Kim, K.-S.
Osaka J. Math.
52 (2015), 1039–1050

CONSTRUCTION OF UNRAMIFIED EXTENSIONS WITH A PRESCRIBED GALOIS GROUP

KWANG-SEOB KIM

(Received September 5, 2013, revised July 14, 2014)

Abstract

In this article, we shall prove that for any finite solvable group G, there exist infinitely many abelian extensions $K/\mathbb{Q}$ and Galois extensions $M/\mathbb{Q}$ such that the Galois group $\mathrm{Gal}(M/K)$ is isomorphic to G and M/K is unramified. The difference between our result and [3, 4, 6, 7, 13] is that we have a base field K which is not only Galois over $\mathbb{Q}$, but also has very small degree compared to their results. We will also get another proof of Nomura's work [9], which gives us a base field of smaller degree than Nomura's. Finally for a given finite nonabelian simple group G, we will show there exists an unramified extension M/K' such that the Galois group is isomorphic to G and K' has relatively small degree.

1. Introduction

The existence of unramified extensions with a prescribed Galois group has been studied by various authors. Fröhlich [4] proved that for any positive integer n, there exists a number field K of finite degree and an unramified extension M/K such that the Galois group $\mathrm{Gal}(M/K)$ is isomorphic to the symmetric group S_n of degree n. This result implies that any finite group can be realized as the Galois group of some unramified extension. Although for a given finite group G we can find an unramified extension M/K' such that $G \simeq \mathrm{Gal}(M/K')$ by Fröhlich's work, it is more or less meaningless because K' has extremely high degree and it is not even Galois over $\mathbb{Q}$. Therefore, researchers have tried to find a base field which has degree smaller than the order of G and is Galois over $\mathbb{Q}$.

Uchida [11], Yamamoto [13], Elstrodt–Grunewald–Mennicke [3], Kondo [7] and Kedlaya [6] studied the existence of an unramified extension over a quadratic field whose Galois group is isomorphic to the alternating group A_n. Using their results, we see that the base field K of an unramified S_n-extension can be chosen as a quadratic field, and that a given finite group G, we can find an unramified extension M/K' such that $G \simeq \mathrm{Gal}(M/K')$. In this case, the degree of the base field K' is smaller than Fröhlich's but is still extremely high.

Recently Ozaki [10] and Nomura [9] studied p-group cases. Ozaki [10] proved that for any finite p-group G, there exists a number field K of finite degree such

2010 Mathematics Subject Classification. Primary 12F12; Secondary 11R29.

that the Galois group of its maximal unramified p-extension is isomorphic to G. But the degree of the base field K is also extremely high in this case. Nomura sacrificed the maximality of unramified p-extension to greatly reduce the degree of the base field. Nomura [9] proved that for any finite p-group G, there exists an elementary abelian p-extension $K/\mathbb{Q}$ and an unramified extension M/K such that the Galois group $\mathrm{Gal}(M/K)$ is isomorphic to G, and reduced the degree of the base field K as much as possible. The base field K can be chosen such that $[K : \mathbb{Q}] = p^{a+1}$, where $|G^p[G, G]| = p^a$.

In this article, we will mainly consider the case of finite solvable groups. We shall prove that for any finite solvable group G, there exist infinitely many abelian extensions $K/\mathbb{Q}$ and Galois extensions $M/\mathbb{Q}$ such that the Galois group $\mathrm{Gal}(M/K)$ is isomorphic to G and M/K is unramified. The difference between our result and that of [3, 4, 6, 7, 13] is that we have a base field which is not only Galois over $\mathbb{Q}$, but also has very small degree compared to their results. In doing this, we will also consider the case of p-groups. We will find an alternative to Nomura's proof that gives a base field of degree smaller than Nomura's.

Finally for a given finite nonabelian simple group G, we will demonstrate the existence of an unramified extension M/K' such that the Galois group is isomorphic to G and K' has relatively small degree. This is a consequence of Kedlaya's work [6].

2. Embedding problems

In this section, we recall some facts from the theory of embedding problems of Galois extensions to prove our main theorem. General studies on embedding problems can be found in Chapter III §5 and Chapter IV §6 of [8].

Let k be a number field of finite degree and G_k the absolute Galois group of k. Let K/k be a finite Galois extension with the Galois group G. For a group extension $1 \to A \to E \xrightarrow{j} G \to 1$ of finite groups, the embedding problem (G, φ, j) is defined by the diagram

$$\begin{array}{ccccccccc} & & & & & & G_k & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{j} & G & \longrightarrow & 1 \end{array}$$

where φ is the canonical surjection. A continuous homomorphism ψ of G_k to E is called a *solution* of (G, φ, j) if it satisfies the condition $j \circ \psi = \varphi$. When (G, φ, j) has a solution, we call (G, φ, j) is *solvable*. A solution ψ is called a proper solution if it is surjective. A field N is called a *solution field* (resp. a *proper solution field*) of (G, φ, j) if N is the fixed field of the kernel of a solution (resp. a proper solution).

