Constructing PGL(2, 7)-extensions with restricted ramifications

Masanari Kida*and Nozomu Suzuki

May 9, 2024

Abstract

By specializing regular polynomial with Galois group PGL(2, 7) and using Newton polygon technique, we construct PGL(2, 7)-extensions over $\mathbb{Q}$ unramified over their unique quadratic subfields. The Galois group over the quadratic field is a simple group PSL(2, 7).

Keywords: unramified extension, quadratic field, regular extension.

1 Introduction

Unramified abelian extensions over a number field are well described by class field theory. However, no unified description is known for unramified nonabelian extensions. Despite this situation, many examples of unramified nonabelian extensions are known, especially over quadratic fields. Among these examples, Yamamoto's classical result [14] shows that infinitely many real quadratic fields have unramified A_n-extensions for $n \geq 3$, and its extension by Yamamura [15] is worth mentioning as well. Recently, a systematic method to generate such extensions was found in [1] based on the idea of [5], and applied to the construction of an easily describable infinite family from certain regular polynomials. Another technique for such construction can be found in [4].

The aim of this paper is to construct PGL(2, 7)-extensions over $\mathbb{Q}$ providing unramified PSL(2, 7)-extensions over the unique quadratic subfields. There are several literature on unramified PSL(2, 7)-extensions over quadratic fields and the above-mentioned [4] is one of them. In that paper, the authors construct unramified PSL(2, 7)-extensions over quadratic fields with the Galois group isomorphic to $C_2 \times$ PSL(2, 7). Our approach is quite different: starting from a regular realization of PGL(2, 7)-extension, we deduce ramification information using Newton polygon to construct such unramified extensions.

*This work was supported by JSPS KAKENHI Grant Number 20K03521.

2020 *Mathematics Subject Classification.* Primary 12F12; Secondary 11R09, 11R32.

There are several researches on $\mathrm{PGL}(2,7)$-extension recently. We mention to two of them. In the paper [3], they study $\mathrm{PGL}(2,7)$-extensions defined by a similar polynomial as ours imposing local conditions. Our study is different in purpose and we need wider range of parameter variation. On the other hand, in the paper [10], the authors construct $\mathrm{PGL}(2,7)$-extensions ramified only at one prime using non-liftable modular forms of positive characteristic.

The outline of this paper is as follows. In Section 2, we give some preliminaries on regular $\mathrm{PGL}(2,7)$-polynomials and on the Newton polygon method to deduce ramification properties of these polynomials. In Section 3, based on the above-developed technique, we analyze prime decomposition in $\mathrm{PGL}(2,7)$-extension, and in particular, we compute the decomposition groups and the inertia groups of at most tamely ramified primes. In Section 4, we construct $\mathrm{PGL}(2,7)$-extensions with only one ramified prime and unramified $\mathrm{PSL}(2,7)$-extensions over quadratic fields by using the results in Section 3.

Throughout this paper, we mean by a number field a finite extension of the field of rational numbers $\mathbb{Q}$. For a number field K, we denote by D_K the discriminant of K, by $\mathfrak{O}_K$ the ring of integers of K, and by $\widetilde{K}$ the Galois closure of K over $\mathbb{Q}$. For a rational prime p, we denote by v_p the p-adic (exponential) valuation. For a prime ideal $\mathfrak{p}$ of a number filed K lying above p, we denote the ramification index and the inertia degree by $e(\mathfrak{p}/p)$ and $f(\mathfrak{p}/p)$, respectively.

All computation in this paper has been done by Magma [2].

2 Preliminaries

Our study on arithmetic of $\mathrm{PGL}(2,7)$-extensions is based on the polynomial

$$F(T,X) = X^8 + X^7 + 7X^6 - TX - T \ \in \ \mathbb{Q}(T)[X] \tag{2.1}$$

given in [8, Table 6 in Appendix]. Here, we consider $\mathrm{PGL}(2,7)$ as a transitive subgroup of S_8:

$$\mathrm{PGL}(2,7) \simeq \langle (3\ 4\ 6\ 5\ 7\ 8), (1\ 8\ 2)(4\ 5\ 6) \rangle \subset S_8.$$

In the below, we identify these two groups. The above regular polynomial is computed by the rigidity method described as [8, Chapter I]. We shall explain the method briefly.

Definition 2.1 ([12])**.** Let G be a finite group and $r(\geq 3)$ an integer. An r-point *Hurwitz parameter* is a triple $h = (G, C, \nu)$ consisting of

- $C = (\Gamma_1, \ldots, \Gamma_k)$ is a k-tuple of distinct conjugacy classes of G,
- $\nu = (\nu_1, \ldots, \nu_k)$ is a partition of r

satisfying the two conditions

- $\Gamma_1, \ldots, \Gamma_k$ generate G,
- $\prod [\Gamma_i]^{\nu_i} = 1$ holds in the abelianization G^{ab}.

When G is clear from the context, we write $h = (C, \nu)$ for simplicity.

If a Hurwitz parameter satisfies so-called the rigidity, rationality, and genus-zero conditions, then we can obtain the polynomial over $\mathbb{Q}(T)$ of the form

$$f_0(X) - T \cdot f_\infty(X) \quad (f_0, f_\infty \in \mathbb{Q}[X])$$

defining a G-extension (see [8, Chapter I]).

The conjugacy classes of $\mathrm{PGL}(2,7)$ are listed in Table 1.

