Dummit and Kisilevsky *Res. Number Theory*
DOI 10.1007/s40993-017-0085-7

Research in Number Theory

RESEARCH Open Access

Decomposition types in minimally tamely ramified extensions of $\mathbb{Q}$

David S. Dummit[1*] and Hershy Kisilevsky[2]

*Correspondence:
dummit@math.uvm.edu
[1]Department of Mathematics, University of Vermont, Lord House, 16 Colchester Ave., Burlington, VT 05405, USA
Full list of author information is available at the end of the article

Abstract

We examine whether it is possible to realize finite groups G as Galois groups of minimally tamely ramified extensions of $\mathbb{Q}$ and also specify both the inertia groups and the further decomposition of the ramified primes.

Keywords: Splitting, Inertia, Decomposition, Primes in tamely ramified extensions, Cyclotomic fields

Mathematics Subject Classification: Primary 12F12; Secondary 11R18, 11S15

Contents

1 Introduction

Let G be a finite group and let s, the rank of G ($=\text{rank}(G)$) denote the minimal number of elements required to *normally* generate G, i.e., s is the minimal number of elements of G which together with all their conjugates in G generate G. It is known [6] that s is the minimal number of generators of the maximal abelian quotient $G/[G, G]$ of G.

If K is a finite Galois extension of $\mathbb{Q}$, then because $\mathbb{Q}$ has no unramified extensions, $\text{Gal}(K/\mathbb{Q})$ is generated by the inertia groups for the primes p ramifying in K. If all of the ramification in K is tame then these inertia groups are cyclic, and taking a generator for one fixed representative of the (conjugate) inertia groups for each prime p gives a set of normal generators for $\text{Gal}(K/\mathbb{Q})$. It follows that if a finite group G can be realized as the

Springer Open

Galois group of a number field K over $\mathbb{Q}$ having only tame ramification, then rank(G) is the smallest possible number of primes p that are ramified in K. In [7] and [8] it is shown that all finite nilpotent semi-abelian groups can be realized by such a minimally tamely ramified extension over $\mathbb{Q}$.

In this paper we consider the finer question of whether it is possible to realize finite groups G as Galois groups of minimally tamely ramified extensions of $\mathbb{Q}$ and also specify both the cyclic subgroups of G arising as the inertia groups and the further decomposition of the ramified primes in K.

2 Minimal tame ramification and decomposition configurations

We first make precise what is meant by a specification of the inertia and decomposition groups in a realization of a finite group G as a Galois group over $\mathbb{Q}$.

Definition 2.1 A (minimal) tame ramification configuration is a pair $(G, \mathcal{T})$, where G is a finite group of rank s and $\mathcal{T}$ is a (necessarily minimal) collection $\mathcal{T} = \{T_1, \ldots, T_s\}$ of cyclic subgroups of G that normally generate G.

Definition 2.2 A tame ramification configuration is realizable over $\mathbb{Q}$ if there exists a tamely ramified Galois extension $K/\mathbb{Q}$ and an isomorphism φ: $\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow G$ such that $\varphi(T(\wp_i/(p_i))) = T_i$ for each $i = 1, \ldots s$, where $\{p_1, \ldots, p_s\}$ is the set of all finite primes of $\mathbb{Q}$ ramified in K and for each i, $\wp_i$ is a prime of K dividing (p_i) with inertia group $T(\wp_i/(p_i))$ in $\mathrm{Gal}(K/\mathbb{Q})$.

An extension $K/\mathbb{Q}$ is minimally tamely ramified if and only if it is tamely ramified and is the realization of a minimal tame ramification configuration.

With the evident minor modifications one could consider tame ramification configurations that are not minimal (where the cardinality n of $\mathcal{T}$ need not be the same as the rank of G and the T_i need not normally generate G), and realizations over number fields F other than $\mathbb{Q}$. So, for example, if $\mathcal{T} = \emptyset$, then $(G, \mathcal{T})$ would be realizable over F if and only if F has an unramified G-extension. If F has no unramified extensions, as is the case for $\mathbb{Q}$, then for a tame ramification configuration $(G, \mathcal{T})$ to be realizable, the groups T_i must normally generate G, and hence $n \geq s$. Our definitions above reflect the fact that we shall only consider minimally tamely ramified extensions over $\mathbb{Q}$ in this paper.

If $K/\mathbb{Q}$ is a Galois extension of number fields and $\wp$ is a prime of K lying above the prime (p), then the decomposition group $Z(\wp/(p))$ for $\wp$ in $\mathrm{Gal}(K/\mathbb{Q})$ contains the inertia group $T(\wp/(p))$ as a normal subgroup and the quotient is a cyclic group, which leads to the following definitions.

Definition 2.3 A (minimal) tame decomposition configuration is a triple $(G, \mathcal{T}, \mathcal{Z})$, where $(G, \mathcal{T})$ is a tame ramification configuration, and $\mathcal{Z}$ is a collection $\mathcal{Z} = \{Z_1, \ldots, Z_s\}$ of subgroups of G where T_i is a normal subgroup of Z_i and Z_i/T_i is cyclic.

Definition 2.4 A (minimal) tame decomposition configuration is realizable over $\mathbb{Q}$ if there exists a tamely ramified Galois extension $K/\mathbb{Q}$ and an isomorphism φ: $\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow G$ such that $\varphi(T(\wp_i/(p_i))) = T_i$ as in Definition 2.2 and $\varphi(Z(\wp_i/(p_i))) = Z_i$ for each $i = 1, \ldots s$, where $Z(\wp_i/(p_i))$ is the decomposition group for $\wp_i$ in $\mathrm{Gal}(K/\mathbb{Q})$.

Recall that if $K/\mathbb{Q}$ is a Galois extension and K_0 is a subfield of K Galois over $\mathbb{Q}$, then the inertia and decomposition groups in $\mathrm{Gal}(K/\mathbb{Q})$ project to the inertia and decomposition groups in $\mathrm{Gal}(K_0/\mathbb{Q})$ for the corresponding primes of K_0.

Definition 2.5 Call a tame ramification configuration $(H, \mathcal{S})$ a quotient of a tame ramification configuration $(G, \mathcal{T})$ if $\mathrm{rank}(H) = \mathrm{rank}(G)$ and there is a surjective group homomorphism $\pi: G \longrightarrow H$ such that $\pi(T_i) = S_i$ for all $T_i \in \mathcal{T}$ and all $S_i \in \mathcal{S}$. Similarly, a tame decomposition configuration $(H, \mathcal{S}, \mathcal{W})$ is a quotient of a tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$ if $(H, \mathcal{S})$ a quotient of $(G, \mathcal{T})$ and in addition $\pi(Z_i) = W_i$ for all $Z_i \in \mathcal{Z}$ and $W_i \in \mathcal{W}$.

If $K/\mathbb{Q}$ is a realization of the tame ramification configuration $(G, \mathcal{T})$ (respectively, of the tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$), then $K_0/\mathbb{Q}$ will be a realization of the tame ramification configuration $(H, \mathcal{S})$ (respectively, of the tame decomposition configuration $(H, \mathcal{S}, \mathcal{W})$), where K_0 is the subfield of K fixed by subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ corresponding (under φ) to the kernel of π, which proves the following.

Proposition 2.6 *Suppose* $(H, \mathcal{S})$ (*respectively,* $(H, \mathcal{S}, \mathcal{W})$) *is a quotient of some tame ramification configuration* $(G, \mathcal{T})$ *(respectively, tame decomposition configuration* $(G, \mathcal{T}, \mathcal{Z})$*). Then*

(a) *if* $(H, \mathcal{S})$ (*resp.,* $(H, \mathcal{S}, \mathcal{W})$) *cannot be realized over* $\mathbb{Q}$*, then neither can* $(G, \mathcal{T})$ (*resp.,* $(G, \mathcal{T}, \mathcal{Z})$)*, and*
(b) *if* $(G, \mathcal{T})$ (*resp.,* $(G, \mathcal{T}, \mathcal{Z})$) *can be realized over* $\mathbb{Q}$*, then so can* $(H, \mathcal{S})$ (*resp.,* $(H, \mathcal{S}, \mathcal{W})$).

3 Decomposition configurations in finite abelian groups

The rank s of a finite abelian group G is the number of cyclic factors in its invariant factor decomposition, and a tame ramification configuration is simply a specification of s generators, $x_1, \ldots, x_s$ of G, the minimum possible. Then a tame decomposition configuration is an additional choice of elements $z_1, \ldots, z_s \in G$.

We first use Proposition 2.6 to show that tame decomposition configurations can be realized for abelian groups if they can be realized for the particular abelian groups $(\mathbb{Z}/n\mathbb{Z})^s$.

Proposition 3.1 *Let* H *be a finite abelian group with* $\mathrm{rank}(H) = s$*, and let* $(H, \mathcal{S}, \mathcal{W})$ *be a tame decomposition configuration. Then there is a tame decomposition configuration* $(G, \mathcal{T}, \mathcal{Z})$ *with* $G = (\mathbb{Z}/n\mathbb{Z})^s$ *that has* $(H, \mathcal{S}, \mathcal{W})$ *as a quotient. In particular, if* $(H, \mathcal{S})$ *is a tame ramification configuration, then there is a tame ramification configuration* $(G, \mathcal{T})$ *with* $G = (\mathbb{Z}/n\mathbb{Z})^s$ *which has* $(H, \mathcal{S})$ *as a quotient.*

Proof For each $i = 1, \ldots, s$ let $x_i \in S_i$ be a generator of the cyclic group $S_i \in \mathcal{S}$ and suppose the decomposition group $W_i \in \mathcal{W}$ is generated by $\{x_i, z_i\}$. Let $\psi: \mathbb{Z}^s \longrightarrow H$ be the group homomorphism defined by $\psi(\epsilon_i) = x_i$, where $\epsilon_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in the ith position. For each $i = 1, \ldots, s$, choose $\eta_i \in \mathbb{Z}^s$ so that $\psi(\eta_i) = z_i$. Fix any positive integer n divisible by the exponent of H, so that $n \cdot x = 0$ for all $x \in H$, and let $f: \mathbb{Z}^s \longrightarrow G = \mathbb{Z}^s/n\mathbb{Z}^s$ be the natural projection. Then $n\mathbb{Z}^s$ is contained in the kernel of ψ, so ψ factors through f and induces a surjective homomorphism $\pi = \overline{\psi}: G \longrightarrow H$. For $i = 1, \ldots, s$, let $T_i = \langle f(\epsilon_i) \rangle$ be the subgroup of G generated by $f(\epsilon_i)$ and let $Z_i = \langle f(\epsilon_i), f(\eta_i) \rangle$ be the subgroup of G generated by $f(\epsilon_i)$ and $f(\eta_i)$. If $\mathcal{T} = \{T_1, \ldots, T_s\}$ and $\mathcal{Z} = \{Z_1, \ldots, Z_s\}$, then $(G, \mathcal{T}, \mathcal{Z})$ is

a tame decomposition configuration with rank $G = s = \text{rank}\, H$ that has $(H, \mathcal{S}, \mathcal{W})$ as a quotient. □

It follows from Propositions 2.6 and 3.1 that to construct a realization for the tame ramification configuration $(H, \mathcal{S})$ or for the tame decomposition configuration $(H, \mathcal{S}, \mathcal{W})$ for an abelian group H, it would suffice if we could construct a realization for all possible configurations for the group $G = (\mathbb{Z}/n\mathbb{Z})^s$. We shall see that this can be done for *ramification* configurations (see Theorem 3.4) but not in general for all possible *decomposition* configurations.

