Admissibility of Finite Groups over Number Fields

Danny Neftin

Admissibility of Finite Groups over Number Fields

Research Thesis

In Partial Fulfillment of the
Requirements for the
Degree of Doctor of Philosophy

Danny Neftin

Submitted to the Senate of
the Technion- Israel Institute of Technology

Iyar, 5771 Haifa May 2011

Acknowledgments

The research thesis was done under the supervision of Professor Jack Sonn in the Department of Mathematics at the Technion.

The generous financial help of the Council for Higher Education, the Pollak Foundation and the Technion is gratefully acknowledged.

I would like to thank Jack Sonn for investing infinite time and patience in guiding and teaching me. I am grateful to him for being a kind, encouraging and supportive teacher.

Special thanks to my friend Lior Bary-Soroker, for his advice and helpful comments on my writing and for many interesting conversations.

I would like to express my deepest gratitude to my wife Shifra Reif and my parents Ludmila and Shimon Neftin, for encouraging me in times of difficulty and supporting me persistently.

Related papers

The third chapter is based on the paper:
D. Neftin, *Admissibility and field relations,* to appear in Israel J. Math.

Contents

Contents (continuation)

List of Figures

Abstract

A finite group G is called K-admissible over a field K if there exists a Galois extension L/K with Galois group G such that L is a maximal subfield of division algebra with center K.

Over number fields K, Schacher presented a criterion for admissibility in the form of a realization problem (of groups as a Galois group) with prescribed local conditions. We extract these necessary local conditions and call them preadmissibility.

In Chapter 1, we shall compare admissibility to preadmissibility for various families of groups and show that often these two notions coincide. We shall use the Grunwald-Wang theorem to show that there exist only very speical examples of K-preadmissible abelian groups A that are not K-admissible and give the precise conditions on A and K under which this phenomena occurs.

Over the field of rational numbers $\mathbb{Q}$, it is conjectured that $\mathbb{Q}$-preadmissibility implies $\mathbb{Q}$-admissibility. This conjecture was proved for solvable groups by Sonn. In Chapter 2, we generalize a theorem of Liedahl and Sonn's theorem to arbitrary number fields. We define the notion of tame admissibility which explains the kind of admissibility that occurs over $\mathbb{Q}$ and in this generalization.

In Chapter 3, we discuss an arithmetic equivalence relation that is induced by admissiblity. Namely, two number fields K and L are equivalent by admissibility if they have the same admissible groups. In 1985, Sonn asked whether two number fields K and L that are equivalent by admissibility necessarily have the same degree over $\mathbb{Q}$. We provide evidence for a negative answer to this problem by constructing infinitely many pairs of number fields that have the same preadmissibile groups and the same odd order admissible groups.

List of symbols and notations

G - a finite group

K - a field

D - a finite dimensional division algebra

$\mathrm{Gal}(L/K)$ - the Galois group of a Galois extension L/K

K_v - the completion of K by a prime v

$\mathrm{inv}_v(D)$ - the Hasse invariant of D at a prime v

$\mathrm{rk}(A)$ - the minimal number of generators of a finite abelian group A

μ_n - the group of n-th roots of unity

0.1 Introduction

0.1.1 Admissibility and Preadmissibility

A division algebra D with center K is called a G-crossed product for a finite group G, if there exists a maximal subfield L of D that is Galois over K and has Galois group $\mathrm{Gal}(L/K) \cong G$. The crossed product notion is central in the theory of finite dimensional algebras. It provides an explicit description for most of the division algebras constructed so far.

We shall be interested in the following problem that arose first in 1968 from [44] and since then has been extensively studied.

Problem 0.1.1. Let K be a field. What are the groups G for which there exists a G-crossed product division algebra with center K?

If there exists a G-crossed product division algebra with center K, G is called *K-admissible*. We shall focus on the cases in which K is a number field. Over such fields we have the following criterion for admissibility.

For a prime v of K, we denote by K_v the completion of K by v.

Theorem 0.1.2. (Schacher [44]) *Let K be a number field. A finite group G is K-admissible if and only if there exists a Galois extension L/K with Galois group $\mathrm{Gal}(L/K) \cong G$ such that for every rational prime $p||G|$, there are two primes v_1, v_2 of K for which $\mathrm{Gal}(L_{w_i}/K_{v_i})$ contains a p-Sylow subgroup of G, for $w_i|v_i$ and $i = 1, 2$.*

Note that the property of containing a p-Sylow subgroup does not depend on the choice of the prime w_i that divides v_i.

It follows that over number fields Problem 0.1.1 takes the form of an inverse Galois problem with local conditions. We extract these local conditions and call them K-preadmissibility:

Definition 0.1.3. Let K be a number field. A finite group G is called
K- preadmissible if for every prime $p||G|$ there exist two primes $v_1(p), v_2(p)$ and two subgroups $G^{(1,p)}, G^{(2,p)} \leq G$ such that $G^{(i,p)}$ contains a p-Sylow subgroup of G and is realizable over $K_{v_i(p)}$, for all $p||G|$, $i = 1, 2$.

In many studies of admissibility, a group was first shown to satisfy local preadmissibility conditions and then to have global realizations that satisfy these local conditions. Since in most cases preadmissibility is much easier to verify and since it often implies admissibility, this method has proven to be effective.

In Chapter 1, we compare admissibility with preadmissibility. We start with abelian groups. An abelian group is K-admissible if and only if its Sylow subgroups are K-admissible (see Section 1.1.1) and therefore it suffices to consider the case of abelian p-groups. An abelian p-group A is K-preadmissible if and only if A is realizable over K_v for at least two primes v of K.

In [4], Charbit and Sonn used the Grunwald-Wang theorem to prove that away from the theorem's special case, an abelian p-group is K-preadmissible if and only

if it is K-admissible. They used this equivalence to obtain explicit conditions for K-admissibility of abelian groups, assuming one is not in a special case. Since special cases occur only for $p = 2$, it remains to consider abelian 2-groups.

Given a cyclic group C, Wang ([58]) characterized the (special) examples of finite sets S of primes of K and corresponding extensions $L(v)/K_v$ with Galois group $C_v \leq C$ for every $v \in S$, that cannot be lifted to a C-extension L/K such that $L_v \cong L(v)$ for every $v \in S$.

As opposed to Wang's examples, the main difficulty in constructing an example of a p-group G and a field K such that G is K-preadmissible but not K-admissible, lies in showing that for every choice of primes v_1, v_2 of K and for every choice of G-extensions (extensions with Galois group G) $L(v_i)/K_{v_i}$, $i = 1, 2$, there is no G-extension L/K such that $L_{v_i} \cong L(v_i)$, $i = 1, 2$.

It turns out that there are abelian 2-groups A and number fields K such that A is K-preadmissible but not K-admissible (see Example 1.1.9). However, the following theorem shows that such examples are rare.

Let μ_n denote the group of n-th roots of unity.

Theorem 0.1.4. *Let K be a number field and A an abelian K-preadmissible 2-group. Then A is <u>not</u> K-admissible if and only if all of the following six conditions hold:*

(A1) *A is realizable over K_v for exactly two primes $v = v_1, v_2$ of K that divide 2;*

(A2) *$K(\mu_{2^n})/K$ is not cyclic for large enough n;*

Let s be the largest integer for which $K(\mu_{2^s})/K$ is cyclic;

(A3) *The extensions $K_v(\mu_{2^{s+1}})/K_v$ are cyclic for all primes v except at one prime w;*

(A4) *The prime w (defined by 3) must be one of the prime v_1, v_2 (defined by 1);*

Write $A = A_s \oplus A'_s$ where A_s is of exponent dividing 2^s and $A'_s = \prod_{i=1}^{r} C_{2^{k_i}}$ where $k_i > s$ for all $i = 1, \ldots, r$;

(A5) *A_s is either trivial or $A_s \cong C_2$;*

(A6) *$r = \mathrm{rk}(A'_s) = [K_w : \mathbb{Q}_2] + 1$.*

In the rest of Chapter 1, we provide examples in which preadmissibility implies admissibility (not necessarily for abelian groups). Our main tools are the theorems of Neukirch that are introduced in Section 0.2.2.

0.1.2 Tame admissibility

Over the field of rational numbers $\mathbb{Q}$, Schacher used Theorem 0.1.2 to prove that the Sylow subgroups of a $\mathbb{Q}$-admissible group must be metacyclic. The same argument shows that if G is $\mathbb{Q}$-preadmissible then G has metacyclic Sylow subgroups. The

converse also holds (see [30, Theorem 29]). Thus, a group is $\mathbb{Q}$-preadmissible if and only if it has metacyclic Sylow subgroups.

It is conjectured that groups with metacyclic Sylow subgroups are also $\mathbb{Q}$-admissible, i.e. that $\mathbb{Q}$-preadmissibility implies $\mathbb{Q}$-admissibility. In a series of papers (see [50], [6] and [51]), Sonn settled this conjecture for solvable groups:

Theorem 0.1.5. (Sonn) *Let G be a solvable group with metacyclic Sylow subgroups. Then G is $\mathbb{Q}$-admissible.*

In [30], Liedahl extended Schacher's observation as follows. Let K be a number field and $\sigma_{t,n}$ the automorphism of $\mathbb{Q}(\mu_n)$ for which $\sigma_{t,n}(\zeta) = \zeta^t$ for all $\zeta \in \mu_n$. If G is K-admissible and every rational prime that divides $|G|$ does not decompose in K (has only one prime of K that divides p) then for every $p||G|$, the p-Sylow subgroups of G are metacyclic and admit a presentation

$$\langle x, y | x^m = y^i, y^n = 1, x^{-1}yx = y^t \rangle \tag{0.1.1}$$

such that $\sigma_{t,n} \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/(\mathbb{Q}(\mu_n) \cap K))$. In Chapter 2, we prove the converse of Liedahl's observation for solvable groups. This provides the following natural analogue of Theorem 0.1.5 to arbitrary number fields:

Theorem 0.1.6. *Let K be a number field and G a solvable group. Assume that for every $p||G|$, the p-Sylow subgroups of G admit a presentation as in* (0.1.1) *such that $\sigma_{t,n} \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/(\mathbb{Q}(\mu_n) \cap K))$. Then G is K-admissible.*

This theorem was known when G is a metacyclic group by [30, Theorem 27]. Note that Sonn's proof of Theorem 0.1.5 does not extend to arbitrary number fields since it relies on a theorem of Neukirch [35, Main Theorem] (see Theorem 0.2.7) that assumes K does not have any non-trivial odd order roots of unity.

Our method is to prove a refinement of Theorem 0.1.5 that yields many G-extensions $L/\mathbb{Q}$ that are contained in $\mathbb{Q}$-division algebras as maximal subfields, and prove that for some of these extensions, LK/K is a G-extension which is contained in a K-division algebra as a maximal subfield. The proof of the refinement is an adaptation of Sonn's proof of Theorem 0.1.5.

As a corollary to Liedahl's observation and Theorem 0.1.6 we have:

Corollary 0.1.7. *Let K be a number field and G a solvable group such that every rational prime that divides $|G|$ does not decompose in K. Then G is K-admissible if and only if for every $p||G|$, the p-Sylow subgroups of G admit a presentation as in* (0.1.1) *for which $\sigma_{t,n} \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/(\mathbb{Q}(\mu_n) \cap K))$.*

In Chapter 2, we shall define a notion of tame K-admissibility which, as opposed to K-admissibility, allows only division algebras from a certain subgroup of the Brauer group $\mathrm{Br}(K)$. We shall show that tame admissibility is precisely the kind of admissibility that occurs in Theorem 0.1.6.

Note that if p decomposes in K, there are many K-admissible p-groups that are not metacyclic (and in particular not tamely K-admissible).

0.1.3 Arithmetic equivalences

Equivalence relations between number fields are often used to determine the extent to which certain arithmetic properties of a field determine the field. One example is *arithmetic equivalence* (see [39] or [25, Chap. III]), under which two number fields K and L are equivalent if they have the same Dedekind zeta function. Two arithmetically equivalent fields have the same $\mathbb{Q}$-normal closure, degree over $\mathbb{Q}$, inertia degrees of rational primes and a long list of other properties (see [25, Chap. III, Theorem 1.4]). In particular, if $L/\mathbb{Q}$ is Galois, there is no number field K different from L that is arithmetically equivalent to L.

In [38], Neukirch proved that if two number fields K and L have isomorphic absolute Galois groups then they have the same $\mathbb{Q}$-normal closure and asked if necessarily $K \cong L$. This was proved independently by Ikeda, Iwasawa and Uchida (see [57]).

In [55], Sonn asked an analogous question for admissibility. Two number fields K and L are *equivalent by admissibility* if K and L have the same admissible groups. In [55], Sonn showed that number fields which are equivalent by admissibility have the same $\mathbb{Q}$-normal closure. It is unknown whether two number fields which are equivalent by admissibility are necessarily isomorphic. In fact, even the following problem is open (see [55],[56]):

Problem 0.1.8. Let K and L be two number fields that are equivalent by admissibility. Do K and L necessarily have the same degree over $\mathbb{Q}$?

So far, this problem was found to have an affirmative answer in several cases. In [32, Theorem 5], Lochter showed that if in addition $[K : \mathbb{Q}]$ is a prime or $[K : \mathbb{Q}] = 4$ then necessarily $[K : \mathbb{Q}] = [L : \mathbb{Q}]$.

We shall say that two number fields K and L are *equivalent by preadmissibility* if they have the same preadmissible groups. In Chapter 3, we construct (infinitely many) examples of number fields L, Galois over $\mathbb{Q}$, and proper subfields $K \subset L$ such that K and L are equivalent with respect to preadmissibility and have the same odd order admissible groups. The often indistinguishable behavior of admissibility and preadmissibility and these constructions lead us to conjecture that Problem 0.1.8 has a negative answer in the following form:

Conjecture 0.1.9. *There exists a number field L that has a proper subfield K such that K and L have the same admissible groups.*

Even though equivalence by admissibility is a complete mystery, in many cases equivalence by preadmissibility is within reach and allows one to study equivalence by admissibility with respect to various families of groups. Sonn's proof of [55, Theorem 1] can be adapted to show that number fields that are equivalent by preadmissibility must have the same $\mathbb{Q}$-normal closure (see Proposition 3.1.2). In particular $\mathbb{Q}$ is equivalent by preadmissibility only to itself. However, there are number fields L that are Galois over $\mathbb{Q}$ and have proper subfields K that are preadmissibly equivalent to L (see Corollary 3.2.3). We use the following theorem to reduce this assertion to a group theoretical statement on split double cosets.

For two subgroups A, B of a finite group $\mathcal{G}$, a double coset AxB is called *split* if $|AxB| = |A||B|$.

Theorem 0.1.10. *Let l be a prime and $\mathcal{G}$ an l-group. Let $L/\mathbb{Q}$ be a $\mathcal{G}$-extension in which l splits completely. Let K be a subfield of L and $\mathcal{H} = \mathrm{Gal}(L/K)$. If for every subgroup $D \leq \mathcal{G}$ that appears as a decomposition group there are two split double cosets of the form $Dx\mathcal{H}$, $x \in \mathcal{G}$, then K and L are equivalent by preadmissibility. If $\mathcal{G}$ is non-metacyclic the converse also holds.*

Note that the requirement on l to split completely is satisfied in many known realizations of l-groups including those of Scholz-Reichardt (see [45]) and Shafarevich (see [40]). By observing that extensions $L/\mathbb{Q}$ as in Theorem 0.1.10 are tamely ramified and hence have metacyclic decomposition groups and using the realizations of [40],[45] and Neukirch's Theorem (see [37]), we obtain the following group theoretic criterion:

Corollary 0.1.11. *Let l be a prime. Let $\mathcal{G}$ be an l-group and $\mathcal{H} \leq \mathcal{G}$ a subgroup such that for every metacyclic subgroup $D \leq \mathcal{G}$ there are two split double cosets of the form $Dx\mathcal{H}$. Then there is a $\mathcal{G}$-extension $L/\mathbb{Q}$ such that L and $K := L^{\mathcal{H}}$ are equivalent by preadmissibility and have the same odd order admissible groups.*

In Section 3.2.1, we give simple group theoretic conditions for the construction of infinitely many pairs $(\mathcal{G}, \mathcal{H})$ as in Corollary 0.1.11. In particular Corollary 0.1.11 yields examples of preadmissibly equivalent fields K, L with $[L : \mathbb{Q}] > [K : \mathbb{Q}]$.

We then compare equivalence by preadmissibility to arithmetic equivalence and other arithmetic relations.

0.2 Preliminaries

In this section we shall establish notations and summarize known results from algebraic number theory and Galois theory which we use repeatedly.

We shall start with the Grunwald-Wang theorem which provides realizations of abelian groups with prescribed local conditions. We shall then establish our setup of embedding problems and state theorems of Neukirch on embedding problems with prescribed local conditions. Finally, we shall discuss the structure of local Galois groups.

0.2.1 The Grunwald-Wang theorem

Let μ_n denote the group of n-th roots of unity and

$$\mu_{2^\infty} := \bigcup_{k \in \mathbb{N}} \mu_{2^k}.$$

Let $(\zeta_{2^k})_{k=0}^{\infty} \subseteq \mu_{2^\infty}$ a sequence such that $\zeta_1 = 1$ and $\zeta_{2^{k+1}}^2 = \zeta_{2^k}$ for all $k \geq 1$. Let $\eta_k := \zeta_{2^k} + \zeta_{2^k}^{-1}$ for all $k \geq 0$. In particular, $\eta_0 = 2, \eta_1 = -1, \eta_2 = 0 \in K$ and

$$\eta_{k+1}^2 = \eta_k + 2 \text{ for all } k \geq 0. \tag{0.2.1}$$

Let $s \geq 2$ be the largest integer such that $\eta_s \in K$ and

$$S_0 := \{v \mid K_v(\mu_{2^{s+1}})/K_v \text{ is not cyclic }\}.$$

In particular, S_0 consists only of primes that divide 2.

Following [2, Chapter 10] and [35, Theorem 9.1.3], we define a special case as follows. We shall say $K(\mu_{2^\infty})/K$ is non-cyclic if its Galois group is not the cyclic pro-2 group, i.e. if $\mathrm{Gal}(K(\mu_{2^\infty})/K) \ncong \mathbb{Z}_2$.

Definition 0.2.1. Let S be a finite set of primes of K. Let $m = 2^r m'$, where $m' \in \mathbb{N}$ is odd and $r \in \mathbb{Z}^{\geq 0}$. We say that the triple (K, m, S) *falls into a special case* if the following conditions hold:

(1) the extension $K(\mu_{2^\infty})/K$ is non-cyclic;

(2) $S_0 \subseteq S$;

(3) $r > s$.

Remark 0.2.2. ([2, Chapter X]) Note that (1) is equivalent to $K \cap \mathbb{Q}(\mu_{2^\infty}) = \mathbb{Q}(\eta_s)$. Thus, (1) holds if and only if $\sqrt{-1}, \eta_{s+1}, \sqrt{-1}\eta_{s+1} \notin K$. In particular, conditions (1)+(3) are equivalent to $K(\mu_{2^r})/K$ being non-cyclic.

For abelian groups A such that $(K, \exp(A), S)$ does not fall into a special case, the Grunwald-Wang theorem (see [35, Theorem 9.1.3]) asserts that the following restriction map is surjective:

$$\theta_A : \mathrm{Hom}(G_K, A)_{sur} \to \prod_{v \in S} \mathrm{Hom}(G_{K_v}, A),$$

where absolute Galois groups are equipped with Krull's topology and A with the discrete topology, Hom denotes the group of all continuous homomorphisms and $\mathrm{Hom}(G_K, A)_{sur}$ denotes all continuous epimorphisms.

As a corollary one has:

Corollary 0.2.3. *Let K be a number field and S a finite set of primes of K. Let A be an abelian group such that $(K, \exp(A), S)$ does not fall into a special case. For every $v \in S$, fix a Galois extension $L^{(v)}/K_v$ whose Galois group is isomorphic to a subgroup of A. Then there exist a Galois extension L/K with $\mathrm{Gal}(L/K) \cong A$ such that $L_v = L^{(v)}$ for all $v \in S$.*

To state a full version of the Grunwald-Wang theorem, let us recall some facts from class fields theory. Let C_K be the idèle class group of K equipped with its standard topology. By global class field theory the norm residue symbol map induces an isomorphism $\mathrm{Hom}(G_K, A) \cong \mathrm{Hom}(C_K, A)$ that is compatible with the isomorphism $\mathrm{Hom}(G_{K_v}, A) \cong \mathrm{Hom}(K_v^*, A)$ induced by the local norm residue map. In particular, the following diagram is commutative:

$$\begin{array}{ccc} \mathrm{Hom}(G_K, A) & \xrightarrow{\mathrm{res}} & \prod_{v \in S} \mathrm{Hom}(G_{K_v}, A) \\ \downarrow & & \downarrow \\ \mathrm{Hom}(C_K, A) & \xrightarrow{\mathrm{res}} & \prod_{v \in S} \mathrm{Hom}(K_v^*, A), \end{array} \tag{0.2.2}$$

where res denotes the restriction maps and the vertical maps are the isomorphisms induced by the norm residue symbol maps. Thus, realizations of A over K correspond to continuous epimorphisms $C_K \to A$ and realizations of A over K_v corresponds to epimorphisms $K_v^* \to A$.

The Grunwald-Wang theorem (see [2, Theorem 5, Chapter 10]) describes the image of the restriction maps in (0.2.2) as follows:

Theorem 0.2.4. (Grunwald-Wang) *Let C be the cyclic group of order m. Let S be a finite set of primes of K and for every $v \in S$, let ψ_v be an element of $\mathrm{Hom}(K_v^*, C)$ of exponent $m_v | m$. Then there is an element of $\mathrm{Hom}(C_K, C)$ that restricts to $(\psi_v)_{v\in S}$ if and only if one of the following conditions holds:*

1. *(K, m, S) does not fall into a special case;*
2. *m is even and*
$$\sum_{v\in S_0} \psi_v(2+\eta_s)^{\frac{m}{2}} = 0. \tag{0.2.3}$$

Note that since $m_v | m$, the element $\psi_v(2+\eta_s)^{\frac{m}{2}} \in C$ is of order dividing 2.

Remark 0.2.5. If m is not divisible by 2^s, (K, m, S) does not fall into a special case, in which case the theorem implies that the restriction map is surjective.

Remark 0.2.6. Assume S_0 consists of one prime w such that $K_w \cong \mathbb{Q}_2$. In particular, $s = 2$. Since $16 = (2+\eta_s)^{\frac{8}{2}}$ is not a norm from the unramified 8-extension of $\mathbb{Q}_2$ (see e.g. [2, Chapter X, Consequence]), one deduces from [59] that there is no C_8-extension Ω/K for which Ω_w/K_w is the unramified C_8-extension. Wang's original counterexample ([58]) to Grunwald's theorem was precisely this example for $K = \mathbb{Q}$ and $w = (2)$.

0.2.2 Embedding problems

Global embedding problems

Let K be a number field and G_K the absolute Galois group of K. An embedding problem over K consists of a Galois extension L/K and an epimorphism $\pi : G \to \Gamma := \mathrm{Gal}(L/K)$. We shall abbreviate and denote such an embedding problem by $\pi : G \to \mathrm{Gal}(L/K)$. The following diagram corresponds to such an embedding problem:

$$\begin{array}{ccccc} & & G_K & & \\ & & \downarrow{\scriptstyle \mathrm{res}_L} & & \\ G & \xrightarrow{\pi} & \Gamma & \longrightarrow & 0, \end{array} \tag{0.2.4}$$

where $\mathrm{res}_L : G_K \to \Gamma$ denotes the restriction map.

Two homomorphisms $\psi_1, \psi_2 : G_K \to G$ are called equivalent if there is an $a \in ker(\pi)$ such that $a^{-1}\psi_1(g)a = \psi_2(g)$ for all $g \in G_K$. A solution is an equivalence class of homomorphisms $\psi : G_K \to G$ that makes diagram (0.2.4) commutative, i.e $\phi = \pi \circ \psi$. The set of solutions is denoted by $\mathrm{Hom}_\Gamma(G_K, G)$ and the set of surjective solutions is denoted by $\mathrm{Hom}_\Gamma(G_K, G)_{sur}$. For a surjective solution ψ, the fixed field of $\ker(\psi)$ is a field M that contains L and has Galois group $\mathrm{Gal}(M/K) \cong G$.

Induced local embedding problems

Following Neukirch ([36], [37]), we fix an algebraic closure $\overline{K}$ of K and for each prime v an algebraic closure $\overline{K}_v$ of K_v and an embedding of $\overline{K}$ into $\overline{K}_v$. In particular this identifies G_{K_v} as a subgroup of G_K. A Galois extension M/K is identified uniquely as a subfield of $\overline{K}$ and its image in $\overline{K}_v$ is denoted by M_v/K_v.

Let L/K be a Galois extension with Galois group $\Gamma := \mathrm{Gal}(L/K)$. Consider the global embedding problem $\pi : G \to \Gamma$. Since $G_{K_v} \leq G_K$, the global embedding problem induces a local embedding problem:

$$\begin{array}{ccccc} & & G_{K_v} & & \\ & & \downarrow{\scriptstyle \mathrm{res}_{L_v}} & & \\ G & \xrightarrow{\pi} & \Gamma & \longrightarrow & 0, \end{array} \tag{0.2.5}$$

for every prime v of K.

Every solution to the global embedding problem induces by restriction a solution to the local embedding problems. For a finite set S of primes of K, let

$$\theta_G^\Gamma(S) : \mathrm{Hom}_\Gamma(G_K, G)_{sur} \to \prod_{v \in S} \mathrm{Hom}_\Gamma(G_{K_v}, G)$$

denote the restriction map.

Fix an element $(\psi_v)_{v\in S} \in \prod_{v\in S} \mathrm{Hom}_\Gamma(G_{K_v}, G)$ and let $M^{(v)}$ be the fixed field of $\ker(\psi_v)$, for $v \in S$. Then the existence of ψ such that $\theta_G^\Gamma(S)(\psi) = (\psi_v)_{v\in S}$ implies that the fixed field M of $\ker(\psi)$ has Galois group $\mathrm{Gal}(M/K) \cong G$ and completions M_v at $v \in S$.

We shall need such Grunwald-Wang type of results and therefore state several results on the surjectivity of the maps $\theta_G^\Gamma(S)$.

Embedding problems with prescribed local conditions

The main tools we use to solve embedding problems are [37, Main Theorem] and [36, Korollar 2.5].

Theorem 0.2.7. (Neukirch [37, Main Theorem]) *Let L/K be a Galois extension with Galois group $\Gamma := \mathrm{Gal}(L/K)$ and $m(L)$ the number of roots of unity in L. Let $\pi : G \to \Gamma$ be an epimorphism with a prosolvable kernel of finite exponent which is prime to $m(L)$. If*

$$\prod_v \mathrm{Hom}_\Gamma(G_{K_v}, G) \neq \emptyset,$$

where the product runs over all primes of K, then for every finite set S of primes of K the map $\theta_G^\Gamma(S)$ is surjective.

As a corollary one has the following Grunwald-Wang type of assertion:

Theorem 0.2.8. (Neukirch [37, Corollary 2]) *Let K be a number field with $m(K)$ roots of unity and S be a finite set of primes of K. Let G be a prosolvable group of*

finite exponent which is prime to $m(K)$. For every $v \in S$, fix a Galois extension $L^{(v)}/K_v$ whose Galois group is isomorphic to a subgroup of G. Then there exist a Galois extension L/K with $\mathrm{Gal}(L/K) \cong G$ such that $L_v = L^{(v)}$ for all $v \in S$.

For embedding problems with abelian kernel $A := \ker(\pi)$, we shall also use the following theorem of Neukirch to insure the surjectivity of $\theta_G^\Gamma(S)$. In such problems A is a Γ-module and the action of Γ on A induces an action of G_K on A via the restriction map.

Theorem 0.2.9. (Neukirch, [36, Korollar 2.5]) *Let K be a number field and S a finite set of primes of K. Let L/K be a finite Galois extension with Galois group $\Gamma := \mathrm{Gal}(L/K)$. Let $\pi : G \to \Gamma$ be an epimorphism with finite abelian kernel $A := \ker(\pi)$. Assume that $\mathrm{Hom}_\Gamma(G_K, G) \neq 0$ and that the restriction map*

$$\mathrm{H}^1(G_K, A) \to \prod_{v \in S} \mathrm{H}^1(G_{K_v}, A) \tag{0.2.6}$$

is surjective. Then the map $\theta_G^\Gamma(S)$ is surjective.

Neukirch also provides sufficient criteria for the map (0.2.6) to be surjective which we describe below. Let A' be the dual G_K-module $\mathrm{Hom}(A, \mu_n)$ with the action $f^\sigma(a) = f(a^{\sigma^{-1}})^\sigma$ for all $a \in A, \sigma \in G$ and $f : A \to \mu_n$. Let

$$G'_K = \{\sigma \in G_K | f^\sigma = f \text{ for all } f \in A'\}.$$

Let $K(A')$ be the fixed field of G'_K and $G' := \mathrm{Gal}(K(A')/K)$. For a prime v of K denote by G'_v the Galois group $\mathrm{Gal}(K(A')_v/K_v)$. Since the action of G'_K on A' is trivial, the action of G_K on A' induces an action of G' on A' and hence an action of G'_v on A'. For $v \in S$, let

$$\Gamma(G'_v, A') := \ker(\mathrm{H}^1(G'_v, A') \to \prod_{g \in G'_v} \mathrm{H}^1(\langle g \rangle, A')).$$

Theorem 0.2.10. (Neukirch [36, Korollar 6.4]) *Let K be a number field and S a finite set of primes of K. Let A be a finite G_K-module. Then the map*

$$\mathrm{H}^1(G_K, A) \to \prod_{v \in S} \mathrm{H}^1(G_{K_v}, A) \tag{0.2.7}$$

is surjective in each of the following cases:

(a) *$\Gamma(G'_v, A')$ for all $v \in S$,*

(b) *for every $v \in S$, the group G'_v is cyclic or a semidirect product of two cyclic groups of relatively prime orders,*

(c) *$\mathrm{H}^1(G', A') = 0$,*

(d) *$|G'| = \mathrm{lcm}\{|G'_v| | v \notin S\}$,*

(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 (see Definition 0.2.1).*

Remark 0.2.11. Theorems 0.2.7 and 0.2.9 were originally stated in a more general and "abstract" setup of embedding problems.

