COMPOSITIO MATHEMATICA

On the minimal ramification problem for ℓ-groups

Hershy Kisilevsky and Jack Sonn

Compositio Math. **146** (2010), 599–606.

doi:10.1112/S0010437X10004719

Compositio Math. 146 (2010) 599–606
doi:10.1112/S0010437X10004719

On the minimal ramification problem for ℓ-groups

Hershy Kisilevsky and Jack Sonn

Abstract

Let ℓ be a prime number. It is not known whether every finite ℓ-group of rank $n \geqslant 1$ can be realized as a Galois group over $\mathbb{Q}$ with no more than n ramified primes. We prove that this can be done for the (minimal) family of finite ℓ-groups which contains all the cyclic groups of ℓ-power order and is closed under direct products, (regular) wreath products and rank-preserving homomorphic images. This family contains the Sylow ℓ-subgroups of the symmetric groups and of the classical groups over finite fields of characteristic not ℓ. On the other hand, it does not contain all finite ℓ-groups.

1. Introduction

Let K be a global field and L/K a finite Galois extension with Galois group $G = G(L/K)$. Let $\mathfrak{p}$ be a finite prime of K. If $\mathfrak{p}$ ramifies in L and $\mathfrak{P}$ is a prime of L dividing $\mathfrak{p}$, then the inertia group $T(\mathfrak{P}/\mathfrak{p})$ is a non-trivial subgroup of G. If T is the subgroup of G generated by all $T(\mathfrak{P}/\mathfrak{p})$, then the fixed field of T is an unramified extension of K. If $K = \mathbb{Q}$, then by Minkowski's theorem there are no non-trivial unramified algebraic extensions of $\mathbb{Q}$, so $T = G$. Suppose, in addition, that $L/\mathbb{Q}$ is tamely ramified, i.e. for every prime p ramified in $L/\mathbb{Q}$, all the $T(\mathfrak{P}/p)$ are cyclic of order prime to p. It follows, in particular, that if for each ramified p we fix an inertia group $T(\mathfrak{P}/\mathfrak{p}) = \langle g_p \rangle$, then the normal subgroup of G generated by the g_p is all of G.

We are interested in the case where $G = G(L/\mathbb{Q})$ is an ℓ-group, with ℓ being a prime. Here $L/\mathbb{Q}$ is tamely ramified if and only if all the primes p that ramify in L are prime to $|G|$. Let $\bar{G} = G/\Phi(G)$ be the quotient of G by its Frattini subgroup $\Phi(G)$. Then the normal subgroup of G generated by the g_p is all of G if and only if the images $\bar{g}_p$ in $\bar{G}$ generate $\bar{G}$, and this is true if and only if (by Burnside's basis theorem) the g_p generate G. It follows that rank(G), the minimal number of generators of G, is less than or equal to the number of primes p that ramify in L or, equivalently, that the number of primes that ramify in L is at least rank(G).

It is an open problem as to whether or not every finite ℓ-group G can be realized as the Galois group of a tamely ramified extension of $\mathbb{Q}$ with exactly rank(G) ramified primes (see, e.g., [Pla04]). We call this *the minimal ramification problem*. Using Dirichlet's theorem on primes in arithmetic progressions, it is easy to show that this problem has an affirmative answer for abelian ℓ-groups G. It has been remarked in [Ser92] that for odd ℓ, the Scholz–Reichardt method for realizing ℓ-groups over $\mathbb{Q}$ yields realizations of an ℓ-group of order ℓ^n with no more than n

Received 19 November 2008, accepted in final form 29 July 2009, published online 18 March 2010.
2000 Mathematics Subject Classification 11R32, 20D15 (primary).
Keywords: Galois group, p-group, ramified primes, wreath product, semiabelian group.
The research of the first author was supported by grants from NSERC and FQRNT. The research of the second author was supported by the Fund for the Promotion of Research at the Technion and the E. and M. Mendelson Research Fund.

ramified primes. However, $n = \operatorname{rank}(G)$ only if G is elementary abelian. In [Pla04], Plans improved this bound by showing that the Scholz–Reichardt method yields a bound equal to the sum of the ranks of the factors of the lower central series of G (without the bottom factor). Thus the minimal ramification problem has an affirmative solution for odd-order ℓ-groups G of nilpotency class 2. Nomura (see [Nom08]) refined Plans' result and proved that the minimal ramification problem has an affirmative solution for 3-groups of order less than or equal to 3^5.