For a Galois extension K/k, we set

$$\mathrm{Ram}(K/k) := \{\mathfrak{p} \text{ of a prime of } k \mid \mathfrak{p} \text{ ramifies in } K/k\},$$
$$\mathfrak{S}_p = \mathfrak{S}(k)_p := \{\mathfrak{p} \text{ of a prime of } k \text{ dividing } p\},$$
$$\mathfrak{S}_\infty = \mathfrak{S}(k)_\infty := \{\text{infinite (i.e., archimedean) primes of } k\}.$$

Theorem 2.1 (Theorem 9.6.7 in [8]). *Let K/k be a finite Galois extension of the global field k and let $\varphi\colon G_k \twoheadrightarrow \mathrm{Gal}(K/k) = G$. Then every split embedding problem*

$$\begin{array}{ccccccccc} & & & & & & G_k & & \\ & & & & & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & P & \longrightarrow & P \rtimes G & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

with finite p-group P has a proper solution N/k. If $p \neq \mathrm{char}(k)$, we can choose the solution in such a way that the following conditions are satisfied:
(i) *All $\mathfrak{p} \in \mathrm{Ram}(K/k) \cup \mathfrak{S}_p \cup \mathfrak{S}_\infty$ are completely decomposed in N/K.*
(ii) *If $\mathfrak{p}$ is ramified in N/K, then $\mathfrak{p}$ splits completely in K/k and $N_\mathfrak{p}/k_\mathfrak{p}$ is a cyclic totally ramified extension of local fields.*

3. Some lemmas

In this section, we quote useful and important lemmas to prove our main theorem.

Lemma 3.1 (Abhyankar's lemma, Theorem 1 of [2]). *Let F be a local field. Let E_1 and E_2 be finite extensions of F with ramification indices e_1 and e_2 respectively. Suppose E_2 is tamely ramified and $e_2 \mid e_1$. Then E_1E_2 is an unramified extension of E_1.*

REMARK 3.2. Let E_1/F and E_2/F be extensions of global fields such that the ramification indicies at $\mathfrak{p}$ satisfy the conditions of Lemma 3.1. Then the extension E_1E_2/E_1 is unramified at $\mathfrak{p}$ since this is a local question. If this holds for each prime $\mathfrak{p}$ of F, then E_1E_2/E_1 is unramified everywhere.

To prove our main theorem, we need the following Proposition 3.5. The following lemmas will be used to prove Proposition 3.5.

Lemma 3.3 (Lemma 14.4 of [12]). *Let E/F be an unramified, finite Galois extension where E and F are finite extension of $\mathbb{Q}_p$. Then $E = F(\zeta_n)$ for some n with $p \nmid n$.*

Lemma 3.4 (Lemma 14.5 of [12]). *Let E and F be finite extension of $\mathbb{Q}_p$ and let $\mathfrak{p}_F$ be the maximal ideal of the integers of F. Suppose E/F is totally ramified of*

degree e with $p \nmid e$ (i.e., E/F is tamely ramified). Then there exists $\pi \in \mathfrak{p}_F \setminus \mathfrak{p}_F^2$ and a root of α of

$$X^e - \pi = 0$$

such that $E = F(\alpha)$.

Proposition 3.5. *If $E/\mathbb{Q}_p$ is a totally ramified abelian extension of degree e with $p \nmid e$, then $e \mid (p-1)$.*

Proof. Let $E/\mathbb{Q}_p$ be a totally ramified abelian extension of degree e with $p \nmid e$ (i.e., $E/\mathbb{Q}_p$ is tamely ramified). By Lemma 3.4, $E = \mathbb{Q}_p(\pi^{1/e})$ where $\pi = -up$ for some unit $u \in \mathbb{Q}_p$. Since u is a unit and $p \nmid e$ the discriminant of $f(X) = X^e - u$ is not divisible by p, hence $\mathbb{Q}_p(u^{1/e})/\mathbb{Q}_p$ is unramified. By Lemma 3.3,

$$\mathbb{Q}_p(u^{1/e}) \subset \mathbb{Q}_p(\zeta_n)$$

for some n with $p \nmid n$. Let T be the compositum of the fields $\mathbb{Q}_p(\zeta_n)$ and E. Then T is abelian. Since $u^{1/e}$ and $\pi^{1/e}$ are contained in T, $(-p)^{1/e}$ is also contained in T. It follows that $\mathbb{Q}_p((-p)^{1/e})/\mathbb{Q}_p$ is Galois, since it is a subextension of the abelian extension $T/\mathbb{Q}$, so

$$\mathbb{Q}_p((-p)^{1/e}) = \mathbb{Q}_p(\zeta_e(-p)^{1/e})$$

for a primitive eth root of unity ζ_e. Therefore

$$\zeta_e \in \mathbb{Q}_p((-p)^{1/e}).$$

Since $\mathbb{Q}_p((-p)^{1/e})$ is totally ramified, so is the subextension $\mathbb{Q}_p(\zeta_e)/\mathbb{Q}_p$. But $p \nmid e$, so the latter extension is trivial and $\zeta_e \in \mathbb{Q}_p$. Therefore $e \mid (p-1)$. □

The following lemma will be used in comparing our result and the previous one.

