof of Theorem 1.1: Let $v \in \mathcal{V}$. Then $k(t)_v \cong k(\beta)((t-\beta))$, where β is a root of an irreducible polynomial in $k[t]$ corresponding to v. By Lemma 1.2, it suffices to prove that

$$H^2(G_k, k_s(t)^*)_p \to \prod_{\beta \in k_s/G_k} H^2(G_{k(\beta)}, E_\beta^*)_p$$

is injective, where $E_\beta = k_s.k(\beta)((t-\beta))$.

We decompose $k_s(t)^*$ as a G_k-module:

$$k_s(t)^* = k_s^* \times \coprod_{\alpha \in k_s/G_k} \langle t-\alpha \rangle^{G_k}$$

where $\langle t-\alpha\rangle^{G_k} = \prod_{\sigma \in G_k/G_{k(\alpha)}} \langle t-\alpha\rangle^\sigma$, and k_s/G_k denotes the orbit space of k_s under G_k. Similarly we decompose E_β^* as a $G_{k(\beta)}$-module:

$$E_\beta^* = U_\beta \times \langle t-\beta \rangle$$

where U_β is the group of units of (the valuation ring of) E_β. Passing to cohomology, we have

$$(*) \qquad H^2(G_k, k_s(t)^*)_p \cong H^2(G_k, k_s^*)_p \oplus [\bigoplus_\alpha H^2(G_k, \langle t-\alpha\rangle^{G_k})_p]$$

and

$$H^2(G_{k(\beta)}, E_\beta^*)_p = H^2(G_{k(\beta)}, U_\beta)_p \oplus H^2(G_{k(\beta)}, \langle t-\beta\rangle)_p.$$

Since the map $k_s(t)^* \hookrightarrow E_\beta^*$ carries k_s^* and $\langle t-\alpha\rangle^{G_k}$ into U_β for $\alpha \ne \beta$, the induced map carries $H^2(G_k, k_s^*)_p$ and $\bigoplus_{\alpha\neq\beta} H^2(G_k, \langle t-\alpha\rangle^{G_k})_p$ into $H^2(G_{k(\beta)}, U_\beta)_p$. The remaining summand involves $\langle t-\beta\rangle^{G_k}$ which as $G_{k(\beta)}$-module decomposes as $\langle t-\beta\rangle \times M$, where M is the product of $\langle t-\beta'\rangle$, β' running through the conjugates of β different from β. The map $k_s(t)^* \hookrightarrow E_\beta^*$ carries $\langle t-\beta\rangle$ into $\langle t-\beta\rangle$ and M into U_β. The map

$$H^2(G_k, \langle t-\beta\rangle^{G_k})_p \to H^2(G_{k(\beta)}, \langle t-\beta\rangle)_p \oplus H^2(G_{k(\beta)}, U_\beta)_p$$

factors as follows:

$$\begin{aligned} H^2(G_k, \langle t-\beta\rangle^{G_k})_p &\to H^2(G_{k(\beta)}, \langle t-\beta\rangle \times M)_p \\ &= H^2(G_{k(\beta)}, \langle t-\beta\rangle)_p \oplus H^2(G_{k(\beta)}, M)_p \\ &\to H^2(G_{k(\beta)}, \langle t-\beta\rangle)_p \oplus H^2(G_{k(\beta)}, U_\beta)_p. \end{aligned}$$

By Shapiro's lemma [Ri, Theorem 7.4, p. 146], projection onto the first summand yields an isomorphism

$$H^2(G_k, \langle t-\beta\rangle^{G_k})_p \xrightarrow{\sim} H^2(G_{k(\beta)}, \langle t-\beta\rangle)_p.$$

Now suppose $c \in \mathrm{Br}(k(t))_p$ is in the kernel of all the maps $\mathrm{Br}(k(t))_p \to \mathrm{Br}(k(t)_v)_p$. Looking at the components of c in the decomposition (*) we see that for each β, the component of c in $H^2(G_k, \langle t-\beta\rangle^{G_k})_p$ is zero. Thus $c \in \mathrm{Br}(k)_p$. Finally, take a prime v of degree one, corresponding to t, say. Then the summand $\mathrm{Br}(k)_p$ is carried isomorphically to itself in $\mathrm{Br}(k((t)))_p$, so $c = 0$. ∎

