UNRAMIFIED EXTENSIONS OF QUADRATIC NUMBER FIELDS WITH CERTAIN PERFECT GALOIS GROUPS

JOACHIM KÖNIG

Abstract. We provide infinite families of quadratic number fields with everywhere unramified Galois extensions of Galois group $\text{SL}_2(7)$ and $2.A_7$, respectively. To my knowledge, these are the first instances of infinitely many such realizations for perfect groups which are not generated by involutions, a property which makes them difficult to approach for the problem in question and leads to somewhat delicate local-global problems in inverse Galois theory.

1. Introduction and main results

The following is a folklore conjecture in inverse Galois theory:

Conjecture 1. For any finite group $G$, there exist infinitely many quadratic number fields $K$ such that $K$ possesses a Galois extension with Galois group $G$ unramified at all (finite and infinite) primes of $K$.

This is known to be true only in some special cases, including the case of cyclic groups (from class field theory, cf. [1]), symmetric and alternating groups (e.g., [22] (which does not consider ramification at infinity) or [6] (which does)), and a few other almost simple finite groups (e.g., [10]). The common idea for the nonsolvable cases is to carefully specialize suitable function field extensions over $\mathbb{Q}$ (or equivalently, multiparameter polynomials over $\mathbb{Q}$) with prescribed Galois group to obtain extensions of $\mathbb{Q}$ with a desired ramification behavior. Further evidence for Conjecture 1 is provided by analogs over global function fields, which have proved fruitful and led to concrete distribution heuristics, in [21], for extensions $L/K$ with $[K : \mathbb{Q}] = 2$ and $\text{Gal}(L/K) = G$. We will neither present nor use those heuristics in the present paper, although it is useful to keep in mind that the expected distribution differs depending on the concrete Galois group $\text{Gal}(\tilde{L}/\mathbb{Q}) \leq G \wr C_2$, where $\tilde{L}$ denotes the Galois closure of $L/\mathbb{Q}$.

Notably, for groups such as $G = S_n$, in order to solve Conjecture 1 it suffices to obtain Galois extensions $L/\mathbb{Q}$ with group $S_n$ in which all nontrivial inertia groups are generated by transpositions and then base change to suitable quadratic number fields, killing ramification via Abhyankar’s lemma; in the above terminology, this corresponds to the case $\text{Gal}(L/\mathbb{Q}) = G \times C_2$. The same “direct” approach can in principle succeed for all groups $G$ generated by involutions, but only for those. In particular, all non-abelian simple groups are generated by involutions (due to the Feit-Thompson theorem). Admittedly, in practice, realizations with involution inertia are not always easy to obtain; in particular, their existence still seems unknown for arbitrary alternating groups, whence those are instead dealt with via the above $S_n$-extensions $L/\mathbb{Q}$, in which $L/L^{A_n}$ is automatically unramified.

In this paper, we wish to progress to nonsolvable groups which are not generated by involutions, i.e., for which the “$G \times C_2$” approach cannot possibly be employed. Concretely, we show:

1Or more generally, by involutions, although allowing this does not seem to make the problem much easier.
Theorem 1.1. Let $G$ be one of $SL_2(7)$ and $2.A_7$. Then there exist infinitely many quadratic number fields possessing an everywhere unramified Galois extension with Galois group $G$.

We remark that for the cases treated in Theorem 1.1 there are explicit polynomials available, which make a concrete enumeration of infinitely many quadratic number fields with the above property possible. In Theorem 5.1 we give such an explicit family in the case $G = SL_2(7)$. At the same time, it should be noted that the proof of Theorem 1.1 itself does not rely on the concrete shape of these polynomials, instead requiring only general theoretical results such as the rigidity method, and results on the behavior of inertia and decomposition groups under specialization of function field extensions (as well as the subgroup structure of the groups in question).

Note also that the analog of Theorem 1.1 is known for the group $SL_2(3)$ (which, however, is a solvable group, namely a double cover of $A_4$) due to [18] (cf. also [23, Proposition 7]).

We also prove the following result applicable to infinitely many groups $SL_2(p)$, although with a weaker conclusion.

Theorem 1.2. Let $p$ be a prime with $p \equiv 3 \mod 4$ and $p \not\equiv -1 \mod 24$. Then there exist infinitely many quadratic number fields possessing an $SL_2(p)$-extension unramified everywhere outside of the prime ideal(s) dividing $p$.

We give some further motivation for the consideration of the groups above, as well as some insights about the difficulties in dealing with them, in the next section.

2. Some further motivation

There are different classes of nonsolvable groups not generated by involutions, all interesting in their own right, and regarding unramified extensions of quadratic number fields, little seems to be known about any of them. Just to give one example, even though explicit families of quadratic number fields are known for each of $G = S_n$ ($n \geq 5$) and $H = C_m$ ($m \geq 3$), considering the same problem for the group $G \times H$ leads to delicate arithmetic questions (namely, about existence of discriminants falling into two classes simultaneously; see also Remark 5).

We focus instead on a different class of groups, namely quasisimple groups $G$ not generated by involutions. Here, a group $G$ is called quasisimple if it fits into an exact sequence $1 \rightarrow Z \rightarrow G \rightarrow S \rightarrow 1$ with $Z = Z(G)$, $S$ a simple group, and $G$ is perfect (i.e., equal to its commutator subgroup). Perfectness is a logical assumption in order to make the problem of identifying unramified $G$-extensions “disjoint” from the problem of class number divisibility of quadratic fields. Instead, several other challenges arise. Notably, in inverse Galois theory, Galois extensions with such groups are usually obtained via first realizing a suitable quotient group such as $S = G/Z(G)$ and then solving a central embedding problem. This alone is usually a nontrivial problem; see, for example, the realization of covering groups of the alternating and symmetric groups, which was investigated by many authors ([17], [23], [18], [14] are just some of the relevant papers on this topic).

