Journal of Number Theory 129 (2009) 418–427

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Galois extensions ramified only at one prime

Jing Long Hoelscher

University of Arizona, Department of Mathematics, 617 N. Santa Rita Ave., Tucson, AZ 85721, United States

ARTICLE INFO

Article history:
Received 12 December 2007
Revised 31 May 2008
Available online 16 September 2008
Communicated by David Goss

ABSTRACT

This paper gives some restrictions on finite groups that can occur as Galois groups of extensions over $\mathbb{Q}$ and over $\mathbb{F}_q(t)$ ramified only at one finite prime. Over $\mathbb{Q}$, we strengthen results of Jensen and Yui about dihedral extensions and rule out some non-solvable groups. Over $\mathbb{F}_q(t)$ restrictions are given for symmetric groups and dihedral groups to occur as tamely ramified extension over $\mathbb{F}_q(t)$ ramified only at one prime.

0. Introduction

This paper studies Galois groups with prescribed ramification in both the function field and number field cases. We are particularly interested in the case with a single finite ramified place.

In the geometric case, we are concerned with curves over a field k of characteristic $p > 0$. Let X be a smooth connected projective curve of genus g over k and let $S = \{\xi_1, \ldots, \xi_n\}$ be a finite set of $n > 0$ closed points on X. Then $U = X - S$ is an open subset of X. Define $\pi_A(U)$ to be the set of finite groups that occur as Galois groups over X with ramifications only at S, and $\pi_A^t(U)$ the subset of $\pi_A(U)$ corresponding to covers in which only tame ramifications occur. In the case k is algebraically closed, Corollary 2.12 of Chapter XIII in [Gro] implies that: if G is a Galois cover of X ramified only at S, then $G/p(G)$ has $2g + n - 1$ generators. Here $p(G)$ denotes the quasi-p part of G, i.e. the subgroup of G generated by elements of order a power of p. This statement can be carried over to the case where k is a finite field $\mathbb{F}_q$ of order q, a power of p, if we restrict to regular covers Y/X, i.e. where k is algebraically closed in the function field of Y. If $X/\mathbb{F}_q(t)$ is a tame regular cover with Galois group G, then G has at most $2g + n - 1$ generators. Here we count the number n of ramified primes according to their degree, i.e. n is the degree of S as a divisor over $\mathbb{F}_q$. Proposition 3.1, of Section 3 below, gives further restrictions on $\pi_A^t(\mathbb{A}^1_{\mathbb{F}_q} - (f))$, where (f) is the divisor of zeroes of an irreducible $f \in \mathbb{F}_q[t]$. The following two corollaries of Proposition 3.1 show that dihedral groups and symmetric groups tend to not occur in $\pi_A^t(\mathbb{P}^1_{\mathbb{F}_q} - (f))$.

E-mail address: jlong@math.arizona.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.06.006

Corollary A. *For any integer $k \geqslant 1$ and irreducible $f \in \mathbb{F}_q[t]$, the dihedral group $D_{4k} \notin \pi_A^t(\mathbb{P}^1_{\mathbb{F}_q} - (f))$. If the degree $d = \deg(f)$ is odd, we also have $D_{4k+2} \notin \pi_A^t(\mathbb{P}^1_{\mathbb{F}_q} - (f))$.*

Corollary B. *If $2 \mid q$ and $n > 2$, the symmetric group $S_n \notin \pi_A^t(\mathbb{P}^1_{\mathbb{F}_q} - (f))$ for each irreducible $f \in \mathbb{F}_q[t]$. If $2 \nmid q$ and the prime f is of odd degree, then the same conclusion holds.*

In the arithmetic case, we consider Galois extensions over $\mathbb{Q}$. Denote $U_n = \operatorname{Spec}(\mathbb{Z}[\frac{1}{n}])$, an open subset of $\operatorname{Spec}(\mathbb{Z})$. Then $\pi_A(U_n)$ is the set of finite groups that occur as Galois groups over $\mathbb{Q}$ ramified only at primes dividing n. Motivated by Corollary 2.12 in Chapter XIII of [Gro] and the analogy between function fields and number fields, Harbater posed a corresponding conjecture in [Ha]:

Conjecture *(Harbater, 1994). There is a constant C such that for every positive square free integer n, every group in $\pi_A^t(U_n)$ has a generating set with at most $\log n + C$ elements.*

Consequences of Theorem 1.1 in Section 1 give some evidence for this conjecture and also generalizes Proposition 2.17 in [Ha] assuming the Galois group is solvable. In addition, this theorem also gives the following corollary, which gives a complement of a result of Jensen and Yui in [JY]. They showed that any dihedral extension with Galois group D_{2n} over $\mathbb{Q}$ ramified only at one regular prime p, with $p \equiv 1 \pmod 4$, has degree prime to p.

Corollary C. *Suppose $p \equiv 1 \pmod 4$ is a regular prime such that the class number of $\mathbb{Q}(\sqrt{p})$ is 1. Then there are no non-abelian dihedral groups in $\pi_A(U_p)$.*

Example. In the range $2 \leqslant p \leqslant 100$, the primes $p = 5, 13, 17, 29, 41, 53, 61, 73, 89, 97$ satisfy the conditions in Corollary C. So there are no non-abelian dihedral groups which can occur as Galois groups over $\mathbb{Q}$ ramified only at such p and possibly ∞.

Applying Theorem 1.1 to the prime $p = 3$ gives the following two corollaries, which are also related to results for the prime 2 (Theorems 2.20 and 2.23) in [Ha].

Corollary D. *If G is a solvable group in $\pi_A(U_p)$, where $p = 3$, then either G is cyclic, or $G/p(G) \cong \mathbb{Z}/2$, or G has a cyclic quotient of order 27.*

Corollary E. *Suppose $K/\mathbb{Q}$ is a Galois extension with non-trivial Galois group G, ramified only at the prime $p = 3$ and possibly at ∞, with ramification index e. Then $9 \mid e$ unless $G/p(G) \cong \mathbb{Z}/2$ or $G \cong \mathbb{Z}/3$.*

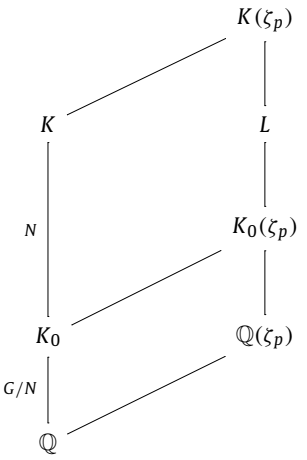
In Section 2, we deal with the non-solvable case. We use the upper bound and lower bound of the discriminant to rule out some non-solvable groups. The main result is the following, which generalizes a result for $p = 2$ in [Ha].

