Pacific Journal of Mathematics

MINIMAL RAMIFICATION IN NILPOTENT EXTENSIONS

NADYA MARKIN AND STEPHEN V. ULLOM

Volume 253 No. 1 September 2011

PACIFIC JOURNAL OF MATHEMATICS
Vol. 253, No. 1, 2011

MINIMAL RAMIFICATION IN NILPOTENT EXTENSIONS

NADYA MARKIN AND STEPHEN V. ULLOM

Let G be a finite nilpotent group and K a number field with torsion relatively prime to the order of G. By a sequence of central group extensions with cyclic kernel we obtain an upper bound for the minimum number of prime ideals of K ramified in a Galois extension of K with Galois group isomorphic to G. This sharpens and extends results of Geyer and Jarden and of Plans. Alternatively, we show how to use Fröhlich's result on realizing the Schur multiplicator in order to realize a family of groups given by central extensions with minimal ramification.

1. Introduction

Given a number field K and a finite group G an important problem is to find a Galois extension L of K such that its Galois group $\mathrm{Gal}(L/K)$ is isomorphic to G. Scholz and Reichardt (see [Serre 1992] for a modern account) proved independently that any l-group G, l an odd prime, occurs as the Galois group of an extension of the rationals. Shafarevich [1954] has shown for any solvable group G and number field K that there exists a Galois extension L/K with $G \cong \mathrm{Gal}(L/K)$. In this paper we ask, for given K and nilpotent G, what is the minimum number

$$\min \mathrm{ram}_K(G)$$

of prime ideals of K ramified in L as L runs over extensions of K that satisfy $\mathrm{Gal}(L/K) \cong G$? We rephrase the question for l-groups G: For a given finite set S of prime ideals of K, let $K(l, S)$ denote the maximal l-extension of K that is unramified outside S. How large must S be so that G is isomorphic to a quotient group of $\mathrm{Gal}(K(l, S)/K)$ for some S?

One knows from [Serre 1992] that $\min \mathrm{ram}_{\mathbb{Q}}(G) \leq n$ if G is an l-group of order l^n, where $l \neq 2$. If G is an abelian group, an application of class field theory (Theorem 5.2) shows $\min \mathrm{ram}_K(G) \leq d(G) :=$ minimum number of generators of G. In fact for the case $K = \mathbb{Q}$, Boston's conjecture [Boston and Markin 2009] implies that $\min \mathrm{ram}_{\mathbb{Q}}(G) \leq d(G)$ for all finite groups G.

Markin's research was supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006.

MSC2000: 12F12, 11S31, 12F10, 11R32.

Keywords: class field theory, inverse Galois theory, nilpotent groups.

Suppose G is a nilpotent group and the field K is such that, for each prime l dividing the order $|G|$ of G,

(1) K does not contain a primitive l-th root of unity ζ_l, and

(2) K has no ideal classes of order l^2.

Then Theorem 8.4 states that

$$\min \operatorname{ram}_K(G) \leq \sum_{i \geq 1} d(G_i/G_{i+1}) + t(K).$$

Here $\{G_i\}$ is the lower central series of G and $t(K)$ is a constant depending only on K. This extends Plans' result [2004] on $\min \operatorname{ram}_{\mathbb{Q}}(G)$ to all number fields K satisfying conditions (1) and (2) above. Secondly, Geyer and Jarden [1998] obtain the bound $\min \operatorname{ram}_K(G) \leq n + t(K)$, where the l-group G has order l^n and $\zeta_l \notin K$. We obtain an improved bound by considering central embedding problems with a cyclic kernel, not just a kernel of prime order. Note that without condition (2), the methods of Section 8 still generalize the results of [Geyer and Jarden 1998] to nilpotent groups, giving a weaker bound for a nilpotent group G of order $\prod_{l \,||G|} l^{n_l}$, namely

$$\min \operatorname{ram}_K(G) \leq \max_{l \,||G|}\{n_l\} + t(K).$$

We generalize Geyer and Jarden's definition of an exceptional set T of primes to the prime power setting in Section 4; this provides the technical tool for constructing idèle class characters with strictly controlled ramification.

The realization of l-groups is carried out in three steps, similarly to [Geyer and Jarden 1998; Serre 1992; Plans 2004]. The first step involves solving an embedding problem given a Scholz extension; in the second we remove ramification in the solution outside the set of exceptional primes, and in the third step we force the solution to be Scholz at the cost of one extra ramifying prime. Finally in Section 8, for G nilpotent this prime is chosen to be the same for all primes l dividing the order of G.

We take another approach to the problem of realization of Galois groups with minimal ramification in Section 9. Take $K = \mathbb{Q}$ or an imaginary quadratic field with $\zeta_l \notin K$. We consider a family of l-extensions of K obtained from central extensions by the Schur multiplicator and observe that a result of Fröhlich [1983] for $K = \mathbb{Q}$, extended to imaginary quadratic fields by Watt [1985], realizes the corresponding family of groups with minimal ramification.

2. The embedding problem

Fix an algebraic closure $\bar{K}$ of a number field K and let $G_K = \operatorname{Gal}(\bar{K}/K)$ denote the absolute Galois group of K. An *embedding problem* (G_K, ρ, α) for G_K (see

[Neukirch et al. 2000], for example) is a diagram with an exact sequence of finite groups and epimorphism ρ:

(2-1)
$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & \swarrow^{\phi} & \downarrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & C & \longrightarrow & G & \xrightarrow[\alpha]{} & \bar{G} & \longrightarrow & 1. \end{array}$$

A solution ϕ of the embedding problem is a homomorphism $\phi : G_K \to G$ such that $\alpha \circ \phi = \rho$; a solution is *proper* if ϕ is surjective. If G, $\bar{G}$ are l-groups with the same number of generators, it is easily seen that every solution is proper. When the kernel group C is contained in the center of G, the embedding problem ((2-1)) is called a *central embedding problem*. Every nilpotent group can be realized as a Galois group by solving a sequence of central embedding problems. For every prime $\mathfrak{p}$ of K, fix a prime of $\bar{K}$ above $\mathfrak{p}$ and let $D_\mathfrak{p}$ and $I_\mathfrak{p}$ denote its decomposition and inertia subgroups in G_K.

Let

(2-2)
$$\begin{array}{ccccccccc} & & & & & & D_\mathfrak{p} & & \\ & & & & & \swarrow^{\phi_\mathfrak{p}} & \downarrow{\scriptstyle \rho_\mathfrak{p}} & & \\ 1 & \longrightarrow & C & \longrightarrow & G_\mathfrak{p} & \xrightarrow[\alpha_\mathfrak{p}]{} & \bar{G}_\mathfrak{p} & \longrightarrow & 1 \end{array}$$

denote the corresponding local embedding problem, where $\bar{G}_\mathfrak{p} = \rho(D_\mathfrak{p})$, $G_\mathfrak{p} = \alpha^{-1}(\bar{G}_\mathfrak{p})$, and $\alpha_\mathfrak{p}$, $\rho_\mathfrak{p}$ are restrictions of α, ρ.

In this section we assume in (2-1) that G is an l-group and the kernel C has prime order. Let S_0 be any finite set of primes of K containing the infinite primes, the prime divisors of l, and the prime divisors of a set of ideals representing the ideal classes of K. (In Section 8, where G is any finite nilpotent group, S_0 will contain in addition the divisors of the order of G.) It is known from [Geyer and Jarden 1998] that a solution to a global embedding problem (2-1) exists if and only for every prime $\mathfrak{p}$ of K there exists a solution to the local embedding problem (2-2). The local embedding problem is solvable if $\rho(I_\mathfrak{p}) = 1$, since $D_\mathfrak{p}/I_\mathfrak{p} \cong \hat{\mathbb{Z}}$ is a free group; the Scholz condition ensures solvability at the ramified primes. Let $\mathrm{Ram}(\rho) = \{\mathfrak{p} \text{ of } K \mid \rho(I_\mathfrak{p}) \neq 1\}$.