In this setup, $\pi : G \to \Gamma$ is an epimorphism of (abstract) profinite groups and there is a given continuous epimorphism $\phi : G_K \to \Gamma$ which replaces the role of the restriction map. The solutions $\mathrm{Hom}_\Gamma(G_K, A)$ are equivalence classes of continuous homomorphisms $\psi : G_K \to G$ for which $\phi = \pi \circ \psi$. The local solutions $\mathrm{Hom}_\Gamma(G_{K_v}, A)$ are equivalence classes of continuous homomorphisms $\psi_v : G_{K_v} \to G$ for which $\phi_{|G_{K_v}} = \pi \circ \psi_v$.

We shall make use of this setup only once when discussing examples in Section 1.2.2.

0.2.3 Local Galois groups

In the following we shall describe the structure of p-extensions and tamely ramified extensions of a p-adic field k. For a full treatment see [35, Chap. VII §5] or [47, §2.5.6].

Let q the size of the residue field $\overline{k}$, k_{un} (resp. k_{tr}) the maximal unramified (resp. tamely ramified) extension of k, $n := [k : \mathbb{Q}_p]$ and p^s the number of p-power roots of unity in k.

1. The group $\mathrm{Gal}(k_{un}/k)$ is profinitely generated by an automorphism σ, i.e. it is the profinite closure of the subgroup $\langle\sigma\rangle$. In particular $\mathrm{Gal}(k_{un}/k) \cong \hat{\mathbb{Z}}$.

2. The group $\mathrm{Gal}(k_{tr}/k_{un})$ is profinitely generated by an automorphism τ of order prime to p and is isomorphic to $\hat{\mathbb{Z}}_{(p')}$ (the complement of $\mathbb{Z}_p$ in $\hat{\mathbb{Z}}$).

3. The group $\mathrm{Gal}(k_{tr}/k)$ is profinitely generated by two elements σ (lifting the above mentioned automorphism) and τ such that:

$$\mathrm{Gal}(k_{tr}/k) \cong \langle \sigma, \tau \mid \sigma^{-1}\tau\sigma = \tau^q \rangle,$$

   where in the right hand side σ generates $\hat{\mathbb{Z}}$ and τ generates $\mathbb{Z}_{(p')}$.

4. Let $M_p(k)$ be the maximal pro-p extension of k and denote by $\mathfrak{G}_k$ the Galois group $\mathrm{Gal}(M_p(k)/k)$. If $\mu_p \not\subseteq k$, $\mathfrak{G}_k$ is the free pro-p group on $n+1$ generators.

5. If $\mu_p \subseteq k$ and $p^s \neq 2$, then $\mathfrak{G}_k$ has the following presentation of pro-p groups:

$$\langle x_1, \ldots, x_{n+2} \mid x_1^{p^s}[x_1, x_2] \cdots [x_{n+1}, x_{n+2}] = 1 \rangle. \tag{0.2.8}$$

6. If $p^s = 2$ (and hence $p = 2$) and n is even then $\mathfrak{G}_k$ has one of the following presentations of pro-2 groups:

$$\langle x_1, \ldots, x_{n+2} \mid x_1^2[x_1, x_2]x_3^{2^f}[x_3, x_4] \cdots [x_{n+1}, x_{n+2}] = 1 \rangle, \tag{0.2.9}$$

$$\langle x_1, \ldots, x_{n+2} \mid x_1^{2+2^f}[x_1, x_2] \cdots [x_{n+1}, x_{n+2}] = 1 \rangle, \tag{0.2.10}$$

where $f \geq 2$ is an integer.

7. If $p^s = 2$ and n is odd, $\mathfrak{G}_k$ has the following presentation of pro-2 groups:

$$\langle x_1, \ldots, x_{n+2} \mid x_1^2 x_2^4 [x_2, x_3] \cdots [x_{n+1}, x_{n+2}] = 1 \rangle. \tag{0.2.11}$$

Chapter 1

Preadmissibility

In this chapter we shall compare admissibility to preadmissibility for several families of groups. At first we consider abelian groups. After reducing to the case of abelian 2-groups we shall prove (Theorem 0.1.4) that an abelian K-preadmissible 2-group A is not K-admissible if and only if the following six conditions hold:

(A1) A is realizable over K_v for exactly two primes $v = v_1, v_2$ of K that divide 2;

(A2) $K(\mu_{2^\infty})/K$ is non-cyclic;

Let s be the largest integer for which $K(\mu_{2^s})/K$ is cyclic;

(A3) The extensions $K_v(\mu_{2^{s+1}})/K_v$ are cyclic for all primes v except at one prime w;

(A4) The prime w (defined by 3) must be one of the prime v_1, v_2 (defined by 1);

Write $A = A_s \oplus A'_s$ where A_s is of exponent dividing 2^s and $A'_s = \prod_{i=1}^{r} C_{2^{k_i}}$ where $k_i > s$ for all $i = 1, \ldots, r$;

(A5) A_s is either trivial or $A_s \cong C_2$;

(A6) $r = \mathrm{rk}(A'_s) = [K_w : \mathbb{Q}_2] + 1$.

We shall also see that there are infinitely many examples of preadmissible abelian 2-groups that are not admissible. The smallest possible degree $[K : \mathbb{Q}]$ in such an example is 3 and the smallest possible order of A is 2^7.

In Section 1.2, we shall define the Grunwald-Neukirch property (GN-property). A group that admits this property over K is K-admissible if and only if it is K-preadmissible. We shall summarize known results asserting that certain groups have the GN-property and iterate these results to discuss the GN-property for families of solvable groups that are closed under semidirect products with cyclic kernels and under quotients. This section will provide us many examples of non-abelian groups for which preadmissibility implies admissibility.

1.1 Admissibility of abelian groups

1.1.1 Admissibility away from the special case

Let us recall what is known about admissibility of abelian groups over number fields.

Let K be a number field. Following [44], we call a field L *K-adequate* if it is contained as a maximal subfield of a finite dimensional division algebra with center K. Note that Schacher's criterion asserts furthermore that the field L in Theorem 0.1.2 is in fact K-adequate.

Assume A is an abelian group that decomposes into primary components as $A = \prod_p A_p$. It follows from Schacher's criterion that:

1. K-admissibility is closed under quotients,
2. the compositum of two K-adequate fields L_1, L_2 of degrees $[L_1 : \mathbb{Q}]$ and $[L_2 : \mathbb{Q}]$ that are prime to each other is also K-adequate.

Thus, A is K-admissible if and only if A_p is K-admissible for every p. Similarly, preadmissibility is closed under quotients and for any two preadmissible groups G_1, G_2 such that $(|G_1|, |G_2|) = 1$, $G_1 \times G_2$ is also preadmissible. Thus, A is preadmissible if and only if A_p is preadmissible for every p. Therefore the problems of determining K-admissibility and K-preadmissibility reduce to the case of abelian p-groups.

If A is a metacyclic p-group then the same proof as in [44, Theorem 6.1] (see also remark after [30, Theorem 27]) shows that A is realizable over K_v for infinitely many primes v of K, A is K-preadmissible and that A is K-admissible. We therefore reduce to abelian p-group of rank ≥ 3.

In [4], Charbit and Sonn used the Grunwald-Wang theorem to prove:

Theorem 1.1.1. (Charbit and Sonn [4]) *Let p be an odd prime and A an abelian p-group of rank* $\mathrm{rk}(A) \geq 3$. *Then the following conditions are equivalent:*

1. *A is K-admissible;*
2. *A is realizable over K_v for two primes $v = v_1, v_2$, i.e. A is K-preadmissible;*
3. *there are two primes v_1, v_2 of K that divide p such that for each of them one of the following holds:*
   - *(a)* $\mathrm{rk}(A) \leq [K_{v_i} : \mathbb{Q}_p] + 1$,
   - *(b)* $\mathrm{rk}(A) = [K_{v_i} : \mathbb{Q}_p] + 2$ *and there is an element $a \in A \setminus A^p$ of order dividing p^{s_i}, where p^{s_i} is the number of roots of unity in K_{v_i}.*

The implication (2) $\to$ (1) was also proved for $p = 2$, when $(K, \exp(A), \{v_1, v_2\})$ does not fall into a special case. It therefore remains to compare admissibility and preadmissibility for abelian 2-groups of rank ≥ 3.

1.1.2 The Grunwald-Wang theorem for abelian groups

In order to consider admissibility in the special cases we shall first derive a version of Theorem 0.2.4 for abelian groups.

Let A be an abelian group and S a finite set of primes of K. We can decompose A into cyclic primary components as

$$A = \prod_{i=1}^{a} \prod_{j=1}^{b} C_{p_i^{k_{i,j}}}, \tag{1.1.1}$$

for some primes $p_1 < \ldots < p_a$ and integers $k_{i,j} \geq 0$ such that $p_1 = 2$. Let $\pi_{i,j}$ be the projection onto the direct summand $C_{p_i^{k_{i,j}}}$ along the other summands in this decomposition. Then one has the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}(C_K, A) & \xrightarrow{\text{res}} & \prod_{v\in S} \mathrm{Hom}(K_v^*, A) \\ \downarrow{\scriptstyle \prod_{i=1,j=1}^{a,b} (\pi_{i,j})_*} & & \downarrow{\scriptstyle \prod_{i=1,j=1}^{a,b} (\pi_{i,j})_*} \\ \prod_{i=1,j=1}^{a,b} \mathrm{Hom}(C_K, C_{p_i^{k_{i,j}}}) & \xrightarrow{\text{res}} & \prod_{i=1,j=1}^{a,b} \prod_{v\in S} \mathrm{Hom}(K_v^*, C_{p_i^{k_{i,j}}}), \end{array}$$

where $(\pi_{i,j})_*$ is defined by $(\pi_{i,j})_*(f) = \pi_{i,j} \circ f$. Since the vertical maps are isomorphisms, an element $(\psi_v : {K_v}^* \to A)_{v\in S}$ is in the image of the restriction map if and only if for every for every $i \in \{1, \ldots, a\}$ and $j \in \{1, \ldots, b\}$, the element $(\pi_{i,j} \circ \psi_v)_{v\in S}$ is a restriction of some element of $\mathrm{Hom}(C_K, C_{p_i^{k_{i,j}}})$.

By Remark 0.2.5, it suffices to consider the prime $p_1 = 2$ and only the powers $k_{1,j} > s$. We therefore have the following corollary to Theorem 0.2.4.

Let A_{odd} be the product of the odd order direct summands in (1.1.1) and A_s the product of the direct summands of exponent dividing 2^s in (1.1.1), so that

$$A = A_s \times A_{odd} \times \prod_{j=1}^{r} C_{2^{k_j}} \tag{1.1.2}$$

for some $r \geq 0$ and $k_j > s$ for all $i \in \{1, \ldots, r\}$. Note that the k_j's are those indices $k_{1,j}$ in (1.1.1) that are greater than s. Let π_i be the projection from A onto $C_{2^{k_i}}$ along the other direct summands in (1.1.2).

Corollary 1.1.2. *For every $v \in S$, fix $\psi_v \in \mathrm{Hom}(K_v^*, A)$. Then $(\psi_v)_{v\in S}$ is not in the image of the restriction map if and only if all of the following conditions hold:*

1. *$K(\mu_{2^\infty})/K$ is non-cyclic,*
2. *$S_0 \subseteq S$,*
3. *$r > 0$ and there is a $j \in \{1, \ldots, r\}$ such that*

$$\sum_{v\in S_0} \pi_j \circ \psi_v (2 + \eta_s)^{2^{k_j - 1}} \neq 0.$$

Remark 1.1.3. In particular, if $S_0 = \emptyset$, (3) fails and every $(\psi_v : k_v^* \to A)_{v\in S}$ is in the image of the restriction map.

1.1.3 Admissibility in the special cases

In order to apply Corollary 1.1.2 to admissibility, we shall need several lemmas on abelian groups and epimorphisms from the multiplicative group of a 2-adic field.

Generators

The following lemma recalls basic properties of abelian groups.

Let A be an abelian p-group. Recall that an element $a \in A$ is called *non-generating* if for every set $S \subseteq A$ such that $\langle a, S\rangle = A$, one has $\langle S\rangle = A$. Otherwise a is called a *generator*.

Lemma 1.1.4. *Let $\psi : B \to A$ an epimorphism of abelian p-groups. Let $\pi : A \to A/A^p$ be the natural projection. Then:*

1. *An element $a \in A$ is a generator of A if and only if $\pi(a) \neq 0$;*
2. *For a generator $a \in A$, every $b \in \psi^{-1}(a)$ is a generator of B;*
3. *ψ induces an epimorphism $\widetilde{\psi} : B/B^p \to A/A^p$ defined by $\widetilde{\psi}(bB^p) := \psi(b)A^p$;*
4. *If $\mathrm{rk}(A) = \mathrm{rk}(B)$ then $\widetilde{\psi}$ is an isomorphism. In particular, a generator $a \in A$ is mapped to a generator $\psi(a)$ of B;*
5. *If $\mathrm{rk}(A) < \mathrm{rk}(B)$ there is a generator $b \in \ker(\psi)$ of B;*
6. *If $a \in A$ is a generator of order p then $\langle a\rangle$ is a direct summand of A.*

Proof. 1. A basic example of the Burnide Basis Theorem ([18, Theorem 12.2.1]).

2. Since $\psi(B^p) \subseteq A^p$, any element of $\psi^{-1}(a)$ is not in B^p and hence a generator of B.

3. Since ψ is an epimorphism, the map $\psi_0 := \pi\circ\psi : B \to A/A^p$ is also an epimorphism. Since $\psi(B^p) \subseteq A^p$, $\psi_0(B^p) = 0$ and hence the map $\widetilde{\psi} : B/B^p \to A/A^p$ defined by $\widetilde{\psi}(bB^p) = \psi(b)A^p$ is well defined and is an epimorphism.

4. Since $\mathrm{rk}(A/A^p) = \mathrm{rk}(A) = \mathrm{rk}(B) = \mathrm{rk}(B/B^p)$ and since $A/A^p, B/B^p$ are elementary abelian p-groups, $\widetilde{\psi}$ is an isomorphism.

   For a generator $b \in B$, $b \notin B^p$ and hence the image $\widetilde{\psi}(bB^p)$ is non-trivial. Thus, $\psi(b) \notin A^p$ and $\psi(b)$ is a generator of A.

5. Since $\mathrm{rk}(A/A^p) < \mathrm{rk}(B/B^p)$, there is a $b \in B \setminus B^p$ for which $\widetilde{\psi}(bB^p) = 0$. Thus b is a generator of B such that $\psi(b) = a^p$ for some $a \in A$. Let $x \in \psi^{-1}(a)$ and set $b' = bx^{-p}$. Then $b' \in B$ is also a generator of B and $\psi(b') = \psi(b)\psi(x)^{-p} = 0$ implying $b' \in \ker(\psi)$.

6. Since A/A^p is elementary abelian, we can write $A/A^p = \langle\pi(a)\rangle \oplus A_0$. Thus, $A = \langle a\rangle + \pi^{-1}(A_0)$. As $a \notin \pi^{-1}(A_0)$ we have $\langle a\rangle \cap \pi^{-1}(A_0) = \{0\}$ and hence $A = \langle a\rangle \oplus \pi^{-1}(A_0)$.

□

Epimorphic images of the multiplicative group

Let k be a 2-adic field such that $\eta_s \in k$ but $\sqrt{-1}, \eta_{s+1}, \sqrt{-1}\eta_{s+1} \notin k$ and let $n = [k : \mathbb{Q}_2]$.

Let $A = A_s \times \prod_{j=1}^{r} C_{2^{k_j}}$ be an abelian 2-group such that A_s is of exponent dividing 2^s, $r \geq 0$ and $k_j > s$ for all $j \in \{1, \ldots, r\}$. Let m be the exponent of A and for $j = 1, \ldots, r$, let π_j be the projection of A onto the direct summand $C_{2^{k_j}}$ along the other r direct summands appearing above.

Recall (e.g. [21, Chapter 2]) that $k^* \cong C_2 \times \mathbb{Z} \times \mathbb{Z}_2^n$ and hence that

$$k^*/k^{*m} \cong C_2 \times C_m^{n+1}.$$

Note that $\mathrm{Hom}(k^*, A) \cong \mathrm{Hom}(k^*/k^{*m}, A)$ and therefore we shall often use a homomorphism from k^*/k^{*m} to represent a homomorphism from k^*.

To construct epimorphisms we shall use the following decompositions of k^*/k^{*m}.

Lemma 1.1.5. *Assume $m > 1$. Let $x \in k^*/k^{*m}$ be a generator such that $x \not\equiv -1 \pmod{k^{*2}}$. Then there is a subgroup $B_x \leq k^*/k^{*m}$ such that*

$$k^*/k^{*m} = \langle -1 \rangle \oplus \langle x \rangle \oplus B_x$$

and $B_x \cong C_m^n$.

Proof. As $\sqrt{-1} \notin k^*$, -1 is a generator in k^*/k^{*m}. Since $x \not\equiv \pm 1 \pmod{k^{*2}}$ $\langle -1, x \rangle = \langle -1 \rangle \oplus \langle x \rangle$ is a $C_2 \times C_2$ subgroup of k^*/k^{*2}. Thus, $\mathrm{rk}(k^*/\langle -1, x \rangle k^{*2}) = n$ and hence $k^*/\langle -1, x \rangle k^{*m} \cong C_m^n$. Since k^*/k^{*m} is of exponent m, the sequence

$$0 \to \langle -1 \rangle \oplus \langle x \rangle \to k^*/k^{*m} \to C_m^n \to 0$$

splits and $k^*/k^{*m} = \langle -1 \rangle \oplus \langle x \rangle \oplus B_x$ where $B_x \cong C_m^n$. □

Since $\eta_{s+1} \notin k$ and $\eta_{s+1}^2 = \eta_s + 2$ (see (0.2.1)), $2 + \eta_s$ is not a square in k^* and hence $(2 + \eta_s)k^{*m}$ is a generator of k^*/k^{*m}. Since $\sqrt{-1}\eta_{s+1} \notin k$, we have

$$2 + \eta_s \not\equiv -1 \pmod{k^{*2}}.$$

Thus, by Lemma 1.1.5 we can write:

$$k^*/k^{*m} = \langle -1 \rangle \oplus \langle (2 + \eta_s)k^{*m} \rangle \oplus B \tag{1.1.3}$$

where $B \cong C_m^n$. Note that $\langle (2 + \eta_s)k^{*m} \rangle \cong C_m$.

We shall use the following lemma to construct epimorphisms $\psi : k^* \to A$ with a given value $\psi(2 + \eta_s) \in A$.

Lemma 1.1.6. *Assume $m > 1$. Let $a \in A$ and assume $\psi : k^*/k^{*m} \to A$ is an epimorphism for which $\psi^{-1}(a)$ contains a generator b of k^*/k^{*m} such that*

$$b \not\equiv -1 \ (\mathit{mod}\ k^{*2}).$$

Then there is an epimorphism $\psi' : k^* \to A$ such that $\psi'(2 + \eta_s) = a$.

Proof. Since b is a generator of k^*/k^{*m} such that $b \not\equiv -1 \pmod{k^{*2}}$, we can apply Lemma 1.1.5 and write:

$$k^*/k^{*m} = \langle -1 \cdot k^{*m} \rangle \oplus \langle b \rangle \oplus B_b \tag{1.1.4}$$

where $B_b \cong C_m^n$ and $\langle b \rangle \cong C_m$.

Since (1.1.3) and (1.1.4) hold, one has an automorphism $\phi : k^*/k^{*m} \to k^*/k^{*m}$ such that $\phi((2+\eta_s)k^{*m}) = b$, $\phi(-1) = -1$ and $\phi(B) = B_b$. Thus,

$$\psi_0 = \psi \circ \phi : k^*/k^{*m} \to A$$

is an epimorphism for which $\psi_0((2+\eta_s)k^{*m}) = \psi(b) = a$. In particular ψ_0 defines an epimorphism $\psi' : k^* \to A$ such that $\psi'(2+\eta_s) = a$, as required.

□

We shall use the following lemma to determine when can the special cases be avoided.

Lemma 1.1.7. *Assume A is an epimorphic image of k^*. Then the following conditions are equivalent:*

1. *for every epimorphism $\psi : k^* \to A$, $\psi(2+\eta_s)$ is a generator of A of order greater than 2^s,*
2. *for every epimorphism $\psi : k^* \to A$, there is a $j \in \{1, \ldots, r\}$ such that $\pi_j \circ \psi(2+\eta_s)$ is a generator of $C_{2^{k_j}}$,*
3. *$r = n+1$ and A_s is either $\{0\}$ or C_2.*

Proof. We shall prove (2) ⇒ (1) ⇒ (3) ⇒ (2).

If A is trivial the three conditions fail. We can therefore assume $A \neq \{0\}$ and $m > 1$. As in (1.1.3) write

$$k^*/k^{*m} = \langle -1 \rangle \oplus \langle (2+\eta_s)k^{*m} \rangle \oplus B$$

where $B \cong C_m^n$. Let $B' = \langle (2+\eta_s)k^{*m} \rangle \oplus B$.

(2) ⇒ (1) : Lemma 1.1.4.(2) applied for π_j shows that if $\pi_j \circ \psi(2+\eta_s)$ is a generator then $\psi(2+\eta_s)$ is a generator of A. Also, if $\pi_j \circ \psi(2+\eta_s)$ is of order greater than 2^s, the order of $\psi(2+\eta_s)$ is also greater than 2^s. Thus, (2) implies (1).

Note that the converse is not immediate since a generator $a \in A$ need not generate a direct summand of A.

(3) ⇒ (2) : Assume at first that $A_s = \{0\}$ and let $\psi : k^* \to A$ be an epimorphism. Since $\psi(-1)$ is of order at most 2 and A has no C_2-direct summands, $\psi(-1)$ is not a generator of A. Thus, $A = \mathrm{Im}(\psi) = \langle \psi(-1), \psi(B') \rangle$ implies $\psi(B') = A$.

Since $\mathrm{rk}(B') = \mathrm{rk}(A)$, it follows from Lemma 1.1.4.(4) that ψ maps generators of B' to generators of A and hence $\psi(2+\eta_s) \notin A^2$. Thus, there is a j such that $\pi_j \circ \psi(2+\eta_s) \notin (C_{2^{k_j}})^2$ and hence $\pi_j \circ \psi(2+\eta_s)$ is a generator of $C_{2^{k_j}}$.

Now assume $A_s \cong C_2$. Since in this case $\mathrm{rk}(k^*/k^{*m}) = \mathrm{rk}(A)$, Lemma 1.1.4.(4) implies that ψ maps generators of k^*/k^{*m} to generators of A and that the induced map

$$\widetilde{\psi} : k^*/(k^*)^2 \to A/A^2 = A_sA^2/A^2 \times \prod_{j=1}^{n+1} C_{2^{k_j}}/(C_{2^{k_j}})^2$$

is an isomorphism. Thus, $\psi(-1)$ is a generator of order 2. Since all elements of order 2 in A are in A_sA^2, we have $\langle\widetilde{\psi}(-1)\rangle = A_sA^2/A^2$. Since

$$2 + \eta_s \not\equiv \pm 1 \pmod{k^{*2}},$$

we have $\widetilde{\psi}((2+\eta_s)(k^*)^2) \notin A_sA^2/A^2$. Therefore there is a $j \in \{1, \ldots, n+1\}$ such that the $C_{2^{k_j}}/(C_{2^{k_j}})^2$-coordinate of $\widetilde{\psi}(2+\eta_s)$ is non-trivial and hence the element $\pi_j \circ \psi(2+\eta_s)$ is a generator of $C_{2^{k_j}}$.

(1) $\Rightarrow$ (3): Since A is an epimorphic image of k^*/k^{*m} we have

$$\mathrm{rk}(A) \leq \mathrm{rk}(k^*/k^{*m}) = n+2.$$

If $\mathrm{rk}(A) \leq n$, there is an epimorphism $\psi_1 : k^* \to A$ that sends B onto A and such that $2 + \eta_s \in \ker(\psi_1)$, contradicting (1). Thus, $\mathrm{rk}(A)$ must be at least $n+1$ and we have

$$n+1 \leq \mathrm{rk}(A) \leq n+2.$$

Assume at first $\mathrm{rk}(A) = n+2 = \mathrm{rk}(k^*/k^{*m})$ and let $\psi : k^*/k^{*m} \to A$ be an epimorphism. By Lemma 1.1.4.(4), $\psi(-1)$ is a generator of A and hence by Lemma 1.1.4.(6), $\langle -1\rangle$ is a C_2-direct summand of A.

Assume on the contrary that A has two direct summands. Thus, there is an $a \in A$ such that $a^{2^s} = 1$ and $a \not\equiv 1, \psi(-1) \pmod{A^2}$.

By Lemma 1.1.4.(2), an element $b \in \psi^{-1}(a)$ is necessarily a generator of k^*/k^{*m} and since $\psi(b) \not\equiv \psi(-1) \pmod{A^2}$ we have $b \not\equiv -1 \pmod{k^2}$. We can therefore apply Lemma 1.1.6 and deduce that there is an epimorphism $\psi' : k^* \to A$ such that $\psi'(2+\eta_s) = a$, contradiction. Thus, if $\mathrm{rk}(A) = n+2$, A has only one non-trivial direct summand of order dividing 2^s and it is a C_2-summand.

Now assume $\mathrm{rk}(A) = n+1 < n+2 = \mathrm{rk}(k^*/k^{*m})$. By Lemma 1.1.4.(5), there is a generator x of k^*/k^{*m} such that $\psi(x) = 1$. If $x \not\equiv -1 \pmod{k^{*2}}$, Lemma 1.1.6 implies that there is an epimorphism $\psi' : k^* \to A$ such that $\psi'(2+\eta_s) = 1$. We can therefore assume $x \equiv -1 \pmod{k^2}$ and hence $\psi(-1) \in A^2$.

Assume on the contrary that A has a non-trivial direct summand $\langle a\rangle$ of order dividing 2^s. By Lemma 1.1.4.(2), an element $b \in \psi^{-1}(a)$ is necessarily a generator of k^*/k^{*m} and since $\psi(b) = a \not\equiv 1 = \psi(-1) \pmod{A^2}$ we have $b \not\equiv -1 \pmod{k^2}$. Lemma 1.1.6 then implies that there is an epimorphism $\psi' : k^* \to A$ such that $\psi'(2+\eta_s) = a$, contradicting (1). Thus, if $\mathrm{rk}(A) = n+1$, A does not have a non-trivial direct summand of order dividing 2^s. □

The Main Theorem and its proof

We shall prove the following version of Theorem 0.1.4.

Theorem 1.1.8. *Let A be a K-preadmissible 2-group. Then A is not K-admissible if and only if all of the following conditions hold:*

(B1) *$K(\mu_{2^\infty})/K$ is non-cyclic,*

(B2) *A is realizable over K_v for exactly two (even) primes v_1, v_2 of K,*

(B3) *$S_0 = \{w\}$ where $w \in \{v_1, v_2\}$,*

(B4) *one of the following two conditions holds:*

- (a) *A does not have non-trivial direct summands of exponent dividing 2^s and $\mathrm{rk}(A) = [K_w : \mathbb{Q}_2] + 1$,*
- (b) *A has only one non-trivial direct summand of exponent dividing 2^s, it is a C_2-summand and $\mathrm{rk}(A) = [K_w : \mathbb{Q}_2] + 2$.*

Note that conditions (B1)-(B4) are equivalent to conditions (A1)-(A6) since (A1) is (B2), (A2) is (B1), (A3)+(A4) together are equivalent to (B3), and (A5)+(A6) together are equivalent to (B4).

Proof of Theorem 1.1.8. **If part:** Assume Conditions (B1)-(B4) hold. Assume on the contrary that A is K-admissible and hence that there is an epimorphism $\psi : C_K \to A$ that restricts at two primes w_1, w_2 to epimorphisms $\psi_{w_i} : K^*_{w_i} \to A$, $i = 1, 2$. Since (B2) holds, A is realizable over K_v only for $v = v_1, v_2$ and hence $\{w_1, w_2\} = \{v_1, v_2\}$. Assume without loss of generality that $w = w_1$.

If conditions (B4.a) or (B4.b) hold then by Lemma 1.1.7 there is a $j \in \{1, \dots, b\}$ such that $\pi_j \circ \psi_w(2 + \eta_s)^{2^{k_j - 1}} \neq 0$. This is a contradiction since Corollary 1.1.2 implies that in such a case, there is no epimorphism $\psi : K^*_w \to A$ that restricts to ψ_w.

Only if part: Assume A is not K-admissible. As noted in Section 1.1.1 this implies that A is not metacyclic, i.e. $\mathrm{rk}(A) \geq 3$. Thus, A is realizable over K_v only for primes v that divide 2. Since A is K-preadmissible, A is realizable over K_v for at least two primes $v = v_1, v_2$ of K that divide 2. Thus, there are epimorphisms $\psi_i : K^*_{v_i} \to A$, $i = 1, 2$.

Since A is not K-admissible, there is no epimorphism $\psi : C_K \to A$ that restricts to ψ_1, ψ_2 at v_1, v_2, respectively. We deduce from Corollary 1.1.2 and Remark 1.1.3 that:

(i) $K(\mu_{2^\infty})/K$ is non-cyclic and hence that (B1) holds,

(ii) $\emptyset \neq S_0 \subseteq S := \{v_1, v_2\}$.

Let us show that (B2) holds. Assume on the contrary that there is another prime v_3 such that A is realizable over K_{v_3} and fix an epimorphism $\psi_3 : K^*_{v_3} \to A$. Since $S_0 \neq \emptyset$, we can assume without loss of generality that $v_1 \in S_0 \subseteq S$. Then the set $S' := \{v_2, v_3\}$ does not contain S_0 and hence by Corollary 1.1.2 there is a $\psi : C_K \to A$ that restricts to ψ_2, ψ_3 at v_2, v_3, respectively. This contradicts the

assumption that A is not K-admissible. Thus, A is realizable over K_v only for $v = v_1, v_2$ and (B2) holds.