The additional condition that $G$ should not be generated by involutions means in particular that none of the involutions of $S$ lift to involutions in $G$, implying that $|Z|$ is even and the 2-Sylow group of $G$ does not contain a subgroup isomorphic to $C_2 \times C_2$, and hence must be cyclic or generalized quaternion. Since it is well-known that a nonabelian simple group cannot have a cyclic 2-Sylow subgroup, we are left with the quaternion case. Here, the 2-Sylow group of $S$ for what it’s worth, our proof yields quadratic fields in which $p$ is inert, i.e., extended only by a single prime ideal.
must be (the central quotient of a generalized quaternion group, and hence) dihedral, and it is then
known ([3, Theorem 2]) that $S$ is either $A_7$ or a group $PSL_2(q)$ with $q \geq 5$ an odd prime
power.

Through this consideration (and via the known Schur multipliers of the simple groups above),
we have arrived naturally at the set of groups to be considered: they are the double covers
$SL_2(q) = 2.PSL_2(q)$ (with $q$ odd) as well as the even degree covering groups $2.A_7$, $6.A_7$ and
$6.PSL(2,9) \cong 6.A_6$.

The joint idea to attack these groups for our problem is the fact that they embed as index-2
normal subgroups into groups which are generated by involutions (namely, central extensions of
$\Gamma = PGL_2(q)$ and of $\Gamma = S_7$ by $C_2$ (and in two cases, noncentral extensions by $C_6$), respectively).
This is analogous to the embedding of $A_n$ into $S_n$ as discussed above, but additional problems
arise here. Namely, we additionally need to begin with a prescribed ramification behavior in
the $\Gamma$-extension, and make sure that the embedding problem with kernel $C_2$ is solvable without
introducing extra ramification. We use a function field approach to control the behavior of
inertia and decomposition groups under specialization. In this setting, it turns out that the
embedding problem usually leads to simultaneous requirements on the ramification index as well
as the residue extension at given branch points of the function field extension. E.g., recall once
more that the problem for the simple group $A_n$ itself is solved via constructing $S_n$-extensions
of $\mathbb{Q}$ in which all non-trivial inertia groups are generated by transpositions, which is achieved
via finding degree-$n$ extensions with squarefree discriminant, whose existence is well-known.
However in order to ensure that such an $S_n$-extension has no local obstruction to embedding
into an extension with Galois group $2.S_n$, one needs to impose conditions on the Frobenius class
of (all!) prime divisors of the squarefree values of such discriminants. This is usually difficult to
guarantee without relying on open conjectures (cf., e.g., [6, Section 4] for some informal remarks
on the difficulty of such problems), and in a setting of specialization of function field extensions
amounts to finding values of certain (discriminant) polynomials with all prime divisors in some
prescribed Chebotarev set. In this light, Theorem 1.1 means that in some special cases, these
extra requirements can be obtained unconditionally.

3. Prerequisites

3.1. Local behavior of specialization of function field extensions. We review some known
results about the behaviour of inertia and decomposition groups in specializations of function
field extensions. Since these occur in several predecessor works, we restrict to the most directly
relevant results. For further background on function field extensions and their specialization, cf.,
e.g., [3], Sections 2 and 3.

For a finite Galois extension $N/K(t)$ of function fields and any value $t_0 \in \mathbb{P}^1(K)$, we denote by
$N_{t_0}/K$ the specialization of $N/K(t)$ at $t \mapsto t_0$, i.e., the residue extension at any place extending
t $\mapsto t_0$ in $N$. Recall that $N/K(t)$ is called $K$-regular if $K$ is algebraically closed in $N$. The
following well-known theorem, cf. [3, Prop. 4.2], ties the ramification in specializations of a
function field extension to the inertia groups at branch points of that function field extension.

**Theorem 3.1.** Let $K$ be a number field and $N/K(t)$ a finite $K$-regular Galois extension with
Galois group $G$. Then there exists a finite set $S_0$ of primes, depending only on $N/K(t)$, such
that the following holds for every prime $\mathfrak{p}$ of $K$ not in $S_0$:
If $t_0 \in K$ is not a branch point of $N/K(t)$ then the following condition is necessary for $\mathfrak{p}$ to be
ramified in the specialization $N_{t_0}/K$:
e_i := I_{\mathfrak{p}}(t_0, t_i) > 0$ for some (automatically unique, up to algebraic conjugates) branch point $t_i$. 

Here \( I_p(t_0, t_i) \) is the intersection multiplicity of \( t_0 \) and \( t_i \) at the prime \( p \). Furthermore, the inertia group of a prime extending \( p \) in the specialization \( N_{t_0}/K \) is then conjugate in \( G \) to \( \langle \tau^a \rangle \), where \( \tau \) is a generator of an inertia subgroup over the branch point \( t \mapsto t_i \) of \( K(t) \).

Regarding the definition of intersection multiplicity \( I_p \) occurring in Theorem 3.2, note that in the special case \( K = \mathbb{Q} \) this may be defined conveniently in the following way: Let \( f(X) \in \mathbb{Z}[X] \) be the irreducible polynomial of \( t_i \) over \( \mathbb{Z} \) and \( \tilde{f}(X, Y) \) its homogenization (with \( \tilde{f} := Y \) in the special case \( t_i = \infty \)). Let \( t_0 = \frac{x}{y} \) with \( a, b \in \mathbb{Z} \) coprime, and let \( p \) be a prime number. Then \( I_p(t_0, t_i) \) is the multiplicity of \( p \) in \( \tilde{f}(a, b) \).

The following result (cf. [9, Thm. 4.1]) clarifies the structure of decomposition groups in specializations. To state it, we need to introduce a bit more notation. Given a finite Galois extension \( N/K(t) \) with group \( G \) and a \( K \)-rational place \( t \mapsto a \in \mathbb{P}^1(K) \), denote by \( D_a \) and \( I_a \) the decomposition and inertia group at the place \( t \mapsto a \) respectively. Furthermore, given a prime \( p \) of \( K \), denote by \( D_{a,p} \) the decomposition group at \( p \) in the residue extension \( N_a/K \). Note that the Galois group of \( N_a/K \) is identified with \( D_a/i_a \), and hence \( D_{a,p} \) is identified with a subgroup of this group.

