MINIMAL NUMBER OF FROBENIUS ELEMENTS OF \( G_{K,S} \) WHOSE CONJUGACY CLASSES GENERATE THE WHOLE GROUP \( G_{K,S} \)

KWANG-SEOB KIM

Abstract. Assume that \( K \) is a number field and \( S \) is a finite set of primes of \( K \). Let \( G_{K,S} \) be the Galois group \( \text{Gal}(K_S/K) \), where \( K_S \) is the maximal extension of \( K \), which is unramified outside the primes in \( S \). It is conjectured that \( G_{K,S} \) is topologically finitely generated, details there of remain largely unknown. However, it has been proved that \( G_{K,S} \) is topologically generated by finitely many conjugacy classes by Ihara [1]. Then we can ask two natural questions. a) Is the Galois group \( G_{K,S} \) also generated by a finite number of conjugacy classes of the Frobenius elements? b) If \( G_{K,S} \) can be generated by a finite number of conjugacy classes of the Frobenius elements, what is the minimal number of generators? Let \( G_{K,S}^{ab} \) be the abelianization of \( G_{K,S} \). Suppose that the rank of \( G_{K,S}^{ab} \) is \( r \). In this article, we define a new topology on \( \text{Spec} \, O_K \setminus S \) and use this topology to show that \( G_{K,S} \) can be generated by \( r \) (or 1 if \( r = 0 \)) Frobenius classes and \( r \) is minimal.

1. Introduction

Let \( K \) be a number field and \( S \) be the finite set of primes of \( K \). In recent years, there has been considerable interest in the properties of the Galois group

\[
G_{K,S} = G_S(K) = \text{Gal}(K_S/K),
\]

where \( K_S \) is the maximal extension of \( K \), which is unramified outside the primes in \( S \). Although it is conjectured that \( G_{K,S} \) is topologically finitely generated, details there of remain largely unknown. However, it has been proved that \( G_{K,S} \) is topologically generated by finitely many conjugacy classes. This result can be proved in two ways.

First, this result can be deduced from the result obtained by Ihara [1].

Theorem 1.1. (Proposition 1 of [1]) Assume that \( k \) is an algebraic number field and \( M/k \) is an infinite unramified Galois extension of \( k \). Let \( p \) be a finite prime of \( k \) and \( f(p) \) be the residue extension degree of \( p \) in \( M/k \). Define \( T(M/k) := \{ p | p \in \text{Spec} \, O_k, f(p) < \infty \} \). Then, we have

\[
\sum_{p \in T(M/k)} \frac{\log N(p)}{N(p)f(p)-1} \leq C_k
\]

for some constant \( C_k \) depending on \( k \), i.e., the expression on the left is convergent.

From the above theorem, we know that the Galois group \( G_{K,S} \) can be topologically generated by a finite number of conjugacy classes; refer to Corollary 10.9.11

2010 Mathematics Subject Classification. Primary 11R99.
Key words and phrases. Minimal number of generators and Frobenius elements.
of [2]. Moreover, in the proof of this corollary, we also know that the Galois group \( \text{Gal}(K_{ur}/K) \) is generated by finitely many Frobenius classes, where \( K_{ur} \) is the maximal unramified extension of \( K \). (Note that a conjugacy class does not need to be a Frobenius class in the case of infinite extensions.)

Some aspects of the proof of Ihara’s theorem appear to closely approximate a bound of the set of conjugacy classes generating \( G_{K,S} \). Let \( G_{ab}^{\text{K,S}} \) be the abelianization of \( G_{K,S} \), i.e., \( G_{ab}^{\text{K,S}} = \text{Gal}(K_{ab}^{\text{S}}/K) \) where \( K_{ab}^{\text{S}} \) is the maximal abelian extension of \( K \), which is unramified outside the primes in \( S \). The fact that \( G_{ab}^{\text{K,S}} \) is finitely generated means that the following purely group theoretical result yields not only the alternative proof but also the effective bound of the set of generators of \( G_{K,S} \).

**Theorem 1.2.** (Guralnick, Weiss, Theorem 10.2.6 in [2]) Let \( G \) be a profinite group with abelianization of rank \( r \). Then, \( G \) can be topologically generated by \( r \) (or \( 1 \) if \( r = 0 \)) conjugacy classes.

