

# TAMELY RAMIFIED SUBFIELDS OF DIVISION ALGEBRAS

DANNY NEFTIN

ABSTRACT. For any number field  $K$ , it is unknown which finite groups appear as Galois groups of extensions  $L/K$  such that  $L$  is a maximal subfield of a division algebra with center  $K$  (a  $K$ -division algebra). For  $K = \mathbb{Q}$ , the answer is described by the long standing  $\mathbb{Q}$ -admissibility conjecture.

We extend a theorem of Neukirch on embedding problems with local constraints in order to determine for every number field  $K$ , what finite solvable groups  $G$  appear as Galois groups of tame maximal subfields of  $K$ -division algebras, generalizing Liedahl's theorem for metacyclic  $G$  and Sonn's solution of the  $\mathbb{Q}$ -admissibility conjecture for solvable groups.

## 1. INTRODUCTION

A division algebra  $D$  which is finite dimensional over its center  $K$  (a  $K$ -division algebra), is called a  $G$ -crossed product if there exists a Galois extension  $L/K$  with Galois group  $G$  (a  $G$ -extension) such that  $L$  is a maximal subfield of  $D$ . Crossed products are fundamental in the study of division algebras and are accompanied by a structure which explicitly describes them (see [20, Chp. 14-19]). A group  $G$  is called  $K$ -admissible if there exists a  $G$ -crossed product  $K$ -division algebra; a field extension  $L/K$  is called *adequate* if  $L$  is a maximal subfield of a  $K$ -division algebra<sup>1</sup>.

It is known by the Brauer-Hasse-Noether theorem that over a number field  $K$ , all  $K$ -division algebras are crossed products with respect to a cyclic group. However, it is unknown for which groups  $G$  there exists a  $G$ -crossed product  $K$ -division algebra, i.e. what groups are  $K$ -admissible?

Over  $\mathbb{Q}$ , Schacher observed ([21]) that the Sylow subgroups  $P$  of a  $\mathbb{Q}$ -admissible group are *metacyclic*, that is  $P$  has a cyclic normal subgroup  $C \triangleleft P$  such that  $P/C$  is also cyclic. The converse of this observation is known as the  $\mathbb{Q}$ -admissibility conjecture:

**Conjecture 1.1.** *Every group with metacyclic Sylow subgroups is  $\mathbb{Q}$ -admissible.*

---

<sup>1</sup>In fact by [21],  $L/K$  is adequate if and only if  $L$  is a subfield of a  $K$ -division algebra. Thus, the maximality requirement can be omitted.

This conjecture was studied extensively (e.g. [4],[5],[6],[10],[11],[21]) and proven by Sonn for solvable groups in a series of papers ([3], [23] and [24]).

Recently, analogs of this conjecture were proved by Harbater, Hartmann and Krashen over function fields of curves over complete discretely valued fields with algebraically closed residue fields ([13], cf. [12]), by Paran and the author over two dimensional complete local domains with algebraically closed residue fields ([16]), and by Surendranath and Suresh over function fields of curves over complete discretely valued fields which contain enough roots of unity ([25]). However, the situation over number fields is far from being understood.

Schacher's observation extends to number fields under an additional assumption of tameness as follows. Let  $\mu_n$  denote the set of  $n$ -th roots of unity and  $\sigma_{t,n}$  be the automorphism of  $\mathbb{Q}(\mu_n)$  for which  $\sigma_{t,n}(\zeta) = \zeta^t$  for all  $\zeta \in \mu_n$ . Using a similar argument to Liedahl's [14, Theorem 28], we observe that if  $G$  appears as a Galois group of a tamely ramified adequate extension of a number field  $K$  then its Sylow subgroups are metacyclic, and furthermore for every  $l \mid |G|$ , the  $l$ -Sylow subgroups  $G(l)$  of  $G$  admit a presentation:

$$(1.1) \quad G(l) \cong \mathcal{M}(m, n, i, t) := \langle x, y \mid x^m = y^i, y^n = 1, x^{-1}yx = y^t \rangle$$

such that  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$  (see "only if part" of Theorem 1.3).

This observation suggests the following natural generalization of Conjecture 1.1:

**Question 1.2.** Let  $K$  be a number field and  $G$  a group whose  $l$ -Sylow subgroups admit a presentation  $\mathcal{M}(m, n, i, t)$  such that  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$ , for every  $l \mid |G|$ . Is  $G$  necessarily  $K$ -admissible? Furthermore, is there necessarily a tamely ramified adequate  $G$ -extension of  $K$ ?

The first part of this question is known to have an affirmative answer for metacyclic  $G$  ([14, Theorem 27]) and for some small order groups:  $A_5$  ([11]), the central extension  $\mathrm{SL}_2(5)$  of  $A_5$  ([9]),  $A_6, A_7$  ([22]), the double covers of  $A_6$  and  $A_7$  ([8]),  $\mathrm{PSL}_2(7)$  ([1]) and  $\mathrm{PSL}_2(11)$  ([7]).

In this paper we give a positive answer to Question 1.2 for solvable groups, generalizing Liedahl's [14, Theorem 27] and Sonn's [24, Theorem 1]:

**Theorem 1.3.** *Let  $K$  be a number field and  $G$  a solvable group. Then there exists a tamely ramified adequate  $G$ -extension  $L/K$  if and only if for every  $l \mid |G|$ , the  $l$ -Sylow subgroups of  $G$  admit a presentation  $\mathcal{M}(m, n, i, t)$  such that  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$ .*

We note that since the proof of Sonn's theorem ([24]) over  $\mathbb{Q}$  is based on Neukirch's [17, Main Theorem] which makes an assumption on the absence of roots of unity in  $K$ , Sonn's proof does not apply over arbitrary number fields.

A key ingredient in our proof is an extension of [18, Korollar 6.4]. Neukirch's Korollar 6.4 is a highly useful tool that under the assumption of at least one of six conditions on a finite set  $S$  of primes of the base field, allows to change solutions of embedding problems to satisfy any prescribed local conditions at  $S$  (generalizing the Grunwald-Wang theorem). We extend Korollar 6.4 by showing that under the assumption of at least one of four of these six conditions on  $S$ , it is possible to change a solution to satisfy prescribed conditions at  $S$  leaving the solution unchanged at any given finite set of primes  $T$ .

We use this extension to strengthen Sonn's proof of [24, Theorem 1] in order to obtain tamely ramified adequate  $G$ -extensions of  $\mathbb{Q}$  with prescribed local behavior at given finite sets of primes. This gives us a strong control over the ramification of  $G$ -crossed product  $\mathbb{Q}$ -division algebras, allowing us to lift these to division algebras over a given number field and by that prove Theorem 1.3.

This work is partially based on the author's Ph.D. thesis ([15]). I would like to thank my thesis advisor Jack Sonn for investing time and effort into teaching and guiding me, and for helpful comments on this manuscript.

## 2. EMBEDDING PROBLEMS AND LOCAL GALOIS GROUPS

**2.1. Embedding problems.** The theory of embedding problems is central in the study of the inverse Galois problem and is a key ingredient in our proof of Theorem 1.3. We shall describe a setup for these problems, recall Neukirch's [18, Korollar 6.4] and extend it.

**2.1.1. Setup.** Embedding problems are a strong generalization of the inverse Galois problem which ask whether a Galois extension can be embedded into a larger Galois extension with a given Galois group. The precise setup is as follows.

A (*finite*) *embedding problem* over a number field  $K$  consists of a finite Galois extension  $L/K$  and an epimorphism of finite groups  $\pi : E \rightarrow G := \text{Gal}(L/K)$ . For our purposes it suffices to consider embedding problems with abelian kernel  $A := \ker(\pi)$ .