**Theorem 3.2.** Let \( K \) be a number field and \( N/K(t) \) a finite \( K \)-regular Galois extension with Galois group \( G \). Let \( t \mapsto t_i \in \mathbb{P}^1(K) \) be a branch point of \( N/K(t) \), and let \( I_{t_i} \) and \( D_{t_i} \) denote the inertia and decomposition group at \( t \mapsto t_i \) in \( N(t_i)/K(t_i)(t) \). Then there exists a finite set \( S_1 \) of primes of \( K \), depending only on \( N/K(t) \) and containing the set \( S_0 \) from Theorem 3.1, such that for all primes \( p \) of \( K \) not in \( S_1 \) and all non-branch points \( a \in \mathbb{P}^1(K) \) of \( N/K(t) \), the following hold:

a) Assume that \( p \) ramifies in \( N_a/K \) and \( I_p(a, t_i) > 0 \). Let \( D_{t_i,p'} \) denote the decomposition group of \( N(t_i)_{p'}/K(t_i) \) at the (unique) prime \( p' \) of \( K(t_i) \) extending \( p \) such that \( I_{p'}(a, t_i) > 0 \). Then the decomposition group \( D_{a,p} \) at \( p \) in \( N_a/K \) fulfills \( \varphi(D_{a,p}) = D_{t_i,p'} \), where \( \varphi : D_{t_i} \to D_{t_i}/I_{t_i} \) is the canonical epimorphism.

b) In particular, if additionally \( I_p(a, t_i) = 1 \), then \( D_{a,p} = \varphi^{-1}(D_{t_i,p}) \).

**Remark 1.**

a) The finite exceptional set \( S_1 \) in Theorem 3.2 can be made explicit, and this is sometimes relevant when doing calculations with concrete extensions, as we will do in Theorem 5.1. In order to avoid too much technicality, we only refer to [11, Theorem 2.2] for an effective version of Theorem 3.2.

b) For many applications, it is enough to obtain some specialization values \( a \in \mathbb{P}^1(K) \) yielding a certain prescribed local behavior, rather than controlling the behavior for all specialization values. In this context, the notion of a universally ramified prime (see [2] or [10]) becomes useful: let \( \mathcal{U}(N/K(t)) \) be the set of all primes of \( K \) ramifying in all specializations \( N_a/K \) where \( a \in \mathbb{P}^1(K) \) is a non-branch point of \( N/K(t) \). Let \( \mathcal{S} \) be any finite set of primes of \( K \) disjoint from \( \mathcal{U}(N/K(t)) \). Then there exists a non-empty and \( \mathcal{S} \)-adically open set of values \( a \in \mathbb{P}^1(K) \) such that \( N_a/K \) is unramified at all \( p \in \mathcal{S} \) (an easy consequence of Krasner’s lemma). In particular, by choosing \( \mathcal{S} := \mathcal{S}_1 \setminus \mathcal{U}(N/K(t)) \) with \( \mathcal{S}_1 \) as in Theorem 3.2, we see that for all such values \( a \), the assertion of Theorem 3.2 actually holds with \( \mathcal{S}_1 \) replaced by \( \mathcal{U}(N/K(t)) \), and the latter set is often much more accessible and can be bounded very effectively by simply comparing some very few specializations.

---

[3]: The latter is guaranteed to happen for some branch point \( t_i \), unique up to algebraic conjugates, by Theorem 3.2.
We will also require the following lemma, describing the behavior of residue extensions under certain rational pullbacks.

**Lemma 3.3.** Let $N/K(t)$ be a $K$-regular Galois extension with group $G$, let $I$ and $D$ denote the inertia and decomposition group at the place $t \mapsto 0$, and assume that the extension $1 \rightarrow I \rightarrow D \rightarrow D/I \rightarrow 1$ splits. Then there exists $\alpha \in K^*$ such the following holds:

If $\varepsilon := |I|$ and $u$ is such that $u^e = \alpha t$, then the extension $N(u)/K(u)$ is unramified at $u \mapsto 0$ with decomposition group isomorphic to $D/I$.

*Proof.* Let $U$ be a complement to $I$ in $D$, let $\hat{N}/K((t))$ denote the completion of $N/K(t)$ at $t \mapsto 0$, and $F/K$ the residue extension of $N/K(t)$ at $t \mapsto 0$. In particular, $Gal(\hat{N}/K((t))) \cong D$, and $\zeta \in F$. Let $\hat{N}^U$ denote the fixed field of $U$. Then $\hat{N}^U/K((t))$ is totally ramified of degree $e$, and hence equal to $K((\sqrt{\alpha t})) =: K((u))$ for a suitable $\alpha \in K$. Consequently, $\hat{N} = F((u))$. Now firstly, since $K(u)/K(t)$ is totally ramified of index $e$ at $t \mapsto 0$, the extension $E(u)/K(u)$ is unramified at $u \mapsto 0$. Furthermore, the residue extension $E(u)_0/K$ is necessarily contained in the compositum of $K(\zeta)(u)$ (i.e., the Galois closure of $K((u))/K((t))$) and $\hat{N} = F((u))$; since $\zeta \in F$, this compositum is $F((u))$, and thus its residue extension is $F$. Conversely, the completion at $u \mapsto 0$ has to be of degree at least $|D|/[K(u) : K(t)] = |D/I| = |F : K|$, yielding the assertion. □

**Remark 2.** The splitting condition in the assumption of Lemma 3.3 is necessary. Indeed, an analog of Theorem 3.2 (with the base field $K$ replaced by the function field $K(u)$) shows that the decomposition group at $u \mapsto 0$ in $N(u)/K(u)$ is a subgroup of $D$ projecting onto $D/I$. This observation is essentially the reason why we are so far unable to include the (smaller) group $G = SL_2(5)$ in Theorem 3.4.

3.2. Embedding problems. We recall some basic terminology around embedding problems; cf., e.g., [13, Chapter III.5]. A finite embedding problem over a field $K$ is a pair $(\varphi : G_K \rightarrow G, \varepsilon : G \rightarrow G)$, where $\varphi$ is a (continuous) epimorphism from the absolute Galois group $G_K$ of $K$ onto $G$, and $\varepsilon$ is an epimorphism between finite groups $\hat{G}$ and $G$ fitting in an exact sequence $1 \rightarrow N \rightarrow \hat{G} \rightarrow G \rightarrow 1$. The kernel $N = \ker(\varepsilon)$ is called the kernel of the embedding problem. An embedding problem is called central if $\ker(\varepsilon) \leq Z(\hat{G})$. A (continuous) homomorphism $\psi : G_K \rightarrow \hat{G}$ is called a solution to $(\varphi, \varepsilon)$ if the composition $\varepsilon \circ \psi$ equals $\varphi$. In this case, the fixed field of $\ker(\psi)$ is called a solution field to the embedding problem. A solution $\psi$ is called a proper solution if it is surjective. In this case, the field extension of the solution field over $K$ has full Galois group $\hat{G}$.