From the above theorem, we know that \( G_{K,S} \) can be topologically generated by \( r \) (or \( 1 \) if \( r = 0 \)) conjugacy classes. Now, two natural questions arise.

1. Considering that the proof that \( G_{K,S} \) can be topologically generated by a finite number of conjugacy classes already exists, is the Galois group \( G_{K,S} \) also generated by a finite number of conjugacy classes of the Frobenius elements?

2. If \( G_{K,S} \) can be generated by a finite number of conjugacy classes of the Frobenius elements, what is the minimal number of generators?

In this article, we prove the following theorem by using topological methods.

**Theorem 1.3.** Let \( K \) be a number field and \( S \) be the finite set of primes of \( K \). Define \( G_{K,S} = \text{Gal}(K_S/K) \), where \( K_S \) is the maximal extension of \( K \), which is unramified outside the primes in \( S \). Suppose that the rank of \( G_{ab}^{\text{K,S}} \) is \( r \). Then, \( G_{K,S} \) can be generated by \( r \) (or \( 1 \) if \( r = 0 \)) conjugacy classes of Frobenius elements of \( G_{K,S} \).

**2. Proof of Theorem 1.3**

2.1. **A new topology in** \((\text{Spec } O_K) \setminus S\). Let \( \text{Spec } O_K \) be the set of prime ideals of \( O_K \), where \( O_K \) is the ring of integers of \( K \). When we think about the topology of \( (\text{Spec } O_K) \), we generally think about the Zariski topology. In this section, we define a new topology on \( (\text{Spec } O_K) \setminus S \).

Define

\[ T := \{ p \mid p \text{ is a prime number and } p\text{-part of } G_{ab}^{\text{K,S}} \text{ is nontrivial} \}. \]

Since \( G_{ab}^{\text{K,S}} \) is finitely generated, \( P \) is a finite set, i.e., \( T = \{ p_1, p_2, \ldots, p_m \} \).

Let us consider the finite quotients of \( G_{K,S} \). Then, they can be roughly classified as follows:

- The largest elementary abelian \( p_i \)-quotient of \( G_{K,S} \) for each \( p_i \in T \).
- A finite nonabelian simple quotient of \( G_{K,S} \).

(Note that every quotient of \( G_{K,S} \) has at least one quotient in the above.) Now,
Kwang-Seob Kim  
Minimal number of generators of $G_{K,S}$

let us define some field extensions of $K$.

i) Let $P_i$ be the largest elementary abelian $p_i$-quotient of $G_{S}(K)$ for each $p_i \in T$. Then, $P_i$ corresponds to a Galois extension $F_i/K$ which is the $P_i$-extension of $K$ unramified outside $S$. Here is a diagram.

\[
\begin{array}{ccc}
K & K_{S}^{ab} & G_{K,S}^{ab} \\
| & | & | \\
| & | & \downarrow \\
| & | & G_{K,S} \\
K_p & F_i & G_{K,S}^{ab} \\
| & | & | \\
| & | & \downarrow \\
| & | & F_i \\
K & K_{S}^{ab} & G_{K,S}^{ab} \\
| & | & | \\
| & | & \downarrow \\
| & | & F_i \\
K
\end{array}
\]

By the definition of $P_i$,

$$P_i \simeq \prod_{j=1}^{r_i} \mathbb{Z}/p_i \mathbb{Z}. $$

Define $F_{i,j}$ as the Galois extension of $K$ corresponding to $\mathbb{Z}/p_i \mathbb{Z}$ for each $j$.