Let  $G_K$  denote the absolute Galois group of  $K$ . Two homomorphisms  $\psi_1, \psi_2 : G_K \rightarrow E$  are called equivalent if there is an  $a \in A$  such that  $a^{-1}\psi_1(g)a = \psi_2(g)$  for all  $g \in G_K$ . A *solution* for  $\pi$  is an equivalence class of homomorphisms  $\psi : G_K \rightarrow E$  (not necessarily surjective) for which  $\pi \circ \psi$  is the restriction map  $\text{res}_L : G_K \rightarrow G$ . For a surjective solution  $\psi$ , the fixed field  $M = \overline{K}^{\ker(\psi)}$  contains  $L$  and has Galois group  $\text{Gal}(M/K) \cong E$ .

The epimorphism  $\pi$  defines an action of  $G$  on  $A$  and hence induces a  $G_K$ -module structure on  $A$  via  $\text{res}_L$ . For every crossed homomorphism  $\chi \in H^1(G_K, A)$  and solution  $\psi : G_K \rightarrow E$ , the map  $\psi' = \chi \cdot \psi$  given by  $\psi'(\sigma) = \chi(\sigma)\psi(\sigma)$  for all  $\sigma \in G_K$ , is also a solution (see [19, Chp.

IX, §4]). In fact, for every two solutions  $\psi, \psi'$  of  $\pi$ , there is a unique  $\chi \in H^1(G_K, A)$  such that  $\psi' = \chi \cdot \psi$ . We think of  $\chi$  as the element that “changes”  $\psi$  to  $\psi'$ .

**2.1.2. Embedding problems with prescribed local conditions.** By a prime  $\mathfrak{p}$  of  $K$  we mean a finite or infinite prime. Fix an algebraic closure  $\overline{K}$  of  $K$ , an algebraic closure  $\overline{K}_{\mathfrak{p}}$  of the completion  $K_{\mathfrak{p}}$ , and an inclusion of  $\overline{K}$  into  $\overline{K}_{\mathfrak{p}}$  for every prime  $\mathfrak{p}$  of  $K$ . In particular, the embedding problem  $\pi$  induces a local embedding problem  $\pi_{\mathfrak{p}} : \pi^{-1}(G_{\mathfrak{p}}) \rightarrow G_{\mathfrak{p}}$  where  $G_{\mathfrak{p}} = \text{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}})$ ,  $L_{\mathfrak{p}} := LK_{\mathfrak{p}}$ . Moreover, the restriction  $\psi_{\mathfrak{p}}$  of a solution  $\psi : G_K \rightarrow E$  to the subgroup  $G_{K_{\mathfrak{p}}}$  is a solution for  $\pi_{\mathfrak{p}}$ .

Let  $S$  be a finite set of primes of  $K$  and for every  $\mathfrak{p} \in S$  fix (prescribe) a solution  $\psi^{(\mathfrak{p})}$  to  $\pi_{\mathfrak{p}}$ , assuming such (local) solutions exist. Similarly to the Grunwald-Wang theorem, one is interested in solutions  $\psi$  of  $\pi$  such that  $\psi_{\mathfrak{p}} = \psi^{(\mathfrak{p})}$  for all  $\mathfrak{p} \in S$ .

Assume  $\pi$  has a solution  $\phi$ . Then for every  $\mathfrak{p} \in S$  there is  $\chi^{(\mathfrak{p})} \in H^1(G_{K_{\mathfrak{p}}}, A)$  such that  $\psi^{(\mathfrak{p})} = \chi^{(\mathfrak{p})} \cdot \phi_{\mathfrak{p}}$ . If the element  $(\chi^{(\mathfrak{p})})_{\mathfrak{p} \in S}$  has a source  $\chi$  under the restriction map:

$$\rho_S : H^1(G_K, A) \rightarrow \prod_{\mathfrak{p} \in S} H^1(G_{K_{\mathfrak{p}}}, A)$$

then  $\psi := \chi \cdot \phi$  is a solution for  $\pi$  which restricts to  $\psi^{(\mathfrak{p})} = \chi^{(\mathfrak{p})} \cdot \phi_{\mathfrak{p}}$  at all  $\mathfrak{p} \in S$ . Thus, if the map  $\rho_S$  is surjective, every solution for  $\pi$  can be “changed” to a solution with prescribed local conditions at  $S$ .

**2.1.3. Neukirch’s Korollar.** [18, Korollar 6.4] is a highly useful criteria for the map  $\rho_S$  to be surjective. Let  $A$  be a  $G_K$ -module and  $n = \exp(A)$ . Let  $A' = \text{Hom}(A, \mu_n)$  be the dual  $G_K$ -module and  $K(A')$  the fixed field of the centralizer of  $A'$  in  $G_K$ . Let  $G' := \text{Gal}(K(A')/K)$  and for a prime  $\mathfrak{p}$  of  $K$ , let  $G'_{\mathfrak{p}} := \text{Gal}(K(A')_{\mathfrak{p}}/K_{\mathfrak{p}})$ . Denote  $\Gamma(G, A) := \ker \left( H^1(G, A) \rightarrow \prod_{g \in G} H^1(\langle g \rangle, A) \right)$ .

**Theorem 2.1.** (Neukirch [18, Korollar 6.4]) *Let  $S$  be a finite set of primes of  $K$ . Then the map  $\rho_S$  is surjective in each of the following cases:*

- (a)  $\Gamma(G'_{\mathfrak{p}}, A') = 0$  for all  $\mathfrak{p} \in S$ ,
- (b) for every  $\mathfrak{p} \in S$ , the group  $G'_{\mathfrak{p}}$  is cyclic or a semidirect product of two cyclic groups of relatively prime orders,
- (c)  $H^1(G', A') = 0$ ,
- (d)  $|G'| = \text{lcm}\{|G'_{\mathfrak{p}}| \mid \mathfrak{p} \notin S\}$ ,
- (e)  $A$  is cyclic of odd order,
- (f) the action of  $G_K$  on  $A$  is trivial and  $(K, \exp(A), S)$  does not fall into a special case.

In (f), when  $\exp(A) = 2^t m$ ,  $m$  odd, one says that the triple  $(K, \exp(A), S)$  falls into a special case if  $K(\mu_{2^t})/K$  is noncyclic and  $S$  contains all primes  $\mathfrak{p}$  for which  $K_{\mathfrak{p}}(\mu_{2^t})/K_{\mathfrak{p}}$  is noncyclic.

Thus, under each of these conditions one can change a solution to satisfy arbitrary prescribed local conditions at  $S$ . Furthermore, we show that under each of conditions (a), (b), (c) or (e) it is possible to change a solution to satisfy prescribed local conditions at  $S$  leaving the solution unchanged at a given finite set of primes  $T$ .

**Proposition 2.2.** *Let  $A$  be a finite  $G_K$ -module. Assume that conditions (a) or (b) hold for a finite set  $S$ . Then the subgroup*

$$\prod_{\mathfrak{p} \in S} H^1(G_{K_{\mathfrak{p}}}, A) \times \prod_{\mathfrak{p} \in T} \{0\}$$

*is in the image of  $\rho_{S \cup T}$  for every finite set  $T$  disjoint from  $S$ .*

*Proof.* Since by [18, Satz 6.2] condition (b) implies (a), it suffices to prove the assertion when (a) holds. Assume that  $\Gamma(G'_{\mathfrak{p}}, A') = 0$  for all  $\mathfrak{p} \in S$ . Let  $P$  be the set of all primes of  $K$  and  $\prod'_{\mathfrak{p} \in P} H^1(G_{K_{\mathfrak{p}}}, A)$  the restricted product over the subgroup  $\prod_{\mathfrak{p} \in P} H^1_{un}(G_{K_{\mathfrak{p}}}, A)$ . Recall that the Poitou-Tate theorem gives a non-degenerate bilinear map

$$\beta : \prod'_{\mathfrak{p} \in P} H^1(G_{K_{\mathfrak{p}}}, A) \times \prod'_{\mathfrak{p} \in P} H^1(G_{K_{\mathfrak{p}}}, A') \rightarrow \mathbb{Q}/\mathbb{Z}$$

which is defined as the product of local bilinear maps

$$\beta_{\mathfrak{p}} : H^1(G_{K_{\mathfrak{p}}}, A) \times H^1(G_{K_{\mathfrak{p}}}, A') \rightarrow \mathbb{Q}/\mathbb{Z}$$

for every  $\mathfrak{p} \in P$ .