Lemma 3.6. *Let n be a product of at least two distinct primes, i.e., $n = p_1^{r_1} \cdots p_t^{r_t}$. Put $s = \sum_{i=1}^{t} r_i$. Then*

$$n^s < 2(n-1)!.$$

Proof. We claim that n^s divides $n!$. It suffices to show that $p_i^{r_i s} \mid n!$ for each p_i. Let us show the following terms divide $n!$:

- $p_1^x p_2^{r_2} \cdots p_t^{r_t}$ where $1 \le x \le r_1$;
- $p_1^{r_1} \cdot y$ where $1 \le y \le (r_2 + \cdots + r_t)$;
- p_1^z where $1 \le z \le (r_1 - 1)$.

Note that $p_2^{r_2} p_3^{r_3} \cdots p_t^{r_t} > p_2^{r_2} + p_3^{r_3} + \cdots + p_t^{r_t} > r_2 + r_3 + \cdots + r_t$. It is clear that any two of above terms are distinct. The product of all p_1-factors of the above terms is $p_1^{r_1 s}$. So $p_i^{r_i s}$ divides $n!$ for each i.

Since n and $n-1$ are relatively prime, it is clear that $n^{s-1} \mid (n-2)!$, i.e., $n^{s-1} \le (n-2)!$. Since $n < 2(n-1)$, $n^s < 2(n-1)!$. □

4. Main theorem

Main theorem. *Let $L/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) = G$. Let $K/\mathbb{Q}$ be a Galois extension such that LK/K is unramified and $L \cap K = \mathbb{Q}$, i.e., $\mathrm{Gal}(LK/K) \simeq \mathrm{Gal}(L/\mathbb{Q})$. Let H be a finite nilpotent group satisfying*

$$1 \to H \to H \rtimes G \to G \to 1.$$

Then there exist infinitely many cyclic extensions $K_0/\mathbb{Q}$ and Galois extensions $L'/\mathbb{Q}$ such that
(i) $L' \supset L$, $L' \cap K' = \mathbb{Q}$,
(ii) $\mathrm{Gal}(L'/\mathbb{Q}) \simeq H \rtimes G$, *i.e.,* $\mathrm{Gal}(L'K'/K') \simeq H \rtimes G$ *and*
(iii) $L'K'/K'$ *is unramified at all primes,*
where K' is the compositum of the fields K and K_0. We can take K_0 satisfying $[K_0 : \mathbb{Q}] \leq m$ where m is the maximal order of elements in H.

To prove our main theorem, we need the following Theorem 4.1.

Theorem 4.1. *Let $L/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) = G$. Let $K/\mathbb{Q}$ be a Galois extension such that LK/K is unramified and $L \cap K = \mathbb{Q}$, i.e., $\mathrm{Gal}(LK/K) \simeq \mathrm{Gal}(L/\mathbb{Q})$. Let P be a finite p-group satisfying*

$$1 \to P \to P \rtimes G \to G \to 1.$$

Then there exist infinitely many cyclic p-extensions $K_0/\mathbb{Q}$ and Galois extensions $L'/\mathbb{Q}$ such that
(i) $L' \supset L$, $L' \cap K' = \mathbb{Q}$,
(ii) $\mathrm{Gal}(L'/\mathbb{Q}) \simeq P \rtimes G$, *i.e.,* $\mathrm{Gal}(L'K'/K') \simeq P \rtimes G$ *and*
(iii) $L'K'/K'$ *is unramified at all primes,*
where K' is the compositum of the fields K and K_0. We can take K_0 satisfying $[K_0 : \mathbb{Q}] \leq p^m$ where p^m is the maximal order of elements in P.

Proof. Define $G_0 := \mathrm{Gal}(LK/\mathbb{Q}) = G \times \mathrm{Gal}(K/\mathbb{Q})$. Consider the embedding problem

$$\begin{array}{ccccccccc} & & & & & & & & G_k \\ & & & & & & & & \downarrow{\scriptstyle \varphi} \\ 1 & \longrightarrow & P & \longrightarrow & P \rtimes G_0 & \longrightarrow & G_0 & \longrightarrow & 1 \end{array}$$

($\mathrm{Gal}(K/\mathbb{Q})$ acts trivially on P). Theorem 2.1 implies that $N/\mathbb{Q}$ exists such that $\mathrm{Gal}(N/\mathbb{Q}) \simeq (P \rtimes G) \times \mathrm{Gal}(K/\mathbb{Q})$. Then N is the composite of $K/\mathbb{Q}$ and Galois extension $L'/\mathbb{Q}$ with $\mathrm{Gal}(L'/\mathbb{Q}) \simeq P \rtimes G$, $L' \supset L$ and $L' \cap K = \mathbb{Q}$. L is a Galois subfield of L'. By Theorem 2.1, we can take N satisfying the following conditions (i) (ii).