If $G = (\mathbb{Z}/n\mathbb{Z})^s$, each $T_i \in \mathcal{T}$ has order at most n, so the fact that rank $G = s$ and G is generated by the T_i implies that $T_i \simeq Z/n\mathbb{Z}$ for all $i = 1, \ldots, s$ and that $G = T_1 \times \cdots \times T_s$ in Proposition 3.1 (so, up to an evident equivalence, there is essentially only one tame ramification configuration for $(\mathbb{Z}/n\mathbb{Z})^s$). Then if $K/\mathbb{Q}$ is a realization of $(G, \mathcal{T})$, taking the fixed fields of the subgroups $T_1 \times \cdots \times T_{i-1} \times T_{i+1} \times \cdots T_s$ for $i = 1, \ldots s$ shows that K would be the composite of cyclic extensions of degree n, each of which is totally and tamely ramified at one odd prime and otherwise unramified at finite primes. These extensions are the cyclic subextensions of prime cyclotomic fields:

Definition 3.2 If n is a positive integer and p is a prime with $p \equiv 1 \bmod n$, let $K_n(p)$ denote the subfield of degree n contained in the cyclotomic field of pth roots of unity.

If ζ_p is any primitive pth root of unity, the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is canonically isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ under the map sending $a \in \mathbb{Z}$ to the automorphism σ_a: $\zeta_p \mapsto \zeta_p^a$. The Galois group $\text{Gal}(K_n(p)/\mathbb{Q})$ of the unique subfield of degree n in $\mathbb{Q}(\zeta_p)$ is then isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times/(\mathbb{Z}/p\mathbb{Z})^{\times n}$. This latter group is (non-canonically) isomorphic to $\mathbb{Z}/n\mathbb{Z}$, with an isomorphism obtained by choosing a generator for the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$, i.e., by choosing a primitive root g modulo p. Then

$$\text{Gal}(K_n(p)/\mathbb{Q}) = \langle \tau_g \rangle, \tag{1}$$

where τ_g is the restriction to $K_n(p)$ of the automorphism $\sigma_g \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. In particular, if l is a prime distinct from p, then since σ_l is the Frobenius automorphism for (l) in $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, whose restriction to $K_n(p)$ is the Frobenius automorphism for (l) in $\text{Gal}(K_n(p)/\mathbb{Q})$, we see that

$$\text{Fr}_{K_n(p)/\mathbb{Q}}(l) = \tau_g^b \in \text{Gal}(K_n(p)/\mathbb{Q}) \quad \text{if} \quad l \equiv g^b \mod p. \tag{2}$$

By Dirichlet's Theorem, there exist distinct primes $l_1, \ldots, l_s$ each of which is congruent to 1 mod n. By the remarks above, the composite $K = K_n(l_1) \ldots K_n(l_s)$ is then a realization over $\mathbb{Q}$ of the tame ramification configuration $(G, \mathcal{T})$ with $G = (\mathbb{Z}/n\mathbb{Z})^s$ and $T_i = \mathbb{Z}/n\mathbb{Z}$ for $i = 1, \ldots, s$. With little additional effort we can do slightly more. We first give a name to the decomposition configurations corresponding to the situation in which the ramifying primes are otherwise totally split:

Definition 3.3 A tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$ is a (minimal) tame split decomposition configuration if $T_i = Z_i$ for $1 \le i \le s$.

The field $K = K_n(l_1) \ldots K_n(l_s)$ considered above will be a realization over $\mathbb{Q}$ of the tame split decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$ where $G = (\mathbb{Z}/n\mathbb{Z})^s$ and $Z_i = T_i = \mathbb{Z}/n\mathbb{Z}$

for $i = 1, \ldots, s$ if the prime l_i is totally split in every field $K_n(l_j)$ with $i \neq j$. This can be arranged by choosing the sequence of primes $l_1, l_2, \ldots$ inductively, as follows. Begin with any prime l_1 with $l_1 \equiv 1 \mod n$. Suppose inductively for $1 \leq t < s$ that $\{l_1, l_2, \ldots, l_t\}$ are distinct primes congruent to 1 modulo n satisfying the condition that each l_i is totally split in every field $K_n(l_j)$ with $j \neq i$. It would suffice to find a prime l_{t+1} with $l_{t+1} \equiv 1 \pmod{nl_1l_2 \ldots l_t}$ (which implies both that $l_{t+1} \equiv 1 \mod n$ and that l_{t+1} splits completely in each $K_n(l_i)$ for $i \leq t$) such that also $l_1, \ldots, l_t$ each split completely in $K_n(l_{t+1})$. That is, we want $l_{t+1} \equiv 1 \pmod{nl_1l_2 \cdots l_t}$ and, by Eq. (2), for each $1 \leq i \leq t$, $l_i \equiv y_i^n \pmod{l_{t+1}}$ for some y_i. These conditions are satisfied for any prime l_{t+1} which splits completely in the field $\mathbb{Q}(\zeta_{nl_1l_2\cdots l_t}, l_1^{1/n}, l_2^{1/n}, \ldots, l_t^{1/n})$, and Chebotarev's density theorem ensures that there are infinitely many such primes.

The proof of Proposition 3.1 shows that every tame split decomposition configuration $(H, \mathcal{S}, \mathcal{W})$ is the quotient of a tame split decomposition configuration with $G = (\mathbb{Z}/n\mathbb{Z})^s$ (take $\eta_i = 0$ in the proof), which we have just seen can all be realized over $\mathbb{Q}$. By Proposition 2.6 this proves the following theorem.

Theorem 3.4 *Every tame split decomposition configuration for a finite abelian group G can be realized over $\mathbb{Q}$. In particular, every tame ramification configuration for G can be realized over $\mathbb{Q}$.*

This theorem shows that every finite abelian group arises as the Galois group of a tamely ramified extension of $\mathbb{Q}$ with a minimal set of ramifying primes (which as mentioned in Sect. 1 is already an easy special case of the results in [7] and [8]), with the added feature that the inertia groups for the ramifying primes can be taken to be any collection of cyclic subgroups that minimally generate G, and where the ramified primes are otherwise completely split in the extension.

If now $(G, \mathcal{T}, \mathcal{Z})$, with $\mathcal{T} = \{T_1, \ldots, T_s\}$ and $\mathcal{Z} = \{Z_1, \ldots, Z_s\}$ is a decomposition configuration with $G = (\mathbb{Z}/n\mathbb{Z})^s$, then as noted above we have $G = T_1 \times T_2 \times \cdots \times T_s$ where each T_i is cyclic of order n; any realization over $\mathbb{Q}$ must necessarily be the composite of fields $K_n(l_i)$ for distinct primes $l_i \equiv 1 \pmod n$, whose additional splitting information is given by the groups Z_i. If x_i is a generator for T_i for $i = 1, \ldots, s$, then this additional decomposition information is determined by choosing a Frobenius element $z_i \in Z_i$ such that $Z_i = \langle x_i, z_i \rangle$. Since $G = T_1 \times \cdots \times T_s$, we may, by adjusting z_i by a multiple of x_i if necessary, write z_i in terms of the generators x_j for $j \neq i$:

$$z_i = \prod_{j=1}^{s} x_j^{a_{ij}} \quad \text{with} \quad a_{ij} \in \mathbb{Z}/n\mathbb{Z} \quad \text{and} \quad a_{ii} = 0. \tag{3}$$

Conversely, given exponents a_{ij} with $a_{ii} = 0$, we can define z_i by Eq. (3) to give a decomposition configuration with $Z_i = \langle x_i, z_i \rangle$. The associated $s \times s$ matrix

$$M_{\mathcal{Z}} = \begin{pmatrix} 0 & a_{12} & \ldots & a_{1s} \\ a_{21} & 0 & \ldots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \ldots & 0 \end{pmatrix}, \quad a_{ij} \in \mathbb{Z}/n\mathbb{Z}, \quad a_{ii} = 0, \tag{4}$$

attached to the decomposition configuration $(G = (\mathbb{Z}/n\mathbb{Z})^s, \mathcal{T} = \{T_1, \ldots, T_s\}, \mathcal{Z} = \{Z_1, \ldots, Z_s\})$ through Eq. (3) and the choice of generators $x_1, \ldots x_s$ for the T_i therefore

carries all of the additional decomposition information for the configuration. The matrix $M_{\mathcal{Z}}$ is, of course, generally not unique—for example, we can multiply any row or column by an element in $(\mathbb{Z}/n\mathbb{Z})^*$ (corresponding to a change of generator x_i or z_i). A realization of this configuration involves finding the primes l_i whose Frobenius is given by (3) and (4).

Theorem 3.4 proves that all split decomposition configurations (whose associated matrix (4) is simply the zero matrix) can be realized over $\mathbb{Q}$. We shall see in the next subsection that, even for abelian groups, decomposition configurations that are not split may not be realizable over $\mathbb{Q}$.

3.1 Finite abelian 2-groups

In this subsection we consider tame decomposition configurations for abelian groups of 2-power order. We begin with the case $G = (\mathbb{Z}/2\mathbb{Z})^s$ of a finite elementary abelian 2-group.

Suppose $(G, \mathcal{T}, \mathcal{Z})$ is a tame decomposition configuration with $G = (\mathbb{Z}/2\mathbb{Z})^s$, $\mathcal{T} = \{T_1, \ldots, T_s\}$ and $\mathcal{Z} = \{Z_1, \ldots, Z_s\}$. In this case the generators x_i for T_i are unique, as are the elements z_i in Eq. (3), and the elements a_{ij} in the associated matrix $M_{\mathcal{Z}}$ in Eq. (4) can be taken to be in $\{0, 1\}$. We convert the nondiagonal elements of $M_{\mathcal{Z}}$ to $\{\pm 1\}$ instead of $\{0, 1\}$ by defining $S_{\mathcal{Z}} = \left(m_{ij}\right)$ to be the $s \times s$ matrix such that $m_{ii} = 0$ and $m_{ij} = (-1)^{a_{ij}}$ for $i \neq j$.

Definition 3.5 An $s \times s$ matrix M is a sign matrix if it has diagonal entries equal to 0, and off-diagonal entries equal to ± 1.

Definition 3.6 A sign matrix M is a QR (quadratic residue) matrix if $M = \left(m_{ij}\right)$ where $m_{ij} = \left(\frac{p_i}{p_j}\right)$ is given by the Legendre symbols for some set of distinct odd primes $\{p_1, \ldots, p_s\}$.

Theorem 3.7 *With notation as above, the tame decomposition configuration* $(G, \mathcal{T}, \mathcal{Z})$ *for* $G = (\mathbb{Z}/2\mathbb{Z})^s$ *is realizable over* $\mathbb{Q}$ *if and only if the corresponding sign matrix* $S_{\mathcal{Z}}$ *is a QR matrix. For* $s \leq 2$, *every tame decomposition configuration is realizable over* $\mathbb{Q}$, *but for* $s \geq 3$ *there exist tame decomposition configurations that cannot be realized over* $\mathbb{Q}$.

Proof Since $n = 2$, a realization $K/\mathbb{Q}$ of $(G, \mathcal{T}, \mathcal{Z})$ would be given by the composite field $K = K_2(l_1) \cdots K_2(l_s)$ for distinct odd primes $l_1, \ldots, l_s$. Here $K_2(l_i)$ is the quadratic subfield of the l_i^{th} roots of unity, so $K_2(l_i) = \mathbb{Q}(\sqrt{l_i^*})$ where $l_i^* = (-1)^{(l_i-1)/2} l_i$. Then for $i \neq j$, $m_{ij} = +1$ in $S_{\mathcal{Z}}$ if and only if $a_{ij} = 0$, i.e., if and only if $Z_i \subseteq \mathrm{Gal}(K/K_2(l_j)) = T_1 \times \cdots T_{j-1} \times T_{j+1} \times \cdots \times T_s$, hence if and only if l_i splits in $K_2(l_j)$. Since l_i splits in $K_2(l_j)$ if and only if $\left(\frac{l_j^*}{l_i}\right) = \left(\frac{l_i}{l_j}\right) = +1$, it follows that $m_{ij} = \left(\frac{l_i}{l_j}\right)$ so $S_{\mathcal{Z}}$ is precisely the QR matrix for the primes $\{l_1, \ldots, l_s\}$.

Conversely, suppose $S_{\mathcal{Z}}$ is a QR matrix given by the Legendre symbols for the distinct odd primes $\{l_1, \ldots, l_s\}$. Then by the equivalences in the previous paragraph, the extension $K = \mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*})$ is a realization over $\mathbb{Q}$ of $(G, \mathcal{T}, \mathcal{Z})$.