Table 1: Conjugacy classes of $\mathrm{PGL}(2,7)$

Class	order	length	representative
c_1	1	1	id
c_2	2	21	(1 6)(2 4)(3 7)(5 8)
c_3	2	28	(1 7)(2 4)(3 8)
c_4	3	56	(1 8 2)(4 5 6)
c_5	4	42	(1 5 6 8)(2 7 4 3)
c_6	6	56	(1 3 4 7 8 2)
c_7	7	48	(1 5 3 7 6 8 2)
c_8	8	42	(1 7 5 4 6 3 8 2)
c_9	8	42	(1 4 8 7 6 2 5 3)

The $\mathrm{PGL}(2,7)$-polynomial (2.1) is computed from the three-point Hurwitz parameter $(C, \nu) = ((c_3, c_6, c_7), (1, 1, 1))$. There are 3 other three-point Hurwitz parameters giving rise to $\mathrm{PGL}(2,7)$-polynomials. They are

$$(C, \nu) = ((c_6, c_4), (2, 1)),\ ((c_6, c_2), (2, 1)),\ ((c_3, c_5, c_6), (1, 1, 1)).$$

Each parameter respectively leads to

$$\begin{aligned}
&X^6(X^2 + 9X + 21) - T(7X^2 - 9X + 3),\\
&X^6(X^2 + 6X + 21) + T(7X^2 - 12X + 12),\\
&(X^2 + 63)^4 - T(7X^2 + 18X + 567).
\end{aligned}$$

As our main task in this paper is to study the decomposition of rational primes in $\mathrm{PGL}(2,7)$-extensions obtained by specializations of (2.1) by the aid of Newton polygons, we recall the definition of a Newton polygon. Let $p \in \mathbb{Z}$ be a fixed rational prime and $f(X) = \sum a_i X^i \in \mathbb{Q}_p[X]$. The lower convex envelope Γ of the set of points $\{(i, v_p(a_i))\}$ in $\mathbb{R}^2$ is called the Newton polygon of f with respect to p. Let $S_1, \ldots, S_g$ be the segments of Γ.

To state a theorem of Ore, which is a key tool of our study, we need additional definitions. We further assume that $f(X) \in \mathbb{Z}[X]$ is a monic polynomial. In this case, the Newton polygon decreases monotonically to the horizontal axis. For a segment S_i of Γ starting from $(s, v_p(a_s))$ ending at $(t, v_p(a_t))$ $(s < t)$, we set $E_i = t-s$ and $H_i = v_p(a_s) - v_p(a_t)$. Let $d_i = \gcd(E_i, H_i)$, $e_i = E_i/d_i$, and $h_i = H_i/d_i$. We define the integer sequence $(b_j)_{0 \le j \le d_i}$ by

$$b_j = \begin{cases} a_{s+je_i}/p^{v_p(a_{s+je_i})} & \text{if } v_p(a_{s+je_i}) = v_p(a_s) - jh_i, \\ 0 & \text{otherwise.} \end{cases}$$

Then the polynomial

$$f_{S_i}(Y) = \sum_{j=0}^{d_i} b_{d_i - j} Y^j$$

is called the *associated polynomial* of the segment S_i (see [6, p.32]). If the discriminant of f_{S_i} is not divisible by p, then f is called S_i*-regular*. If f is S_i-regular for all segments S_i of Γ, then f is called Γ*-regular*.

Remark 2.2. We add some comments on the above definitions.

We adopt the definition of Newton polygon in [9, p.144], in which the points are taken in the reverse order of [6]. By adopting this definition, our polygon is symmetric about a vertical line with one in [6].

The associated polynomial is defined also in the reverse order from [6]. They relate by $f_{i'}(Y) = Y^{d_i} f_{S_i}(1/Y)$, where $f_{i'}$ on the left hand side is the polynomial defined in [6] and S_i and $S_{i'}$ are the corresponding segments. In the following theorem, we only need the factorization type of $f_{S_i} \pmod p$ and therefore, this definition does not affect the result below.

In the original paper [11] by Ore, the Newton polygon and the associated polynomial are defined using a factor $\varphi(X)$ of $f(X) \pmod p$. By translating $f(X)$ linearly, we may assume $\varphi(X) = X$ and recover the mordern definition of them as in [6].

Theorem 2.3 (Ore [6, Theorem 6])**.** *Keep all the above notation. Then, the decomposition of p in $\mathbb{Q}[X]/(f(X))$ is*

$$(p) = \mathfrak{A}_1^{e_1} \cdots \mathfrak{A}_g^{e_g}.$$

Moreover, for each S_i, if f is S_i-regular and the factorization of f_{S_i} over $\mathbb{F}_p$ is

$$\phi_{i,1}(Y) \cdots \phi_{i,k_i}(Y),$$

then the prime decomposition of $\mathfrak{A}_i$ is

$$\mathfrak{A}_i = \mathfrak{p}_{i,1} \cdots \mathfrak{p}_{i,k_i}, \quad f(\mathfrak{p}_{i,j}/p) = \deg(\phi_{i,j}).$$

Remark 2.4. Theorem 2.3 also holds for a monic polynomial in $\mathbb{Q}[X]$. Let $f(X) = \sum_{i=0}^{d} a_i X^i \in \mathbb{Q}[X]$ be a monic polynomial. If we define $m = \max\{-v_p(a_i) \mid i = 0, \ldots, d\}$, then $g(X) = p^{md} f(X/p^m)$ is a monic polynomial over $\mathbb{Z}_p$. The polynomials $f(X)$ and $g(X)$ have the same number of segments in their Newton polygons with respect to p. The differences between the slopes of the corresponding segments equal m and therefore, they share the same associated polynomial.

