ISRAEL JOURNAL OF MATHEMATICS 119 (2000), 1–8

# FREE PRO-$p$ GROUPS AS GALOIS GROUPS OVER $\mathbb{Q}(p)(t)$

BY

JACK SONN

*Department of Mathematics, Technion — Israel Institute of Technology*
*32000 Haifa, Israel*
*e-mail: sonn@math.technion.ac.il*

ABSTRACT

Let $p$ be a prime and let $\mathbb{Q}(p)$ denote the maximal $p$-extension of $\mathbb{Q}$. We prove that for every prime $p$, the free pro-$p$ group on countably many generators is realizable as a regular extension of $\mathbb{Q}(p)(t)$. As a consequence, if $\mathbb{Q}_{nil}$ denotes the maximal nilpotent extension of $\mathbb{Q}$, then every finite nilpotent group is realizable as a regular extension of $\mathbb{Q}_{nil}(t)$.

## 1. Introduction

Let $k$ be a field, $G$ a profinite group. We 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 $\mathbb{Q}_{nil}$ denote the maximal nilpotent extension of the rationals $\mathbb{Q}$, and let $\mathbb{Q}(p)$ denote the maximal $p$-extension of $\mathbb{Q}$. We prove that for every prime $p$, the free pro-$p$ group on countably many generators is regular over $\mathbb{Q}(p)$. This in particular implies that every finite nilpotent group is regular over $\mathbb{Q}_{nil}$. This result is an improvement on a previous result of the author [4] that the free pro-$p$ group on countably many generators is regular over the maximal $p$-extension $\mathbb{Q}(\mu_p)(p)$ of $\mathbb{Q}(\mu_p)$, the field of $p$th roots of unity, and that every finite nilpotent group is regular over $\mathbb{Q}_{abnil}$, where $\mathbb{Q}_{abnil}$ denotes the maximal nilpotent extension of the maximal abelian extension of $\mathbb{Q}$. The proof is an adaptation of [4, Theorem 3.4], using classical methods of Scholz and Reichardt.

Received June 3, 1999 and in revised form August 4, 1999

## 2. Embedding problems

We recall the notation and terminology of embedding problems. Let $K$ be any field. An **embedding problem** $\mathcal{E}$ over $K$ is given by a short exact sequence of finite groups

$$1 \to A \to E \to_e G \to 1$$

with $G = G(L/K)$ a Galois group. We will assume $A$ abelian. The embedding problem is 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 $e \cdot f = res$, where $res$ denotes the restriction map from $G_K$ to $G$. ($G_K = G(K_s/K)$, where $K_s$ denotes the separable closure of $K$.) If the group extension $e\colon E \to G$ happens to split, then there is the trivial solution $s \cdot res$, where $s\colon G \to E$ is a section. If $f$ is surjective, $f$ is called a **proper** solution, and the fixed field of the kernel of $f$ is a **solution field** $N$ with $G(N/K) \cong E$. It is known [1, Prop. 24.49] that if $K$ is hilbertian (and $A$ is abelian), then every embedding problem that has a solution has a proper solution.

Let $p$ be a prime number and let $K$ be a field of characteristic different from $p$, $K_1 = K(\mu_p)$, where $\mu_p$ denotes the group of $p$th roots of unity. Let $T = G(K_1/K) = \langle\tau\rangle$, where $\tau$ acts on a primitive $p$th root of unity $\zeta$ by raising $\zeta$ to the power $g$. By Kummer Theory we have a canonical $T$-isomorphism between the Galois group of the maximal elementary abelian $p$-extension of $K_1$ and $\mathrm{Hom}(K_1^*/K_1^{*p}, \mu_p)$; in particular, if $a \in K_1^*$, then $K_1(a^{1/p})$ is abelian over $K$ $\Leftrightarrow a^{\tau-g} \in K_1^{*p}$. We will need a lemma, which we put in a slightly more general setting, and which will be useful in comparing embedding problems over $K$ with the corresponding embedding problems over $K_1$.