Proposition. *Let $2 \leqslant p < 23$ be a prime number. If $G \in \pi_A(U_p)$ and $|G| \leqslant 300$, then G is solvable.*

1. Solvable extensions over $\mathbb{Q}$

In this section, we will give some conditions on solvable groups that can occur as Galois groups over $\mathbb{Q}$ ramified only at one finite prime. A consequence of Harbater's Conjecture would be that if $G \in \pi_A(U_p)$ for some prime p, without assuming the ramification to be tame, then $G/p(G)$ is generated by at most $\log(p) + C$ elements. Thus if p is very small, we expect G to be very close to being a quasi-p group. In fact, this holds when $p < 23$ as seen in Corollary 2.7 of [Ha], i.e. $G/p(G)$ is cyclic of order dividing $p - 1$. The following theorem is a generalization of this idea and of Proposition 2.17 in [Ha], but with an extra assumption on solvability.

Theorem 1.1. *Let K be a finite Galois extension of $\mathbb{Q}$ ramified only at a single finite prime $p > 2$, with the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ solvable. Let $K_0/\mathbb{Q}$ be an intermediate abelian extension of $K/\mathbb{Q}$. Let $N = \mathrm{Gal}(K/K_0)$ and $p(N)$ be the quasi-p part of N.*



Then either

(i) $N/p(N) \subset \mathbb{Z}/(p-1)$; *or*
(ii) *there is a non-trivial abelian unramified sub-extension $L/K_0(\zeta_p)$ of $K(\zeta_p)/K_0(\zeta_p)$ of degree prime to p with L Galois over $\mathbb{Q}$.*

We will first give some corollaries, then prove a lemma and a proposition that will be used in the proof of Theorem 1.1, given at the end of this section.

Remarks 1.2.

(I) If we let $K_0 = \mathbb{Q}$ and $p < 23$, Theorem 1.1 is just Corollary 2.7 in [Ha] in the solvable case.
(II) In fact we will show in the proof of Theorem 1.1 that the condition (i) can be replaced by the condition $K/\mathbb{Q}$ is a quasi-p extension of a totally ramified extension.

As a direct consequence of Theorem 1.1, we have:

Corollary 1.3. *Let $K/\mathbb{Q}$ be a solvable Galois extension ramified only at a prime p and possibly at ∞. Suppose $K_0 \subset \mathbb{Q}(\zeta_{p^n})$ is a sub-extension of $K/\mathbb{Q}$ with Galois group $\mathrm{Gal}(K/K_0) = G$ and the class number of $K_0(\zeta_p)$ is 1. Then $G/p(G)$ is cyclic of order dividing $p-1$.*

Proof. Apply Theorem 1.1 to the sub-extension $K_0/\mathbb{Q}$. Since the class number of $K_0(\zeta_p)$ is 1, the condition (ii) in Theorem 1.1 does not hold. So condition (i) holds, i.e. $G/p(G)$ is cyclic of order dividing $p-1$. □

Example. We can apply Corollary 1.3 to the case $K_0 = \mathbb{Q}(\zeta_{p^n})$, where the class number of K_0 is 1, i.e. $p^n = 4, 8, 16, 32, 3, 9, 27, 5, 25, 7, 11, 13, 17, 19$. Let G be the Galois group of any solvable extension K/K_0, which is Galois over $\mathbb{Q}$ and ramified at only p and ∞ over $\mathbb{Q}$. Then $G/p(G)$ is cyclic of order dividing $p-1$. Furthermore,

1. If $p \nmid |G|$, then $G \subset \mathbb{Z}/(p-1)$.
2. When $K_0 = \mathbb{Q}(\zeta_4), \mathbb{Q}(\zeta_8), \mathbb{Q}(\zeta_{16})$, the Galois group G of K/K_0 has to be quasi-2.

Using Theorem 1.1, we can prove Corollary C.

Proof of Corollary C. Suppose that $K/\mathbb{Q}$ is a Galois extension with group D_{2n} of order $2n$, ramified only at a finite prime p and possibly at ∞. Denote by K_0 the fixed field of the cyclic subgroup $\mathbb{Z}/n < D_{2n}$. By Theorem 1.2.2 in [JY], we know n is not divisible by p. Now apply Theorem 1.1. By the assumption the class number of K_0 is 1, we know that the condition (ii) in Theorem 1.1 fails. By the second remark above we have $K/\mathbb{Q}$ is totally ramified, since p does not divide the order of D_{2n}. So $\mathrm{Gal}(K/\mathbb{Q}) \cong P \rtimes C$, where P is a p-group and C is a cyclic group. We know P has to be trivial, again since $p \nmid 2n$. Thus $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic. □

Lemma 1.4. *Under the hypotheses of Theorem* 1.1*, if K_0 is a maximal p-power Galois sub-extension of $K/\mathbb{Q}$, then the condition* (i) *can be replaced by the condition that either G is a cyclic p-group or $N/p(N)$ is a non-trivial subgroup of $\mathbb{Z}/(p-1)$.*