3 Decomposition of primes in $\mathrm{PGL}(2,7)$-extensions

Let $F(T, X)$ be the polynomial defined in (2.1) with the discriminant

$$-7^7 T^5 (T + 108)^3. \tag{3.1}$$

We denote by K_t the number field defined by the polynomial $F(t, X)$ specialized by $t \in \mathbb{Q}$. We assume that the Galois group $\mathrm{Gal}(\widetilde{K_t}/\mathbb{Q})$ is isomorphic to $\mathrm{PGL}(2,7)$. In this section, we only consider the case $t \in \mathbb{Z}$. The possible ramifying primes in $K_t/\mathbb{Q}$ divide $-7^7 t^5 (t+108)^3$. In this section, we study the decomposition a rational prime p dividing t in K_t. The other cases will be treated in Section 4. We fix the notation used in this section. If the prime factorization of an ideal $\mathfrak{A}$ of $\mathfrak{O}_{K_t}$ is

$$\mathfrak{A} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \ f_i = f(\mathfrak{p}_i/p),$$

then we say that $\mathfrak{A}$ has the decomposition type

$$(f_1^{e_1}, \ldots, f_g^{e_g})$$

and we write $\mathfrak{A} = (f_1^{e_1}, \ldots, f_g^{e_g})$. Moreover, if $e_i = 1$, then we simply write f_i instead of f_i^1. We denote by $N(\mathfrak{A})$ denote the absolute norm of $\mathfrak{A}$ and by $\left(\frac{\cdot}{p}\right)$ the Legendre symbol. When $p \equiv 1 \mod 3$, then we define $\mathrm{cub}_p = \{x^3 \mid x \in \mathbb{F}_p^\times\}$.

We compute the decompositions of primes in two steps. The following two propositions give the first step.

Proposition 3.1. *Let $p \geq 5$ be a prime not equal to 7. If $v_p(t) > 0$, then the prime p decomposes in K_t as*

$$p\mathfrak{O}_{K_t} = \mathfrak{A}\mathfrak{B}, \ N(\mathfrak{A}) = p^6, N(\mathfrak{B}) = p^2. \tag{3.2}$$

Here the ideal $\mathfrak{B}$ has the factorization

$$\mathfrak{B} = \begin{cases} (1,1) & \text{if } \left(\frac{-3}{p}\right) = 1, \\ (2) & \text{if } \left(\frac{-3}{p}\right) = -1. \end{cases}$$

Proposition 3.2. *The prime 7 decomposes in K_t as follows:*

(i) if $0 < v_7(t) < 7$, *then* $7\mathfrak{O}_{K_t} = (1, 1^7)$.

(ii) if $v_7(t) = 7$, *then*

$$7\mathfrak{O}_{K_t} = \begin{cases} (1,7) & \text{if } n \equiv 1 \mod 7, \\ (1,1,3,3) & \text{if } n \equiv 2,4 \mod 7, \\ (1,1,6) & \text{if } n \equiv 3,5 \mod 7, \\ (1,1,2,2,2) & \text{if } n \equiv 6 \mod 7. \end{cases}$$

(iii) if $v_7(t) > 7$, *then* $7\mathfrak{O}_{K_t} = \mathfrak{A}\mathfrak{B}$ *with* $N(\mathfrak{A}) = 7^6$ *and* $\mathfrak{B} = (1,1)$.

As a second step, we decompose the ideal $\mathfrak{A}$ which remains in the first step.

Proposition 3.3. *Let* $p \geq 5$ *be a rational prime and write* $t = p^{v_p(t)}n \in \mathbb{Z}$. *Let* $\mathfrak{A}$ *be the ideal in Propositions 3.1 and 3.2.*

(i) The case $p \neq 7$*:*

(1) if $\gcd(v_p(t), 6) = 1$, *then* $\mathfrak{A} = (1^6)$.

(2) if $\gcd(v_p(t), 6) = 2$, *then*

$$\mathfrak{A} = \begin{cases} (1^3, 1^3) & \text{if } \left(\frac{7n^{-1}}{p}\right) = 1, \\ (2^3) & \text{if } \left(\frac{7n^{-1}}{p}\right) = -1. \end{cases}$$

(3) if $\gcd(v_p(t), 6) = 3$, *then*

$$\mathfrak{A} = \begin{cases} (1^2, 2^2) & \text{if } 3 \nmid p-1, \\ (1^2, 1^2, 1^2) & \text{if } 3 \mid p-1 \text{ and } 7n^{-1} \in \mathrm{cub}_p, \\ (3^2) & \text{if } 3 \mid p-1 \text{ and } 7n^{-1} \notin \mathrm{cub}_p. \end{cases}$$

(4) if $\gcd(v_p(t), 6) = 6$, *then*

$$\mathfrak{A} = \begin{cases} (1,1,1,1,1,1) & \text{if } 3 \mid p-1,\ 7n^{-1} \in \mathrm{cub}_p \text{ and } \left(\frac{7n^{-1}}{p}\right) = 1, \\ (2,2,2) & \text{if } 3 \mid p-1,\ 7n^{-1} \in \mathrm{cub}_p \text{ and } \left(\frac{7n^{-1}}{p}\right) = -1, \\ (3,3) & \text{if } 3 \mid p-1,\ 7n^{-1} \notin \mathrm{cub}_p \text{ and } \left(\frac{7n^{-1}}{p}\right) = 1, \\ (6) & \text{if } 3 \mid p-1,\ 7n^{-1} \notin \mathrm{cub}_p \text{ and } \left(\frac{7n^{-1}}{p}\right) = -1, \\ (1,1,2,2) & \text{if } 3 \nmid p-1 \text{ and } \left(\frac{7n^{-1}}{p}\right) = 1, \\ (2,2,2) & \text{if } 3 \nmid p-1 \text{ and } \left(\frac{7n^{-1}}{p}\right) = -1. \end{cases}$$

(ii) The case $p = 7$ *and* $v_7(t) > 7$*:*

(1) if $\gcd(v_7(t)-1,6)=1$*, then* $\mathfrak{A}=(6)$.