Following [18], for a finite set  $U$  of primes of  $K$  we let:

$$\rho'_U : H^1(G_K, A') \rightarrow \prod'_{\mathfrak{p} \notin U} H^1(G_{K_{\mathfrak{p}}}, A')$$

be the restriction map,  $\Delta = \text{coker}(\rho_{S \cup T})$  and  $\nabla = \ker(\rho'_{S \cup T}) / \ker(\rho'_0)$ . By [18, Satz 4.4],  $\beta$  induces a non-degenerate bilinear form  $\beta_0 : \Delta \times \nabla \rightarrow \mathbb{Q}/\mathbb{Z}$ , which is given on  $\chi := (\chi_{\mathfrak{p}})_{\mathfrak{p} \in S \cup T} \in \Delta$  and  $\lambda \in \nabla$  by  $\beta_0(\chi, \lambda) := \beta(\tilde{\chi}, \rho'_0(\lambda))$  where  $\tilde{\chi} \in \prod'_{\mathfrak{p} \in P} H^1(G_{K_{\mathfrak{p}}}, A)$  is any element whose  $\mathfrak{p}$ -th component is  $\chi_{\mathfrak{p}}$  at all  $\mathfrak{p} \in S \cup T$ .

Let  $\chi = \prod_{\mathfrak{p} \in S \cup T} \chi_{\mathfrak{p}}$  be an element of  $\Delta$  such that  $\chi_{\mathfrak{p}} = 0$  for all  $\mathfrak{p} \in T$ . We claim that  $\chi$  is orthogonal to  $\nabla$  and therefore it is the zero element in  $\Delta$ , proving the proposition.

Letting  $\tilde{\chi} = (\tilde{\chi}_{\mathfrak{p}})_{\mathfrak{p} \in P} \in \prod'_{\mathfrak{p} \in P} H^1(G_{K_{\mathfrak{p}}}, A)$  where  $\tilde{\chi}_{\mathfrak{p}} = \chi_{\mathfrak{p}}$  for  $\mathfrak{p} \in S$  and  $\tilde{\chi}_{\mathfrak{p}} = 0$  for  $\mathfrak{p} \notin S$ , we have  $\beta_0(\chi, \nabla) = \beta(\tilde{\chi}, \rho'_0(\nabla))$ . Since  $\tilde{\chi}_{\mathfrak{p}} = 0$  for  $\mathfrak{p} \notin S$ , it suffices to show that  $\beta_{\mathfrak{p}}(\chi_{\mathfrak{p}}, \rho'_0(\nabla)_{\mathfrak{p}}) = 0$  for all  $\mathfrak{p} \in S$ , where  $\rho'_0(\nabla)_{\mathfrak{p}}$  is the projection of  $\rho'_0(\nabla)$  to the  $\mathfrak{p}$ -th factor. But [18, Satz 6.3] implies that the image of  $\nabla$  under the restriction map

$$\rho_{S \cup T, A'} : H^1(G_K, A') \rightarrow \prod_{\mathfrak{p} \in S \cup T} H^1(G_{K_{\mathfrak{p}}}, A')$$

lies in  $\prod_{\mathfrak{p} \in S \cup T} \Gamma(G'_{\mathfrak{p}}, A')$ . Since by assumption  $\Gamma(G'_{\mathfrak{p}}, A') = 0$  for  $\mathfrak{p} \in S$ , we get  $\rho'_{\emptyset}(\nabla)_{\mathfrak{p}} = \rho_{S \cup T, A'}(\nabla)_{\mathfrak{p}} = 0$  and hence  $\beta_{\mathfrak{p}}(\chi_{\mathfrak{p}}, \pi_{\mathfrak{p}} \rho'_{\emptyset}(\nabla)) = 0$  for all  $\mathfrak{p} \in S$ , proving the claim.  $\square$

From Proposition 2.2 and the discussion above it we get:

**Corollary 2.3.** *Let  $\pi : E \rightarrow \text{Gal}(L/K)$  be an embedding problem with solution  $\phi$ . Fix solutions  $\psi^{(\mathfrak{p})}$  for  $\pi_{\mathfrak{p}}$  at all primes  $\mathfrak{p}$  in a finite set  $S$  and let  $T$  be a finite set of primes disjoint from  $S$ . Assume that at least one of conditions (a),(b),(c) or (e) hold for  $S$ .*

*Then there exists a solution  $\psi$  such that  $\psi_{\mathfrak{p}} = \psi^{(\mathfrak{p})}$  for all  $\mathfrak{p} \in S$  and  $\psi_{\mathfrak{p}} = \phi_{\mathfrak{p}}$  for all  $\mathfrak{p} \in T$ .*

*Proof.* Since conditions (c) and (e) are independent of  $S$ , the image of  $\rho_{S \cup T}$  contains  $\prod_{\mathfrak{p} \in S} H^1(G_{K_{\mathfrak{p}}}, A) \times \prod_{\mathfrak{p} \in T} \{0\}$  under these conditions as well. For  $\mathfrak{p} \in S$ , let  $\chi^{(\mathfrak{p})} \in H^1(G_{K_{\mathfrak{p}}}, A)$  be the element for which  $\psi^{(\mathfrak{p})} = \chi^{(\mathfrak{p})} \cdot \psi_{\mathfrak{p}}$ . By Proposition 2.2, the element  $(\chi^{(\mathfrak{p})})_{\mathfrak{p} \in S} \times (0)_{\mathfrak{p} \in T}$  has a source  $\chi \in H^1(G_K, A)$  under the map  $\rho_{S \cup T}$ . Then the solution  $\psi := \chi \cdot \phi$  restricts to  $\chi^{(\mathfrak{p})} \cdot \phi_{\mathfrak{p}} = \psi^{(\mathfrak{p})}$  at all  $\mathfrak{p} \in S$  and to  $0 \cdot \phi_{\mathfrak{p}} = \phi_{\mathfrak{p}}$  at all  $\mathfrak{p} \in T$ .  $\square$

*Remark 2.4.* (1) Proposition 2.2 need not hold under conditions (d) or (f). For example, let  $K$  be a quadratic extension of  $\mathbb{Q}$  in which 2 splits and let  $\mathfrak{p}_1, \mathfrak{p}_2$  be the primes above it. Let  $S = \{\mathfrak{p}_1\}$ ,  $T = \{\mathfrak{p}_2\}$  and let  $A = \mathbb{Z}/8$  be the trivial  $G_K$ -module. Then  $A' \cong \mu_8$  as  $G_K$ -modules and  $K(A') = K(\mu_8)$ . Both conditions (d) and (f) hold for  $S$  and hence  $\rho_S$  is surjective.

However, since  $K(A')_{\mathfrak{p}}/K_{\mathfrak{p}}$  is cyclic for all  $\mathfrak{p} \neq \mathfrak{p}_1, \mathfrak{p}_2$ , conditions (d) and (f) fail for  $S \cup T$ . Furthermore, the Grunwald-Wang theorem shows that

$$\prod_{\mathfrak{p} \in S} H^1(G_{K_{\mathfrak{p}}}, A) \times \prod_{\mathfrak{p} \in T} \{0\} \not\subseteq \text{Im } \rho_{S \cup T}.$$

Indeed, letting  $\psi^{(\mathfrak{p}_2)} = 0$  and  $\psi^{(\mathfrak{p}_1)} \in \text{Hom}(G_{K_{\mathfrak{p}_1}}, A)$  be such that the fixed field of  $\ker(\psi^{(\mathfrak{p}_1)})$  is the unramified  $\mathbb{Z}/8$ -extension of  $K$ , [2, Chp. X, Theorem 5] shows that  $(\psi^{(\mathfrak{p}_1)}, \psi^{(\mathfrak{p}_2)}) \notin \text{Im}(\rho_{S \cup T})$ .