Let $p$ be a prime, $T = \langle\tau\rangle$ be a cyclic group of order dividing $p-1$. Let $V$ be a $\mathbb{Z}T$-module whose $p$-torsion subgroup $V_p = \{v \in V : pv = 0\}$ is of order 1 or $p$. Let $x$ be a generator of $V_p$. Then $\tau(x) = gx$ for some positive integer $g$, so $x$ is killed by $\tau - g$. If $m$ is the order of $T$, then $g^m \equiv 1 \bmod p$. We may assume $g^m \not\equiv 1 \bmod p^2$, since otherwise we may replace $g$ by $g+p$. Let $\Sigma$ denote the element $\tau^{m-1} + \tau^{m-2}g + \cdots + g^{m-1}$ of $\mathbb{Z}T$. Then $\Sigma(\tau - g) = (\tau - g)\Sigma = \tau^m - g^m = 1 - g^m \equiv 0 \bmod p$ and $\not\equiv 0 \bmod p^2$. Set $\bar{V} := V/pV$, $\bar{\Sigma}, \overline{\tau - g}$ the corresponding elements in $\mathbb{F}_pT$. ($\bar{V}$ is an $\mathbb{F}_pT$-module.)

2.1 Lemma (see [3, p. 123]): *Let $V$ be as above. Then the sequence*

$$\bar{V} \xrightarrow{\bar{\Sigma}} \bar{V} \xrightarrow{\overline{\tau-g}} \bar{V}$$

*is exact.*

*Proof:* From the above discussion, $\overline{\tau - g}\overline{\Sigma} = 0$. Assume $v \in V$, $(\tau - g)v = pw$, $w \in V$. Then applying $\Sigma$, we get $p\Sigma w = \Sigma(\tau - g)v = (1 - g^m)v = prv$, where $p \nmid r$. Then $rv - \Sigma w = sx$, $s \in \mathbb{Z}$. Let $t$ be a solution to the congruence $rt \equiv 1 \bmod p$. Then $\bar{v} = \overline{\Sigma} t\bar{w} + st\bar{x}$. Now $\overline{\Sigma}\bar{x} = mg^{m-1}\bar{x}$, so since $mg^{m-1} \not\equiv 0 \bmod p$, we may choose a multiple $y$ of $x$ such that $\overline{\Sigma}\bar{y} = \bar{x}$. It follows that $\bar{v} = \overline{\Sigma} t\bar{w} + \overline{\Sigma} st\bar{y} = \overline{\Sigma}(t\bar{w} + st\bar{y})$ as desired. ∎

*Remark:* The sequence

$$\bar{V} \xrightarrow{\overline{\Sigma}} \bar{V} \xrightarrow{\overline{\tau - g}} \bar{V}$$

is also exact, by a similar argument.

Let a central embedding problem $\mathcal{E}$:

$$1 \to A \to E \to_e G \to 1$$

be given, $G = G(L/K)$ a finite $p$-group, $A \cong \mathbb{Z}/p\mathbb{Z}$. Consider the inflated embedding problem $\mathcal{E}_1$:

$$1 \to A \to E_1 \to_{e_1} G_1 \to 1$$

with $G_1 = G(L_1/K)$, $L_1 = L(\mu_p) = LK_1$, where the following diagram is exact and commutative:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E_1 & \xrightarrow{e_1} & G_1 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \tilde{\pi}} & & \downarrow{\scriptstyle \pi} & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{e} & G & \longrightarrow & 1 \end{array}$$

We have $G_1 \cong G \times T$, $E_1 \cong E \times T$, where $T = \langle \tau \rangle$ is again $G(K_1/K)$.