(i) All $\mathfrak{p} \in \mathrm{Ram}(LK/\mathbb{Q}) \cup \mathfrak{S}_p \cup \mathfrak{S}_\infty$ are unramified in N/LK.
(ii) If q_i is in $\mathrm{Ram}(N/\mathbb{Q}) \setminus \mathrm{Ram}(LK/\mathbb{Q})$, then q_i splits completely in $LK/\mathbb{Q}$ and $N_{\bar{\mathfrak{q}}_i}/\mathbb{Q}_{q_i} = L'_{\mathfrak{q}_i}/\mathbb{Q}_{q_i}$ is a cyclic totally ramified extension of local fields, where $\bar{\mathfrak{q}}_i$ (resp. $\mathfrak{q}_i$) is a prime ideal in N (resp. L') satisfying $\bar{\mathfrak{q}}_i \mid q_i$ (resp. $\mathfrak{q}_i \mid q_i$) and $N_{\bar{\mathfrak{q}}_i}$ (resp. $L'_{\mathfrak{q}_i}$) is the $\bar{\mathfrak{q}}_i$-completion of N (resp. $\mathfrak{q}_i$-completion of L').

Thus every $q_i \in \mathrm{Ram}(N/\mathbb{Q}) \setminus \mathrm{Ram}(LK/\mathbb{Q}) = \{q_1, q_2, \ldots, q_n\}$ is tamely ramified and $\mathrm{Gal}(L'_{\mathfrak{q}_i}/\mathbb{Q}_{q_i}) \simeq \mathbb{Z}/p^{a_i}\mathbb{Z}$ for all q_i, where p^{a_i} is the ramification index for each q_i. By Proposition 3.5, $p^{a_i} \mid (q_i - 1)$. Let K_i be a cyclic subfield of $\mathbb{Q}(\zeta_{q_i})$ with degree p^{a_i}. Then $K_i/\mathbb{Q}$ is a totally ramified extension with ramification index p^{a_i}.

Define $a := \max\{a_1, a_2, \ldots, a_n\}$. Let q_{n+1} be a prime which is unramified in $N/\mathbb{Q}$ and congruent to 1 mod p^a. Infinitely many such primes exist, this fact is responsible for *the existence of infinitely many cyclic p-extensions* K_0. Then a $\mathbb{Z}/p^a\mathbb{Z}$-extension $K_{n+1} \subset \mathbb{Q}(\zeta_{q_{n+1}})$ exist. Let χ_i be the character corresponding to K_i. Define

$$\chi = \chi_1 \cdots \chi_{n+1}$$

and let K_0 be the corresponding field. Then K_0 is a $\mathbb{Z}/p^a\mathbb{Z}$-extension unramified outside $\{q_1, q_2, \ldots, q_{n+1}\}$ with ramification index $e_i = p^{a_i}$ for each q_i $(1 \le i \le n+1)$.

Define $K' := KK_0$. Because q_{n+1} is unramified in N, $N \cap K_0 = \mathbb{Q}$. Thus $\mathrm{Gal}(NK_0/\mathbb{Q}) \simeq \mathrm{Gal}(N/\mathbb{Q}) \times \mathrm{Gal}(K_0/\mathbb{Q}) \simeq (\mathrm{Gal}(L'/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})) \times \mathrm{Gal}(K_0/\mathbb{Q}) \simeq (\mathrm{Gal}(L'/\mathbb{Q}) \times \mathrm{Gal}(K'/\mathbb{Q}))$. Then $L' \cap K' = \mathbb{Q}$. We know that N/K is unramified outside $\{q_1, q_2, \ldots, q_n\}$. By Abhyankar's lemma, $NK_0/KK_0 = L'K'/K'$ is unramified at all finite primes and $\mathrm{Gal}(L'K'/K') \simeq \mathrm{Gal}(L'/\mathbb{Q}) \simeq P \rtimes G$. Now the remaining task is to show that $L'K'/K'$ is unramified at archimedean primes. Because all fields that we are considering are Galois over $\mathbb{Q}$, they are either totally complex or totally real. If K is totally complex, then every extension of K is unramified at the archimedean primes, this completes the proof. If K is totally real, then by the condition (i) of Theorem 2.1 (i), N is also totally real. Thus $L'K'/K' = NK_0/KK_0$ is unramified at the archimedean primes, whether K_0 is totally real or complex. □

Proof of Main theorem. Let H be a finite nilpotent group. Then H is the direct product of its Sylow p_i-subgroups, i.e., $H \simeq P_1 \times P_2 \times \cdots \times P_n$ where P_i is a Sylow p_i-subgroup of H and $|P_i| = (p_i)^{r_i}$ for each $1 \le i \le n$. Define H_i as $P_1 \times \cdots \times P_i$. Because p_i's are distinct, one can easily show that every P_i (resp. H_i) is a characteristic subgroup of H, i.e., every P_i (resp. H_i) is invariant under the action of G on H. So the action of G on H induces an action of G on P_i (resp. H_i) for each i. We will proceed by induction on i.