Definition 2.1 [Geyer and Jarden 1998, §3.2]. Let K be a number field, G an l-group, and N a positive integer such that l^N is divisible by the exponent of G. Denote by T a set of l^N-exceptional primes as defined in Section 4. An epimorphism $\phi : G_K \to G$ is l^N-Scholz if

- for $\mathfrak{p} \in \mathrm{Ram}(\phi) \cup T$, $\phi(D_\mathfrak{p}) = \phi(I_\mathfrak{p})$;
- for $\mathfrak{p} \in \mathrm{Ram}(\phi)$, the absolute norm $N(\mathfrak{p}) \equiv 1 \pmod{l^N}$;
- for $\mathfrak{p} \in S_0$, $\phi(D_\mathfrak{p}) = 1$.

The last condition is an example of local data of [Geyer and Jarden 1998]. We will also say the extension L/K is l^N-Scholz, where L is the subfield of $\bar{K}$ fixed by $\ker\phi$.

The definition of l^N-Scholz does not depend on the choice of prime of $\bar{K}$ above each $\mathfrak{p}$. Clearly an l^N-Scholz homomorphism is l^k-Scholz for all integers $k \leq N$.

3. Existence of solutions

Theorem 3.1 (existence). *Let (G_K, ρ, α) be a central embedding problem, with $\bar{G} = \rho(G_K)$ an l-group and $C = \ker\alpha$ cyclic of order l^e. Suppose ρ is l^N-Scholz (the exponent of G divides l^N) and $\zeta_l \notin K$. Then the embedding problem*

(3-1)
$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & \swarrow^{\psi_0} & \downarrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & C & \longrightarrow & G & \xrightarrow[\alpha]{} & \bar{G} & \longrightarrow & 1. \end{array}$$

has a solution.

Proof. If G is a split extension of $\bar{G}$, we may apply Proposition 5.3, so assume the extension is Frattini, i.e., C is contained in the Frattini subgroup of G. We may break (3-1) into a sequence of e embedding problems each with kernel group of order l, which we may solve by Proposition 7.3 of [Geyer and Jarden 1998] at the cost of one ramified prime at each step. We obtain an l^N-Scholz solution ψ_0 to (3-1) such that

$$\mathrm{Ram}(\psi_0) \cup T = \mathrm{Ram}(\rho) \cup T \cup \{e \text{ primes of } K\} \qquad \square$$

In Sections 5–7 we will show that the embedding problem (3-1) has an l^N-Scholz solution at the cost of only one additional ramified prime (assuming K has no ideal classes of order l^2 if $|C| > l$).

4. The exceptional set of primes

The key result, Lemma 4.2, was originally proved in a different way in [Markin 2006]. The next lemma below generalizes [Gras 2003, Chapter II, Theorem 6.3.2] and [Rubin 1991, Lemma 4.1, p. 361].

Lemma 4.1. *Let L/K be a Galois l-extension, $\tilde{K} = K(\mu_m)$, $\tilde{L} = L(\mu_m)$, where m is a power of l. If $\zeta_l \notin K$, then the canonical map*

$$K^\times/K^{\times m} \to \tilde{L}^\times/\tilde{L^\times}^m$$

is injective.

Proof. From Kummer theory, we have $H^1(\mathrm{Gal}(\bar{K}/K), \mu_m) \cong K^\times/K^{\times m}$ and $H^1(\mathrm{Gal}(\bar{K}/\tilde{L}), \mu_m) \cong \tilde{L}^\times/\tilde{L^\times}^m$, where $\bar{K}$ denotes an algebraic closure of K. The extensions $K \subseteq \tilde{L} \subseteq \bar{K}$ give the following exact sequence of cohomology groups via the restriction-inflation maps

$$1 \to H^1(\mathrm{Gal}(\tilde{L}/K), \mu_m^\gamma) \to H^1(\mathrm{Gal}(\bar{K}/K), \mu_m) \to H^1(\mathrm{Gal}(\bar{K}/\tilde{L}), \mu_m),$$

where $\gamma = \mathrm{Gal}(\bar{K}/\tilde{L})$. It suffices to prove $H^1(\mathrm{Gal}(\tilde{L}/K), \mu_m^\gamma) = 0$; note that $\mu_m^\gamma = \mu_m$. By a second application of the restriction-inflation sequence, now to the extensions $K \subseteq L \subseteq \tilde{L}$, we have the exact sequence

$$1 \to H^1(\Gamma/\Delta, \mu_m^\Delta) \to H^1(\Gamma, \mu_m) \to H^1(\Delta, \mu_m),$$

where $\Gamma = \mathrm{Gal}(\tilde{L}/K)$, $\Delta = \mathrm{Gal}(\tilde{L}/L)$. The cohomology group $H^1(\Gamma/\Delta, \mu_m^\Delta)$ vanishes since $\mu_m^\Delta = \mu_m \cap L = \{1\}$ (we have $\zeta_l \notin K$ and L/K is an l-extension). Since Δ is cyclic, by Herbrand theory, the orders of the Tate cohomology groups $H^i(\Delta, \mu_m)$ are equal for $i = 0, 1$. But $H^0(\Delta, \mu_m) = \mu_m^\Delta/\mathrm{Norms} = 0$. This completes the proof. □

Let K_S be the group of S-units of K, where S contains the infinite primes of K. By Dirichlet's unit theorem, the $\mathbb{Z}$-rank of K_S is

$$u := rk_{\mathbb{Z}}(K_S) = |S| - 1.$$

Lemma 4.2. *Assume $\zeta_l \notin K$. With the notation of Lemma 4.1, let M be an abelian extension of L containing $\tilde{L}$. There are isomorphisms*

$$\mathrm{Gal}(\tilde{K}(\sqrt[m]{K_S})/\tilde{K}) \overset{f_1}{\cong} \mathrm{Gal}(\tilde{L}(\sqrt[m]{K_S})/\tilde{L}) \overset{f_2}{\cong} \mathrm{Gal}(M(\sqrt[m]{K_S})/M) \cong (\mathbb{Z}/m\mathbb{Z})^u.$$

Proof. Apply Lemma 4.1 restricted to the image of K_S in $\tilde{L}^\times$ to conclude that f_1 is an isomorphism. Next we show f_2 is an isomorphism. Let $F = \tilde{L}(\sqrt[m]{K_S}) \cap M$. We show $F = \tilde{L}$, so that f_2 would be an isomorphism. Since $F \subset M$, the extension F/L is abelian. And $\tilde{L} \subset F \subset L(\sqrt[m]{K_S})$. If F is not $\tilde{L}$, then F contains a cyclic extension $F_0/\tilde{L}$, $[F_0 : \tilde{L}] = l$. From Kummer theory, $F_0 = \tilde{L}(\sqrt[l]{b})$, $b \in K_S$. But $\mathrm{Gal}(\tilde{L}(\sqrt[l]{b})/L)$ is not abelian; thus $F = \tilde{L}$. □

The corollary below will be used in Section 8.

Corollary 4.3. *Let K be a number field, S a finite set of primes of K and let $a > 1$ be an integer. For each $l \mid a$ let L_l/K be a Galois l-extension. Suppose that $\zeta_l \notin K$ for each l dividing a. Set $M_l = L_l(\zeta_{l^N}, \zeta_a)$ and $M = \prod_l M_l$. Then we have a series of isomorphisms*

$$\begin{aligned}\mathrm{Gal}\big(K\big(\sqrt[l^N]{K_S}\big)/K(\zeta_{l^N})\big) &\cong \mathrm{Gal}\big(L_l\big(\sqrt[l^N]{K_S}\big)/L_l(\zeta_{l^N})\big)\\ &\cong \mathrm{Gal}\big(M_l\big(\sqrt[l^N]{K_S}\big)/M_l\big) \cong \mathrm{Gal}\big(M\big(\sqrt[l^N]{K_S}\big)/M\big).\end{aligned}$$

The diagram below contains the fields involved in these isomorphisms.

$$\begin{array}{ccccccc} K(\sqrt[l^N]{K_S}) & \longrightarrow & L_l(\sqrt[l^N]{K_S}) & \longrightarrow & M_l(\sqrt[l^N]{K_S}) & \longrightarrow & M(\sqrt[l^N]{K_S}) \\ \uparrow & & \uparrow & & \uparrow & & \uparrow \\ K(\zeta_{l^N}) & \longrightarrow & L_l(\zeta_{l^N}) & \longrightarrow & M_l & \longrightarrow & M \end{array}$$