Let us show that (B3) holds. As $\emptyset \neq S_0 \subseteq S$, we have $1 \leq |S_0| \leq 2$. We claim that $|S_0| = 1$. Assume on the contrary that $|S_0| = 2$ and hence that $S_0 = S$. In particular $\sqrt{-1}, \eta_{s+1}, \sqrt{-1}\eta_{s+1} \notin K_{v_i}$, for $i = 1, 2$. Let $n_i := [K_{v_i} : \mathbb{Q}_2]$ and assume without loss of generality $n_1 \geq n_2$. We can then write

$$K^*_{v_2}/K^{*m}_{v_2} \cong C_m^{n_2+1} \times C_2, \tag{1.1.5}$$

$$K^*_{v_1}/K^{*m}_{v_1} \cong C_m^{n_2+1} \times C_2 \times C_m^{n_1-n_2} \cong K^*_{v_2}/K^{*m}_{v_2} \times C_m^{n_1-n_2}. \tag{1.1.6}$$

Let $\lambda_i := (2 + \eta_s)K^{*m}_{v_i}$, for $i = 1, 2$. Since λ_2 is not a square in $K^*_{v_2}/K^{*m}_{v_2}$, we can modify the isomorphism in (1.1.5) and (1.1.6) so that λ_2 corresponds to the element $(1, 0, \ldots, 0) \in C_m^{n_2+1} \times C_2$ in (1.1.5) and $\lambda_1 = (2 + \eta_s)K^{*m}_{v_1} \in K_{v_1}/K^{*m}_{v_1}$ corresponds to $(\lambda_2, 0, \ldots, 0) \in K^*_{v_2}/K^{*m}_{v_2} \times C_m^{n_1-n_2}$ in (1.1.6).

Since A is realizable over K_{v_2} there is an epimorphism $\psi_2 : K^*_{v_2} \to A$. We define an epimorphism $\psi_1 : K^*_{v_1} \to A$ using (1.1.6) to be ψ_2 on $K^*_{v_2}$ and 0 on $C_m^{n_1-n_2}$. In particular $\psi_1(2 + \eta_s) = \psi_2(2 + \eta_s)$.

Therefore $\pi_j \circ \psi_1(2+\eta_s)^{2^{k_j-1}} = \pi_j \circ \psi_2(2+\eta_s)^{2^{k_j-1}}$ is an element of order dividing 2 in $C_{2^{k_j}}$ and hence

$$\pi_j \circ \psi_1(2 + \eta_s)^{2^{k_j-1}} + \pi_j \circ \psi_2(2 + \eta_s)^{2^{k_j-1}} = 0, \tag{1.1.7}$$

for all $j = 1, \ldots, r$. By Corollary 1.1.2, (1.1.7) implies that there is an epimorphism $\psi : C_K \to A$ that restricts to ψ_1 at v_1 and to ψ_2 at v_2 and hence that A is K-admissible, contradiction. Thus, $S_0 = \{w\} \subseteq S$ and (B3) holds. Assume without loss of generality $w = v_1$.

It remains to show that one of the conditions (B4.a) or (B4.b) holds. Since A is not K-admissible there is no epimorphism $\psi : C_K \to A$ that restricts to an epimorphism at w and to ψ_2 at v_2. We deduce from Corollary 1.1.2, that for every epimorphism $\psi_w : K^*_w \to A$ there is a $j \in \{1, \ldots, r\}$ such that $\pi_j \circ \psi_w(2+\eta_s)^{2^{k_j-1}} \neq 0$. This shows that $\pi_j \circ \psi_w(2+\eta_s)$ is an element of order 2^{k_j} and hence a generator of $C_{2^{k_j}}$. Thus, $\psi_w(2 + \eta_s)$ is a generator of A.

It follows that for every epimorphism $\psi_w : K^*_w \to A$, $\psi_w(2 + \eta_s)$ is a generator of A of order greater than 2^s and hence by Lemma 1.1.7 one of conditions (B4.a) or (B4.b) must hold.

□

Examples

We shall construct examples of preadmissible groups that are not admissible over a field K that appears as a base field of an example of Wang [58, after Lemma 1].

Example 1.1.9. Let θ be a root of the polynomial $f(x) = x^3 + x + 8$. Let K be the number field $\mathbb{Q}(\theta)$ and A the abelian group $C_2 \times C_{2^k} \times C_{2^k}$ (for $k \geq 3$). Then A is K-preadmissible but A is not K-admissible.

Proof. First we note that $\sqrt{2}, \sqrt{-1}, \sqrt{-2} \notin K$ and hence $s = 2$. Using Newton's polygon one can observe that the polynomial f has a root over $\mathbb{Q}_2$ of the form -8ε where ε is a unit in $\mathbb{Q}_2$. Dividing f by $x + 8\varepsilon$ one has:

$$x^3 + x + 8 = (x + 8\varepsilon)(x^2 - 8\varepsilon x + 1 + 64\varepsilon^2). \tag{1.1.8}$$

The roots of the quadratic factor in (1.1.8) are $4\varepsilon \pm i\sqrt{1 + 48\varepsilon^2}$. As $1 + 48\varepsilon^2$ is a square in $\mathbb{Q}_2$ the splitting field over $\mathbb{Q}_2$ of the quadratic factor is $\mathbb{Q}_2(\sqrt{-1})$. Thus, K has two primes v and w that divide 2, for which $K_w \cong \mathbb{Q}_2$ and $K_v \cong \mathbb{Q}_2(\sqrt{-1})$. In particular, $S_0 = \{w\}$ and conditions (B1) and (B3) hold.

The maximal abelian group $A_{k,v}$ (resp. $A_{k,w}$) of exponent 2^k that is realizable over K_v (resp. K_w) is the maximal quotient of K_v^* (resp. K_w^*) of exponent 2^k. Therefore $A_{k,w} \cong A$ and $A_{k,v} \cong C_4 \times C_{2^k}^3$. In particular, A is realizable over K_v and K_w and hence K-preadmissible. Since A is not metacyclic it is not realizable over K_u for any prime u that does not divide 2 and (B2) holds.

In this example $A_s = C_2$ and $A'_s = C_{2^k} \times C_{2^k}$ and hence

$$\mathrm{rk}(A'_s) = [K_w : \mathbb{Q}_2] + 1 = 2.$$

Thus, (B4.b) holds.

Conditions (B1)-(B4) hold and hence, by Theorem 1.1.8, A is K-preadmissible but not K-admissible. □

Remark 1.1.10. (i) Since $\mathbb{Q}$ has only one even prime, all abelian $\mathbb{Q}$-preadmissible groups are $\mathbb{Q}$-admissible. Any quadratic extension $K/\mathbb{Q}$ either has only one prime that divides 2 or has two in which case $|S_0| = 2$. Thus, the smallest possible degree $[K : \mathbb{Q}]$ of a field K over which there are K-preadmissible groups that are not K-admissible is 3.

(ii) Since metacyclic abelian groups are realizable over completions at infinitely many primes, the smallest rank $\mathrm{rk}(A)$ of a K-preamissible group that is not K-admissible (over any number field) is 3. Since s was defined so that $s \geq 2$, a group A that is K-preadmissible but not K-admissible over some number field, must be of the form $A = A_s \oplus A'_s$ where $A_s \cong C_2$ or trivial and A'_s consists of summands of the form C_{2^k} where $k \geq 3$. Thus, $A = C_2 \times C_8 \times C_8$ is the smallest group that is K-preadmissible but not K-admissible over some number field K.

(iii) It follows that Example 1.1.9 for $k = 3$, has the minimal possible order $|A|$ and the minimal degree $[K : \mathbb{Q}]$.

Remark 1.1.11. For $k = 3$ in Example 1.1.9, it can be seen directly (without using Theorem 1.1.8) that $A = C_2 \times C_8 \times C_8$ is not K-admissible, as follows.

Assume on the contrary there is a K-adequate A-extension L/K. Since A is realizable over K_u only for $u = v, w$, it follows from Schacher's criterion that

$$\mathrm{Gal}(L_w/K_w) \cong A. \tag{1.1.9}$$

Since A is the maximal abelian group of exponent 8 realizable over $\mathbb{Q}_2$, the unique unramified cyclic 8-extension of $\mathbb{Q}_2$ corresponds to an extension Ω/K contained in L for which

$$\mathrm{Gal}(\Omega/K) \cong \mathrm{Gal}(\Omega_w/K_w) \cong C_8.$$

and Ω_w/K_w is the unramified 8-extension. Since $S_0 = \{w\}$, it follows from Remark 0.2.6 that there is no such field Ω, contradiction.

1.2 Examples in which preadmissibility implies admissibility

1.2.1 The Grunwald-Neukirch property

In this section we shall discuss the following property.

Definition 1.2.1. We say that a group G has the *Grunwald-Neukirch (GN) property* over a number field K if for every finite set S of primes of K and corresponding subgroups $G_v \leq G$, $v \in S$, such that G_v is realizable over K_v, there exists a G-extension L/K such that $\mathrm{Gal}(L_v/K_v) \cong G_v$ for all $v \in S$.

We shall discuss the implications of the GN-property on admissibility and show that it appears frequently.

If a group G has the GN-property over a number field K, the problem of determining whether a division algebra D with center K is a G-crossed product reduces to a local realization problem. Indeed, if G has the GN-property over K and D has Hasse invariants $\mathrm{inv}_u(D) = \frac{m_u}{n_u}$, $(m_u, n_u) = 1$, then D is a G-crossed product if and only if for every u there is a subgroup $G_u \leq G$ such that G_u is realizable over K_u and $n_u || G_u|$.

As to admissibility the GN-property implies the following proposition.

Definition 1.2.2. (see [1]) Let K be a field and G a finite group. Then G is called *infinitely often K-admissible* if there are fields $(L_r)_{r\in\mathbb{N}}$ such that $L_{r+1} \cap L_1 \cdots L_r = K$ and L_r is an adequate G-extension of K, for every $r \in \mathbb{N}$.

Proposition 1.2.3. *Let G be a group that has the GN-property over a number field K, the following conditions are equivalent:*

1. *G is K-preadmissible,*
2. *G is K-admissible,*
3. *G is infinitely often K-admissible,*
4. *there is a K-division algebra with infinitely many maximal (non-isomorphic) subfields Galois over K with Galois group G.*

To prove Proposition 1.2.3 we shall need several lemmas on preadmissibility. The goal of the first three lemmas is to show that the primes $v_i(p)$ in the definition of preadmissibility can be chosen to be distinct. The following lemma (see [30, Theorem 28]) is based on the description of tame local extensions (see Section 0.2.3). Let $\sigma_{t,n}$ be the automorphism of $\mathbb{Q}(\mu_n)$ for which $\sigma_{t,n}(\zeta) = \zeta^t$ for $\zeta \in \mu_n$.

Definition 1.2.4. Let M be a metacyclic group. Then there are $m, n, i, t \in \mathbb{Z}$ for which

$$M \cong \langle x, y | x^m = y^i, y^n = 1, x^{-1}yx = y^t \rangle, \tag{1.2.1}$$

and for which $t^m \equiv 1 (\mathrm{mod}\ n)$, $n|(t-1)i, 0 < t < n$. Denote such a presentation by

$$M = \mathcal{M}(m, n, i, t).$$

Lemma 1.2.5. (Liedahl [30]) *Let K a number field, G a finite group and P a p-Sylow subgroup of G. Assume there is a prime v of K that does not divide p and for which G is realizable over K_v. Then P is a metacyclic p-group with a presentation $\mathcal{M}(m, n, i, t)$ for which*

$$\sigma_{t,n} \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/(\mathbb{Q}(\mu_n) \cap K)). \tag{1.2.2}$$

Lemma 1.2.6. (Liedahl [30, Theorem 29]) *Let K be a number field and $P = \mathcal{M}(m, n, i, t)$ a p-group for which (1.2.2) holds. Then P is realizable over K_v for infinitely many primes v of K.*

Lemma 1.2.7. *Let G be a K-preadmissible group. Then there exist <u>distinct</u> primes $w_i(p)$, $i = 1, 2$, $p||G|$, and corresponding subgroups $G^{(i,p)}$ such that $G^{(i,p)}$ is realizable over $K_{w_i(p)}$ and contains a p-Sylow subgroup of G for every $i = 1, 2$, $p||G|$.*

Proof. For every $p||G|$, let $v_1(p), v_2(p)$ primes and $H^{(1,p)}, H^{(2,p)} \leq G$ subgroups such that $H^{(i,p)}$ is realizable over $K_{v_i(p)}$ and contains a p-Sylow subgroup of G. It follows from Lemma 1.2.5 that for a prime p for which $v_i(p)$ does not divide p for some $i = 1, 2$, the p-Sylow subgroups of G admit a presentation $\mathcal{M}(m, n, i, t)$ that satisfies (1.2.2). By Lemma 1.2.6, for such primes p, the p-Sylow subgroups of G are realizable over K_v for infinitely many v.

The primes $w_i(p)$ and subgroups $G^{(i,p)}$ can therefore be obtained using the following procedure. For every p for which both $v_1(p), v_2(p)$ divide p set $w_i(p) := v_i(p)$ and $G^{(i,p)} := H^{(i,p)}$, for $i = 1, 2$. For the rest of the primes, we can choose $G^{(i,p)}$ to be a p-Sylow subgroup $G(p)$ of G. Since for such p, $G(p)$ is realizable over K_v for infinitely many primes v, the primes $w_i(p)$ can be chosen to be distinct and not from the set $\{v_i(p) \mid p||G|, i = 1, 2\}$. □

We shall use the following lemma to produce adequate extensions that are disjoint from a given number field.

Lemma 1.2.8. *Let G be a group, K a number field and M/K a Galois extension. with Galois group $\Gamma = \mathrm{Gal}(M/K)$. Assume there is a set*

$$S = \{v_C | \ C \text{ is a cyclic subgroup of } \Gamma\}$$

of primes of K such that $\mathrm{Gal}(M_{v_C}/K_{v_C}) \cong C$ *for every cyclic subgroup* $C \leq \Gamma$. *Then every G-extension L/K in which the primes of S split completely is disjoint from M, i.e. $L \cap M = K$.*

Proof. Assume on the contrary there is a $\sigma \in \Gamma \setminus \mathrm{Gal}(M/(M \cap L))$. Then for $v = v_{\langle\sigma\rangle}$, we have $\mathrm{Gal}((M \cap L)_v/K_v) \neq \{1\}$ which contradicts the assumption that v splits completely in L. □

Note that by Chebotarev's density theorem for every cyclic $C \leq G$ there are infinitely many primes v of K for which $\mathrm{Gal}(M_v/K_v) = C$.

Proof of Proposition 1.2.3. Clearly (4) ⇒ (3) ⇒ (2) ⇒ (1). Let us show (1) ⇒ (4). By Lemma 1.2.7, there are distinct primes $v_i(p), p||G|, i = 1, 2$, and corresponding subgroups $G^{(i,p)} \leq G$ such that $G^{(i,p)}$ is realizable over $K_{v_i(p)}$ and contains a p-Sylow subgroup of G, for every $p||G|$, $i = 1, 2$.

For every $p||G|$, let p^{k_p} be the largest p-power dividing $|G|$. Let D be the K-division algebra with Hasse invariants

$$\mathrm{inv}_{v_1(p)}(D) = -\mathrm{inv}_{v_2(p)}(D) = \frac{1}{p^{k_p}}$$

for every $p||G|$ and $\mathrm{inv}_u(D) = 0$ if $u \notin \{v_i(p) \mid i \in \{1, 2\}, p||G|\}$.

Let $L_1, ..., L_r$ be a list of maximal subfields of D with Galois group $\mathrm{Gal}(L_i/K) = G$. Let $T = \{v_i(p) \mid i = 1, 2, p||G|\}$ and $S = \{v_C \mid C \leq G \text{ a cyclic subgroup}\}$ a (finite) set of primes such that $\mathrm{Gal}(M_{v_C}/K_{v_C}) = C$. Since G has the GN-property over K, there is a Galois G-extension $L_{r+1}/\mathbb{Q}$ such that for every $v_i(p) \in T$, $\mathrm{Gal}((L_{r+1})_{v_i(p)}/K_{v_i(p)}) = G^{(i,p)}$ and in which the primes of S split completely. By Lemma 1.2.8, L_{r+1} is disjoint from $L_1L_2...L_r$ over K. Thus, L_{r+1} is a G-extension of K and is contained in D, as a maximal subfield that is disjoint from $L_1...L_r$. Therefore (4) holds. □

The relationship between the GN-property, K-preadmissibility and K-admissibility is described in Figure 1.1. Note that there are K-admissible groups that do not admit the GN-property over K. Such examples can be obtained by considering abelian 2-groups that are realizable over K_v for more than two primes v, i.e. when Condition (A1) of Theorem 0.1.4 fails.

Examples

In [42], Saltman proves that a group that has a generic extension over K satisfies the GN-property over K. The family of generic groups contains:

1. ([42]) all abelian groups A of exponent that is not divisible by 8;
2. ([43]) all groups of order p^3 that are not the cyclic group of order 8, when $\mu_p \subseteq K$;
3. ([42]) the symmetric groups S_n;

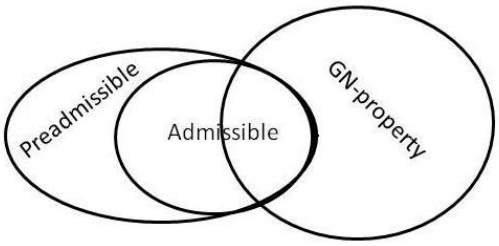

Figure 1.1: Relations between admissibility, preadmissibility and the GN-property

and has the following properties:

a. ([42]) if H and G have generic extensions over K then $H \wr G$ has a generic extension over K;

b. ([42]) if G has a generic extension, $N \lhd G$ and if the epimorphism $G \to G/N$ splits then G/N has a generic extension.

By iterating (a) and (b) on the groups in (1)-(3) one can obtain many examples of groups with the GN-property.

Although generic extensions is a rich source of examples, in what follows we shall study admissibility and the GN-property using the approach of embedding problems and the tools of Section 0.2.2.

The first immediate consequence from these powerful tools is that every group G of order prime to the number of roots of unity in K, has the GN-propoerty over K (see Corollary 0.2.8).

1.2.2 Admissibility in certain families of groups

The families

We shall consider admissibility for the following two families:

Definition 1.2.9. Let $\mathcal{SD}$ be the minimal family of groups such that $\{1\} \in \mathcal{SD}$ and if $H \in \mathcal{SD}$ and C a finite cyclic group, then every semidirect product $C \rtimes H$ is also in $\mathcal{SD}$.

Definition 1.2.10. Let $\mathcal{SC}$ be the minimal family of groups satisfying the following properties:

1. $\{1\} \in \mathcal{SC}$,
2. if $H \in \mathcal{SC}$ and C a finite cyclic group, then every semidirect product
$$C \rtimes H \in \mathcal{SC},$$
3. if $G \in \mathcal{SC}$ and $N \lhd G$, then $G/N \in \mathcal{SC}$.

We call such groups *semicyclic*.

Semicyclic groups are also characterized by the following proposition which is similar to a property proved by Dentzer (in [8]) for semiabelian groups.

Proposition 1.2.11. *A finite group G is semicyclic if and only if there exists a cyclic normal subgroup $C \lhd G$ and a proper semicyclic subgroup $H < G$ such that $G = CH$.*

Proof. First, assume there exist such subgroups C and H. Therefore there is a surjective homomorphism $\beta : C \rtimes H \to G$ where the action H on C is induced from the conjugation action in G. Thus, $G \cong (C \rtimes H)/ker\beta$ and G is semicyclic.

For the converse, let $G \neq \{1\}$ be semicyclic. There is a sequence $(H_i)_{i=1}^r$ such that $H_{i+1} = (C_i \rtimes H_i)/K_i$, $H_1 = \{1\}$, $H_r = G$. Assume $(H_i)_{i=1}^r$ is a sequence of shortest length satisfying the above properties. Then G is not a quotient of H_{r-1}, otherwise there would be a shorter sequence for G. The subgroups $C' = C_{r-1}K_{r-1}/K_{r-1}$, $H' = H_{r-1}K_{r-1}/K_{r-1}$ satisfy $C'H' = G$ and $C' \lhd G$. Since $H' \cong H_{r-1}/(H_{r-1} \cap K_{r-1})$ and since G is not a quotient of H_{r-1}, H' is a proper semicyclic subgroup of G. Therefore $G = C'H'$ is the required decomposition. □

As we have seen in Example 1.1.9, there are number fields K over which K-preadmissibility of 2-groups in $\mathcal{SD}$ does not imply K-admissibility. We shall therefore restrict our discussion on admissibility to odd order groups.

Remark 1.2.12. For an odd prime p, the smallest example of a p-group that is not semicyclic is the Hiesenberg group:

$$N = \langle x, y, z | x^p = y^p = z^p = 1, [x, y] = z, [x, z] = [y, z] = 1 \rangle.$$

However, all groups of order p^3 have the GN-property. Indeed, if $\mu_p \not\subseteq K$ this follows from Corollary 0.2.8 and if $\mu_p \subseteq K$ it follows from [42] (see examples in Section 1.2.1).

Admissibility in $\mathcal{SD}$

By iterating theorems 0.2.9 and 0.2.10, we obtain the following proposition:

Proposition 1.2.13. *Let K be a number field. An odd order group in $\mathcal{SD}$ has the GN-property over K.*

Proof. Let S be a finite set of primes of K. We argue by induction on $|G|$, where $G \in \mathcal{SD}$ is of odd order, that the map

$$\theta_G : \mathrm{Hom}(G_K, G)_{sur} \to \prod_{v \in S} \mathrm{Hom}(G_{K_v}, G)$$

is surjective. This will clearly imply our claim.

The induction assertion holds for $G = \{1\}$. Let $G = C \rtimes H$ for $H \in \mathcal{SD}$ and $C \neq \{1\}$ a cyclic group (of odd order). Let $\pi : G \to H$ be the natural map.

Fix an element $(f_v)_{v\in S} \in \prod_{v\in S} \mathrm{Hom}(G_{K_v}, G)$. By induction the map

$$\theta_H : \mathrm{Hom}(G_K, H)_{sur} \to \prod_{v\in S} \mathrm{Hom}(G_{K_v}, H),$$

is surjective and therefore the element

$$(h_v)_{v\in S} = (\pi \circ f_v)_{v\in S} \in \prod_{v\in S} \mathrm{Hom}(G_{K_v}, H), \tag{1.2.3}$$

has a source under θ_H. We consider the following embedding problem (in the abstract setup)

$$\begin{array}{ccccc} & & G_{K_v} & & \\ & & \downarrow{\scriptstyle h_v} & & \\ G & \xrightarrow{\pi} & H & \longrightarrow & 0, \end{array} \tag{1.2.4}$$

and apply theorems 0.2.9 and 0.2.10 (see Remark 1.2.4). Since C is cyclic of odd order, it follows from Theorem 0.2.10.(e) that the map

$$\mathrm{H}^1(G_K, C) \to \prod_{v\in S} \mathrm{H}^1(G_{K_v}, C)$$

is surjective. Since π splits, (1.2.4) has a solution for every prime v. Thus, by Theorem 0.2.9, θ_G^H is surjective. Since f_v is a solution to the embedding problem (1.2.4) for every $v \in S$, $(f_v)_{v\in S}$ is in the image of θ_G^H and hence of θ_G. □

Admissibility for semicyclic groups

Let us consider admissibility for a subfamily of odd order semicyclic K-preadmissible groups.

Let p be an odd prime, v a prime of K that divides p, $M_p(K_v)$ the maximal pro-p extension of K_v and $\mathfrak{G}_{K_v} = \mathrm{Gal}(M_p(K_v)/K_v)$. See Section 0.2.3 for a description of $\mathfrak{G}_{K_v}$. If $\mu_p \not\subseteq K_v$ then $\mathfrak{G}_{K_v}$ is a free pro-p group of rank $N_v := [K_v : \mathbb{Q}_p] + 1$.

If $\mu_p \subseteq K_v$, the degree $[K_v : \mathbb{Q}_p]$ is even and we define $N_v := \frac{[K_v:\mathbb{Q}_p]+2}{2}$. In such a case $\mathfrak{G}_{K_v}$ is a pro-p group generated by $x_1, ..., x_{2N_v}$ with one relation (see Section 0.2.3):

$$x_1^q [x_1, x_2] \dots [x_{2N_v-1}, x_{2N_v}].$$

By sending $x_i \to 1$ for every odd i, one obtains an epimorphism $\mathfrak{G}_{K_v} \to F_p(N_v)$ onto the free pro-p group on N_v-generators. In fact, N_v is the maximal rank of a free pro-p quotient of $\mathfrak{G}_{K_v}$ (see [54]). Let

$$N_p = \max_{v_i, v_j | p} \{\min\{N_{v_i}, N_{v_j}\}\}, \tag{1.2.5}$$

where v_i, v_j are distinct primes of K that divide p. If p does not decompose in K, set $N_p = 1$.

All p-groups of rank $\leq N_p$ are clearly K-preadmissible. Furthermore, every group G whose p-Sylow subgroups are of rank $\leq N_p$, for every $p||G|$, is K-preadmissible. We shall prove that every such semicyclic group of odd order is in fact K-admissible.

Proposition 1.2.14. *Let G be a semicyclic group of odd order whose p-Sylow subgroups are generated by at most N_p generators, for every $p||G|$. Then G is K-admissible.*

Proposition 1.2.14 essentially follows from the following lemma. Denote the set of homomorphisms $\{\pi : G_{K_v} \to G\}$ that split through a free pro-p group (and hence through a free pro-p group of rank $\leq N_v$) by $S_v(G)$.

Lemma 1.2.15. *For every odd order semicyclic group G and every finite set S of primes of K,*

$$\prod_{v\in S} S_v(G) \subseteq \mathrm{Im}(\theta_G). \tag{1.2.6}$$

Remark 1.2.16. In the proof we shall use the fact that the free pro-p group F is projective in the category of profinite groups (not only in the category of pro-p groups). Indeed given a p-group P and two epimorphisms $\phi : F \to P, \psi : G \to P$, there is a p-Sylow subgroup $G(p) \leq G$ that maps under ψ onto P. One can therefore lift ϕ to a homomorphism $\widetilde{\phi} : F \to G(p)$ such that $\widetilde{\phi} \circ \psi = \phi$.

Proof of Lemma 1.2.15. We argue by induction on $|G|$ for semicyclic groups G of odd order.

The claim holds for $G = \{1\}$. Let G be a non-trivial semicyclic group of odd order. By Proposition 1.2.11, $G = CH$ for $C \lhd G$ and a proper semicyclic subgroup $H < G$. By induction our claim holds for H. We shall deduce the claim for G in two steps. In step I we prove the claim for $\hat{G} = C \rtimes H$ and in step II for G.

Step I: Let $\pi : \hat{G} \to H$ be the natural map. Fix an element

$$(g_v)_{v\in S} \in \prod_{v\in S} S_v(\hat{G}).$$

Then $f_v = \pi \circ g_v$ also splits through a free pro-p group. Thus, $(f_v)_{v\in S} \in \prod_{v\in S} S_v(H)$. By the induction hypothesis there is an epimorphism $f : G_K \to H$ such that $\theta_H(f) = (f_v)_{v\in S}$. By definition of f_v, the diagram:

$$\begin{array}{ccccc} & & & & G_{K_v} \\ & & & \swarrow^{g_v} & \downarrow{\scriptstyle f_v} \\ \hat{G} & \xrightarrow{\pi} & H & \longrightarrow & 0, \end{array} \tag{1.2.7}$$

is commutative. By Theorem 0.2.10.(e) the map

$$\mathrm{H}^1(G_K, C) \to \prod_{v\in S} \mathrm{H}^1(G_{K_v}, C)$$

is surjective. Since π splits the embedding problem (1.2.7) has a solution for all primes v. Therefore we may apply Theorem 0.2.9 and deduce that the map

$$\theta^H_{\hat{G}} : \mathrm{Hom}_H(G_K, \hat{G})_{sur} \to \prod_{v\in S} \mathrm{Hom}_H(G_{K_v}, \hat{G})$$

is surjective. Since $(g_v)_{v\in S} \in \prod_{v\in S} \mathrm{Hom}_H(G_{K_v}, \hat{G})$ it follows that $\theta_{\hat{G}}^{-1}((g_v)_{v\in S}) \neq \emptyset$. Thus, $\prod_{v\in S} S_v(\hat{G}) \subseteq \mathrm{Im}(\theta_{\hat{G}})$.

Step II: Let $\pi : \hat{G} \to G$ be the natural map and K its kernel. Fix an element $(g_v)_{v\in S} \in \prod_{v\in S} S_v(G)$. We shall make use of the following maps:

$$\pi_* : \mathrm{Hom}(G_K, \hat{G}) \to \mathrm{Hom}(G_K, G),$$

$$\pi_*(v) : \mathrm{Hom}(G_{K_v}, \hat{G}) \to \mathrm{Hom}(G_{K_v}, G)$$

and the induced map

$$\widetilde{\pi}_*(v) : S_v(\hat{G}) \to S_v(G)$$

for $v \in S$. The map $\widetilde{\pi}_*(v)$ is surjective since by Remark 1.2.16, every $f_v : G_{K_v} \to G$ that splits through $F_p(N_v)$ can be lifted to $\widetilde{f}_v : G_{K_v} \to \hat{G}$ as described in the following diagram:

$$\begin{array}{ccccc} & & G_{K_v} & & \\ & & \downarrow & & \\ & & F_p(N_v) & & \\ & \swarrow & \downarrow & & \\ \hat{G} & \xrightarrow{\pi} & G & \longrightarrow & 0. \end{array}$$

It follows that the map $\prod_{v\in S} \widetilde{\pi}_*(v)$ is surjective and hence that there is an element $(\widetilde{g}_v)_{v\in S} \in \prod_{v\in S} S_v(\hat{G})$ for which $(\prod_{v\in S} \widetilde{\pi}_*(v))((\widetilde{g}_v)_{v\in S}) = (g_v)_{v\in S}$. Since $\prod_{v\in S} S_v(\hat{G}) \subseteq \mathrm{Im}(\theta_{\hat{G}})$, there is an element $\widetilde{g} : G_K \to \hat{G}$ for which

$$(\prod_{v\in S} \pi_*(v)) \circ \theta_{\hat{G}}(\widetilde{g}) = (g_v)_{v\in S}.$$

Since the following diagram

$$\begin{array}{ccc} \mathrm{Hom}(G_K, \hat{G})_{sur} & \xrightarrow{\pi_*} & \mathrm{Hom}(G_K, G)_{sur} \\ \downarrow{\scriptstyle \theta_{\hat{G}}} & & \downarrow{\scriptstyle \theta_G} \\ \prod_{v\in S} \mathrm{Hom}(G_{K_v}, \hat{G}) & \xrightarrow{\prod_{v\in S} \pi_*(v)} & \prod_{v\in S} \mathrm{Hom}(G_{K_v}, G) \end{array}$$

is commutative, we have $(\theta_G \circ \pi_*)(\widetilde{g}) = (g_v)_{v\in S}$ and $(g_v)_{v\in S} \in \mathrm{Im}(\theta_G)$. □

Proof of Corollary 1.2.14. Let S be the set of primes $p||G|$ such that $N_p > 1$. For $p \in S$, let $v_1(p)$, $v_2(p)$ be two primes of K that divide p, for which $N_{v_1(p)}, N_{v_2(p)} \geq N_p$. In particular, $N_p = \min\{N_{v_1(p)}, N_{v_2(p)}\}$. For such p, every p-Sylow subgroup $G(p)$ of G is generated by at most N_p generators and hence we have an epimorphism $f_{v_i(p)} \in S_{v_i(p)}(G(p))$, for $i = 1, 2$.