(2) if $\gcd(v_7(t)-1,6)=2$*, then*

$$\mathfrak{A}=\begin{cases}(1^3,1^3) & \text{if } n\equiv 1,2,4 \mod 7,\\ (2^3) & \text{if } n\equiv 3,5,6 \mod 7.\end{cases}$$

(3) if $\gcd(v_7(t)-1,6)=3$*, then*

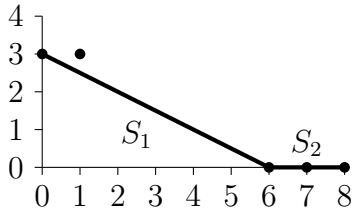
$$\mathfrak{A}=\begin{cases}(1^2,1^2,1^2) & \text{if } n\equiv \pm 1 \mod 7,\\ (3^2) & \text{if } n\not\equiv \pm 1 \mod 7.\end{cases}$$

(4) if $\gcd(v_7(t)-1,6)=6$*, then*

$$\mathfrak{A}=\begin{cases}(1,1,1,1,1,1) & \text{if } n\equiv 1 \mod 7,\\ (3,3) & \text{if } n\equiv 2,4 \mod 7,\\ (6) & \text{if } n\equiv 3,5 \mod 7,\\ (2,2,2) & \text{if } n\equiv 6 \mod 7.\end{cases}$$

We shall prove these propositions at the same time.

Proof of Propositions. Let p be a prime $\neq 7$. For $t\in\mathbb{Z}$ with $v_p(t)>0$, the Newton polygon of $F(t,X)$ with respect to p is as follows.



Let us denote the segments of the Newton polygon with the horizontal length 6 and 2 by S_1 and S_2, respectively. Then S_1 corresponds to $\mathfrak{A}$ and S_2 corresponds to $\mathfrak{B}$ in the notation of Proposition 3.1. To decompose $\mathfrak{B}$ by using Ore's theorem (Theorem 2.3), we consider the factorization of the associated polynomial

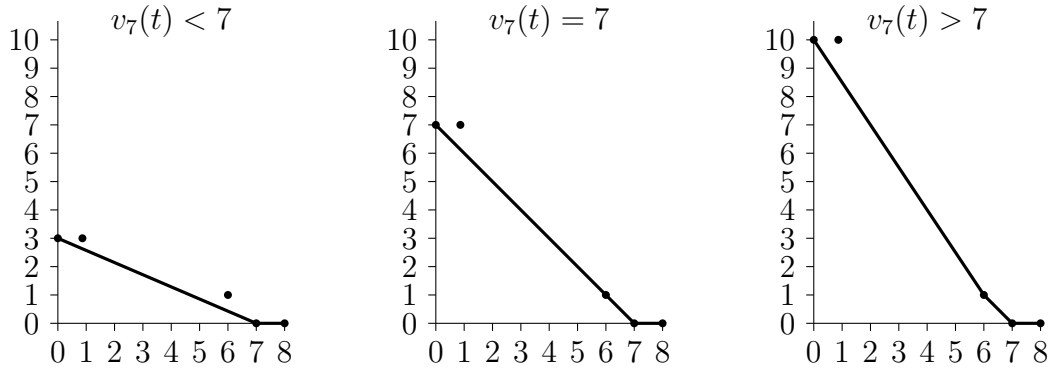
$$F_{S_2}(Y)=7Y^2+Y+1$$

of S_2 in $\mathbb{F}_p$ with $\mathrm{Disc}(F_{S_2})=-3^3$. Since $2\neq 0$ in $\mathbb{F}_p$, we have

$$7\cdot 2^2 F_{S_2}(Y)=(7\cdot 2Y+1)^2+27.$$

This implies that F_{S_2} is reducible in $\mathbb{F}_p$ if and only if $\left(\frac{-27}{p}\right)=\left(\frac{-3}{p}\right)=1$. This proves Proposition 3.1.

On the other hand, the possible Newton polygon with respect to $p=7$ is one of the following forms.



If $v_7(t) > 7$, then the Newton polygon has a segment with the horizontal lengths of 6 and two segments with the horizontal length of 1. This proves Proposition 3.2 (iii) for the case $v_7(t) > 7$. If $v_7(t) \leq 7$, then the Newton polygon has segments of the horizontal length 1 and 7. This shows that 7 decomposes as

$$7\mathfrak{O}_K = \mathfrak{A}\mathfrak{q},\ N(\mathfrak{A}) = 7^7$$

where $\mathfrak{q}$ is a prime of K_t. This completes the proof of (i) in Proposition 3.2.

It remains to decompose the ideal $\mathfrak{A}$. For our purpose, we use Theorem 2.3. We demonstrate the computation only for the cases:

(i) The case when $p \neq 7$ and $\gcd(v_p(t), 6) = 3$;

(ii) the case when $p \neq 7$, $3 \nmid (p-1)$ and $\left(\frac{7n^{-1}}{p}\right) = -1$.

While the case (i) covers the generic cases, the case (ii) needs some careful arguments.

We begin with case (i). In this case, the associated polynomial of S_1 is

$$F_{S_1}(Y) = -nY^3 + 7$$

with $n = t \cdot p^{-v_p(t)}$. The discriminant of the above polynomial is $-3^3 7^2 n^2$. Thus we can apply Theorem 2.3 to the polynomial. If $3 \nmid p-1$, then $\mathbb{F}_p$ has no primitive third roots of unity. This implies that F_{S_1} has only one root in $\mathbb{F}_p$ for all n. On the other hand, if $3 \mid p-1$, then $\mathbb{F}_p$ has a primitive third root of unity. This implies that F_{S_1} has a root in $\mathbb{F}_p$ if and only if F_{S_1} has 3 roots in $\mathbb{F}_p$. Thus we have obtained

$$F_{S_1}(Y) = \begin{cases} (\text{degree1}) \times (\text{degree2}) & \text{if } 3 \nmid p-1, \\ (\text{degree1}) \times (\text{degree1}) \times (\text{degree1}) & \text{if } 3 \mid p-1,\ 7n^{-1} \in \text{cub}_p, \\ (\text{degree3}) & \text{if } 3 \mid p-1,\ 7n^{-1} \notin \text{cub}_p. \end{cases}$$

This shows the decomposition of $\mathfrak{A}$.