Proof. The first two isomorphisms follow from Lemma 4.2. To show the rightmost isomorphism note that $M_l(\sqrt[l^N]{K_S})/M_l$ is an l-extension, while $l \nmid [M : M_l]$. □

Lemma 4.4. *For each l dividing a, assume that $\zeta_l \notin K$. Let R_l denote the field $L_l(\sqrt[l^N]{K_S})$ and let $\sigma_l \in \mathrm{Gal}(R_l/L_l(\mu_{l^N}))$. Define $R = \prod_{l|a} R_l$. Then there exists $\sigma \in \mathrm{Gal}(R/K(\mu_a))$ such that $\sigma|_{R_l} = \sigma_l$ for all $l|a$.*

Proof. By Corollary 4.3, each σ_l extends to an element, say $\hat{\sigma}_l$, of $\mathrm{Gal}(R_l M_l/M_l)$. The latter group is a subgroup of the l-group $\mathrm{Gal}(R_l M_l/K(\mu_a))$. Now observe that $\mathrm{Gal}(R/K(\mu_a)) \cong \prod_{l|a} \mathrm{Gal}(R_l M_l/K(\mu_a))$. Therefore we may define $\sigma \in \mathrm{Gal}(R/K(\mu_a))$ as $\sigma = \prod_{l|a} \hat{\sigma}_l$. □

For an abelian group A and a prime number l, let $A_l = \{a \in A : a^l = 1\}$. We define a subgroup of $K^\times$ by

$$V = V(l) := \{a \in K^\times : (a) = \mathfrak{a}^l \text{ for a fractional ideal } \mathfrak{a} \text{ of } K\}.$$

We have the following split exact sequence (see [Koch 1970, §11.2], for example):

$$1 \to E/E^l \to V/K^{\times l} \to Cl(K)_l \to 1,$$

where E denotes the group of units of K and the right hand map sends $a \bmod K^{\times l}$ to the ideal class of $\mathfrak{a}$, where $(a) = \mathfrak{a}^l$. Similarly,

$$1 \to E/E^{l^N} \to EV^{l^{N-1}}/K^{\times l^N} \to Cl(K)_l \to 1.$$

Let $w_1, \ldots, w_s$ be a $\mathbb{Z}$-basis of E mod torsion. As in [Geyer and Jarden 1998], choose ideles $\alpha_1, \ldots, \alpha_r \in J$ whose images are an $\mathbb{F}_l$-basis of the l-torsion subgroup $(J/K^\times U)_l$ of the ideal class group of K. Then for $j = 1, \ldots, r$

$$\alpha_j^l = a_j^{-1}\epsilon_j, \quad a_j \in K^\times, \epsilon_j = (\epsilon_{j,v}) \in U, \epsilon_{j,v} \in U_v.$$

For all j and all primes v of K, a_j and $\epsilon_{j,v}$ have the same image in $K_v^\times/K_v^{\times l}$. Taken $\bmod K^{\times l}$, the set $\{w_1, \ldots, w_s, a_1, \ldots, a_r\}$ is a basis of $V/K^{\times l}$.

We define a governing field Ω_l as follows (compare [Gras 2003, Chapter 5] or [Geyer and Jarden 1998] for $N = 1$):

$$\begin{aligned} \Omega_l &= K(\mu_{l^N}, \sqrt[l^N]{EV^{l^{N-1}}}) = K(\mu_{l^N}, \sqrt[l^N]{E}, \sqrt[l]{V}) \\ &= K(\mu_{l^N}, \sqrt[l^N]{w_i}, \sqrt[l]{a}_j : 1 \le i \le s, 1 \le j \le r). \end{aligned} \tag{4-1}$$

It follows from Lemma 4.2 that the Kummer extension satisfies

$$\mathrm{Gal}(\Omega_l/K(\mu_{l^N})) \cong (\mathbb{Z}/l^N\mathbb{Z})^s \oplus (\mathbb{Z}/l\mathbb{Z})^r.$$

Of course, if $K = \mathbb{Q}$, we have $r = s = 0$.

Define subfields of Ω_l by

$$N_i = K\big(\mu_{l^N}, \sqrt[l^N]{w_k}, \sqrt[l]{a_j} : 1 \le k \le s,\ k \ne i,\ 1 \le j \le r\big), \quad 1 \le i \le s,$$
$$N_j' = K\big(\mu_{l^N}, \sqrt[l^N]{E}, \sqrt[l]{a_k} : 1 \le k \le r,\ k \ne j\big) \qquad 1 \le j \le r.$$

Then $\mathrm{Gal}(\Omega_l/N_i)$ is cyclic of order l^N, while $\mathrm{Gal}(\Omega_l/N_j')$ has order l.

Definition 4.5. (Compare [Geyer and Jarden 1998, (5.5)] for $N = 1$.) A set $T_l = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{q}_1, \ldots \mathfrak{q}_r\}$ of prime ideals of K such that $T_l \cap S_0 = \varnothing$ is called l^N-*exceptional* if

$$\mathrm{Gal}(\Omega_l/N_i) = D_{\mathfrak{p}_i}(\Omega_l/K) \quad \text{for } 1 \le i \le s$$

and

$$\mathrm{Gal}(\Omega_l/N_j') = D_{\mathfrak{q}_j}(\Omega_l/K) \quad \text{for } 1 \le j \le r.$$

(This property is independent of the primes of Ω_l above $\mathfrak{p}_i$ and $\mathfrak{q}_j$, since N_i and N_j' are normal extensions of K.)

For a prime ideal $\mathfrak{p}$ of K unramified in a Galois extension F/K, $\mathrm{Frob}(\mathfrak{p}, F/K)$ denotes the conjugacy class in $\mathrm{Gal}(F/K)$ consisting of the Frobenius elements of all prime ideals of F above $\mathfrak{p}$.

Choose $\sigma_i(l) \in \mathrm{Frob}(\mathfrak{p}_i(l), \Omega_l/K)$ for $1 \le i \le s$ and $\tau_j(l) \in \mathrm{Frob}(\mathfrak{q}_j(l), \Omega_l/K)$ for $1 \le j \le r_l$; here we make the dependence on l explicit. Note that

$$\big\{\sigma_i(l), \tau_j(l) : 1 \le i \le s,\ 1 \le j \le r_l\big\}$$

is a minimal generating set of the abelian group $\mathrm{Gal}(\Omega_l/K(\mu_{l^N}))$. Further if a is the product of the primes dividing $|G|$, the latter group is isomorphic to $\mathrm{Gal}(\Omega_l(\mu_{a^N})/K(\mu_{a^N}))$ by Lemma 4.2.

By the Chebotarev density theorem, there exists an l^N-exceptional set of primes disjoint from any given set of primes of K of density 0. Note that since v splits completely in $K(\mu_{l^N})/K$ for all $v \in T_l$, we have $\zeta_{l^N} \in K_v$ for all $v \in T_l$.

It follows from Kummer theory for primes $\mathfrak{p}_i, \mathfrak{q}_j \in T_l$ that

- w_i not an l-th power in $U_{\mathfrak{p}_i}$;
- $w_i \in U_v^{l^N}$ for all $v \in T_l$ distinct from $\mathfrak{p}_i$;
- a_j not an l-th power in $U_{\mathfrak{q}_j}$;
- $a_j \in U_v^l$ for all $v \in T_l$ distinct from $\mathfrak{q}_j$.

If T_l is l^N-exceptional, then T_l is l^k-exceptional for all $1 \leq k \leq N$. We will therefore fix a set T_l of l^N-exceptional primes, where l^N is divisible by the exponent of the l-group G. From now on until Section 8 we will let T denote T_l, as the prime l is implicit.

5. The split case

We begin with a generalization of [Geyer and Jarden 1998, Lemma 4.2]. If $K = \mathbb{Q}$ and b is an integer greater than one, the result follows at once from the fact there are infinitely many primes $q \equiv 1 \pmod{b}$, and we take subfield M of $\mathbb{Q}(\mu_q)$ of degree b.