If $i = 1$, H_1 is a p_1-group. Consider the exact sequence

$$1 \to H_1 \to H_1 \rtimes G \to G \to 1$$

(the action is induced by the action of G on H). By Theorem 4.1, there exist infinitely many cyclic p_1-extensions $K^1/\mathbb{Q}$ and Galois extensions $L_1/\mathbb{Q}$ such that

(i) $L_1 \supset L$, $L_1 \cap K_1 = \mathbb{Q}$,
(ii) $\mathrm{Gal}(L_1/\mathbb{Q}) \simeq H_1 \rtimes G$, i.e., $\mathrm{Gal}(L_1K_1/K_1) \simeq H_1 \rtimes G$ and
(iii) L_1K_1/K_1 is unramified at all primes.
Here K_1 is defined as the compositum of the fields K and K^1.

Now we assume that we have already found a cyclic extension $K^i/\mathbb{Q}$ whose degree $[K^i : \mathbb{Q}]$ is coprime to p_{i+1} and a Galois extension $L_i/\mathbb{Q}$ such that
(i) $L_i \supset L$, $L_i \cap K_i = \mathbb{Q}$,
(ii) $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq H_i \rtimes G$, i.e., $\mathrm{Gal}(L_iK_i/K_i) \simeq H_i \rtimes G$ and
(iii) L_iK_i/K_i is unramified at all primes,
where K_i is the compositum of K and K^i. Consider the split exact sequence

$$1 \to P_{i+1} \to H_{i+1} \rtimes G \to H_i \rtimes G \to 1.$$

We can easily show that $H_{i+1} \rtimes G$ is a split extension of $H_i \rtimes G$ by P_{i+1}. (The actions are induced by the action of G on H.) By Theorem 4.1, there exist infinitely many cyclic p_{i+1}-extensions $K^{(i+1)}/\mathbb{Q}$ and Galois extensions $L_{i+1}/\mathbb{Q}$ such that
(i) $L_{i+1} \supset L_i$, $L_{i+1} \cap K_{i+1} = \mathbb{Q}$,
(ii) $\mathrm{Gal}(L_{i+1}/\mathbb{Q}) \simeq H_{i+1} \rtimes G$, i.e., $\mathrm{Gal}(L_{i+1}K_{i+1}/K_{i+1}) \simeq H_{i+1} \rtimes G$ and
(iii) $L_{i+1}K_{i+1}/K_{i+1}$ is unramified at all primes,
where K_{i+1} is the compositum of the fields K_i and $K^{(i+1)}$. Put $K^{i+1} = K^iK^{(i+1)}$. Since $[K^i : \mathbb{Q}]$ is coprime to p_{i+1}, K^{i+1} is cyclic, i.e., $K_{i+1} = K_iK^{(i+1)} = KK^{i+1}$ is the compositum of the fields K and cyclic extension K^{i+1}.

Therefore there exist Galois extensions $L_n/\mathbb{Q}$, $K_n/\mathbb{Q}$ such that
(i) $L_n \supset L$, $K_n \supset K$, $L_n \cap K_n = \mathbb{Q}$,
(ii) $\mathrm{Gal}(L_n/\mathbb{Q}) \simeq H_n \rtimes G$, i.e., $\mathrm{Gal}(L_nK_n/K_n) \simeq H_n \rtimes G$ and
(iii) L_nK_n/K_n is unramified at all primes,
where K_n is the compositum of the fields K and K^n. Put $K_0 := K^{(1)}K^{(2)} \cdots K^{(n)} = K^n$. Because p_i's are distinct, one can easily show that K_0 is cyclic and $[K_0 : \mathbb{Q}] \leq p^{m_1}p^{m_2} \cdots p^{m_n} = m$ where p^{m_i} is the maximal order of elements in P_i. Putting $L' := L_n$ and $K' := K_n$, we have proved our main theorem. □

5. Application 1—*p*-groups

Corollary 5.1. *For any finite p-group P, there exist infinitely many extensions M/K of number fields such that*
– *K is p-cyclic over $\mathbb{Q}$;*
– *M/K is unramified;*
– $\mathrm{Gal}(M/K) \simeq P$;
– $[K : \mathbb{Q}] \leq p^m$;
where p^m is the maximal order of elements in P.

Proof. By Theorem 4.1, there exists $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq P$ and cyclic p-extension K such that LK/K is unramified and $\mathrm{Gal}(LK/K) \simeq P$. Because $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to a cyclic subgroup of P, $[K : \mathbb{Q}] \leq p^m$. Putting $M := LK$, we have proved our assertion. □

REMARK 5.2. This is another proof of Nomura's result [9]. One main difference is that Nomura's base fields are elementary abelian p-extensions whereas our base fields are cyclic p-extensions. Moreover, the degree of base field is reduced. Note that $p^m \leq |P^p| \cdot p \leq |P^p[P, P]| \cdot p$.