(2) Let  $A$  be a trivial  $G_K$ -module of exponent  $2^t m'$  where  $m'$  is odd. If  $K(\mu_{2^t})/K$  is cyclic then condition (f) holds for all finite sets  $S$ .

**2.2. Tame Galois groups of local fields.** We shall make use of a few well known facts about Galois groups of tame local extensions, all of which can be found in [26] and [19, Chp. VII, §5]. Let  $L/K$  a tamely ramified  $G$ -extension of  $p$ -adic fields,  $I$  its inertia group,  $n := |I|$ , and  $q$  the cardinality of the residue field of  $K$ .

The subfield  $L^I$  contains  $\mu_n$  and  $L/L^I$  is a (cyclic) Kummer extension. The Galois group of  $L^I/K$  is generated by the Frobenius automorphism  $\sigma_L$  which acts on  $\mu_n$  by raising each element to the power  $q$ . In particular the restriction of  $\sigma_L$  to  $\mathbb{Q}(\mu_n)$  is  $\sigma_{q,n}$  and fixes  $\mathbb{Q}(\mu_n) \cap K$ . The action of  $\sigma$  on  $I$  via conjugation in  $G$  is equivalent to its action on  $\mu_n$ . Thus,

$$G = \mathcal{M}(m, n, i, t) = \langle x, y \mid x^m = y^i, y^n = 1, x^{-1}yx = y^t \rangle,$$

where  $t \equiv q \pmod{n}$ ,  $I = \langle y \rangle$  and  $x = \sigma \pmod{I}$ . In particular, one has the following observation which is the basis to [14, Theorem 28]:

**Lemma 2.5.** *Let  $p, l$  be two distinct rational primes and  $K$  a  $p$ -adic field. Then every group  $G$  that appears as a Galois group over  $K$  has a metacyclic  $l$ -Sylow subgroup  $\mathcal{M}(m, n, i, t)$  such that  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$ .*

*Proof.* Let  $L/K$  be a  $G$ -extension,  $M$  the fixed subfield of an  $l$ -Sylow subgroup  $H$  of  $G$  and  $t$  the cardinality of the residue field of  $M$ . Then  $H \cong \mathcal{M}(m, n, i, t)$  and  $\sigma_{t,n}$  fixes  $M \cap \mathbb{Q}(\mu_n)$ . In particular  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$ .  $\square$

Consider the converse problem of realizing  $\mathcal{M}(m, n, i, t)$  over  $K$  and assume  $t \equiv q \pmod{n}$  so that  $\mathcal{M}(m, n, i, t) = \mathcal{M}(m, n, i, q)$ . The Galois group  $G_K^{tr}$  of the maximal tamely ramified extension of  $K$  is profinitely generated by two automorphisms  $\sigma$  and  $\tau$  and one relation  $\sigma^{-1}\tau\sigma = \tau^q$ , where  $\tau$  is of order prime to  $q$  and  $\sigma$  is the Frobenius automorphism. Letting  $M$  be the (unique) unramified degree  $m$  extension of  $K$ ,  $\sigma$  restricts to the Frobenius automorphism of  $M/K$ . Thus, an embedding problem  $\pi : \mathcal{M}(m, n, i, t) \rightarrow \text{Gal}(M/K)$  with kernel  $\langle y \rangle$  has a surjective solution whose corresponding field is a tamely ramified  $\mathcal{M}(m, n, i, t)$ -extension of  $K$ .

### 3. GALOIS GROUPS OF TAMELY RAMIFIED ADEQUATE EXTENSIONS

**3.1. Proof of Theorem 1.3.** We consider a refined notion of adequacy. For a number field  $K$  and a finite set  $S$  of primes of  $K$ , we say that  $L/K$  is  $S$ -adequate if  $L$  is a maximal subfield of a  $K$ -division algebra that is unramified outside  $S$ . Let  $D(L/K, \mathfrak{P})$  denote the decomposition group of a prime  $\mathfrak{P}$  of  $L$ . The same proof as of Schacher's criterion ([21, Proposition 2.6]) gives the following criterion for  $S$ -adequacy:

**Proposition 3.1.** *Let  $L/K$  be a  $G$ -extension of number fields and  $S$  a finite set of primes of  $K$ . Then  $L/K$  is  $S$ -adequate if and only if for every rational prime  $l \mid |G|$ , there are two primes  $\mathfrak{p}_1, \mathfrak{p}_2 \in S$  for which  $D(L/K, \mathfrak{P}_i)$  contains an  $l$ -Sylow subgroup of  $G$ , where  $\mathfrak{P}_i$  is a prime of  $L$  which divides  $\mathfrak{p}_i$ ,  $i = 1, 2$ .*

Note that the condition of containing an  $l$ -Sylow subgroup of  $G$  is independent of the choice of prime  $\mathfrak{P}_i$  dividing  $\mathfrak{p}_i$ .

A key ingredient in our proof of Theorem 1.3 is the following generalization of Sonn's theorem ([24, Theorem 1]) which asserts the existence of  $S$ -adequate  $G$ -extensions for prescribed sets  $S$ . Since  $\mathcal{M}(m, n, i, t)$  is realizable over  $\mathbb{Q}_p$  when  $p \equiv t \pmod{n}$  (see Section 2.2), we consider the following sets  $S$ :

**Definition 3.2.** We call a set  $S$  of distinct odd rational primes  $p_i^{(l)}, i = 1, 2, l \mid |G|$  which are prime to  $|G|$ , a *tame supporting set for  $G$*  if for every  $l \mid |G|$ , the  $l$ -Sylow subgroups of  $G$  admit a presentation  $\mathcal{M}(m, n, i, t)$  such that  $p_1^{(l)}, p_2^{(l)} \equiv t \pmod{n}$ .

**Theorem 3.3.** *Let  $G$  be a solvable group with metacyclic Sylow subgroups. Let  $S$  be a tame supporting set for  $G$  and  $T$  a finite set of rational primes which is disjoint from  $S$ . Then there exists an  $S$ -adequate  $G$ -extension  $L/\mathbb{Q}$  in which the primes of  $T$  split completely.*

The proof of this theorem is based on Corollary 2.3 and on Sonn's proof of [24], and is given in Section 4. We now use this theorem to prove Theorem 1.3:

*Proof of Theorem 1.3.* “Only if part”: Let  $l$  be a prime that divides  $|G|$ . By Proposition 3.1, there is a prime  $\mathfrak{p}$  of  $K$  such that  $D(L/K, \mathfrak{P}), \mathfrak{P} \mid \mathfrak{p}$ , contains an  $l$ -Sylow subgroup  $P$  of  $G$ . If  $\mathfrak{p} \mid l$ ,  $\mathfrak{p}$  is unramified in  $L$  and hence  $P$  is cyclic. Otherwise, Lemma 2.5 implies that  $P$  has a presentation  $\mathcal{M}(m, n, i, t)$  such that  $\sigma_{t,n}$  fixes  $K_{\mathfrak{p}} \cap \mathbb{Q}(\mu_n)$  and hence  $K \cap \mathbb{Q}(\mu_n)$ . In both cases,  $P$  has the required presentation.

“If part”: Let  $l \mid |G|$  be a rational prime and let  $P^{(l)}$  be the set of primes of  $K$  that are unramified over  $\mathbb{Q}$  with residue degree 1, and whose restriction  $p$  to  $\mathbb{Q}$  satisfies  $p \equiv t_l \pmod{n_l}$ .