2. Embedding problems

Let K be any field. An **embedding problem** over K is an exact diagram

(2.1)
$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & \swarrow^{f} & \downarrow{\scriptstyle \mathrm{res}} & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow[e]{} & G & \longrightarrow & 1 \end{array}$$

with E finite, $G = G(L/K)$. We will assume A abelian. An embedding problem (2.1) will be called **central** if A maps into the center of E. A (weak) **solution** is a continuous homomorphism $f\colon G_K \to E$ such that $e \circ f = \mathrm{res}$. If the group extension $e\colon E \to G$ happens to split, then there is the **trivial** solution $s \circ \mathrm{res}$, where $s\colon G \to E$ is a section. If f is surjective, f is called a **proper** solution, and the fixed field of $\ker f$ is a **solution field** N with $G(N/K) \cong E$. It is known [FJ, Prop. 24.49] that if K is Hilbertian (and A is abelian), then every embedding problem that has a solution has a proper solution.

PROPOSITION 2.1 ([H, 1.1]): *Let $c \in H^2(G, A)$ correspond to the group extension $1 \to A \to E \to G \to 1$. Then there is a solution to (2.1) if and only if $\inf(c) = 0$, where $\inf : H^2(G, A) \to H^2(G_K, A)$ is the inflation map.*

Now let $\mathcal{V}$ be an index set, and let $\{K_v\colon v \in \mathcal{V}\}$ be a family of extensions of K. Given an embedding problem (2.1) over K, there is an induced embedding problem

$$
(2.2) \qquad \begin{array}{ccccccccc}
 & & & & G_{K_v} & \longrightarrow & G_K & & \\
 & & & {\scriptstyle f_v}\swarrow & \big\downarrow {\scriptstyle \mathrm{res}_v = \mathrm{res}|_{G_{K_v}}} & & & & \\
1 & \longrightarrow & A & \longrightarrow & E_v & \xrightarrow[e_v]{} & G_v & \longrightarrow & 1
\end{array}
$$

where $G_v = \mathrm{res}(G_{K_v}) \subseteq G$, $E_v = e^{-1}(G_v)$. A "global" solution f induces a "local" solution $f_v = f|_{G_{K_v}}$.

PROPOSITION 2.2 (N, 2.2): *Suppose the map*

$$\mathrm{res}\colon H^2(G_K, A) \to \prod_{v \in \mathcal{V}} H^2(G_{K_v}, A)$$

is injective. If the local embedding problem (2.2) *has a solution for all* $v \in \mathcal{V}$, *then the global embedding problem* (2.1) *has a solution.*

Proof: Consider the commutative diagram

$$
\begin{array}{ccc}
H^2(G_K, A) & \xrightarrow{\mathrm{res}} & \prod_v H^2(G_{K_v}, A) \\
\big\uparrow {\scriptstyle \mathrm{inf}} & & \big\uparrow {\scriptstyle \mathrm{inf}} \\
H^2(G, A) & \xrightarrow{\mathrm{res}} & \prod_v H^2(G_v, A)
\end{array}
$$

and apply Proposition 2.1. ∎

Assume now that A (considered as a G_K-module via G) is G_K-isomorphic to μ_n, the group of nth roots of unity in K, where n is a power of a prime $p \neq \mathrm{char}(k)$. We can then identify $H^2(G_K, A)$ with $H^2(G_K, \mu_n)$ which is isomorphic to $\mathrm{Br}_n(K)$, the subgroup of $\mathrm{Br}(K)$ killed by n (consider the exact sequence $0 \to H^2(G_K, \mu_n) \to H^2(G_K, K_s^*) = \mathrm{Br}(K) \xrightarrow{n} H^2(G_K, K_s^*)$ corresponding to the short exact sequence $1 \to \mu_n \to K_s^* \to K_s^* \to 1$).

PROPOSITION 2.3: *Let n be a power of a prime $p \neq \mathrm{char}(k)$, and suppose $A \cong \mu_n$ as G_K-modules. If the map $\mathrm{Br}(K)_p \to \prod_v \mathrm{Br}(K_v)_p$ is injective, then the existence of a solution to the local embedding problem* (2.2) *for all $v \in \mathcal{V}$ implies the existence of a solution to the global embedding problem* (2.1).