EXAMPLE 5.3. Let $P = (\mathbb{Z}/p^2\mathbb{Z})^l$. Construct a p-unramified extension M/K whose Galois group is P by both methods. Because $P^p[P, P] \simeq (\mathbb{Z}/p\mathbb{Z})^l$, Nomura's base field K is an elementary abelian p-extension $K/\mathbb{Q}$ with degree $p^{l+1} = |P^p[P, P]| \cdot p$. But our base field is a cyclic p-extension with degree $p^2 \leq p^{l+1}$.

Corollary 5.4. *For any finite nilpotent group H, there exist infinitely many extensions M/K of number fields such that*
- *K is cyclic over $\mathbb{Q}$;*
- *M/K is unramified;*
- *$\mathrm{Gal}(M/K) \simeq H$;*
- *$[K : \mathbb{Q}] \leq m$;*

where m is the maximal order of elements in H.

Proof. By our main theorem, there exists $L/\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \simeq H$ and cyclic extension K such that LK/K is unramified and $\mathrm{Gal}(LK/K) \simeq H$. Because $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to a cyclic subgroup of H, $[K : \mathbb{Q}] \leq m$. Putting $M := LK$, we have proved our assertion. □

Corollary 5.5. *For any finite abelian group G, there exist infinitely many cyclic extensions K of $\mathbb{Q}$ such that the ideal class group of K contains a subgroup isomorphic to G.*

Proof. Since any finite abelian group G is nilpotent, the corollary follows from the Corollary 5.4. □

6. Application 2—solvable groups

In order to deduce the case of finite solvable groups, we need two facts from group theory and we recall the following definitions. Suppose that G is a finite nontrivial group.

DEFINITION 6.1. $\Phi(G)$ is the intersection of all maximal subgroups of G and is called the *Frattini subgroup* of G.

DEFINITION 6.2. $F(G)$ is the composite of all nilpotent normal subgroups of G and is called the *Fitting subgroup* of G.

$\Phi(G)$ is a characteristic subgroup of G and is contained in $F(G)$. The group $F(G)$ is a normal nilpotent subgroup of G. We cite the following two facts, see [5], Kapitel III, Satz 3.2 (b) and Satz 4.2 (c).

Proposition 6.3. *Let N be a normal subgroup of the finite group G such that $N \not\subseteq \Phi(G)$. Then there exists a partial complement U of N in G, i.e., $U \subsetneq G$ and $G = N \cdot U$.*

Proposition 6.4. *Let G be a nontrivial finite solvable group. Then $\Phi(G)$ is a proper subgroup of $F(G)$.*

Let G be a nontrivial finite solvable group. By the two propositions above, $F(G)$ has a solvable partial complement $U \subsetneq G$, so $G = F(G) \cdot U$. Since G is a solvable group, U is also a solvable group. We will define a solvable group sequence $\{G_i\}$:
– Define G_1 as G.
– Let G_i be a solvable group. Then $G_i = F(G_i) \cdot U$ for some partial complement $U \subsetneq G_i$. Define G_{i+1} as U.
Since G_i is a proper subgroup of G_{i-1}, the order of G_i decreases as i increases. So we get a trivial group G_{k+1} for some k. Because $G_k = F(G_k) \cdot G_{k+1} = F(G_k)$, G_k is a nilpotent group. That is the key idea in proving our main goal. Let g_i be the maximal order of elements in $F(G_i)$ for $1 \leq i \leq k-1$ and g_k be the maximal order of elements in G_k. Define $g = \prod_{i=1}^{k} g_i$.

Corollary 6.5. *For any finite solvable group $G \neq \{1\}$, we give constructions of infinitely many extensions M/K of number fields with*
– *K is abelian over $\mathbb{Q}$;*
– *M/K is unramified;*
– $\mathrm{Gal}(M/K) \simeq G$;
– $[K : \mathbb{Q}] \leq g$.

Proof. Let us recall the definition of the solvable group sequence $\{G_i\}$. Define $G_1 := G$ and $G_{i+1} := U$ where U is a partial complement of $F(G_i)$ in G_i i.e., $G_{i+1} \subsetneq G_i$ and $G_i = F(G_i) \cdot G_{i+1}$. Since G_{i+1} is a proper subgroup of G_i, the order of G_i decreases as i increases. So we get a nilpotent group G_k for some k. We will proceed by induction on i.

If $i = k$, G_k is a nilpotent group. By Corollary 5.4, we give L_k and K_k with
– K_k is cyclic over $\mathbb{Q}$;
– $L_k \cap K_k = \mathbb{Q}$;
– $L_k K_k / K_k$ is unramified;

– $\mathrm{Gal}(L_kK_k/K_k) \simeq G_k$;
– $[K_k : \mathbb{Q}] \leq g_k$.

Now we assume that we have already found L_i, K_i satisfying the following conditions:

(i) $L_i \cap K_i = \mathbb{Q}$,
(ii) $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq G_i$, i.e., $\mathrm{Gal}(L_iK_i/K_i) \simeq G_i$,
(iii) L_iK_i/K_i is unramified,
(iv) $[K_i : \mathbb{Q}] \leq g_i \cdots g_k$.