For the case (ii), the decomposition type of $\mathfrak{A}$ is given by the associated polynomial $-nY^6 + 7$. We have to consider the splitting field of the polynomial. A decomposition of the polynomial to quadratic factors in an algebraic closure $\overline{\mathbb{F}_p}$ is

$$Y^6 - 7^{-1}n = (Y^2 - b)(Y^2 - b\omega)(Y^2 - b\omega^2),$$

where $b \in \mathbb{F}_p$ and ω is a primitive third root of unity. This implies that the degree of the splitting field of $-nY^6+7$ is 2. On the other hand, $-nY^6+7$ has no degree one factors, because $\left(\frac{7n^{-1}}{p}\right) = -1$. Hence, the irreducible decomposition of $-nY^6+7$ consists of three degree 2 irreducible factors over $\mathbb{F}_p$, and thus, the decomposition type of $\mathfrak{A}$ is $(2,2,2)$. □

If a prime divisor p of t ramifies tamely in $K_t/\mathbb{Q}$, then we can calculate the decomposition and inertia groups in Galois closure $\widetilde{K_t}$. Let K be a Galois extension over $\mathbb{Q}$ with Galois group G. For a prime p and a prime ideal $\mathfrak{p}$ in K lying over p, we denote the decomposition group by $Z(\mathfrak{p}/p)$ and the inertia group by $T(\mathfrak{p}/p)$. We simply write Z and T if no confusion can occur.

The decomposition and inertia groups have the following fundamental properties:

- The both groups are subgroups of the Galois group G;
- The group $T(\mathfrak{p}/p)$ is normal in $Z(\mathfrak{p}/p)$;
- The quotient Z/T is cyclic;
- If p ramifies tamely, then the group T is cyclic.

By using the following lemma, we can calculate ramification indices and inertia degrees in $K_t/\mathbb{Q}$ from the pair (Z,T).

Lemma 3.4 ([13]). *Let K be a number field and $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. We denote by H the subgroup of G fixing K. Let p be a prime. For a prime ideal $\mathfrak{P}$ of $\widetilde{K}$ lying above p, we denote by Z and T the decomposition and the inertia groups of $\mathfrak{P}$, respectively. Then there is a one-to-one correspondence between the double cosets $Z\backslash G/H$ and the distinct prime ideals in K lying above p. For a prime ideal $\mathfrak{p}$ of K corresponding to $Z\sigma H$, the following equalities hold:*

$$e(\mathfrak{p}/p)f(\mathfrak{p}/p) = (\sigma^{-1}Z\sigma : \sigma^{-1}Z\sigma \cap H);$$
$$e(\mathfrak{p}/p) = (\sigma^{-1}T\sigma : \sigma^{-1}T\sigma \cap H).$$

By applying Lemma 3.4 to K_t and $\widetilde{K_t}$, we obtain the possible pairs (Z,T) for the decomposition types of the tamely ramified primes in $K_t/\mathbb{Q}$.

We explain the notation in Table 2 and Table 3.

Table 2 contains the all subgroups of $\mathrm{PGL}(2,7)$ up to conjugacy. In the table, the "length" column contains the conjugacy length of the group. Figure 1 shows the subgroup lattice of $\mathrm{PGL}(2,7)$, which is downloadable from

`https://people.maths.bris.ac.uk/~matyd/GroupNames/321/PGL(2,7).html`.

Table 2: Subgroups of $\mathrm{PGL}_2(7)$.

No.	subgroups	generators	order	length	No.	subgroups	generators	order	length
1	C_1	(1)	1	1	14	D_4	(1 6 4 7)(2 5 3 8), (1 8)(2 7)(3 6)(4 5)	8	21
2	C_2	(1 3)(2 4)(5 6)(7 8)	2	21					
3	C_2	(1 7)(2 6)(3 5)	2	28	15	D_4	(1 3 2 5)(4 7 6 8), (1 5)(2 3)(7 8)	8	21
4	C_3	(3 7 6)(4 8 5)	3	28					
5	C_7	(1 6 8 5 4 7 2)	7	8	16	C_8	(1 6 5 7 2 4 3 8)	8	21
6	C_2^2	(1 3)(2 4)(5 6)(7 8), (1 4)(2 3)(5 8)(6 7)	4	14	17	A_4	(3 7 6)(4 8 5), (1 8)(2 7)(3 6)(4 5)	12	14
7	C_4	(1 6 4 7)(2 5 3 8)	4	21	18	D_6	(2 4 8 7 3 5), (1 6)(2 8)(5 7)	12	28
8	C_2^2	(1 5)(2 3)(7 8), (1 2)(3 5)(4 6)(7 8)	4	42					
					19	F_7	(1 6 3 7 2 5), (1 4 7 6 3 5 2)	42	8
9	C_6	(1 6 3 7 2 5)	6	28					
10	S_3	(1 6)(2 8)(5 7), (2 8 3)(4 7 5)	6	28	20	D_8	(1 6 5 7 2 4 3 8), (1 5)(2 3)(7 8)	16	21
11	S_3	(1 3)(2 4)(5 6)(7 8), (1 4 5)(2 3 6)	6	28	21	S_4	(1 6 4 7)(2 5 3 8), (3 7 6)(4 8 5)	24	14
12	D_7	(1 7)(2 6)(3 5), (1 4 7 6 3 5 2)	14	8	22	$\mathrm{PSL}_2(7)$	(1 5)(2 8)(3 6)(4 7), (1 5 7 6)(2 4 8 3)	168	1
13	$C_7 \rtimes C_3$	(1 5 8)(2 6 7), (1 6 8 5 4 7 2)	21	8	23	$\mathrm{PGL}_2(7)$	(1 6)(2 4)(3 7)(5 8), (1 2 3 8 6 4)	336	1

Figure 1: The lattice of subgroups of $\mathrm{PGL}_2(7)$.