2.2 LEMMA: *The inflated embedding problem $\mathcal{E}_1$ has a proper solution if and only if the original embedding problem $\mathcal{E}$ has a proper solution. In fact, there is a canonical one-one correspondence between proper solutions to the two embedding problems.*

*Proof:* Suppose $f_1$ is a proper solution to $\mathcal{E}_1$. Then $\tilde{\pi} f_1 = f$ is a proper solution to $\mathcal{E}$. Conversely suppose $f\colon G_K \to E$ is a proper solution to $\mathcal{E}$. Then since there is a unique monomorphism (section) $\tilde{s}\colon E \to E_1$ such that $\tilde{\pi}\tilde{s} = id_E$, $f_1 := \tilde{s} f \times res_{K_s/K_1}\colon G_K \longrightarrow E_1$ is a proper solution to $\mathcal{E}_1$ uniquely determined by $f$. ∎

We now wish to describe *all* solutions to $\mathcal{E}_1$.

2.3 PROPOSITION: *Let $\mathcal{E}_1$ have solution field $L_1(\alpha^{1/p})$ ($L_1$ contains $\mu_p$). Then every other solution field looks like $L_1(\beta^{1/p})$ with $\beta = a\alpha$, $a \in K_1$, $a^{\tau-g} \in K_1^* \cap L_1^{*p}$, where $\zeta^\tau = \zeta^g$ as above.*

*Proof:* Let $N_1 = L_1(\beta^{1/p})$ be a solution field, $\beta \in L_1$. By [4, Prop. 2.5], $\beta = a\alpha$, $a \in K_1$, since $N_1$ is also a solution to the restricted embedding problem for $L_1/K_1$. The condition that $G(N_1/L_1)$ be central in $G(N_1/K)$ is equivalent by Kummer theory to $G(L_1/K)$ acting trivially on the dual $\mathrm{Hom}(\langle\beta\rangle L_1^{*p}/L_1^{*p}, \mu_p)$, i.e. $\beta^{\tau-g} \in L_1^{*p}$. Since the same holds for $\alpha$, we have $a^{\tau-g} = (\beta/\alpha)^{\tau-g} \in L_1^{*p}$.

Conversely, if $a \in K_1^*$, and $a^{\tau-g} \in L_1^{*p}$, then since $\alpha^{\tau-g} \in L_1^{*p}$, $(a\alpha)^{\tau-g} \in L_1^{*p}$, and $L_1((a\alpha)^{1/p})$ is also a solution field. ∎

We now assume further that $K = k(t)$ is a rational function field in one variable. Let $\mathcal{P}$ denote the set of all finite primes of $K/k$, i.e. monic irreducible polynomials in $k[t]$, $\mathcal{P}_1$ the set of finite primes of $K_1/k_1$, where $k_1 = k(\mu_p)$ and $K_1 = K(\mu_p)$. (The infinite prime corresponds to the negative degree valuation.) By [4, Theorem 1.1], the upper map in the commutative diagram of restriction maps

$$\begin{array}{ccc} H^2(G_{K_1}, A) & \longrightarrow & \prod_{\mathfrak{p}_1\in\mathcal{P}_1} H^2(G_{K_{1\mathfrak{p}_1}}, A) \\ \uparrow & & \uparrow \\ H^2(G_K, A) & \longrightarrow & \prod_{\mathfrak{p}\in\mathcal{P}} H^2(G_{K_\mathfrak{p}}, A) \end{array}$$

is injective. ($K_\mathfrak{p}$ denotes the completion of $K$ at $\mathfrak{p}$.) Since the left vertical arrow is injective ($cor \cdot res = m$ and $m|p-1$), the lower right arrow is also injective. By [4, Prop. 2.2], the local-global principle holds for $\mathcal{E}_1$, i.e. there is a solution to $\mathcal{E}_1$ $\Leftrightarrow$ there is a solution to the induced local embedding problem $\mathcal{E}_{1\mathfrak{p}}$ corresponding to

$$1 \to A \to E_{1\mathfrak{p}} \to G(L_{1\mathfrak{p}}/K_\mathfrak{p}) \to 1$$

for every finite prime $\mathfrak{p}$ of $K/k$.

Define $L/K$ to be **Scholz** iff every prime of $K$ which ramifies in $L$ is of relative degree 1 in $L/K$ (totally ramified).