If $K$ is a number field and $p$ is a prime of $K$, every embedding problem $(\varphi, \varepsilon)$ induces an associated local embedding problem $(\varphi_p, \varepsilon_p)$ defined as follows: $\varphi_p$ is the restriction of $\varphi$ to $G_{K_p}$ (well defined up to fixing an embedding of $K$ into $\overline{K_p}$), and $\varepsilon_p$ is the restriction of $\varepsilon$ to $\varepsilon^{-1}(G(p))$, where $G(p) := \varphi_p(G_{K_p})$.

We require two well-known results on central embedding problems. The first (cf. [13, Chapter IV, Cor. 10.2]) is a local-global-principle for the solvability of such embedding problems, which is essentially a consequence of the local-global principle for Brauer embedding problems over number fields ([13, Chapter IV, Cor. 7.8]).

**Proposition 3.4.** Let $\Gamma = C.G$ be a central extension of $G$ by a cyclic group $C$ of prime order and $\varepsilon : \Gamma \rightarrow G$ the canonical projection. Let $\varphi : G_Q \rightarrow G$ be a continuous epimorphism. Then the embedding problem $(\varphi, \varepsilon)$ is solvable if and only if all associated local embedding problems $(\varphi_p, \varepsilon_p)$ are solvable, where $p$ runs through all primes of $\mathbb{Q}$ (including the infinite one).
Since the local embedding problem at an unramified prime is always solvable, the above lemma gives an efficient method to check for global solvability of a given embedding problem by investigating only the finitely many ramified primes of $K/Q$.

The second result (see [17, Prop. 2.1.7]) is a tool to control ramification in solutions of central embedding problems, assuming solvability.

**Proposition 3.5.** Let $\Gamma = C.G$ be a central extension of $G$ by a finite abelian group $C$, let $\varepsilon : \Gamma \to G$ be the canonical projection, and let $\varphi : G_Q \to G$ be a continuous epimorphism such that the embedding problem $(\varphi, \varepsilon)$ has a solution. For each finite prime $p$, let $\tilde{\varphi}_p : G_{Q_p} \to \Gamma$ be a solution of the associated local embedding problem $(\tilde{\varphi}_p, \varepsilon_p)$, chosen such that all but finitely many $\tilde{\varphi}_p$ are unramified. Then there exists a (not necessarily proper) solution $\tilde{\varphi} : G_Q \to \Gamma$ of $(\varphi, \varepsilon)$ such that for all finite primes $p$, the restrictions of $\tilde{\varphi}$ and $\tilde{\varphi}_p$ to the inertia group inside $G_{Q_p}$ coincide. In particular, $\tilde{\varphi}$ is ramified exactly at those finite primes $p$ for which $\tilde{\varphi}_p$ is ramified.

4. Proof of Theorem 1.2

**Proof.** We first describe the general strategy. We will show the assertion by first constructing “suitable” $PGL_2(p)$-extensions of $\mathbb{Q}$ and then embedding them into $2.PGL_2(p)$-extensions using Propositions 3.4 and 3.5. Here, by $2.PGL_2(p)$, we mean the stem extension of $PGL_2(p)$ in which the “outer” involutions (i.e., the one not contained in $PSL_2(p)$) are generated by involutions outside of $PSL_2(p)$ where away from $PSL_2(p)$, meaning that all nontrivial inertia groups other than possibly over $p$ must be generated by involutions outside of $PSL_2(p)$. There is only one class of such involutions in $PGL_2(p)$. The decomposition group $D$ at a prime with such an inertia subgroup must of course be contained in the centralizer of such an involution; this centralizer contains (e.g.) a subgroup $C_2 \times C_2$, which is non-split in $2.PGL_2(p)$ and whose preimage is isomorphic to the dihedral group $D_4$. Thus, if in the given $PGL_2(p)$-extension, some prime $q$ had this decomposition and inertia subgroup, then assuming the existence of a lifting to $2.PGL_2(p)$, the decomposition group at $q$ would be $D_4$. Since however the “outer” involution lifts to a (non-central) element of order 2 in $D_4$, this would imply that the inertia subgroup in the $2.PGL_2(p)$-extension would be a non-normal of the decomposition group, a contradiction. In other words, a prime with decomposition group $C_2 \times C_2$ would constitute a local obstruction to the solvability of the central embedding problem. In our construction below, we thus need to ensure among others (using Theorem 3.2 that such primes do not occur. As we will see, for primes with inertia group generated by an outer involution, the above is in fact the only local obstruction.