In [1] it is shown that an $s \times s$ sign matrix S is a QR matrix if and only if the diagonal entries of S^2 consist of $s - k$ occurrences of $s - 1$ and k occurrences of $s - 2k + 1$ for some integer k with $1 \leq k \leq s$. If

$$S = \begin{pmatrix} 0 & -1 & -1 \\ -1 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}$$

then S^2 has diagonal entries 0, 0 and -2 and hence is not a QR matrix. The corresponding tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$ with $G = (\mathbb{Z}/2\mathbb{Z})^3$, $T_i = \langle x_i \rangle$, $1 \leq i \leq 3$, and $Z_1 = \langle x_1, x_2x_3 \rangle$, $Z_2 = \langle x_2, x_1x_3 \rangle$ and $Z_3 = \langle x_3 \rangle$ cannot be realized over $\mathbb{Q}$. In a similar way there are, for any $s \geq 3$, tame decomposition configurations that are not realizable over $\mathbb{Q}$. For $s \leq 2$, all sign matrices are QR matrices, so all tame decomposition configurations are realizable over $\mathbb{Q}$. □

Since a tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$ is invariant under permutations of the indices $1 \leq i \leq s$, we only consider the matrices $S_{\mathcal{Z}}$ up to conjugation by $s \times s$ permutation matrices. If $S_{\mathcal{Z}}$ is a QR matrix and $K = \mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*})$ is a realization over $\mathbb{Q}$, this corresponds to a permutation of the primes l_i.

The number of such permutation classes of $s \times s$ sign matrices is at least $2^{s^2-s}/s!$ which is greater than $2^{s^2(1-\delta)}$ for any $\delta > 0$ as $s \to \infty$ by Sterling's formula. On the other hand, as in [1], every permutation class of $s \times s$ QR matrices contains a (generally non-unique) block matrix of the ("reduced") form

$$\begin{pmatrix} A & B \\ B^t & S \end{pmatrix} \tag{5}$$

where A is a $k \times k$ skew-symmetric sign matrix, S is an $(s-k) \times (s-k)$ symmetric sign matrix, B is a $k \times (s-k)$ matrix all of whose entries are ± 1 and B^t is the transpose of B. But every such matrix is determined by its entries above the diagonal and the integer k, $1 \leq k \leq s$. Therefore the number of permutation classes of $s \times s$ QR matrices is at most $s2^{(s^2-s)/2} < 2^{s^2(1+\delta)/2}$ as $s \to \infty$. Hence

$$\frac{\#\{\text{permutation classes of } s \times s \text{ QR matrices}\}}{\#\{\text{permutation classes of } s \times s \text{ sign matrices}\}} < \frac{1}{2^{s^2(1-\delta)/2}}$$

for any $\delta > 0$, as $s \to \infty$. Therefore the proportion of *realizable* tame decomposition configurations over $\mathbb{Q}$ to *all possible* tame decomposition configurations becomes vanishingly small as $s \to \infty$.

These results show that in general it is not possible in minimally tamely ramified multiquadratic extensions of $\mathbb{Q}$ to specify the further splitting of the ramified primes arbitrarily (even rapidly less possible as the number of ramifying primes increases)—this splitting data must give rise to a QR matrix. The next result shows that it *is* possible to at least specify the inertia *indices* for the ramifying primes, i.e., in the usual terminology, we may specify "$f = 1$ or 2" arbitrarily for the s tamely ramified primes:

Corollary 3.8 *For any integer r with $0 \leq r \leq s$, there is a multiquadratic extension $K/\mathbb{Q}$ of degree 2^s in which precisely s primes ramify and ramify tamely (so have ramification index $e = 2$), and precisely r of the ramified primes have inertial degree f equal to 2 and the remaining $s - r$ ramified primes are otherwise totally split in K (i.e., have $f = 1$).*

Proof As previously mentioned, it is shown in [1] that every QR-matrix is permutation equivalent to an $s \times s$ matrix of the form in Eq. (5). Let $S = (m_{ij})$ be the $s \times s$ symmetric sign matrix whose first row has r entries equal to -1, and $s - r$ entries which are $+1$ and all other entries above the diagonal are $+1$. Then S is a QR-matrix, so by Theorem 3.7 the corresponding tame decomposition configuration is realizable by a multiquadratic extension $K/\mathbb{Q}$. In this realization, the inertial degree for the ith prime, f_i, is 2 (i.e., $|Z_i/T_i| =$

2) if and only if $z_i \notin T_i$, i.e., if and only if the ith row of S contains an entry equal to -1 (by Eq. (3) since $m_{ij} = (-1)^{a_{ij}}$). It follows from the form of the matrix S that precisely r of the ramified primes have $f_i = 2$ and the remaining ramified primes have $f_i = 1$. □

Remark 3.9 This Corollary shows in particular that the question of realizing tame decomposition configurations is more precise than the simpler question of specifying the ramification index e and the inertial degree f for each of the (tamely) ramifying primes.

Theorem 3.7 shows that, for an elementary abelian 2-group of rank at least 3, not every tame decomposition configuration can be realized over $\mathbb{Q}$. It follows by Proposition 2.6 that if G is *any* finite abelian group with 2-rank at least 3 then not every tame decomposition configuration can be realized over $\mathbb{Q}$, since there are quotients of such configurations that cannot be realized.

Suppose now that $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so that $s = 2$. For a tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$, we must have (after a suitable ordering), $T_1 = \langle x_1 \rangle$ with $x_1 \in G$ of order 4, and $T_2 = \langle x_2 \rangle$ with $x_2 \notin T_1$. Suppose $K/\mathbb{Q}$ is a realization over $\mathbb{Q}$ of $(G, \mathcal{T}, \mathcal{Z})$ and let p_i be primes of $\mathbb{Z}$ whose inertia groups are the images of T_i in $\mathrm{Gal}(K/\mathbb{Q})$. Since x_1 has order 4, it follows that $p_1 \equiv 1 \pmod 4$ (the ramification is tame, so T_1 is isomorphic to a subgroup of the multiplicative group $(\mathbb{Z}/p_1\mathbb{Z})^*$ of the residue field). If F is the (unique) biquadratic subfield of K (the fixed field of x_1^2), then F is ramified only at the two primes p_1 and p_2, so $F = \mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*})$ with $p_1^* = p_1$ and $p_2^* = (-1)^{(p_2-1)/2} p_2$ as usual. But then p_1 splits in $\mathbb{Q}(\sqrt{p_2^*})$ if and only if p_2 splits in $\mathbb{Q}(\sqrt{p_1^*})$ since $\left(\frac{p_2^*}{p_1}\right) = \left(\frac{p_1}{p_2}\right) = \left(\frac{p_1^*}{p_2}\right)$, so the decomposition of p_1 and p_2 cannot be chosen independently. It follows that there exist some tame decomposition configurations $(G, \mathcal{T}, \mathcal{Z})$ for $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that are not realizable over $\mathbb{Q}$. For an explicit example, the configuration $Z_1 = T_1$ and $Z_2 = G$ is not realizable over $\mathbb{Q}$ (it requires that p_1 split in $\mathbb{Q}(\sqrt{p_2^*})$ but p_2 to be inert in $\mathbb{Q}(\sqrt{p_1^*})$). This also shows that not all ramification and inertial indices are possible—it is not possible to have $e = 4, f = 1$ (i.e., ramified of degree 4 and otherwise totally split) for one prime and $e = 2, f = 4$ (i.e., ramified of degree 2 and otherwise completely inert) for the other. It is easy to check that this reciprocity condition is the statement that $Z_1 = T_1$ if and only if $Z_2 \leq \langle T_2, x_1^2 \rangle$.

If we write $G = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \langle x_1 \rangle \times \langle y \rangle$ then up to an isomorphism of G or an interchange of $\{T_1, Z_1\}$ and $\{T_2, Z_2\}$, there are nine possible tame decomposition configurations for G. Searching explicit examples in the number field data base [3] shows that all configurations satisfying the reciprocity condition can be realized by a tame decomposition extension over $\mathbb{Q}$, so in fact this is the only obstruction to finding a realization in this case. In Table 1 we list the nine possible tame decomposition configurations $\{T_1, Z_1\}$ and $\{T_2, Z_2\}$ for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. For each realizable configuration we give a polynomial and primes p_1 and p_2 (with ramification index e and inertial degree f) realizing the configuration.

As before, since there are configurations that cannot be realized over $\mathbb{Q}$, it follows that *any* finite abelian group G whose 2-primary part has rank 2 but not exponent 2 will have tame decomposition configurations that cannot be realized over $\mathbb{Q}$, since it has quotients that cannot be realized.

Finally, if $G = \mathbb{Z}/2^n\mathbb{Z}$, then $s = 1$ and the only tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$ is $T = Z = G$ which is realizable over $\mathbb{Q}$ by the subfield $K_{2^n}(l)$ of degree 2^n of the cyclotomic field of lth roots of unity for any prime $l \equiv 1 \pmod{2^n}$.

Table 1 Decomposition configurations for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

T_1	Z_1	T_2	Z_2	p_1 (e,f)	p_2 (e,f)	Realization (when possible)
$\langle x_1 \rangle$	$\langle x_1 \rangle$	$\langle y \rangle$	$\langle y \rangle$	13 (4, 1)	3 (2, 1)	$x^8 - x^7 - x^6 - 10x^5 + 5x^4 + 14x^3 + 10x^2 + 12x + 9$
$\langle x_1 \rangle$	$\langle x_1 \rangle$	$\langle y \rangle$	$\langle y, x_1^2 \rangle$	37 (4, 1)	3 (2, 2)	$x^8 - x^7 - 4x^6 + 9x^5 - 31x^4 + 63x^3 - 196x^2 - 343x + 2401$
$\langle x_1 \rangle$	$\langle x_1 \rangle$	$\langle y \rangle$	G			Not realizable
$\langle x_1 \rangle$	G	$\langle y \rangle$	$\langle y \rangle$			Not realizable
$\langle x_1 \rangle$	G	$\langle y \rangle$	$\langle y, x_1^2 \rangle$			Not realizable
$\langle x_1 \rangle$	G	$\langle y \rangle$	G	5 (4, 2)	3 (2, 4)	$x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$
$\langle x_1 \rangle$	$\langle x_1 \rangle$	$\langle x_1 y \rangle$	$\langle x_1 y \rangle$	5 (4, 1)	29 (4, 1)	$x^8 - x^7 - 47x^6 + 40x^5 + 581x^4 - 655x^3 - 1603x^2 + 1968x + 36$
$\langle x_1 \rangle$	$\langle x_1 \rangle$	$\langle x_1 y \rangle$	G			Not realizable
$\langle x_1 \rangle$	G	$\langle x_1 y \rangle$	G	5 (4, 2)	13 (4, 2)	$x^8 - x^7 - 21x^6 + 18x^5 + 89x^4 - 19x^3 - 89x^2 - 38x - 4$

3.2 A reciprocity theorem

Before considering finite abelian groups further, we first prove a reciprocity theorem which may be of independent interest.

Fix an integer $n \geq 1$, a prime $p \equiv 1 \bmod n$, and distinct primes $l_1, \ldots, l_s$ different from p and prime to n.

Lemma 3.10 *Suppose* $\mathbf{a} = (a_1, \ldots, a_s)$ *and* $\mathbf{b} = (b_1, \ldots, b_s) \in \mathbb{Z}^s$ *have the property that for any* $(A_1, \ldots, A_s) \in \mathbb{Z}^s$,

$$(a_1, \ldots, a_s) \cdot (A_1, \ldots, A_s) \in n\mathbb{Z} \text{ if and only if } (b_1, \ldots, b_s) \cdot (A_1, \ldots, A_s) \in n\mathbb{Z}.$$

Then there is an integer u relatively prime to n so that $u(a_1, \ldots, a_s) \equiv (b_1, \ldots, b_s) \mod n$, *i.e.,* $ua_i \equiv b_i \mod n$ *for all* $i = 1, \ldots, s$.