We first claim that  $P^{(l)}$  is infinite. Let  $M$  be the  $\mathbb{Q}$ -normal closure of  $K$ . Since  $\sigma_{t_l, n_l}$  fixes  $K \cap \mathbb{Q}(\mu_{n_l})$ ,  $\sigma_{t_l, n_l}$  extends to an automorphism of  $K(\mu_{n_l})$  that fixes  $K$  and hence lifts to an automorphism  $\tau_l \in \text{Gal}(M(\mu_{n_l})/K)$ . By Chebotarev's density theorem there are infinitely many primes  $\mathfrak{P}$  of  $M(\mu_{n_l})$  that are unramified over  $\mathbb{Q}$ , and whose Frobenius automorphism in  $M(\mu_{n_l})/\mathbb{Q}$  is  $\tau_l$ . In particular, the restriction  $p$  of such  $\mathfrak{P}$  to  $\mathbb{Q}$  has Frobenius  $\sigma_{t_l, n_l}$  in  $\mathbb{Q}(\mu_{n_l})/\mathbb{Q}$ , and hence  $p \equiv t_l \pmod{n_l}$ . Since  $\tau_l$  fixes  $K$ , the restriction of each such  $\mathfrak{P}$  to  $K$  has residue degree 1 over  $\mathbb{Q}$  and hence is in  $P^{(l)}$ , proving the claim.

Since  $P^{(l)}$  is infinite, we can choose two primes  $\mathfrak{p}_1^{(l)}, \mathfrak{p}_2^{(l)} \in P^{(l)}$  such that the restrictions  $p_i^{(l)}$  of  $\mathfrak{p}_i^{(l)}$  to  $\mathbb{Q}$ ,  $i = 1, 2, l \mid |G|$ , are all distinct rational primes which are prime to  $|G|$ . Thus, the set  $S := \{p_i^{(l)} \mid i = 1, 2, l \mid |G|\}$  is a tame supporting set for  $G$  and by Theorem 3.3 there exists an  $S$ -adequate  $G$ -extension  $L/\mathbb{Q}$  in which all of the primes  $l$  dividing  $|G|$  split completely.

We claim that  $N := LK$  is an adequate extension of  $K$ . This proves the theorem since  $L/\mathbb{Q}$  and hence  $N/K$  is tamely ramified. Since  $\mathfrak{p}_i^{(l)}$



has residue degree 1 over  $\mathbb{Q}$ , we have  $K_{\mathfrak{p}_i^{(l)}} \cong \mathbb{Q}_{p_i}$  and hence:

$$(3.1) \quad [N_{\mathfrak{P}_i^{(l)}} : K_{\mathfrak{p}_i^{(l)}}] = [L_{\mathfrak{P}_i^{(l)} \cap L} : \mathbb{Q}_{p_i^{(l)}}] \text{ for } \mathfrak{P}_i^{(l)} \mid \mathfrak{p}_i^{(l)}, i = 1, 2, l \mid |G|.$$

Letting  $l^{\alpha_i}$  be the maximal power of  $l$  dividing  $|G|$ , (3.1) shows that  $l^{\alpha_i} \mid [N : K]$  for every  $l \mid |G|$  and hence that  $\text{Gal}(N/K) \cong G$ . Furthermore, (3.1) shows that  $D(\mathfrak{P}_i^{(l)}, N/K)$  contains an  $l$ -Sylow subgroup of  $G$  for  $i = 1, 2, l \mid |G|$ , showing that  $N/K$  is adequate, as required.  $\square$

*Remark 3.4.* (1) In [14], Liedahl uses Lemma 2.5, similarly to the “only if part” of Theorem 1.3, to show that under the assumption that  $l$  does not decompose in  $K$ , the  $l$ -Sylow subgroups of a  $K$ -admissible group admit a presentation  $\mathcal{M}(m, n, i, t)$  such that  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$ . He also uses the flexibility of [23, Theorem 1] to prove that if  $G$  itself has a presentation  $\mathcal{M}(m, n, i, t)$  such that  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$ , then  $G$  is  $K$ -admissible.

(2) Note that the proof of the “only if part” of Theorem 1.3 applies more generally without the assumption that  $G$  is solvable.

(3) The proof of Theorem 3.3 gives furthermore that  $l^{\alpha_i} \mid [L_{\mathfrak{P}_i^{(l)} \cap L} : \mathbb{Q}_{p_i^{(l)}}]$  for all  $l \mid |G|, i = 1, 2$ .

**3.2. Consequences.** For solvable groups  $G$  we get the following characterization of  $K$ -admissibility under the assumption that every  $l \mid |G|$  does not decompose in  $K$ :

**Corollary 3.5.** *Let  $K$  be a number field and  $G$  a solvable group. Assume that every prime  $l$  that divides  $|G|$  does not decompose in  $K$ . Then the following conditions are equivalent:*

- (1) *There exists a tamely ramified  $K$ -adequate  $G$ -extension;*
- (2)  *$G$  is  $K$ -admissible;*
- (3) *for every  $l \mid |G|$ , the  $l$ -Sylow subgroups of  $G$  admit a presentation  $\mathcal{M}(m, n, i, t)$  such that  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$ .*

*Proof.* The implication (1)  $\Rightarrow$  (2) is immediate and (2)  $\Rightarrow$  (3) follows from Remark 3.4 ([14, Theorem 28]). The implication (3)  $\Rightarrow$  (1) is the “if part” of Theorem 1.3.  $\square$

Recall that a group  $G$  is called *infinitely often  $K$ -admissible* if there exist infinitely many adequate  $G$ -extensions  $L_i/K$ ,  $i \in \mathbb{N}$ , such that  $L_{r+1} \cap (L_1 \cdots L_r) = K$  (cf. [1]).

**Corollary 3.6.** *Let  $K$  be a number field and  $G$  a solvable group such that for every  $l \mid |G|$ , the  $l$ -Sylow subgroups admit a presentation  $\mathcal{M}(m, n, i, t)$  such that  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$ . Then  $G$  is infinitely often  $K$ -admissible.*

*Furthermore, there exists a  $K$ -division algebra  $D$  that has infinitely many disjoint maximal subfields  $L_i, i \in \mathbb{N}$ , such that  $\text{Gal}(L_i/K) \cong G$ .*

The following lemma is useful in the proof of Theorem 3.3 and is used here to prove Corollary 3.6. Given a Galois extension  $N/\mathbb{Q}$ , define the following condition on a finite set of rational primes  $T$ :

( $A_N$ ) The decomposition groups  $D(N/\mathbb{Q}, \mathfrak{p}), p \in T, \mathfrak{p} | p$ , generate  $\text{Gal}(N/\mathbb{Q})$ .

**Lemma 3.7.** *Assume  $T$  satisfies ( $A_N$ ). Then every finite extension  $K/\mathbb{Q}$  in which the primes of  $T$  split completely is disjoint from  $N$ .*

*Proof.* Let  $H := \text{Gal}(N/N \cap K)$  and assume on the contrary that  $H \neq G$ . By condition ( $A_N$ ) there exists a prime  $p \in T$  and  $\mathfrak{p} | p$  such that  $D := D(N/\mathbb{Q}, \mathfrak{p}) \not\subseteq H$ . In particular,  $[N_{\mathfrak{p}} : K_{\mathfrak{p} \cap K}] = |D \cap H| < |D| = [N_{\mathfrak{p}} : \mathbb{Q}_p]$  and hence  $[K_{\mathfrak{p} \cap K} : \mathbb{Q}_p] > 1$  contradicting the assumption that  $p$  splits completely in  $K$ .  $\square$

Note that by Chebotarev's density theorem for every cyclic subgroup  $C \leq G$  there are infinitely many primes  $\mathfrak{p}$  of  $N$  for which  $D(N/\mathbb{Q}, \mathfrak{p}) = C$ . Thus, we can always choose a finite set  $T$  which satisfies ( $A_N$ ).