Lemma 5.1. *Given an integer $b > 1$ and a number field K, there are infinitely many prime ideals $\mathfrak{q}$ of K and cyclic extensions $M = M(\mathfrak{q})$ of K of degree b such that $\mathfrak{q}$ is the unique ramified prime of M/K, $\mathfrak{q}$ is totally ramified, and $\mathfrak{q}$ does not divide b.*

Proof. Let S be a finite set of primes of K containing S_0 and prime divisors of b and let $\Omega = K(\sqrt[b]{K_S})$. By Chebotarev's theorem there exist infinitely many primes $\mathfrak{q}$ of K, $\mathfrak{q} \notin S$, such that $\mathfrak{q}$ splits completely in Ω/K. For such $\mathfrak{q}$, Ω is contained in the completion $K_\mathfrak{q}$ and so $K_S \subset (K_\mathfrak{q}^\times)^b$.

Define

$$J_S = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} U_v \subset J.$$

By class field theory, cyclic extensions of K are given by idèle class characters. Since $J/K^\times \cong J_S/K_S$, we want to define an epimorphism $\chi : J_S/K_S \to \mu_b$ with $\chi(K_S) = \{1\}$. The group $U_\mathfrak{q}/U_\mathfrak{q}^b$ is cyclic of order b, so there is an epimorphism $\chi_\mathfrak{q} : U_\mathfrak{q} \to \mu_b$ with kernel $U_\mathfrak{q}^b$. For $\alpha = (\alpha_v) \in J_S$, define $\chi(\alpha) = \chi_\mathfrak{q}(\alpha_\mathfrak{q})$. Note $\chi(K_S) = \{1\}$ and $\chi(K_v^\times) = \{1\}$, $v \in S$. By class field theory, χ corresponds to a cyclic, degree b extension $M(\mathfrak{q})/K$ in which $\mathfrak{q}$ is totally and tamely ramified and the other primes of K are unramified. □

Theorem 5.2. *Let A be a finite abelian group with d generators. There exist infinitely many Galois extensions N/K such that* $\mathrm{Gal}(N/K) \cong A$ *and exactly d primes of K ramify in N. Such N is its own genus field relative to K.*

Proof. Write A as a direct product of d cyclic groups and apply Lemma 5.1 to each factor. The resulting extensions $M(\mathfrak{q}_i)$, $1 \leq i \leq d$ are linearly disjoint over K by ramification considerations. Take N to be the composite of the fields $M(\mathfrak{q}_i)$. These $\mathfrak{q}_i$ are not to be confused with the ones defined in Definition 4.5. □

Proposition 5.3 (split case). *Let G be an l-group of exponent dividing l^N. Suppose the homomorphism $\rho : G_K \to \bar{G}$ is l^N-Scholz and the central exact sequence is split*:

$$1 \to C \to G \to \bar{G} \to 1,$$

where the kernel C of $\alpha : G \to \bar{G}$ is cyclic. There is an l^N-Scholz solution ϕ to the embedding problem (G_K, ρ, α) and a prime $\mathfrak{q}$ not in $S = \mathrm{Ram}(\rho) \cup S_0 \cup T$ such that $\mathrm{Ram}(\phi) = \mathrm{Ram}(\rho) \cup \{\mathfrak{q}\}$.

Proof. We apply the argument in Lemma 5.1 with $b = |C|$, $\Omega = L(\mu_{l^N}, \sqrt[b]{K_S})$, where L is the subfield of $\bar{K}$ fixed by $\ker \rho$, to obtain $\mathfrak{q}$ and an idèle class character χ of order b; $\mathfrak{q}$ splits completely in Ω/K. By the Reciprocity law χ corresponds to an epimorphism $\eta : G_K \to C$. Then $\phi = (\rho, \eta) : G_K \to \bar{G} \times C$, $\sigma \mapsto (\rho(\sigma), \eta(\sigma))$, is a proper solution to the embedding problem. It remains to check that ϕ is l^N-Scholz, given that ρ is l^N-Scholz.

If $v \in S_0$, then $\phi(D_v) = 1$ since $\rho(D_v) = 1$ (given) and $\eta(D_v) = 1$ for $v \in S$.

If $v \in T$, then $\phi(D_v) = \phi(I_v)$ since $\rho(D_v) = \rho(I_v)$ (given) and $\eta(D_v) = 1$ for $v \in S$.

Suppose $v \in \mathrm{Ram}(\phi) = \mathrm{Ram}(\rho) \cup \{\mathfrak{q}\}$.

If $v = \mathfrak{q}$, then $\mathfrak{q}$ splits completely in $K(\mu_{l^N})/K$, hence $N(\mathfrak{q}) \equiv 1 \pmod{l^N}$. Since $\mathfrak{q}$ splits completely in L/K, $\rho(D_\mathfrak{q}) = 1$. As $\eta(I_\mathfrak{q}) = C$ for $\eta : G_K \to C$, we have $\eta(D_\mathfrak{q}) = \eta(I_\mathfrak{q})$. Thus $\phi(D_\mathfrak{q}) = \phi(I_\mathfrak{q})$.

If $v \in \mathrm{Ram}(\rho)$, then $N(v) \equiv 1 \pmod{l^N}$ and $\rho(D_v) = \rho(I_v)$ (given). But $\eta(D_v) = 1$ since $v \in \mathrm{Ram}(\rho) \subset S$. Thus $\phi(D_v) = \phi(I_v)$ for $v \in \mathrm{Ram}(\phi)$.

We conclude $\phi = (\rho, \eta)$ is an l^N-Scholz solution with one additional ramified prime. □

6. Removing ramification

Lemma 6.1. *Let K be a number field not containing ζ_l, and assume $N \geq e \geq 1$. Let S be a finite set of primes disjoint from an l^N-exceptional set T, and $\chi_v : U_v \to \mu_{l^e}$, for $v \in S$, be characters, at least one of which is onto. Assume K has no ideal classes of order l^2 when $e > 1$. There exists an idèle class character*

$$\chi : J/K^\times \to \mu_{l^e}$$

such that $\chi|_{U_v} = \chi_v$ for all $v \in S$ and $\chi|_{U_v} = 1$ for all $v \notin S \cup T$.

Proof. It suffices to prove the result when $S = \{v_0\}$ and then take the product of the resulting characters. Let $I = T \cup \{v_0\}$.

***Step 1:** Defining f on $UK^\times/K^\times$.* We define an epimorphism $f : U \to \mu_{l^e}$ of the form

$$f = \prod_{v \in I} \chi_v,$$

with $f|_{U_v} = 1$ for $v \notin I$. The character χ_{v_0} is given and the characters χ_v, $v \in T$, are to be defined suitably. Each character χ_v is trivial for $v \notin I$.

By the definition of an l^N-exceptional set of primes, the image of each unit w_i generates $U_{\mathfrak{p}_i}/U_{\mathfrak{p}_i}^{l^e}$, $\mathfrak{p}_i \in T$, hence we can define $\chi_{\mathfrak{p}_i} : U_{\mathfrak{p}_i} \to \mu_{l^e}$, $1 \leq i \leq s$, to

satisfy

$$\chi_{\mathfrak{p}_i}(w_i)\chi_{v_0}(w_i) = 1.$$

Similarly $\epsilon_{j,\mathfrak{q}_j}$ generates $U_{\mathfrak{q}_j}/U_{\mathfrak{q}_j}^l$ (hence also modulo $U_{\mathfrak{q}_j}^{l^e}$) and we can define $\chi_{\mathfrak{q}_j} : U_{\mathfrak{q}_j} \to \mu_{l^e}$, $1 \le j \le r$, to satisfy

$$\chi_{\mathfrak{q}_j}(\epsilon_{j,\mathfrak{q}_j})\chi_{v_0}(\epsilon_{j,v_0}) = 1.$$

Next we establish the "off-diagonal" vanishing of $\prod_{v\in I}\chi_v$. Recall that $\epsilon_{j,v} \in U_v^l$ for $\mathfrak{q}_j \ne v \in T$ for each j, and $w_i \in U_v^{l^e}$ for $\mathfrak{p}_i \ne v \in T$ for each i. Thus we have

$$\prod_{v\in I}\chi_v(w_i) = \chi_{\mathfrak{p}_i}(w_i)\chi_{v_0}(w_i)\prod_{\mathfrak{p}_i\ne v\in T}\chi_v(w_i) = 1$$

and

$$\prod_{v\in I}\chi_v(\epsilon_{j,v}^{l^{e-1}}) = \chi_{\mathfrak{q}_j}(\epsilon_{j,\mathfrak{q}_j}^{l^{e-1}})\chi_{v_0}(\epsilon_{j,v_0}^{l^{e-1}})\prod_{\mathfrak{q}_j\ne v\in T}\chi_v(\epsilon_{j,v}^{l^{e-1}}) = 1.$$

It follows that $\prod_{v\in I}\chi_v$ is trivial on the image of $E \oplus \left(\bigoplus_{j=1}^r \langle\epsilon_j\rangle\right)$ in $\prod_{v\in I} U_v/U_v^{l^e}$. Letting $\Delta : K^\times \to J$ be the diagonal embedding, we thus have $f(\Delta(E)) = 1$, so f is defined on $U/\Delta(E)$, which we write as $U/E \cong UK^\times/K^\times$.