Proof: Consider the commutative diagram

$$\begin{array}{ccc} \mathrm{Br}(K)_p & \longrightarrow & \prod_v \mathrm{Br}(K_v)_p \\ \uparrow \subseteq & & \uparrow \subseteq \\ \mathrm{Br}_n(K) & \longrightarrow & \prod_v \mathrm{Br}_n(K_v) \\ \uparrow \cong & & \uparrow \cong \\ H^2(G_K, A) & \longrightarrow & \prod_v H^2(G_{K_v}, A) \end{array}$$

and apply Proposition 2.2. ∎

THEOREM 2.4: *Let K be a rational function field $k(t)$, and $\mathcal{V}$ be the set of finite primes of K (trivial on k). Let n be a power of a prime $p \neq \mathrm{char}(k)$, and let (2.1) be an embedding problem over K with $A \cong \mu_n$ as G_K-modules. If there is a solution to the local embedding problem (2.2) for all $v \in \mathcal{V}$, then there is a proper solution to the global embedding problem (2.1).*

Proof: By Theorem 1.1 and Proposition 2.3, there is a solution to the global embedding problem (2.1). Since K is Hilbertian, there is a proper solution. ∎

We will require the following classical fact about embedding problems.

PROPOSITION 2.5. (cf. [Sh, p.109]): *Let (2.1) be a central embedding problem with $A \cong \mathbb{Z}/p\mathbb{Z}$, p prime, $\mu_p \subseteq K$. Assume there is a solution with solution field $L(\alpha^{1/p})$, $\alpha \in L^*$. Then the set of solution fields coincides with the set of fields $L((a\alpha)^{1/p})$, $a \in K^*$.*

Proof: We begin with the following lemma.

LEMMA 2.6: *Let G be a finite group, p a prime, and let*

$$1 \to \mathbb{Z}/p\mathbb{Z} \to E_i \xrightarrow[e_i]{} G \to 1$$

$i = 1, 2$, be two central group extensions. Then there exists an isomorphism $\varphi: E_1 \to E_2$ such that $e_2\varphi = e_1$ if and only if the two group extensions

$$1 \to \mathbb{Z}/p\mathbb{Z} \to E_1 \times_G E_2 \xrightarrow[\pi_i]{} E_i \to 1$$

split, $i = 1, 2$, where

$$E_1 \times_G E_2 = \{(x_1, x_2) \in E_1 \times E_2 \colon e_1(x_1) = e_2(x_2)\},$$

and π_i: $E_1 \times_G E_2 \to E_i$ is the projection onto E_i.

Proof: Suppose there exists an isomorphism φ: $E_1 \to E_2$ such that $e_2\varphi = e_1$. Then φ induces a homomorphism $\tilde{\varphi}$: $E_1 \to E_1 \times_G E_2$, $\tilde{\varphi}(x) = (x, \varphi(x))$ such that $\pi_1\tilde{\varphi} = \mathrm{id}$, so $1 \to \mathbb{Z}/p\mathbb{Z} \to E_1 \times_G E_2 \xrightarrow{\pi_1} E_1 \to 1$ splits. Applying the same argument to φ^{-1} yields the splitting over π_2.

Conversely suppose the group extensions $1 \to \mathbb{Z}/p\mathbb{Z} \to E_1 \times_G E_2 \xrightarrow{\pi_i} E_i \to 1$ split. Then there exists a homomorphism ψ: $E_1 \to E_1 \times_G E_2$ such that $\pi_1\psi = \mathrm{id}$. Writing $\psi(x) = (\psi_1(x), \psi_2(x))$, we have $\psi_1(x) = x$, and ψ_2: $E_1 \to E_2$ is a homomorphism such that $e_2\psi_2(x) = e_1(x)$ for all $x \in E_1$, so $e_2\psi_2 = e_1$. Then $\ker(\psi_2) \subseteq \ker(e_1) \cong \mathbb{Z}/p\mathbb{Z}$. If $\ker(\psi_2) = 1$, we are done. Otherwise, $\ker(\psi_2) = \ker(e_1) = \mathbb{Z}/p\mathbb{Z}$, ψ_2 factors through $E_1/\ker(e_1)$, so E_2 splits over G. By symmetry, we are reduced to the case where both E_1, E_2 split over G. Since both extensions are central, we are done. ∎

Now to prove Proposition 2.5, let $N_i = L(\alpha_i^{1/p}) \neq L$ be Galois over $K, E_i = G(N_i/K)$, $i = 1, 2$. Suppose first that N_1 is a solution field to the given embedding problem, and that $\alpha_2 = a\alpha_1, a \in K^*$. Then $N = N_1N_2 = N_1(a^{1/p}) = N_1K(a^{1/p})$, so if $N_1 \neq N_2$, $G(N/K) \cong E_1 \times_G E_2$ is a split extension of E_1, so by Lemma 2.6, N_2 is also a solution field.