*Proof of Corollary 3.6.* Let  $S$  and  $l^{\alpha_i}$  be as in the proof of Theorem 1.3. Define  $D := D_0 \otimes_{\mathbb{Q}} K$  where  $D_0$  is the  $\mathbb{Q}$ -division algebra with Hasse invariants  $1/l^{\alpha_i}$  at  $p_1^{(l)}$ ,  $-1/l^{\alpha_i}$  at  $p_2^{(l)}$  for  $l | |G|$ , and 0 at all other primes.

It suffices to show that given  $r$  disjoint  $G$ -extensions  $L_1, \dots, L_r$  of  $K$  which are maximal subfields of  $D$  there exists a maximal subfield  $L_{r+1}$  of  $D$  such that  $\text{Gal}(L_{r+1}/K) = G$  and  $L_{r+1} \cap (L_1 \cdots L_r) = K$ .

Let  $M$  be the  $\mathbb{Q}$ -normal closure of  $K$  and  $N := L_1 \cdots L_r M$ . Let  $T$  be a finite set which is disjoint from  $S$ , contains all primes  $l | |G|$ , and for which condition ( $A_N$ ) holds.

As remarked in 3.4.(3), Theorem 3.3 gives a maximal subfield  $L$  of  $D_0$  in which the primes of  $T$  split completely. By Lemma 3.7,  $L \cap N = \mathbb{Q}$  and hence  $L_{r+1} := LK$  is a  $G$ -extension of  $K$  and  $L_{r+1} \cap (L_1 \cdots L_r) = K$ . Since in addition  $L_{r+1}$  splits  $D$ ,  $L_{r+1}$  is a maximal subfield of  $D$ .  $\square$

#### 4. PROOF OF THEOREM 3.3

In this section we prove Theorem 3.3. In Sections 4.1 and 4.2 we treat the cases of 2-groups and  $\{2, 3\}$ -groups (groups of order  $2^a 3^b$ ), respectively. We first show how the theorem follows from the latter case.

As in Section 2, we fix an embedding of an algebraic closure of  $\mathbb{Q}$  into an algebraic closure of each of its completions. We shall say that a set of primes  $T$  *splits completely* in  $L$  if every prime in  $T$  splits completely in  $L$ .

*Proof of Theorem 3.3.* Let  $n = |G|$ . By [3, Lemma 1.4], there is a normal subgroup  $N \triangleleft G$  of order prime to 2 and 3 and a  $\{2, 3\}$ -subgroup  $H$  such that  $G = NH$ .

Extend  $T$  to a finite set  $T_0$  disjoint from  $S$  which satisfies condition ( $A_{\mathbb{Q}(\mu_n)}$ ). By the case of  $\{2, 3\}$ -groups (Section 4.2), there exists a  $\{p_1^{(2)}, p_2^{(2)}, p_1^{(3)}, p_2^{(3)}\}$ -adequate  $H$ -extension  $K/\mathbb{Q}$  in which  $T_0 \cup \{p_1^{(l)}, p_2^{(l)} | l > 3\}$  splits completely. Since by Lemma 3.7,  $K \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$ ,

and since the embedding problem  $G \rightarrow \text{Gal}(K/\mathbb{Q})$  splits, we may apply [17]. It follows that  $K/\mathbb{Q}$  embeds into a  $G$ -extension  $L/\mathbb{Q}$  such that  $T$  splits completely in  $L$  and  $\text{Gal}(L_{p_i^{(l)}}/\mathbb{Q}_{p_i^{(l)}})$ ,  $i = 1, 2$ , is an  $l$ -Sylow subgroup of  $N$  for all  $l \mid |N|$ . In particular,  $L/\mathbb{Q}$  is an  $S$ -adequate  $G$ -extension in which  $T$  splits completely, as required.  $\square$

**4.1. 2-groups.** The  $\mathbb{Q}$ -admissibility of metacyclic 2-group was proved in [23] using Theorem 2.1. We use Corollary 2.2 in order to prove Theorem 3.3 for 2-groups, generalizing [23]:

*Proof of Theorem 3.3 for 2-groups.* Let  $G$  be a metacyclic 2-group with presentation  $G \cong \mathcal{M}(m, n, i, t)$  such that  $\sigma_{t,n}$  fixes  $K \cap \mathbb{Q}(\mu_n)$ , and let  $k$  be the order of  $x$  in  $G$ . Let  $S = \{p_1, p_2\}$  be a tame supporting set for  $G$  such that  $p_i \equiv t \pmod{n}$ ,  $i = 1, 2$ .

Since  $S$  consists of odd primes, the Grunwald-Wang theorem (see Theorem 2.1.(f)) implies that there exists a  $\mathbb{Z}/k$ -extension  $\hat{K}/\mathbb{Q}$  in which the primes of  $S$  are inert and  $T$  splits completely. We identify  $\text{Gal}(\hat{K}/\mathbb{Q})$  with  $\langle x \rangle$  and let  $K/\mathbb{Q}$  be the unique  $\mathbb{Z}/m$ -extension inside  $\hat{K}$ . The embedding problem  $\pi : G \rightarrow \text{Gal}(K/\mathbb{Q})$  with kernel  $A := \langle y \rangle$  has a solution  $\phi : G_{\mathbb{Q}} \rightarrow \langle x \rangle \subseteq G$  which is given by the restriction map to  $\text{Gal}(\hat{K}/\mathbb{Q})$ .

Let  $\pi_i : G \rightarrow \text{Gal}(K_{p_i}/\mathbb{Q}_{p_i})$  be the corresponding local embedding problem at  $p_i$ ,  $i = 1, 2$ . Since  $p_i \equiv t \pmod{n}$ ,  $\pi_i$  has a surjective solution  $\psi^{(i)} : G_{\mathbb{Q}_{p_i}} \rightarrow G$  whose fixed field  $L^{(i)}$  is totally ramified over  $K_{p_i}$  and in particular  $\mu_n \subseteq K_{p_i}$ , for  $i = 1, 2$  (see Section 2.2).

In order to change  $\phi$  to a solution with the desired properties, we apply Corollary 2.3. Let  $A' = \text{Hom}(A, \mu_n)$  be the dual  $G_{\mathbb{Q}}$ -module,  $K' := \mathbb{Q}(A')$ ,  $G' = \text{Gal}(K'/\mathbb{Q})$  and  $G'_{p_i} := \text{Gal}(K'_{p_i}/\mathbb{Q}_{p_i})$ ,  $i = 1, 2$ . Since every automorphism in  $G_{\mathbb{Q}}$  that fixes  $A$  and  $\mu_n$  also fixes  $A'$ , we have  $K' \subseteq K(\mu_n)$  and hence  $K'_{p_i} \subseteq K_{p_i}(\mu_n) = K_{p_i}$ , for  $i = 1, 2$ . Thus,  $G'_{p_i}$  is cyclic and condition 2.1.(b) holds. By Corollary 2.3, there exists a solution  $\psi : G_{\mathbb{Q}} \rightarrow G$  of  $\pi$ , whose restriction at  $p_i$  is  $\psi^{(i)}$ ,  $i = 1, 2$ , and the restriction remains the trivial solution at each  $p \in T$ . Since  $\psi^{(1)}, \psi^{(2)}$  are surjective,  $\psi$  is also surjective. Thus, the fixed field  $L$  of  $\ker \psi$  is an  $S$ -adequate  $G$ -extension of  $\mathbb{Q}$  in which  $T$  splits completely, as required.  $\square$

*Remark 4.1.* Note that we use Corollary 2.2 since Theorem 2.1 cannot be applied for the set  $S \cup T$ . In fact, the Grunwald-Wang theorem shows that the map  $\rho_{S \cup T}$  need not be surjective if  $2 \in T$ .