Due to the assumption $p \equiv 3 \mod 4$ and $p \not\equiv -1 \mod 24$, at least one of 2 and 3 is a non-square modulo $p$. Thus, by [13, Chapter I, Cor. 8.10], there exists a $\mathbb{Q}$-regular Galois extension $E/Q(t)$ with Galois group $PGL_2(p)$, and with the following properties: $E$ is ramified at exactly three points $t_i \in \mathbb{P}^1(\mathbb{Q})$ ($i = 1, 2, 3$), all $\mathbb{Q}$-rational, and the corresponding inertia groups are generated by elements of conjugacy class $pA$ (for $t_1$), $4A$ or $6A$ (for $t_2$, depending on whether 2 or 3 is a non-square modulo $p$), and $2B$ (for $t_3$), in Atlas notation. Here $2B$ is the unique class of involutions outside of $PSL_2(p)$. Up to a fractional linear transformation in $t$, we may and will assume $t_1 = 0$, $t_2 = \infty$ and $t_3 = 1$. Now consider the residue extensions at the branch points $t_1$ and $t_3$. Since $p \equiv 3 \mod 4$, the elements of class $2B$ are involutions with exactly two fixed points in the standard action of $PGL_2(p)$ on $p + 1$ points. The centralizer of an element of class $2B$ is $PGL_2p$ isomorphic to $C_2 \times D_{(p-1)/2}$, where $D_{(p-1)/2}$ denotes the dihedral group of order $p - 1$, and thus the residue extension at $t_1$ is of degree dividing $p - 1$, with Galois group a subgroup of $D_{(p-1)/2}$. Assume that it is indeed of even degree. Then it has a unique quadratic subextension, which we denote by $Q(\sqrt{b})/Q$. Consider the extension $E(s)/Q(s)$, where $s$ is such that $\beta t = s^2$. 
This is still a $\mathbb{Q}$-regular $PGL_2(p)$-extension (indeed, the quadratic extension $\mathbb{Q}(s)/\mathbb{Q}(t)$) has only one branch point in common with the quadratic subextension of $E/\mathbb{Q}(t)$, ramified at $s = 0$, $s = \infty$ and $s = \pm \sqrt{3}$. In particular, the residue field at the latter two branch points “swallows” the above quadratic subextension, whence the residue extension at any of those two branch points in $E(s)/\mathbb{Q}(s)$ is now cyclic of odd degree.

Now consider the residue extension at $t_1$. Since the normalizer of a subgroup of order $p$ in $PGL_2(p)$ is isomorphic to $C_p \times C_{p-1}$, the residue extension at this branch point is of degree dividing $p - 1$; and since furthermore, the residue extension at a branch point of ramification index $e$ must always contain the $e$-th roots of unity (e.g.,[3, Lemma 2.3]), it follows that this residue extension in fact equals $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Since $s \to 0$ is the unique place over $t \to 0$ in $E(s)$, the same holds for the residue extension of $E(s)/\mathbb{Q}(s)$ at $s = 0$. It then follows from Lemma 3.3 that for suitable $s = \mathbb{Q}$, the extension $E(u)/\mathbb{Q}(u)$, where $u$ is such that $s = \alpha u^p$, is $\mathbb{Q}$-regular with group $PGL_2(p)$, unramified at $u = 0$ and with residue field extension still equal to $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ (in particular, unramified outside of $p$ and $\infty$). Furthermore, at the branch points of $E(u)/\mathbb{Q}(u)$ extending $s = \pm \sqrt{3}$, the Galois group of the residue extension is guaranteed to inject into the one at $s = \pm \sqrt{3}$. This is because $\mathbb{Q}(u)/\mathbb{Q}(s)$ is unramified at those points, whence the inertia group $I$ at such a branch point in $E(u)/\mathbb{Q}(u)$ is the same as the corresponding one in $E(s)/\mathbb{Q}(s)$, and the decomposition group $D$ certainly cannot grow under pullback, implying the quotient of decomposition over inertia group cannot grow either.

Now from Theorem 3.2, we obtain the following: For all $u_0 \in \mathbb{Q}$ of the form $u_0 = \frac{a}{b^2}$ (with integers $u_1, u_2$ and all but finitely many primes $q$, if the specialization $E(u_0)/\mathbb{Q}$ is ramified at $q$, then its inertia group in generated by an element of class $2B$ and its decomposition group embeds into $C_2 \times C_{(p-1)/2} \equiv C_{p-1}$. In particular, no such prime yields a local obstruction to the embedding problem induced by $2PGL_2(p) \to PGL_2(p)$, since the group elements of order $2B$, and a fortiori the odd order elements of $C_{(p-1)/2}$ are split in the central extension. To deal with the remaining finitely many primes $q$, it suffices to additionally choose $u_0$ $q$-adically sufficiently close to $u = 0$. Indeed, $E(u_0)/\mathbb{Q} = \mathbb{Q}(\zeta_p)/\mathbb{Q}$ is unramified away from $\{p, \infty\}$. Remark 1b) yields that for $q \neq p$ finite, the extension $E(u_0)$ is then unramified at $q$; whereas for $q = p$, it is cyclic and totally ramified of degree $p - 1$. Again, as above, the cyclic subgroups of order $p - 1$ are split in the central extension. Finally, the infinite prime yields no local obstruction either, since specializing sufficiently close to $u = 0$ (in the archimedean absolute value yields as complex conjugation an involution inside $C_{p-1}$, i.e., once again an element of class $2B$ in $PGL_2(p)$.

Via Proposition 3.3, we may thus solve the embedding problem induced by $G_0 \to \text{Gal}(E(u_0)/\mathbb{Q})$ and $2PGL_2(p) \to PGL_2(p)$, and due to Proposition 3.3, this can in fact be achieved without any ramification inside the kernel (since all non-trivial inertia groups were split). Thus, if $K$ denotes the fixed field of $SL_2(p)$ in the resulting extension $L/\mathbb{Q}$, then all inertia groups in $\text{Gal}(L/\mathbb{Q})$, except the ones at $p$, are generated by involutions outside of $\text{Gal}(L/K)$, whence $L/K$ is ramified only above $p$. This concludes the proof.

Remark 3. The extensions of $\mathbb{Q}$ with Galois group $PGL_2(p)$ constructed in the above proof are in particular locally cyclic, i.e., all decomposition groups at primes of $\mathbb{Q}$ are cyclic. This property was previously studied in [4], and locally cyclic extensions were obtained, e.g., for the special case $G = PGL_2(7)$ ([4, Theorem 5.5]). Our above result (for infinitely many primes $p$) in particular improves on [4, Theorem 2.1].

---

4The power in the denominator indeed only needs to be a multiple of the ramification index at $\infty$ in $E(u)/\mathbb{Q}(u)$, in order to avoid ramification induced by this branch point; by construction, this ramification index is either 2 or 3, depending on which of the two possible ramification types we started with.

5Note that this is possible within the set of values $u_0$ chosen above.
5. Proof of Theorem 1.1

We first prove Theorem 1.1 in a purely theoretical way, using only ramification data and group-theoretical properties. Afterwards, we will make the conclusion more concise using computations with some explicit polynomials.