If l does not divide the class number of K, then f already provides the desired idèle class character since the l-part of the ideal class group $J/K^\times U$ will be trivial. Otherwise we must extend f from $K^\times U/K^\times$ to $J/K^\times$.

Step 2: *Characters of order l.* Define $f_1 : U \to \mu_l$ by $f_1 = f^{l^{e-1}}$. By the techniques of the proof of Lemma 6.1 of [Geyer and Jarden 1998], f_1 extends to an idèle class character χ_1 of order l with $\chi_1|_{U_v} = \chi_v^{l^{e-1}}$, for $v \in I$ and $\chi_1|_{U_v} = 1$ if $v \notin I$. This follows from the trivial fact that an l^e-exceptional set T is l-exceptional.

We have

$$\frac{K^\times U}{K^\times \ker f_1} \cap \frac{K^\times \ker \chi_1}{K^\times \ker f_1} \equiv 1.$$

Also, $|J/K^\times \ker f_1| = |J/K^\times U| \cdot |K^\times U/K^\times \ker f_1| = h \cdot l$, where h is the class number of K, which we may assume is a power of l. Thus

$$|K^\times \ker \chi_1/K^\times \ker f_1| = \frac{|J/K^\times \ker f_1|}{|J/K^\times \ker \chi_1|} = \frac{h\cdot l}{l} = |J/K^\times U|.$$

This implies that the exact sequence

$$1 \to \frac{K^\times U}{K^\times \ker f_1} \to \frac{J}{K^\times \ker f_1} \to J/K^\times U \to 1$$

splits, with $(K^\times \ker \chi_1)/(K^\times \ker f_1)$ mapping isomorphically onto $J/K^\times U$. The image $J/K^\times U$ has exponent l by assumption and the kernel is cyclic of order l. Hence $J/(K^\times \ker f_1)$ has exponent l.

Step 3: *Extending to a character of order l^e.* We use the following fact about finite abelian l-groups: *If Γ is a finite abelian l-group and $\gamma \subseteq \Gamma$ is a cyclic subgroup of order l^e such that Γ/γ^l has exponent l, then γ is a direct summand of Γ.*

Indeed, the exponent of Γ is l^e, since for any element $g \in \Gamma$ we have $g^l \in \gamma^l$ and hence $g^{l^e} = 1$. Therefore γ is a subgroup generated by an element of maximal order, and hence is a direct summand.

Now consider the following diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \dfrac{(K^\times U)^l K^\times \ker f}{K^\times \ker f} & = & \dfrac{(K^\times U)^l K^\times \ker f}{K^\times \ker f} & & & & \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & \gamma := \dfrac{K^\times U}{K^\times \ker f} & \longrightarrow & \Gamma := \dfrac{J}{K^\times \ker f} & \longrightarrow & \dfrac{J}{K^\times U} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow = & & \\
1 & \longrightarrow & \dfrac{K^\times U}{K^\times \ker f_1} & \longrightarrow & \dfrac{J}{K^\times \ker f_1} & \longrightarrow & \dfrac{J}{K^\times U} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array}$$

It follows from the diagram that Γ/γ^l is isomorphic to $J/K^\times \ker f_1$, which by assumption has exponent l. Applying the fact just proved about abelian groups, we see that γ is a direct summand of Γ. Thus we can extend f to a character $\chi : J/K^\times \to \mu_{l^e}$ by defining χ to agree with f on U and to be trivial on a complement of $K^\times U/K^\times \ker f$. □

Theorem 6.2 (removing ramification). *Suppose K has no ideal classes of order l^2 and does not contain ζ_l. If the Frattini embedding problem (G_K, ρ, α) has a solution ψ_0, then it has a solution $\psi : G_K \to G$ with* $\mathrm{Ram}(\psi) \subset \mathrm{Ram}(\rho) \cup T$.

Proof. The proof is similar to that of [Geyer and Jarden 1998, Lemma 6.2], except that we twist ψ_0 by a character of order l^e. Let $S = \mathrm{Ram}(\psi_0) \setminus \{\mathrm{Ram}(\rho) \cup T\}$, so if $v \in S$, then $\psi_0(I_v) \subseteq C$. Set $l^e = \max\{|\psi_0(I_v)| : v \in S\}$.

For $v \in S$ we define $\chi_v := \psi_0|_{I_v}$ viewed as $\chi_v : U_v \to \mu_{l^e}$ by reciprocity. By Lemma 6.1 there exists an idèle class character χ of order l^e with certain local properties. We identify χ with $\eta : G_K \to C$ via reciprocity and set $\psi = \psi_0 \eta^{-1}$. Since the embedding problem (G_K, ρ, α) is Frattini, ψ is surjective. □

Remark 6.3. If $e = 1$, the hypothesis on the order of ideal classes in Theorem 6.2 can be dropped.

7. Finding an m-Scholz solution

We generalize Lemma 7.1 of [Geyer and Jarden 1998] to prime powers.

Lemma 7.1. *Suppose given integers $N \geq e \geq 1$, a Galois l-extension L/K, and characters $\chi_v : K_v^\times \to \mu_{l^e}$ for all v in a finite set $S \supseteq S_0$. Assume that K does not contain ζ_l. There exists a prime ideal $\mathfrak{q}$ of K outside S and a character $\chi : J_K/K^\times \to \mu_{l^e}$ such that*

- *$\mathfrak{q}$ splits completely in $L(\mu_{l^N})/K$;*
- *$\chi|_{K_v^\times} = \chi_v$ for all $v \in S$;*
- *$\chi(U_\mathfrak{q}) = \mu_{l^e}$;*
- *$\chi(U_v) = 1$ for all $v \notin S \cup \{\mathfrak{q}\}$.*

Proof. Since S_0 is chosen large enough, we have $J_S/K_S \cong J/K^\times$. It therefore suffices to define a character $g : J_S \to \mu_{l^e}$ such that

$$g((\alpha_v)) = \chi_\mathfrak{q}(\alpha_\mathfrak{q}) \times \prod_{v \in S} \chi_v(\alpha_v) \quad \text{for all } (\alpha_v) \in J_S,$$

for some prime $\mathfrak{q}$ and some epimorphism $\chi_\mathfrak{q} : U_\mathfrak{q} \to \mu_{l^e}$ chosen so that $\mathfrak{q}$ splits completely in $L(\mu_{l^N})/K$ and $g(K_S) = \{1\}$.

We define a character $h : K_S \to \mu_{l^e}$ as the composition

$$K_S \xrightarrow{j} J_S \to \mu_{l^e},$$

where the left map j is the embedding of K_S in $\prod_{v \in S} K_v^\times$ and the right map is $\prod_{v \in S} \chi_v$. Thus for $x \in K_S$, $g(x) = h(x)\chi_\mathfrak{q}(x)$, so $\chi_\mathfrak{q}$ must be chosen to make $g(x) = 1$ for all $x \in K_S$.

Case $h(K_S) = \{1\}$. If $\mathfrak{q}$ satisfies $K_S \subset U_\mathfrak{q}^{l^e}$, then for any character $\chi_\mathfrak{q} : U_\mathfrak{q} \to \mu_{l^e}$, we have $\chi_\mathfrak{q}(K_S) = \{1\}$. By Chebotarev's theorem, there exists a prime ideal $\mathfrak{q} \notin S$ of K which splits completely in

$$\Omega := L\big(\mu_{l^N}, \sqrt[l^e]{K_S}\big).$$

Note that $\mathfrak{q}$ splitting completely in $K(\mu_{l^N})/K$ implies that the absolute norm $N_\mathbb{Q}^K(\mathfrak{q})$ is congruent to 1 $(\mathrm{mod}\, l^N)$. Thus $K_S \subseteq U_\mathfrak{q}^{l^e}$ by Kummer theory.