By Lemma 1.2.15, there is an epimorphism $f \in \mathrm{Hom}(G_K, G)$ whose restriction to $G_{K_{v_i(p)}}$ is $f_{v_i(p)}$ for every $p \in S$ and $i = 1, 2$. Thus, the fixed field M of $\ker(f)$ has Galois group $\mathrm{Gal}(M/K) \cong G$ and local Galois groups

$$\mathrm{Gal}(M_{v_i(p)}/K_{v_i(p)}) \cong G(p)$$

for every $p \in S$ and $i = 1, 2$.

For every prime $p||G|$ that is not in S, we have $N_p(K) = 1$. Thus, for such p the p-Sylow subgroups $G(p)$ of G are cyclic and by Chebotarev's density theorem there are infinitely many primes v of K for which $\mathrm{Gal}(M_v/K_v) \cong G(p)$. We conclude that M/K is K-adequate and G is K-admissible. $\square$

Chapter 2

Tame admissibility of Sylow metacyclic groups

If K is a number field different from $\mathbb{Q}$, then the set of K-preadmissible groups is much larger than the set of groups with metacyclic Sylow subgroups. We will explain this sharp difference using the notions of tame and wild admissibility defined below.

In this chapter, we shall focus on studying tame admissibility. Tame admissibility describes the kind of admissibility we meet over $\mathbb{Q}$ and the phenomenon that occurs in Corollary 0.1.7. We shall prove that a solvable group G is tamely K-admissible if and only if its p-Sylow subgroups admit a presentation

$$\langle x, y | x^m = y^i, y^n = 1, x^{-1}yx = y^t \rangle$$

such that $\sigma_{t,n} \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/(\mathbb{Q}(\mu_n) \cap K))$, for every $p||G|$. This assertion is a strengthening of Theorem 0.1.6. We shall then describe the relationship between the various types of admissibility.

2.1 Tame admissibility

In this section we shall define tame and wild admissibility and discuss their basic properties.

Let K be a number field and L/K a Galois extension. The Brauer group $\mathrm{Br}(K)$ has the following well known characterization in terms of Hasse invariants,

$$0 \to \mathrm{Br}(K) \to \bigoplus_{v \in P_{fin}} \mathbb{Q}/\mathbb{Z} \bigoplus_{v \in P_{real}} \tfrac{1}{2}\mathbb{Z}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where P_{fin} is the set of finite primes of K, P_{real} is the set of real primes of K, the first map is $\bigoplus_{v \in P_{fin} \bigcup P_{real}} \mathrm{inv}_v$ and the second is summation. Denote $P = P_{fin} \bigcup P_{real}$.

Let $\alpha \in \mathrm{Br}(K)$ and for $v \in P$ denote $\mathrm{inv}_v(\alpha) = \frac{a_v}{b_v}$ where $(a_v, b_v) = 1$. Then L splits α if and only if $b_v | [L_v : K_v]$ for all $v \in P$. Thus one has the following isomorphism:

$$\mathrm{Br}(L/K) \cong (\bigoplus_{v\in P}(\frac{1}{[L_v : K_v]}\mathbb{Z})/\mathbb{Z})_0, \tag{2.1.1}$$

where $(\cdot)_0$ denotes that the sum of invariants is zero.

Definition 2.1.1. The *locally tamely ramified (relative) Brauer group* $\mathrm{Br}(L/K)_{tr}$ is the subgroup of $\mathrm{Br}(L/K)$ that corresponds to

$$(\bigoplus_{v\in P}\frac{1}{[L_v \cap (K_v)_{tr} : K_v]}\mathbb{Z}/\mathbb{Z})_0, \tag{2.1.2}$$

under the isomorphism in (2.1.1), i.e. the subgroup that is split by the tamely ramified part of every completion of L/K.

This group contains the subgroup $\mathrm{Br}(L/K)_{un}$ that is similarly defined in [11].

Recall the a field $L \supseteq K$ is called K-adequate if it is contained in a division algebra with center K as a maximal subfield. In [44, Proposition 2.5], Schacher proved that L is K-adequate if and only if $\mathrm{Br}(L/K)$ has an element of order $[L : K]$. Along these lines we define tame adequacy as follows:

Definition 2.1.2. Let L/K be finite Galois extension of number fields. We say L is *tamely K-adequate* if there is an element of order $[L : K]$ in $\mathrm{Br}(L/K)_{tr}$.

Example 2.1.3. Let $p = 2$, $K = \mathbb{Q}$ and $L = K(\sqrt{3})$. So, L/K is a C_2-extension in which 2 is wildly ramified. Nevertheless, as we shall now see, L is tamely K-adequate. Let $v_1 = (5)$ and $v_2 = (7)$ be two primes of K. Both v_1 and v_2 are inert in L. Let α be an element of $\mathrm{Br}(K)$ with invariants

$$\mathrm{inv}_{v_1}(\alpha) = 1/2, \mathrm{inv}_{v_2}(\alpha) = -1/2, \mathrm{inv}_u(\alpha) = 0 \text{ for any } u \neq v_1, v_2.$$

Then α is an element of exponent 2 in $\mathrm{Br}(L/K)_{tr}$ and hence L is tamely K-adequate.

Definition 2.1.4. Let K be a number field and G a finite group. We say that G is *tamely K-admissible* if there is a tamely K-adequate field L which is Galois over K with Galois group $\mathrm{Gal}(L/K) \cong G$.

The following Lemma characterizes tame K-adequacy in a language of fields. The proof is based on the proof of [44, Proposition 2.5].

Lemma 2.1.5. *Let K be a number field and G a finite group. A G-extension L/K is tamely K-adequate if and only if for every $p||G|$ there are two primes $v_1(p), v_2(p)$ of K that do not divide p and for which $\mathrm{Gal}(L_{v_i(p)}/K_{v_i(p)})$ contains a p-Sylow subgroup of G, for $i = 1, 2$.*

Proof. For $p||G|$, let r_p be the largest integer for which $p^{r_p}||G|$. For the "if" part assume that for every $p||G|$ there are two primes $v_1(p), v_2(p)$ for which $\mathrm{Gal}(L_{v_i(p)}/K_{v_i(p)})$

contains a p-Sylow subgroup of G and hence $p^{r_p}|[L_{v_i(p)} : K_{v_i(p)}]$ for $i = 1, 2$. Let α_p be the element of $\mathrm{Br}(K)$ whose invariants are:

$$\mathrm{inv}_{v_1(p)}(\alpha_p) = \frac{1}{p^{r_p}}, \mathrm{inv}_{v_2(p)}(\alpha_p) = -\frac{1}{p^{r_p}}$$

and $\mathrm{inv}_v(\alpha_p) = 0$ for any other prime v. Let $\alpha = \otimes_{p||G|}\alpha_p$, where the tensor product is over K. Since $\exp(\alpha) = \mathrm{lcm}_p(\exp(\alpha_p))$, we have $\exp(\alpha) = |G|$. Since $v_1(p), v_2(p)$ do not divide p, $\alpha_p \otimes_K K_v$ is split by the tamely ramified part of L_v/K_v for every prime v. It follows that $\alpha \otimes K_v$ is split by the tamely ramified part of L_v/K_v for all primes v and hence that $\alpha \in \mathrm{Br}(L/K)_{tr}$. As $\alpha \in Br(L/K)_{tr}$ and $\exp(\alpha) = |G|$, L/K is tamely K-adequate.

For the "only if" part assume there is an $\alpha \in \mathrm{Br}(L/K)_{tr}$ of exponent $|G|$. Thus for every prime $p||G|$, there is a prime $w_1(p)$ such that $\alpha \otimes_K K_{w_1(p)}$ is of exponent divisible by p^{r_p} and hence $\mathrm{Gal}(L_{w_1(p)}/K_{w_1(p)})$ contains a p-Sylow subgroup of G. Since the sum of invariants of an element in $\mathrm{Br}(K)$ is zero, there is at least one more prime $w_2(p)$ for which $\alpha \otimes_K K_{w_2(p)}$ is of exponent divisible by p^{r_p}. In particular, $\mathrm{Gal}(L_{w_2(p)}/K_{w_2(p)})$ contains a p-Sylow subgroup of G. Since $\alpha \in \mathrm{Br}(L/K)_{tr}$, the tamely ramified part of $L_{w_i(p)}/K_{w_i(p)}$ splits $\alpha \otimes_K K_{w_i(p)}$ for $i = 1, 2$. Therefore if $w_1(p), w_2(p)$ do not divide p, we are done. Let us assume that one of these primes say $w := w_1(p)$ divides p.

Let P be a p-Sylow subgroup of G that is contained in $\mathrm{Gal}(L_w/K_w)$. Let $F_w = L_w^P$. Then the tamely ramified part of L_w/F_w splits $\alpha \otimes_K F_w$. In particular the unramified part of L_w/F_w splits $\alpha \otimes_K F_w$. But since $\exp(\alpha \otimes_K F_w) = p^{r_p} = [L_w : F_w]$, the extension L_w/F_w must be the unramified p^{r_p}-extension of F_w which is cyclic. It follows that the p-Sylow subgroups of G are cyclic. By Chebotarev's density theorem there are infinitely many primes v at which $\mathrm{Gal}(L_v/K_v)$ is isomorphic to the cyclic group P. In particular, there are two primes $v_1(p), v_2(p)$ that do not divide p and for which $\mathrm{Gal}(L_v/K_v)$ is a p-Sylow subgroup of G.

□

For some of our arguments it will be possible to relax the tame admissibility condition and require instead the following notion of non-wild admissibility.

Definition 2.1.6. Let L/K be a G-extension. We call L *wildly K-adequate* if L is K-adequate and there is a prime $p||G|$ for which $\mathrm{Gal}(L_v/K_v)$ contains a p-Sylow subgroup of G only for primes v that divide p.

A G-extension L/K is called *non-wildly K-adequate* if L is K-adequate but not wildly K-adequate. We call a group G *non-wildly K-admissible* if there is a non-wildly K-adequate G-extension.

Clearly if L/K is tamely K-adequate then L/K is non-wildly K-adequate. Note that Definition 2.1.6 and the characterization of tame K-admissibility in Lemma 2.1.5 are not negations of each other. We do not know of an example in which a group is non-wildly K-admissible and not tamely K-admissible.

As a corollary to Lemma 1.2.5 we have:

Corollary 2.1.7. *Let G be a non-wildly K-admissible group. Then for every $p||G|$, the p-Sylow subgroups of G admit a presentation $\mathcal{M}(m,n,i,t)$ for which $\sigma_{t,n} \in \mathrm{Gal}(K/(\mathbb{Q}(\mu_n) \cap K))$.*

Proof. Let L/K be a non-wildly K-adequate G-extension. Then for every prime $p||G|$, there is at least one prime v of K that does not divide p and for which $\mathrm{Gal}(L_v/K_v)$ contains a p-Sylow subgroup P of G. By Lemma 1.2.5, this implies that P is metacyclic and admits the required presentation. □

2.2 Refined $\mathbb{Q}$-admissibility

In sections 2.3.1 and 2.3.2, we shall describe the solvable tamely K-admissible groups, the solvable non-wildly K-admissible groups and prove Theorem 0.1.6. The main tool we shall use is a refinement of Theorem 0.1.5 (namely Theorem 2.2.3 below). For this we shall need the following two definitions:

Definition 2.2.1. Let G be a group and for every p let $G(p)$ be a p-Sylow subgroup of G. We call a set $T = \{v_i(p) \mid p||G|,\ i = 1,2\}$ of rational primes a *tame supporting set of primes for G* if the following conditions hold:

1. for every $p||G|$, there exists a presentation $\mathcal{M}(m,n,i,t)$ of the p-Sylow subgroups of G such that $v_1(p) \equiv v_2(p) \equiv t \pmod{n}$,
2. $v_i(p) = v_j(q)$ only if $p = q$ and $i = j$,
3. $v_i(p) \neq 2$ for all $p||G|, i = 1,2$.

Definition 2.2.2. Let $E/\mathbb{Q}$ be a Galois G-extension and T a tame supporting set of primes for G. We say that E is *compatible with the set T* if for every $p||G|$ and $v_i(p) \in T$, $\mathrm{Gal}(E_{v_i(p)}/\mathbb{Q}_{v_i(p)})$ contains a p-Sylow subgroup of G.

We shall call a group *Sylow metacyclic* if it has metacyclic Sylow subgroups.

Theorem 2.2.3. *Let G be a solvable Sylow metacyclic group and S a finite set of odd rational primes. Let T be a tame supporting set of primes for G that is disjoint from S. Then there is a Galois G-extension $L/\mathbb{Q}$ compatible with T (and hence $\mathbb{Q}$-adequate) in which every prime of S splits completely.*

The proof of Theorem 2.2.3 is an adaptation of the proofs of [50, Theorem 1], [6, Theorem 2.1] and [51, Theorem 1]. In Section 2.2.1, Theorem 2.2.3 is proved for metacyclic 2-groups. In Section 2.2.3, these metacyclic 2-groups are embedded into $\{2,3\}$-groups, i.e. groups of order 2^a3^b, and Theorem 2.2.3 is proved for such groups. In Section 2.2.4 these $\{2,3\}$-groups are embedded into Sylow metacyclic groups of arbitrary order and complete the proof of Theorem 2.2.3.

2.2.1 Admissibility of metacyclic 2-groups

As in Section 0.2.2 in what follows we fix an embedding of an algebraic closure of $\mathbb{Q}$ into an algebraic closure of $\mathbb{Q}_p$ for every rational prime p.

The following lemma is Theorem 2.2.3 for metacyclic 2-groups and its proof is an adaptation of [50, Theorem 1].

Lemma 2.2.4. *Let G be a metacyclic 2-group, S a set of odd rational primes and $T = \{v_1(2), v_2(2)\}$ a tame supporting set for G that is disjoint from S. Then there is a $\mathbb{Q}$-adequate G-extension M that is compatible with T and in which all primes of S split completely.*

Proof. First we show that we can assume G has a presentation:

$$G = \mathcal{M}(m, n, 0, t) = \langle x, y | x^m = y^n = 1, x^{-1}yx = y^t \rangle,$$

such that $v_i(2) \equiv 1 \pmod{n}$, for $i = 1, 2$.

Every metacyclic 2-group

$$H = \mathcal{M}(m, n, i, t)$$

is a quotient of a 2-group $G = \mathcal{M}(mo, n, 0, t)$ where o is the order of y^i in H. Note that o is a 2-power and hence G is a 2-group as well. Since G has the same parameters t, n as H, the tame supporting set $\{v_1, v_2\}$ of primes for H is also a tame supporting set for G. Thus it suffice to prove the claim for G.

Fix a presentation $G = \mathcal{M}(m, n, 0, t)$ for which $v_i(p) \equiv t \pmod{n}$, $i = 1, 2$. Let x, y be the generators in the presentation $\mathcal{M}(m, n, 0, t)$. Since $2 \notin S \cup T$, $(\mathbb{Q}, m, S \cup T)$ does not fall into a special case and we may apply the Grunwald-Wang theorem (see Corollary 0.2.3). Thus, there is a cyclic C_m-extension $k/\mathbb{Q}$ for which

(A1) the primes of S split completely in k,

(A2) for every $q \in T$, $k_q/\mathbb{Q}_q$ is the unramified C_m-extension of $\mathbb{Q}_q$.

Condition (A2) guarantees that $k/\mathbb{Q}$ is compatible with T.

Since $v_i(2) \equiv t \pmod{n}$, we have $v_i(2)^m \equiv 1 \pmod{n}$ and therefore $\mu_n \subseteq k_{v_i(2)}$. Thus, $M_i := k_{v_i(2)}(v_i(2)^{\frac{1}{n}})$ is Galois over $\mathbb{Q}_{v_i(2)}$. Let ϕ be the Frobenious automorphism of $v_i(2)$ in $k/\mathbb{Q}$ and τ a generator of $\mathrm{Gal}(M_i/k_{v_i(2)})$. Then by [60],

$$\phi^{-1}\tau\phi = \tau^{v_i(2)} = \tau^t$$

and hence $\mathrm{Gal}(M_i/k_{v_i(2)}) \cong G$.

Consider the embedding problem $G \to \mathrm{Gal}(k/\mathbb{Q})$ with the following prescribed local conditions on a solution M at the primes of $S' := S \cup \{v_1(2), v_2(2)\}$:

(B1) for every prime $v \in S$, $M_v = \mathbb{Q}_v$, i.e. v splits completely in M,

(B2) $M_{v_i(2)} = M_i$ for $i = 1, 2$.

Let $\Gamma := \mathrm{Gal}(k/\mathbb{Q})$, $A := \langle y \rangle$ and $\pi : G \to \Gamma$ an epimorphism with kernel A. In order to find a field M that satisfies (B1) and (B2) it suffices to show that the map $\theta_G^\Gamma(S')$ defined in Section 0.2.2 is surjective. For this, as in [50], we apply Theorem 0.2.9.

The embedding problem $G \to \mathrm{Gal}(k/\mathbb{Q})$ is split and therefore has a trivial solution. In particular $\mathrm{Hom}_\Gamma(G_K, G) \neq \emptyset$. To show that the map

$$\mathrm{H}^1(G_\mathbb{Q}, A) \to \prod_{v \in S'} \mathrm{H}^1(G_{\mathbb{Q}_v}, A) \tag{2.2.1}$$

is surjective we apply Theorem 0.2.10.(b).

As in Theorem 0.2.10, let A' be the dual $G_\mathbb{Q}$-module, $G'_\mathbb{Q}$ the subgroup of $G_\mathbb{Q}$ that fixes A', $k' := \mathbb{Q}(A')$ the fixed field of $G'_\mathbb{Q}$, $G' = \mathrm{Gal}(k'/\mathbb{Q})$ and for a rational prime v, let $G'_v = \mathrm{Gal}(k'_v/\mathbb{Q}_v)$.

Let H_1 (resp. H_2) be the subgroup of $G_\mathbb{Q}$ that fixes A (resp. μ_n) and k_1 the fixed field of H_1. The fixed field of $H_1 \cap H_2$ is $k_1(\mu_n)$. As k_1 is a subfield of k we have $k_1(\mu_n) \subseteq k(\mu_n)$. Since $H_1 \cap H_2$ acts trivially on A', $H_1 \cap H_2 \subseteq G'_\mathbb{Q}$ and hence $k' \subseteq k(\mu_n)$.

In particular for $v \in T$, one has $k'_v \leq (k(\mu_n))_v = k_v(\mu_n) = k_v$ and hence G'_v is cyclic. For $v \in S$, one has $k'_v \leq (k(\mu_n))_v = k_v(\mu_n) = \mathbb{Q}_v(\mu_n)$. As n is a 2-power and $2 \notin S$, $\mathrm{Gal}(\mathbb{Q}_v(\mu_n)/\mathbb{Q}_v)$ and hence G'_v are cyclic for all $v \in S$. Thus, G'_v is cyclic for every $v \in S'$ and we may apply Theorem 0.2.10.(b).

Therefore the map (2.2.1) is surjective and we may apply Theorem 0.2.9. It follows that there is a field $M \supseteq k$ with Galois group $\mathrm{Gal}(M/\mathbb{Q}) \cong G$ in which all primes of S splits completely and such that $M_{v_i(2)} = k_{v_i(2)}(v_i(2)^{\frac{1}{n}})$ for $i = 1, 2$. This completes the proof. □

2.2.2 Solvable Sylow metacyclic $\{2, 3\}$-groups

In this section we summarize some properties of $\{2, 3\}$-groups that are used in the proof of Theorem 2.2.3. These properties are all given in [51].

Let G be a solvable Sylow metacyclic $\{2, 3\}$-group. Let $G(p)$ denote a p-Sylow subgroup of G and $G(p) = \mathcal{M}(m_p, n_p, i_p, t_p)$ a presentation of $G(p)$ for $p = 2, 3$. Let $F = F(G)$ be the Fitting subgroup of G (the maximal normal nilpotent subgroup of G) and $F(p)$ the p-Sylow subgroup of F, for $p = 2, 3$. The proof requires understanding the structure of $G/F, F(2)$ and $G/F(3)$ when $G(3)$ is not a normal subgroup of G.

Assume $G(3)$ is not a normal subgroup of G. Then by [51], G/F is isomorphic to S_3 or A_3 and $F(2)$ is either the quaternion group Q_8 or a group of the form $C_{2^u} \times C_{2^u}$, i.e. a homocyclic group. The following cases cover all possibilities:

Case 1.1. $G/F \cong A_3$ and $F(2) \cong C_{2^u} \times C_{2^u}$. In such a case $G/(F(3))$ is the unique extension of $C_{2^u} \times C_{2^u}$ by a non trivial automorphism of order 3.

Case 1.2. $G/F \cong A_3$ and $F(2) \cong Q_8$. In such a case $G/(F(3)) \cong SL_2(3)$ (the unique extension of Q_8 by a non trivial automorphism of order 3).

Case 2.1. $G/F \cong S_3$ and $F(2)$ is homocyclic. Then $F(2) \cong C_2 \times C_2$ and

$$G/(F(3)) \cong S_4.$$

Case 2.2. $G/F \cong S_3$, $F(2) \cong Q_8$. Then $G/(F(3))$ is one of the two central extensions of S_4 with kernel C_2, denoted by S_4^* and S_4^{**}. The groups S_4^* and S_4^{**} have metacyclic 2-Sylow subgroups that are isomorphic to

$$Q_{16} = \langle x, y | x^2 = y^4, y^8 = 1, x^{-1}yx = y^7 \rangle \tag{2.2.2}$$

and

$$D_{16}^* = \langle x, y | x^2 = y^8 = 1, x^{-1}yx = y^3 \rangle, \tag{2.2.3}$$

respectively.

In the above cases the 2-Sylow subgroups of $G/(F(3))$ all have unique parameters m, n, t [1] that are described in the following lemma that is based on [30].

Lemma 2.2.5. *Let $G \cong \mathcal{M}(m, n, i, t)$.*

1. *If $G \cong C_{2^u} \times C_{2^u}$ then $m = 2^u, n = 2^u, t = 1$.*
2. *If $G \cong Q_8$ then $m = 2, n = 4, t = 7$.*
3. *If $G \cong D_{16}^*$ then $m = 2, n = 8, t = 3$.*
4. *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 $t = 1$.

(2)–(4) are conclusions from Theorem 22, Case 3 in [30]. In Theorem 22, Liedahl gives necessary and sufficient conditions on a presentation $\mathcal{M}(m, n, i, t)$ for a group as in one of the cases (2)–(4) to have an equivalent presentation with other parameters, but these conditions require $m \geq 4$ which fails for the presentations in (2)–(4). □

2.2.3 Admissibility of Sylow metacyclic $\{2, 3\}$-groups

In this section we prove Theorem 2.2.3 for $\{2, 3\}$-groups (Proposition 2.2.8). The proof is an adaptation of Sonn's proof of [51, Theorem 3] and requires the following lemmas:

Lemma 2.2.6. *Let G be a finite group and $K/\mathbb{Q}$ a Galois extension such that $L_0 := K(\sqrt{\eta})/\mathbb{Q}$, for $\eta \in K$, is a Galois G-extension of $\mathbb{Q}$. Let S be a finite set of primes of $\mathbb{Q}$ that split completely in K and W a finite set of rational primes that is disjoint from S. Then there is a rational integer m for which $L = K(\sqrt{m\eta})$ is Galois over $\mathbb{Q}$ and satisfies:*

(1) $\mathrm{Gal}(L/\mathbb{Q}) \cong G$,

(2) *every prime of S splits completely in L,*

(3) *for every prime $p \in W$, $L_p = (L_0)_p$.*

[1] The parameter i is also unique up to multiplication by an odd number.

Proof. By Proposition 2.5 in [53], for every L of the form $L = K(\sqrt{m\eta})$ either $L = K$ or L has Galois group

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{Gal}(L_0/\mathbb{Q}).$$

We shall choose an m such that $L \neq K$ and satisfies (2) and (3).

Let $q \neq 2$ be a prime that splits completely in K and is not in $S \cup W$. Let ε be a non-square unit in $\mathbb{Q}_q$. For every $p \in P = S \cup W \cup \{t\}$ define m_p by:

$$m_p = \begin{cases} 1 & \text{if } p \in W \\ \eta & \text{if } p \in S \\ \varepsilon\eta & \text{if } p = q \end{cases}$$

For every $p \in P$, let u_p denote the standard valuation on $\mathbb{Q}_p$. Since the primes of $S \cup \{q\}$ split completely in K, $m_p \in \mathbb{Q}_p$ for all $p \in P$. By the approximation theorem ([60],3-1-4) there is a rational integer m for which $u_p(\frac{m}{m_p} - 1)$ is large enough to insure $m \equiv m_p \pmod{K_p^{*2}}$ for every $p \in P$.

Letting $L = K(\sqrt{m\eta})$ we have:

$$L_p = \begin{cases} K_p(\sqrt{m\eta}) = K_p(\sqrt{\eta}) = (L_0)_p & \text{if } p \in W \\ K_p(\sqrt{m\eta}) = K_p(\sqrt{\eta^2}) = K_p = \mathbb{Q}_p & \text{if } p \in S \\ K_p(\sqrt{m\eta}) = K_p(\sqrt{\varepsilon}) \neq K_p & \text{if } p = q. \end{cases}$$

Since at $p = q$, L/K is a non-trivial extension, we have $L \neq K$ and hence L is the required extension.

□

The following lemma is proved in [51, Theorem 3] (beginning of pg. 418).

Lemma 2.2.7. *Let $K/\mathbb{Q}$ be a Galois extension with Galois group*

$$\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \mid \tau^2 = \sigma^3 = 1, \tau\sigma\tau = \sigma^2 \rangle \cong S_3,$$

and $F := K^\tau$. Let $p \equiv 3 \pmod 4$ be a rational prime, w a prime of F that divides p and v a prime of K that divides w. Assume K_v/F_w is ramified and $F_w \cong \mathbb{Q}_p$. Assume $\beta \in F$ is a non-square unit in K_v^* such that β^σ and β^{σ^2} are uniformizers in K_v. Then $\beta^{\sigma^2} \equiv \beta\beta^\sigma \pmod{K_v^{*2}}$.

Proposition 2.2.8. *Let G be a Sylow metacyclic $\{2,3\}$-group. Let S be finite set of odd rational primes and T a tame supporting set for G that is disjoint from S. Then there is a Galois G-extension $L/\mathbb{Q}$ compatible with T for which every prime of S splits completely in L.*

Proof. We follow [51, Theorem 3] closely. Let $n = |G|$. By Chebotarev's density theorem for every cyclic subgroup $C \leq \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}))$ there is a prime v_C such that $\mathrm{Gal}(\mathbb{Q}(\mu_n)_{v_C}/\mathbb{Q}_{v_C}) = C$ and $v_C \notin T$. Let $S_0 = \{v_C \mid C \leq \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})\}$. By Lemma 1.2.8 any field in which the primes of S_0 split completely is disjoint from $\mathbb{Q}(\mu_n)$.

At first we consider the case in which G has a normal 3-Sylow subgroup $G(3)$. Let $\{v_1(2), v_2(2), v_1(3), v_2(3)\}$ be the primes of T. By Lemma 2.2.4 there is a $\mathbb{Q}$-adequate Galois extension M with Galois group $\mathrm{Gal}(M/\mathbb{Q}) \cong G(2)$ such that:

1. every prime in $S \cup S_0 \cup \{v_1(3), v_2(3)\}$ splits completely in M,

2. M is compatible with the supporting set $\{v_1(2), v_2(2)\}$.

It follows from Lemma 1.2.8 that $M \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$. By Theorem 0.2.7, M embeds into a larger field E, Galois over $\mathbb{Q}$, with Galois group $\mathrm{Gal}(E/\mathbb{Q}) = G$ such that:

$$\mathrm{Gal}(E_{v_i(3)}/\mathbb{Q}_{v_i(3)}) \cong G(3) \text{ for } i = 1, 2, \tag{2.2.4}$$

and in which the primes of S split completely. Since M is compatible with $\{v_1(2), v_2(2)\}$ and since (2.2.4) holds, E is compatible with T as required.

Let us assume $G(3)$ is not a normal subgroup of G. As in [51] the strategy is as follows. Let $F = F(G)$ denote the Fitting subgroup of G and $F(2)$ and $F(3)$ its Sylow subgroups. We shall first construct a G/F-extension $K/\mathbb{Q}$ that is compatible with T and in which the primes of $S \cup S_0$ split completely. In particular, $K \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$. By Theorem 0.2.7, K can be embedded into a $G/(F(3))$-extension that is compatible with T and in which the primes of S split completely. Thus, our goal will be to embed $K/\mathbb{Q}$ into a $G/(F(2))$-extension L that is compatible with T and in which the primes of S split completely. Since G is the pullback in the following diagram:

$$\begin{array}{ccc} G & \dashrightarrow & G/(F(2)) \\ \vdots & & \downarrow \\ G/(F(3)) & \longrightarrow & G/F, \end{array} \tag{2.2.5}$$

the extension $EL/\mathbb{Q}$ will then be a G-extension that is compatible with T and in which the primes of S split completely as required.