Since $F(G_{i-1}) \cdot G_i = G_{i-1}$, there exists a surjection

$$F(G_{i-1}) \rtimes G_i \twoheadrightarrow G_{i-1}.$$

By our main theorem, there exist $L'/L_i/\mathbb{Q}$ and $K_{i-1}/K_i/\mathbb{Q}$ such that

(i) $L' \cap K_{i-1} = \mathbb{Q}$,
(ii) $\mathrm{Gal}(L'/\mathbb{Q}) \simeq F(G_{i-1}) \rtimes G_i$, i.e., $\mathrm{Gal}(L'K_{i-1}/K_{i-1}) \simeq F(G_{i-1}) \rtimes G_i$,
(iii) $L'K_{i-1}/K_{i-1}$ is unramified.

By the proofs of Theorem 4.1 and our main theorem, K_{i-1} is the compositum of K_i and a cyclic extension $K_0/\mathbb{Q}$ such that $K_i \cap K_0 = \mathbb{Q}$. Thus $K_{i-1}/\mathbb{Q}$ is an abelian extension when $K_i/\mathbb{Q}$ is abelian. Note that $\mathrm{Gal}(K_0/\mathbb{Q})$ is isomorphic to cyclic subgroup of $F(G_{i-1})$. Thus $[K_{i-1} : \mathbb{Q}] \leq g_{i-1}g_i \cdots g_k$. Because $\mathrm{Gal}(L'/\mathbb{Q}) \simeq F(G_{i-1}) \rtimes G_i$, a subfield $L_{i-1} \subset L'$ exists such that $\mathrm{Gal}(L_{i-1}/\mathbb{Q}) \simeq G_{i-1}$. Because $L'K_{i-1}/K_{i-1}$ is unramified, $L_{i-1}K_{i-1}/K_{i-1}$ is also unramified and $\mathrm{Gal}(L_{i-1}K_{i-1}/K_{i-1}) \simeq G_{i-1}$.

Therefore there exist L_1, K_1 satisfying the following conditions:

(i) $L_1 \cap K_1 = \mathbb{Q}$,
(ii) $\mathrm{Gal}(L_1/\mathbb{Q}) \simeq G_1$, i.e., $\mathrm{Gal}(L_1K_1/K_1) \simeq G_1$,
(iii) L_1K_1/K_1 is unramified,
(iv) $[K_1 : \mathbb{Q}] \leq g_1g_2 \cdots g_k = g$.

Define $M := L_1K_1$ and $K := K_1$. From our setting of K, K is the compositum of cyclic extensions of $\mathbb{Q}$, thus $K/\mathbb{Q}$ is an abelian extension. This completes the proof. □

REMARK 6.6. We will compare our result with previous ones [3, 6, 7, 13].

Let G be a finite solvable group which is not nilpotent. Then we cannot use Corollary 5.4. Let n be the order of G. Since G is not nilpotent, n is a product of at least two distinct primes, i.e., $n = p_1^{r_1} \cdots p_t^{r_t}$. Put $s := \sum_{i=1}^{t} r_i$ and $p := \min\{p_1, p_2, \ldots, p_t\}$. Let us construct unramified extension M/K whose Galois group is G by our method.

By Corollary 6.5, $[K : \mathbb{Q}] \leq g = g_1g_2 \cdots g_k$. Since all $F(G_i)$'s and G_k are proper subgroups of G, we easily check that $g_i \leq n/p$ for each $1 \leq i \leq k$ and $k \leq s$, thus $[K : \mathbb{Q}] \leq (n/p)^s$.

Now let us construct it with Kedlaya's result [6]. Kedlaya proved that there exist infinitely many number fields F of degree $n = r + 2s$ and signature (r, s) such that the Galois closure L of F has Galois group S_n over $\mathbb{Q}$ and the discriminant of F is

squarefree. These conditions ensure that L is an unramified A_n-extension of $\mathbb{Q}(\sqrt{d_F})$. (See [3], or [7] Theorem 1 for a slightly stronger statement). Let $R = \mathbb{Q}(\sqrt{p \cdot d_F})$ where $p \nmid d_F$. By Lemma 3.1, LR/R is unramified and $\mathrm{Gal}(LR/R) \simeq \mathrm{Gal}(L/\mathbb{Q}) \simeq S_n$. So we can find an unramified extension LR/K' such that $\mathrm{Gal}(LR/K') \simeq G$ by his result. In this method, $[K' : \mathbb{Q}]$ is exactly $2(n-1)!$.

By Lemma 3.6, $[K : \mathbb{Q}] \leq (n/p)^s < n^s < 2(n-1)!$. So the degree of K is smaller in our method than Kedlaya's.

Let us see an example. Let G be a finite solvable group of order 100. Let us construct unramified extension M/K whose Galois group is G by our method. Since $100 = 2^2 \cdot 5^2$, the degree of K is at most 6.25×10^6 in our method, contrary to the fact that it is exactly $2 \cdot 99! = 1.8665 \cdots \times 10^{156}$ in Kedlaya's result.