Proof. It suffices to show that if N is a quasi-p group, then G is a cyclic p-group. So assume G is not a cyclic group (in particular G is non-trivial). The Galois group $\mathrm{Gal}(K_0/\mathbb{Q})$ is cyclic, say of order p^n for some n, since any finite p-group in $\pi_A(U_p)$ is cyclic (see Theorem 2.11 in [Ha]). By Class Field Theory $K_0/\mathbb{Q}$ is the unique cyclic sub-extension of degree p^n in $\mathbb{Q}(\zeta_{p^{n+1}})$ since $p > 2$. If K_0' is another maximal p-power sub-extension of $K/\mathbb{Q}$, then $K_0' = K_0$ by the same argument. So K_0 is the unique maximal p-power sub-extension of $K/\mathbb{Q}$. Denote by N the Galois group $\mathrm{Gal}(K/K_0)$. Then N is normal in G and it is the minimal subgroup of G with index a power of p, since it corresponds to the unique maximal p-power sub-extension K_0. We know N is non-trivial, since G is not a p-group by assumption. Now G is a non-trivial solvable group, so G has a normal subgroup $\bar{N} \subset N$ such that $N/\bar{N}$ is of the form $(\mathbb{Z}/q)^n$ for some prime q and some integer $n \geqslant 1$. We know $q \neq p$ from the minimality of N. So N is not a quasi-p group since every p-subgroup of N is contained in the proper subgroup $\bar{N}$. □

The above lemma gives evidence for the conjecture in the introduction. Next we will apply Lemma 1.4 to the prime 3 to get Corollary D and consequently Corollary E.

Proof of Corollary D. Let $K/\mathbb{Q}$ be a solvable Galois extension ramified only at $p = 3$ with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Take $K_0/\mathbb{Q}$ to be a maximal p-power Galois sub-extension of $K/\mathbb{Q}$. The same argument as in Lemma 1.4 shows that the Galois group $\mathrm{Gal}(K_0/\mathbb{Q})$ is cyclic and K_0 is the unique maximal p-power Galois sub-extension of $K/\mathbb{Q}$. If G is not cyclic, then N is not quasi-p by Lemma 1.4; hence $N/p(N)$ is non-trivial. Now suppose G is not cyclic and $G/p(G) \ncong \mathbb{Z}/2$ and apply Theorem 1.1. Since the condition (i) in the theorem does not hold, the condition (ii) has to hold; thus the class group of $K_0(\zeta_p)$ is non-trivial. So $K_0(\zeta_p)$ contains the cyclotomic field $\mathbb{Q}(\zeta_{81})$, thus $|\mathrm{Gal}(K_0/\mathbb{Q})| \geqslant 27$, i.e. G has a cyclic quotient of order 27. □

Example. Let G be a Galois group of any Galois extension over $\mathbb{Q}$ ramified only at 3 and possibly ∞.

1. If $2 \nmid |G|$ and $27 \nmid |G|$, then G is a cyclic group.
2. If G is a solvable quasi-3 group and $27 \nmid |G|$, then G is a cyclic group. For example the quasi-3 group $\mathbb{Z}/l \rtimes \mathbb{Z}/3 \notin \pi_A(U_3)$, where l is a prime such that $3 \mid l-1$.

Proof of Corollary E. If G is solvable, by Corollary D we know $27 \mid e$ unless $G/p(G) \cong \mathbb{Z}/2$ or G is cyclic. In the case G is cyclic, we know by class field theory $K/\mathbb{Q}$ is totally ramified, so $e = n = |G|$, i.e. either $e = n = 3$ or $9 \mid e$. If G is non-solvable, it has order $\geqslant 60$. On the one hand, we know $|\mathfrak{d}_{K/\mathbb{Q}}|^{\frac{1}{n}} \geqslant 12.23$ from the discriminant table (p. 400 in [Od]) for extensions of degree $\leqslant 60$; on the other hand, considering the discriminant upper bound (Theorem 2.6, Chapter III, [Ne]), we have $|\mathfrak{d}_{K/\mathbb{Q}}|^{\frac{1}{n}} \leqslant 3^{1+v_3(e)-\frac{1}{e}} < 3^{1+v_3(e)}$. Combining these two inequalities gives $12.23 \leqslant |\mathfrak{d}_{K/\mathbb{Q}}|^{\frac{1}{n}} < 3^{1+v_3(e)}$, thus $v_3(e) \geqslant 2$ and $9 \mid e$. □

Remark. Corollary E does not assume the solvability of $\mathrm{Gal}(K/\mathbb{Q})$.

For the proof of Theorem 1.1, we first need a lemma and a proposition.

Lemma 1.5. *Let $G = P \rtimes \mathbb{Z}/(l_1 l_2)$ be a semi-direct product of a p-group P by a cyclic group $\mathbb{Z}/l_1 l_2$, with p, l_2 distinct primes and $p \nmid l_1$. Denote by s the highest power of l_2 which divides l_1, i.e. $l_2^s \parallel l_1$. Suppose G has a normal subgroup $N \cong \mathbb{Z}/l_2^{s+1}$ with the quotient group $G/N \cong \mathbb{Z}/(l_1 l_2^{-s} p^m)$. Then $G = \mathbb{Z}/p^m \times \mathbb{Z}/(l_1 l_2)$.*

Proof. Let $\theta : \mathbb{Z}/(l_1 l_2) \longrightarrow \mathrm{Aut}(P)$ be the homomorphism corresponding to the semi-direct product $G = P \rtimes \mathbb{Z}/(l_1 l_2)$, which sends an element $a \in \mathbb{Z}/(l_1 l_2)$ to an automorphism $\theta_a \in \mathrm{Aut}(P)$. Since the l_2-Sylow subgroup N is normal in G, it is the unique l_2-Sylow subgroup by Sylow's theorem. Identify $\mathbb{Z}/l_2^{s+1}$ with the subset of $G = P \rtimes \mathbb{Z}/(l_1 l_2) \cong P \rtimes (\mathbb{Z}/l_1 l_2^{-s} \times \mathbb{Z}/l_2^{s+1})$, consisting of all pairs of the form $(1, b)$ with $b \in \mathbb{Z}/l_2^{s+1}$. We claim $\mathbb{Z}/l_2^{s+1}$ acts trivially on P in G. Now for any $(k, a) \in P \rtimes \mathbb{Z}/(l_1 l_2)$, we have

$$\begin{aligned}(k,a)(1,b)(k,a)^{-1} &= (k, ab)\big(\big(\theta_{a^{-1}}(k)\big)^{-1}, a^{-1}\big)\\ &= \big(k\theta_{ab}\big(\big(\theta_{a^{-1}}(k)\big)^{-1}\big), b\big)\\ &= \big(k\theta_{ba}\big(\theta_{a^{-1}}\big(k^{-1}\big)\big), b\big)\\ &= \big(k\theta_b\big(k^{-1}\big), b\big).\end{aligned}$$

Since $\mathbb{Z}/l_2^{s+1} = N \lhd G$ by the assumption, we know $(k, a)(1, b)(k, a)^{-1}$ is of the form $(1, b)$. So $\theta_b(k^{-1}) = k^{-1}, \forall k \in \mathbb{Z}/p^m$, i.e. θ_b is trivial for all $b \in \mathbb{Z}/l_2^{s+1} = N$.