2.4 PROPOSITION: *Assume $k$ is an algebraic extension of $\mathbb{Q}$ containing the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, $K = k(t)$, and $L/K$ Scholz. Then every embedding problem*

$$\mathcal{E}\colon 1 \to \mathbb{Z}/p\mathbb{Z} \to E \to_e G \to 1$$

*has a proper solution.*

*Proof:* By the local-global principle, it suffices to show local solvability at every finite prime $\mathfrak{p}$.

CASE 1. $\mathfrak{p}$ UNRAMIFIED: Then $K_\mathfrak{p} = k'((u))$ (formal power series field), where $k'$ is a finite extension of $k$, and $L_\mathfrak{p} = LK_\mathfrak{p}$ is an unramified extension $\ell((u))$ of $k'((u))$. The local embedding problem descends to a central embedding problem over $k'$, and has a solution by [2, p. 211] ($k'$ has cohomological $p$-dimension $\leq 1$).

CASE 2. $\mathfrak{p}$ RAMIFIED: Then $\mathfrak{p}$ has relative degree one in $L$, so $L_\mathfrak{p}/K_\mathfrak{p}$ is a (cyclic) totally ramified extension. If the local embedding problem splits, then it has a (trivial) solution. If not, then by [5, 3-4-3], $K_\mathfrak{p}$ contains the $p$th roots of unity, hence all $p$-power roots of unity ($k$ contains the cyclotomic $\mathbb{Z}_p$ -extension of $\mathbb{Q}$). Therefore the local embedding problem has a solution. ∎

2.5 PROPOSITION: *Let $k$ be arbitrary, $K = k(t)$. Then every nonsplit central embedding problem with $A \cong \mathbb{Z}/p\mathbb{Z}$, which has a (proper) solution, has a (proper) solution with solution field $N$ such that every finite prime unramified in $L/K$ is unramified in $N/K$ as well.*

*Proof:* Let $N$ be the given solution field. Then by Lemma 2.2 and Proposition 2.3, the corresponding inflated embedding problem has solution field $N_1 := N(\mu_p) = L_1(\alpha^{1/p})$, $\alpha \in L_1$, with $G_1 \cong G \times T$ acting on $\langle\alpha\rangle L_1^{*p}/L_1^{*p}$ by $\alpha^{\sigma-1} \in L_1^{*p}$, $\sigma \in G$, and $\alpha^{\tau-g} \in L_1^{*p}$, $\tau \in T$ the fixed generator.

Let $k_1 = k(\mu_p)$ as before, and let $R$ be the integral closure of $k_1[t]$ in $L_1$. $R$ is a Dedekind domain with fraction field $L_1$. Let $I = I_{L_1}$ be the group of fractional ideals of $L_1$. The principal ideal $(\alpha)$ has its factorization $\prod_\mathfrak{P} \mathfrak{P}^{n_\mathfrak{P}}$. For $\sigma \in G$, $(\alpha)^\sigma = \prod_\mathfrak{P} (\mathfrak{P}^\sigma)^{n_\mathfrak{P}} \equiv \prod_\mathfrak{P} \mathfrak{P}^{n_\mathfrak{P}} \bmod^\times I^p$, so $n_\mathfrak{P} \equiv n_{\mathfrak{P}^\sigma} \bmod p$ for $\sigma \in G$, hence $(\alpha) \equiv \mathfrak{A}\mathfrak{B} \bmod^\times I^p$ where $\mathfrak{A}$ is a product of ramified prime ideals (in $L_1/K_1$) with conjugate primes occurring to the same power, and $\mathfrak{B}$ is a product of prime ideals unramified in $L_1/K_1$ (hence also in $L_1/K$ since $K_1/K$ is unramified), again with conjugate primes occurring to the same power, hence we may assume $\mathfrak{B}$ to be a product of primes of $K_1$, since $\mathfrak{B}$ (as well as $\mathfrak{A}$) is $G$-invariant mod $p$-th powers.