In fact, when G is solvable, we cannot specify the degree of the base field due to the process of quotienting groups. Like two examples below, if there is no process of quotienting groups, the degree of a base field is smaller than $|G|$.

EXAMPLE 6.7. Suppose that $G = S_3$. In this case, we cannot use Corollary 5.4, because although G is solvable, it is not nilpotent. We know $G \simeq C_3 \rtimes C_2$. By Corollary 5.1, there exist quadratic extensions L, K such that $\mathrm{Gal}(LK/K) \simeq C_2$ and LK/K is unramified. By proof of our main theorem, there exist L', K' such that $\mathrm{Gal}(L'K'/K') \simeq C_3 \rtimes C_2 \simeq S_3$ and $L'K'/K'$ is unramified. Here, K' is a compositum of K and some cyclic cubic extension, thus the degree of base field K' is $6 = |S_3|$.

EXAMPLE 6.8. Suppose that $G = S_4$. This group G is also solvable, not nilpotent. G can be written as $V_4 \rtimes S_3$. By Example 6.7, there exist L', K' such that $\mathrm{Gal}(L'K'/K') \simeq S_3$ and $L'K'/K'$ is unramified. By proof of our main theorem, there exist L'', K'' such that $\mathrm{Gal}(L''K''/K'') \simeq V_4 \rtimes S_3 \simeq S_4$ and $L''K''/K''$ is unramified. Because the maximal order of elements of V_4 is 2, K'' is a compositum of K' and some quadratic field which is linearly disjoint with K'. Thus the degree of base field K' is $12 < |S_4|$.

REMARK 6.9. Suppose that G is a nonabelian simple group. Because G does not contain proper normal subgroups, we cannot use the embedding problem, but we can simply make nonabelian simple unramified extensions with simple observation based on Kedlaya's work [6].

Let G be a nonabelian simple group. Let H be a proper subgroup of G and $n := [G : H]$. Then there is a natural inclusion $G \hookrightarrow A_n$. We know that there are infinitely many unramified A_n-extensions M/K where K is a quadratic field. Let $K' := M^G$. Then M/K' is unramifed and $\mathrm{Gal}(M/K') \simeq G$.

As previously stated, we want to reduce the degree of the base field K' as much as possible; i.e. finding the minimal index of the subgroup of a nonabelian simple group G is sufficient.

(i) $G = A_n$—the minimal index of A_n is n.
(ii) $G = \mathrm{PSL}_n(q)$—the minimal index of $\mathrm{PSL}_n(q)$ is $(q^n-1)/(q-1)$ except for $(n,q) = (2, 5), (2, 7), (2, 9), (2, 11)$ or $(4, 2)$. (See [1]).
For example, let $G := \mathrm{PSL}_2(7)$. Then the minimal index of $\mathrm{PSL}_2(7)$ is 7. (See [1]). Thus we can choose a base field K' with degree $30 = 7!/|\mathrm{PSL}_2(7)|$.

References

[1] B.N. Cooperstein: *Minimal degree for a permutation representation of a classical group*, Israel J. Math. **30** (1978), 213–235.
[2] G. Cornell: *Abhyankar's lemma and the class group*; in Number Theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math. **751**, Springer, Berlin, 1979, 82–88.
[3] J. Elstrodt, F. Grunewald and J. Mennicke: *On unramified A_m-extensions of quadratic number fields*, Glasgow Math. J. **27** (1985), 31–37.
[4] A. Fröhlich: *On non-ramified extensions with prescribed Galois group*, Mathematika **9** (1962), 133–134.
[5] B. Huppert: Endliche Gruppen, I, Die Grundlehren der Mathematischen Wissenschaften **134**, Springer, Berlin, 1967.
[6] K.S. Kedlaya: *A construction of polynomials with squarefree discriminants*, Proc. Amer. Math. Soc. **140** (2012), 3025–3033.
[7] T. Kondo: *Algebraic number fields with the discriminant equal to that of a quadratic number field*, J. Math. Soc. Japan **47** (1995), 31–36.
[8] J. Neukirch, A. Schmidt and K. Wingberg: Cohomology of Number Fields, second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer, Berlin, 2008.
[9] A. Nomura: *On the existence of unramified p-extensions with prescribed Galois group*, Osaka J. Math. **47** (2010), 1159–1165.
[10] M. Ozaki: *Construction of maximal unramified p-extensions with prescribed Galois groups*, Invent. Math. **183** (2011), 649–680.
[11] K. Uchida: *Unramified extensions of quadratic number fields*, II, Tôhoku Math. J. (2) **22** (1970), 220–224.
[12] L.C. Washington: Introduction to Cyclotomic Fields, Graduate Texts in Mathematics **83**, Springer, New York, 1982.
[13] Y. Yamamoto: *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57–76.

School of Mathematics
Korea Institute for Advanced Study
Seoul, 130-722
Korea
e-mail: kwang12@kias.re.kr