Next we will show the isomorphism

$$P \rtimes_\theta \big(\mathbb{Z}/\big(l_1 l_2^{-s}\big) \times \mathbb{Z}/l_2^{s+1}\big) \cong \big(P \rtimes_{\theta'} \mathbb{Z}/\big(l_1 l_2^{-s}\big)\big) \times \mathbb{Z}/l_2^{s+1} \tag{1.6}$$

where the homomorphism $\theta' : \mathbb{Z}/l_1 l_2^{-s} \longrightarrow \mathrm{Aut}(P)$ is the restriction of θ onto $\mathbb{Z}/(l_1 l_2^{-s})$. On the one hand the left-hand side and right-hand side of (1.6) are the same as underlying sets; on the other hand we consider the binary operation in each group. Pick any two elements $(a_1, b_1, c_1), (a_2, b_2, c_2) \in \mathbb{Z}/p^m \rtimes (\mathbb{Z}/(l_1 l_2^{-s}) \times \mathbb{Z}/l_2^{s+1})$. We have

$$\begin{aligned}(a_1,b_1,c_1)(a_2,b_2,c_2) &= \big(a_1, (b_1, c_1)\big)\big(a_2, (b_2, c_2)\big)\\ &= \big(a_1\theta_{(b_1,c_1)}(a_2), (b_1 b_2, c_1 c_2)\big)\\ &= \big(a_1\theta_{(b_1,c_1)}(a_2), b_1 b_2, c_1 c_2\big).\end{aligned}$$

And if we pick any two elements $(a_1, b_1, c_1), (a_2, b_2, c_2) \in (\mathbb{Z}/p^m \rtimes \mathbb{Z}/l_1 l_2^{-s}) \times \mathbb{Z}/l_2^{s+1}$,

$$\begin{aligned}(a_1,b_1,c_1)(a_2,b_2,c_2) &= \big((a_1, b_1)(a_2, b_2), c_1 c_2\big)\\ &= \big(\big(a_1\theta'_{b_1}(a_2), b_1 b_2\big), c_1 c_2\big)\\ &= \big(a_1\theta'_{b_1}(a_2), b_1 b_2, c_1 c_2\big).\end{aligned}$$

Since $\mathbb{Z}/l_2^{s+1}$ acts trivially on P, we know $\theta_{(b_1,c_1)}(a_2) = \theta'_{b_1}(a_2)$. So the left-hand side and right-hand side of (1.6) have the same binary operations. We conclude isomorphism (1.6). Now we consider the quotient group $G/(\mathbb{Z}/l_2^{s+1})$. By the assumption it is isomorphic to $\mathbb{Z}/(l_1 l_2^{-s} p^m)$. So by isomorphism (1.6) we have

$$\mathbb{Z}/\big(l_1 l_2^{-s} p^m\big) \cong G/\big(\mathbb{Z}/l_2^{s+1}\big) \cong P \rtimes_{\theta'} \mathbb{Z}/l_1 l_2^{-s}.$$

So $G \cong (P \rtimes_{\theta'} \mathbb{Z}/(l_1 l_2^{-s})) \times \mathbb{Z}/l_2^{s+1} \cong \mathbb{Z}/(l_1 l_2^{-s} p^m) \times \mathbb{Z}/(l_2^{s+1}) \cong \mathbb{Z}/p^m \times \mathbb{Z}/(l_1 l_2)$. □

Proposition 1.7. *Let K be a finite solvable Galois extension of $\mathbb{Q}$ ramified only over one finite prime $p > 2$, and let $M/\mathbb{Q}$ be a proper abelian sub-extension of $K/\mathbb{Q}$ such that $p \nmid |\mathrm{Gal}(K/M)|$. Assume there is no non-trivial abelian unramified extension of $M(\zeta_p)$ of degree prime to p which is contained in $K(\zeta_p)$ and is Galois over $\mathbb{Q}$. Then there is a proper sub-extension M_1/M in K/M such that $M_1/\mathbb{Q}$ is abelian.*

Proof. Since $\mathrm{Gal}(M/\mathbb{Q})$ is abelian and ramified only at p, we know by class field theory that $\mathrm{Gal}(M/\mathbb{Q})$ is a subgroup of $\mathbb{Z}/p^m \times \mathbb{Z}/(p-1)$. Write $\mathrm{Gal}(M/\mathbb{Q}) = \mathbb{Z}/(p^m l_1)$ with $l_1 \mid p-1$. Let $N = \mathrm{Gal}(K/M)$. Since N is solvable, being a normal subgroup of the solvable group G, there is a normal subgroup N_0 of N such that $N/N_0 \cong \mathbb{Z}/l_2$, for some prime l_2 such that $(l_2, p) = 1$. Let M_0 be the fixed field of N_0 in K/M, so $\mathrm{Gal}(M_0/M) \cong \mathbb{Z}/l_2$. Let M_1 be the Galois closure of M_0 over $\mathbb{Q}$, so $\mathrm{Gal}(M_1/M)$ is a minimal normal subgroup of a solvable group $\mathrm{Gal}(M_1/\mathbb{Q})$. From p. 85 of [Rot], we know that $\mathrm{Gal}(M_1/M) \cong (\mathbb{Z}/l_2)^t$ for some $t \geqslant 1$. So the Galois group $\mathrm{Gal}(M_1/M_0) \cong (\mathbb{Z}/l_2)^{t-1}$.