Proof For any $\mathbf{a}$, the map $f_{\mathbf{a}} : \mathbb{Z}^s \to Z/nZ$ defined by the usual dot product mod $n, f_{\mathbf{a}}(\mathbf{z}) = \mathbf{a} \cdot \mathbf{z} \mod n$, is a homomorphism of abelian groups. The assumption of the Lemma is that $\ker f_{\mathbf{a}} = \ker f_{\mathbf{b}}$, so that $\mathbb{Z}^s / \ker f_{\mathbf{a}} = \mathbb{Z}^s / \ker f_{\mathbf{b}}$. Since $\mathbb{Z}^s / \ker f_{\mathbf{a}} \simeq d\mathbb{Z}/n\mathbb{Z}$ for some divisor d of n, also $\mathbb{Z}^s / \ker f_{\mathbf{b}} \simeq d\mathbb{Z}/n\mathbb{Z}$. Any automorphism of $d\mathbb{Z}/n\mathbb{Z}$ is given by multiplication by some element u relatively prime to n, so $uf_{\mathbf{a}}(\mathbf{z}) = f_{\mathbf{b}}(\mathbf{z})$ for all $\mathbf{z}$. Evaluating this for $\mathbf{z}$ the usual vectors $\epsilon_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ gives $u(a_1, \ldots, a_s) \equiv (b_1, \ldots, b_s) \mod n$. □

Let $K_n(p)$ be the degree n subfield of the cyclotomic field of pth roots of unity as in Definition 3.2 and the following discussion.

Let F be the cyclotomic field of nth roots of unity and let

$$L = F(l_1^{1/n}, \ldots, l_s^{1/n}).$$

The field L is Galois over $\mathbb{Q}$ with Galois group isomorphic to the semidirect product of $\mathrm{Gal}(L/F)$ by $\mathrm{Gal}(F/\mathbb{Q})$. The abelian normal subgroup $\mathrm{Gal}(L/F)$ is canonically isomorphic to μ_n^s where μ_n is the group of nth roots of unity under the map $\sigma \mapsto (\ldots, \eta_i, \ldots)$, where

$$\sigma(l_i^{1/n}) = \eta_i(l_i^{1/n}), \quad 1 \leq i \leq s.$$

Choosing a fixed primitive nth root of unity ζ_n defines a (noncanonical) isomorphism of μ_n with $\mathbb{Z}/n\mathbb{Z}$, inducing a (noncanonical) isomorphism of μ_n^s with $(\mathbb{Z}/n\mathbb{Z})^s$. The corresponding (noncanonical) isomorphism of $\mathrm{Gal}(L/F)$ with $(\mathbb{Z}/n\mathbb{Z})^s$ maps the automorphism $\lambda_1^{x_1} \ldots \lambda_s^{x_s}$ to $(x_1, \ldots, x_s)$ where for $i = 1, \ldots, s$, the automorphism $\lambda_i \in \mathrm{Gal}(L/F)$ is defined by

$$\lambda_i = \begin{cases} l_i^{1/n} \mapsto \zeta_n \, l_i^{1/n} \\ l_j^{1/n} \mapsto l_j^{1/n} \qquad \text{for } j \neq i. \end{cases} \tag{6}$$

The automorphisms $\sigma_a \in \mathrm{Gal}(F/\mathbb{Q})$ for $(a, n) = 1$ lift to elements of $\mathrm{Gal}(L/\mathbb{Q})$ by defining $\sigma_a(l_i^{1/n}) = l_i^{1/n}$ for $i = 1, \ldots, s$. Conjugation by σ_a on the abelian normal subgroup $\mathrm{Gal}(L/F)$ in the semidirect product is by raising to the ath power: $\sigma_a(\lambda_1^{x_1} \ldots \lambda_s^{x_s})\sigma_a^{-1} = \lambda_1^{ax_1} \ldots \lambda_s^{ax_s}$. In particular, every subgroup of $\mathrm{Gal}(L/F)$ is normal in $\mathrm{Gal}(L/\mathbb{Q})$.

The prime p splits completely in F since $p \equiv 1 \bmod n$, and if $\wp$ is any one of the $\varphi(n)$ distinct primes of F dividing (p) then the Frobenius automorphism $\mathrm{Fr}_{L/F}(\wp)$ in the abelian extension L/F depends only on $\wp$. If $\sigma_a(\wp)$ ($\sigma_a \in \mathrm{Gal}(F/\mathbb{Q})$) is any other prime of F lying over (p), then $\mathrm{Fr}_{L/F}(\sigma_a(\wp)) = \mathrm{Fr}_{L/F}(\wp)^a$.

Theorem 3.11 (Reciprocity Theorem) *Let* $\mathrm{Fr}_{L/F}(\wp) \in \mathrm{Gal}(L/F)$ *be the Frobenius element for any prime of* F *lying above* (p) *and suppose* $\mathrm{Fr}_{L/F}(\wp) = \lambda_1^{a_1} \ldots \lambda_s^{a_s}$ *where the* $\lambda_i \in \mathrm{Gal}(L/F)$ *are as in Eq.* (6). *Then there is a generator* τ *for* $\mathrm{Gal}(K_n(p)/\mathbb{Q})$ *with* $\mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_i) = \tau^{a_i}$ *for all* $i = 1, \ldots, s$.

Proof If $\mathrm{Fr}_{L/F}(\wp) = \lambda_1^{a_1} \ldots \lambda_s^{a_s}$, then for any $A_1, \ldots, A_s \in \mathbb{Z}$,

$$\mathrm{Fr}_{L/F}(\wp)((l_1^{1/n})^{A_1} \ldots (l_s^{1/n})^{A_s}) = \zeta_n^{a_1A_1+\cdots+a_sA_s}(l_1^{1/n})^{A_1} \ldots (l_s^{1/n})^{A_s}. \tag{7}$$

It follows that $(a_1, \ldots, a_s) \cdot (A_1, \ldots, A_s) \equiv 0 \mod n$ if and only if the decomposition field for $\wp$ in the abelian extension L/F contains the element $(l_1^{1/n})^{A_1} \ldots (l_s^{1/n})^{A_s}$.

Now, the element $(l_1^{1/n})^{A_1} \ldots (l_s^{1/n})^{A_s}$ lies in the decomposition field for $\wp$ if and only if $\wp$ splits completely in the field $F((l_1^{1/n})^{A_1} \ldots (l_s^{1/n})^{A_s})$, and since $\wp$ is a degree one prime of F, this is true if and only if the polynomial $x^n - {l_1}^{A_1} \ldots {l_s}^{A_s}$ has a root mod p, i.e., if and only if ${l_1}^{A_1} \ldots {l_s}^{A_s}$ is an nth power mod p. This is equivalent to the statement that $\sigma_{l_1}^{A_1} \ldots \sigma_{l_s}^{A_s}$ projects to the identity in $\mathrm{Gal}(K_n(p)/\mathbb{Q})$; since σ_{l_i} projects to the Frobenius automorphism $\mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_i)$ in $\mathrm{Gal}(K_n(p)/\mathbb{Q})$, this is in turn equivalent to the statement that $\mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_1)^{A_1} \ldots \mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_s)^{A_s} = 1$ in $\mathrm{Gal}(K_n(p)/\mathbb{Q})$. If $l_i = g^{b_i} \mod p$ for g a primitive root modulo p, then by Eq. (2), $\mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_i) = \tau_g^{b_i}$, so $\mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_1)^{A_1} \ldots \mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_s)^{A_s} = 1$ if and only if $\tau_g^{b_1A_1+\cdots+b_sA_s} = 1$ in $\mathrm{Gal}(K_n(p)/\mathbb{Q})$, i.e., if and only if $(b_1, \ldots, b_s) \cdot (A_1, \ldots, A_s) \in n\mathbb{Z}$.

Hence, $(a_1, \ldots, a_s) \cdot (A_1, \ldots, A_s) \in n\mathbb{Z}$ if and only if $(b_1, \ldots, b_s) \cdot (A_1, \ldots, A_s) \in n\mathbb{Z}$. By Lemma 3.10, there is an integer u relatively prime to n with $u(a_1, \ldots, a_s) \equiv (b_1, \ldots, b_s) \bmod n$. Since $\mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_i) = \tau_g^{b_i} = \tau_g^{ua_i}$, the theorem follows with $\tau = \tau_g^u$. □

Remark 3.12 There are $\varphi(n)$ distinct primes $\wp$ above (p) in F, and there are $\varphi(n)$ distinct generators for $\mathrm{Gal}(K_n(p)/\mathbb{Q})$. Distinct primes $\wp$ correspond to distinct generators τ in Theorem 3.11: if $\wp$ corresponds to τ, then $\sigma_a(\wp)$ for $\sigma_a \in \mathrm{Gal}(F/\mathbb{Q})$ corresponds to τ^a. Note in particular that the subgroup $\langle \mathrm{Fr}_{L/F}(\wp) \rangle \leq \mathrm{Gal}(L/F)$ depends only on p and not on the choice of $\wp$ dividing (p) in F.

Remark 3.13 When $n = 2$, Theorem 3.11 is just quadratic reciprocity for p and the primes l_i, $i = 1, \ldots, s$. For larger values of n, the theorem carries more information than simply the appropriate nth power reciprocity for the individual primes. For example, if $n = 3$ and $s = 2$ the theorem not only considers whether l_1 and l_2 are cubes modulo p, but also when they are not cubes whether they lie in the *same* (or the *inverse*) cubic residue class modulo p.

3.3 Finite abelian groups of odd order

In this subsection we show that, unlike the case of abelian 2-groups where quadratic reciprocity intervened, for finite abelian groups of odd order there are no constraints to realizing tame decomposition configurations over $\mathbb{Q}$:

Theorem 3.14 *Every tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$ with G an abelian group of odd order is realizable over $\mathbb{Q}$.*

The method of proof will be similar to the proof of Theorem 3.4: by Propositions 2.6 and 3.1 (noting in the proof of the latter than n can be taken odd if H has odd exponent) it suffices to prove that all tame decomposition configurations are realizable over $\mathbb{Q}$ for the group $G = (\mathbb{Z}/n\mathbb{Z})^s$ when n is odd, which we do using subfields of appropriate cyclotomic fields, whose existence will be proved using the Reciprocity Theorem of the previous subsection.

For the remainder of this subsection let n be an odd positive integer.

A tame decomposition configuration for $G = (\mathbb{Z}/n\mathbb{Z})^s$ is encoded in a matrix $M_{\mathcal{Z}}$ as in Eq. (4). To prove Theorem 3.14 we must show that any such matrix containing arbitrary elements of $\mathbb{Z}/n\mathbb{Z}$ in the off-diagonal positions arises from the decomposition information for the distinct primes $l_1, \ldots, l_s$ in the composite extension $K = K_n(l_1) \cdots K_n(l_s)$ (where $K_n(l_i)$ is the field in Definition 3.2), which we now make explicit.

As in Eq. (1), let g_i be a primitive root modulo l_i and let τ_{g_i} be the corresponding generator for $\mathrm{Gal}(K_n(l_i)/\mathbb{Q})$, viewed as an element in $\mathrm{Gal}(K/\mathbb{Q})$ with τ_{g_i} acting trivially on each $K_n(l_j)$ with $j \neq i$ (which amounts to choosing $g_i \equiv 1 \pmod{l_j}$ for $j \neq i$), so that $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau_{g_1} \rangle \times \cdots \times \langle \tau_{g_s} \rangle$. The decomposition group for the prime l_i in $\mathrm{Gal}(K/\mathbb{Q})$ is generated by τ_{g_i} and the Frobenius automorphism for l_i in $\mathrm{Gal}(K/K_n(l_i)) = \langle \tau_{g_1} \rangle \times \cdots \langle \tau_{g_{i-1}} \rangle \times \langle \tau_{g_{i+1}} \rangle \cdots \times \langle \tau_{g_s} \rangle$. This Frobenius automorphism is $\tau_{g_1}^{a_{i1}} \ldots \tau_{g_s}^{a_{is}}$ where $\tau_{g_j}^{a_{ij}}$ is the restriction to $K_n(l_j)$ of the automorphism $\sigma_{l_i} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{l_j})/\mathbb{Q})$ for $j \neq i$ and $a_{ii} = 0$. By Eq. (2) the a_{ij} are given by $l_i \equiv g_j^{a_{ij}} \pmod{l_j}$.