5.1. The case $G = SL_2(7)$.

Proof. In the following, we adapt the proof of Theorem 1.2 somewhat for the special case $p = 7$, in order to get rid of ramification at $p$. Note that since $3$ is a non-square modulo $7$, the extensions $E/Q(t)$ used in the proof of Theorem 1.2 are of ramification type $(pA, 6A, 2B) = (7A, 6A, 2B)$. After pullback by an extension $Q(u)/Q(t)$ of rational function fields as in the above proof, we obtain a $PGL_2(7)$-extension $E(u)/Q(u)$ with the following ramification data: inertia group of order $3$ at $u = \infty$, and a total of $14$ branch points of ramification index $2$ and with residue extension of odd degree; furthermore, no ramification above $u \mapsto 0$. We specialize $u \mapsto u_0$ essentially as above, except that we will choose $u_0$ $7$-adically close to $u = \infty$ rather than to $u = 0$. Note that the normalizer of a subgroup of order $3$ in $PGL_2(7)$ is isomorphic to $S_3 \times C_2 \cong C_3 \rtimes (C_2 \times C_2)$, whence the residue extension $E(u)_{\infty}/Q$ is of degree dividing $4$, and on the other hand (due to the ramification index being $3$) contains $Q(C_3)$. Note furthermore that $Q_7$ contains the third roots of unity, whence the completion of $E(u) \cdot Q_7/Q_7(u)$ at $u \mapsto \infty$ has Galois group embedding into the centralizer $C_{PGL_2(7)}(C_3)$ and in particular the residue extension $E(u)_{\infty}/Q_7/Q_7$ is either trivial or generated by an involution centralizing $C_3$. Such an involution necessarily lies outside of $PSL_2(7)$.

As before, Lemma 3.3 yields that there exists $\gamma \in \mathbb{Q}$ such that for $v$ defined via $u = \gamma v^3$, the extension $E(v)/Q(v)$ is still $\mathbb{Q}$-regular of group $PGL_2(7)$, unramified at $v = \infty$ and with residue extension $E(v)_{\infty}/Q$ contained in the above residue extension $E(u)_{\infty}/Q$.

Specialize $v \mapsto v_0$ $7$-adically close to $v = \infty$. Then by Krasner’s lemma, the local behavior of $E(v)/Q(v)$ at $p = 7$ is the same as that of $E(v)_{\infty}/Q$. In particular, by the above, the completion $E(v)_{\infty} \cdot Q_7/Q_7$ is either trivial or quadratic with Galois group generated by an involution of class $2B$. As before, this constitutes no local obstruction to the central embedding problem with kernel $C_2$, and we thus obtain (for $p = 7$) the conclusion of Theorem 1.2 without the exception at $p$. \hfill \Box

Remark 4. Theorem 1.2 and its proof explicitly include also the case $p = 3$. We leave it as an exercise to the reader to adapt the argument in the proof of Theorem 1.1 above to regain the analogous (and already known) statement for $p = 3$ (i.e., infinitely many quadratic number fields with everywhere unramified $SL_2(3)$-extensions).

In the following, we make the assertion of Theorem 1.1 more precise by giving a fully explicit family of quadratic number fields possessing unramified $SL_2(7)$-extensions. Theorem 5.1 should be compared with previous results on explicit families of number fields with class number divisible by prescribed integers $n$ (see, e.g., [4] for an overview as well as new results).

Theorem 5.1. For all odd integers $t \in 2\mathbb{Z} + 1$, the quadratic number field $Q(\sqrt{-7 \cdot (108 + t^4)}/7^t)$ possesses an everywhere unramified $SL_2(7)$-extension.

\footnote{Here we have used the general fact that the action of the decomposition group on an inertia subgroup of order $\epsilon$ is via the Galois action of the $\epsilon$-th cyclotomic extension; see, e.g., [1], Lemma 2.1(1)].}
Proof. We consider the splitting field $E$ of the degree-8 polynomial $f(t, X) = 7^3X^7(X + 7) - t(X^2 + X + 7)$ over $\mathbb{Q}(t)$. This has Galois group $G = PGL_2(7)$ over $\mathbb{Q}(t)$ (e.g., it is, up to multiplication of the variables by suitable constants, the special case $a = 0$ of the polynomial in [12, Theorem 5.1]). Furthermore, $E/\mathbb{Q}(t)$ is ramified exactly over $t \mapsto 0$, $t \mapsto \infty$ and one more rational point $t \mapsto t_0 := -7^{10}/(2^2 \cdot 3^4)$, with inertia group generator of cycle structure $(7, 1)$, $(6, 1^2)$ and $(2^3, 1^2)$ respectively. Following the above proofs, we manipulate $f$ in such a way that all ramification in specializations will be “decided” by the branch point of ramification index 2. We first find out about the residue extension at this branch point. Firstly, the decomposition group at this branch point needs to be contained in the centralizer of an element of cycle structure $(2^3, 1^2)$ in $PGL_2(7)$, which is of order 12. Thus the residue extension at $t \mapsto t_0$ is a Galois extension of group embedding into $C_6/I \cong S_3$, and from factorizing $f(t_0, X)$ (which is the product of a quadratic polynomial and the square of a cubic polynomial), we find that it is indeed an $S_3$-extension, with quadratic subextension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$. This happens to be the same quadratic extension as $\mathbb{Q}(\sqrt{t_0})/\mathbb{Q}$. Thus, setting $t(s) := 1/s^2$, the splitting field $E(s)$ of $f(t(s), X)$ over $\mathbb{Q}(s)$ is a $PGL_2(7)$-extension ramified exactly over $s \in \{0, \infty, \pm \sqrt{t_0}\}$ (with ramification index 3 at $s \mapsto 0$ due to Abhyankar’s lemma, since this place extends $t \mapsto \infty$ of ramification index 2), and now, the residue extension at $s \mapsto \pm \sqrt{1/t_0}$ is a $C_3$-extension of the base field $\mathbb{Q}(\sqrt{t_0})$. Pulling back further by setting $s(u) := u^3$, we obtain a $PGL_2(7)$-extension $E(u)/\mathbb{Q}(u)$ ramified only at the 6-th roots of $1/t_0$, as well as $u \mapsto \infty$ (and in particular, unramified at $u \mapsto 0$ due to Abhyankar’s lemma). Since the residue field $\mathbb{Q}(\sqrt{t_0})$ contains $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{-3})$, it still remains true that the residue extension of $E(u)/\mathbb{Q}(u)$ at any of these finite branch points is a $C_3$-extension. Theorem 3.2 then gives the following: There exists a finite set $S$ of primes such that, for any integral specialization $u \mapsto u_0 \in \mathbb{Z}$ and any prime $p$ not contained in $S$, if $p$ ramifies in $E(u)/\mathbb{Q}(u)$, then its inertia group must be generated by an involution of cycle type $(2^1, 1^2)$, and its decomposition group must be either $C_2$ or $C_2 \times C_3$. Since both these groups split in $PGL_2(7)$, the corresponding central embedding problem then has no local obstruction coming from any finite prime $p$ outside $S$. We now verify computationally that in fact the primes in the exceptional set $S$ pose no obstruction either. This is done by specializing $f(t(s(u)), X)$, which up to constant factor equals