**4.2.  $\{2, 3\}$ -groups.** Let  $G$  be a  $\{2, 3\}$ -group and  $G(3)$  a 3-Sylow subgroup of  $G$ . If  $G(3)$  is normal in  $G$  then Theorem 3.3 essentially follows from the 2-groups case by applying [17]:

*Proof of Theorem 3.3 for  $\{2, 3\}$ -groups when  $G(3) \triangleleft G$ .*

Let  $S = \{p_1^{(2)}, p_2^{(2)}, p_1^{(3)}, p_2^{(3)}\}$  be a tame supporting set for  $G$ . Extend  $T$  to a finite set  $T_0$  disjoint from  $S$  which satisfies condition  $(A_{\mathbb{Q}(\mu_n)})$  where  $n = |G|$ .

As shown in Section 4.1, there exists a  $\{p_1^{(2)}, p_2^{(2)}\}$ -adequate  $G/G(3)$ -extension  $M/\mathbb{Q}$  in which  $T_0 \cup \{p_1^{(3)}, p_2^{(3)}\}$  splits completely.

The embedding problem  $G \rightarrow \text{Gal}(M/\mathbb{Q})$  splits and by Lemma 3.7,  $M \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$ . Thus, we may apply [17] and embed  $M/\mathbb{Q}$  into a  $G$ -extension  $L/\mathbb{Q}$  such that  $T$  splits completely in  $L$  and

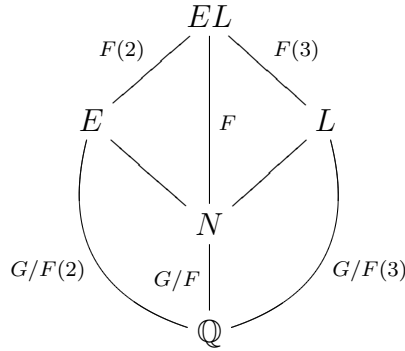
$$\text{Gal}(L_{p_i^{(3)}}/\mathbb{Q}_{p_i^{(3)}}) \cong G(3) \text{ for } i = 1, 2.$$

Therefore  $L/\mathbb{Q}$  is an  $S$ -adequate  $G$ -extension in which  $T$  splits completely, as required.  $\square$

For  $\{2, 3\}$ -groups  $G$  that do not have a normal 3-Sylow subgroup, we show that the proof of [24, Theorem 1] can be adjusted to give Theorem 3.3.

Let  $F = F(G)$  denote the Fitting subgroup of  $G$  and  $F(2)$  and  $F(3)$  its 2-Sylow and 3-Sylow subgroups, respectively. The approach of [24] is to construct an adequate  $G/F$ -extension  $N/\mathbb{Q}$  and embed it into an adequate  $G/F(2)$ -extension  $E/\mathbb{Q}$  and an adequate  $G/F(3)$ -extension  $L/\mathbb{Q}$ . Since  $[EL : L]$  and  $[EL : E]$  are coprime, the compositum  $EL$  is an adequate  $G$ -extension of  $\mathbb{Q}$ .

(4.1)



When  $G(3)$  is not a normal subgroup of  $G$ , [24] shows that  $G/F$  is isomorphic either to (1)  $S_3$  or to (2)  $\mathbb{Z}/3$  and that in these cases we have the following partition into subcases:

Case	$G/F$	$F(2)$	$G/F(3)$	2-Sylow
1.1	$\mathbb{Z}/3$	$\mathbb{Z}/2^u \times \mathbb{Z}/2^u$	$\mathbb{Z}/3 \ltimes (\mathbb{Z}/2^u \times \mathbb{Z}/2^u)$	$\mathbb{Z}/2^u \times \mathbb{Z}/2^u$
1.2	$\mathbb{Z}/3$	$Q_8$	$\text{SL}_2(3)$	$Q_8$
2.1	$S_3$	$\mathbb{Z}/2 \times \mathbb{Z}/2$	$S_4$	$D_8$
2.2	$S_3$	$Q_8$	$S_4^*$ or $S_4^{**}$	$Q_{16}$ or $D_{16}^*$

Here  $Q_8$  is the quaternions group,  $D_8$  the dihedral group of order 8,  $S_4^*$  and  $S_4^{**}$  are the two central extensions of  $S_4$  with kernel  $\mathbb{Z}/2$ , and

$$\begin{aligned} Q_{16} &= \langle x, y | x^2 = y^4, y^8 = 1, x^{-1}yx = y^7 \rangle, \\ D_{16}^* &= \langle x, y | x^2 = y^8 = 1, x^{-1}yx = y^3 \rangle \end{aligned}$$

are their 2-Sylow subgroups, respectively.

In all of the above cases the 2-Sylow subgroups have unique parameters  $m, n$  and  $t$ <sup>2</sup>.

**Lemma 4.2.** *Let  $G \cong \mathcal{M}(m, n, i, t)$ .*

- (a) *If  $G \cong \mathbb{Z}/2^u \times \mathbb{Z}/2^u$  then  $m = 2^u, n = 2^u, t = 1$ .*
- (b) *If  $G \cong Q_8$  then  $m = 2, n = 4, t = 3$ .*
- (c) *If  $G \cong D_8$  then  $m = 2, n = 4, t = 3$ .*
- (d) *If  $G \cong D_{16}^*$  then  $m = 2, n = 8, t = 3$ .*
- (e) *If  $G \cong Q_{16}$  then  $m = 2, n = 8, t = 7$ .*

*Proof.* (1) Let  $x, y$  be the generators of a presentation  $\mathcal{M}(m, n, i, t)$ . Since  $m, n | 2^u$  and  $mn = |G| = 2^{2u}$ , one has  $m = n = 2^u$ . For  $1 < t < 2^u$  the group  $\mathcal{M}(2^u, 2^u, i, t)$  is non-abelian and hence  $t = 1$ .

(b)–(e) are conclusions from [14, Theorem 22, Case 3]. In this theorem, Liedahl gives necessary and sufficient conditions on a presentation  $\mathcal{M}(m, n, i, t)$  of a group as in (b)–(e) to have an equivalent presentation with other parameters. However, these conditions require  $m \geq 4$ <sup>3</sup> which fails for the presentations in (b)–(e).  $\square$

*Proof of Theorem 3.3 for  $\{2, 3\}$ -groups when  $G(3)$  is not normal.*

We claim that the fields  $N, L, E$  in diagram (4.1) can be in fact chosen to be  $S$ -adequate extensions of  $\mathbb{Q}$  in which  $T$  splits completely. This will imply that  $EL/\mathbb{Q}$  is an  $S$ -adequate  $G$ -extension in which  $T$  splits completely, as required.

We first construct the field  $E$  and let  $N = E^{F/(F(2))}$ .

In Case (1),  $G/F(2) \cong G(3)$  is of odd order and therefore [17] gives a  $\{p_1^{(3)}, p_2^{(3)}\}$ -adequate  $G(3)$ -extension  $E/\mathbb{Q}$  in which  $T \cup \{p_1^{(2)}, p_2^{(2)}\}$  splits completely.

In Case (2), let  $q \equiv 1 \pmod{8}$  be a prime which is not in  $S \cup T$  and such that  $p_1^{(2)} p_2^{(2)} q \equiv 1 \pmod{p}$  for all  $p \in T_0 \cup \{p_1^{(3)}, p_2^{(3)}\}$ . Let  $k = \mathbb{Q}(\sqrt{p_1^{(2)} p_2^{(2)} q})$  and let  $\mathfrak{q}$  be the prime of  $k$  which lies above  $q$ . Note that  $k$  is  $\{p_1^{(2)}, p_2^{(2)}\}$ -adequate and  $T$  splits completely in  $k$ . Since the embedding problem  $G/F(2) \rightarrow \text{Gal}(k/\mathbb{Q})$  splits, we may apply [17] and embed  $k$  into an  $S$ -adequate  $G/F(2)$ -extension  $E/\mathbb{Q}$  in which  $T$  and  $\mathfrak{q}$  split completely. In both Cases (1) and (2),  $E/\mathbb{Q}$  is  $S$ -adequate and  $T$  splits completely in  $E$ .