In this paper we produce (for every ℓ, including $\ell = 2$) a new family of ℓ-groups for which the minimal ramification problem has an affirmative solution. To be precise, given a prime ℓ, let $\mathcal{G}(\ell)$ be the minimal family of ℓ-groups that contains the cyclic ℓ-groups and which is closed under direct products, (regular) wreath products and rank-preserving homomorphic images. Then every group G in $\mathcal{G}(\ell)$ is tamely realizable over $\mathbb{Q}$ with exactly $\operatorname{rank}(G)$ ramified (finite) primes. The family $\mathcal{G}(\ell)$ contains all direct products of iterated wreath products of cyclic groups of ℓ-power order and, in particular, all Sylow ℓ-subgroups of the symmetric groups [Kal48] and of the classical groups over finite fields of characteristic prime to ℓ (see [Wei55]). On the other hand, as we shall see, it does not contain all finite ℓ-groups.

2. ℓ-groups as Galois groups with minimal ramification

Let G and H be finite (abstract) groups. We define the (regular) *wreath product* $H \wr G$ of H with G to be the semidirect product $H^{|G|} \rtimes G$, where $H^{|G|}$ is the direct product of $|G|$ copies of H, with G acting on $H^{|G|}$ by permuting the copies of H like the regular (Cayley) representation of G. Define the nth iterated wreath product $G^{\wr n}$ of G by $G^{\wr 1} := G$ and $G^{\wr n} := G^{\wr(n-1)} \wr G$ for $n > 1$.

Proposition 1 (Ribes and Wong [RW91]). *Let G and H be finite ℓ-groups of ranks m and n, respectively. Then* $\operatorname{rank}(H \wr G) = m + n$.

Proof. Let G have minimal generating set $\{g_1, \dots, g_m\}$ and let H have minimal generating set $\{h_1, \dots, h_n\}$. Then it is clear that $H \wr G$ is generated by $\{g_1, \dots, g_m, h_1, \dots, h_n\}$, so $\operatorname{rank}(H \wr G) \leqslant m + n$. Now, if $\operatorname{rank}(H \wr G) < m + n$, then, by Burnside's basis theorem, a proper subset of $\{g_1, \dots, g_m, h_1, \dots, h_n\}$ would generate $H \wr G$. But if a g_i is dropped from this generating set, the resulting subgroup is of the form $H \wr G_1$ with G_1 a proper subgroup of G, so $H \wr G_1$ is a proper subgroup of $H \wr G$. Similarly, if an h_i is dropped from this generating set, the resulting subgroup is of the form $H_1 \wr G$ with H_1 a proper subgroup of H, so $H_1 \wr G$ is a proper subgroup of $H \wr G$. □

We will say that an extension of global fields L/K contains no non-trivial unramified subextension, or that L contains no non-trivial unramified subextension of K, if whenever $K \subseteq E \subseteq L$ are field extensions with E/K unramified, we have $E = K$.

Fix an arbitrary global field k and a prime $\ell \neq \operatorname{char}(k)$. Define a family $\mathcal{F}^{\min} := \mathcal{F}^{\min}_{k,\ell}$ of (isomorphism classes of) finite ℓ-groups as follows: $G \in \mathcal{F}^{\min}$ if and only if given any finite set S of primes of k and any finite separable extension K/k, there exists a finite Galois extension L/K with $G(L/K) \cong G$ such that the set of primes $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ of K that ramify in L satisfy the following five conditions.

(1) $n = \operatorname{rank}(G)$, the minimal number of generators of G.

(2) The primes $p_1, \dots, p_n$ of k below $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ are distinct.

(3) $\{p_1, \dots, p_n\} \cap S = \emptyset$.

(4) $p_1, \ldots, p_n$ split completely in K.

(5) L contains no non-trivial unramified subextension of K.

The main result of this paper is the next theorem.