Conversely, suppose N_1,N_2 are distinct solution fields to the given embedding problem. Then (with $N = N_1N_2$) $G(N/K) \cong E_1 \times_G E_2$, and π_i: $E_i \to G$ is the restriction map. By Lemma 2.6, the group extension $1 \to \mathbb{Z}/p\mathbb{Z} \to G(N/K) \to G(N_1/K) \to 1$ splits, which implies that $N = N_1(a^{1/p})$ with $a \in K^*$. But $N = N_1(\alpha_2^{1/p})$ which by Kummer theory means that $\alpha_2 a^{-1} \in N_1^{*p}$ (replacing a by a power of a if necessary). Then $\alpha_2 a^{-1} \in N_1^{*p} \cap L^*$ implies $L((\alpha_2 a^{-1})^{1/p}) \subseteq N_1$. If equality holds, then by Kummer theory, $\alpha_2 a^{-1}\alpha_1^{-1} \in L^{*p}$ (replacing α_1 by some power of itself if necessary) as desired. Otherwise, $\alpha_2 a^{-1} \in L^{*p}$ and we are in the split case, which implies that also $\alpha_1 \in K^*L^{*p}$, as desired. ∎

3. p-groups as Galois groups

Let p be a fixed prime and k a field of characteristic $\neq p$ such that

(3.1) k contains all p-power roots of unity,

(3.2) every central embedding problem (2.1) over any finite extension k' of k with $A \cong \mathbb{Z}/p\mathbb{Z}$ has a solution.

(3.2) holds e.g. if $\mathrm{cd}_p G_k \leq 1$ [Ri, Prop. 3.1, p. 211].

Example: Every algebraic extension k of $\mathbb{Q}(\mu(p^\infty)), \mu(p^\infty)$ =group of all p-power roots of unity, satisfies (3.1) and (3.2). Indeed, $\mathrm{cd}_p G_k \leq 1$ by [Ri, Theorem 8.8, p. 302].

Definition: Let $K = k(t)$ and let L/K be a finite Galois extension with Galois group G. L/K is a **Scholz** extension iff every prime of K (trivial on k) which ramifies in L is tamely ramified and of degree one in L/K. In other words, if v is a prime of K that ramifies in L, then the local extension L_v/K_v is totally and tamely ramified.

PROPOSITION 3.1: *Assume k satisfies* (3.1) *and* (3.2). *If L/K is a Scholz extension, then every central embedding problem* (2.1) *with $A \cong \mathbb{Z}/p\mathbb{Z}$ has a proper solution.*

Proof: Since $\mu_p \subseteq K$, we have $A \cong \mathbb{Z}/p\mathbb{Z} \cong \mu_p$, so we may apply Theorem 2.4, which reduces the proof to checking that there is a solution to the local embedding problem (2.2) for each finite prime v of K. Let v be a finite prime of K. There are two possibilities.

CASE 1: v is unramified in L. Then $K_v \cong k'((u))$ (formal power series field) where k' is a finite extension of k, and $L_v = LK_v$ is an unramified extension $\ell((u))$ of $k'((u))$. The local embedding problem translates down to an embedding problem over k' with $G = G(\ell/k')$, which has a solution by property (3.2). The solution translates back up to a (unramified) solution to the local embedding problem over K_v.

CASE 2: v ramifies in L. Then L_v/K_v is totally and tamely ramified. Hence $K_v = k'((u))$ and $L_v = k'((u^{1/e}))$, where e is the ramification index [W, 3-4-3], and k' contains the eth roots of unity because L_v/K_v is Galois. The local embedding problem therefore has a proper solution with solution field $k'((u^{1/pe}))$ (note that k' contains the peth roots of unity) if the extension

$$1 \to A \to E_v \to G_v \to 1$$

does not split, and has the trivial solution if the extension splits. ∎

PROPOSITION 3.2: *Let k satisfy* (3.1) *and* (3.2), *L/K a Scholz extension. Then every nonsplit central embedding problem* (2.1) *over K with $A \cong \mathbb{Z}/p\mathbb{Z}$ has a proper solution whose solution field N has the property that every finite prime v of K which is unramified in L remains unramified in N.*