Then $P_i$ can be written as the following.

$$P_i \simeq \text{Gal}(F_i/K) \simeq \text{Gal}(F_{i,1}F_{i,2} \cdots F_{i,r_i}/K) \simeq \prod_{j=1}^{r_i} \text{Gal}(F_{i,j}/K),$$

where $r_i$ is the rank of $P_i$ and $F_{i,j}$ is a $\mathbb{Z}/p_i \mathbb{Z}$-extension of $K$ for each $j$. We easily verify that $r := \max(r_1, r_2, \ldots, r_n)$ is the rank of $G_{S}^{ab}(K)$. Define $L_i := F_{i,1}$ and $G_i := \text{Gal}(F_{i,1}/K)$ for $1 \leq i \leq n$.

ii) The finite nonabelian simple quotient of $G_{S}(K)$ corresponds to a finite non-abelian simple extension of $K$, which is unramified outside $S$. Then, there is a possibility that $K$ has infinitely many such extensions and let $\mathcal{R}$ be the set comprising these extensions. If we assume that $\mathcal{R}$ is an infinite set, then $\mathcal{R}$ can be represented as follows:

$$\mathcal{R} = \{M_i | M_i/K \text{ is unramified outside } S \text{ and } \text{Gal}(M_i/K) \text{ is nonabelian simple.}\}$$

for each $1 \leq i < \infty$. Define $L_{m+i} := M_i$ and $G_{m+i} := \text{Gal}(M_i/K)$ for $1 \leq i < \infty$. 

3
Now, let $\hat{L}$ be the compositum of all $L_i$’s ($1 \leq i < \infty$). Then,

$$\text{Gal}(\hat{L}/K) \simeq \prod_{i=1}^{\infty} \text{Gal}(L_i/K).$$

We want to define a topology in the Galois group $\text{Gal}(\hat{L}/K)$. First, let us define a topology in the Galois group $\text{Gal}(L_i/K)$ for each $i$. $\text{Gal}(L_i/K)$ can be represented as a union of two sets $C_{i,1}$ and $C_{i,2}$, where $C_{i,1}$ is the set of the identity $\{e\}$ and $C_{i,2}$ is the union of all non-trivial conjugacy classes of $\text{Gal}(L_i/K)$. We define $C_{i,1}$ and $C_{i,2}$ as the open basis for $\text{Gal}(L_i/K)$. Then, we easily verify that $\text{Gal}(L_i/K)$ is a topological space and is compact for all $i$. Finally, we present the product topology in $\text{Gal}(\hat{L}/K)$ and this topological space is also compact by the Tychonoff theorem.

Next, we define a topology in $(\text{Spec } O_K) \setminus S$. Let $S_i$ be the set of primes of $K$, which splits completely in $L_i/K$ and let $N_i$ be the set of primes of $(\text{Spec } O_K) \setminus S$ which does not split completely in $L_i/K$ for all $i$. (Note that $(\text{Spec } O_K) \setminus S = S_i \cup N_i$).

Now, we define all of the finite intersections of $S_i$ and $N_j$ as the open basis for $(\text{Spec } O_K) \setminus S$ for all $i$ and $j$.

### 2.2. Compactness of $(\text{Spec } O_K) \setminus S$. By the Chebotarev density theorem, there is a natural correspondence between the open basis of $(\text{Spec } O_K) \setminus S$ and that of $\text{Gal}(\hat{L}/K)$:

First, let us determine the correspondence between $S_i$ (resp. $N_i$) and $C_{i,1}$ (resp. $C_{i,2}$). Then the following hold.

\begin{equation}
\{\text{open basis of } (\text{Spec } O_K) \setminus S\} \leftrightarrow \{\text{open basis of } \text{Gal}(\hat{L}/K)\}
\end{equation}

\begin{equation}
S_i \leftrightarrow C_{i,1} \times \prod_{k=1,k\neq i}^{\infty} \text{Gal}(L_k/K) \quad \text{and} \quad N_i \leftrightarrow C_{i,2} \times \prod_{k=1,k\neq i}^{\infty} \text{Gal}(L_k/K).
\end{equation}

From the Chebotarev density theorem, we also know that the whole space $(\text{Spec } O_K) \setminus S$ corresponds to the whole space $\text{Gal}(\hat{L}/K)$:

\begin{equation}
(\text{Spec } O_K) \setminus S \leftrightarrow \text{Gal}(\hat{L}/K) \quad \text{and} \quad \text{the empty set} \leftrightarrow \text{the empty set}.
\end{equation}
Similarly, we verify the correspondence between the intersection of an open basis of \((\text{Spec } O_K) \setminus S\) and the intersection of an open basis of \(\text{Gal}(\hat{L}/K)\). For example,

\[
\{\text{open basis of } (\text{Spec } O_K) \setminus S\} \iff \{\text{open basis of } \text{Gal}(\hat{L}/K)\}
\]