Theorem 1. *The family $\mathcal{F}^{\min}$ has the following properties.*

(a) *$\mathcal{F}^{\min}$ contains all cyclic groups of ℓ-power order.*

(b) *If $G, H \in \mathcal{F}^{\min}$, then $G \times H \in \mathcal{F}^{\min}$.*

(c) *If $G \in \mathcal{F}^{\min}$ and N is a normal subgroup of G contained in the Frattini subgroup $\Phi(G)$ of G, then $G/N \in \mathcal{F}^{\min}$.*

(d) *If $G, H \in \mathcal{F}^{\min}$, then $H \wr G \in \mathcal{F}^{\min}$.*

Before proving the theorem, we note the following immediate consequence when $k = K = \mathbb{Q}$.

Corollary 1. *Let $\mathcal{G}(\ell)$ be the minimal family of ℓ-groups satisfying conditions (a)–(d) of Theorem 1, i.e. $\mathcal{G}(\ell)$ contains all cyclic groups of ℓ-power order and is closed under direct products, (regular) wreath products and rank-preserving homomorphic images. Then all $G \in \mathcal{G}(\ell)$ of rank n are tamely realizable over $\mathbb{Q}$ with exactly n ramified primes.*

We will use the following lemma in the proof of Theorem 1.

Lemma 1. *Suppose that K_1 and K_2 are Galois extensions of K with $\mathrm{Gal}(K_i/K) = G_i$, for $i = 1, 2$, such that K_2/K contains no non-trivial unramified subextensions. Suppose also that the extensions K_1/K and K_2/K are ramified at disjoint sets of primes of K. Then $K_1 \cap K_2 = K$ (and hence $G = \mathrm{Gal}(K_1 \cdot K_2/K) \cong G_1 \times G_2$), and for any unramified subextension $K \subseteq E \subseteq K_1 \cdot K_2$ we have $K \subseteq E \subseteq K_1$. In particular, if K_1/K also contains no non-trivial unramified subextensions, then $K_1 \cdot K_2/K$ contains no non-trivial unramified subextensions.*

Proof. Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ be the primes of K ramified in K_1 and let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$ be the primes of K ramified in K_2. Then, by assumption, $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\} \cap \{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\} = \emptyset$. Since $K_1 \cap K_2 \subseteq K_1$, we see that $K_1 \cap K_2/K$ is ramified only at primes in $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$, and similarly $K_1 \cap K_2 \subseteq K_2$ implies that $K_1 \cap K_2/K$ is ramified only at primes in $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$. Therefore $K_1 \cap K_2/K$ is unramified, and since K_2/K contains no non-trivial unramified subextension, we see that $K_1 \cap K_2 = K$ and so $\mathrm{Gal}(K_1 \cdot K_2/K) \cong G_1 \times G_2$. Let $T_{\mathfrak{Q}} \subseteq G = \mathrm{Gal}(K_1 \cdot K_2/K)$ be the subgroup generated by the inertia groups $T(\mathfrak{Q}_i/\mathfrak{q}_i)$ where $\mathfrak{Q}_i$ runs over all primes of $K_1 \cdot K_2$ dividing some prime $\mathfrak{q}_i \in \{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$. Since K_1/K is unramified at the primes $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_t\}$, we see that $K \subseteq K_1 \subseteq (K_1 \cdot K_2)^{T_{\mathfrak{Q}}}$. But since $G \cong G_1 \times G_2$, we have that the restriction map $\mathrm{res}: \mathrm{Gal}(K_1 \cdot K_2/K_1) \longrightarrow G_2$ is an isomorphism. Also, since K_2/K contains no non-trivial unramified subextension, it follows that $\mathrm{res}(T_{\mathfrak{Q}}) = G_2$, and therefore $T_{\mathfrak{Q}} = \mathrm{Gal}(K_1 \cdot K_2/K_1)$ and $K_1 = (K_1 \cdot K_2)^{T_{\mathfrak{Q}}}$. Suppose that $K \subseteq E \subseteq K_1 \cdot K_2$ with E/K unramified. Then E is contained in the subfield of $K_1 \cdot K_2$ fixed by $T_{\mathfrak{Q}}$. But then E is fixed by $T_{\mathfrak{Q}}$ and therefore $E \subseteq K_1$. If K_1/K contains no non-trivial unramified subextension, we must have $E = K$. □

We will also need a lemma from [KS06].