Case $h(K_S) \neq \{1\}$. The image $h(K_S)$ is cyclic of order l^k, $1 \leq k \leq e$. Thus there exists $x_1 \in K_S$ with $h(x_1)$ of order l^k. $K_S/K_S^{l^k}$ may be generated by $\{x_1, x_2, \ldots, x_u\}$, with $h(x_i) = 1, i > 1$. By Burnside's basis theorem $\{x_1, \ldots, x_u\}$ also generate $K_S/K_S^{l^e}$. We want to pick a prime $\mathfrak{q} \notin S$ such that

- $\mathfrak{q}$ splits completely in $L(\mu_{l^N})/K$,
- $x_1 \in U_{\mathfrak{q}}^{l^{e-k}} \setminus U_{\mathfrak{q}}^{l^{e-k+1}}$, and
- $x_i \in U_{\mathfrak{q}}^{l^e}$ if $i > 1$.

To that end let

$$\Omega_k = L\big(\mu_{l^N},\ \sqrt[l^{e-k}]{x_1},\ \sqrt[l^e]{x_i} : i > 1\big).$$

The field Ω_k is a normal extension of K. By Lemma 4.2, $\mathrm{Gal}(\Omega/L(\mu_{l^N})) \cong (\mathbb{Z}/l^e\mathbb{Z})^u$ and $\mathrm{Gal}(\Omega/\Omega_k)$ is cyclic of order l^k. By Chebotarev's theorem we may choose $\mathfrak{q} \notin S$ such that $\mathrm{Frob}(\mathfrak{q}, \Omega/K)$ generates $\mathrm{Gal}(\Omega/\Omega_k)$, in particular $\mathfrak{q}$ splits completely in Ω_k/K. This guarantees that the above three conditions on $\mathfrak{q}$ are satisfied.

Having chosen $\mathfrak{q}$, we define $\chi_{\mathfrak{q}}$, a character of order l^e. Choose $y \in U_{\mathfrak{q}}$ such that $y^{l^{e-k}} = x_1 \in U_{\mathfrak{q}}$. We want $\chi_{\mathfrak{q}}(y)$ of order l^e, then $\chi_{\mathfrak{q}}(x_1)$ has order l^k. If $\beta = h(x_1)$ is an element of μ_{l^e} of order l^k, then $\beta = \alpha^{l^{e-k}}$, where α is a generator of μ_{l^e}. Set $\chi_{\mathfrak{q}}(y) = \alpha^{-1}$. Then $\chi_{\mathfrak{q}}(x_1) = \beta^{-1}$.

So we have chosen $\chi_{\mathfrak{q}}$ so that $\chi_{\mathfrak{q}}(x_1)h(x_1) = 1$. Thus $g(K_S) = 1$ and we have proved the lemma for prime power order characters. □

Proposition 7.2. *Suppose that the central embedding problem (G_K, ρ, α), G an l-group, is Frattini, ρ is l^N-Scholz, and $\zeta_l \notin K$. Assume there exists a solution ψ with $\mathrm{Ram}(\psi) \cup T = \mathrm{Ram}(\rho) \cup T$. Then there exists a prime $\mathfrak{q} \notin S := \mathrm{Ram}(\psi) \cup S_0 \cup T$ and an l^N-Scholz solution φ such that $\mathrm{Ram}(\varphi) = \mathrm{Ram}(\psi) \cup \{\mathfrak{q}\}$.*

Proof. ***Step 1.*** Define homomorphisms $\eta_v : D_v \to C$, $v \in S$. There are two cases.

If $v \in S \setminus S_0$, we lift Frobenius at v to $\sigma_v \in D_v$. Since ρ is l^N-Scholz and $\mathrm{Ram}(\psi) \cup T = \mathrm{Ram}(\rho) \cup T$, after adjusting the lift σ_v we may assume $\psi(\sigma_v) \in C$ (see [Geyer and Jarden 1998, p. 36]). Then let η_v be the unique homomorphism $D_v \to C$ satisfying $\eta_v(\sigma_v) = \psi(\sigma_v)$ and $\eta_v(I_v) = \{1\}$.

If $v \in S_0$, $\alpha(\psi(D_v)) = \rho(D_v) = \{1\}$, again since ρ is l^N-Scholz. Thus $\psi(D_v) \subset \ker\alpha = C$. So define $\eta_v = \psi|_{D_v}$.

We have defined η_v, for $v \in S$; now we apply Lemma 7.1 to get a map $\eta : G_K \to C$ and a prime $\mathfrak{q} \notin S$ such that $\eta|_{D_v} = \eta_v$, $v \in S$, $\eta(I_{\mathfrak{q}}) = C$, and η unramified for $v \notin \mathrm{Ram}(\psi) \cup T \cup \{\mathfrak{q}\}$. Finally set $\varphi = \eta^{-1}\psi$. Note that $\varphi(\sigma_v) = 1$, so $\varphi(D_v) = \varphi(I_v)$ if $v \in \mathrm{Ram}(\psi) \cup T \setminus S_0$.

Step 2. We claim φ is unramified outside $\mathrm{Ram}(\psi) \cup \{\mathfrak{q}\}$. In fact if $v \in S \setminus S_0$, we have $\eta(I_v) = \eta_v(I_v) = \{1\}$, so $\varphi(I_v) = \psi(I_v)$. The result follows.

Step 3. We claim φ is l^N-Scholz. Since the extension is Frattini, any solution is proper. The check of the three points of Definition 2.1 is similar to pg. 37 of [Geyer and Jarden 1998] except for the proof that $\varphi(D_{\mathfrak{q}}) = \varphi(I_{\mathfrak{q}})$. For that, note that $\mathfrak{q}$ is chosen to split completely in the fixed field of $\ker\psi$, so $\psi(D_{\mathfrak{q}}) = \{1\}$. Putting this together with $\eta(I_{\mathfrak{q}}) = C$, we conclude that $\varphi(D_{\mathfrak{q}}) = \varphi(I_{\mathfrak{q}})$. □

Putting together the existence theorem 3.1, Proposition 5.3, Theorem 6.2, and Proposition 7.2 we have the next result.

Proposition 7.3. *Suppose $\zeta_l \notin K$ and K has no ideal classes of order l^2. Given a central embedding problem (G_K, ρ, α) with G an l-group, cyclic C and ρ l^N-Scholz. If the extension is split or of Frattini type, then there exists an l^N-Scholz solution φ and a prime $\mathfrak{q}$ of K such that*

$$\mathrm{Ram}(\varphi) \cup T = \mathrm{Ram}(\rho) \cup T \cup \{\mathfrak{q}\}.$$

Recall that the lower central series $\{G_i\}$ of G is defined by $G_1 = G$ and $G_{i+1} := [G_i, G]$ for $i \geq 1$. If G is nilpotent, the smallest positive integer c such that $G_{c+1} = \{1\}$ is called the nilpotency class of G. Our main result below generalizes [Plans 2004, Proposition 2.5], which considers only the case $K = \mathbb{Q}$. It also improves [Geyer and Jarden 1998, Theorem 7.4] when the kernel C of the embedding problem is not of prime order.

Theorem 7.4. *Let a number field K, a prime l, and an l-group G of nilpotency class c be given. If G is nonabelian, suppose $\zeta_l \notin K$ and K has no ideal classes of order l^2. Then*

$$\min \mathrm{ram}_K(G) \leq d(G) + |T| + \sum_{i=2}^{c-1} d(G_i/G_{i+1}).$$

Remark 7.5. (1) This bound may be achieved by a tamely ramified extension L/K with $G \cong \mathrm{Gal}(L/K)$.

(2) If G is of nilpotency class 2,

$$\min \mathrm{ram}_K(G) \leq d(G) + |T|.$$

(3) If we allow K to have ideal classes of order l^2, the bound has the form

$$\min \mathrm{ram}_K(G) \leq g + |T| \quad \text{when } |G| = l^g,$$

as proved in [Geyer and Jarden 1998].