$$F(u, X) = (7u^2)^3X^7(X + 7) - (X^2 + X + 7),$$

at odd integer values $u \mapsto u_0 \in 2\mathbb{Z} + 1$. Calculating the discriminant of $F(u, X)$ with respect to $X$ and using [11, Theorem 2.2], as indicated in Remark [11], one verifies that one may in fact take $S = \{2, 3, 7, \infty\}$. Firstly note that $F(u_0, X)$ mod 2 is separable for odd $u_0$, whence 2 is unramified in all such specializations and thus poses no problem. Neither does the infinite prime, since our $PGL_2(7)$-extensions are such that the quadratic subextension is imaginary, i.e., complex conjugation is given by an involution of cycle structure $(2^1, 1^2)$. For the remaining primes $p = 3$ and 7, it may be directly verified, aided by Magma, that all specializations which ramify at $p$ (in the case of $p = 7$, these are actually all specializations $u \mapsto u_0 \in 2\mathbb{Z} + 1$; in the case of $p = 3$, ramification happens only when $3|u_0$) have cyclic decomposition group generated by an involution of cycle type $(2^1, 1^2)$.\footnote{Note that, in order to strictly verify this claim, one of course need not do calculations for infinitely many specializations, since the behavior of the decomposition group is the same for all values $u_0$ which are sufficiently close to each other $p$-adically, by Kränsler’s lemma. Further tricks are available to ease the task, e.g., over $\mathbb{Q}(\sqrt{7})$, one may perform a change of variable $X \mapsto X/\sqrt{7}$ and consider the polynomial $7u^2F(u, X/\sqrt{7u}) = X^7(X + 7\sqrt{7u}) - (X^2 + \sqrt{7u}X + 49u^2)$, which, as already a low-precision calculation verifies, splits into distinct linear factors over $\mathbb{Q}(\sqrt{7})$.}

Note furthermore that, since no odd integer is a branch point of the $PGL_2(7)$-extension $E(u)/\mathbb{Q}(u)$, all specializations at such values are Galois extensions of $\mathbb{Q}$ with group a subgroup
of $\text{PSL}_2(7)$. Since the Galois group is generated by the set of all inertia subgroups, we obtain a subgroup of $\text{PSL}_2(7)$ generated by involutions of cycle type $(2^4 \cdot 1^2)$. Furthermore, the polynomial $F(1, X)$ is irreducible (of degree 8) modulo 2, whence the Galois group for all specializations at odd integers must contain an 8-cycle (namely, the Frobenius at 2)! One may now verify directly that $\text{PSL}_2(7)$ has no proper subgroup which is generated by involutions as above while also containing an 8-cycle. Hence, $\text{Gal}(E(u)/\mathbb{Q}) = \text{PSL}_2(7)$ without exception. Propositions 5.4 and 5.5 now yield that $(E(u))_{\text{ram}}/\mathbb{Q}$ embeds into an extension $L/\mathbb{Q}$ with group $\text{SL}_2(7), 2$, and if $F$ denotes the fixed field of $\text{SL}_2(7)$ in $L$, then $L/F$ can be chosen everywhere unramified. It remains to calculate the quadratic field $F$, which is just given by the square-root of the discriminant of $F(u_0, X)$ above. Computation with Magma confirms the shape claimed in the statement of the theorem.

\[ \square \]

**Remark 5.** A logical next step would be to try to realize more general central extensions of $\text{PSL}_2(7)$ as Galois groups of unramified extensions of quadratic number fields, using, e.g., Theorem 5.1. This is easy for the direct product $\text{SL}_2(7) \times C_2$. Indeed, the values $-7 \cdot (108 + 7^{10}t^6)$ featuring in the assertion of Theorem 5.1 are all strictly divisible by 7, and the factor $(108 + 7^{10}t^6)$ is not a square (due to being too close to another square). Hence, the extension $\mathbb{Q}(\sqrt{-7 \cdot (108 + 7^{10}t^6)}, \sqrt{-7})/\mathbb{Q}(\sqrt{-7}, \sqrt{-7})$ is an unramified quadratic extension (necessarily linearly disjoint from the $\text{SL}_2(7)$-extension constructed above, which has no quadratic subextensions). In comparison, the same question for the group $\text{SL}_2(7) \times C_3$ already seems challenging: quadratic number fields with class number divisible by 3 can be parameterized effectively, but requiring them to simultaneously have the shape of Theorem 5.1 leads to difficult diophantine conditions. E.g., it is easy to exhibit infinitely many quadratic number fields of the shape $\mathbb{Q}(\sqrt{-u(4u + 27)})$ with class number divisible by 3 (for a more general result, see [8, Main Theorem]). Demanding those to simultaneously fall into the shape of Theorem 5.1 amounts to finding (suitable) integral points on the conic $U(4U + 27) - 7DV^2 = 0$, with $D = 108 + 7^{10}t^6$ for some odd integer $t$, as in the Theorem. I do not know whether such points exist for infinitely many $D$ of the prescribed shape.