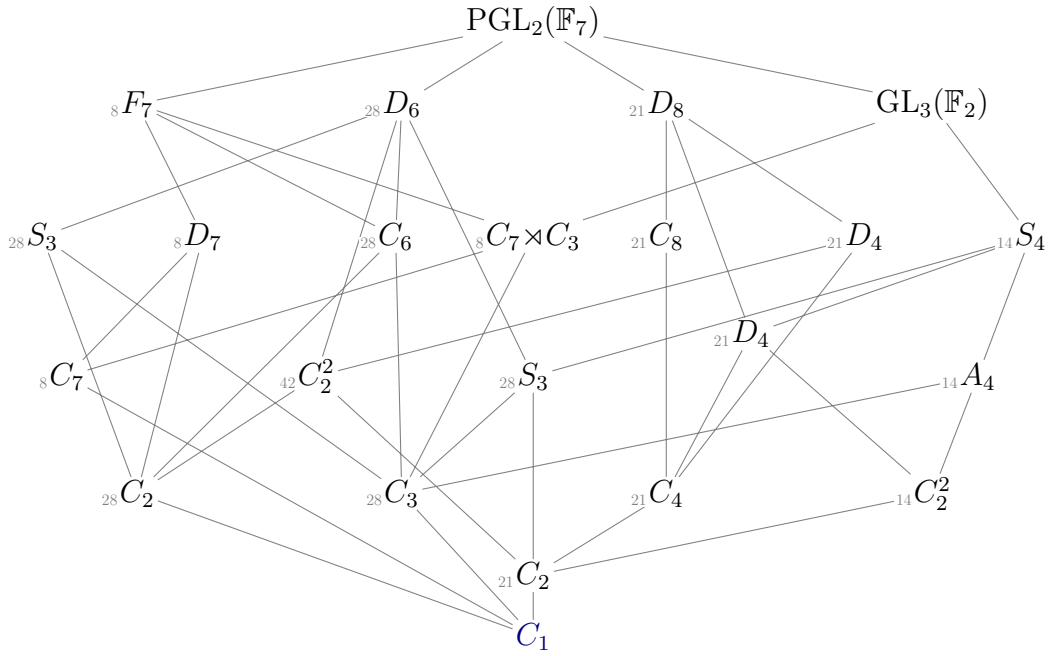


Table 3: The decomposition and inertia groups.

Z	T	decomposition type	$v_p(D_{K_t})$
C_1	C_1	$(1,1,1,1,1,1,1,1)$	0
C_2(No.3)	C_1	$(1,1,2,2,2)$	0
C_3	C_1	$(1,1,3,3)$	0
C_6	C_1	$(1,1,6)$	0
C_2(No.3)	C_2(No.3)	$(1,1,1^2,1^2,1^2)$	3
C_6	C_2(No.3)	$(1,1,3^2)$	3
C_3	C_3	$(1,1,1^3,1^3)$	4
C_6	C_3	$(1,1,2^3)$	4
C_6	C_6	$(1,1,1^6)$	5
C_7	C_1	$(1,7)$	0
C_7	C_7	$(1,1^7)$	6
$C_7 \rtimes C_3$	C_7	$(1,1^7)$	6
D_7	C_7	$(1,1^7)$	6
F_7	C_7	$(1,1^7)$	6
C_2(No.2)	C_1	$(2,2,2,2)$	0
C_2^2(No.8)	C_2(No.3)	$(2,1^2,2^2)$	3
S_3(No.10)	C_3	$(2,1^3,1^3)$	4
S_3(No.11)	C_3	$(2,2^3)$	4
D_6	C_6	$(2,1^6)$	5
C_4	C_1	$(4,4)$	0
C_8	C_1	(8)	0
C_2(No.2)	C_2(No.2)	$(1^2,1^2,1^2,1^2)$	4
C_2^2(No.8)	C_2(No.2)	$(1^2,1^2,2^2)$	4
C_2^2(No.6)	C_2(No.2)	$(2^2,2^2)$	4
C_4	C_2(No.2)	$(2^2,2^2)$	4
C_8	C_2(No.2)	(4^2)	4
C_4	C_4	$(1^4,1^4)$	6
D_4(No.15)	C_4	$(1^4,1^4)$	6
C_8	C_4	(2^4)	6
D_4(No.14)	C_4	(2^4)	6
C_8	C_8	(1^8)	7
D_8	C_8	(1^8)	7

In Table 3, to distinguish the isomorphic subgroups, we add the number from Table 2. Since the ramification is tame, the p-order of D_{K_t} can be calculated by the formula

$$v_p(D_{K_t}) = \sum_{\mathfrak{p}} f(\mathfrak{p}/p)(e(\mathfrak{p}/p) - 1).$$

The pairs of the decomposition and inertia groups for tamely ramified primes $p \geq 5$ in the $\mathrm{PGL}(2,7)$-extensions defined by (2.1) can be determined. For example, by Proposition 3.1 and Proposition 3.3 (i)(2), we obtain that, if $p \geq 5,\ p \neq 7,\ \gcd(v_p(t), 6) = 2$, and $\left(\frac{7n^{-1}}{p}\right) = -1$, then the decomposition type of p is $(1, 1, 2^3)$. Since (C_6, C_3) is the unique pair having the decomposition type, p has (C_6, C_3) as the decomposition and the inertia groups at $\widetilde{K}_t/\mathbb{Q}$. Similarly, if $p = 7,\ v_7(t) > 7,\ \gcd(v_7(t) - 1, 6) = 2$, and $n \equiv 3, 5, 6 \mod 7$, then 7 has (C_6, C_3) as the pair.