Proof: By Proposition 3.1, there is a solution field N. We may write $N = L(\alpha^{1/p})$, with $\alpha \in$L. Since $G(N/K)$ is a central extension of $G(L/K)$, α is fixed by $G = G(L/K)$ modulo L^{*p}, i.e. $\sigma(\alpha) = \alpha\beta_\sigma^p$, $\beta_\sigma \in L^*$, for every $\sigma \in G$. (Indeed, since N/K is Galois, we have $L(\sigma(\alpha)^{1/p}) = L(\alpha^{1/p}) = N$ for every $\sigma \in G(L/K)$. Fix σ and extend it to N. Then $\sigma(\alpha^{1/p}) = \alpha^{i/p}\beta$, $\beta \in L^*$, $0 \leq i \leq p-1$. Choose $\tau \in G(N/L)$ such that $\tau(\alpha^{1/p}) = \zeta\alpha^{1/p}$, where ζ is a primitive pth root of unity. Then $\sigma\tau(\alpha^{1/p}) = \sigma(\zeta\alpha^{1/p}) = \zeta\alpha^{i/p}\beta$, while $\tau\sigma(\alpha^{1/p}) = \tau(\alpha^{i/p}\beta) = \zeta^i\alpha^{i/p}\beta$. Since τ is in the center of $G(N/K)$, $\zeta^i = \zeta$, so $i = 0$ and $\sigma(\alpha) = \alpha\beta^p$.) Let R be the integral closure of $k[t]$ in L. R is a Dedekind domain with fraction field L. Let $\mathcal{I} = \mathcal{I}_L$ denote the group of fractional ideals of R. It follows that the principal ideal (α) is fixed by G modulo $\mathcal{I}^p$. Write $(\alpha) = \prod_V V^{n_V}$, where V runs through the primes of L. Then $(\sigma(\alpha)) = \prod_V \sigma(V)^{n_V} \equiv \prod_V V^{n_V} (\bmod \mathcal{I}^p)$, for all $\sigma \in G$. Since G acts transitively on the set of prime divisors in L of a fixed prime v of K, we have $n_V \equiv n_{V'} (\bmod p)$ for V, V' dividing the same prime v of K. It follows that $(\alpha) \equiv \mathcal{A}\mathcal{B} (\bmod \mathcal{I}^p)$, where $\mathcal{A}$ and $\mathcal{B}$ are G-invariant ideals, $\mathcal{A}$ is divisible only by primes unramified in L/K and hence is the image in $\mathcal{I}_L$ of an ideal in $\mathcal{I}_K$, which is necessarily principal (since K is a rational function field): $\mathcal{A} = (a)$, $a \in K$; and $\mathcal{B}$ is a product (possibly empty) of primes ramified in L/K, with multiplicities n'_V, $1 \leq n'_V \leq p-1$ and $n'_V \equiv n'_{V'} (\bmod p)$ if V, V' divide the same prime v of K. Replacing α with $a^{-1}\alpha = \beta$ yields a solution field $N' = L(\beta^{1/p})$ to the same embedding problem, by Proposition 2.5, and the only primes ramifying in N'/L are the divisors of $(\beta) \equiv \mathcal{B} \bmod \mathcal{I}_L^p)$, proving Proposition 3.2. ∎

Proposition 3.3: *Let k satisfy* (3.1), (3.2), *and*

(3.3) k^* *is p-divisible, i.e.* $k^{*p} = k^*$.

Let an embedding problem (2.1) *be given, where* $K = k(t)$, $A \cong \mathbb{Z}/p\mathbb{Z}$, *and* L/K *is a Scholz p-extension* (L/K *is Scholz and* $G(L/K)$ *is a p-group). Assume that all the primes of* K *that ramify in* L *are of degree one over* k. *Then there is a proper solution field* $N \supseteq L$ *such that* N/K *is a Scholz extension and all the primes of* K *that ramify in* N *are of degree one over* k.

Proof:

Case 1: *The embedding problem is nonsplit.* Let N be the solution field of Proposition 3.2. Let v be a finite prime of K ramified in N. Then v is ramified in L and therefore v is of degree one over k and L_v/K_v is totally ramified. Claim N_v/K_v is totally ramified. If not, then $N_v = L_vM_v$ where M_v/K_v

is cyclic unramified of degree p. Since v is of degree one, $K_v \cong k((u))$, and $M_v \cong \ell((u))$, where ℓ/k is cyclic of degree p, contradicting (3.3). Thus N_v/K_v is totally ramified. Tame ramification is automatic, since $p \neq \mathrm{char}(k)$.