It therefore remains to construct a G/F-extension $K/\mathbb{Q}$ and embed it into a $G/(F(3))$-extension $L/\mathbb{Q}$ that is compatible with T and in which the primes of S split completely (this implies that the same properties also hold for K). To do so, in each of the 4 cases that appear in Section 2.2.2, we adopt the constructions of [51, Theorem 3] to have the properties that are required from L.

Case 1.1: In this case $G/F \cong A_3$ and $A := F(2) \cong C_{2^u} \times C_{2^u}$. By the Grunwald-Wang theorem we can choose $K/\mathbb{Q}$ to be an A_3-extension compatible with $\{v_1(3), v_2(3)\}$ such that the primes of $S \cup S_0 \cup \{v_1(2), v_2(2)\}$ split completely in K.

To construct L one has to solve the embedding problem $G/(F(3)) \to \mathrm{Gal}(K/\mathbb{Q})$ with the corresponding conditions at $S \cup T$. As in [51], this can be done using theorems 0.2.9 and 0.2.10.(b).

For the kernel A, denote $A' = \mathrm{Hom}(A, \mu_n)$ and $G' = \mathrm{Gal}(\mathbb{Q}(A')/\mathbb{Q})$. By Lemma 2.2.5.(1), $v_i(2) \equiv 1 \pmod{2^u}$ and hence $v_i(2)$ splits completely in $\mathbb{Q}(\mu_{2^u})$, for $i = 1, 2$. Since $v_i(2)$ also splits completely in K, it splits completely in $K(\mu_{2^u})$, for $i = 1, 2$. As in Lemma 2.2.4 one has:

$$G'_{v_i(2)} \leq \mathrm{Gal}(K_{v_i(2)}(\mu_{2^u})/\mathbb{Q}_{v_i(2)}) = 1,$$

for $i = 1, 2$. Every prime v of S is odd and hence $G'_v \leq \mathrm{Gal}(\mathbb{Q}_v(\mu_{2^u})/\mathbb{Q}_v)$ is cyclic. It follows that for every $v \in S \cup \{v_1(2), v_2(2)\}$, G'_v is cyclic and hence we may apply

theorems 0.2.9 and 0.2.10.(b). Theorem 0.2.9 implies that there is an $L \supseteq K$ for which:

1. $\mathrm{Gal}(L/\mathbb{Q}) \cong G/(F(3))$,
2. $\mathrm{Gal}(L_{v_i(2)}/\mathbb{Q}_{v_i(2)}) \cong F/(F(3)) \cong F(2)$, for $i = 1, 2$, and
3. all primes of S split completely in L.

Therefore L has all the required properties and $EL/\mathbb{Q}$ is the desired extension.

Case 1.2: In this case $G/F \cong A_3$, $F(2) \cong Q_8$ and $G/(F(3)) \cong \mathrm{SL}_2(3)$. Let K be as in Case 1.1.

The primes $v_i(2)$, $i = 1, 2$, split completely in K and hence one can write $(v_i(2)) = \mathfrak{p}_i\mathfrak{p}_i^{\sigma}\mathfrak{p}_i^{\sigma^2}$ where $\mathfrak{p}_i$ is a prime of K. Let $\mathfrak{m}$ be the modulus of K consisting of (8), the infinite primes, the ramified primes of $K/\mathbb{Q}$, $\mathfrak{p}_i^{\sigma}$, $\mathfrak{p}_i^{\sigma^2}$, $i = 1, 2$, and the prime divisors of primes of S. Let $\gamma \in K$ be an element that is totally positive, congruent to 1 mod (8), the ramified primes of $K/\mathbb{Q}$, the prime divisors of primes of S and $\mathfrak{p}_i^{\sigma}$, and congruent to a non-square unit mod $\mathfrak{p}_i^{\sigma^2}$, $i = 1, 2$.

By the generalized Dirchlet theorem the ray class mod $\mathfrak{m}$ of $\mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1}\gamma$ contains a prime ideal $\mathfrak{q}$ of degree 1. Thus, there is an element $\delta \in K$ such that

$$\delta \equiv 1 \pmod{\mathfrak{m}} \text{ and } (\gamma\delta) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}.$$

The element $\beta = \gamma\delta$ satisfies the conditions imposed on γ. Then $\alpha = \beta^{\sigma}\beta^{\sigma^2}$ is non-square at $\mathfrak{p}_i$, α^{σ} is prime at $\mathfrak{p}_i$ and $\alpha^{\sigma^2} \equiv \alpha\alpha^{\sigma} \pmod{K^{*2}}$, for $i = 1, 2$. Thus, $F = K(\sqrt{\alpha}, \sqrt{\alpha^{\sigma}})$ is Galois over $\mathbb{Q}$ with Galois group $\mathrm{Gal}(F/\mathbb{Q}) \cong A_4$,

$$\mathrm{Gal}(F_{v_i(2)}/\mathbb{Q}_{v_i(2)}) \cong C_2 \times C_2$$

and all primes of S split completely in F.

Consider the embedding problem $\mathrm{SL}_2(3) \to \mathrm{Gal}(F/\mathbb{Q})$. At $v_i(2)$ the induced local embedding problem is $Q_8 \to \mathrm{Gal}(F_{v_i(2)}/\mathbb{Q}_{v_i(2)}) \cong C_2 \times C_2$. Note that the extension $F_{v_i(2)}/\mathbb{Q}_{v_i(2)}$ is the maximal abelian exponent 2 extension of $\mathbb{Q}_{v_i(2)}$. By Lemma 2.2.5, we have $v_i(2) \equiv -1 \pmod 4$, $i = 1, 2$. Thus by the description in Section 0.2.3 there is an epimorphism:

$$\mathrm{Gal}((\mathbb{Q}_{v_i(2)})_{tr}/\mathbb{Q}_{v_i(2)}) \to \langle \sigma, \tau \mid \sigma^2 = \tau^2, \tau^4 = 1, \sigma^{-1}\tau\sigma = \tau^{-1} \rangle \cong Q_8,$$

and hence a solution for the local embedding problems at $v_i(2)$ for $i = 1, 2$. Therefore the embedding problem $\mathrm{SL}_2(3) \to \mathrm{Gal}(F/\mathbb{Q})$ has a local solution at all primes except perhaps at the restriction of $\mathfrak{q}$ to $\mathbb{Q}$. By [52, Lemma 2], there is a global solution $L_0 = K(\sqrt{\eta})$. Since $Q_8 \to \mathrm{Gal}(F_{v_i(2)}/\mathbb{Q}_{v_i(2)})$ is a Frattini embedding problem its solutions must be surjective and hence

$$\mathrm{Gal}((L_0)_{v_i(2)}/\mathbb{Q}_{v_i(2)}) \cong Q_8 \text{ and } \mathrm{Gal}(L_0/\mathbb{Q}) \cong \mathrm{SL}_2(3). \tag{2.2.6}$$

Applying Lemma 2.2.6 for L_0, $W = \{v_1(2), v_2(2)\}$ and S yields a Galois $\mathrm{SL}_2(3)$-extension $L/\mathbb{Q}$ that is compatible with T and in which the primes of S split completely.

Case 2.2 (including **Case 2.1**): In this case $G/F \cong S_3$, $G/(F(3)) \cong S_4^*$ or S_4^{**} and $F(2) \cong Q_8$. The 2-Sylow subgroups of G are isomorphic to Q_{16} if $G/(F(3)) \cong S_4^*$ and $D_{16}^* = \langle x, y | x^2 = y^8 = 1, x^{-1}yx = y^3 \rangle$ if $G/(F(3)) \cong S_4^{**}$. By Lemma 2.2.5, we have:

1. $v_i(2) \equiv -1 \pmod 8$ if $G/(F(3)) \cong S_4^*$,
2. $v_i(2) \equiv 3 \pmod 8$ if $G/(F(3)) \cong S_4^{**}$.

Let t be a rational prime for which:

1. $v_1(2)v_2(2)t \equiv 1 \pmod u$ for every odd prime u in $S \cup S_0$,
2. $t \equiv 1 \pmod 8$ and
3. $t \notin S \cup T$.

Then $k := \mathbb{Q}(\sqrt{v_1(2)v_2(2)t})$ is compatible with $\{v_1(2), v_2(2)\}$ and all primes of $S \cup S_0 \cup \{2\}$ split in k. Since the roots of unity in k are $\{1, -1\}$, we may apply Theorem 0.2.7 and embed $k/\mathbb{Q}$ into a $G/(F(2))$-extension $E/\mathbb{Q}$ compatible with T, in which the primes of S split completely and such that the ramified prime $\mathfrak{t}$ of k that lies above t also splits completely in E. Set $K = E^{F/(F(2))}$.

We would now like to embed $K/\mathbb{Q}$ into a $G/(F(3))$-extension $L/\mathbb{Q}$ compatible with T and in which the primes of S split completely. Then KL will be the required G-extension.

Fix a presentation $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau | \sigma^3 = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle \cong S_3$. Let F be the fixed subfield of τ. By the description in Section 0.2.3, there is no S_3-extension of $\mathbb{Q}_{v_i(2)}$ with inertial degree 3 and hence the prime $v_i(2)$ decomposes in F, for $i = 1, 2$. The primes $v_i(2), i = 1, 2$, also cannot split completely in F since then they would split completely in the $\mathbb{Q}$-normal closure of F which is K. Thus, $v_1(2), v_2(2)$ decompose in the following way:

$$(v_1(2))_F = \mathfrak{p}_1\mathfrak{p}_2^2, (\mathfrak{p}_1)_K = \mathfrak{p}^2, (\mathfrak{p}_2)_K = \mathfrak{p}^\sigma\mathfrak{p}^{\sigma^2},$$

$$(v_2(2))_F = \mathfrak{q}_1\mathfrak{q}_2^2, (\mathfrak{q}_1)_K = \mathfrak{q}^2, (\mathfrak{q}_2)_K = \mathfrak{q}^\sigma\mathfrak{q}^{\sigma^2}.$$

Let R be the set of primes of F whose prime divisors in K ramify in K/k. Construct a modulus $\mathfrak{m}$ of F consisting of (8), the infinite primes, $\mathfrak{p}_1, \mathfrak{q}_1$, the prime divisors of t, the primes in R and the prime divisors of primes of S. Choose $\gamma \in F$ such that γ is congruent to 1 mod 8, the primes of R, the prime divisors of primes in $S \cup \{t\}$ and congruent to a non-square unit at $\mathfrak{p}_1$,$\mathfrak{q}_1$.

By the generalized Dirchlet Theorem, the ray class mod $\mathfrak{m}$ of the ideal $\mathfrak{p}_2^{-1}\mathfrak{q}_2^{-1}\gamma$ contains a prime ideal $\mathfrak{r}$ and hence there exists a $\delta \in F$ such that $\delta \equiv 1 \pmod{\mathfrak{m}}$ and $(\gamma\delta) = \mathfrak{p}_2\mathfrak{q}_2\mathfrak{r}$. The element $\beta = \gamma\delta \in F$ satisfies the conditions imposed above on γ.

Since $K_\mathfrak{p}/F_{\mathfrak{p}_1}$ is totally ramified and β is a non-square unit at $\mathfrak{p}_1$, β is also a non-square unit at $\mathfrak{p}$. Since β is a uniformizer in $F_{\mathfrak{p}_2}$ and $\mathfrak{p}_2$ splits in K, β is also a uniformizer at $\mathfrak{p}^\sigma$ and $\mathfrak{p}^{\sigma^2}$. Thus, β^σ and β^{σ^2} are uniformizers at $\mathfrak{p}$. We can therefore

apply Lemma 2.2.7 and deduce $\beta^{\sigma^2} \equiv \beta\beta^{\sigma}$ (*mod* $K_{\mathfrak{p}}^{*2}$). Thus $\beta^{\sigma}\beta^{\sigma^2} \equiv \beta \pmod{K_{\mathfrak{p}}^{*2}}$ (resp. mod $K_{\mathfrak{q}}^{*2}$). By setting $\alpha = \beta^{\sigma}\beta^{\sigma^2}$ we have:

$$K_{\mathfrak{p}}(\sqrt{\beta^{\sigma}}, \sqrt{\beta^{\sigma^2}}) = K_{\mathfrak{p}}(\sqrt{\alpha^{\sigma}}, \sqrt{\alpha^{\sigma^2}}) \text{ (resp. } K_{\mathfrak{q}}(\sqrt{\beta^{\sigma}}, \sqrt{\beta^{\sigma^2}}) = K_{\mathfrak{q}}(\sqrt{\alpha^{\sigma}}, \sqrt{\alpha^{\sigma^2}})).$$

and:

$$\alpha^{\sigma^2} \equiv \alpha\alpha^{\sigma} \pmod{K^{*2}},\ \alpha^{\tau} = \alpha, \alpha^{\sigma\tau} = \alpha^{\sigma^2} \text{ and } \alpha^{\sigma^2\tau} = \alpha^{\sigma}. \tag{2.2.7}$$

In particular $M = K(\sqrt{\alpha}, \sqrt{\alpha^{\sigma}})/\mathbb{Q}$ is Galois. Since $M_{v_i(2)}/\mathbb{Q}_{v_i(2)}$ is a Galois extension of order 8 and ramification index 4, it follows from Section 0.2.3 that

$$\mathrm{Gal}(M/F) \cong \mathrm{Gal}(M_{v_i(2)}/\mathbb{Q}_{v_i(2)}) \cong Q_8 \text{ or } D_8.$$

Since $C_2 \times C_2 \cong \mathrm{Gal}(M/K) \lhd \mathrm{Gal}(M/F)$ and Q_8 does not have a $C_2 \times C_2$-subgroup one has $\mathrm{Gal}(M/F) \cong D_8$. Thus, the extension of 2-Sylow subgroups

$$1 \to \mathrm{Gal}(M/K) \to \mathrm{Gal}(M/F) \to \mathrm{Gal}(K/F) \to 1$$

splits. Since the extensions of all p-Sylow subgroups split for all primes p, it follows from a theorem of Gaschütz [10, Pg. 118] that the entire extension

$$1 \to \mathrm{Gal}(M/K) \to \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 1$$

splits. By (2.2.7) the action of $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$ on $\mathrm{Gal}(M/K) \cong C_2 \times C_2$ is equivalent to the action of an S_3 subgroup of S_4 on the normal $C_2 \times C_2$ subgroup of S_4 and hence $\mathrm{Gal}(M/\mathbb{Q}) \cong S_4$.

The local Galois groups at $v_1(2), v_2(2)$ are $\mathrm{Gal}(M_{v_i(2)}/\mathbb{Q}_{v_i(2)}) \cong D_8$ for $i = 1, 2$. The primes of S split completely and the Galois group at t remains

$$\mathrm{Gal}(M_t/\mathbb{Q}_t) \cong\ \mathbb{Z}/2\mathbb{Z}.$$

Therefore M is compatible with T and hence $\mathbb{Q}$-adequate, proving Case 2.1.

Consider the embedding problem $G/(F(3)) \twoheadrightarrow \mathrm{Gal}(M/\mathbb{Q})$. At the rational primes v whose divisors are ramified in K/k the Galois group $\mathrm{Gal}(M_v/\mathbb{Q}_v)$ is either C_3 or S_3 (with odd ramification index). Since the kernel of this embedding problem is of order 2, it is solvable at these primes. Since $t \equiv 1 \pmod 8$ and $\mathfrak{t}$ splits completely at M the local embedding problem at t is solvable. For $G/(F(3)) = S_4^*$ (resp. S_4^{**}) we have $v_i(2) \equiv -1 \pmod 8$ (resp. $v_i(2) \equiv 3 \pmod 8$) and hence the (unique) D_8-extension $M_{v_i(2)}$ of $\mathbb{Q}_{v_i(2)}$ can be embedded in a Q_{16}-extension (resp. D_{16}^*-extension).

Therefore the induced local embedding problems are solvable everywhere except perhaps at r. It follows from [52, Lemma 2] that this embedding problem is solvable at r and it has a global solution $L_0 = M(\sqrt{\eta})$. Since the embedding problem at $v_i(2)$ is Frattini we have $[(L_0)_{v_i(2)} : \mathbb{Q}_{v_i(2)}] = 16$, for $i = 1, 2$, and hence

$$\mathrm{Gal}(L_0/\mathbb{Q}) \cong G/(F(3)).$$

By applying Lemma 2.2.6 for L_0, $W = \{v_1(2), v_2(2)\}$ and S, we obtain the required Galois $G/(F(3))$-extension $L/\mathbb{Q}$ which is compatible with T and in which all primes of S split completely.

□

2.2.4 Proof of a refined $\mathbb{Q}$-admissibility theorem

The following proof is based on [6, Theorem 2.1].

Proof of Theorem 2.2.3. Let $n = |G|$. By [6, Lemma 1.4], G has a $\{2,3\}$-normal complement. In other words, there is a normal subgroup $N \lhd G$ of order prime to 6 (to 2 and 3) and a $\{2,3\}$-subgroup A for which $G = NA$.

Denote by T_N the subset $\{v_i(p) | i = 1, 2, p||N|\}$ of T. As in Proposition 2.2.8, for every cyclic subgroup $C \leq \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}))$ fix a prime v_C such that

$$\mathrm{Gal}(\mathbb{Q}(\mu_n)_{v_C}/\mathbb{Q}_{v_C}) = C$$

and $v_C \notin T$ and let $S_0 = \{v_C \mid C \leq \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})\}$.

By Proposition 2.2.8 there is a $\mathbb{Q}$-adequate Galois A-extension $K/\mathbb{Q}$ compatible with the supporting set $\{v_1(2), v_2(2), v_1(3), v_2(3)\}$ in which all primes of $T_N \cup S \cup S_0$ split completely. By Lemma 1.2.8, $K \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$. Since $(|N|, |A|) = 1$ the embedding problem $G \to \mathrm{Gal}(K/\mathbb{Q})$ is split and we may apply Theorem 0.2.7. It follows that there is a surjective solution L in which the primes of S split completely and such that $\mathrm{Gal}(L_{v_i(p)}/\mathbb{Q}_{v_i(p)})$ is a p-Sylow subgroup of N for every $p||N|$. In particular L is compatible with T. □

2.3 Tame admissibility over number fields

2.3.1 Lifting $\mathbb{Q}$-admissibility

We shall now lift the above construction to a general number field K. A similar approach was used in [30, Theorem 27].

Theorem 2.3.1. *Let K be a number field and S a finite set of odd primes of K. Let G be a solvable group such that for every $p||G|$, the p-Sylow subgroups of G admit a presentation $\mathcal{M}(m_p, n_p, i_p, t_p)$ for which*

$$\sigma_{t_p,n_p} \in \mathrm{Gal}(\mathbb{Q}(\mu_{n_p})/(\mathbb{Q}(\mu_{n_p}) \cap K)). \tag{2.3.1}$$

Then there is a tamely K-adequate Galois G-extension in which the primes of S split completely.

Furthermore, there is a $\mathbb{Q}$-division algebra D_0 with a maximal subfield L such that $\mathrm{Gal}(L/\mathbb{Q}) \cong G$ and $D_0 \otimes_{\mathbb{Q}} K$ is a division algebra with maximal subfield LK.

Note that in the second part of Theorem 2.3.1, $\dim_K(D_0) = |G|^2$, and hence the maximal subfield LK must be of degree $[LK : K] = |G|$. In particular $\mathrm{Gal}(LK/K) \cong G$, LK is a K-adequate and $D_0 \otimes_{\mathbb{Q}} K$ is a G-crossed product division algebra over K.

Proof of Theorem 2.3.1. Let $S_{\mathbb{Q}}$ be the set of rational primes that lie below the primes of S. Let M be the $\mathbb{Q}$-Galois closure of K. Fix a prime $p||G|$. As

$$\sigma_{t_p,n_p} \in \mathrm{Gal}(\mathbb{Q}(\mu_{n_p})/(\mathbb{Q}(\mu_{n_p}) \cap K)),$$

σ_{t_p,n_p} extends to an automorphism of $K(\mu_{n_p})$ that fixes K. Therefore there is an automorphism $\tau_p \in \mathrm{Gal}(M(\mu_{n_p})/K)$ that restricts to σ_{t_p,n_p}. By the Chebotarev density Theorem there are infinitely many rational primes $(v_i(p))_{i\in\mathbb{N}}$ whose Frobenius automorphism is τ_p. In particular σ_{t_p,n_p} is the Frobenius automorphism of $v_i(p)$ in $\mathbb{Q}(\mu_{n_p})$ and hence $v_i(p) \equiv t_p \pmod{n_p}$, for all $i = 1, 2$, $p||G|$.

Since for every $p||G|$ there are infinitely many such primes $v_i(p)$, one can fix primes $w_i(p)$, for $i = 1, 2$ and $p||G|$ such that:

(A1) the primes $w_i(p)$, $i = 1, 2$, $p||G|$, are distinct,

(A2) $w_i(p) \notin S_{\mathbb{Q}}$, for all $i = 1, 2$ and $p||G|$,

(A3) $w_i(p) \neq 2$ for all $p||G|$, $i = 1, 2$,

(A4) τ_p is the Frobenius automorphism of $w_i(p)$ in $M(\mu_{n_p})/\mathbb{Q}$,

(A5) $w_i(p) \neq p$ for all $p||G|$, $i = 1, 2$.

Conditions (A1), (A3) and (A4) imply that $T = \{w_i(p)|i = 1, 2, p||G|\}$ is a tame supporting set for G and the primes of T split completely in K. By Theorem 2.2.3 there is a Galois G-extension $L/\mathbb{Q}$ compatible with T in which the primes of $S_{\mathbb{Q}}$ split completely.

Let $N := LK$. Since $w_i(p)$ splits completely in K, $[K_v : \mathbb{Q}_{w_i(p)}] = 1$ for every $i = 1, 2$, $p||G|$ and $v|w_i(p)$. Letting u be a prime of N that divides $w_i(p)$ we have:

$$[N_u : K_u] = \frac{[N_u : \mathbb{Q}_{w_i(p))}]}{[K_u : \mathbb{Q}_{w_i(p)}]} = [N_u : \mathbb{Q}_{w_i(p)}] = [L_u : \mathbb{Q}_{w_i(p)}][N_u : L_u], \tag{2.3.2}$$

where L_u (resp. K_u) denotes the completion of L (resp. K) at the restriction of u to L (resp. K). Since $[N_u : K_u]|[L_u : \mathbb{Q}_{w_i(p)}]$ we deduce

$$[N_u : L_u] = 1 \text{ and } [N_u : K_u] = [L_u : \mathbb{Q}_{w_i(p)}].$$

Thus, $\mathrm{Gal}(N_v/K_v)$ contains a p-Sylow subgroup of G for all $v|w_i(p), i = 1, 2$ and $p||G|$. In particular this implies $[N : K] = |G| = [L : \mathbb{Q}]$ and hence $K \cap L = \mathbb{Q}$.

Let $v' \in S$ and q its restriction in $S_{\mathbb{Q}}$. Then

$$[N_{v'} : K_{v'}]|[L_q : \mathbb{Q}_q] = 1, \tag{2.3.3}$$

and therefore v' splits completely in N. The Galois extension N/K is therefore K-adequate with Galois group G and every prime of S splits completely in N. Moreover since $w_i(p)$ satisfies (A5), its divisors in K are not divisors of p for all $i = 1, 2$, $p||G|$ and hence Lemma 2.1.5 implies that N/K is also tamely K-adequate.

To prove the second part of the theorem we construct a $\mathbb{Q}$-division algebra D_0 such that $D_0 \otimes_{\mathbb{Q}} K$ is a division algebra with maximal subfield LK. For a prime $p||G|$ and let p^{k_p} be the largest p-power dividing $|G|$. Let D_p be the $\mathbb{Q}$-division algebra whose invariants are:

$$\mathrm{inv}_{w_1(p)}(D_p) = \frac{1}{p^{k_p}}, \mathrm{inv}_{w_2(p)}(D_p) = -\frac{1}{p^{k_p}}$$

and $\mathrm{inv}_u(D_p) = 0$ for any other prime u. Let $D_0 = \otimes_{p||G|} D_p$ where the tensor is taken over $\mathbb{Q}$. Then L splits D_p for every p and hence D_0. Since $w_1(p)$ splits completely in K, we have $\mathrm{inv}_v(D_p \otimes_{\mathbb{Q}} K)$ is of order p^{k_p}, for every p and for every prime v of K that divides $w_i(p)$. In particular, the Brauer class α of $D := D_0 \otimes_{\mathbb{Q}} K$ is of order $|G|$. This shows that the underlying division algebra in α is of dimension $|G|^2$ and hence isomorphic to D. In particular D is a K-division algebra.

Since L splits D_0, LK splits D. Since $\sqrt{\dim_K(D)} = |G| = [LK : K]$ and LK splits D, LK is a maximal subfield of D. □

2.3.2 Conclusions

As a corollary to Theorem 2.3.1, we have the following characterization of tame admissibility of solvable groups.

Corollary 2.3.2. *Let K be a number field and G a solvable group. Then G is tamely K-admissible if and only if for every $p||G|$, the p-Sylow subgroups of G admit a presentation $\mathcal{M}(m_p, n_p, i_p, t_p)$ for which:*

$$\sigma_{t_p,n_p} \in \mathrm{Gal}(\mathbb{Q}(\mu_{n_p})/(\mathbb{Q}(\mu_{n_p}) \cap K)). \tag{2.3.4}$$

Proof. If G is tamely K-admissible then by lemmas 2.1.5 and 1.2.5, the p-Sylow subgroups have such a presentation. The converse follows from Theorem 2.3.1. □

For solvable groups G we can also characterize K-admissibility under the assumption that every p which divides $|G|$ does not decompose in K.

Corollary 2.3.3. *Let K be a number field and G a solvable group. Assume that every prime p that divides $|G|$ does not decompose in K. Then the following conditions are equivalent:*

1. *G is tamely K-admissible,*
2. *G is non-wildly K-admissible,*
3. *G is K-admissible,*
4. *G is K-preadmissible,*
5. *for every $p||G|$, the p-Sylow subgroups of G admit a presentation $\mathcal{M}(m_p, n_p, i_p, t_p)$ that satisfies (2.3.4).*

If moreover G is of odd order the conditions above are equivalent to:

(6) there is a tamely ramified K-adequate Galois G-extension.

Proof. The implications (6) ⇒ (1) ⇒ (2) ⇒ (3) ⇒ (4) ⇒ (5) are clear from the definitions and Lemma 1.2.5. The implication (5) ⇒ (1) follows directly from Theorem 2.3.1. We are left to prove (1) ⇒ (6) for groups G of odd order. Let S be the set of primes of K that whose restriction to $\mathbb{Q}$ divides $|G|$. By Theorem 2.3.1 there is a K-adequate Galois G-extension L/K in which all primes of S split completely. In particular, L/K is tamely ramified. □

The difficulty in proving Corollary 2.3.3 for non-solvable Sylow metacyclic groups G arises in the implication (5) $\Rightarrow$ (6). In fact, the following problem is open:

Problem 2.3.4. Let K be a number field and G a finite group (not necessarily solvable) such that for every $p||G|$, the p-Sylow subgroups of G admit a presentation $\mathcal{M}(m_p, n_p, i_p, t_p)$ that satisfies (2.3.4). Is there necessarily a tamely ramified K-adequate Galois G-extension?

If the answer to this problem is positive then conditions (1)-(6) are all equivalent for every finite group G.

Theorem 2.3.1 can also be used to study infinitely often admissible groups.

Corollary 2.3.5. *Let K be a number field and G a solvable group such that for every $p||G|$, the p-Sylow subgroups admit a presentation $\mathcal{M}(m_p, n_p, i_p, t_p)$ for which (2.3.4) holds. Then G is K-admissible infinitely often.*

Moreover there is a K-division algebra D with infinitely many maximal Galois subfields $(L_r)_{r\in\mathbb{N}}$ with $\mathrm{Gal}(L_r/K) \cong G$ and such that $L_{r+1} \cap L_1 \cdots L_r = K$ for every $r \in \mathbb{N}$. In particular the fields $(L_r)_{i\in\mathbb{N}}$ are non-isomorphic.

Proof. Let $w_i(p)$, $i = 1, 2$, $p||G|$, D_0 and D be as in the proof of Theorem 2.3.1. In particular $T := \{w_i(p) \mid i = 1, 2, p||G|\}$ is a supporting set for G over $\mathbb{Q}$ and every G-extension $F/\mathbb{Q}$ that is compatible with T splits D_0.

Let M be the $\mathbb{Q}$-normal closure of K. Let $L_1, ..., L_r$ be a sequence of disjoint Galois G-extensions of K which are maximal subfields of D and let $N := L_1 \cdots L_r M$. For every $C \leq \mathrm{Gal}(N/\mathbb{Q})$ fix a rational prime v_C such that $\mathrm{Gal}(N_{v_C}/\mathbb{Q}_{v_C}) = C$ and $v_C \notin T$. Let $S_0 = \{v_C \mid C \leq \mathrm{Gal}(N/\mathbb{Q})\}$. By Theorem 2.3.1, there is a Galois G-extension $F/\mathbb{Q}$ compatible with T in which all primes of S_0 split completely.

By Lemma 1.2.8, $F \cap N = \mathbb{Q}$. Letting $L_{r+1} = FK$, we have $\mathrm{Gal}(L_{r+1}/K) \cong G$, $L_{r+1}K \cap N = K$ and hence $L_{r+1} \cap L_1 \dots L_r = K$.

Since F is compatible with T, it splits D_0. It follows that L_{r+1} splits D and hence it is a maximal subfield of D.

We have found another maximal subfield L_{r+1} of D with Galois group

$$\mathrm{Gal}(L_{r+1}/K) \cong G$$

which is disjoint from $L_1 \cdots L_r$. By iterating this process we obtain an infinite sequence $(L_r)_{r\in\mathbb{N}}$ of maximal subfields of D that are disjoint as required. □

Let us say G is tamely K-preadmissible if the local conditions of tame K-admissibility are satisfied. Namely, if there is a set $T = \{v_i(p)|p||G|, i = 1, 2\}$ of primes of K and corresponding Galois extensions $(L^{(v)})_{v\in T}$ of K_v such that for every $p||G|$:

1. $v_1(p) \neq v_2(p)$,
2. $\mathrm{Gal}(L^{(v_i(p))} \cap (K_{v_i(p)})_{tr}/K_{v_i(p)})$ contains a p-Sylow subgroup of G for $i = 1, 2$,

A similar proof to that of Lemma 2.1.5 shows that if G is tamely K-preadmissible then the primes $v_i(p)$, $i = 1, 2$, can be chosen so that $v_i(p) \not| p$ for all $p||G|$. Theorefore, Lemma 1.2.5 shows that the p-Sylow subgroups of G admit a presentation $\mathcal{M}(m_p, n_p, i_p, t_p)$ for which (2.3.4) holds.