$$K \text{ ——— } M_1 = (K^{N_0})^{\mathrm{Gal}} \xrightarrow{(\mathbb{Z}/l_2)^{t-1}} M_0 = K^{N_0} \xrightarrow{\mathbb{Z}/l_2} M \xrightarrow{\mathbb{Z}/(l_1 p^m)} \mathbb{Q}.$$

Pick a prime $\mathfrak{p}$ of M_1 over the prime p of $\mathbb{Q}$, let $I_0 \subset \mathrm{Gal}(M_1/M)$ be the inertia group of $\mathfrak{p}$ in M_1 over M. Since $\mathrm{Gal}(M_1/M) \cong (\mathbb{Z}/l_2)^t$ is abelian, its subgroup I_0 is normal and the quotient by I_0 is abelian. So the fixed field $M_{1,0} = M_1^{I_0}$ of I_0 in M_1/M is unramified over M at the prime $\mathfrak{p} \cap \mathcal{O}_{M_{1,0}}$, thus $M_{1,0}$ is an unramified extension of M contained in M_1. Let $\bar{M}_{1,0}$ be the Galois closure of $M_{1,0}$ over $\mathbb{Q}$. So $\bar{M}_{1,0}$ is contained in M_1 and unramified over M, being the composite of unramified extensions (the conjugates of $M_{1,0}$) of M. And $\bar{M}_{1,0}$ is abelian over M since it is contained in M_1. The extensions $\bar{M}_{1,0}/M$ and $M(\zeta_p)/M$ are disjoint since $\bar{M}_{1,0}/M$ is unramified at p and $M(\zeta_p)/M$ is totally ramified at p. Therefore if $\bar{M}_{1,0}/M$ is a non-trivial extension, $\bar{M}_{1,0}(\zeta_p)/M(\zeta_p)$ is also non-trivial. Also we know $M(\zeta_p) = \mathbb{Q}(\zeta_{p^{m+1}})$ since $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathbb{Z}/(l_1 p^m)$. So $\bar{M}_{1,0}(\zeta_p)$ is a non-trivial abelian unramified extension of $\mathbb{Q}(\zeta_{p^{m+1}})$ of degree prime to p such that $\bar{M}_{1,0}(\zeta_p) \subset K(\zeta_p)$ and $\bar{M}_{1,0}$ is Galois over $\mathbb{Q}$, contrary to the assumption.

$$K \supset M_1 \supset \bar{M}_{1,0} = M_{1,0}^{\mathrm{Gal}} \supset M_{1,0} = M_1^{I_0} \supset M \supset \mathbb{Q}.$$

So actually $\bar{M}_{1,0} = M$, and so $I_0 = \mathrm{Gal}(M_1/M) \cong (\mathbb{Z}/l_2)^t$. But the inertia group I_0 is cyclic (see Corollary 4, p. 68 of [Se]), because M_1 is at most tamely ramified at $\mathfrak{p}$ over M as the degree of the extension M_1/M is prime to p. So $t = 1$, and the field M_1 is totally ramified over M at $\mathfrak{p}$ with $\mathrm{Gal}(M_1/M) \cong \mathbb{Z}/l_2$. It follows M_1 is totally ramified over $\mathbb{Q}$ at the prime p, since $M/\mathbb{Q}$ is abelian thus totally ramified at p. So $\mathrm{Gal}(M_1/\mathbb{Q})$ is isomorphic to the inertia group $I \cong P \rtimes C$ of M_1 over $\mathbb{Q}$ at $\mathfrak{p}$, where P is a p-group and C a cyclic group of order prime to p. So C is a cyclic group of order $l_1 l_2$, thus $I \cong \mathbb{Z}/p^m \rtimes \mathbb{Z}/l_1 l_2$ with l_1, l_2 relatively prime to p. On the other hand, let l_2^s be the highest power of l_2 which divides l_1, so $s \geqslant 0$. Consider the invariant field $M^{\mathbb{Z}/l_2^s}$ of $\mathbb{Z}/l_2^s \subset \mathrm{Gal}(M/\mathbb{Q})$ in M.

$$K \text{ ——— } M_1 \xrightarrow{I_0 = \mathbb{Z}/l_2} M \xrightarrow{\mathbb{Z}/(l_2^s)} M^{\mathbb{Z}/l_2^s} \xrightarrow{\mathbb{Z}/(l_1 l_2^{-s} p^m)} \mathbb{Q}.$$

It is Galois over $\mathbb{Q}$ since $M/\mathbb{Q}$ is abelian, so $\mathrm{Gal}(M_1/M^{\mathbb{Z}/l_2^s}) \lhd \mathrm{Gal}(M_1/\mathbb{Q})$. Since $M_1/M^{\mathbb{Z}/l_2^s}$ is totally ramified, and tamely ramified, $\mathrm{Gal}(M_1/M^{\mathbb{Z}/l_2^s})$ is a cyclic group. So $\mathrm{Gal}(M_1/M^{\mathbb{Z}/l_2^s}) \cong \mathbb{Z}/l_2^{s+1}$, and the quotient group $I/(\mathbb{Z}/l_2^{s+1}) \cong \mathbb{Z}/(l_1 l_2^{-s} p^m)$. It follows from the Lemma 1.5 that $I \cong \mathbb{Z}/(p^m) \times \mathbb{Z}/l_1 l_2$. So $M_1/\mathbb{Q}$ is abelian and $M_1 \neq M$. □

Now we can give the proof for Theorem 1.1:

Proof of Theorem 1.1. The quasi-p part $p(N)$ of N is normal in G, since it is characteristic in the normal subgroup $N \lhd G$. Replacing G and N by $G/p(N)$ and $N/p(N)$ respectively, we may assume N

has degree prime to p. We will show either K/K_0 is cyclic of order dividing $p-1$, or (ii) holds. If $K/\mathbb{Q}$ is abelian, then K is inside some cyclotomic field $\mathbb{Q}(\zeta_{p^n})$ and N is a subgroup of $\mathbb{Z}/p^{n-1} \times \mathbb{Z}/(p-1)$ and of order prime to p, thus N is cyclic of order dividing $p-1$. Now we may assume $K_0 \neq K$ and $K/\mathbb{Q}$ is non-abelian.