CASE 2: *The embedding problem is split.* Take a finite prime v_0 of degree one of K which is unramified in L, and let $t-a$ be the corresponding polynomial in $k[t]$. (Note k is infinite by (3.1).) Then $N = L((t-a)^{1/p})$ is a solution field, and all the primes of K that ramify in L are of degree one over k. Hence all the primes of K that ramify in N are of degree one over k. Indeed, the only finite prime that ramifies in $K((t-a)^{1/p})$ is v_0, hence if v is a prime of K that ramifies in N, then it must ramify either in L or in $K((t-a)^{1/p})$, so either v is of degree one by hypothesis or v is v_0 which is of degree one as well. Claim: N/K is a Scholz extension. Since N/K is a p-extension, so is N_v/K_v for every prime v of K. For primes v of degree one over k, the inertia field is a constant p-extension of $k((t))$, which is necessarily trivial, by (3.3). (Again tame ramification is automatic.) ∎

THEOREM 3.4: *Let k satisfy (3.1)–(3.3), and let S be a finite set of primes of $k(t)$ of degree one over k, containing the infinite prime. Let $K = K_S(p)$ be the maximal p-extension of $k(t)$ unramified outside S. Then K is a regular extension of k and $G(K/k(t))$ is the free pro-p group on r generators, where $r = |S| - 1$.*

Proof: We begin by noting that K is a regular extension of k by (3.1) and (3.3). Let $t-a_1, \ldots, t-a_r$ correspond to the finite primes in S. Then $k(t)((t-a_1)^{1/p}, \ldots, (t-a_r)^{1/p}) \subseteq K$ is a Scholz extension of $k(t)$ regular over k with Galois group C_p^r (where C_p denotes the cyclic group of order p), in which the set of ramified primes is exactly S. Let G be the free pro-p group on r generators, $G_1 = \Phi(G) = G^p[G,G]$, the Frattini subgroup of G, and let $G_1 \supset G_2 \supset \cdots$ be a descending chain of open normal subgroups of G with $[G_i\colon G_{i+1}] = p$ for all $i \geq 1$, and $\bigcap_i G_i = \{1\}$. Then $G \cong \varprojlim G/G_i$. By case 1 of the proof of Proposition 3.3, we can inductively construct a tower of fields $k(t) \subset K_1 \subset K_2 \subset \cdots$ such that $K_i/k(t)$ is Galois with group G/G_i, and unramified outside S, since from K_1 onwards, no new primes ramify (Prop. 3.2). Let $L = \bigcup_i K_i$. Then $G(L/k(t)) \cong G$, and $L \subseteq K = K_S(p)$. It remains to show $L = K$. The rank of $G(K/k(t))$ is r, since K_1 is the maximal elementary abelian p-extension of $k(t)$ unramified outside S. It follows that the canonical epimorphism res: $G(K/k(t)) \to G(L/k(t))$ induces the identity map modulo the Frattini subgroups. Since $G(L/k(t))$ is free, res is an isomorphism, hence $L = K$. ∎

Taking the limit over all finite sets of primes of degree one over k (containing the infinite prime) yields

COROLLARY 3.5: *Let k satisfy (3.1)–(3.3). Let $K_1(p)$ be the maximal p-extension of $k(t)$ unramified outside the set of primes of degree one over k. Then $G(K_1(p)/k(t))$ is a free pro-p group on $|k|$ generators.*

Since k is an infinite field, we immediately get

COROLLARY 3.6: *Let k satisfy (3.1)–(3.3). Then every finite p-group G is regular over k, i.e. G is the Galois group of an extension of $k(t)$ which is regular over k.*

4. Examples

1. The maximal extension $\mathbb{Q}_{\rm sol}$ of $\mathbb{Q}$ satisfies (3.1)–(3.3) for all p. We therefore have

COROLLARY 4.1: *For any prime number p, the free pro-p group $\hat{F}_p(\omega)$ on countably many generators is regular over $\mathbb{Q}_{\rm sol}$. Every finite nilpotent group is regular over $\mathbb{Q}_{\rm sol}$.*

Remark: For $k = \mathbb{Q}_{\rm sol}$, $\mathrm{cd}_p G_k = 1$ for all p, by [Ri, Theorem 8.8, p. 302], since e.g. the alternating group A_n is realizable over k for all $n > 4$, and every p divides the order of A_n for some n. Therefore $\mathrm{cd}_p G_{k(t)} = 2$, by [Ri, Prop. 5.2, p. 272], but $\hat{F}_p(\omega)$ is regular over k for every p.