By [30, Theorem 29], the converse statement also holds: if the Sylow subgroups of G admit such presentations then G is tamely K-preadmissible. Thus, Problem 2.3.4 can be reformulated as follows: let G be a tamely K-preadmissible group. Is there necessarily a tamely ramified K-adequate Galois G-extension?

Chapter 3

Admissibility as an arithmetic relation

In this chapter we shall study equivalence by admissibility and by preadmissibility. Similarly to many arithmetic relations, these equivalence relations are closely related to conditions on the decomposition of rational primes.

We shall focus on the case $K \subseteq L$, where $L/\mathbb{Q}$ is a Galois extension and find conditions on decomposition of rational primes in two fields $K \subseteq L$ that are necessary for equivalence by preadmissibility. We shall prove that these conditions are equivalent to the following condition on $\mathcal{G} := \mathrm{Gal}(L/\mathbb{Q})$ and $\mathcal{H} := \mathrm{Gal}(L/K)$:

For every $D \leq \mathcal{G}$ that appears as a decomposition group in the extension $L/\mathbb{Q}$, there should be two split double cosets of the form $Dx\mathcal{H}$, i.e. two double cosets $Dx_1\mathcal{H}, Dx_2\mathcal{H}$ such that $|Dx_iH| = |D||H|$, for $i = 1, 2$.

Let l be a rational prime. In Section 3.1.3, we show that the latter condition is also sufficient for equivalence by preadmissibility if $\mathcal{G}$ is an l-group that is not metacyclic and l splits completely in L. This proves Theorem 0.1.10 and as a result we shall also deduce Corollary 0.1.11.

In Section 3.2.1, we give simple group theoretic conditions for the construction of infinitely many pairs $(\mathcal{G}, \mathcal{H})$ such that $\mathcal{G}$ is an l-group and $\mathcal{H}$ is a proper subgroup for which there are two split double cosets of the form DxH for every metacyclic subgroup $D \leq \mathcal{G}$. Corollary 0.1.11 then asserts that for every such pair there exists a $\mathcal{G}$-extension $L/\mathbb{Q}$ such that $K := L^{\mathcal{H}}$ and L are equivalent by preadmissibility and have the same odd order admissible groups.

In Section 3.2.2, we use the conditions from Section 3.2.1 to show that the above pair $(\mathcal{G}, \mathcal{H})$ can be chosen so that $\mathcal{G}$ is an l-Sylow subgroup of the symmetric group S_{l^n} and $\mathcal{H} \leq \mathcal{G}$ a cyclic subgroup of order l, for every $n \geq 3$ and prime l.

For further insight into equivalence by admissibility, in Section 3.3 we compare equivalence by preadmissibility to other relations. Namely, we compare it to arithmetic equivalence and *local isomorphism*, under which two number fields K and L are equivalent if they have isomorphic Adele rings (see [25, Chap. VI, §2]). We discuss the implications diagram in Figure 3.1 and prove that every other implication that holds is a composition of these implications.

Note that an example for the non-implication $2 \not\Rightarrow 1$ appears in [27] and a

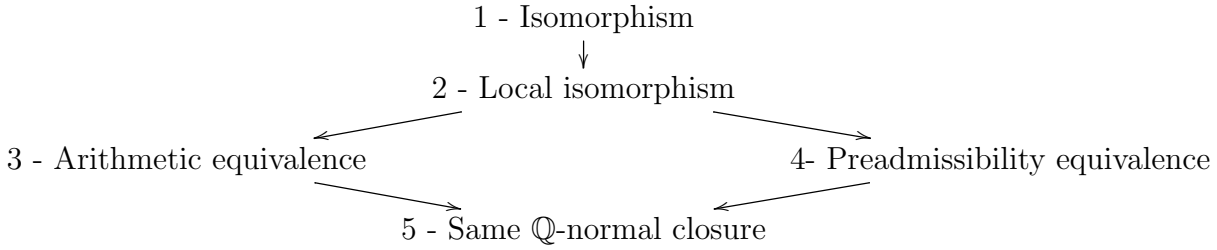

Figure 3.1: Implications between arithmetic equivalences

different approach that yields a rich source of examples is given in Example 3.3.2. The non-implication $3 \not\Rightarrow 2$ is known by [26]. It is unknown how equivalence by admissibility fits into diagram (3.1) and whether it implies or is implied by the preadmissibility equivalence.

3.1 Equivalence by preadmissibility

3.1.1 Primes and double cosets

To understand equivalence by preadmissibility it is necessary to first understand how equivalent fields lie inside their $\mathbb{Q}$-normal closure. For this, we first recall a well known connection between prime decompositions in subfields of Galois extensions and double cosets.

Let $\mathcal{G}$ be a finite group, $M/\mathbb{Q}$ a $\mathcal{G}$-extension, K a subfield of M and $\mathcal{H} := \mathrm{Gal}(M/K)$. Let p be a rational prime and let $v_1, ..., v_k$ be the primes of K lying above it. Assume the primes $v_1, ..., v_k$ are ordered such that $[K_{v_i} : \mathbb{Q}_p] \geq [K_{v_j} : \mathbb{Q}_p]$ for $i \geq j$. We shall call the vector $([K_{v_1} : \mathbb{Q}_p], ..., [K_{v_k} : \mathbb{Q}_p])$ the *local degree type* of p in K.

The parallel notion in group theory is the double coset type. Let $Dx_1\mathcal{H}, ..., Dx_s\mathcal{H}$ be the double cosets of $D \leq \mathcal{G}$ and $\mathcal{H}$ in $\mathcal{G}$, ordered by decreasing cardinality: $|Dx_1\mathcal{H}| \geq ... \geq |Dx_s\mathcal{H}|$. We call the vector $(|Dx_1\mathcal{H}|, ..., |Dx_s\mathcal{H}|)$ the *double coset type* $(D, \mathcal{H})$. Denote by $(D, \mathcal{H})_k$ the k-th entry of the vector $(D, \mathcal{H})$.

Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial, a root α of which generates $K/\mathbb{Q}$. Then f splits over M. Let $\alpha_1 := \alpha, \alpha_2, ..., \alpha_r$ be the roots of f in M. Then $\mathcal{G}$ acts transitively on the set $R_f := \{\alpha_1, ..., \alpha_r\}$. This action is equivalent to the action of $\mathcal{G}$ on the set of left cosets $\mathcal{G}/\mathcal{H}$. Let w_1 be a prime of M dividing v_1 and $D := D(M/\mathbb{Q}, w_1) \leq \mathcal{G}$ the decomposition group of w_1 in $M/\mathbb{Q}$. Then D acts on the set R_f which breaks into orbits under this action. Denote these orbits by $O_1, ..., O_s$. These orbits correspond to the orbits of the action of D (as a subgroup of $\mathcal{G}$) on $\mathcal{G}/\mathcal{H}$ which are $\{dx_i\mathcal{H} | d \in D\}$, $i = 1, ..., s$. Furthermore, the cardinality of O_i equals the number of elements in the orbit of $x_i\mathcal{H}$ which is $\frac{|Dx_i\mathcal{H}|}{|\mathcal{H}|}$, for any $i = 1, ..., s$.

The group D is isomorphic to the Galois group of $M_{w_1}/\mathbb{Q}_p$ which is a splitting

field of f over $\mathbb{Q}_p$ with an isomorphism that preserves the action on R_f. Thus, f factors over $\mathbb{Q}_p$ into $f(x) = f_1(x)...f_s(x)$ where f_i is irreducible over $\mathbb{Q}_p$ and the roots of f_i are the elements of the orbit O_i. In particular $k = s$ and for all $i = 1, \ldots, s$,

$$[K_{v_i} : \mathbb{Q}_p] = \deg(f_i(x)) = |O_i| = \frac{|Dx_i\mathcal{H}|}{|\mathcal{H}|}. \tag{3.1.1}$$

We arrive to the following well known description of prime decomposition in K:

Lemma 3.1.1. *Let $\mathcal{G}$ be a finite group and $\mathcal{H}$ a subgroup of $\mathcal{G}$. Let M be a $\mathcal{G}$-extension of $\mathbb{Q}$ and $K = M^{\mathcal{H}}$. Let p be a rational prime and v a prime of M dividing p with decomposition group $D := D(M/\mathbb{Q}, v) \leq \mathcal{G}$. Then the local degree type of p in K equals $\frac{1}{|\mathcal{H}|}(D, \mathcal{H})$.*

Note that for a different prime v' of M dividing p, the decomposition group $D' = D(M/\mathbb{Q}, v')$ is a conjugate of D and hence D and D' have the same double coset type $(D', \mathcal{H}) = (D, \mathcal{H})$.

Since for any two subgroups $A, B \leq \mathcal{G}$ we have $|AB| = \frac{|A||B|}{|A \cap B|}$, (3.1.1) equals:

$$\frac{|Dx_i\mathcal{H}|}{|\mathcal{H}|} = \frac{|x_i^{-1}Dx_i\mathcal{H}|}{|\mathcal{H}|} = \frac{|x_i^{-1}Dx_i||\mathcal{H}|}{|x_i^{-1}Dx_i \cap \mathcal{H}||\mathcal{H}|} = \frac{|D|}{|x_i^{-1}Dx_i \cap \mathcal{H}|}. \tag{3.1.2}$$

We shall use (3.1.1) and (3.1.2) repeatedly throughout the text.

3.1.2 The $\mathbb{Q}$-normal closure

Similarly to [55] one has:

Proposition 3.1.2. *Two number fields that are equivalent by preadmissibility have the same $\mathbb{Q}$-normal closure.*

A proof for Proposition 3.1.2 can be obtained by adjusting the proof of [55, Theorem 1] to preadmissibly equivalent fields as follows.

In all cases choose p to be an odd prime, in Cases 1 and 2.1 one may pick B to be $C_p \wr C_p$ and in Case 2.2 pick A to be $(C_p)^3$. Letting F be any of the fields K and L in [55, Theorem 1], one observes that both A and B are F-admissible if and only if they are F-preadmissible. Indeed by Corollary 0.2.3, A is F-admissible if and only if it is F-preadmissible over any number field F and by [42, Theorems 3.3 and 5.10(b)] (see Section 1.2.1) B admits the same property. Therefore making this choice of A and B separates K and L by preadmissibility in the same way [55, Theorem 1] separates K and L by admissibility.

Note that having the same $\mathbb{Q}$-normal closure is considered a weak arithmetic equivalence and by [25, Chap. II, Corollary 1.6.b] is characterized by the set of rational primes that split completely.

The following proposition presents further properties of preadmissibly equivalent fields.

Proposition 3.1.3. *Let K and L be two number fields that have the same $\mathbb{Q}$-normal closure M and $\mathcal{H} = \mathrm{Gal}(M/K), \mathcal{H}' = \mathrm{Gal}(M/L)$. Let p be a rational prime, v a prime of M dividing p and $D = D(M/\mathbb{Q}, v)$. If K and L are equivalent by preadmissibility then:*

(1) *p decomposes in K if and only if p decomposes in L,*

(2) *if p decomposes in K and L then $\frac{(D,\mathcal{H})_2}{|\mathcal{H}|} = \frac{(D,\mathcal{H}')_2}{|\mathcal{H}'|}$.*

The idea behind the proof of Proposition 3.1.3 lies in [55, Theorems 1 and 2]. A similar proposition, with the assumptions that K and L are equivalent by admissibility and p is odd, appears in [32] without proof.

Proof of Proposition 3.1.3. (1) Assume on the contrary that p decomposes in L but not in K and let v_1, v_2 be two primes of L that divide p. Then it follows from Lemma 1.2.5 that every K-preadmissible p-group is metacyclic. Let $G = C_p \wr C_p$ for odd p and $G = C_2 \wr C_4$ for $p = 2$. Then G is not metacyclic and hence not K-preadmissible. We shall show that G is L-preadmissible which leads to a contradiction.

For this, it suffices to prove that G is realizable over L_{v_1} and L_{v_2}. Let k be a p-adic field, $M_p(k)$ the maximal pro-p extension of k and denote by $\mathfrak{G}_k$ the Galois group $\mathrm{Gal}(M_p(k)/k)$. See Section 0.2.3 for a description of $\mathfrak{G}_k$. At first let p be odd. If $\mu_p \not\subseteq k$ then $\mathfrak{G}_k$ is a free pro-p group on at least two generators and hence G is realizable over such k. If $\mu_p \subseteq k$, then $\mathfrak{G}_k$ has a presentation as in (0.2.8) with $n \geq 2$. Thus, the quotient $\mathfrak{G}_k/\langle x_1, x_3\rangle$ is a free pro-p group on two generators and hence G is realizable over such fields as well. It follows that for odd p, G is realizable over any p-adic field and in particular over $k = L_{v_1}, L_{v_2}$.

Now let $p = 2$ and k a 2-adic field of degree $n = [k : \mathbb{Q}_2]$. Let $\langle a\rangle = C_2, \langle b\rangle = C_4$. From each of the presentations (0.2.8)-(0.2.11), there is an epimorphism from $\mathfrak{G}_k$ to $G = \langle a\rangle \wr \langle b\rangle = \langle a\rangle^4 \rtimes \langle b\rangle$ simply by sending x_1 to one of the conjugates of a, $x_2 \to 1, x_3 \to b$ and $x_i \to 1$ for $i \geq 4$. Thus, $C_2 \wr C_4$ is realizable over every 2-adic field. It follows that for any prime p, G is realizable over L_{v_1}, L_{v_2} and hence is L-preadmissible.

(2) Let v be a prime of K dividing p. By local class field theory the Galois group $A_v := \mathrm{Gal}(K_{v,ab,p}/K_v)$, where $K_{v,ab,p}$ is the maximal abelian pro-p extension of K_v, is isomorphic to the pro-p completion of the group K_v^*. Thus the rank r_v of the maximal free abelian pro-p quotient of A_v is $r_v = [K_v : \mathbb{Q}_p] + 1$ (see e.g. [48, Chap. 14, §6]). Let p^{n_0} be larger then the exponent of the torsion part of A_v for all primes v of K and L that divide p. Then, for a prime v of K dividing p, the group $(C_{p^{n_0}})^N$ is realizable over K_v if and only if $N \leq r_v$. Let v_2 (resp. w_2) be a prime of K (resp. L) dividing p such that $[K_{v_2} : \mathbb{Q}_p]$ (resp. $[L_{w_2} : \mathbb{Q}_p]$) is second in the local degree type of p in K (resp. in L).

Assume on the contrary that $\frac{(D,\mathcal{H})_2}{|\mathcal{H}|} > \frac{(D,\mathcal{H}')_2}{|\mathcal{H}'|}$. By (3.1.1), $[K_{v_2} : \mathbb{Q}_p] = \frac{(D,\mathcal{H})_2}{|\mathcal{H}|}$ and $[L_{w_2} : \mathbb{Q}_p] = \frac{(D,\mathcal{H}')_2}{|\mathcal{H}'|}$. Thus, $r_{v_2} \geq [K_{v_2} : \mathbb{Q}_p] + 1 \geq [L_{w_2} : \mathbb{Q}_p] + 2 \geq 3$. The group $G = (C_{p^{n_0}})^{r_{v_2}}$ is therefore not metacyclic and hence realizable only over completions at primes dividing p. The above discussion shows that G is realizable over two completions of K but over at most one of L. Thus, G is K-preadmissible but not L-preadmissible, contradiction. □

Note that by Corollary 0.2.3, for odd p the group G in the proof of Proposition 3.1.3.(2) is in fact K-admissible.

3.1.3 Equivalent subfields

Let K and L be number fields that are equivalent by preadmissibility and let M be their $\mathbb{Q}$-normal closure. Let us now assume further that L is Galois over $\mathbb{Q}$. Then $L = M$ and K is a subfield of L. As we shall now see, in this case Proposition 3.1.3 implies the second assertion of Theorem 0.1.10 using Corollary 3.1.4 below.

For two subgroups A, B of a finite group $\mathcal{G}$, denote by $S(A, B)$ the number of distinct split double cosets of A, B in $\mathcal{G}$. By (3.1.2), $|AxB| = \frac{|A||B|}{|x^{-1}Ax \cap B|}$ and hence AxB is a split double coset if and only if $x^{-1}Ax \cap B = 1$.

Corollary 3.1.4. *Let $\mathcal{G}$ be a finite group and $L/\mathbb{Q}$ a $\mathcal{G}$-extension in which every rational prime decomposes. Let K be a subfield of L that is equivalent to L by preadmissibility and $\mathcal{H} := \mathrm{Gal}(L/K)$. Then $S(D, \mathcal{H}) > 1$ for every $D \leq \mathcal{G}$ that appears as a decomposition group.*

Proof. Let p be a rational prime and v_0 a prime of L dividing p. All primes v of L dividing p have the same degree $[L_v : \mathbb{Q}_p] = |D|$, where $D = D(L/\mathbb{Q}, v_0)$. Since p decomposes in L, and K is equivalent by preadmissibility to L, Proposition 3.1.3 implies that p decomposes in K and $\frac{(D,\mathcal{H})_2}{|\mathcal{H}|} = |D|$. We deduce that $(D, \mathcal{H})_1 = (D, \mathcal{H})_2 = |D||\mathcal{H}|$ and hence $S(D, \mathcal{H}) > 1$. □

If $\mathcal{G}$ is an l-group and $L/\mathbb{Q}$ is a $\mathcal{G}$-extension in which l splits completely then the ramification in $L/\mathbb{Q}$ is tame and all decomposition groups are metacyclic. If in addition $\mathcal{G}$ is a non-metacyclic then every rational prime decomposes in L and Corollary 3.1.4 applies. In particular Corollary 3.1.4 implies the second assertion of Theorem 0.1.10 (the "converse" part).

Note that by the Chebotarev density theorem every cyclic subgroup appears as a decomposition group and hence Corollary 3.1.4 implies that $S(C, \mathcal{H}) > 1$ holds for every cyclic subgroup $C \leq \mathcal{G}$.

We shall now prove the first assertion of Theorem 0.1.10 (the "forward" part). The following proposition proves a part of this implication:

Proposition 3.1.5. *Let l be a prime and $\mathcal{G}$ an l-group. Let $L/\mathbb{Q}$ be a $\mathcal{G}$-extension in which l splits completely and every rational prime decomposes. Let K be a subfield of L. Then every K-preadmissible group is also L-preadmissible.*

Note that the condition $S(D, \mathcal{H}) > 1$ for every subgroup $D \leq \mathcal{G}$ that appears as a decomposition group in $L/\mathbb{Q}$ insures that every rational prime decomposes in K and hence in L. Therefore, Proposition 3.1.5 shows that under the conditions of the first assertion of Theorem 0.1.10, every K-preadmissible group is also L-preadmissible. Our proof of Proposition 3.1.5 requires two lemmas.

Lemma 3.1.6. *Let G be a finite group. Let L/K be an extension of p-adic fields such that $p \nmid [L : K]$. Assume there is a subgroup $G_1 \leq G$ that contains a p-Sylow subgroup of G and is realizable over K. Then there is a subgroup $G_2 \leq G_1$ that contains a p-Sylow subgroup of G and is realizable over L.*

Proof. Let F/K be a G_1-extension. Let $G_2 := \mathrm{Gal}(F/F \cap L) \leq G_1 \leq G$. Then G_2 is isomorphic to $\mathrm{Gal}(FL/L)$ and hence realizable over L. But as $p \nmid [F \cap L : K] = [G_1 : G_2]$, G_2 must also contain a p-Sylow subgroup of G. □

We shall use the following lemma to pass from tame realizations to wild realizations:

Lemma 3.1.7. *Let G be a metacyclic p-group and k a p-adic field. Then G is realizable over k.*

Proof. Let $k \neq \mathbb{Q}_2$ be a p-adic field, $n := [k : \mathbb{Q}_p]$ and q the number of p-power roots of unity in k. At first assume $q > 2$. Let $M_p(k)$ be the maximal pro-p extension of k and $\mathfrak{G}_k := \mathrm{Gal}(M_p(k)/k)$. Then $\mathfrak{G}_k$ has the pro-p presentation (0.2.8).

In such a case $n \geq 2$ and $\mathfrak{G}_k$ has an epimorphism onto the free pro-p group $F_p(2) = \langle f_1, f_2 \rangle$ on the 2 generators f_1, f_2 which can be obtained simply by sending $x_2 \to f_1$, $x_4 \to f_2$ and $x_i \to 1$ for every $i \neq 2, 4$. In particular, G is realizable over k.

Now assume $q \leq 2$. If $p \neq 2$, then $q = 1$ and $\mathfrak{G}_k$ is the free pro-p group $F_p(n+1)$. Since $n \geq 1$, in this case as well G is realizable over k.

Assume $p = q = 2$ and $n \geq 2$, then $\mathfrak{G}_k$ has one of the pro-p presentations given by (0.2.9) and (0.2.10) if n is even and (0.2.11) if n is odd. In the cases described in (0.2.9) and (0.2.10), $F_2(2) = \langle f_1, f_2 \rangle$ is an epimorphic image of $\mathfrak{G}_k$ by again sending $x_2 \to f_1, x_4 \to f_2$ and $x_i \to 1$ for every $i \neq 2, 4$. If $n > 1$ is odd ($n \geq 3$) then $\mathfrak{G}_k$ has a presentation as in (0.2.11) and hence admits an epimorphism onto $F_2(2) = \langle f_1, f_2 \rangle$ by sending $x_3 \to f_1, x_5 \to f_2$ and $x_i \to 1$ for $i \neq 3, 5$.

We are left with the case $p = 2$, $k = \mathbb{Q}_2$ which is covered in [34]. □

Let us turn back to prove Proposition 3.1.5:

Proof. Let G be a K-preadmissible group and $p \,|\, |G|$. There are two primes $v_1(p), v_2(p)$ of K and corresponding subgroups $G^{v_1(p)}, G^{v_2(p)}$ such that $G^{v_i(p)}$ is realizable over $K_{v_i(p)}$ and contains a p-Sylow subgroup of G, for $i = 1, 2$. For every p, we shall choose two primes $w_1(p), w_2(p)$ of L, and corresponding subgroups $G^{w_i(p)} \leq G$ such that:

(1) $G^{w_i(p)}$ contains a p-Sylow subgroup of G,

(2) $G^{w_i(p)}$ is realizable over $L_{w_i(p)}$,

(3) $w_1(p) \neq w_2(p)$ and $w_i(p)|p$,

for all $i = 1, 2$ and $p \,|\, |G|$. In particular, $w_i(p) \neq w_j(q)$ for any $i, j \in \{1, 2\}$ and $p \neq q$. Such a choice of primes and corresponding subgroups will show that G is L-preadmissible.

Let $p \,|\, |G|$. If one of $v_i(p)$, $i = 1, 2$, does not divide p then by Lemma 1.2.5, the p-Sylow subgroups of G are metacyclic and hence by Lemma 3.1.7, realizable over any completion L_w for any prime w of L that divides p. As p decomposes in L, we can choose both $w_1(p), w_2(p)$ to be any distinct primes of L dividing p and $G^{w_i(p)} := G(p)$, $i = 1, 2$. So let us assume $v_1(p), v_2(p)|p$ and split our proof into two cases: $p = l$ and $p \neq l$.

Case $p = l$: for every prime w of L dividing l with restriction v to K, we have $K_v \cong L_w \cong \mathbb{Q}_l$. In particular, if l divides both $v_1(l), v_2(l)$ then $G^{v_i(l)}$ is realizable over $K_{v_i(l)} \cong L_{w_i(l)}$, for any prime $w_i(l)$ of L that divides $v_i(l)$, $i = 1, 2$. Thus by setting $G^{w_i(l)} := G^{v_i(l)}$ for $i = 1, 2$, conditions (1)-(3) are satisfied for $p = l$.

Case $p \neq l$: By Lemma 3.1.6, for any $w_1(p)|v_1(p), w_2(p)|v_2(p)$ primes of L, there are two subgroups $G^{w_1(p)} \leq G^{v_1(p)}, G^{w_2(p)} \leq G^{v_2(p)}$, each containing a p-Sylow subgroup of G, such that $G^{w_i(p)}$ is realizable over $L_{w_i(p)}$, for $i = 1, 2$.

The primes $w_i(p)$, and the corresponding subgroups $G^{w_i(p)} \leq G$ for $i = 1, 2$, $p \,|\, |G|$ were chosen so that conditions (1)-(3) hold and therefore G is L-preadmissible. □

Lemma 3.1.6 can also be used to extend admissibility from K to L. However certain restrictions are required:

Corollary 3.1.8. *Let l be a prime and $\mathcal{G}$ an l-group. Let $L/\mathbb{Q}$ be a $\mathcal{G}$-extension in which l splits completely and K a subfield of L. Then any group G that is K-admissible and has no metacyclic Sylow subgroups is also L-admissible.*

Proof. As G is K-admissible there is a G-extension F/K such that for every $p \,|\, |G|$ there are two primes $v_1(p), v_2(p)$ of K, the decomposition groups of which in F/K contain a p-Sylow subgroup of G.

We claim FL/L is a G-extension that satisfies Schacher's criterion (Theorem 0.1.2). The decomposition groups of $v_i(p)$ in F/K are not metacyclic and hence $v_i(p)|p$ for all $p \,|\, |G|, i = 1, 2$. For every $i = 1, 2$, $p \,|\, |G|$, choose a prime $w_i(p)$ of L that divides $v_i(p)$. By Lemma 3.1.6, for $p \neq l$ that divides $|G|$ and $i = 1, 2$, the decomposition groups of $w_i(p)$ in FL/L contain a p-Sylow subgroup of G. When $p = l$, $K_{v_i} \cong L_{w_i}$ and hence the decomposition groups of v_i in F/K are the same as those of w_i in FL/L, for $i = 1, 2$.

For all $p||G|$, we have a p-Sylow subgroup of G that is contained in a decomposition group of $\mathrm{Gal}(FL/L)$ and hence in $\mathrm{Gal}(FL/L)$. In particular if $p^k||G|$ then $p^k|| \,\mathrm{Gal}(FL/L)|$ and hence $|G|$ divides $|\,\mathrm{Gal}(FL/L)|$. Since $\mathrm{Gal}(FL/L)$ is isomorphic to a subgroup of G we have $\mathrm{Gal}(FL/L) \cong G$. It follows that FL/L is a G-extension and for every $p||G|$ there are two primes $w_1(p), w_2(p)$ of L whose decomposition groups contain p-Sylow subgroups of G. This proves the claim and hence that G is L-admissible. □

To prove Theorem 0.1.10 we are left to prove:

Proposition 3.1.9. *Let l be a prime and $\mathcal{G}$ an l-group. Let $L/\mathbb{Q}$ be a $\mathcal{G}$-extension in which l splits completely. Let $\mathcal{H} \leq \mathcal{G}$ be a subgroup for which $S(D, \mathcal{H}) > 1$ for every subgroup $D \leq \mathcal{G}$ that appears as a decomposition group. Then any L-preadmissible group is also $K = L^{\mathcal{H}}$ preadmissible.*

Proof. Let G be an L-preadmissible group. For every $p \,|\, |G|$, there are two primes $w_1(p), w_2(p)$ of L and corresponding subgroups $G^{w_1(p)}, G^{w_2(p)}$, such that $G^{w_i(p)}$ is realizable over $L_{w_i(p)}$ and contains a p-Sylow subgroup of G.

Similarly to the proof of Proposition 3.1.5, we show that the primes $w_i(p)$ can be chosen such that $w_i(p)|p$ for every $i = 1, 2$ and $p \,|\, |G|$. If $w_i(p)$ does not divide

p by Lemma 1.2.5, every p-Sylow subgroup $G(p)$ is metacyclic. In such a case, by Lemma 3.1.7, $G(p)$ is realizable over L_w for every prime w that divides p. We replace every $w_i(p)$ that does not divide p by a prime w that divides p and is different from $w_j(p)$, $j = 1, 2$, and set $G^w := G(p)$. We obtain a set of primes $\{w_i(p) | i = 1, 2, p \,|\, |G|\}$ and corresponding subgroups $G^{w_i(p)}$ such that for every $i = 1, 2$ and $p \,|\, |G|$:

(1) $w_i(p)|p$,

(2) $G^{w_i(p)}$ is realizable over $L_{w_i(p)}$,

(3) $G^{w_i(p)}$ contains a p-Sylow subgroup of G.

Fix a rational prime $p \,|\, |G|$, a prime w_0 of L dividing p and set $D = D(L/\mathbb{Q}, w_0)$. Since $L/\mathbb{Q}$ is Galois, for every $i = 1, 2$, $G^{w_i(p)}$ is realizable over $L_{w_i(p)}$ and hence over L_w for any prime w of L that divides p. By the correspondence in Section 3.1.1 the existence of two split double cosets in $(D, \mathcal{H})$ implies by (3.1.1) that there are two primes $v_1(p), v_2(p)$ of K for which $[K_{v_i(p)} : \mathbb{Q}_p] = |D|$. Thus, there is a unique prime w_i of L that divides $v_i(p)$. For this prime we have $L_{w_i} \cong K_{v_i(p)}$. Therefore $G^{w_i(p)}$ is realizable over $K_{v_i(p)}$ for $i = 1, 2$ and $p \,|\, |G|$, which shows that G is K-preadmissible. □

Theorem 0.1.10 follows and we can now also prove Corollary 0.1.11:

Proof. Let S be the set of rational primes p for which $\mathbb{Q}(\mu_p)$ is contained in a $\mathcal{G}$-extension. Since such primes p must satisfy $[\mathbb{Q}(\mu_p) : \mathbb{Q}] = p - 1 \leq |\mathcal{G}|$, S is finite.