First suppose that K/K_0 is totally ramified. Then $K/\mathbb{Q}$ is totally ramified, since $K_0/\mathbb{Q}$ is totally ramified at p, so $G \cong P \rtimes C$ with P a p-group and C a subgroup of $\mathbb{Z}/(p-1)$. Since $K_0/\mathbb{Q}$ is Galois, $N \lhd G$. So $N \subset C$ and is cyclic of order dividing $p-1$.

Otherwise, K/K_0 is not totally ramified. Assume (ii) does not hold. Let M be the fixed field of $G/[G,G]$ in $K/\mathbb{Q}$. Since G is solvable, we have $K \neq M$ and $M/\mathbb{Q}$ is the maximal abelian sub-extension in $K/\mathbb{Q}$. We now apply Proposition 1.7. So there is a subfield $M_1 \neq M$ in K/M such that $M_1/\mathbb{Q}$ is abelian, contradicting the maximality of M.

We now justify Part II of Remarks 1.2. After replacing G and N by $G/p(N)$ and $N/p(N)$ respectively, it suffices to show K/K_0 is totally ramified since $K_0/\mathbb{Q}$ is abelian thus totally ramified by class field theory. If K/K_0 is not totally ramified, the condition (ii) holds by above. □

2. Non-solvable extensions over $\mathbb{Q}$

In this section, we will prove the proposition in the introduction. We will start by considering non-abelian simple groups, which form an extreme sub-class of the non-solvable groups.

Lemma 2.1. *Let $2 \leqslant p < 23$ be a prime, and $G \in \pi_A(U_p)$ with G non-abelian. Then $p \mid |G|$; furthermore, if G is simple, then G is a quasi-p group.*

Proof. If $p \nmid |G|$, then the quasi-p part $p(G)$ of G is trivial since it is generated by all p-Sylow subgroups of G. By Corollary 2.7 in [Ha], we know $G = G/p(G)$ is cyclic of order dividing $p-1$. Contradiction; thus $p \mid |G|$. Now if G is simple, then $p(G) \lhd G$ implies $p(G) = G$, i.e. G is a quasi-p group. □

We can use above lemmas together with the Odlyzko discriminant bound to show various simple groups cannot be in $\pi_A(U_p)$:

Examples 2.2. For $2 \leqslant p < 23$, we consider A_5, S_5, $\mathrm{SL}(3,2)$.

- $\mathrm{SL}(3,2) \notin \pi_A(U_p)$ for $2 \leqslant p < 23$.

  Proof. The group $\mathrm{SL}(3,2)$ is of order $168 = 2^3 \cdot 3 \cdot 7$. When $p \neq 2, 3, 7$, if we assume $G \in \pi_A(U_p)$, by Lemma 2.1 we would have $p \mid |G|$, contradiction. In the case $p = 2$, Harbater showed $\mathrm{SL}(3,2) \notin \pi_A(U_2)$ (Example 2.21(c), [Ha]). In the case $p = 7$, Brueggeman showed $\mathrm{SL}(3,2) \notin \pi_A(U_7)$ in Theorem 4.1 [Br]. For the case $p = 3$, we assume $G \in \pi_A(U_3)$. Let $L/\mathbb{Q}$ be a corresponding Galois extension and let e be the ramification index of the prime above p. Applying the discriminant upper bound (Theorem 2.6, Chapter III, [Ne]), we get $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/168} \leqslant 3^{1+v_3(e)-1/e}$. The largest power of 3 dividing $|\mathrm{SL}(3,2)| = 168$ is 3, so $v_3(e) \leqslant 1$, thus $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/168} \leqslant 3^{1+v_3(e)-1/e} \leqslant 3^{1+1} = 9$. On the other hand, by the Odlyzko discriminant bound (Table 1, [Od]), $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/168} \geqslant 15.12$ when the degree of the extension is at least 160. Contradiction. □

- The alternating group $A_5 \notin \pi_A(U_p)$ for $2 \leqslant p < 23$.

  Proof. The group A_5 is of order $60 = 2^2 \cdot 3 \cdot 5$. When $p \neq 2, 3, 5$, by Lemma 2.1, we know $G \in \pi_A(U_p)$ would imply $p \mid |G|$, contradiction. For $p = 2$, Harbater showed that $A_5 \notin \pi_A(U_p)$ (Example 2.21(a), [Ha]). For $p = 5$, we know $A_5 \notin \pi_A(U_5)$ from the table [Jo]. For $p = 3$, we assume the simple group A_5 lies in $\pi_A(U_3)$ and let $L/\mathbb{Q}$ be a corresponding Galois extension. Applying the discriminant upper bound, we have $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/60} \leqslant 3^{1+v_3(e)-1/e}$. Since the largest power of 3

dividing $|A_5| = 60$ is 3, we get $v_3(e) \leqslant 1$, thus $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/60} \leqslant 3^{1+v_3(e)-1/e} \leqslant 3^{1+1} = 9$. On the other hand, by the Odlyzko discriminant bound (Table 1, [Od]), $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/60} \geqslant 12.23$ when the degree of the extension is at least 60. Contradiction. □

- The symmetric group $S_5 \notin \pi_A(U_p)$ for $2 \leqslant p < 23$.

Proof. The group S_5 is of order $120 = 2^3 \cdot 3 \cdot 5$. When $p \neq 2, 3, 5$, by Lemma 2.1 we know $G \notin \pi_A(U_p)$, for otherwise we would have $p \mid |G|$, contradiction. For $p = 2$, Harbater showed $S_5 \notin \pi_A(U_p)$ (Example 2.21(a), [Ha]). For $p = 5$, we know $S_5 \notin \pi_A(U_p)$ from the table [Jo]. For $p = 3$, similarly as A_5, we have $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/120} \leqslant 3^{1+v_3(e)-1/e} \leqslant 3^{1+1} = 9$. But by the Odlyzko bound, we have $|\mathfrak{d}_{L/\mathbb{Q}}|^{1/120} \geqslant 14.38$ for extensions of degree at least 120, this is a contradiction. □

Now we are ready to prove the proposition in the introduction using above examples.