It is not known if $\mathbb{Q}_{\rm sol}$ is a PAC field [FJ, p.136]. If it is, then the second statement in Corollary 3.7 is a special case of a recent theorem of Fried and Völklein, which says that every finite group is regular over k if k is a PAC field of characteristic zero. We give below an example of a non-PAC field which replaces $\mathbb{Q}_{\rm sol}$ in Corollary 3.7.

2. Let p be fixed, and let $k(p)$ be the maximal p-extension of $\mathbb{Q}(\mu_p)$, where μ_p denotes the pth roots of unity. Then $k(p)$ satisfies (3.1)–(3.3). Thus:

COROLLARY 4.2: *The free pro-p group on countably many generators is regular over $k(p)$. Every finite p-group is regular over $k(p)$.*

We will see below that $k(p)$ is not PAC.

Now let $k = \mathbb{Q}_{\rm abnil}$, the maximal nilpotent extension of the maximal abelian extension $\mathbb{Q}_{ab}$ of $\mathbb{Q}$. It is not true that k satisfies (3.3) for all p. However:

COROLLARY 4.3: *Every finite nilpotent group is regular over* $\mathbb{Q}_{\mathrm{abnil}}$.

Proof: First observe that $k(p) \subseteq \mathbb{Q}_{\mathrm{abnil}}$ for all p. Thus every finite p-group is regular over $\mathbb{Q}_{\mathrm{abnil}}$ for all p. Hence so is every finite nilpotent group. ∎

We now show that $\mathbb{Q}_{\mathrm{abnil}}$ is not PAC. By [FJ, p.132], this implies that every subfield of $\mathbb{Q}_{\mathrm{abnil}}$ is also not PAC; in particular the fields $k(p)$ are not PAC.

PROPOSITION 4.4: $\mathbb{Q}_{\mathrm{abnil}}$ *is not PAC.*

Proof (cf. [FJ, Cor. 10.15]): Assume $k = \mathbb{Q}_{\mathrm{abnil}}$ is PAC. Since $k\mathbb{Q}_p \cap \tilde{\mathbb{Q}}$ is Henselian ($\tilde{\mathbb{Q}}$=algebraic closure of $\mathbb{Q}$), it follows from [FJ, Theorem 10.14] that $k\mathbb{Q}_p \supseteq \tilde{\mathbb{Q}}$. By Krasner's lemma [W, 3-2-5], $\tilde{\mathbb{Q}}_p$ (=algebraic closure of $\mathbb{Q}_p$) $= \tilde{\mathbb{Q}}\mathbb{Q}_p$, so $k\mathbb{Q}_p = \tilde{\mathbb{Q}}_p$. Now $\mathbb{Q}_{ab}\mathbb{Q}_p \subseteq \mathbb{Q}_{p,ab}$ (in fact equality holds by local Kronecker–Weber, but we do not need it here). Hence $\tilde{\mathbb{Q}}_p = k\mathbb{Q}_p \subseteq k\mathbb{Q}_{p,ab} \subseteq \mathbb{Q}_{p,\mathrm{abnil}} \subseteq \tilde{Q}_p$, so $\tilde{\mathbb{Q}}_p = \mathbb{Q}_{p,\mathrm{abnil}}$. It remains to show that, for some p, $G(\tilde{\mathbb{Q}}_p/\mathbb{Q}_{p,ab})$ $(= G'_{\mathbb{Q}_p})$ is not nilpotent. Let us show this for $p = 2$ (this holds in fact for all p). If (the commutator subgroup) $G'_{\mathbb{Q}_2}$ were nilpotent, then for every finite Galois extension $K/\mathbb{Q}_p$, $G(K/\mathbb{Q}_p)'$ would be nilpotent. Since $S'_4 = A_4$ is not nilpotent, it suffices to realize S_4 over $\mathbb{Q}_2$:

LEMMA 4.5: S_4 *is a Galois group over* $\mathbb{Q}_2$.