Proof. As in [Plans 2004, Proposition 2.5] we use induction on i for a central embedding problem

$$1 \to G_i/G_{i+1} \to G/G_{i+1} \to G/G_i \to 1.$$

For $i = 1$, by Proposition 5.3 the embedding problem has an l^N-Scholz solution with at most $d(G^{ab}) = d(G)$ ramified primes. For $i \geq 1$, each extension is of Frattini type, and we may break the i-th problem up into $d(G_i/G_{i+1})$ cyclic Frattini problems. As shown in Proposition 7.3, each such problem may be solved at the cost of one more ramified prime. And since we can make the solution l^N-Scholz at each stage, it is guaranteed that we may solve the next embedding problem. □

8. Ramification bound on nilpotent groups

We use the notation that a is the product of the primes dividing the order of G and integer N satisfies a^N is a multiple of the exponent of G. The purpose of this section is to extend Theorem 7.4 to groups $G = \prod_l G_l$ that are the direct product of their Sylow l-subgroups G_l, that is *nilpotent groups*. Assume $\zeta_l \notin K$ for all l dividing $|G|$. We will obtain G by a sequence of central embedding extensions with cyclic kernel; each of these extensions is a "product" of central extensions of l-groups as in sections 6 and 7. The nilpotent case was initially handled in the first author's thesis [Markin 2006]. In this section we obtain an improved bound on $\min \mathrm{ram}_K(G)$ for fields K which do not contain ideal classes of order l^2, where l divides $|G|$.

The first step is to define a set T (as small as possible) of primes of K that contains an l^N-exceptional set T_l of primes for each l dividing $|G|$.

Let

$$\Omega_l = K\left(\sqrt[l^N]{E}, \sqrt[l]{V(l)}\right)$$

as in (4-1) and let $\hat{\Omega} = \prod_{l|a} \Omega_l$. Since $\mathrm{Gal}(\Omega_l(\mu_{a^N})/K(\mu_{a^N}))$ is an l-group, we have

$$\mathrm{Gal}(\hat{\Omega}/K(\mu_{a^N})) \cong \prod_{l|a} \mathrm{Gal}(\Omega_l(\mu_{a^N})/K(\mu_{a^N})). \tag{8-1}$$

Using this isomorphism we define elements of $\mathrm{Gal}(\hat{\Omega}/K(\mu_{a^N}))$ by

$$\sigma_i = \prod_{l|a} \sigma_i(l), \quad 1 \le i \le s \quad \text{and} \quad \tau_j = \prod_{l|a} \tau_j(l), \quad 1 \le j \le r.$$

Here $r = \max_{l|a} r_l$ and we set $\tau_j(l) = 1$ if $r_l < j \le r$. By Chebotarev's theorem, in K there is a set of $s + r$ prime ideals $T = \{\mathfrak{p}_i, \mathfrak{q}_j : 1 \le i \le s, 1 \le j \le r\}$, disjoint from any given finite set and such that

$$\mathrm{Frob}(\mathfrak{p}_i, \hat{\Omega}/K) = C(\mathrm{Gal}(\hat{\Omega}/K), \sigma_i) \quad \text{for } 1 \le i \le s$$

and

$$\mathrm{Frob}(\mathfrak{q}_j, \hat{\Omega}/K) = C(\mathrm{Gal}(\hat{\Omega}/K), \tau_j) \quad \text{for } 1 \le j \le r,$$

where $C(\mathrm{Gal}(\hat{\Omega}/K), \gamma)$ denotes the conjugacy class of γ in $\mathrm{Gal}(\hat{\Omega}/K)$. By the properties of the Frobenius, for each l dividing a, the restriction of σ_i to Ω_l is $\sigma_i(l)$, and that of τ_j is $\tau_j(l)$.

Lemma 8.1. *We keep the notation of Corollary 4.3 and Lemma 4.2. For each l dividing a, let L_l be an l^N-Scholz l-extension of K fixed by the kernel of homomorphism $\rho_l : G_K \to \bar{G}_l$ and let (G_K, ρ_l, α_l) be a Frattini central embedding problem as in* (2-1)*. Assume, for all l dividing a, that ζ_l is not in K and that the exponent*

of G_l divides l^N. When $|\ker \alpha_l| > l$, assume additionally that no ideal class of K has order l^2. Then, for each l dividing a, there exists a solution

$$\phi_l : G_K \to G_l$$

for which $\mathrm{Ram}(\phi_l) \subseteq \mathrm{Ram}(\rho_l) \cup T$.

Proof. The existence of any solution is Theorem 3.1. Our set of primes T contains l^N-exceptional subsets T_l, hence we may apply Theorem 6.2 to get a solution ϕ_l such that $\mathrm{Ram}(\phi_l) \subseteq \mathrm{Ram}(\rho_l) \cup T$ for all primes $l \mid a$. □

In the next lemma we apply Lemma 4.4 to find a single prime $\mathfrak{q}$ that we use to lift local characters indexed by divisors l of a.

Lemma 8.2. *Let S be a finite set of primes of K that contains S_0. For each prime l dividing a, we are given integers e_l, $N \geq e_l \geq 1$, Galois l-extension L_l/K, character $\chi_{v,l} : K_v^\times \to \mu_{l^{e_l}}$ for all $v \in S$. Assume, for each l dividing a, that K does not contain ζ_l. There exists a prime ideal $\mathfrak{q}$ of K outside S and idèle class characters $\chi_l : J_K/K^\times \to \mu_{l^{e_l}}$ such that, for all l dividing a,*

- *$\mathfrak{q}$ splits completely in $L_l(\mu_{l^N})/K$;*
- *$\chi_l|_{K_v^\times} = \chi_{v,l}$ for all $v \in S$;*
- *$\chi_l(U_\mathfrak{q}) = \mu_{l^{e_l}}$;*
- *$\chi_l(U_v) = 1$ for all $v \notin S \cup \{\mathfrak{q}\}$.*

Proof. Let R_l denote the field $L_l\big(\sqrt[l^N]{K_S}\big)$, $R = \prod_{l|a} R_l$, $\Gamma_l = \mathrm{Gal}(R_l/K)$ and $\Gamma = \mathrm{Gal}(R/K)$.

In Lemma 7.1, for all $l \mid a$ we have defined a special prime $\mathfrak{q}_l$ (not to be confused with the $\mathfrak{q}_i$ defined in Definition 4.5). Define $\sigma_l \in \Gamma_l$ by $\mathrm{Frob}(\mathfrak{q}_l, R_l/K) = C(\Gamma_l, \sigma_l)$. Next we show that a single prime $\mathfrak{q}$ can be chosen. By Lemma 4.4 there exists an element $\sigma \in \Gamma$ whose restriction to R_l equals σ_l for all $l|a$. By Chebotarev's theorem, there exists a prime $\mathfrak{q}$ of K outside S such that $\mathrm{Frob}(\mathfrak{q}, R/K) = C(\Gamma, \sigma)$. By restriction $\mathrm{Frob}(\mathfrak{q}, R_l/K) = C(\Gamma_l, \sigma_l)$ for all $l \mid a$ and the conditions of Lemma 8.2 are satisfied. □

Remark 8.3. The method by which we replaced $\{\mathfrak{q}_l : l \mid a\}$ by $\mathfrak{q}$ is similar to that where we replaced $\{T_l : l \mid a\}$ by T.

Theorem 8.4. *Given a number field K and a finite nilpotent group G of class c. If G is nonabelian, suppose* $\gcd(|G|, |\mu_K|) = 1$ *and assume for all primes dividing $|G|$ that the ideal class group of K has no elements of order l^2. Then*

$$\min \mathrm{ram}_K(G) \leq d(G) + (r+s) + \sum_{i=2}^{c-1} d(G_i/G_{i+1}).$$

Here $s = \mathbb{Z}$-rank of units of K and $r = \max_{l\,||G|}\{\dim Cl(K)_l\}$.

Proof. By Theorem 5.2 it remains to prove the result for nonabelian groups G. Since G is nilpotent, for each l dividing $|G|$, we may apply Proposition 7.2, Proposition 7.3, and Theorem 7.4 inductively. By Lemma 8.2 there exists a single prime $\mathfrak{q}$ to which Proposition 7.2 may be applied, and the conclusion follows. □

9. Schur extensions

In this section we use Fröhlich's result on realizing the Schur multiplicator without additional ramification to realize a class of nilpotent groups given by central extensions

$$1 \to \mathcal{M}(\Gamma) \to G \to \Gamma \to 1.$$

The group $\mathcal{M}(\Gamma)$ is the Schur multiplicator of a profinite group Γ as defined in [Fröhlich 1983].