Proof of Proposition. Assume there exist non-solvable groups $G \in \pi_A(U_p)$ with order $\leqslant 300$, and let G be such a group of smallest order. Pick a non-trivial normal subgroup N of G. The quotient group G/N is also in $\pi_A(U_p)$ but with smaller order, hence solvable. We know N is non-solvable, so the order of the group N is at least 60. So $|G/N| \leqslant 5$, thus G/N is abelian. By Lemma 2.5 in [Ha] we know G is isomorphic to either A_5, S_5 or $\mathrm{SL}(3, 2)$. By examples above, these groups do not lie in $\pi_A(U_p)$ for $2 \leqslant p < 23$. □

3. Tamely ramified covers of the affine line over $\mathbb{F}_q$

In this section, we will denote by k the rational function $\mathbb{F}_q(t)$, and denote by $\mathfrak{f}$ the ideal generated by an irreducible polynomial $f \in \mathbb{F}_q[t]$. Let $U_\mathfrak{f} = \mathbb{A}^1_{\mathbb{F}_q} - (f = 0)$.

Proposition 3.1. *Let K be the function field of a geometric Galois cover of the affine line over $\mathbb{F}_q$ with Galois group G and ramified only at a finite prime $\mathfrak{f}$ and possibly at ∞, with all ramification tame. Then there exist $x_1, x_2, \ldots, x_d, x_\infty \in G$ such that $\langle x_1, \ldots, x_d, x_\infty \rangle = G$ and $x_1 \cdots x_d x_\infty = 1$ with $x_1^q \sim x_2, \ldots, x_d^q \sim x_1$ and $x_\infty^q \sim x_\infty$ (i.e. conjugate in G). Moreover, the order of each of $x_1, \ldots, x_d$ is equal to the ramification index over $\mathfrak{f}$, and the order of x_∞ is the ramification index at ∞. So if $K/\mathbb{F}_q(t)$ is unramified at ∞, then $x_\infty = 1$.*

Proof. Suppose $\deg(\mathfrak{f}) = d$. After the base change to $\mathbb{F}_{q^d}(t)$, the prime $\mathfrak{f}$ splits into d primes $\mathfrak{f}_1, \ldots, \mathfrak{f}_d$ with degree 1, which correspond to d finite places $P_1, \ldots, P_d$ of $\mathbb{F}_{q^d}(t)$. Since ∞ has degree 1 in $\mathbb{F}_q(t)$, there is a unique place P_∞ of $\mathbb{F}_{q^d}(t)$ above ∞. For each place P_i, where $1 \leqslant i \leqslant d$ or $i = \infty$, there are g (independent on i) places $Q_{i,1}, Q_{i,2}, \ldots, Q_{i,g}$ of $\bar{K}$ above P_i, since $\bar{K}$ is Galois over $\mathbb{F}_q(t)$. Each place $Q_{i,j}$ has an inertia group $I_{i,j}$. Since the extension is tamely ramified, each $I_{i,j}$ is cyclic, say generated by $x_{i,j}$, i.e. $I_{i,j} = \langle x_{i,j} \rangle$. Fixing i, the inertia groups $I_{i,j}$ are all conjugate in G. The Galois group $\mathrm{Gal}(F_{q^d}(t)/F_q(t)) \cong \mathbb{Z}/d = \langle \sigma \rangle$ is generated by the Frobenius map σ, which cyclicly permutes the places P_i where $1 \leqslant i \leqslant d$; say $\sigma(P_i) = P_{i+1}$ with (i mod d). Also, $\sigma(P_\infty) = P_\infty$. On the other hand, there is a choice of places Q_i above P_i for $1 \leqslant i \leqslant d$ and $i = \infty$ such that the generators x_i of the corresponding inertia groups generate the Galois group G, i.e. $\langle x_1, \ldots, x_d, x_\infty \rangle = G$, and $x_1 x_2 \cdots x_d x_\infty = 1$. (Namely, these Q_i's are specializations of corresponding ramification points of a lift of this tame cover to characteristic 0, as in [Gro, XIII].) Since all the places P_i with $1 \leqslant i \leqslant d$ lie over the same closed point $\mathfrak{f}$, there is an additional condition on the group G. Namely, the Frobenius map σ takes the place Q_1 to some Q_2' over P_2; but the inertia group I_2 and I_2' are conjugate, so $x_1^q \sim x_2$. Similarly $x_2^q \sim x_3, \ldots, x_d^q \sim x_1$. Since the Frobenius map σ maps the place Q_∞ to some place Q_∞' over P_∞, we have $x_\infty^q \sim x_\infty$. □

Now we consider Galois covers of the projective line $\mathbb{P}^1_{\mathbb{F}_q(t)}$ ramified only at a finite prime $\mathfrak{f}$, generated by an irreducible polynomial f in $\mathbb{F}_q[t]$, and unramified at ∞. So $U_\mathfrak{f} = \mathbb{P}^1_{\mathbb{F}_q(t)} - (f = 0)$.

Corollary 3.2. *Let n be a positive integer, and let q be a power of an odd prime or $q = 2$ or 4. Suppose the degree d of the prime $\mathfrak{f}$ is not divisible by n, and consider any semi-direct product $G = P \rtimes \mathbb{Z}/(q^n - 1)$, where P is a p-group of order q^n. Then $G \notin \pi_A^t(U_\mathfrak{f})$ where $U_\mathfrak{f} = \mathbb{P}^1_{\mathbb{F}_q(t)} - (f = 0)$.*

Proof. Otherwise suppose $G \in \pi_A^t(U_\mathfrak{f})$, where $d = \deg(f)$ is not divisible by n. By Proposition 3.1, we have $G = \langle x_1, \ldots, x_d \rangle$ with relations $x_1^q \sim x_2, \ldots, x_d^q \sim x_1$ and $x_1 \cdots x_d = 1$. From the relation $x_1^q \sim x_2, \ldots, x_d^q \sim x_1$, we have $x_i^{q^d} \sim x_i$ for $1 \leqslant i \leqslant d$. Write $x_i = (a_i, b_i)$, where $a_i \in P$ and $b_i \in \mathbb{Z}/(q^n - 1)$. Then $x_i \notin P$, for otherwise all x_i's are in the normal subgroup P and cannot generate the group G. Also one of the b_i has to be a generator of $\mathbb{Z}/(q^n - 1)$, otherwise the x_i's will not generate the whole group G. Now $x_i^{q^d} \sim x_i$ implies $b_i^{q^d} = b_i$, i.e. $q^d \equiv 1 \bmod (q^n - 1)$. Since $q^d \equiv 1 \bmod (q^n - 1)$ if and only if $n \mid d$, we have $n \mid d$. This is a contradiction. □