The construction of the field  $L$  is the same as in [24] with few modifications. Since the construction in [24] is involved and long, we do not

<sup>2</sup>The parameter  $i$  is also unique up to multiplication by an odd number.

<sup>3</sup>Note that our  $m$  is denoted as  $2^m$  in the notation of [14].

repeat it here. A self contained version of the modified construction can be found in the author's thesis ([15]). For the reader to whom [24] is available, we give below the list of required modifications.

Note that our field  $N$  was denoted in Case (1) of [24] by  $k$  and in Case (2) by  $K$ .

- (1) Replace the primes  $p_1, p_2$  (resp.  $p, q$ ) in Case (1) (resp. Case (2)) of [24] by the primes  $p_1^{(2)}, p_2^{(2)}$ , respectively. Since  $S$  is a supporting set, Lemma 4.2 implies that the prime  $p_1^{(2)}, p_2^{(2)}$  satisfy the congruence relations required in [24] from  $p_1, p_2, p, q$ . Note that in Case (1), the primes  $p_1^{(2)}, p_2^{(2)}$  split completely in  $N(\mu_n)$  as required in [24]. Also note that since  $p_1^{(2)}, p_2^{(2)}$  are prime to  $|G|$ , they are greater than 3 as required in Case (2) of [24].
- (2) In Case (2), we add the prime  $\mathfrak{q}$  to the modulus  $\mathfrak{m}$  and require that the element  $\gamma$  is congruent to 1 mod  $\mathfrak{q}$ . The field  $M$  constructed in [24] then satisfies  $\text{Gal}(M_q/\mathbb{Q}_q) \cong \mathbb{Z}/2\mathbb{Z}$ . Since  $q \equiv 1 \pmod{8}$ ,  $\text{Gal}(M_q/\mathbb{Q}_q)$  can be embedded into a  $\mathbb{Z}/4\mathbb{Z}$  extension and therefore the embedding problem  $G/(F(3)) \rightarrow \text{Gal}(M/\mathbb{Q})$  is solvable at  $q$  as well. As shown in [24] it is solvable at all other primes and hence globally solvable.

With these changes the field  $L$  constructed in [24] gives an  $S$ -adequate  $G/F(3)$ -extension. In order to make the set  $T$  split completely in  $L$ , we make the following additional modifications:

- (1) In Case (1.1), the embedding problem  $G/(F(3)) \rightarrow \text{Gal}(N/\mathbb{Q})$  splits and hence has the trivial solution  $\phi$ . Instead of applying Theorem 2.1, we apply Corollary 2.3 insuring the same prescribed conditions at  $S$  but in addition that the solution remains trivial at primes of  $T$ .
- (2) In Cases (1.2) and (2), we add the primes of  $N$  that lie over primes of  $T$  to the modulus  $\mathfrak{m}$  and require that  $\gamma \equiv 1 \pmod{\mathfrak{p}}$  for every  $\mathfrak{p} \cap \mathbb{Q} \in T$ . This insures that  $T$  splits completely in  $K$  (resp. in  $M$ ) in Case (1.2) (resp. Case (2)).

Let  $\phi$  be the solution obtained in Case (1.2) (resp. Case (2)) of [24] to the embedding problem  $G/F(3) \rightarrow \text{Gal}(K/\mathbb{Q})$  (resp.  $G/F(3) \rightarrow \text{Gal}(M/\mathbb{Q})$ ). We apply Theorem 2.1 in order to change  $\phi$  to a solution  $\psi$  which is trivial at primes of  $T$ . Since the local embedding problem at  $p_i^{(2)}$  is Frattini,  $\psi$  is surjective at  $p_i^{(2)}$ ,  $i = 1, 2$ . Thus, the fixed field  $L$  of  $\ker \psi$  is  $S$ -adequate and  $T$  splits completely in  $L$ .

□

## REFERENCES

- [1] E. ALLMAN, M. SCHACHER, Division algebras with  $PSL(2, q)$ -Galois maximal subfields. *J. Algebra* **240** (2001), 808–821.
- [2] E. ARTIN, J. TATE, Class field theory. Addison-Wesley Publishing Company, Redwood City, CA (1990).
- [3] D. CHILLAG, J. SONN, Sylow-metacyclic groups and  $\mathbb{Q}$ -admissibility. *Israel J. Math.* **40** (1981), 307–323.
- [4] B. FEIN, M. SCHACHER,  $\mathbb{Q}$ -admissibility questions for alternating groups. *J. Algebra* **142** (1991), 360–382.
- [5] W. FEIT,  $SL(2, 11)$  is  $\mathbb{Q}$ -admissible. *J. Algebra* **257** (2002), 244–248.
- [6] W. FEIT, The  $\mathbb{Q}$ -admissibility of  $2A_6$  and  $2A_7$ . Algebraic geometry and its applications (West Lafayette, IN, 1990), Springer, New York (1994), 197–202.
- [7] W. FEIT,  $PSL_2(11)$  is admissible for all number fields. Algebra, arithmetic and geometry with applications, Springer, Berlin (2004), 295–299.
- [8] W. FEIT, The  $K$ -admissibility of  $2A_6$  and  $2A_7$ . *Israel J. Math.* **82** (1993), 141–156.
- [9] P. FEIT, W. FEIT, The  $K$ -admissibility of  $SL(2, 5)$ . *Geom. Dedicata* **36** (1990), 1–13.
- [10] W. FEIT, P. VOJTA, Examples of some  $\mathbb{Q}$ -admissible groups. *J. Number Theory* **26** (1987), 210–226.
- [11] B. GORDON, M. SCHACHER, The admissibility of  $A_5$ . *J. Number Theory* **11**, (1979), 498–504.
- [12] D. HARBATER, J. HARTMANN, Division algebras and patching. Lecture notes for the 2012 Arizona Winter School (2012).
- [13] D. HARBATER, J. HARTMANN, D. KRASHEN, Patching subfields of division algebras. *Transactions of the AMS*, **363** (2011), 3335–3349.
- [14] S. LIEDAHL, Presentations of metacyclic  $p$ -groups with applications to  $K$ -admissibility questions. *J. Algebra* **169** (1994), 965–983.
- [15] D. NEFTIN, Admissibility of finite groups over number fields. Ph.D. Thesis, Technion (2011).
- [16] D. NEFTIN, E. PARAN, Patching and admissibility over two dimensional complete local domains. *Algebra and Number theory* **4** (2010), 743–762.
- [17] J. NEUKIRCH, On solvable number fields. *Invent. Math.* **53** (1979), 135–164.
- [18] J. NEUKIRCH, Über das Einbettungsproblem der algebraischen Zahlentheorie. *Invent. Math.* **21** (1973), 59–116.
- [19] J. NEUKIRCH, A. SCHMIDT, K. WINGBERG, Cohomology of number fields. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin (2000).
- [20] R.S. PIERCE, Associative Algebras. Springer-Verlag (1982).
- [21] M. SCHACHER, Subfields of division rings. I. *J. Algebra* **9** (1968), 451–477.
- [22] M. SCHACHER, J. SONN,  $K$ -admissibility of  $A_6$  and  $A_7$ . *J. Algebra* **145** (1992), 333–338.
- [23] J. SONN, Rational division algebras as solvable crossed products. *Israel J. Math.* **37** (1980), 246–250.
- [24] J. SONN,  $\mathbb{Q}$ -admissibility of solvable groups. *J. Algebra* **84** (1983), 411–419.
- [25] B. SURENDRANATH REDDY, V. SURESH, Admissibility of groups over function fields of  $p$ -adic curves, arXiv:1201.1938.
- [26] E. WEISS, Algebraic number theory. McGraw-Hill Book Co., Inc., New York-San Francisco-Toronto-London (1963).

DEPARTMENT OF MATHEMATICS, 530 CHURCH ST., UNIVERSITY OF MICHIGAN, ANN ARBOR 48109.

*E-mail address:* `neftin@umich.edu`