Let K be a global field, $\mathfrak{p}$ a finite prime of K, $I_{\mathfrak{p}}$ the group of fractional ideals prime to $\mathfrak{p}$, $P_{\mathfrak{p}}$ the group of principal fractional ideals in $I_{\mathfrak{p}}$, and $P_{\mathfrak{p},1}$ the group of principal fractional ideals in $P_{\mathfrak{p}}$ generated by elements congruent to 1 mod $\mathfrak{p}$. Then $\mathrm{Cl}_K = I_{\mathfrak{p}}/P_{\mathfrak{p}}$ is the class group of K, $\mathrm{Cl}_{K,\mathfrak{p}} = I_{\mathfrak{p}}/P_{\mathfrak{p},1}$ is the ray class group with conductor $\mathfrak{p}$, and $\overline{P}_{\mathfrak{p}} = P_{\mathfrak{p}}/P_{\mathfrak{p},1}$ is the principal ray

https://doi.org/10.1112/S0010437X10004719 Published online by Cambridge University Press

with conductor $\mathfrak{p}$. We have a short exact sequence

$$1 \longrightarrow \overline{P}_{\mathfrak{p}} \longrightarrow \mathrm{Cl}_{K,\mathfrak{p}} \longrightarrow \mathrm{Cl}_K \longrightarrow 1. \qquad (*)$$

For prime $\ell \neq \mathrm{char}(K)$, we consider the following exact sequence of ℓ-primary components:

$$1 \longrightarrow \overline{P}_{\mathfrak{p}}^{(\ell)} \longrightarrow \mathrm{Cl}_{K,\mathfrak{p}}^{(\ell)} \longrightarrow \mathrm{Cl}_K^{(\ell)} \longrightarrow 1. \qquad (*_\ell)$$

We are interested in primes $\mathfrak{p}$ for which the sequence $(*_\ell)$ splits. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_s \in I_K$ be such that their images $\bar{\mathfrak{a}}_i$ in $\mathrm{Cl}_K^{(\ell)}$ form a basis of the finite abelian ℓ-group $\mathrm{Cl}_K^{(\ell)}$. Let ℓ^{m_i} be the order of $\bar{\mathfrak{a}}_i$, with $i = 1, \ldots, s$. Then $\mathfrak{a}_i^{\ell^{m_i}} = (a_i) \in P_K$ for $i = 1, \ldots, s$. Write K' for $K(\zeta_{\ell^m}, \sqrt[\ell^m]{\epsilon}, \sqrt[\ell^{m_i}]{a_i}, 1 \leqslant i \leqslant s)$, the field extension obtained by adjoining a primitive ℓ^mth root of unity ζ_{ℓ^m}, the ℓ^mth roots of all units ϵ of K, and the ℓ^{m_i}th roots of the elements $a_i \in K$, where $m \geqslant \max\{1, m_1, \ldots, m_s\}$.

Lemma 2 (Splitting lemma [KS06, Lemma 2.1]). *For the sequence $(*_\ell)$ to split, it is sufficient that $\mathfrak{p}$ splits completely in K'.*

For the proof of this lemma, see [KS06].

Proof of Theorem 1. Let K and S be given.

(a) Let $p \notin S$ be a prime of k which splits completely in K', where K' is the field defined in the splitting lemma for K. Let $\mathfrak{p}$ be a prime of K dividing p. Then, by the splitting lemma, the ℓ-ray class field $R_{\mathfrak{p}}$ of K belonging to the ray class group $\mathrm{Cl}_{K,\mathfrak{p}}^{(\ell)}$ has Galois group isomorphic to $\mathrm{Cl}_K^{(\ell)} \times \overline{P}_{\mathfrak{p}}^{(\ell)}$. Since the ℓ-Hilbert class field $H_K^{(\ell)}$ belongs to $\mathrm{Cl}_K^{(\ell)}$, we see that $R_{\mathfrak{p}} = H_K^{(\ell)} \cdot L'$ with $H_K^{(\ell)} \cap L' = K$ and that $\mathrm{Gal}(L'/K) \cong \overline{P}_{\mathfrak{p}}^{(\ell)}$. Under our assumption that all units are ℓ^mth powers modulo $\mathfrak{p}$, it follows that