5.2. The case $G = 2.A_7$.

**Proof.** We consider the splitting field $E/\mathbb{Q}(t)$ of $f(t, X) = X^7 - 7t(X - 1)$. This is well-known to be $\mathbb{Q}$-regular with Galois group $S_7$, and inertia groups generated by a 7-cycle (at $t \rightarrow 0$), a 6-cycle (at $t \rightarrow \infty$) and a transposition (at the only further branch point $t_3$); indeed, this is a special case of the family $X^n - t(X - 1)$ corresponding to a rigid class triple in $S_n$ for all $n \geq 3$ (e.g., 12, Chapter I, Prop. 5.2); our choice to replace $t$ by $7t$ is merely to make $t_3$ a rational square $t_3 = \frac{7^2}{u}$ and thus have $\mathbb{Q}(\sqrt{t_3}) = \mathbb{Q}$ as in the proof of Theorem 1.2. Note that the normalizers of the cyclic groups generated by the 7- and the 6-cycle are the same as in $\text{PSL}_2(7)$, whence much of the argument from that case carries over. The difference is that the centralizer of the transposition is larger than the one of the involution dealt with in the case $G = \text{SL}_2(7)$, namely isomorphic to $\langle (1, 2), \text{Sym}(\{3, 4, 5, 6, 7\}) \rangle \cong C_2 \times S_5$. We need to exclude local obstructions to the embedding problem induced by $2.S_7 \hookrightarrow S_7$ (where $2.S_7$ denotes the double cover of $S_7$ in which the transpositions - as well as the triple transpositions - are split), for primes whose inertia group in an $S_7$-extension is generated by a transposition. Obviously there is no obstruction if the Frobenius element (inside $S_5$) is of odd order; furthermore, note that if the decomposition group at $p$ is conjugate in $S_7$ to $\langle (1, 2), (3, 4) \rangle (5, 6)$ (with inertia group generated by $(1, 2)$), then there is no local obstruction at $p$ either, since that group lifts to $C_2 \times C_4 \leq 2.S_7$, i.e., the local embedding problem at $p$ is solvable (and without ramification in the kernel) via extending the unramified quadratic extension of $\mathbb{Q}_p$ to the degree 4 one. In total, there is no local obstruction as long as the Frobenius is contained in $\text{Alt}(\{3, 4, 5, 6, 7\}) \cong A_5$. Now we are in a situation
entirely analogous to the case $G = SL_2(7)$; namely, let $Q(\sqrt{\beta})/Q$ be the quadratic subextension of the residue extension at the branch point $t_3^8$. Set $\beta = s^2$, and proceed as in the proof of Theorem 1.2 and the case $G = SL_2(7)$ of Theorem 1.1. □

Remark 6. Turning the above proof into an explicit family of quadratic number fields possessing unramified $2.A_7$-extensions works just like in the previous section. We leave this to the interested reader.

Acknowledgement: I would like to thank Kwang-Seob Kim for many helpful discussions.

References

[1] N.C. Ankeny, S. Chowla, On the divisibility of the class numbers of quadratic fields. Pacific J. Math. 5 (3) (1955), 321–324.
[2] L. Bary-Soroker, T. Schlank, Sieves and the minimal ramification problem. J. Inst. Math. Jussieu 19 (3) (2020), 919–945.
[3] S. Beckmann, On extensions of number fields obtained by specializing branched coverings. J. Reine Angew. Math. 419 (1991) 27–53.
[4] K. Chakraborty, A. Hoquie, Y. Kishi, P.P. Pandey, Divisibility of the class numbers of imaginary quadratic fields. J. Number Theory 185 (2018), 339–348.
[5] D. Gorenstein, J.H. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. J. J. Algebra 2 (1965), 85–151.
[6] K. Kedlaya, A construction of polynomials with squarefree discriminants. Proc. Amer. Math. Soc. 140 (9) (2012), 3025–3033.
[7] K.-S. Kim, J. König, On Galois extensions with prescribed decomposition groups. J. Number Theory 220 (2021), 266–294.
[8] Y. Kishi, K. Miyake, Parametrization of the quadratic fields whose class numbers are divisible by three. J. Number Theory 80 (2000), 209–217.
[9] J. König, F. Legrand, D. Neftin, On the local behavior of specializations of function field extensions. Int. Math. Res. Not. IMRN Vol. 2019 (2019), 2951–2980.
[10] J. König, D. Neftin, J. Sonn, Unramified extensions over low degree number fields. J. Number Theory 212 (2020), 72–87.
[11] J. König, D. Neftin, The local dimension of a finite group over a number field. Preprint (2020). https://arxiv.org/abs/2007.05383
[12] G. Malle, Multi-parameter polynomials with given Galois group. J. Symbol. Comput. 30 (2000), 717–731.
[13] G. Malle, B.H. Matzat, Inverse Galois Theory, 2nd edition, Springer, 2018.
[14] J.-F. Mestre, Extensions régulières de $Q(T)$ de groupe de Galois $A_n$. J. Algebra 131 (1990), 483–495.
[15] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields. Springer Verlag, Berlin, 2000.
[16] M. Schacher, J. Sonn, Double covers of the symmetric groups as Galois groups over number fields. J. Algebra 116 (1) (1988), 243–250.
[17] J.-P. Serre, Topics In Galois Theory. Research Notes in Math., vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992.
[18] J.-P. Serre, Modular forms of weight one and Galois representations, Algebraic number fields: $L$-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975) (A.

---

One verifies quickly that this residue extension is indeed an $S_5$-extension, and hence, has a unique quadratic subextension, which in this concrete case equals $Q(\sqrt{3})$. 
19] J.-P. Serre, *L’invariant de Witt de la forme $\text{Tr}(x^2)$*. Comm. Math. Helv. 59 (1984), 651–676.

[20] N. Vila, *On central extensions of $A_n$ as Galois groups over $\mathbb{Q}$*. Arch. Math. 44 (1985), 424–437.

[21] M. Matchett Wood, *Nonabelian Cohen-Lenstra moments*. Duke Math. J. 168(3) (2019), 377–427.

[22] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*. Osaka J. Math. 7 (1) (1970), 57–76.

[23] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors*. J. Théor. Nombres Bord. 9 (2) (1997), 405–448.

Korea National University of Education, Department of Mathematics Education, 28173 Cheongju, South Korea