$k_1[t]$ is a principal ideal domain, so $\mathfrak{B} = (b)$, $b \in K_1^*$. $(\alpha)^{\tau-g} \in I^p \implies \mathfrak{A}^{\tau-g}\mathfrak{B}^{\tau-g} \in I^p$. The set of primes of $L_1$ ramified in $L_1/K_1$ is equal to the set of primes of $L_1$ ramified in $L_1/K$, so is $\tau$-invariant. It follows that $\mathfrak{A}^{\tau-g}$, $\mathfrak{B}^{\tau-g}$ each lie in $I^p$, since they are relatively prime. $\mathfrak{B} = (b)$, $b \in K_1$, so $(b)^{\tau-g} \in I^p \cap I_{K_1}$. Since $(b)$ consists of primes unramified in $L_1$, $(b)^{\tau-g} \in I_{K_1}^p$, so we may assume $b^{\tau-g} \in K_1^{*p}$. Then replacing $\alpha$ by $\beta = \alpha b^{-1}$ yields another solution to the embedding problem $\mathcal{E}_1$ (Proposition 2.3), and the ideal $(\beta)$ is divisible only by primes ramified in $L_1/K$. ∎

2.6 THEOREM: *Let $k = \mathbb{Q}(p)$, the maximal p-extension of $\mathbb{Q}$, $K = k(t)$. Let $a_1, \ldots, a_n \in k_1$, mutually nonconjugate over $k$, such that each $a_i$ has $p-1$ distinct $T$-conjugates. Let $p_i(t)$ be the minimal polynomial of $a_i$ over $k$, i.e. $p_i(t) = \prod_{\rho \in T}(t - a_i^\rho)$. Let $S = \{p_1(t), \ldots, p_n(t), \infty\}$. Then the maximal p-extension of $K$ unramified outside $S$ is a regular extension of $k$ and its Galois group is a free pro-p group on $n$ generators.*

*Proof:* Regularity is immediate from the fact that $\mathbb{Q}(p)$ has no $p$-extensions. Set

$$u_i = (t - a_i)^\Sigma = (t - a_i)^{\tau^{p-2} + \tau^{p-3}g + \cdots + g^{p-2}}, \quad i = 1, \ldots, n$$

(here $m = p - 1$). Then $M_1 = K_1(u_1^{1/p}, \ldots, u_n^{1/p})$ is a $C_p^n \times C_{p-1}$-extension of $K$, unramified outside $S$. ($M_1$ is abelian over $K$ by Lemma 2.1 and the Kummer-theoretic argument in the proof of Proposition 2.3.) Let $M$ be the unique $C_p^n$-extension inside it.

CLAIM: *$M$ is the maximal elementary abelian p-extension of $K$ unramified outside $S$.*

Indeed, consider $U = K_1^*/K_1^{*p}$, as an $\mathbb{F}_pT$-module. Then $U = U_0 \oplus (\bigoplus_q U_q)$, where $U_0 = k_1^*/k_1^{*p}$, and for each monic irreducible polynomial $q = q(t) \in k_1[t]$, $U_q$ is the submodule with $\mathbb{F}_p$-basis the (cosets of the) distinct $T$-conjugates of $q$.

By Kummer Theory, each submodule $W$ of $U$ corresponds to an elementary abelian $p$-extension of $K_1$ which is Galois over $K$. Moreover, the primes that ramify in this extension are exactly those which are in the support of nonzero elements of $W$, i.e. those that appear with nonzero coefficient when a nonzero element of $W$ is written as a linear combination of the basis elements coming from the irreducible polynomials $q$ mentioned above. We now take $W = \bigoplus_i U_{t-a_i}$, which corresponds to the maximal elementary abelian $p$-extension $M_1$ of $K_1$ unramified outside (the primes above) $S$. Furthermore, $W$ decomposes into a direct sum of eigenspaces $\bigoplus_r W_r$, where $0 \le r \le p-1$, and $W_r = \{w \in W : \tau(w) = rw\}$. Thus $W_g$ corresponds to the maximal elementary abelian $p$-extension of $K$ contained in $M_1$, i.e. unramified outside $S$. ($W_g$ corresponds via Kummer Theory to the composite of cyclic extensions of degree $p$ of $K_1$ which are abelian over $K$ and contained in $M_1$.) Apply Lemma 2.1 with $V$ the subgroup of $K_1^*$ generated by the $t - a_i$ and their conjugates; so $\bar{V} = W$, and $W_g = W^\Sigma$ (multiplicative notation), which is spanned by the classes $\overline{t - a_i}^\Sigma$, noting, by the remark preceding Lemma 2.1, that