$$\overline{P}_{\mathfrak{p}}^{(\ell)} / (\overline{P}_{\mathfrak{p}}^{(\ell)})^{\ell^m} \cong (\mathcal{O}_K/\mathfrak{p})^* / ((\mathcal{O}_K/\mathfrak{p})^*)^{\ell^m}$$

is cyclic and has order divisible by ℓ^m. Taking $m \geqslant r$, we see that there exists a cyclic extension L/K of degree ℓ^r that is ramified only at $\mathfrak{p}$ and in which $\mathfrak{p}$ is totally ramified. Thus L/K satisfies conditions (1)–(5) (with $n = 1$).

(b) Since $G \in \mathcal{F}^{\min}$, there is an extension K_1/K with $\mathrm{Gal}(K_1/K) \cong G$ which satisfies properties (1)–(5) with the sets of primes $\{p_1, \ldots, p_n\}$ and $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Set $S' = S \cup \{p_1, \ldots, p_n\}$. Since $H \in \mathcal{F}^{\min}$, let K_2/K be an extension with $\mathrm{Gal}(K_2/K) \cong H$ which satisfies properties (1)–(5) for K and S', with primes $\{q_1, \ldots, q_m\}$ and $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$, respectively. Then, by Lemma 1, $L = K_1K_2$ puts $G \times H$ in $\mathcal{F}^{\min}$ with primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$, and $n + m = \mathrm{rank}(G \times H)$. This establishes (b).

(c) Let L/K be a Galois extension with group G which puts G in $\mathcal{F}^{\min}$. Let N be a normal subgroup of G contained in $\Phi(G)$. Let L' be the fixed field of N. Then $\mathrm{rank}(G/N) = \mathrm{rank}(G)$. The other conditions are immediate.

(d) Let K_1/K be a Galois extension with group G which puts G in $\mathcal{F}^{\min}$, with ramified primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ over $p_1, \ldots, p_n \notin S$. Let $m = \mathrm{rank}(H)$ and $S_1 = S \cup \{p_1, \ldots, p_n\}$. Apply the hypothesis $H \in \mathcal{F}^{\min}$ to the pair K_1, S_1. Then there exists a Galois extension L_1/K_1 with group H, with m primes $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m$ of K_1 ramified in L_1 such that the primes $q_1, \ldots, q_m$ of k below $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m$ are distinct, $q_1, \ldots, q_m$ split completely in K_1, $q_1, \ldots, q_m \notin S_1$, and L_1 contains no non-trivial unramified extension of K_1. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ be the primes of K below $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m$. Then $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ split completely in K_1. So each $\mathfrak{Q}_i$ has $|G|$ distinct conjugates $\{\sigma(\mathfrak{Q}_i) \mid \sigma \in G\}$ over K, for $i = 1, \ldots, m$. For each $\sigma \in G$, the conjugate extension $\sigma(L_1)/K_1$ is well-defined since L_1/K_1 is Galois. Let L be the composite of the $\sigma(L_1)$, $\sigma \in G$. For each $\sigma \in G$, $\sigma(L_1)/K_1$ is Galois with group H, with exactly m ramified primes $\sigma(\mathfrak{Q}_1), \ldots, \sigma(\mathfrak{Q}_m)$ lying above $q_1, \ldots, q_m$, and $\sigma(L_1)$ contains no unramified extension of K_1. Furthermore, the set of primes $\sigma(\mathfrak{Q}_1), \ldots, \sigma(\mathfrak{Q}_m)$ ramified in $\sigma(L_1)/K_1$ is disjoint from the set of primes $\tau(\mathfrak{Q}_1), \ldots, \tau(\mathfrak{Q}_m)$ ramified in $\tau(L_1)/K_1$ if $\sigma \neq \tau$. This is true because if $\sigma(\mathfrak{Q}_i) = \tau(\mathfrak{Q}_j)$, we would have $q_i = q_j$; but then $i = j$ by property (3) in the definition of $\mathcal{F}^{\min}$ and so we would have $\sigma = \tau$.