It follows that the matrix encoding the decomposition information for $K/\mathbb{Q}$ is the matrix (a_{ij}) whose diagonal entries a_{ii} are zero and whose off-diagonal entries a_{ij} for $i \neq j$ are determined by $l_i \equiv g_j^{a_{ij}} \pmod{l_j}$. To prove Theorem 3.14 we must show that we may arrange for arbitrary elements of $\mathbb{Z}/n\mathbb{Z}$ in the off-diagonal positions by choosing the primes $l_1, \ldots, l_s$ appropriately.

We proceed by induction on s, the case $s = 1$ being trivial. Suppose the result is true for s and let S be an $(s+1) \times (s+1)$ matrix which we write as

$$S = \begin{pmatrix} 0 & b_1 & b_2 & \cdots & b_s \\ a_1 & 0 & a_{12} & \cdots & a_{1s} \\ a_2 & a_{21} & 0 & \cdots & a_{2s} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_s & a_{s1} & a_{s2} & \cdots & 0 \end{pmatrix} \tag{8}$$

and let S' be the $s \times s$ minor given by

$$S' = \begin{pmatrix} 0 & a_{12} & \ldots & a_{1s} \\ a_{21} & 0 & \ldots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \ldots & 0 \end{pmatrix}. \tag{9}$$

By induction, there are distinct primes $l_i \equiv 1 \pmod{n}$ and primitive roots $g_i \bmod l_i$ for $i = 1, \ldots, s$ so that the decomposition configuration for the composite field $K = K_n(l_1) \ldots K_n(l_s)$ gives the matrix S', and we must find a prime $p \equiv 1 \pmod{n}$ distinct from $l_1, \ldots, l_s$ so that the decomposition configuration for the composite extension $K_n(p)K$ is the matrix S. The conditions on $p \equiv 1 \pmod{n}$ in order that $\{p, l_1, \ldots, l_s\}$ produces the matrix S are then

$$1.\ \mathrm{Fr}_{K_n(l_i)/\mathbb{Q}}(p) = \tau_{g_i}^{b_i} \quad \text{for } i = 1, \ldots, s, \quad \text{and} \tag{10}$$

$$2.\ \mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_i) = \tau_g^{a_i} \quad \text{for } i = 1, \ldots, s \text{ for some primitive root } g \bmod p. \tag{11}$$

As in Sect. 3.2, let $F = \mathbb{Q}(\zeta_n)$ and $L = F(l_1^{1/n}, \ldots, l_s^{1/n})$. Since n is odd, the Galois extensions L and K are linearly disjoint with Galois composite LK. Extending the elements in $\mathrm{Gal}(L/\mathbb{Q})$ to $\mathrm{Gal}(LK/\mathbb{Q})$ by having them act trivially on K, and similarly for $\mathrm{Gal}(K/\mathbb{Q})$, we can identify $\mathrm{Gal}(LK/\mathbb{Q})$ with $\mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$.

By the remarks following Eq. (6), the conjugacy class in $\mathrm{Gal}(LK/\mathbb{Q})$ of the element $(\lambda_1^{a_1} \ldots \lambda_s^{a_s}, \tau_{g_1}^{b_1} \ldots \tau_{g_s}^{b_s})$ consists of the elements $(\lambda_1^{aa_1} \ldots \lambda_s^{aa_s}, \tau_{g_1}^{b_1} \ldots \tau_{g_s}^{b_s})$ where the $\lambda_1^{aa_1} \ldots \lambda_s^{aa_s}$ are the generators for the subgroup $\langle \lambda_1^{a_1} \ldots \lambda_s^{a_s} \rangle$ in $\mathrm{Gal}(L/\mathbb{Q})$.

By Chebotarev's density theorem, there exists a prime p whose Frobenius automorphisms in $\mathrm{Gal}(LK/\mathbb{Q})$ give the conjugacy class of $(\lambda_1^{a_1} \ldots \lambda_s^{a_s}, \tau_{g_1}^{b_1} \ldots \tau_{g_s}^{b_s})$. Then $\mathrm{Fr}_{K_n(l_i)/\mathbb{Q}}(p) = \tau_{g_i}^{b_i}$ for $i = 1, \ldots, s$, so the conditions in (10) are satisfied for p. Also, there is a prime $\mathfrak{p}$ lying over p in L with $\mathrm{Fr}_{L/\mathbb{Q}}(\mathfrak{p}) = \lambda_1^{a_1} \ldots \lambda_s^{a_s}$. Since $\lambda_1^{a_1} \ldots \lambda_s^{a_s}$ is trivial on the subfield $\mathbb{Q}(\zeta_n)$, p splits completely in $\mathbb{Q}(\zeta_n)$, i.e., $p \equiv 1 \pmod{n}$, and if $\wp = \mathfrak{p} \cap \mathbb{Q}(\zeta_n)$ then $\mathrm{Fr}_{L/F}(\wp) = \lambda_1^{a_1} \ldots \lambda_s^{a_s}$ in the abelian extension L/F.

By the Reciprocity Theorem 3.11, $\mathrm{Fr}_{L/F}(\wp) = \lambda_1^{a_1} \ldots \lambda_s^{a_s}$ implies $\mathrm{Fr}_{K_n(p)/\mathbb{Q}}(l_i) = \tau^{a_i}$, $1 \le i \le s$, for some generator τ of $\mathrm{Gal}(K_n(p)/\mathbb{Q})$. If g is a primitive root mod p so that $\tau = \tau_g$ as in (1), this shows the conditions in (11) are also satisfied for p, completing the proof of Theorem 3.14 by induction. □

Remark 3.15 We note that n odd was needed to ensure $L = \mathbb{Q}(\zeta_n, l_1^{1/n}, \ldots, l_s^{1/n})$ and $K = K_n(l_1) \ldots K_n(l_s)$ are linearly disjoint, which allowed us to find a prime p that satisfied both (10) and (11) simultaneously. Since the fields $\mathbb{Q}(\sqrt{l_1}, \sqrt{l_2})$ and $\mathbb{Q}(\sqrt{l_1^*}, \sqrt{l_2^*})$ always have a nontrivial intersection, the fields L and K are never linearly disjoint when n is even. This reflects the intervention of quadratic reciprocity constraints preventing some decomposition configurations from being realizable over $\mathbb{Q}$ for abelian groups of even order as in the previous subsection.

3.4 Finite abelian groups with cyclic or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ Sylow-2 subgroup

We have seen that if the abelian group G has trivial Sylow-2 subgroup then all tame decomposition configurations can be realized over $\mathbb{Q}$, and that if the Sylow-2 subgroup has rank at least 3 or has rank 2 but not exponent 2 then there are configurations that cannot be realized. In this subsection we complete the analysis for finite abelian groups by showing that in the two remaining cases, namely where the Sylow-2 subgroup of the abelian group is either cyclic or isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then again all tame decomposition configurations can be realized over $\mathbb{Q}$:

Theorem 3.16 *Every tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$ with G an abelian group with cyclic or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ Sylow-2 subgroup is realizable over $\mathbb{Q}$.*

In both cases the argument will be by induction on the number of generators of G, with the inductive hypothesis used to provide an 'initial realization' for a tame decomposition configuration related to the desired configuration. A Chebotarev density theorem argument will show the existence of an additional prime and corresponding abelian extensions which, when taken together with the initial realization, can be used to construct a realization of the desired decomposition configuration. While somewhat more technically detailed, the arguments are fundamentally similiar to those in the previous subsection, so we indicate the proofs more briefly.

We first note a variant of Proposition 3.1. Suppose $(H, \mathcal{S}, \mathcal{W})$ and $(G, \mathcal{T}, \mathcal{Z})$ are as in Proposition 3.1. Write $H = H_2 \times H_{\text{odd}}$ where H_2 is the Sylow-2 subgroup of H and H_{odd} has odd order and write $G = G_2 \times G_{\text{odd}}$ similarly. The surjection π in the proof of Proposition 3.1 restricted to G_2 gives a surjection to H_2, and if J_2 denotes the kernel of this latter map, then π induces a surjective homomorphism $G/J_2 \to H$, and the induced minimal tame decomposition configuration on G/J_2 has the minimal tame decomposition configuration $(H, \mathcal{S}, \mathcal{W})$ on H as quotient.

It follows that to show all tame decomposition configurations can be realized over $\mathbb{Q}$ for finite abelian groups G whose Sylow-2 subgroup is cyclic or isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, it suffices to prove all configurations can be realized in the following two cases:

1. $G \simeq \mathbb{Z}/2^A\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^s$, where $A \geq 1$, $s \geq 0$, and $n \geq 1$ is odd, and
2. $G \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})^s$, where $s \geq 0$ and $n \geq 1$ is odd.

By previous results, we may assume $s \geq 1$. We handle each case in turn.

3.4.1 Finite abelian groups with cyclic Sylow-2 subgroup

Suppose

$$G = \langle \sigma \rangle \times \langle x_1 \rangle \times \cdots \times \langle x_s \rangle \simeq \mathbb{Z}/2^A\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^s \tag{12}$$

with $A \geq 1$, $s \geq 1$ and $n \geq 1$ is odd. Then a tame decomposition configuration is given by a choice, for $i = 1, 2, \ldots, s$, of inertia groups

$$T_i = \langle \sigma^{2^{a_i}} \rangle \times \langle x_i \rangle, \quad \text{where} \quad a_1 = 0, \tag{13}$$

that generate G, and a choice

$$Z_i = \langle \sigma^{2^{b_i}} \rangle \times \langle x_i, z_i \rangle \quad \text{with} \quad b_i \leq a_i \quad \text{and} \quad z_i = \prod_{j=1}^{s} x_j^{a_{ij}} \quad (a_{ii} = 0), \tag{14}$$

for the decomposition groups.

If $s = 1$ then G is cyclic, a case already considered. Assume $s \geq 2$ and by induction that all tame decomposition configurations can be realized for groups as in (12) of rank $s - 1$. Let $a = \min(a_2, a_3, \ldots, a_s)$ and consider the group of rank $s - 1$ defined by

$$\langle T_2, T_3, \ldots, T_s \rangle = \langle \sigma^{2^a}, x_2, x_3, \ldots, x_s \rangle \simeq \mathbb{Z}/2^{A-a}\mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})^{s-1}.$$

For $i = 2, 3, \ldots, s$ set $\tilde{z}_i = z_i / x_1^{a_{i1}}$ and consider the configuration defined by

$$\widetilde{T}_i = T_i = \langle \sigma^{2^{a_i}}, x_i \rangle \simeq \mathbb{Z}/2^{A-a_i}\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}. \quad i = 2, 3, \ldots, s$$
$$\widetilde{Z}_i = \langle \sigma^{2^{a_i}}, x_i, \tilde{z}_i \rangle.$$

By induction, this configuration has a realization over $\mathbb{Q}$ which is the composite of the extension $K_n(l_2)\cdots K_n(l_s)$ for primes $l_2,\ldots,l_s$ and a cyclic extension K_0 of degree 2^{A-a}. For each $i=2,3,\ldots,s$, the prime l_i is ramified of degree 2^{A-a_i} in K_0 and since this is the precise power of 2 in $|\widetilde{Z}_i|$, the prime l_i is otherwise totally split in K_0.

We now find another prime p to adjust this 'initial configuration' to realize the decomposition (13) and (14).

Choose the prime p distinct from $l_2,\ldots,l_s$ so that $p\equiv 1$ modulo 2^A and so that for $i=2,3,\ldots,s$ the residue degree of l_i in $K_{2^A}(p)$ is 2^{A-b_i} and l_i is otherwise split, i.e., so that $Z_{K_{2^A}(p)/\mathbb{Q}}(l_i)=\langle {g_1}^{2^{b_i}}\rangle$ if $\mathrm{Gal}(K_{2^A}(p)/\mathbb{Q})=\langle g_1\rangle$. By the Reciprocity Theorem 3.11, this is a choice of Frobenius for p in the extension $\mathbb{Q}(\zeta_{2^A})(l_2^{1/2^A},\ldots,l_s^{1/2^A})$.