Definition 9.1. Suppose $M \supseteq L \supseteq K$ are number fields with M/K and L/K Galois extensions. Let M' be the maximal central extension of L/K in M and let E be the maximal abelian extension of K in M. Fröhlich defines a certain surjective homomorphism

$$\mathcal{M}(\mathrm{Gal}(L/K)) \to \mathrm{Gal}(M'/EL). \tag{9-1}$$

If it is an isomorphism, one says that M *realizes the multiplicator* $\mathcal{M}(\mathrm{Gal}(L/K))$.

Remark 9.2. For two central extensions M_1 and M_2 for L/K, both realizing the multiplicator of $\mathrm{Gal}(L/K)$, the Galois groups $\mathrm{Gal}(M_1/K)$ and $\mathrm{Gal}(M_2/K)$ need not be isomorphic.

Proposition 3.2 of [Fröhlich 1983] says that if L/K is a finite-degree extension, there is a finite-degree central extension M of L/K that realizes $\mathcal{M}(\mathrm{Gal}(L/K))$.

For a prime l and a finite set of primes S of K, $K(l, S)$ denotes the maximal l-extension field of K with ramification restricted to S, and $K(l, S)^{ab}$ is the maximal abelian subextension of $K(l, S)$. If S contains no divisors of l, then the degree $[K(l, S)^{ab} : K]$ is finite. From now on suppose L/K is a finite-degree l-extension, so $\mathcal{M}(\mathrm{Gal}(L/K))$ is a finite abelian l-group. Let S be the set of primes of K ramified in L.

For $K = \mathbb{Q}$ or K imaginary quadratic with $\zeta_l \notin K$, there exists such an extension M that is ramified at worst at primes above S. This is [Fröhlich 1983, Corollary 2 of Theorem 3.13] for the case of $\mathbb{Q}$ and [Watt 1985, Theorem 3.1] for the quadratic case. In these cases, Since M is central for L/K, we have $M = M'$. Furthermore if $L \supseteq K(l, S)^{ab}$, then $L \supseteq E$, so $EL = L$ and (9-1) asserts that

$$\mathcal{M}(\mathrm{Gal}(L/K)) \cong \mathrm{Gal}(M/L).$$

Remark 9.3. Fröhlich does not require L/K to be an l-extension.

Thus from the results of Fröhlich and Watt we have:

Theorem 9.4. *Let K be $\mathbb{Q}$ or imaginary quadratic with $\zeta_l \notin K$ and let L/K be a finite Galois l-extension tamely ramified only at S; suppose $L \supseteq K(l, S)^{ab}$. Then there exists a central extension M of L/K with* $\mathrm{Ram}(M/K) \subseteq S$ *such that* $\mathcal{M}(\mathrm{Gal}(L/K)) \cong \mathrm{Gal}(M/L)$. □

Remark 9.5. We may apply the theorem repeatedly by replacing the extension L/K by M/K.

Remark 9.6. Since the number of generators of $\mathrm{Gal}(K(l, S)/K)$ equals the number of generators of $\mathrm{Gal}(K(l, S)^{ab}/K)$, we have that $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(M/K)$ have the same number of generators.

Acknowledgement

Ullom thanks Marcin Mazur for a useful discussion regarding Lemma 4.1.

References

[Boston and Markin 2009] N. Boston and N. Markin, "The fewest primes ramified in a G-extension of $\mathbb{Q}$", *Ann. Sci. Math. Québec* **33**:2 (2009), 145–154. MR 2729805 Zbl 1219.11165

[Fröhlich 1983] A. Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemporary Mathematics **24**, American Mathematical Society, Providence, RI, 1983. MR 85c:11101 Zbl 0519.12001

[Geyer and Jarden 1998] W.-D. Geyer and M. Jarden, "Bounded realization of l-groups over global fields. The method of Scholz and Reichardt", *Nagoya Math. J.* **150** (1998), 13–62. MR 99d:12001 Zbl 0906.12002

[Gras 2003] G. Gras, *Class field theory: from theory to practice*, Springer, Berlin, 2003. MR 2003j:11138 Zbl 1019.11032

[Koch 1970] H. Koch, *Galoissche Theorie der p-Erweiterungen*, Springer, Berlin, 1970. Translated as *Galois theory of p-extensions*, Springer, Berlin, 2002. MR 45 #233 Zbl 0216.04704

[Markin 2006] N. Markin, *Galois groups with restricted ramification*, Ph.D. thesis, University of Illinois at Urbana-Champaign, 2006. MR 2709854

[Neukirch et al. 2000] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften **323**, Springer, Berlin, 2000. MR 2000j:11168 Zbl 0948.11001

[Plans 2004] B. Plans, "On the minimal number of ramified primes in some solvable extensions of $\mathbb{Q}$", *Pacific J. Math.* **215**:2 (2004), 381–391. MR 2005d:12005 Zbl 1064.11072

[Rubin 1991] K. Rubin, "The one-variable main conjecture for elliptic curves with complex multiplication", pp. 353–371 in *L-functions and arithmetic* (Durham, 1989), edited by J. Coates and M. J. Taylor, London Math. Soc. Lecture Note Ser. **153**, Cambridge Univ. Press, Cambridge, 1991. MR 92j:11055 Zbl 0741.11028

[Serre 1992] J.-P. Serre, *Topics in Galois theory*, Research Notes in Mathematics **1**, Jones and Bartlett Publishers, Boston, MA, 1992. MR 94d:12006 Zbl 0746.12001

[Shafarevich 1954] I. R. Shafarevich, "Construction of fields of algebraic numbers with given solvable Galois group", *Izv. Akad. Nauk SSSR Ser. Mat.* **18** (1954), 525–578. In Russian. Translation in *Transl. Amer. Math. Soc.* (2) **4** (1956), pp. 185–237; reprinted as pp. 139–191 in his *Collected Mathematical Papers*, Springer, New York, 1989. MR 17,131d Zbl 0057.27401

[Watt 1985] S. B. Watt, "Restricted ramification for imaginary quadratic number fields and a multiplicator free group", *Trans. Amer. Math. Soc.* **288**:2 (1985), 851–859. MR 86d:11093 Zbl 0557.12006

Received March 9, 2010.

NADYA MARKIN
DIVISION OF MATHEMATICAL SCIENCES
NANYANG TECHNOLOGICAL UNIVERSITY
SPMS-04-01, 21 NANYANG LINK
SINGAPORE 637371
SINGAPORE

nadyaomarkin@gmail.com
http://www3.ntu.edu.sg/home/nmarkin

STEPHEN V. ULLOM
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
1409 WEST GREEN ST
URBANA, IL 61801
UNITED STATES

ullom@math.uiuc.edu
http://www.math.uiuc.edu/∼ullom/

PACIFIC JOURNAL OF MATHEMATICS

http://www.pjmath.org

Founded in 1951 by
E. F. Beckenbach (1906–1982) and F. Wolf (1904–1989)

See inside back cover or www.pjmath.org for submission instructions.

The subscription price for 2011 is US $420/year for the electronic version, and $485/year for print and electronic.
Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163, U.S.A. Prior back issues are obtainable from Periodicals Service Company, 11 Main Street, Germantown, NY 12526-5635. The Pacific Journal of Mathematics is indexed by Mathematical Reviews, Zentralblatt MATH, PASCAL CNRS Index, Referativnyi Zhurnal, Current Mathematical Publications and the Science Citation Index.

The Pacific Journal of Mathematics (ISSN 0030-8730) at the University of California, c/o Department of Mathematics, 969 Evans Hall, Berkeley, CA 94720-3840, is published monthly except July and August. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices. POSTMASTER: send address changes to Pacific Journal of Mathematics, P.O. Box 4163, Berkeley, CA 94704-0163.

PJM peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS
at the University of California, Berkeley 94720-3840
A NON-PROFIT CORPORATION
Typeset in LaTeX

PACIFIC JOURNAL OF MATHEMATICS

Volume 253 No. 1 September 2011

0030-8730(201109)253:1;1-8