Proof: Let $L = \mathbb{Q}_2(\pi, \omega)$ be the splitting field of $x^3 - 2$ over $\mathbb{Q}_2$, $\pi^3 = 2$, $\omega^3 = 1$, so $L/\mathbb{Q}_2$ is a tamely ramified extension with $G(L/\mathbb{Q}_2) \cong S_3$. Consider the (split) exact sequence

$$1 \to V \to S_4 \to S_3 \to 1$$

where V is the Klein four group. We will solve (properly) the embedding problem given by this sequence. The multiplicative group $L^\star$ of L decomposes into a direct product

$$L^\star = \langle \omega \rangle \times \langle \pi \rangle \times U_L^1$$

where U_L^m = group of units $\equiv 1 \bmod \pi^m$. $U_L^1/U_L^2 \cong \bar{L}^+ \cong \mathbb{F}_4^+$ as abelian groups $[W, 1-5-3]$, where $\bar{L}$ is the residue field of L. U_L^1/U_L^2 is also a G-module, $G = G(L/\mathbb{Q}_2)$, which we can identify with

$$\langle \omega \rangle \times \langle \pi \rangle \times U_L^1/\langle \omega \rangle \times \langle \pi \rangle \times U_L^2 = L^\star/\langle \omega \rangle \times \langle \pi \rangle \times U_L^2.$$

Note $\langle \omega \rangle \times \langle \pi \rangle$ is G-invariant, as is U_L^m. By local class field theory [Se, p. 170 (diagram (3)), p. 174 (Theorem 2), p. 195 (Theorem 1)], U_L^1/U_L^2 is G-isomorphic to $G(N/L)$, where N is an extension of L Galois over $\mathbb{Q}_p$. (N is class field to $\langle\omega\rangle \times \langle\pi\rangle \times U_L^2$.) Thus $E = G(N/\mathbb{Q}_p)$ is an extension of $G(N/L) \cong V$ by $G = G(L/\mathbb{Q}_p) \cong S_3$. Now G acts faithfully on U_L^1/U_L^2, since $\{1, 1+\pi, 1+\omega\pi, 1+\omega^2\pi\}$ are representatives of U_L^1 mod U_L^2. Hence $G = E/V$ acts faithfully on V. It remains to show that $E \cong S_4$. Let C be a subgroup of order 3 of E. C is not normal in E since otherwise C would commute elementwise with V. By Sylow's theorem, the number of conjugate subgroups of C in E is 4, so the normalizer H of C in E is of index 4 in E. The corresponding permutation representation of E on the cosets of H yields a homomorphism of E into S_4 whose kernel J is the intersection of H with its conjugates in E. J does not contain C since C is not normal in E. Hence if J is not trivial, J is of order 2 and normal in E, hence central in E. But this is impossible, since J is not contained in V, and hence maps modulo V to a central element of order 2 in S_3, contradiction. Hence $E \cong S_4$. ∎

References

[AG] M. Auslander and O. Goldman, *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.

[FM] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, 1986.

[FS] B. Fein and M. Schacher, *Brauer groups of rational function fields, in Groupe de Brauer*, Lecture Notes in Math. **844**, Springer-Verlag, Berlin, 1981.

[FV] M. Fried and H. Völklein, *The inverse Galois problem and rational points on modular spaces*, Math. Ann. **290** (1991), 771–800.

[H] K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106.

[J] M. Jarden, *Intersections of local algebraic extensions of a Hilbertian field*, in *Generators and Relations in Groups and Geometries* (A. Barlotti et al., eds.), Kluwer, Dordrecht, 1991.

[M] B.H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Mathematics **1284**, Springer-Verlag, Berlin, 1987.

[N] J. Neukirch, *Über das Einbettungsproblem der algebraische Zahlentheorie*, Inv. Math. **21** (1973), 59–116.

[Ri] L. Ribes, *Introduction of profinite groups and Galois cohomology*, Queens Papers in Pure and Applied Math, 1970.

[Rib] P. Ribenboim, *Theorie des Valuations*, Sem. Math. Sup., University of Montreal Press, 1968.

[Se] J.P. Serre, *Local Fields*, Springer-Verlag, Berlin, 1979.

[Se1] J.P. Serre, *Topics in Galois Theory*, Lecture notes, Harvard University, 1988.

[Sh] I.R. Shafarevich, *On construction of fields with a given Galois group of order* ℓ^α, Transl. Amer. Math. Soc., Ser. 2, **4** (1956), 107–142.

[So] J. Sonn, *On Brauer groups and embedding problems over rational function fields,* J. Algebra **131** (1990), 631–640.

[W] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.