Write $\mathrm{Gal}(K_0/\mathbb{Q})=\langle g_2\rangle$, so the composite of K_0 and $K_{2^A}(p)$ has Galois group $\mathrm{Gal}(K_0K_{2^A}(p)/\mathbb{Q})=\mathrm{Gal}(K_{2^A}(p)/\mathbb{Q})\times\mathrm{Gal}(K_0/\mathbb{Q})=\langle g_1\rangle\times\langle g_2\rangle$ where we lift g_1 by having it act trivially on K_0 and we lift g_2 similarly. Define the field F to be the subfield of $K_0K_{2^A}(p)$ fixed by the subgroup generated by ${g_1}^{2^a}g_2$.

The field F is a cyclic extension of $\mathbb{Q}$ of degree 2^A. If we let $\mathrm{Gal}(F/\mathbb{Q})=\langle\sigma\rangle$, a straightforward computation of the images in $\mathrm{Gal}(F/\mathbb{Q})$ of the inertia and decomposition groups for $p,l_2,\ldots,l_s$ in $K_0K_{2^A}(p)$ shows that

$$T_{F/\mathbb{Q}}(p)=\langle\sigma\rangle,\quad Z_{F/\mathbb{Q}}(p)=\langle\sigma\rangle,\quad T_{F/\mathbb{Q}}(l_i)=\langle\sigma^{2^{a_i}}\rangle,\quad Z_{F/\mathbb{Q}}(l_i)=\langle\sigma^{2^{b_i}}\rangle,$$

i.e., F realizes the even part of the tame decomposition configuration (13) and (14). We may impose additional conditions on p as in the previous subsection so that the field $K_n(p)K_n(l_2)\ldots K_n(l_s)$ realizes the odd part of the configuration.

In summary, the conditions required on the prime p are the following:

(1) p is distinct from $l_2,\ldots,l_s$,
(2) a choice of Frobenius for p in the extension $\mathbb{Q}(\zeta_{2^A})(l_2^{1/2^A},\ldots,l_s^{1/2^A})$,
(3) a choice of Frobenius for p in the extension $K_n(l_2)\ldots K_n(l_s)$, and
(4) a choice of Frobenius for p in the extension $\mathbb{Q}(\zeta_n)(l_2^{1/n},\ldots,l_s^{1/n})$ (which includes the condition $p\equiv 1$ modulo n).

Since the fields involved are linearly disjoint, Chebotarev's density theorem ensures the existence of a prime p satisfying all of the necessary conditions simultaneously, and for this prime, the composite field $FK_n(p)K_n(l_2)\ldots K_n(l_s)$ gives a realization of the tame decomposition configuration (13) and (14).

3.4.2 Finite abelian groups with Sylow-2 subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$

Suppose that $G\simeq(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})^s$, where $s\geq 0$ and $n\geq 1$ is odd. The cases $s=0$ (which has already been considered in Sect. 3.1 in any case) and $s=1$ are quotients of the case $s=2$ in the sense of Definition 2.5, so it suffices to prove Theorem 3.16 when $s\geq 2$. We proceed by induction on s.

If $s=2$, $G=T_1\times T_2\simeq\mathbb{Z}/(2n)\mathbb{Z}\times\mathbb{Z}/(2n)\mathbb{Z}$, so a realization would be the composite $K_{2n}(p)K_{2n}(q)$ for some primes p and q both congruent to 1 modulo $2n$. To prove the existence of appropriate primes p and q we can proceed as we did for abelian groups of odd order, as follows. First let q be any prime congruent to 3 modulo 4 and also congruent to 1 modulo $2n$. A tame decomposition configuration specifies the further splitting of the prime q in $K_{2n}(p)$ for a prime $p\equiv 1$ modulo n and the further splitting of p in $K_{2n}(q)$. The

splitting for p is the choice of a Frobenius element for p in $K_{2n}(q)$, and by the Reciprocity Theorem 3.11, the splitting for q (a choice of Frobenius element for q in $K_{2n}(p)$) is a choice of a Frobenius element for p in the extension $\mathbb{Q}(\zeta_{2n}, q^{1/2n})$. Since q was chosen congruent to 3 modulo 4, the quadratic subfield of $K_{2n}(q)$ is $\mathbb{Q}(\sqrt{-q})$ and it follows that $K_{2n}(q)$ and $\mathbb{Q}(\zeta_{2n}, q^{1/2n})$ are linearly disjoint. By Chebotarev's density theorem, there exists a prime p satisfying all the required constraints simultaneously, completing the proof when $s = 2$.

Suppose now that $s \geq 3$.

The groups $T_1, \ldots, T_s$ in a tame decomposition configuration generate G, so a realization over $\mathbb{Q}$ would be a composite of a biquadratic extension K with Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle$ and fields $K_n(p), K_n(q), K_n(l_3) \ldots K_n(l_s)$ for some primes $p, q, l_3, \ldots, l_s$, each of which is congruent to 1 modulo n, whose ramification information would be given by

$$G = \langle \sigma, \tau \rangle \times \langle x_1 \rangle \times \cdots \times \langle x_s \rangle \simeq (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})^s \tag{15}$$

$$T(p) = \langle \sigma \rangle \times \langle x_1 \rangle \simeq \mathbb{Z}/(2n)\mathbb{Z}, \qquad T(q) = \langle \tau \rangle \times \langle x_2 \rangle \simeq \mathbb{Z}/(2n)\mathbb{Z}, \tag{16}$$

$$T(l_i) = \langle y_i \rangle \times \langle x_i \rangle, \qquad i = 3, 4, \ldots, s, \tag{17}$$

where for $i = 3, 4, \ldots, s$, the element y_i is one of $1, \sigma, \tau$, or $\sigma\tau$. The biquadratic field K would be uniquely determined by this ramification information: if

$$N_\sigma = \prod_{y_i \in \{\tau, \sigma\tau\}} l_i^*, \qquad N_\tau = \prod_{y_i \in \{\sigma, \sigma\tau\}} l_i^*, \qquad N_{\sigma\tau} = \prod_{y_i \in \{\sigma, \tau\}} l_i^*, \tag{18}$$

then $K = \mathbb{Q}(\sqrt{N_\sigma}, \sqrt{N_\tau})$, with quadratic subfields $K_\sigma = \mathbb{Q}(\sqrt{N_\sigma})$, $K_\tau = \mathbb{Q}(\sqrt{N_\tau})$, $K_{\sigma\tau} = \mathbb{Q}(\sqrt{N_{\sigma\tau}})$, fixed by σ, τ and $\sigma\tau$, respectively. We have $p \mid N_\tau, N_{\sigma\tau}$, and $q \mid N_\sigma, N_{\sigma\tau}$. The primes ramifying in K_σ are the primes whose nontrivial inertia group is distinct from $\langle \sigma \rangle$, and similarly for the other two quadratic subfields of K.

The remaining configuration information is given by a choice of decomposition groups:

$$\begin{aligned} &Z(p) = Z_1 = \langle \sigma, w_p \rangle \times \langle x_1, z_1 \rangle, \qquad Z(q) = Z_2 = \langle \tau, w_q \rangle \times \langle x_2, z_2 \rangle, \\ &\quad \text{and} \quad Z(l_i) = Z_i = \langle y_i, w_i \rangle \times \langle x_i, z_i \rangle, \ \ i = 3, 4, \ldots, s, \end{aligned} \tag{19}$$

where $z_i = \prod_{j=1}^{s} x_j^{a_{ij}}$ (and $a_{ii} = 0$) for $i = 1, 2, \ldots, s$, and where w_p, w_q and w_i for $i = 3, 4, \ldots, s$ are in $\langle \sigma, \tau \rangle$.

To prove the existence of suitable primes $p, q, l_3, \ldots, l_s$, we first apply the inductive hypothesis to a decomposition configuration (that will depend on T_s and Z_s) for a group of rank $s - 1$ to obtain the primes $p, q, l_3, \ldots, l_{s-1}$ and then show the existence of a prime l_s and a modification of this initial configuration that realizes the rank s configuration.

Suppose first that $T_s = \langle \sigma \rangle$. If $T_s = Z_s$, define $\epsilon = 1$ and if $T_s \neq Z_s$, define $\epsilon = \sigma$. By induction applied to the group $\langle \sigma, \tau \rangle \times \langle x_1 \rangle \times \cdots \times \langle x_{s-1} \rangle$ of rank $s - 1$, there are primes $p, q, l_3, \ldots, l_{s-1}$ and a realization $K_0 K_n(p) K_n(q) K_n(l_3) \ldots K_n(l_s)$ over $\mathbb{Q}$ with the tame decomposition configuration

$$T(p) = \langle \sigma \rangle \times \langle x_1 \rangle \qquad Z(p) = \langle \sigma, w_p \rangle \times \langle x_1, z_1 / x_s^{a_{1,s}} \rangle \tag{20}$$

$$T(q) = \langle \tau \rangle \times \langle x_2 \rangle \qquad Z(q) = \langle \tau, \epsilon w_q \rangle \times \langle x_2, z_2 / x_s^{a_{2,s}} \rangle \tag{21}$$

$$T(l_i) = \langle y_i \rangle \times \langle x_i \rangle \qquad Z(l_i) = \langle y_i, w_i \rangle \times \langle x_i, z_i / x_s^{a_{i,s}} \rangle, \ i = 3, 4, \ldots, s-1 \tag{22}$$

obtained from the first $s-1$ conditions in (19) by modifying w_q in $Z(q)$ by the ϵ defined above, and, as in the previous subsection, modifying the elements z_i for $1 \le i \le s-1$. Let N'_σ, N'_τ and $N'_{\sigma\tau}$ be the integers in (18) for the biquadratic field K_0 for this rank $s-1$ realization.

Choose a prime $l_s \equiv 1$ modulo $4n$ such that

(1) $\left(\frac{l_s}{q}\right) = \begin{cases} +1 & \text{if } w_s \in \langle\sigma\rangle \\ -1 & \text{if } w_s \notin \langle\sigma\rangle, \end{cases}$

(2) $\left(\frac{l_s}{l}\right) = +1$, for $l \in \{p, l_3, \ldots, l_{s-1}\}$,

(3) The Frobenius for l_s in $K_n(p)K_n(q)K_n(l_3)\ldots K_n(l_{s-1})$ ensures the odd part of the decomposition of l_s in $K_n(p)K_n(q)K_n(l_3)\ldots K_n(l_{s-1})$ is as needed, and

(4) The Frobenius for l_s in $\mathbb{Q}(\zeta_n)(p^{1/n}, q^{1/n}, l_3^{1/n}, \ldots, l_{s-1}^{1/n})$ ensures (by the Reciprocity Theorem (3.11)) the odd part of the decomposition of $p, q, l_3, \ldots, l_{s-1}$ in $K_n(l_s)$ is as needed.

Again, since the fields involved are linearly disjoint, such a prime l_s exists by Chebotarev's density theorem.

Remark 3.17 The condition in (2) can be relaxed to include only p and those primes l_i whose associated y_i in (22) is not trivial.

Let $N_\sigma = N'_\sigma$, $N_\tau = l_s^* N'_\tau = l_s N'_\tau$ and $N_{\sigma\tau} = l_s^* N'_{\sigma\tau} = l_s N'_{\sigma\tau}$, and define $K = \mathbb{Q}(\sqrt{N_\sigma}, \sqrt{N_\tau})$. Then K is a biquadratic extension of $\mathbb{Q}$ with quadratic subfields $K_\sigma = \mathbb{Q}(\sqrt{N_\sigma})$, $K_\tau = \mathbb{Q}(\sqrt{N_\tau})$, and $K_{\sigma\tau} = \mathbb{Q}(\sqrt{N_{\sigma\tau}})$. It is then straightforward to check that the composite field $KK_n(p)K_n(q)K_n(l_3)\ldots K_n(l_s)$ is a realization of the decomposition configuration (16), (17) and (19). For example, the even part of the decomposition behavior (i.e., the 2-primary parts of the ramification and decomposition groups) is realized in the biquadratic field K, as follows. The field K_σ is the same for K_0 and K, and the fact that $l_s = l_s^*$ is a square modulo $p, l_3, \ldots, l_{s-1}$ by condition (2) shows the decomposition behavior for these primes in K is as desired.