By [45] for odd l (see also [49, Chap. 2]) and [40] for $l = 2$ (see also [35, Chap. IX, §6]), there are $\mathcal{G}$-extensions of $\mathbb{Q}$ in which l splits completely. Furthermore, in [49, Chap. 2] and [35, Chap. IX, §6], each ramified prime is chosen from an infinite set and hence there is a $\mathcal{G}$-extension $L/\mathbb{Q}$ in which l-splits completely and the primes of S are unramified. Since any extension by roots of unity that is contained in a $\mathcal{G}$-extension must be ramified at some prime of S, the only roots of unity in L are $\{1, -1\}$.

Let $K = L^{\mathcal{H}}$. By Theorem 0.1.10, K and L are equivalent by preadmissibility. Since there are no odd order roots of unity in K and L, we may apply Corollary 0.2.8 and deduce that every odd order group is K-preadmissible (resp. L-preadmissible) if and only if it is K-admissible (resp. L-admissible). But by Theorem 0.1.10, K and L are equivalent by preadmissibility and hence every odd order group is K-admissible if and only if it is L-admissible. □

3.2 Constructions

3.2.1 Sequences of l-groups

According to Corollary 0.1.11, in order to construct preadmissibly equivalent fields with different degrees over $\mathbb{Q}$, it suffices to find pairs of l-groups $\mathcal{H} < \mathcal{G}$ that satisfy the condition: $S(D, \mathcal{H}) > 1$ for any metacyclic subgroup $D \leq \mathcal{G}$. We shall now provide a criterion on sequences of pairs $\mathcal{H} < \mathcal{G}$ that guarantees that this condition is satisfied.

Fix a rational prime l. Let $(\mathcal{G}_n)_{n\in N}$ denote a sequence of l-groups such that $\mathcal{G}_n \leq \mathcal{G}_{n+1}$ and $\mathcal{G}_n \leq S_{l^n}$ for every $n \in \mathbb{N}$. Let α be an element of order l in $\mathcal{G}_k$ for some $k \in \mathbb{N}$ and $\mathcal{H} = \langle\alpha\rangle$.

Proposition 3.2.1. *Let d_n denote the maximal order of a metacyclic subgroup of $\mathcal{G}_n$, $n \in \mathbb{N}$. Assume the sequence $(\mathcal{G}_n)_{n\in\mathbb{N}}$ satisfies:*
(1) $\lim_{n\to\infty} \frac{|\mathcal{G}_n|}{d_n} = \infty$,
(2) *the element α has infinitely many conjugates in $\cup_{n\in\mathbb{N}}\mathcal{G}_n$.*
Then there is an N such that for every $n \geq N$ and every metacyclic subgroup $D \leq \mathcal{G}_n$ we have $S(D, \mathcal{H}) > 1$.

Remark 3.2.2. Let c_n denote the maximal order of an element in $\mathcal{G}_n$. Then $d_n \leq c_n^2$. Therefore the condition $\lim_{n\to\infty} \frac{|\mathcal{G}_n|}{c_n^2} = \infty$ suffices in order for $\mathcal{G}$ to satisfy (1). Let $O_{\mathcal{G}_n}(\alpha)$ denote the orbit of α under conjugation in $\mathcal{G}_n$. Condition (2) can also be stated as $\lim_{n\to\infty} |O_{\mathcal{G}_n}(\alpha)| = \infty$.

It follows from Proposition 3.2.1 and Corollary 0.1.11 that:

Corollary 3.2.3. *Let $(\mathcal{G}_n)_{n=1}^{\infty}$ and $\mathcal{H}$ be as in Proposition 3.2.1. Then there is an N such that for every $n \geq N$ there exists a $\mathcal{G}_n$-extension $L/\mathbb{Q}$ for which $K = L^{\mathcal{H}}$ and L are equivalent by preadmissibility and have the same odd order admissible groups.*

In order to prove Proposition 3.2.1 we first obtain a bound on the number of occurrences of a given cycle structure (a cycle structure is also often referred to as a partition) in an embedding of a metacyclic group in S_n.

Let S_∞ be the group of all permutations of $\mathbb{N}$ that fix all but finitely many elements. Identify S_n with the subgroup of S_∞ that fixes all elements in $\mathbb{N}\backslash\{1, .., n\}$. Note that S_∞ can also be viewed as $S_\infty = \bigcup_{n\in\mathbb{N}} S_n$. Every element $\sigma \in S_\infty$ has a cycle structure $x = p(\sigma)$ which is a vector $(a_1, a_2, ...)$ with $a_i \geq a_{i+1}$ such that $a_i = 1$ for all $i \in \mathbb{N}$ but a finite number of i's and for which σ is a product of disjoint cycles $(\sigma_i)_{i\in\mathbb{N}}$ where σ_i is an a_i-cycle for all $i \in \mathbb{N}$. The order of σ in S_∞ is $\mathrm{lcm}_{i\in\mathbb{N}}(a_i)$ and hence depends only on the cycle structure x. We denote it by $o(x)$. Denote by $l(x)$ the length of x: $l(x) := \sum_{a_i\neq 1} a_i$.

Definition 3.2.4. Let G be a finite solvable group. Then there is a sequence $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_k = G$ such that H_i is normal in H_{i+1} and H_{i+1}/H_i is cyclic. The cyclicity level of G is defined to be the minimal number k for which such a sequence exists.

Lemma 3.2.5. *Fix a number $k \in \mathbb{N}$ and some cycle structure x in S_∞. Then there is a number $b \in \mathbb{N}$ such that for every solvable group G of cyclicity level k and every embedding $\phi : G \hookrightarrow S_\infty$ there are at most b elements with cycle structure x in $\phi(G)$.*

Proof. By induction on k. The case $k = 0$ is trivial, for example take $b = 1$. Assume by induction that every group of cyclicity level $< k$ has at most e_y elements of cycle structure y (in any embedding). We fix ϕ and show that the number of elements

of cycle structure x in $\phi(G)$ is bounded by a bound that depends only on k and x. We shall identify G with $\phi(G)$.

Let H be a normal subgroup of G of cyclicity level $k-1$ such that $C := G/H$ is cyclic and let $\tau \in G$ be an element for which $\langle \tau H \rangle = C$. Let $u \in G$ be an element of cycle structure x. The order of the coset uH in C divides the order of u which is $o(x)$. As C is cyclic it contains at most $o(x)$ elements of order dividing $o(x)$ and hence there are at most $o(x)$ cosets in C that contain an element of cycle structure x.

It remains to bound the number of elements with cycle structure x in a given coset uH. Let v be another element in uH with cycle structure x. The element uv^{-1} is in H and has length $l(uv^{-1}) \leq 2l(x)$. For every cycle structure y, with length $l(y) \leq 2l(x)$ (clearly there are only finitely many such) there are at most e_y elements with cycle structure y in H and hence H contains at most $\sum_{\{y:l(y)\leq 2l(x)\}} e_y$ elements with a cycle structure of length $\leq 2l(x)$. The map $uH \to H$ that sends $v \in uH$ to $u^{-1}v \in H$ is injective and therefore the coset uH contains at most $\sum_{\{y:l(y)\leq 2l(x)\}} e_y$ elements with cycle structure x. Summing over the cosets of C whose order divide $o(x)$ we get:

$$|\{\sigma \in G | p(\sigma) = x\}| \leq b := o(x) \sum_{\{y:l(y)\leq 2l(x)\}} e_y.$$

□

For $k = 2$, we have:

Corollary 3.2.6. *Let x be any cycle structure. There exists a number $b \in \mathbb{N}$ for which every metacyclic subgroup $D \hookrightarrow S_\infty$ contains at most b elements with cycle structure x.*

Example 3.2.7. The maximal number of transpositions in an abelian 2-group of rank r is r.

Example 3.2.8. The maximal number of transpositions in a metacyclic group is 4. The subgroup $\langle (123)(45), (12) \rangle$ of S_5 is a metacyclic group with 4 transpositions, namely $(12), (23), (13), (45)$. By following one step of the induction in Lemma 3.2.5 and carefully counting the possible cycle structures for the elements $u^{-1}v$, one can show that for any n, there cannot occur 5 transpositions in any metacyclic subgroup of S_n.

In general, given a cycle structure x and some $n \in \mathbb{N}$, it seems an interesting but also a hard problem to find a good bound on the number of occurrences of x in an embedding of a group of cyclicity level n.

We can now prove Proposition 3.2.1:

Proof. For two subgroups $A, B \leq \mathcal{G}_r$ and $n \geq r$, denote

$$X_n(A, B) := |\{x \in \mathcal{G}_n | A \cap B^x = 1\}|,$$

where B^x denotes xBx^{-1}. Since a double coset AxB splits if and only if $A \cap B^x = 1$, the number $X_n(A, B)$ is the number of elements of $\mathcal{G}_n$ that lie in split double cosets of A, B in $\mathcal{G}_n$.

Recall that $\mathcal{H}$ was defined to be a subgroup of $\mathcal{G}_k$. We shall show that there is an N such that for every $n \geq N$ and every metacyclic subgroup D of $\mathcal{G}_n$, $X_n(D, \mathcal{H}) > |D||\mathcal{H}|$. This will prove that there are at least two split double cosets in $\mathcal{G}_n$ for $n \geq N$.

Let T denote the set of all l-cycles in S_{l^n}. Then for $D \leq \mathcal{G}_n$:

$$X_n(D, \mathcal{H}) = |\mathcal{G}_n| - |\{x \in \mathcal{G}_n | D \cap \mathcal{H}^x \neq 1\}| = |\mathcal{G}_n| - |\{x \in \mathcal{G}_n | \alpha^x \in D\}| =$$

$$= |\mathcal{G}_n| - |\dot{\bigcup_{\sigma \in D \cap T}} \{x | \alpha^x = \sigma\}| = |\mathcal{G}_n| - \sum_{\tau \in T \cap D} |\{x | \alpha^x = \tau\}|.$$

By Corollary 3.2.6 there is a number b for which any metacyclic subgroup of S_∞ contains at most b elements of cycle structure $p(\alpha)$. Thus,

$$X_n(D, \mathcal{H}) \geq |\mathcal{G}_n| - b \cdot |N_{\mathcal{G}_n}(\alpha)|. \tag{3.2.1}$$

But by conditions (1) and (2):

$$\lim_{n\to\infty} \frac{|\mathcal{H}|d_n + b \cdot |N_{\mathcal{G}_n}(\alpha)|}{|\mathcal{G}_n|} = \lim_{n\to\infty} \frac{|\mathcal{H}|d_n}{|\mathcal{G}_n|} + \frac{b}{|O_{\mathcal{G}_n}(\alpha)|} = 0. \tag{3.2.2}$$

Therefore there is an N for which $|\mathcal{G}_n| > |\mathcal{H}|d_n + b \cdot |N_{\mathcal{G}_n}(\alpha)|$ holds for all $n \geq N$. Using the inequality (3.2.1) we obtain:

$$X_n(D, \mathcal{H}) \geq |\mathcal{G}_n| - b \cdot |N_{\mathcal{G}_n}(\alpha)| > d_n|\mathcal{H}| \geq |D||\mathcal{H}|$$

for every $n \geq N$ and every metacyclic subgroup $D \leq \mathcal{G}_n$. □

3.2.2 Sylow subgroups of the symmetric group

We use Proposition 3.2.1 to construct explicit examples of pairs $(\mathcal{G}, \mathcal{H})$ that satisfy the conditions of Corollary 0.1.11:

Example 3.2.9. Let l be a prime and $n \geq 2$. Let α_1 be the l-cycle $(1\, 2 \cdots l)$, α_2 the product of l l-cycles:

$$\alpha_2 := (1\ l+1\ 2l+1 \cdots (l-1)l+1)(2\ l+2 \cdots (l-1)l+2) \cdots (l\ 2l\ 3l \cdots l^2).$$

For $1 \leq r \leq n$, define α_r to be the product of l^{r-1} l-cycles:

$$\alpha_r := (1\ l^{r-1}+1 \cdots (l-1)l^{r-1}+1) \cdots (l^{r-1}\ 2l^{r-1} \cdots l^r).$$

The group $\mathcal{G}_n := \langle \alpha_1, \ldots, \alpha_n \rangle$ is a well known example of an l-Sylow subgroup of S_{l^n} (see [18, §5.9]). In particular $|\mathcal{G}_n| = l^{\frac{l^n-1}{l-1}}$. Let $\mathcal{H} = \langle \alpha_1 \rangle$. We shall prove:

Proposition 3.2.10. *If $n \geq 3$, then $S(D, \mathcal{H}) > 1$ for every metacyclic subgroup $D \leq \mathcal{G}_n$.*

It follows from Corollary 0.1.11, that:

Corollary 3.2.11. *For $n \geq 3$, there is a number field L_n which is Galois over $\mathbb{Q}$ with $\mathrm{Gal}(L_n/\mathbb{Q}) \cong \mathcal{G}_n$ such that L_n and $K_n = L_n^{\mathcal{H}}$ are equivalent by preadmissibility.*

Furthermore we shall prove that Proposition 3.2.10 and Corollary 3.2.11 hold for $n \geq 2$ and $l \geq 5$ or $n \geq 3$. The smallest such example therefore appears when $l = 2$ and $n = 3$, i.e. $\mathcal{G} := \mathcal{G}_n = S_8(2)$ which is of order 128. For $l = 3$ and $n = 2$, $\mathcal{G}_n = S_9(3) = \langle (123), (147)(258)(369) \rangle$, $\mathcal{H} = \langle (123) \rangle$ and Proposition 3.2.10 does not hold since $S(D, \mathcal{H}) = 1$ for $D = \langle (123), (456) \rangle$. For $l = 2$ and $n = 2$, $\mathcal{G}_n = S_4(2)$ is the Quaternion group which is itself metacyclic and hence $S(D, \mathcal{H}) = 0$ for $D = \mathcal{G}_n$.

Before proving Proposition 3.2.10, let us find the l-cycles in $\mathcal{G}_n$. The following l^{n-1} l-cycles are conjugates of α_1 in $\mathcal{G}_n$:

$$\beta_1 := (1 \cdots l), \beta_2 := (l+1 \cdots 2l), ..., \beta_{l^{n-1}} := (l^n - l + 1 \cdots l^n).$$

Let $T_0 = \{\beta_i | 1 \leq i \leq l^{n-1}\}$.

Lemma 3.2.12. *1. All l-cycles in $\mathcal{G}_n$ are of the form β_i^j for some i and j.*

2. T_0 is the set of conjugates of α_1 in $\mathcal{G}_n$.

Proof. 1. Assume $\gamma \in \mathcal{G}_n$ is another l-cycle that is not of this form. Without loss of generality we can assume $\gamma = (b_1\ b_2 \cdots b_l)$ where $b_1 = 1$. The subgroup $\langle \alpha_1, \gamma \rangle$ is contained in an l-Sylow subgroup of the symmetric group on symbols $\{1, ..., l, b_2, ..., b_l\}$. The latter is contained in S_{2l-1}. An l-Sylow subgroup of S_{2l-1} is isomorphic to C_l and hence any two l-cycles in such group are powers of each other. Thus $\gamma = \alpha_1^j = \beta_1^j$ for some j, contradiction.

2. The group $\overline{\mathcal{G}}_n := \mathcal{G}_n/[\mathcal{G}_n, \mathcal{G}_n]$ is isomorphic to C_l^n (see [18, §5.9] and [24, Lemma 2.11]). As all β_i, $1 \leq i \leq l^{n-1}$ are conjugates they are mapped under the natural map $\pi : \mathcal{G}_n \to \overline{\mathcal{G}}_n$ to the same nontrivial element. This shows that for $1 \leq i \leq l^{n-1}$ and $1 \leq j \leq l-1$, $\pi(\beta_i^j) = \pi(\alpha_1)$ only if $j = 1$. Thus, the only conjugates of α_1 in $\mathcal{G}_n$ are the elements of T_0.

□

We can now prove Proposition 3.2.10:

Proof. Fix an $n \geq 2$ and a metacyclic subgroup D of $\mathcal{G}_n$. We shall calculate $X_n(D, \mathcal{H}) := |\{x | D \cap \mathcal{H}^x = \{1\}\}|$. Any metacyclic subgroup of $\mathcal{G}_n$ contains at most two elements of T_0 and hence:

$$X_n(D, \mathcal{H}) = |\mathcal{G}_n| - |\{x \in \mathcal{G}_n | D \cap \mathcal{H}^x \neq 1\}| = |\mathcal{G}_n| - |\{x \in \mathcal{G}_n | \alpha_1^x \in D\}| =$$

$$= |\mathcal{G}_n| - |\dot{\bigcup_{\sigma \in D \cap T_0}} \{x | \alpha_1^x = \sigma\}| = |\mathcal{G}_n| - \sum_{\sigma \in D \cap T_0} |\{x | \alpha_1^x = \sigma\}| \geq |\mathcal{G}_n| - 2 \cdot |N_{\mathcal{G}_n}(\alpha_1)|,$$

where $N_{\mathcal{G}_n}(\alpha_1)$ denotes the normalizer of α_1 in $\mathcal{G}_n$. It is of order $N_{\mathcal{G}_n}(\alpha_1) = \frac{|\mathcal{G}_n|}{|O_{\mathcal{G}_n}(\alpha_1)|}$. As $T_0 = O_{\mathcal{G}_n}(\alpha_1)$ is of cardinality l^{n-1}, we have $X_n(D,\mathcal{H}) \geq |\mathcal{G}_n|(1-\frac{2}{l^{n-1}})$.

The maximal order of an element in $S_{l^n}(l)$ is l^n and hence the cardinality of D is at most $l^n \cdot l^n = l^{2n}$. So, $|D||\mathcal{H}| \leq l^{2n} \cdot l = l^{2n+1}$. Thus, in order for $X_n(D,\mathcal{H}) > |D||\mathcal{H}|$ to hold it suffices that:

$$|\mathcal{G}_n|(1-\frac{2}{l^{n-1}}) = l^{\frac{l^n-1}{l-1}}(1-\frac{2}{l^{n-1}}) > l^{2n+1}.$$

This inequality holds whenever:
(1) $n = 2, l \geq 5$,
(2) $n = 3, l \geq 3$ or
(3) $n \geq 4$.

This covers all cases except for $l = 2, n = 3$. We shall now restrict to this case. Let

$$\mathcal{G} := \mathcal{G}_3 = S_8(2) = \langle (12), (13)(24), (15)(26)(37)(48) \rangle.$$

The transpositions in $\mathcal{G}$ are $T_0 = \{(12), (34), (56), (78)\}$.

Assume on the contrary $D \leq \mathcal{G}$ is a metacyclic group for which $S(D,\mathcal{H}) \leq 1$. Then $X_n(D,\mathcal{H}) \leq |D||\mathcal{H}|$. A metacyclic subgroup of $\mathcal{G}$ contains at most 2 transpositions. We shall split the proof into two cases according to whether D contains two transpositions or at most one.

Assume D contains at most one transposition. Then

$$X_n(D,\mathcal{H}) = \{x || x^{-1}\mathcal{H}x \cap D| = 1\} \geq \frac{3}{4}|\mathcal{G}| = 3 \cdot 2^5.$$

But, if $|D||\mathcal{H}| \geq 3 \cdot 2^5$ then $|D||\mathcal{H}| = 2^7$ which implies $D\mathcal{H} = \mathcal{G}$ and $|D| = 2^6$. Let us show that $\mathcal{G}$ has no metacyclic subgroup of order 2^6. Let $\Phi = \mathcal{G}^2[\mathcal{G},\mathcal{G}]$ be the Frattini subgroup of $\mathcal{G}$ and let $\pi : \mathcal{G} \to \mathcal{G}/\Phi = C_2^3$ be the natural map. If D is metacyclic of order 2^6 then it maps under π onto a subgroup of some C_2^2. As $\pi^{-1}(C_2^2)$ contains at most 2^6 elements we must have $D = \pi^{-1}(C_2^2)$. In such a case D contains $[\mathcal{G},\mathcal{G}]$ and a transposition and hence must also contain T_0, contradiction.

Assume now that D contains two transpositions. Then $X_n(D,\mathcal{H}) = 2^6$ and hence $|D| = 2^6$ or $|D| = 2^5$. We have seen $|D| = 2^6$ cannot occur. Let us show that there is no metacyclic subgroup of $\mathcal{G}$ of order 2^5 which contains two transpositions. Assume without loss of generality $(12) \in D$. There are three cases: $D \supseteq \langle (12), (34) \rangle$, $D \supseteq \langle (12), (56) \rangle$ and $D \supseteq \langle (12), (78) \rangle$.

Case $D \supseteq \langle (12), (34) \rangle$: Let $\beta_i = (2i-1, 2i), 1 \leq i \leq 4$, $\tau_1 = (13)(24), \tau_2 = (57)(68)$ and $u = \alpha_3 = (15)(26)(37)(48)$. Then

$$S_8(2) = (\langle \alpha_1 \rangle \wr \langle \alpha_2 \rangle) \wr \langle \alpha_3 \rangle = (\langle \beta_1, \beta_2 \rangle \rtimes \tau_1) \times (\langle \beta_3, \beta_4 \rangle \rtimes \tau_2)) \rtimes \langle u \rangle.$$

Thus, any element $x \in S_8(2)$ can be written uniquely in the form

$$(\prod_{i=1}^{4} \beta_i^{t_i(x)}) \tau_1^{s_1(x)} \tau_2^{s_2(x)} u^{w(x)}$$

for some $t_i(x), s_1(x), s_2(x), w(x) \in \{0,1\}$ and $i = 1,..,4$. If there is an element $x \in D$ that has $w(x) = 1$ then $x^{-1}(12)x$ is a transposition that is not (12) nor (34) leading to a contradiction. Thus D can be assumed to be a subgroup of $\mathcal{G}_0 = (\langle\beta_1, \beta_2\rangle \rtimes \tau_1) \times (\langle\beta_3, \beta_4\rangle \rtimes \tau_2)$. Let Φ_0 be the Frattini subgroup of $\mathcal{G}_0$ and let $\pi_0 : \mathcal{G}_0 \to \mathcal{G}_0/\Phi_0 = C_2^4$ be the natural map. Then for any subgroup $C_2^2 \cong U \leq \mathcal{G}_0/\Phi_0$ one has $|\pi_0^{-1}(U)| \leq 2^4$. Therefore there is no metacyclic subgroup of $\mathcal{G}_0$ of order 2^5.

Case $D \supseteq \langle(12),(56)\rangle$: Clearly $D \subseteq N_{\mathcal{G}}(\langle(12),(56)\rangle)$ but

$$N_{\mathcal{G}}(\langle(12),(56)\rangle) = \langle\beta_1, \beta_2, \beta_3, \beta_4, u\rangle$$

is of cardinality 2^5. Thus, if $|D| = 2^5$ then $D = N_{\mathcal{G}}(\langle(12),(56)\rangle)$ which cannot occur since D would then contain all transpositions.

Case $D \supseteq \langle(12),(78)\rangle$: $D \subseteq N_{\mathcal{G}}(\langle(12),(78)\rangle)$ but

$$N_{\mathcal{G}}(\langle(12),(78)\rangle) = \langle\beta_1, \beta_2, \beta_3, \beta_4, \tau_1\tau_2 u\rangle$$

is of cardinality 2^5. Thus if $|D| = 2^5$, $D = N_{\mathcal{G}}(\langle(12),(78)\rangle)$ which again cannot occur. □

3.3 Arithmetic equivalences

In this section we recall some characterizations of arithmetic equivalence and local isomorphism and use them to show the implications of diagram (3.1) and prove that any other implication that holds is a composition of these implications. To prove the latter, we show that any implication which is not a composition of the implications of the diagram fails to hold. For this, it suffices to give examples for the non-implications: $2 \not\Rightarrow 1$, $3 \not\Rightarrow 4$ and $4 \not\Rightarrow 3$. The non-implication $3 \not\Rightarrow 4$ appears in Example 3.3.4, $2 \not\Rightarrow 1$ appears in [27] and in Example 3.3.2, and $4 \not\Rightarrow 3$ follows from Remark 3.3.1.

3.3.1 Arithmetic equivalence

By [25, Chap. 3, Theorem 1.4], two arithmetically equivalent number fields have the same $\mathbb{Q}$-normal closure. Let us therefore assume K and L are number fields with the same $\mathbb{Q}$-normal closure M and denote $\mathcal{G} = \mathrm{Gal}(M/\mathbb{Q}), \mathcal{H} = \mathrm{Gal}(M/K)$ and $\mathcal{H}' = \mathrm{Gal}(M/L)$.

Let p be a rational prime and $v_1, \ldots, v_r$ the primes of K dividing it, ordered by decreasing inertial degrees $f_i = f(v_i|p)$, $i = 1, \ldots, r$. The *splitting type* of p in K is the vector $(f_1, \ldots, f_r)$.

The fields K and L are arithmetically equivalent if and only if all rational primes have the same splitting type in K and L (see [25, Chap. 3, §1]). It turns out by a similar correspondence to that in Section 3.1.1 (see [39, §1]) that all rational primes have the same splitting type in K and L if and only if the coset types $(C, \mathcal{H})$ and $(C, \mathcal{H}')$ are the same for any cyclic subgroup $C \leq \mathcal{G}$. If $\mathcal{H}$ and $\mathcal{H}'$ satisfy the latter they are said to be *Gassmann equivalent*. It follows that if K

and L are arithmetically equivalent then $\mathcal{H}$ and $\mathcal{H}'$ are Gassmann equivalent and hence $|\mathcal{H}| = |\mathcal{H}'|$ and $[K : \mathbb{Q}] = [L : \mathbb{Q}]$.

Remark 3.3.1. The examples of Section 3.2.2 therefore show that two number fields which are equivalent by preadmissibility (or by admissibility of odd order groups) can have different degrees over $\mathbb{Q}$ and hence need not be arithmetically equivalent.

Note that Gassmann equivalence has another well known characterization, namely $\mathcal{H}$ and $\mathcal{H}'$ are Gassmann equivalent if and only if for every $g \in \mathcal{G}$:

$$|g^{\mathcal{G}} \cap \mathcal{H}| = |g^{\mathcal{G}} \cap \mathcal{H}'|,$$

where $g^{\mathcal{G}}$ denotes the conjugacy class of g in $\mathcal{G}$.

3.3.2 Local isomorphism

For a number field F, let $P(F)$ denote the set of primes of F. By [20], Lemma 7, two number fields K and L are locally isomorphic if and only if there is a bijection $\phi : P(K) \to P(L)$ such that $K_v \cong L_{\phi(v)}$ for every $v \in P(K)$.

It follows that two locally isomorphic number fields K and L (with a map ϕ as above) are also arithmetically equivalent (since every p has the same inertial degree in K_v and $L_{\phi(v)}$) and equivalent by preadmissibility (since a group is realizable over K_v if and only if it is realizable over $L_{\phi(v)}$). This shows the remaining implications in diagram (3.1).

In [27], Komatsu gave an example of two locally isomorphic number fields, given explicitly as radical extensions of $\mathbb{Q}$, that are not isomorphic (showing the non-implication $2 \not\Rightarrow 1$). In fact, a complete classification of locally isomorphic radical extensions appears in [22].

The following is a simple construction, using a different approach from [27] and [22], that assigns to every two Gassmann equivalent subgroups of the symmetric group, two locally isomorphic number fields.

Example 3.3.2. Let $M/\mathbb{Q}$ be a Galois extension of number fields and T/M an unramified S_n-extension which is Galois defined over $\mathbb{Q}$, i.e. there is an S_n-extension $F/\mathbb{Q}$ for which $T = MF$ (for such a construction see [15]).

Let $\mathcal{H}$ and $\mathcal{H}'$ be two Gassmann equivalent subgroups of S_n that are not conjugate in S_n. A method to construct such pairs $\mathcal{H}$ and $\mathcal{H}'$ is given in [39, §3].

Let $\mathcal{G} := \mathrm{Gal}(T/\mathbb{Q}) \cong \mathrm{Gal}(T/F) \times \mathrm{Gal}(T/M) \cong \mathrm{Gal}(T/F) \times S_n$. Let us identify $\mathcal{H}$ and $\mathcal{H}'$ as subgroups of the latter S_n and let $K = T^{\mathcal{H}}$ and $L = T^{\mathcal{H}'}$.

Proposition 3.3.3. *The fields K and L are locally isomorphic but $K \ncong L$.*

Proof. As $\mathcal{H}$ and $\mathcal{H}'$ were chosen to be non-conjugate in S_n and as $\mathrm{Gal}(T/F)$ commutes with S_n in $\mathcal{G}$, $\mathcal{H}$ and $\mathcal{H}'$ are not conjugate in $\mathcal{G}$ and hence $K \ncong L$.

Let us prove that K and L are locally isomorphic. As T/M is unramified all primes of M have cyclic decomposition groups. Let v be a prime of M and C a cyclic subgroup of S_n such that the decomposition group of v in T/M is (the conjugacy class of) C. By the correspondence in Section 3.1.1, there is a

bijection between the primes $v_1, \ldots, v_r$ (resp. $w_1, \ldots, w_s$) of K (resp. of L) that divide v and the double cosets $Cx_1\mathcal{H}, \ldots, Cx_r\mathcal{H}$ (resp. $Cy_1\mathcal{H}', \ldots, Cy_s\mathcal{H}'$) such that $[K_{v_i} : M_v] = \frac{|Cx_i\mathcal{H}|}{|\mathcal{H}|}$ (resp. $[L_{w_i} : M_v] = \frac{|Cy_i\mathcal{H}'|}{|\mathcal{H}'|}$). As $\mathcal{H}$ and $\mathcal{H}'$ are Gassmann equivalent in S_n the coset type $(C, \mathcal{H})$ is the same as the coset type $(C, \mathcal{H}')$. Thus $r = s$, $|\mathcal{H}| = |\mathcal{H}'|$ and one has:

$$d_i := [K_{v_i} : M_v] = \frac{|Cx_i\mathcal{H}|}{|\mathcal{H}|} = \frac{|Cy_i\mathcal{H}'|}{|\mathcal{H}'|} = [L_{w_i} : M_v]$$

for $i = 1, 2, \ldots, r$. But as T/M is unramified and M_v has a unique unramified extension of degree d_i, one has $K_{v_i} \cong L_{w_i}$, for $i = 1, \ldots, r$. This establishes a bijection ϕ for any prime v of M between the prime divisors of v in K and those in L such that $K_{v_K} \cong L_{\phi(v_K)}$ for any prime v_K of K dividing v. We therefore obtain a bijection $\phi : P(K) \to P(L)$ such that $K_{v_K} \cong L_{\phi(v_K)}$ for any prime v_K of K. Thus, K and L are locally isomorphic. □

Given a $\mathcal{G}$-extension $F/\mathbb{Q}$, the process of creating an extension $M/\mathbb{Q}$ for which MF/M is an unramified $\mathcal{G}$-extension is often called swallowing ramification or Abhyankar's Lemma.