Applying Lemma 1 repeatedly, we see that the fields $\{\sigma(L_1) \mid \sigma \in G\}$ are linearly disjoint over K_1. It follows that we have an exact sequence of groups

$$1 \to H^{|G|} \to G(L/K) \to G \to 1, \qquad (\dagger)$$

where G is identified with $G(K_1/K)$ and $H^{|G|}$ is the direct product of $|G|$ copies of H. Furthermore, this exact sequence defines a unique homomorphism $\phi : G \to \mathrm{Out}(H^{|G|})$ (injective in this case), which is equivalent, as a permutation representation on the $|G|$ copies of H, to the regular representation of G. The set of all group extensions of G by $H^{|G|}$ corresponding to a given ϕ, if non-empty, is in one-to-one correspondence with $H^2(G, Z(H^{|G|}))$ (see [JZ71]), where $Z(H^{|G|})$ denotes the center of $H^{|G|}$. Since $Z(H^{|G|}) = Z(H)^{|G|}$ is an induced G-module, $H^2(G, Z(H^{|G|})) = 0$. It follows that the group extension ($\dagger$) splits, and $G(L/K) \cong H \wr G$.

The primes of K that ramify in L are exactly $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$, where $n + m = \mathrm{rank}(H \wr G)$; the primes $p_1, \ldots, p_n, q_1, \ldots, q_m$ below $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$ are distinct, split completely in K, and lie outside S. Finally, L/K does not contain a non-trivial unramified subextension M/K, since if it did, then M would be contained in K_1, and K_1/K contains no non-trivial unramified subextension of K. □

How large is the family $\mathcal{G}(\ell)$? It is smaller than the family of all ℓ-groups, as we will now show.

Lemma 3. *Let G be a non-trivial group in $\mathcal{G}(\ell)$, and let $\mathrm{dl}(G)$ be the derived length (length of the derived series) of G. Then $\mathrm{dl}(G) \leqslant \mathrm{rank}(G)$.*

Proof. We prove this result by induction on the minimal number t of applications of the three types of operations (direct product, wreath product, rank-preserving homomorphic image) defining $\mathcal{G}(\ell)$ which are needed to produce G starting from cyclic ℓ-groups. If $t = 0$ (G cyclic), we have $\mathrm{dl}(G) = \mathrm{rank}(G)$. We examine the behavior of the rank and the derived length under each of the three operations.

(i) If $G, H \in \mathcal{G}(\ell)$, then $\mathrm{rank}(G \times H) = \mathrm{rank}(G) + \mathrm{rank}(H)$ while $\mathrm{dl}(G \times H) = \max(\mathrm{dl}(G), \mathrm{dl}(H))$.

(ii) If $G, H \in \mathcal{G}(\ell)$, then $\mathrm{rank}(H \wr G) = \mathrm{rank}(G) + \mathrm{rank}(H)$ (Proposition 2) while $\mathrm{dl}(H \wr G) \leqslant \mathrm{dl}(G) + \mathrm{dl}(H)$ (easy).

(iii) If $G \in \mathcal{G}(\ell)$ and $\overline{G}$ is a homomorphic image of G (with $\mathrm{rank}(\overline{G}) = \mathrm{rank}(G)$), then $\mathrm{dl}(\overline{G}) \leqslant \mathrm{dl}(G)$.

The result follows. □

Proposition 2. *For every ℓ and $n > 1$, there exist ℓ-groups of rank n not in $\mathcal{G}(\ell)$.*

Proof. It suffices to show that for every $n > 1$, there exist ℓ-groups of rank n and derived length larger than n. Let F be the free group of rank n, and let F_t be the tth term of the descending ℓ-central series of F (i.e. the series with $F_1 = F$ and, for $t > 1$, $F_t = F_{t-1}^{\ell}[F, F_{t-1}]$). It suffices

https://doi.org/10.1112/S0010437X10004719 Published online by Cambridge University Press

to show that the derived length of F/F_t is larger than n for sufficiently large t. But this is true since the derived length of F is infinite and the descending ℓ-central series of F has trivial intersection. (For sufficiently large t, F_t does not contain the (non-trivial) nth term of the derived series of F.) □

Example 1. Here is an example of an ℓ-group not in the family $\mathcal{G}(\ell)$. (We thank John Labute for help with this example.)