\[
S_i \cap S_j \leftrightarrow C_{i,1} \times C_{j,1} \times \prod_{k=1, k \neq i, j}^{\infty} \text{Gal}(L_k/K)
\]

\[
N_i \cap N_j \leftrightarrow C_{i,2} \times C_{j,2} \times \prod_{k=1, k \neq i, j}^{\infty} \text{Gal}(L_k/K)
\]

\[
S_i \cap N_j \leftrightarrow C_{i,1} \times C_{j,2} \times \prod_{k=1, k \neq i, j}^{\infty} \text{Gal}(L_k/K)
\]

(2.3)

\[
N_i \cap S_j \leftrightarrow C_{i,2} \times C_{j,1} \times \prod_{k=1, k \neq i, j}^{\infty} \text{Gal}(L_k/K)
\]

for any \(i\) and \(j\). This correspondence is well defined since the Chebotarev density theorem implies that a Galois extension of \(K\) is uniquely determined by the set of primes of \(K\) that split completely in it. Thus, there is a natural one-to-one correspondence between the open basis of \((\text{Spec } O_K) \setminus S\) and that of \(\text{Gal}(\hat{L}/K)\).

Let \(V\) be an arbitrary open set of \(\text{Gal}(\hat{L}/K)\). Then \(V\) can be written as the union of the open basis of \(\text{Gal}(\hat{L}/K)\), i.e., \(V = \cup B_\alpha\), where \(B_\alpha\) are open bases of \(\text{Gal}(\hat{L}/K)\). We know that for each \(B_\alpha\) in \(\text{Gal}(\hat{L}/K)\), there is a corresponding open basis \(C_\alpha\) in \((\text{Spec } O_K) \setminus S\). Let \(U := \cup C_\alpha\). Then \(V\) corresponds to \(U\).

Similarly, for an arbitrary open set \(U\) of \((\text{Spec } O_K) \setminus S\), we also know that there exists a corresponding open set \(V\) in \(\text{Gal}(\hat{L}/K)\).

From this correspondence, we know that there is a natural one-to-one correspondence between an arbitrary open set \(U\) of \((\text{Spec } O_K) \setminus S\) and an open set \(V\) of \(\text{Gal}(\hat{L}/K)\). Let \(\mathfrak{U}\) be an open cover of \((\text{Spec } O_K) \setminus S\), i.e.,

\[
(\text{Spec } O_K) \setminus S \subset \mathfrak{U} = \bigcup U_\alpha.
\]

Define \(V_\alpha\) as the open set of \(\text{Gal}(\hat{L}/K)\) that corresponds to \(U_\alpha\) for all \(\alpha\) and \(\mathfrak{V}\) as \(\bigcup V_\alpha\). Then \(\mathfrak{V}\) is an open cover of \(\text{Gal}(\hat{L}/K)\), i.e.,

\[
\text{Gal}(\hat{L}/K) \subset \mathfrak{V} = \bigcup V_\alpha.
\]

Since \(\text{Gal}(\hat{L}/K)\) is a compact space, it has a finite subcover, i.e.,

\[
\text{Gal}(\hat{L}/K) \subset (V_{\alpha_1} \cup V_{\alpha_2} \cup \cdots \cup V_{\alpha_l}).
\]

Let \(U_{\alpha_1}\) be the corresponding open set of \(V_{\alpha_1}\). Then we know that there is a correspondence

\[
(\cup_{\alpha_1} \cup U_{\alpha_2} \cup \cdots \cup U_{\alpha_l}) \leftrightarrow (V_{\alpha_1} \cup V_{\alpha_2} \cup \cdots \cup V_{\alpha_l}).
\]

(2.4)

Since \((V_{\alpha_1} \cup V_{\alpha_2} \cup \cdots \cup V_{\alpha_l})\) is the whole space \(\text{Gal}(\hat{L}/K)\), we know that \((U_{\alpha_1} \cup U_{\alpha_2} \cup \cdots \cup U_{\alpha_l}) = (\text{Spec } O_K) \setminus S\). (See (2.2)). In conclusion, we can deduce that the topological space \((\text{Spec } O_K) \setminus S\) is also compact.
2.3. **Proof of Theorem 1.3.** First, we assume that the rank \( r \) of \( G_{K,S}^{ab} \) is nonzero. Now, we define a sequence \( \{X_i\} \) of closed subsets in \((\text{Spec } O_K) \setminus S:\)

- Define \( X_1 \) as \( N_1 \) and \( X_i \) as \( \cap_{j=1}^i N_j \), i.e., \( X_i \supset X_{i+1} \).