$$\overline{u_i}^\tau = \overline{t - a_i}^{\tau\Sigma} = \overline{t - a_i}^{\Sigma\tau} = \overline{t - a_i}^{\Sigma g} = \overline{u_i}^g,$$

proving the claim.

If $G$ is the free pro-$p$ group on $n$ generators, $G(M/K) \cong G/\Phi G$, where $\Phi G$ is the Frattini subgroup of $G$. $M/K$ is Scholz, because all the ramified primes have residue field $\mathbb{Q}(p)$.

Let $G \supset \Phi G = G_1 \supset G_2 \supset \cdots$ be a chain of normal subgroups with quotients $G_i/G_{i+1} \cong \mathbb{Z}/p\mathbb{Z}$, $i \geq 1$, and $\bigcap_i G_i = \{1\}$. We inductively prove that there is a tower of Scholz extensions $N_i$ with $G(N_i/K) \cong G/G_i$ in which only the primes $p_1(t), \ldots, p_n(t), \infty$ ramify. It will then follow that $N := \bigcup_i N_i$ is a $p$-extension of $K$ with Galois group free pro-$p$ on $n$ generators, unramified outside $S$. It is therefore the maximal one, since otherwise $M$ above would not be the maximal elementary abelian $p$-extension of $K$ unramified outside $S$. Set $N_1 = M$. Assume inductively that $N_i/K$ is Scholz and unramified outside $S$, $i \geq 1$. The embedding problem corresponding to

$$1 \to \mathbb{Z}/p\mathbb{Z} \to G/G_{i+1} \to G/G_i \cong G(N_i/K) \to 1$$

is nonsplit ($G_i \subset \Phi G$), so by Propositions 2.4 and 2.5, there is a (proper) solution field $N_{i+1}$ unramified outside $S$. Since $N_i/K$ is Scholz, every prime ramified in $N_i$ has relative degree one, so if a ramified prime $\mathfrak{p}$ in $N_{i+1}$ has degree greater than one, its degree is $p$, and the local extension at $\mathfrak{p}$ contains a $C_p$-extension of $\mathbb{Q}(p)$=residue field of $\mathfrak{p}$, contradiction. It follows that $N_{i+1}/K$ is Scholz. ∎

The remaining discussion parallels that in [4, Sections 3, 4]. Taking the limit over finite sets $S$ as in the preceding theorem, we get

2.7 THEOREM: *The free pro-p group on countably many generators is regular over* $\mathbb{Q}(p)$.

Furthermore, translating up from $\mathbb{Q}(p)(t)$ to $\mathbb{Q}_{nil}(t)$, we get

2.8 THEOREM: *The free pro-p group on countably many generators is regular over* $\mathbb{Q}_{nil}$. *Every finite nilpotent group is regular over* $\mathbb{Q}_{nil}$.

We remark that $\mathbb{Q}_{nil}$ is not PAC [1, Cor. 10.15].

ACKNOWLEDGEMENT: The author is grateful to Moshe Jarden for his corrections and suggestions which have improved the exposition of this paper.

The research was supported by the Fund for the Promotion of Research at the Technion and the Technion VPR Fund.

## References

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

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

[3] I. R. Shafarevich, *On construction of fields with a given Galois group of order* $\ell^\alpha$, American Mathematical Society Translations **4** (1956), 107–142.

[4] J. Sonn, *Brauer groups, embedding problems, and nilpotent groups as Galois groups*, Israel Journal of Mathematics **85** (1994), 391–405.

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