Let F be a free group on two generators x and y, and let G be the quotient of F by the sixth term F_6 of the descending ℓ-central series of F. We claim that $G \notin \mathcal{G}(\ell)$. By Lemma 3, it suffices to show that $\mathrm{dl}(G) = 3$. Indeed, $[[x, y], [x, [x, y]]]$ lies in F_5 but not in F_6, so there are two elements of the commutator subgroup G' of G whose commutator is non-trivial. (For another example see Remark 2 below.)

Remark 1. If we drop condition (1) from the definition of $\mathcal{F}^{\min}$ to obtain the (larger) family $\mathcal{F}$, then we get the following variant of Theorem 1.

Theorem 2. *The family $\mathcal{F}$ has the following properties.*

(a) *$\mathcal{F}$ contains all cyclic groups of ℓ-power order.*

(b) *If $G, H \in \mathcal{F}$, then $G \times H \in \mathcal{F}$.*

(c) *If $G \in \mathcal{F}$, then every homomorphic image of G is in $\mathcal{F}$.*

(d) *If $G, H \in \mathcal{F}$, then $H \wr G \in \mathcal{F}$.*

The proof is the same as that of Theorem 1, *mutatis mutandis*. As with Theorem 1, we obtain the following corollary.

Corollary 2. *Let $\hat{\mathcal{G}}(\ell)$ be the minimal family of ℓ-groups satisfying conditions (a)–(d) of Theorem 2. Then all $G \in \hat{\mathcal{G}}(\ell)$ are tamely realizable over $\mathbb{Q}$.*

Theorem 2 in fact gives tame realizations of the groups in $\hat{\mathcal{G}}(\ell)$ over every global field, which of course follows from the Scholz–Reichardt theorem for ℓ odd, and from Shafarevich's theorem for $\ell = 2$. However, for these groups we obtain a different, perhaps simpler, proof, especially for $\ell = 2$.

Remark 2. A finite group G is called *semiabelian* if and only if there exists a sequence

$$G_0 = \{1\}, \quad G_1, \ldots, G_n = G$$

such that G_i is a homomorphic image of a semidirect product $A_i \rtimes G_{i-1}$ with A_i abelian, $i = 1, \ldots, n$.

It turns out that $\hat{\mathcal{G}}(\ell)$ is the family of all semiabelian ℓ-groups, as we will show. Dentzer [Den95] gives geometric realizations of the semiabelian groups over $k(t)$ for any field k (in particular, for k a global field) and therefore, by Hilbert's irreducibility theorem, realizations over global fields k. However, it does not seem to be known how to produce tame realizations via Hilbert's irreducibility theorem. In [Den95] there is also an example of a three-generator ℓ-group of order ℓ^5 (for any odd ℓ) which is not semiabelian.

Proposition 3. *For any prime ℓ, $\hat{\mathcal{G}}(\ell)$ is the family of all semiabelian ℓ-groups.*

Proof. Let $\mathcal{S}(\ell)$ denote the family of all semiabelian ℓ-groups. It is clear from the definition that $\mathcal{S}(\ell)$ contains all cyclic ℓ-groups and is closed under homomorphic images. Furthermore, by [Den95, Theorem 2.8], $\mathcal{S}(\ell)$ is closed under direct products and (regular) wreath products. Hence $\mathcal{S}(\ell)$ contains $\hat{\mathcal{G}}(\ell)$. For the reverse inclusion, suppose to the contrary that G is a group of minimal order in $\mathcal{S}(\ell)\backslash\hat{\mathcal{G}}(\ell)$. Then G is non-abelian and hence non-trivial. By [Den95, Theorem 2.3], G is a composite AH with H being a proper semiabelian subgroup of G and A an abelian normal subgroup of G. Then G is a homomorphic image of a semidirect product $A \rtimes H$ and, by the induction hypothesis, $H \in \hat{\mathcal{G}}(\ell)$. Now $A \rtimes H$ is a homomorphic image of the (regular) wreath product $A \wr H$; this lies in $\hat{\mathcal{G}}(\ell)$, and hence so does its homomorphic image $AH = G$, which is a contradiction. □