3.3.3 Preadmissibility and arithmetic equivalence

To show $3 \not\Rightarrow 4$, we use an example from [26] of two arithmetically equivalent fields K and L that are not locally isomorphic and show that these K and L are in fact inequivalent by preadmissibility.

Example 3.3.4. Let $K = \mathbb{Q}(\sqrt[32]{m})$ and $L = \mathbb{Q}(\sqrt{2}\sqrt[32]{m})$ where $m \neq \pm 1, \pm 2$ is a square free integer that satisfies $m \equiv 1 \pmod{2^7}$. In [26, Lemma 4], Komatsu shows that K and L are arithmetically equivalent. Let us show that K and L are not equivalent by preadmissibility and nor by admissibility. Since $m \equiv 1 \pmod{2^7}$ there is a unit $u \in \mathbb{Z}_2$ for which $u^{32} = m$. So, the polynomials that define K and L factor over $\mathbb{Q}_2$ into irreducible factors as follows:

$$x^{32} - m = (x-u)(x+u)(x^2+u^2)(x^4+u^4)(x^8+u^8)(x^{16}+u^{16})$$

$$x^{32} - 2^{16}m = (x^2-2u)(x^2+2u)(x^2-2ux+2u)(x^2+2ux+2u)(x^8+16u^8)(x^{16}+2^8u^{16}).$$

Note that by [26, Lemma 10] all the above factors are irreducible in $\mathbb{Q}_2[x]$.

Therefore, there are 6 primes $v_1, \ldots, v_6$ in K and 6 primes $w_1, \ldots, w_6$ in L that divide 2. Let us assume the primes are ordered so that $[K_{v_i} : \mathbb{Q}_2] \geq [K_{v_{i+1}} : \mathbb{Q}_2]$ and $[L_{w_i} : \mathbb{Q}_2] \geq [L_{w_{i+1}} : \mathbb{Q}_2]$ for $i = 1, \ldots, 5$. Considering the above factorizations we have: $K_{v_1} = \mathbb{Q}_2(\mu_{32})$, $K_{v_2} = \mathbb{Q}_2(\mu_{16})$, $L_{w_1} = \mathbb{Q}_2(\sqrt[16]{-2})$, $L_{w_2} = \mathbb{Q}_2(\sqrt[8]{-2})$ and $[K_{v_i} : \mathbb{Q}_2] \leq 4$, $[L_{w_i} : \mathbb{Q}_2] \leq 4$ for $i \geq 3$.

Let $A := C_{16}^{10}$. By local class field theory the maximal abelian extension $K_{v_2,ab,16}$ of exponent 16 of K_{v_2} has Galois group $\mathrm{Gal}(K_{v_2,ab,16}/K_{v_2}) \cong C_{16}^{10} = A$. Similarly, $\mathrm{Gal}(K_{v_1,ab,16}/K_{v_1}) \cong C_{16}^{18}$, $\mathrm{Gal}(L_{w_1,ab,16}/L_{w_1}) \cong C_{16}^{17} \times C_2$, $\mathrm{Gal}(L_{w_2,ab,16}/L_{w_2}) \cong C_{16}^{9} \times C_2$ and $\mathrm{rk}(\mathrm{Gal}(K_{v_i,ab,16}/K_{v_i})), \mathrm{rk}(\mathrm{Gal}(L_{w_i,ab,16}/L_{w_i})) \leq 6$ for $i \geq 3$. We can

now see that A is realizable over two completions of K and only one completion of L. Thus, A is K-preadmissible but not L-preadmissible and K and L are inequivalent by preadmissibility. It also follows that A is not L-admissible but by Corollary 1.1.2, A is K-admissible (as the primes v_1, v_2 are not in S_0). Thus, K and L are inequivalent by admissibility.

Bibliography

[1] E. Allman, M. Schacher, Division algebras with $PSL(2,q)$-Galois maximal subfields. *J. Algebra* **240** (2001), no. 2, 808-821.

[2] E. Artin, J. Tate, Class field theory. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1990.

[3] E. Binz, J. Neukirch, G.H. Wenzel, A subgroup theorem for free products of pro-finite groups. *J. Algebra* **19** (1971), 104–109.

[4] J. Charbit, On p-groups and K-admissibility. Master Thesis, Technion, Haifa,(2005).

[5] S. P. Demuškin, The group of a maximal p-extension of a local field, (Russian) *Izv. Akad. Nauk SSSR Ser. Mat.* **25** (1961), 329–346.

[6] D. Chillag, J. Sonn, Sylow-metacyclic groups and Q-admissibility. *Israel J. Math.* **40** (1981), no. 3-4, 307-323.

[7] S. P. Demuškin, The group of a maximal p-extension of a local field. (Russian) *Izv. Akad. Nauk SSSR Ser. Mat.* **25** (1961), 329-346.

[8] R. Dentzer, On geometric embedding problems and semiabelian groups. *Manuscripta Math.* **86** (1995), no. 2, 199-216.

[9] H. Hasse, Number Theory. Springer-Verlag, Berlin/Heidelberg/New York, 1980.

[10] B. Huppert, Endliche Gruppen I. Springer-Verlag, Berlin/New York, 1967.

[11] B. Fein, M. Schacher, Sums of corestrictions of cyclic algebras. *Israel J. Math.* **96** (1996), part A, 243–258.

[12] B. Fein, M. Schacher, $\mathbb{Q}$-admissibility questions for alternating groups. *J. Algebra* **142** (1991), no.2, 360–382.

[13] W. Feit, $SL(2,11)$ is $\mathbb{Q}$-admissible. J. Algebra **257** (2002), no.2, 244–248.

[14] W. Feit, P. Vojta, Examples of some $\mathbb{Q}$-admissible groups. J. Number Theroy **26** (1987), no.2, 210–226.

[15] A. Frölich, On non-ramified extensions with prescribed Galois group. *Mathematika* **9** (1962), 133–134.

[16] F. Gassmann, Bemerkungen zu der vorstehenden Arbeit von Hurwitz. *Math. Z.* **25** (1926), 124–143.

[17] G. D. Grunwald, *J. Reine Angew. Math.* **169** (1933), 103-107.

[18] M. Hall, The theory of groups, Second edition.

[19] I. N. Herstein, Noncommutative rings. *The Carus Mathematical Monographs*, **no. 15**, Mathematical Association of America, 1968.

[20] K. Iwasawa, On the ring of valuation vectors. *Ann, of Math.* **57** (1953), 331–356.

[21] K. Iwasawa, Local Class Field Theory. *Oxford University Press* (1986).

[22] E. Jacobson, W. Y. Vélez, Fields arithmetically equivalent to a radical extension of the rationals. *Journal of Number Theory* **35** (1990), 227–246.

[23] U. Jannsen, K. Wingberg, Die Struktur der absoluten Galoisgruppe p-adischer Zahlkorper. *Invent. Math.* **70** (1982/83), no. 1, 71-98.

[24] H. Kisilevsky, D. Neftin, J. Sonn, On the minimal ramification problem for semiabelian groups. *to appear in Algebra and Number theory*.

[25] N. Klingen, Arithmetical similarities. *Prime decomposition and finite group theory, Oxford Mathematical Monographs. Oxford Science Publications.* The Clarendon Press, Oxford University Press, New York, 1998.

[26] K. Komatsu, On the adele rings and zeta functions of algebraic number fields. *Kodai Math. J.* **1** (1978), 394–400.

[27] K. Komatsu, On the adele rings of algebraic number fields. *Kodai Math. Sem. Rep.* **28** (1976), 78–84.

[28] J. P. Labute, Classification of Demushkin groups. *Canad. J. Math.* **19** (1967), 106-132.

[29] S. Liedahl, J. Sonn, K-admissibility of metacyclic 2-groups. Recent developments in the inverse Galois problem (Seattle, WA, 1993) *Contemp. Math.* **186** (1995), 65-73.

[30] S. Liedahl, Presentations of metacylic p-groups with applications to K-admissibility questions. *J. Algebra* **169** (1994), no. 3, 965-983.

[31] S. Liedahl, K-admissibility of wreath products of cyclic p-groups. *J. Number Theory* **60** (1996), no. 2, 211-232.

[32] M. Lochter, On equivalent number fields with special Galois groups. *Israel J.Math* **84** (1993) 89–96.

[33] D. Neftin, Admissibility and Realizability over Number fields. Submitted. arXiv:0904.3772v1.

[34] D. Neftin, U. Vishne, Admissibility under extension of number fields. Submitted. arXiv:0911.3792.

[35] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of number fields. *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 323. Springer-Verlag, Berlin* (2000).

[36] J. Neukirch, Uber das Einbettungsproblem der algebraischen Zahlentheorie. *Invent. Math.* **21** (1973), 59-116.

[37] J. Neukirch , On solvable number fields. *Invent. Math.* **53** (1979), no. 2, 135–164.

[38] J. Neukirch, Kennzeichung der p-adischen und der endlichen algebraischen Zahlkörper. *Inv. Math.* **6** (1969), 296–314.

[39] R. Perlis, On the equation $\zeta_K(s) = \zeta_L(s)$. *J. Number Theory* **9** (1977), 342–260.

[40] I. R. Safarevič, Construction of fields of algebraic numbers with given solvable Galois group. (Russian) *Izv. Akad. Nauk SSSR. Ser. Mat.*

[41] I. R. Safarevič, On p-extensions. (Russian. English summary) Rec. Math. *Mat. Sb* **20(62)** (1947), 351-363.

[42] D. Saltman, Generic Galois extensions. *Proc. Natl. Acad. Sci. U.S.A. 77*(1980), **3**, part 1, 1250-1251.

[43] D. Saltman , Galois groups of order p^3. *Comm. Algebra* **15** (1987), no. 7, 1365-1373.

[44] M. Schacher, Subfields of division rings. I. *J. Algebra* **9** (1968) 451-477.

[45] A. Scholz Uber die Bildung algebraischen Zahlkorper mit aufslosbarer galoischer Gruppe. *Math. Z.* **30** (1929),332-356.

[46] J. P. Serre, Structure de certains pro-p-groupes (d'apres Demuskin). *Sem. Bourbaki* **252** (1962-63)

[47] J. P. Serre, Galois cohomology. Springer Monographs in Mathematics. Springer-Verlag, Berlin (2002).

[48] J. P. Serre, Local fields. Graduate Texts in Mathematics, **67**. Springer-Verlag, New York-Berlin, 1979.

[49] J.-P. Serre, Topics in Galois Theory. *Jones and Bartlett*, Boston (1992).

[50] J. Sonn, Rational division algebras as solvable crossed products. *Israel J. Math.* **37** (1980), no. 3, 246-250.

[51] J. Sonn, $\mathbb{Q}$-admissibility of solvable groups. *J. Algebra* **84** (1983), no. 2, 411-419.

[52] J. Sonn, SL(2, 5) and Frobenius Galois groups over Q. *Canad. J. Math.* **32** (1980), no. 2, 281-293.

[53] J. Sonn, Brauer groups, embedding problems, and nilpotent groups as Galois groups. *Israel J. Math* **85** (1994), 391-405.

[54] J. Sonn, Epimorphisms of Demushkin groups. *Israel J. Math.* **17** (1974), 176-190.

[55] J. Sonn, On equivalence of number fields. *Israel J. Math.* **52** (1985), no. 3, 239–244.

[56] J. Sonn, Correction to: "On equivalence of number fields". *Israel J. Math.* **52** (1990), no. 3, 379.

[57] K. Uchida, Isomorphism of Galois groups. *Math. Soc. Japan* **28** (1976), 617–620.

[58] S. Wang, On Grunwald's theorem. *Ann. of Math. (2)* **51** (1950), 471-484.

[59] S. Wang, A counter-example to Grunwald's theorem. *Ann. of Math. (2)* **49** (1948), 1008-1009.

[60] E. Weiss, Algebraic number theory. *McGraw-Hill Book Co., Inc., New York-San Francisco-Toronto-London* (1963)

קבילות של חבורות סופיות
מעל שדות מספרים

דני נפטין

קבילות של חבורות סופיות
מעל שדות מספרים

חיבור על מחקר

לשם מילוי חלקי של הדרישות לקבלת התואר

דוקטור לפילוסופיה

דני נפטין

הוגש לסנט הטכניון- מכון טכנולוגי לישראל

אייר התש"עא חיפה מאי 2011

תודות

המחקר נעשה בהנחיית פרופסור יעקב סון בפקולטה למתמטיקה בטכניון.
אני מודה למועצה להשכלה גבוהה, קרן פולק ולטכניון על התמיכה הנדיבה בהשתלמותי.
ברצוני להודות ליעקב סון על השקעה אינסופית של זמן וסבלנות בהדרכתי ולימודי. אני מודה לו על היותו מורה מעודד, תמוך ונדיב.
תודה מיוחדת לחברי ליאור בארי סורוקר על העצה וההערות המועילות כל כתיבתי ועבור דיונים מעניינים.
ברצוני להודות מקרב לב לאישתי שפרה רייף ולהורי שמעון ולודמילה נפטין על כך שעודדו אותי דרך קשיים ותמכו בי בהתמדה.

תקציר

1. קבילות וקדם קבילות

אלגברת חילוק D עם מרכז K נקראת מכפלה משולבת עבור חבורה סופית G, אם ל־D תת שדה מקסימלי L שהינו גלואה מעל K כך ש־ $G \cong Gal(L/K)$. מכפלה מושלבת הינו מונח מרכזי בתורת האלגברות ממימד סופי אשר מתאר את המבנה של רוב אלגבראות החילוק אשר נבנו עד כה.

עבודה זו מתרכזת בבעיה הבאה, אשר עלתה לראשונה בשנת 1968 מעבודתו של שחר ומאז נלמדה בהרחבה.

1.1 בעיה. יהי K שדה. עבור אילו חבורות G קיימת אלגברת חילוק D עם מרכז K כך ש־D הינה מכפלה ׳משולבת עבור G?

אם ישנה אלגברת חילוק עם מרכז K שהינה מכפלה משולבת עבור G, נאמר כי G קבילה מעל K. אנו נתרכז במקרים בהם K הינו שדה מספרים. מעל שדות אלו יש את האפיון הבא.

עבור ראשוני v של K נסמן ב־K_v את ההשלמה של K על ידי v.

1.2 משפט. (שחר) יהי K שדה מספרים. חבורה סופית G הינה קבילה מעל K אם ורק אם קיימת הרחבת גלואה L/K עם חבורת גלואה $Gal(L/K) \cong G$ כך שעבור כל ראשוני p המחלק את $|G|$ ישנם שני ראשוניים v_1, v_2 של K כך ש־ $Gal(L_{w_i}/K_{v_i})$ מכילה תת חבורת p־סילו של G, עבור w_i המחלק את v_i ו־$i = 1, 2$.

נעיר כי ההכלה של תת חבורת p־סילו של G אינה תלויה בבחירת הראשוני w_i אשר מחלק את v_i.

נובע מכך כי מעל שדות מספרים בעיה 1.1 שקולה לבעית מימוש של חבורה כחבורת גלואה עם תנאים מקומיים. נקרא לתנאים מקומיים אלו קדם־קבילות.

1.3 הגדרה. יהי K שדה מספרים. חבורה סופית G תקרא קדם־קבילה מעל K אם לכל ראשוני p המחלק את $|G|$, ישנם שני ראשוניים $v_1(p), v_2(p)$ ושתי תתי חבורות $G^{1,p}, G^{2,p}$ כך ש־$G^{i,p}$ ניתנת למימוש מעל $K_{v_i(p)}$ ומכילה תת חבורת p־סילו של G, לכל $i = 1, 2$ ו־p המחלק את $|G|$.

במחקרים רבים על קבילות, הראו תחילה כי חבורה מקיימת את התנאים המקומיים של קדם־קבילות ורק לאחר מכן הראו כי היא ניתנת למימוש מעל שדה המספרים כך שהתנאים המקומיים מתקיימים. כיוון שבמרבית המקרים פשוט יותר לאמת קדם־קבילות וכיון שלעיתים קרובות קדם־קבילות גוררת קבילות, שיטה זו נמצאה כיעילה.

בפרק I נשווה בין קבילות לקדם־קבילות. נתחיל בחבורות אבליות. חבורה אבלית הינה קבילה מעל K אם ורק אם תתי חבורות הסילו שלה קבילות מעל K. לכן ניתן להצטמצם למקרה של חבורות־p אבליות. חבורת־p אבלית הינה קדם־קבילה מעל K אם ורק אם היא ניתנת למימוש מעל K_v עבור שני ראשוניים v.

שרביט וסון השתמשו במשפט גרונוולד־וונג כדי להוכיח שפרט למקרים המיוחדים של משפט זה, חבורות־p אבליות הינן קבילות אם ורק אם הן קדם־קבילות. הם השתמשו בשקילות זו בכדי לתת תנאים מפורשים עבור קבילות של חבורות אלו (למעט עבור המקרים המיוחדים). כיון שהמקרים המיוחדים מופיעים אך ורק עבור $p = 2$, נותר להבין את המקרה של חבורות־2 אבליות.

בהינתן חבורה מעגלית (ציקלית) C, וונג אפיין את הדוגמאות (המיוחדות) של קבוצות סופיות של ראשוניים S והרחבות מתאימות $L(v)/K_v$ עם חבורת גלואה שהינה תת חבורה של C לכל $v \in S$, כך שאין אף הרחבה L/K עם חבורת גלואה C עבורה $L_v = L(v)$ לכל $v \in S$.

הקושי העיקרי בבנית חבורת־p G ושדה מספרים K כך G הינה קדם־קבילה מעל K אך אינה קבילה מעליו, טמון בכך שבניגוד לדוגמאות של וונג, יש לבנות דוגמא בה לכל שני ראשוניים v_1, v_2 של K ולכל בחירה של הרחבות $L(v_i)/K_{v_i}$, עבור $i = 1, 2$, אין הרחבה L/K עם חבורת גלואה G כך ש־$L_{v_i} \cong L(v_i)$, עבור $i = 1, 2$.

מסתבר כי ישנן דוגמאות של חבורות־2 אבליות שהינן קדם־קבילות מעל שדה מספרים K ואינן קבילות מעל K. אולם כפי שהמשפט הבא מראה, דוגמאות אלו נדירות.

תהי μ_n חבורת שורשי היחידה מסדר n.

1.4 משפט. יהי K שדה מספרים ותהי A חבורת־2 אבלית שהינה קדם קבילה מעל K. אזי A <u>איננה</u> קבילה מעל K אם ורק אם ששת התנאים הבאים מתקיימים:

(1) Aניתנת למימוש מעל K_v עבור שני ראשוניים v ולא יותר,

(2) ההרחבה $K(\mu_{2^n})/K$ איננה מעגלית, עבור n גדול מספיק,

יהי s השלם הגדול ביותר עבורו $K(\mu_{2^s})/K$ הינה מעגלית,

(3) ההרחבה $K_v(\mu_{2^{s+1}})/K_v$ הינה מעגלית עבור כל ראשוני v, למעט ראשוני אחד w,

(4) הראשוני w (הנתון על ידי 3) הוא אחד מהראשוניים v_1, v_2 (הנתונים על ידי 1),

נכתוב $A = A_s \oplus A'_s$ כך ש־A_s ממעריך המחלק את 2^s ו־$A'_s = \prod_{i=1}^{r} C_{2^{k_i}}$,

כאשר $k_i > s$ לכל $i = 1, \ldots, r$,

(5) A_s הינה טריוויאלית או $A_s \cong C_2$,

(6) $r = rk(A'_s) = [K_w : \mathbb{Q}] + 1$.

בהמשך פרק I אנו מביאים דוגמאות רבות של חבורות שעבורן קדם־קבילות כן גורמת קבילות (לאו דווקא של חבורות אבליות).

2. קבילות מתונה

מעל שדה המספרים הרציונליים $\mathbb{Q}$, שחר השתמש במשפט 1.2 בכדי להראות כי לכל חבורה קבילה מעל $\mathbb{Q}$ יש תתי חבורות סילו מטא־מעגליות (metacylic). אותו טיעון מראה כי לכל חבורה קדם־קבילה יש תתי חבורות סילו מטא־מעגליות. למעשה גם הטענה ההפוכה נכונה. כלומר שכל חבורה הינה קדם־קבילה אם ורק אם יש לה תתי חבורות סילו מטא־מעגליות.

משוער כי חבורות עם תתי חבורות סילו מטא־מעגליות הינן קבילות מעל $\mathbb{Q}$, כלומר כי קדם־קבילות מעל $\mathbb{Q}$ גוררת קבילות מעל $\mathbb{Q}$. בסדרת מאמרים, סון הוכיח השערה זו עבור חבורות פתירות.

2.1 משפט. (סון) כל חבורה פתירה עם חבורות סילו מטא־מעגליות הינה קבילה מעל $\mathbb{Q}$.

לידהל הרחיב את את ההבחנה של שחר באופן הבא. יהי K שדה מספרים ו־$\sigma_{t,n}$ האוטומורפיזם של $\mathbb{Q}(\mu_n)$ עבורו $\sigma_{t,n}(\zeta) = \zeta^t$. אם G קבילה מעל K ולכל ראשוני p המחלק את $|G|$ יש רק ראשוני אחד של K המחלק אותו, אז לכל p שכזה לחבורות p־סילו של G קיים ייצוג

$$\langle x, y | x^m = y^i, y^n = 1, x^{-1}yx = y^t \rangle \tag{1}$$

כך ש־ $\sigma_{t,n} \in Gal(\mathbb{Q}(\mu_n)/K \cap \mathbb{Q}(\mu_n))$. בפרק II נוכיח את הטענה ההפוכה להבחנה של לידהל עבור חבורות פתירות. על ידי כך נוכיח את האנלוג הטבעי הבא למשפט 2.1:

2.2 משפט. יהי K שדה מספרים ו־G חבורה פתירה. נניח כי לכל p המחלק את $|G|$, לתתי חבורות ה־p־סילו של G יש הצגה כמו ב־(1) כך ש־ $\sigma_{t,n} \in Gal(\mathbb{Q}(\mu_n)/K \cap \mathbb{Q}(\mu_n))$. אזי G קבילה מעל K.

משפט זה הוכח על ידי לידהל עבור המקרה בו G עצמה היא חבורה מטא־מעגלית. יש לציין כי לא ניתן להרחיב את ההוכחה של סון עבור משפט 2.1 באופן מידי לכל שדות המספרים, כיוון שההוכחה משתמשת במשפט עמוק של נויקירש אשר אינו מתקיים בכלליות הנדרשת מעל שדות מספרים.

השיטה בה אנחנו מוכיחים את משפט 2.2 היא על ידי הוכחת עידון של משפט 2.1 המיצר הרבה הרחבות $L/\mathbb{Q}$ עם חבורת גלואה G אשר מוכלות ב$\mathbb{Q}$־אלגבראות חילוק כשדות מקסימליים והוכחה כי עבור חלק משדות אלו, ההרחבה LK/K הינה עם חבורת גלואה G ומוכלת בK־אלגברת חילוק כשדה מקסימלי. הוכחת העידון הינה התאמה של הוכחתו של סון למשפט 2.1.

כמסקנה נקבל:

2.3 מסקנה. יהי K שדה מספרים ו־G חבורה פתירה כך שלכל ראשוני p המחלק את $|G|$ יש רק ראשוני אחד של K המחלק אותו. אזי G קבילה מעל K אם ורק אם לכל p המחלק את $|G|$, לתתי החבורות p־סילו של G יש הצגה כמו ב־(1) כך ש־ $\sigma_{t,n} \in Gal(\mathbb{Q}(\mu_n)/K \cap \mathbb{Q}(\mu_n))$.

בנוסף, נגדיר בפרק II את המושג קבילות מתונה, אשר יתאר טוב יותר את סוג הקבילות המופיעה מעל $\mathbb{Q}$ ובמשפט 2.2.

יש לציין כי אם לראשוני p יש יותר ממחלק אחד ראשוני ב־K, אז יש הרבה חבורות־p קבילות מעל K אשר אינן מטא־מעגליות.

3. שקילות אריתמטית

לעיתים קרובות, שקילויות אריתמטיות בין שדות מספרים משמשות בכדי לקבוע את המידה בה תכונה אריתמטית מייחדת את השדה. דוגמא אחת היא שקילות אריתמטית. שני שדות שקולים תחת יחס זה אם יש להם את אותה פונקצית זטא של דדקינד. לשני שדות שקולים אריתמטית יש את אותו סגור $\mathbb{Q}$־נורמלי, אותה דרגה מעל $\mathbb{Q}$, דרגת שדות שארית עבור ראשוניים רציונאליים ורשימה ארוכה של תכונות אריתמטיות משותפות נוספות. בפרט אם $L/\mathbb{Q}$ הינה גלואה אז אין אף שדה מספרים K השונה מ־L אשר שקול לו אריתמטית.

נויקירש שאל האם זוג שדות אשר חבורות גלואה המוחלטות שלהם איזומורפיות, בהכרח איזומורפיים והוכיח כי בהכרח יש להם את אותו סגור $\mathbb{Q}$־נורמלי. שאלתו נענתה בחיוב באופן בלתי תלוי על ידי איוסאוה, איקדה ויושידה.

סון שאל שאלה מקבילה עבור מכלפות משולבות. זוג שדות מספרים נקראים שקולים על ידי קבילות אם אותן חבורות קבילות מעליהם. הוא הוכיח כי לזוג שדות השקולים על ידי קבילות יש את אותו סגור $\mathbb{Q}$־נורמלי. לא ידוע האם שני שדות השקולים על ידי קבילות הם בהכרח איזומורפיים. למעשה השאלה הבאה פתוחה משנת 1985:

3.1 שאלה. יהיו K ו־L שדות מספרים השקולים על ידי קבילות. האם בהכרח יש להם את אותה הדרגה מעל $\mathbb{Q}$?

עד כה שאלה זו נענתה בחיוב רק עבור מקרים מסוימים. לוכטר הראה כי אם בנוסף הדרגה $[K:\mathbb{Q}]$ הינה ראשונית או הינה 4 אז בהכרח $[K:\mathbb{Q}]=[L:\mathbb{Q}]$.

נאמר כי שני שדות שקולים על ידי קדם־קבילות אם אותן חבורות קדם־קבילות מעל שדות אלו. בפרק III, אנו בונים (אינסוף) דוגמאות של שדות מספרים L ותתי שדות (לא טרוויאליים) $K\subset L$ אשר שקולים על ידי קדם־קבילות. בנוסף נראה כי למעשה בדוגמאות אלו אותן חבורות מסדר אי זוגי קבילות מעל K ו־L. בעקבות בניות אלו והמקרים הרבים בהם קבילות וקדם־קבילות מתנהגות באופן זהה, אנו משערים:

3.2 השערה. יש שדה מספרים L ותת שדה לא טרוויאלי $K\subset L$ כך ש־K ו־L שקולים על ידי קבילות.

מעט ידוע על שקילות על ידי קבילות. אף על פי כן, במקרים רבים שקילות על ידי קדם־קבילות הינה בהישג יד ומאפשרת לחקור שקילות על ידי קבילות ביחס למשפחות שונות של חבורות. באופן דומה להוכחתו של סון עבור שקילות על ידי קבילות, ניתן להוכיח כי לזוג שדות השקולים על ידי קדם־קבילות יש את אותו סגור $\mathbb{Q}$־נורמלי. בפרט, $\mathbb{Q}$ שקול על ידי קדם־קבילות רק לעצמו. אף על פי כן ישנם שדות L שהם גלואה מעל $\mathbb{Q}$ השקולים על ידי קדם־קבילות לתתי שדות שלהם. את הטענה האחרונה ניתן לתרגם לטענה בתורת החבורות על ידי המשפט הבא על שקילות על ידי קדם־קבילות.

עבור זוג תתי חבורות A,B של חבורה סופית $\mathcal{G}$, קוסט כפול AxB נקרא מתפצל אם $|AxB|=|A||B|$.

3.3 משפט. יהי l ראשוני ו$\mathcal{G}$ חבורת־l. תהי $L/\mathbb{Q}$ הרחבה עם חבורת גלואה $\mathcal{G}$ כך ש־l מתפצל לחלוטין בL. יהי K תת שדה של L ו־$\mathcal{H}=Gal(L/K)$. אם לכל תת חבורה $D\leq\mathcal{G}$ אשר מופיעה כתת חבורת פירוק, יש שני קוסטים כפולים מתפצלים מהצורה $Dx\mathcal{H}$, אז K ו־L שקולים על ידי קדם־קבילות. אם $\mathcal{G}$ אינה מטא־מעגלית אז גם הטענה ההפוכה נכונה.

יש לציין כי הדרישה מ־l להתפצל לחלוטין מתקיימת במימושים רבים של חבורות־l כחבורות גלואה, כולל המימושים של שולץ־רייכרדט (ל־l אי זוגי) ושפרביץ' (לכל l). על ידי שימוש במשפט 3.3 ניתן להסיק את התנאי הבא לבנית שדות שקולים על ידי קדם־קבילות וקבילות של חבורות מסדר אי זוגי.

3.4 מסקנה. יהי l ראשוני. תהי $\mathcal{G}$ חבורת־l ו־$\mathcal{H}\leq\mathcal{G}$ תת חבורה כך שלכל תת חבורה $D\leq\mathcal{G}$ יש שני קוסטים כפולים מתפצלים מהצורה $Dx\mathcal{H}$. אזי יש הרחבה $L/\mathbb{Q}$ עם חבורת גלואה $\mathcal{G}$ כך ש־L ו־$K:=L^{\mathcal{H}}$ שקולים על ידי קדם־קבילות ואותן חבורות מסדר אי זוגי קבילות מעליהם.

בהמשך פרק III אנו בונים אינסוף דוגמאות לזוגות $(\mathcal{G},\mathcal{H})$ המקיימים את תנאי מסקנה

3.4. בפרט נובע כי יש אינסוף זוגותי $K \subset L$ השקולים על ידי קדם־קבילות, כך ש־

$$[L : \mathbb{Q}] > [K : \mathbb{Q}].$$