The decomposition of l_s in K is the question of whether l_s is split or inert in K_σ (it is ramified in the other two quadratic subfields), i.e., by the Legendre symbol $\left(\frac{N_\sigma}{l_s}\right)$, which equals $\left(\frac{l_s}{q}\right)$ by condition (2) and the fact that $l_s \equiv 1$ modulo 4. By condition (1), this is precisely the desired decomposition for l_s in (17), as desired.

The decomposition of q in K is determined by the splitting of q in K_τ, so by the Legendre symbol $\left(\frac{N_\tau l_s}{q}\right) = \left(\frac{N_\tau}{q}\right)\left(\frac{l_s}{q}\right)$. By the choice of the inductive configuration, $\left(\frac{N_\tau}{q}\right) = +1$ if and only if $\epsilon w_q \in \langle\tau\rangle$ and by condition (2), $\left(\frac{l_s}{q}\right) = +1$ if and only if $w_s \in \langle\sigma\rangle$, i.e., if and only if $T_s = Z_s$. By the definition of ϵ, a quick check shows $\left(\frac{N_\tau l_s}{q}\right) = +1$ if and only if $w_q \in \langle\tau\rangle$, so q decomposes as desired in K.

The cases $T_s = \langle\tau\rangle$ and $T_s = \langle\sigma\tau\rangle$ are handled similarly, as follows. In both cases, let $\epsilon = 1$ if $Z_s = T_s$, let ϵ be the generator of T_s if $Z_s \ne T_s$, and for the inductive rank $s-1$ decomposition configuration replace (20) and (21) with

$$T(p) = \langle\sigma\rangle \times \langle x_1\rangle \qquad Z(p) = \langle\sigma, \epsilon w_p\rangle \times \langle x_1, z_1/x_s^{a_{1,s}}\rangle \tag{20'}$$

$$T(q) = \langle\tau\rangle \times \langle x_2\rangle \qquad Z(q) = \langle\tau, w_q\rangle \times \langle x_2, z_2/x_s^{a_{2,s}}\rangle. \tag{21'}$$

Let N'_σ, N'_τ and $N'_{\sigma\tau}$ be the integers in (18) for the biquadratic field K_0 for this rank $s-1$ realization and if $T_s = \langle\tau\rangle$ (resp., $T_s = \langle\sigma\tau\rangle$), let $N_\sigma = l_s N'_\sigma$, $N_\tau = N'_\tau$ and $N_{\sigma\tau} = l_s N'_{\sigma\tau}$ (resp., $N_\sigma = l_s N'_\sigma$, $N_\tau = l_s N'_\tau$ and $N_{\sigma\tau} = N'_{\sigma\tau}$). Set $K = \mathbb{Q}(\sqrt{N_\sigma}, \sqrt{N_\tau})$. Choose (by Chebotarev's density theorem) a prime $l_s \equiv 1$ modulo $4n$ so that (1) $\left(\frac{l_s}{p}\right) = +1$ if $T_s = Z_s$ and $\left(\frac{l_s}{p}\right) = -1$ if $T_s \neq Z_s$, (2) $\left(\frac{l_s}{l}\right) = +1$ for $l \in \{q, l_3, \ldots, l_{s-1}\}$, and so that the earlier conditions (3) and (4) are all satisfied.

Finally, if $T_s = 1$, set $\epsilon = 1$, take (20)–(22) for the inductive configuration, take $K = K_0$, and replace conditions (1) and (2) for the prime $l_s \equiv 1$ modulo $4n$ by the condition that its Frobenius in K gives the correct decomposition group Z_s.

In all cases, it is easy to check as before that $KK_n(p)K_n(q)K_n(l_3)\ldots K_n(l_s)$ is a realization of the decomposition configuration, completing the proof of Theorem (3.16).

4 Groups of small order

In this section we consider the realizations of (minimal) tame decomposition configurations of some nonabelian groups. In many cases there are restrictions on the configurations that can be realized (for example, every minimally ramified tame Q_8 extension is necessarily a split tame decomposition configuration), and, for those that can be realized, we give explicit realizations. We also observe that it is a difficult (open) question to determine if a given tame decomposition configuration that can be realized over $\mathbb{Q}$ in fact has infinitely many different realizations; this is already an interesting problem for the groups considered here.

4.1 Nonabelian groups of order 8

Consider first $G = Q_8$, the quaternion group of order 8. Then $s = 2$ and a tame decomposition configuration $(G, \mathcal{T}, \mathcal{Z})$ must have T_1 and T_2 cyclic groups of order 4; up to evident equivalence, there are three possible configurations, depending on whether $T_i = Z_i$ or not. If $K/\mathbb{Q}$ is a realization then the unique biquadratic subfield F of K, $F = \mathbb{Q}(\sqrt{p_1^*}, \sqrt{p_2^*})$, must be totally real, hence $p_1 \equiv p_2 \equiv 1 \pmod 4$. As before, this imposes a quadratic reciprocity constraint that implies $Z_1 = T_1$ if and only if $Z_2 = T_2$. But $T_1 \subsetneq Z_1$ means that $Z_1 = Q_8$, and since only $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ occur as Galois groups of order 8 over $\mathbb{Q}_p$ if $p \equiv 1 \pmod 4$ this cannot occur. Alternatively, a theorem of Witt [11] states that $\mathbb{Q}(\sqrt{a}, \sqrt{b})$ can be embedded in a Q_8 extension if and only if $(-a, -b) = (-1, -1)$ (Hilbert symbols), which for $a = p_1^*$, $b = p_2^*$ is equivalent to $p_1 \equiv p_2 \equiv 1 \pmod 4$ and $\left(\frac{p_1}{p_2}\right) = \left(\frac{p_2}{p_1}\right) = +1$. Therefore only the configuration with $Z_1 = T_1$ and $Z_2 = T_2$ could be realizable. In [2], Fröhlich shows this Witt condition is both necessary and sufficient for the existence of a (unique) Q_8 extension of $\mathbb{Q}$ ramified only at the primes p_1 and p_2, and Schmid in [10] identifies it explicitly.

Next consider $G = D_8 = \langle r, s \mid r^4 = s^2 = 1, sr = r^{-1}s\rangle$, the dihedral group of order 8. Again the rank is 2, and up to an isomorphism of G or an interchange of $\{T_1, Z_1\}$ and $\{T_2, Z_2\}$, there are seven possible tame decomposition configurations for G. Searching the number field data base [3] we find that all seven configurations for D_8 can be realized over $\mathbb{Q}$; Table 2 gives the possible tame configurations $\{T_1, Z_1\}$ and $\{T_2, Z_2\}$ for D_8, and for each a polynomial and primes p_1 and p_2 (with ramification index e and inertial degree f) realizing the configuration.

Table 2 Decomposition configurations for D_8

T_1	Z_1	T_2	Z_2	p_1 (e,f)	p_2 (e,f)	Realization
$\langle r\rangle$	$\langle r\rangle$	$\langle s\rangle$	$\langle s\rangle$	5 (4, 1)	29 (2, 1)	$x^8 - x^6 - 4x^4 - 16x^2 + 256$
$\langle r\rangle$	$\langle r\rangle$	$\langle s\rangle$	$\langle s, r^2\rangle$	13 (4, 1)	3 (2, 2)	$x^8 - 9x^6 + 32x^4 - 9x^2 + 1$
$\langle r\rangle$	G	$\langle s\rangle$	$\langle s\rangle$	23 (4, 2)	3 (2, 1)	$x^8 - 3x^7 + 7x^6 - 12x^5 - 8x^4 + 84x^3 + 159x^2 + 63x + 9$
$\langle r\rangle$	G	$\langle s\rangle$	$\langle s, r^2\rangle$	3 (4, 2)	7 (2, 2)	$x^8 - 3x^7 + 4x^6 - 3x^5 + 3x^4 - 3x^3 + 4x^2 - 3x + 1$
$\langle s\rangle$	$\langle s\rangle$	$\langle sr\rangle$	$\langle sr\rangle$	3 (2, 1)	37 (2, 2)	$x^8 - 5x^6 + 28x^4 + 15x^2 + 9$
$\langle s\rangle$	$\langle s\rangle$	$\langle sr\rangle$	$\langle sr, r^2\rangle$	5 (2, 1)	41 (2, 2)	$x^8 + 15x^6 + 48x^4 + 15x^2 + 1$
$\langle s\rangle$	$\langle s, r^2\rangle$	$\langle sr\rangle$	$\langle sr, r^2\rangle$	3 (2, 2)	13 (2, 2)	$x^8 - x^7 + 2x^6 + 3x^5 - x^4 + 3x^3 + 2x^2 - x + 1$

4.2 The groups D_{10}, A_4, F_{20}

The dihedral group of order 10, the alternating group of order 12, and the Frobenius group of order 20 are all of rank $s = 1$ and have, up to an isomorphism of the group, a unique tame decomposition configuration. Each is realized over $\mathbb{Q}$:

D_{10}: $x^5 - 2x^4 + 2x^3 - x^2 + 1$ $(p = 47)$,
A_4: $x^4 - x^3 - 7x^2 + 2x + 9$ $(p = 163)$,
F_{20}: $x^5 - 2x^4 + 7x^3 - 4x^2 + 11x + 6$ $(p = 101)$.

Remark 4.1 It is not difficult to show that any Frobenius group $F = K \rtimes H$ whose Frobenius complement H is cyclic is of rank $s = 1$ and has a unique tame decomposition configuration $T = Z = H$ up to isomorphism. This includes the dihedral groups D_{2n} of order $2n$ where n is odd (H any subgroup of order 2) as well as A_4 (H any subgroup of order 3) and F_{20} (where H is a cyclic subgroup of order 4). For such groups F the existence of a realization over $\mathbb{Q}$ is just the question of realizing F as a Galois group over $\mathbb{Q}$ by an extension with a single (tamely) ramified prime.

Remark 4.2 In any realization $K/\mathbb{Q}$ of the unique tame decomposition configuration for D_{2n} with n odd (for example, for the symmetric group S_3), the (unique) quadratic subfield would be $k = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ for some odd prime $p \in \mathbb{Z}$ with K/k unramified at finite primes. It follows by class field theory that there is a tame realization for D_{2n} if and only if the class group of the quadratic field $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ contains an element of order n for the odd prime p not dividing n. For S_3, this occurs (for $p = 23$ for example), presumably infinitely often, with interesting questions on the statistics.

4.3 The groups S_4, A_5, S_5

Up to isomorphism, there are four distinct tame decomposition configurations for the symmetric group S_4, six configurations for the alternating group A_5, and seven configurations for the symmetric group S_5. Searching the number field data base [3] we find that all seventeen configurations for these three groups of rank $s = 1$ can be realized over $\mathbb{Q}$; Tables 3, 4 and 5 give the possible tame configurations $\{T, Z\}$ and for each a prime p and a polynomial $f(x)$ whose Galois closure realizes the configuration. We also indicate the splitting of the prime p in the extension F generated by a root of $f(x)$, which can be computed from the double coset decomposition of the group G under the actions of Z and the subgroup H of K fixing F. The cases where distinct Z yield the same splitting in F are distinguished by the largest subgroup N of $Z \cap H$ normal in Z—the quotient Z/N is provided in the splitting data in [3] as the Galois closure of the appropriate completion of F. All primes have residue degree 1 unless otherwise indicated.