Remark 3. Given a finite ℓ-group G, let $\mathrm{ram}^t(G)$ denote the minimal n such that G can be realized as a Galois group of a tamely ramified extension $L/\mathbb{Q}$ with exactly n ramified primes. As mentioned in the introduction, Plans [Pla04] has shown that the Scholz–Reichardt method for realizing odd-order ℓ-groups over $\mathbb{Q}$ can be made to yield an upper bound for $\mathrm{ram}^t(G)$ equal to the sum of the ranks of the factors in the lower central series of G, where the bottom factor can be left out of the sum. For most of the groups in the family $\mathcal{G}(\ell)$, this bound is larger than the rank of the group, e.g. for $C_\ell \wr C_\ell,\ \ell > 3$.

Note. Since the submission of this paper, Neftin has proved in [Nef09] that the family $\mathcal{G}(\ell)$ is *equal* to the family $\hat{\mathcal{G}}(\ell)$ of semiabelian ℓ-groups. To give some indication of the size of $\mathcal{G}(\ell)$, the following is known about 'small' ℓ-groups (see [Den95] and also [Sch93]).

(1) For any ℓ, all ℓ-groups of order less than or equal to ℓ^4 are semiabelian.

(2) All 2-groups of order less than or equal to 32 are semiabelian.

(3) Among the 267 groups of order 64, only ten are not semiabelian. Similarly, among the 2328 groups of order 2^7, 82 are not semiabelian; and among the 56 092 groups of order 2^8, 993 are not semiabelian. Among the 67 groups of order 3^5, ten are not semiabelian, and among the 504 groups of order 3^6, 54 are not semiabelian.

References

Den95 R. Dentzer, *On geometric embedding problems and semiabelian groups*, Manuscripta Math. **86** (1995), 199–216.

JZ71 C. E. Johnson and H. Zassenhaus, *On equivalence of finite group extensions*, Math. Z. **123** (1971), 191–200.

Kal48 L. Kaloujnine, *La structure des p-groupes de Sylow des groupes symetriques finis*, Ann. Sci École Norm. Sup. (3) **65** (1948), 239–276.

KS06 H. Kisilevsky and J. Sonn, *Abelian extensions of global fields with constant local degrees*, Math. Res. Lett. **13** (2006), 599–605.

Nef09 D. Neftin, *On semiabelian p-groups*, Preprint, arXiv:0908.1472v2 [math.gr].

Nom08 A. Nomura, *Notes on the minimal number of ramified primes in some l-extensions of* $\mathbb{Q}$, Arch. Math. **90** (2008), 501–510.

Pla04 B. Plans, *On the minimal number of ramified primes in some solvable extensions of* $\mathbb{Q}$, Pacific J. Math. **215** (2004), 381–391.

RW91 L. Ribes and K. Wong, *On the minimal number of generators of certain groups*, in *Groups St Andrews 1989*, London Mathematical Society Lecture Note Series, vol. 159–160 (Cambridge University Press, Cambridge, 1991).

Sch93 L. Schneps, *Reduction of p-groups*, Comm. Algebra **21** (1993), 1603–1609.

Ser92 J.-P. Serre, *Topics in Galois theory* (Jones and Bartlett, Boston, 1992).

Wei55 A. J. Weir, *Sylow p-subgroups of the classical groups over finite fields with characteristic prime to p*, Proc. Amer. Math. Soc. **6** (1955), 529–533.

Hershy Kisilevsky kisilev@mathstat.concordia.ca
Department of Mathematics and Statistics, Concordia University, Montreal, Quebec H3G 1M8, Canada

Jack Sonn sonn@math.technion.ac.il
Department of Mathematics, Technion, 32000 Haifa, Israel

https://doi.org/10.1112/S0010437X10004719 Published online by Cambridge University Press