4 Construction of $\mathrm{PGL}(2,7)$-extensions unramified over quadratic fields

The group $\mathrm{PGL}(2,7)$ has a unique subgroup of index 2, that is $\mathrm{PSL}(2,7)$. This implies that a $\mathrm{PGL}(2,7)$-extension contains the unique quadratic subfield $\mathbb{Q}(\sqrt{D_{K_t}})$ and the Galois group of $\widetilde{K_t}/\mathbb{Q}(\sqrt{D_{K_t}})$ is isomorphic to $\mathrm{PSL}(2,7)$. For a rational prime p, Table 3 shows that if $v_p(D_{K_t}) = 3$, then $T \cong C_2(\text{No.3}) \nsubseteq \mathrm{PSL}(2,7)$. Thus, we have the following lemma, which will be used throughout this section.

Lemma 4.1. *A tamely ramified prime ideal of $\mathbb{Q}(\sqrt{D_{K_t}})$ lying above p in $K_t/\mathbb{Q}$ is unramified in $\widetilde{K_t}/\mathbb{Q}(\sqrt{D_{K_t}})$ if and only if $v_p(D_{K_t}) = 0$ or 3.*

The aim of this section is to prove the following theorem.

Theorem 4.2. *Let n be an integer coprime to 6 and m an integer coprime to 7. Assume that n and m are relatively prime. Then, the following hold.*

(i) If there exists a prime p such that $(7^7n^6 + 108m^7)/p$ is square, then $K_t/\mathbb{Q}$ is unramified outside p for $t = 7^7n^6/m^7$.

(ii) For a rational number $t = 7^7n^3/m^7$, the extension $\widetilde{K_t}/\mathbb{Q}$ is a $\mathrm{PGL}(2,7)$-extension unramified over the unique quadratic subfield.

To prove Theorem 4.2, we have to study the decompositions of the prime divisors of $t + 108$ for the case $t \in \mathbb{Z}$, and the denominators of t for the case $t \in \mathbb{Q}$, because these numbers appear in the discriminant (3.1).

As for the prime factors of $t + 108$, we have the following proposition.

Proposition 4.3. *Let p be a prime $\neq 2, 3, 7$. If $v_p(t + 108) > 0$, then*

$$v_p(D_{K_t}) = \begin{cases} 0 & \text{if } v_p(t + 108) \text{ is even,} \\ 3 & \text{if } v_p(t + 108) \text{ is odd.} \end{cases}$$

To prove Proposition 4.3, we use the following lemma by Dedekind.

Lemma 4.4 (Dedekind [7, Lemma 1])**.** *Let $\varphi(X)$ be an irreducible polynomial over $\mathbb{Q}$, $K = \mathbb{Q}[X]/(\varphi(X))$, D_φ the discriminant of φ, and i the integer satisfying $D_\varphi = i^2 D_K$. If a prime p does not divide i and*

$$\varphi(X) \equiv \varphi_1(X)^{e_1} \cdots \varphi_g(X)^{e_g} \mod p$$

is the factorization into the irreducible factors modulo p, then p decomposes as

$$p\mathfrak{O} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

in K where $f(\mathfrak{p}_j/p) = \deg \varphi_j$ for $j = 1, \ldots, g$.

Proof of Proposition 4.3. Let $D_{F(t)}$ be the discriminant of the octic $F(t, X)$ given in (2.1) and $i(t)$ the integer satisfying $D_{F(t)} = i(t)^2 D_{K_t}$. By assumption,

$$F(t, X) \equiv X^8 + X^7 + 7X^6 + 108(X + 1) \mod p.$$

Note that the right hand side of the above congruence does not depend on t.

Assume $v_p(t + 108) = 1$. Then $v_p(D_{F(t)}) = 3$, which implies $v_p(D_{K_t}) = 1$ or 3. However, since $v_p(D_{K_t}) \neq 1$ by Table 3, we conclude $v_p(D_{K_t}) = 3$ and $v_p(i(t)) = 0$. Hence, by applying Lemma 4.4 to $F(t, X)$, we have

$$F(t, X) \equiv F_1(X)^{E_1} \cdots F_g(X)^{E_g} \mod p,$$

which corresponds to the decomposition of p in $K_t/\mathbb{Q}$, i.e.,

$$p\mathfrak{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},\ E_i = e_i,\ f_i = f(\mathfrak{p}_i/p) = \deg F_i(X).$$

Since $v_p(D_{K_t}) = 3$, and p is tamely ramified, we have

$$\sum_{i=1}^{g} \deg F_i \cdot (E_i - 1) = 3. \tag{4.1}$$

Assume $v_p(t + 108) > 0$. Since the factorization of $F(t, X) \mod p$ does not depend on t, the equation (4.1) holds again. By Hensel's lemma, we obtain

$$\sum f_i \cdot (e_i - 1) \leq \sum_{i=1}^{g} \deg F_i \cdot (E_i - 1) = 3,$$

and hence, from Table 3, it follows $v_p(D_{K_t}) = 0$ or 3. Noting that $v_p(D_{K_t})$ is odd if and only if $v_p(t + 108)$ is odd, we obtain the proposition. □

Next, we study the decomposition of $p = 7$.