Table 3 Decomposition configurations for S_4

T	Z	p	Splitting	Realization
$\langle(1\,2)\rangle$	$\langle(1\,2)\rangle$	283	$\wp_1^2\,\wp_2\,\wp_3$	$x^4 - x - 1$
$\langle(1\,2)\rangle$	$\langle(1\,2),\,(3\,4)\rangle$	229	$\wp_1^2\underset{(f=2)}{\wp_2}$	$x^4 - x + 1$
$\langle(1\,2\,3\,4)\rangle$	$\langle(1\,2\,3\,4)\rangle$	229	$\wp^4$	$x^4 - x^3 + 29x^2 - 43x + 17$
$\langle(1\,2\,3\,4)\rangle$	$\langle(1\,2\,3\,4),\,(1\,3)\rangle$	59	$\wp^4$	$x^4 - x^3 - 7x^2 + 11x + 3$

Table 4 Decomposition configurations for A_5

T	Z	p	Splitting	Realization
$\langle(1\,2\,3)\rangle$	$\langle(1\,2\,3)\rangle$	10,267	$\wp_1^3\,\wp_2\,\wp_3$	$x^5 - 25x^3 - 7x^2 + 116x - 45$
$\langle(1\,2\,3)\rangle$	$\langle(1\,2\,3),\,(1\,2)(4\,5)\rangle$	4253	$\wp_1^3\underset{(f=2)}{\wp_2}$	$x^5 - 2x^4 - 10x^3 + 23x^2 - 6x - 4$
$\langle(1\,2\,3\,4\,5)\rangle$	$\langle(1\,2\,3\,4\,5)\rangle$	1951	$\wp_1^5$	$x^5 - x^4 - 780x^3 + 9911x^2 - 24208x + 15952$
$\langle(1\,2\,3\,4\,5)\rangle$	$\langle(1\,2\,3\,4\,5),\,(2\,5)(3\,4)\rangle$	1039	$\wp_1^5$	$x^5 - 2x^4 - 414x^3 + 4945x^2 - 16574x + 5191$
$\langle(1\,2)(3\,4)\rangle$	$\langle(1\,2)(3\,4)\rangle$	2083	$\wp_1^2\,\wp_2^2\,\wp_3$	$x^5 - x^4 + 5x^3 + 11x^2 + 4x - 1$
$\langle(1\,2)(3\,4)\rangle$	$\langle(1\,2)(3\,4),\,(1\,3)(2\,4)\rangle$	653	$\wp_1^2\underset{(f=2)}{\wp_2}$	$x^5 + 3x^3 - 6x^2 + 2x - 1$

Table 5 Decomposition configurations for S_5

T	Z	p	Splitting	Realization
$\langle(1\,2)\rangle$	$\langle(1\,2)\rangle$	13,219	$\wp_1^2\,\wp_2\,\wp_3\,\wp_4$	$x^5 - 2x^2 - x + 1$
$\langle(1\,2)\rangle$	$\langle(1\,2),\,(3\,4)\rangle$	1609	$\wp_1^2\underset{(f=2)}{\wp_2}\,\wp_3$	$x^5 - x^3 - x^2 + x + 1$
$\langle(1\,2)\rangle$	$\langle(1\,2),\,(3\,4\,5)\rangle$	4903	$\wp_1^2\underset{(f=3)}{\wp_2}$	$x^5 - x^4 - x^3 + 2x^2 - x - 1$
$\langle(1\,2)(3\,4\,5)\rangle$	$\langle(1\,2)(3\,4\,5)\rangle$	151	$\wp_1^2\,\wp_2^3$	$x^5 - 2x^4 - x^3 + 7x^2 - 13x + 7$
$\langle(1\,2)(3\,4\,5)\rangle$	$\langle(1\,2)(3\,4\,5),\,(3\,4)\rangle$	101	$\wp_1^2\,\wp_2^3$	$x^5 - x^4 - 6x^3 + x^2 + 18x - 4$
$\langle(1\,2\,3\,4)\rangle$	$\langle(1\,2\,3\,4)\rangle$	269	$\wp_1^4\,\wp_2$	$x^5 - x^4 - 15x^3 - 11x^2 + 11x - 10$
$\langle(1\,2\,3\,4)\rangle$	$\langle(1\,2\,3\,4),\,(1\,3)\rangle$	619	$\wp_1^4\,\wp_2$	$x^5 - x^4 - 13x^3 - 6x^2 + 8x + 47$

Remark 4.3 We note that a realization K for the tame decomposition configuration $(S_n, \langle(1\,2)\rangle, \langle(1\,2)\rangle)$ gives a Galois extension of the quadratic field $k = Q(\sqrt{(-1)^{(p-1)/2}p}$ with $\mathrm{Gal}(K/k) \simeq A_n$ that is unramified over k at all finite primes and in which the prime over p in k splits completely. The existence of quadratic fields k with class number 1 but which nevertheless have nonabelian Galois extensions unramified outside finite primes was noted by Artin, who gave the example $k = \mathbb{Q}(\sqrt{19 \cdot 151})$. The first realization of the tame decomposition configuration $(S_5, \langle(1\,2)\rangle, \langle(1\,2)\rangle)$ where the class number of k is 1 occurs for the splitting field of $x^5 - 2x^4 - 3x^3 + 5x^2 + x - 1$ where $p = 36497$, and in this case K is totally real, so K/k is also unramified at the infinite primes.

4.4 The group *PSL*(2, 7)

The simple group $G = PSL(2,7) = GL_3(\mathbb{F}_2)$ of order 168 has the presentation $G = \langle a, b \mid a^2 = b^3 = (ab)^7 = [a,b]^4 = 1\rangle$ and an embedding in S_7 in which $a = (1\,2)(3\,6)$, $b = (2\,6\,7)(3\,4\,5)$, $ab = (1\,2\,3\,4\,5\,6\,7)$. The nonidentity elements in G have orders 2,3,4 and 7. Let $r = (1\,3\,2\,6)(5\,7) \in G$ and $s = (1\,2)(5\,7) \in G$. Then $r^2 = a$ and $\langle r, s\rangle \simeq D_8$, the unique

Table 6 Decomposition configurations for $G = PSL(2, 7) = GL_3(\mathbb{F}_2)$

T	Z	p	Splitting	Realization
$\langle a \rangle$	$\langle a \rangle$	6971	$\wp_1^2\ \wp_2^2\ \wp_3\ \wp_4\ \wp_5$	$x^7 - 3x^6 + 4x^5 - 3x^3 + 4x^2 - x - 1$
$\langle a \rangle$	$\langle r \rangle$	3803	$\underset{(f=2)}{\wp_1^2}\ \underset{(f=2)}{\wp_2}\ \wp_3$	$x^7 - 2x^5 - 4x^4 - x^3 + 5x^2 + 5x + 1$
$\langle a \rangle$	$\langle a, s \rangle$	2741	$\wp_1^2\ \wp_2^2\ \underset{(f=2)}{\wp_3}\ \wp_4$	$x^7 - x^6 + 2x^5 - 3x^4 - 4x^3 + 2x^2 + 3x + 1$
$\langle b \rangle$	$\langle b \rangle$		$\wp_1^3\ \wp_2^3\ \wp_3$	Unknown
$\langle b \rangle$	$\langle b, u \rangle$		$\wp_1^3\ \wp_2^3\ \wp_3$	Unknown
$\langle r \rangle$	$\langle r \rangle$	373	$\wp_1^4\ \wp_2^2\ \wp_3$	$x^7 - x^6 - 10x^5 + 14x^4 + x^3 - 4x^2 - 3x + 5$
$\langle r \rangle$	$\langle r, s \rangle$	227	$\wp_1^4\ \wp_2^2\ \wp_3$	$x^7 + 2x^5 - 4x^4 - 5x^3 - 4x^2 - 3x + 10$
$\langle ab \rangle$	$\langle ab \rangle$		$\wp_1^7$	Unknown
$\langle ab \rangle$	$\langle ab, v \rangle$		$\wp_1^7$	Unknown

Sylow-2 subgroup containing $\langle a \rangle$ as a normal subgroup, is the normalizer in G of both $\langle a \rangle$ and $\langle r \rangle$. The normalizer in G of $\langle b \rangle$ is $\langle b, u \rangle \simeq S_3$ where $u = (2\,6)(4\,5)$, and the normalizer in G of ab is the Frobenius group of order 21, $\langle ab, v \rangle$, where $v = (1\ 2\ 4)(3\ 6\ 5)$. Up to isomorphism, there are nine distinct tame decomposition configurations for G. In this case, the number field data base [3] provides realizations for the five configurations whose inertia groups have order 2 or 4. Realizations for the other possible inertia groups would involve totally real fields (see [4]), and there are substantially fewer of these available: of the approximately 100 totally real septic fields currently in [3] and [9], and the 138 currently in [5], none are minimally tamely ramified at a single prime with odd order inertia group. The results for $PSL(2, 7)$ are summarized in Table 6, where all primes have residue degree 1 unless otherwise indicated.

We note that for inertia group of order 3, there are examples in the databases that are tamely ramified at two primes (e.g., at 5 with inertia of order 3, and at 6247 with inertia of order 2). For inertia group of order 7, the smallest number of ramified primes in the databases is three, with a single tamely ramified example (ramified at 11 with inertia of order 7, at 5 with inertia of order 2, and at 19 with inertia of order 4).

Remark 4.4 The configurations $(G, \langle a \rangle, \langle a, s \rangle)$ and $(G, \langle a \rangle, \langle a, sr^3 \rangle)$ are isomorphic under the outer automorphism of G that maps a to a and b to b^{-1} (but are not isomorphic under an inner automorphism), hence define the same tame decomposition configuration for G. We note that this configuration manifests itself in the two nonisomorphic ('sibling' and arithmetically equivalent) subfields of degree 7 in any realization as different splittings of the prime p (making them appear at first to be distinct decomposition configurations in the [3] database). For example, the sibling septic to that in the table above for the configuration $(G, \langle a \rangle, \langle a, s \rangle)$ is the field defined by $f = x^7 - x^6 - 4x^5 + x^4 + 4x^3 - 3x + 1$, in which the prime $p = 2741$ splits as $\underset{(f=2)}{\wp_1^2}\ \wp_2\ \wp_3\ \wp_4$.

5 Conclusion

For finite abelian Galois groups, the only obstruction to obtaining a realization for a (minimal) tame decomposition configuration arises from constraints imposed by quadratic

reciprocity and for nonabelian groups of *odd* order we have no examples of minimal tame decomposition configurations that cannot be realized. Our computations suggest, for example, that every tame decomposition configuration can be realized for groups normally generated by a single element, so in particular for every finite simple group and for the symmetric groups S_n.

Authors' contributions
Both authors contributed equally to this work, although each believes the other contributed more. Both authors read and approved the final manuscript.

Author details
[1]Department of Mathematics, University of Vermont, Lord House, 16 Colchester Ave., Burlington, VT 05405, USA,
[2]Department of Mathematics and Statistics and CICMA, Concordia University, 1455 de Maisonneuve Blvd. West, Montreal, QC H3G 1M8, Canada.

Acknowledgements
We would like to thank Richard Foote for many helpful conversations. The second author was supported in part by a grant from NSERC.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Received: 14 February 2017 Accepted: 22 June 2017
Published online: 02 October 2017

References

1. Dummit, D., Dummit, E., Kisilevsky, H.: A characterization of quadratic residue matrices. J. Number Theory **168**, 167–179 (2016)
2. Fröhlich, A.: Artin root numbers and normal integral bases for quaternion fields. Invent. Math. **17**, 143–166 (1972)
3. Jones, J.: A database of number fields. LMS J. Comput. Math. **17**(1), 595–618 (2014)
4. Jones, J., Roberts, D.: Mixed degree number field computations, preprint, arXiv:1602.09119v1 (2016)
5. Klüners, J., Malle, G.: A database for field extensions of the rationals. LMS J. Comput. Math. **4**, 182–196 (2001)
6. Kutzko, P.: On groups of finite weight. Proc. Am. Math. Soc. **55**(2), 279–280 (1976)
7. Kisilevsky, H., Sonn, J.: On the minimal ramification problem for l-groups. Compos. Math. **146**(3), 599–606 (2010)
8. Kisilevsky, H., Neftin, D., Sonn, J.: On the minimal ramification problem for semiabelian groups. Algebra Number Theory **4**(8), 1077–1090 (2010)
9. The LMFDB Collaboration: The L-functions and modular forms database. http://www.lmfdb.org. Accessed Aug 2016 (2013)
10. Schmid, P.: Quaternion extensions with restricted ramification. Acta Arith. **165**(2), 123–140 (2014)
11. Witt, E.: Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f. J. Crelle **174**, 237–245 (1936)