By the Chebotarev density theorem, we know that \( X_i \) is nonempty for each \( i \). Since \((\text{Spec } O_K) \setminus S\) is compact, we know that

\[
X := \bigcap_{i=1}^{\infty} X_i \neq \emptyset
\]

by Cantor’s intersection theorem.

Now, let us select a nontrivial element \( p \in X \). By definition of \( X_i \), \( p \) is contained in \( N_i \) for all \( i \), i.e., \( p \) does not split completely in all \( L_i/K \). Since each Gal\((L_i/K)\) is a simple group and the Frobenius element of \( p \) is nontrivial, the Frobenius element of \( p \) generates Gal\((L_i/K)\) for all \( i \). Now, let us think about the Frobenius element of \( p \) and recall the Galois group Gal\((\hat{L}/K)\). This Galois group is the direct product of the abelian part \( \prod_{m=1}^i \text{Gal}(L_i/K) \) and the non-solvable part \( \prod_{i=m+1}^{\infty} \text{Gal}(L_i/K) \).

Let us evaluate the abelian part. Since \( \prod_{i=1}^m \text{Gal}(L_i/K) \simeq \prod_{i=1}^m \mathbb{Z}/p_i \mathbb{Z} \) and each \( p_i \) are distinct, we easily verify that the Frobenius element of \( p \) generates the whole group \( \prod_{i=1}^m \text{Gal}(L_i/K) \).

Next, let us consider the non-solvable part. Since each Gal\((L_i/K)\) is a non-abelian simple group and the Frobenius element of \( p \) corresponds to a non-trivial conjugacy class in each Gal\((L_i/K)\), the normal subgroup generated by the Frobenius element of \( p \) is the whole group \( \prod_{i=m+1}^{\infty} \text{Gal}(L_i/K) \), i.e., the Frobenius element of \( p \) generates the whole group \( \prod_{i=m+1}^{\infty} \text{Gal}(L_i/K) \).

In conclusion, the Frobenius element of \( p \) generates Gal\((\hat{L}/K)\). Now, let us recall the definition of \( F_{i,j} \) in Section 2.1. To simplify the notation, we write \( F' \) instead of \( \left( \prod_{i=1}^m \prod_{j=2}^{i-1} F_{i,j} \right) \). Then, we verify that the rank of Gal\((F'/K)\) is \( r - 1 \). Since \( F'/K \) is a finite abelian extension, there exist \( r - 1 \) conjugacy classes of the Frobenius elements \( \text{Frob}_{p_1}, \text{Frob}_{p_2}, \ldots, \text{Frob}_{p_{r-1}} \), which generate Gal\((F'/K)\). (Note that \( r - 1 \) is the minimal number of generators.) The primes \( p_1, p_2, \ldots, p_{r-1} \) can be chosen to be distinct from \( p \) by the Chebotarev density theorem.

Finally, we know that the conjugacy classes of the Frobenius elements of \( p_1, p_2, \ldots, p_{r-1} \) generate \( G_{K,S}^{ab} \), and every nonabelian simple quotient of \( G_{K,S} \). Thus, we know that \( G_{K,S} \) can be generated by conjugacy classes of the Frobenius elements \( \text{Frob}_{p_1}, \text{Frob}_{p_2}, \ldots, \text{Frob}_{p_{r-1}}, \text{Frob}_{p_r} \).

In the case of \( r = 0 \), we can easily verify that the Frobenius element of \( p \) generates the whole group \( G_{K,S} \).

**Acknowledgement**

I would like to thank my advisor, Minhyong Kim, for introducing me to this problem and his steadfast encouragement.
REFERENCES


School of Mathematics, Korea Institute for Advanced Study, Seoul, Korea, 130-722

E-mail address: kwang12@kias.re.kr