Example. If $p = 2$ and $n = 2$ in Corollary 3.2, we can pick G to be the alternating group $A_4 = (\mathbb{Z}/2)^2 \rtimes \mathbb{Z}/3$. So $A_4 \notin \pi_A^t(U_\mathfrak{f})$ for any prime generated by an irreducible polynomial $f \in \mathbb{F}_2[t]$ of odd degree.

Remark. In fact, the conclusion in 3.2 can also be obtained using cyclotomic function fields, i.e. there are no cyclic extensions of order $q^n - 1$ over $\mathbb{F}_q(t)$ ramified only at one finite prime $\mathfrak{f}$ (and the ramification is tame) of degree not divisible by n. In fact, such extension would be inside a cyclotomic function field of degree $q^d - 1$ (see Theorem 2.3, [Hay]).

Applying the proposition to dihedral groups $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$ and symmetric groups S_n, we get Corollaries A and B as follow.

Proof of Corollary A. Suppose that $K/\mathbb{F}_q(t)$ is a geometric Galois extension with group D_{2n}, ramified only at a finite prime f with $\deg f = d$. Applying Proposition 3.1, we know $G = \langle x_1, \ldots, x_d \rangle$ with relations $x_1 \cdots x_d = 1$ and $x_1^q \sim x_2, \ldots, x_d^q \sim x_1$. Now we divide the situation into two cases (n is even and n is odd):

Case *($n = 2k$).* The conjugacy classes in D_{2n} are $\{1\}$, $\{r^k\}$, $\{r^{\pm 1}\}$, $\{r^{\pm 2}\}, \ldots, \{r^{\pm(k-1)}\}$, $\{sr^{2b} \mid b = 1, \ldots, k\}$, $\{sr^{2b-1} \mid b = 1, \ldots, k\}$. If one of $x_1, \ldots, x_d$ is a power of r, then all the x_i's have to be powers of r because of the conjugacy relations. This is a contradiction since such x_i's cannot generate the group D_{2n}. So we have $x_i = sr^{t_i}$, $1 \leqslant i \leqslant d$, for some integers t_i. If some t_i is even, then again by the conjugacy relations all t_i's have to be even. This is a contradiction since such x_i's cannot generate the group D_{2n}. So we can write $x_i = sr^{2k_i+1}$, $1 \leqslant i \leqslant d$, which implies $sr^{2k_1+1} \cdot sr^{2k_2+1} \cdots sr^{2k_{d-1}+1} \cdot sr^{2k_d+1} = 1$. This is impossible. Therefore $D_{4k} \notin \pi_A^t(U_f)$.

Case *($n = 2k + 1$).* The conjugacy classes in D_{2n} are $\{1\}$, $\{r^{\pm 1}\}$, $\{r^{\pm 2}\}, \ldots, \{r^{\pm k}\}, \{sr^b \mid b = 1, \ldots, n\}$. Similarly we can write $x_i = sr^{k_i}$, $1 \leqslant i \leqslant d$, which gives $sr^{k_1} \cdot sr^{k_2} \cdots sr^{k_{d-1}} \cdot sr^{k_d} = 1$. This is impossible if $2 \nmid d$. Thus $D_{4k+2} \notin \pi_A^t(U_f)$ if the degree of the prime f is odd. □

Proof of Corollary B. Suppose that $K/\mathbb{F}_q(t)$ is a geometric Galois extension with group S_n, ramified only at a finite prime f with $\deg f = d$. Applying Proposition 3.1, we know there exist $x_1, \ldots, x_d$ such that $G = \langle x_1, \ldots, x_d \rangle$ with relations $x_1 \cdots x_d = 1$ and $x_1^q \sim x_2, \ldots, x_d^q \sim x_1$. If $2 \mid q$, all x_i's are even permutations since two permutations are conjugate in S_n if and only if they have the same cycle structure. This is impossible since they cannot generate S_n; If $2 \nmid q$, all x_i's are of the same parity. Since they generate S_n, they have to be odd permutations. So if d is odd, the product $\prod_{i=1}^d x_i$ of an odd number of odd permutations x_i's is still an odd permutation, which cannot be 1, contradiction. □

References

[Br] Sharon Brueggeman, Septic number fields which are ramified only at one small prime, J. Symbolic Comput. 31 (2001) 549–555.

[Gro] A. Grothendieck, Revêtements étales et groupe fondamental, in: SGA 1, in: Lecture Notes in Math., vol. 224, Springer-Verlag, Berlin–Heidelberg–New York, 1971.
[Ha] David Harbater, Galois groups with prescribed ramification, in: Contemp. Math., vol. 174, 1994, pp. 35–60.
[Hay] D.R. Hayes, Explicit class field theory for rational function fields, Trans. Amer. Math. Soc. 189 (1974) 77–91.
[JY] Christian Jensen, Noriko Yui, Polynomials with D_p as Galois group, J. Number Theory 15 (1982).
[Jo] John Jones, Tables of number fields with prescribed ramification, available from http://math.asu.edu/~jj/numberfields/.
[Ne] Jurgen Neukirch, Algebraic Number Theory, A Series of Comprehensive Studies in Mathematics, vol. 322, Springer-Verlag, 1999.
[Od] A.M. Odlyzko, On conductor and discriminants, Algebraic Number Fields (1994) 377–407.
[Rot] Joseph J. Rotman, Theory of Groups, Reprint of the 1984 original, Wm. C. Brown Publisher, 1988.
[Se] Jean-Pierre Serre, Local Fields, Grad. Texts in Math., Springer-Verlag, 1979.