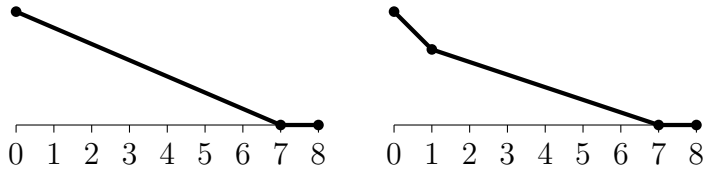
If 7 divides t, then the decomposition of 7 in $K_t/\mathbb{Q}$ is shown in Proposition 3.3. Hence, we consider the two cases where 7 divides $t + 108$ and 7 does not divide $t(t + 108)$.

We first consider the case $7 \mid t + 108$.

Proposition 4.5. *If $0 < v_7(t+108) \leq 2$, then 7 ramifies wildly. If $v_7(t+108) \geq 3$, then*

$$v_7(D_{K_t}) = \begin{cases} 4 & \text{if } v_7(t+108) \text{ is odd,} \\ 5 & \text{if } v_7(t+108) \text{ is even.} \end{cases}$$

Proof. If 7 divides $t+108$, then we obtain $t \equiv 4 \mod 7$. The Newton polygon of $F(t, X-3)$ with respect to 7 is one of the following.



$v_7(t+108) \leq 2$ $\qquad$ $v_7(t+108) > 2$

For the left polygon, the height of the left side is $v_7(t+108)$. This implies that the decomposition of 7 is $(1, 1^7)$. For the right polygon, the height of the center side is 2 so that the decomposition of 7 is $(1,1,1^6)$, $(1,1,1^3,1^3)$ or $(1,1,2^3)$. This implies $v_p(D_{K_t}) = 4$ or 5. Since the discriminant of F is $-7^7 t^5 (t+108)^3$, we see

$$v_7(D_{K_t}) = \begin{cases} \text{even} & \text{if } v_7(t+108) \text{ is odd,} \\ \text{odd} & \text{if } v_7(t+108) \text{ is even.} \end{cases}$$

and hence, the proposition follows. □

When $7 \nmid t(t+108)$, we have $t \equiv 1, 2, 3, 5, 6 \mod 7$. Similarly as in the previous case, we consider the Newton polygons of $F(t, X-7+t)$. As a result, we obtain

$$7\mathfrak{O}_{K_t} = \begin{cases} (1^8) & \text{if } t \equiv 6 \mod 7, \\ (1,1,1^6) & \text{if } t \equiv 12, 16, 29, 45 \mod 49, \\ (1,1^7) & \text{otherwise.} \end{cases}$$

This also shows the tame part of the following proposition.

Proposition 4.6. *Let t be an integer. If $7 \nmid t(t+108)$, then the following hold.*

(i) If $t \equiv 6 \mod 7$, then $v_7(D_{K_t}) = 7$.

(ii) If $t \equiv 1, 2, 3, 5 \mod 7$, then

$$v_7(D_{K_t}) = \begin{cases} 5 & \text{if } t \equiv 12, 16, 29, 45 \mod 49, \\ 7 & \text{otherwise.} \end{cases}$$

Proof. It remains to prove that $v_7(D_{K_t}) = 7$ if $7\mathfrak{O}_{K_t} = (1, 1^7)$. In this case, 7 is wildly ramified in $K_t/\mathbb{Q}$. This implies that $v_7(D_{K_t}) \geq 7$. On the other hand, since $7 \nmid t(t+108)$, we have $v_7(D_{K_t}) \leq 7$. □

Lastly, we compute $v_p(D_{K_t})$ for $t \in \mathbb{Q}$ with $p \neq 2, 3, 7$. We write $t = n/m$ with coprime integers n and m. Since the discriminant of $F(n/m, X)$ is

$$-7^7 \left(\frac{n}{m}\right)^5 \left(\frac{n}{m} + 108\right)^3 = -\frac{7^7 n^5 (n + 108m)^3}{m^8},$$

the ramified prime p in $K_t/\mathbb{Q}$ is 7 or a divisor of $nm(n+108m)$. From Remark 2.4, we can use the technique of the Newton polygon for $F(n/m, X)$. The decomposition of divisors of n prime to 6 are obtained by Proposition 3.3. For divisors of $m(n+108m)$, we have the following propositions.

Proposition 4.7. *Let n and m be coprime integers and p a prime divisor of $n + 108m$. Then the factorization of $F(n/m, X) \mod p$ does not depend on n and m.*

Proof. We can show this proposition similarly as Proposition 4.3. □

Proposition 4.8. *We write $t = n/m$ with coprime integers n and m, and we let p be a prime divisor of m.*

(i) If $7 \nmid v_p(m)$, then p ramifies wildly when $p = 7$, and $v_p(D_{K_t}) = 6$ when $p \neq 7$.

(ii) If $p \neq 7$ and $7 \mid v_p(m)$, then p is unramified at $K_t/\mathbb{Q}$.

Proof. The first statement is clear. Therefore, we assume $p \neq 7$ and $7 \mid v_p(m)$. The Newton polygon of $F(n/m, X)$ has two segments S_1 and S_2 whose horizontal lengths are 1 and 7, respectively. It suffices to consider the associated polynomial F_{S_2} of S_2. Since $7 \mid v_p(m)$, the degree of F_{S_2} is 7 and

$$F_{S_2}(Y) = -\frac{n}{m'} Y^7 + 1$$

with $m' = mp^{-v_p(m)}$. Since the discriminant of F_{S_2} is $-7^7(\frac{n}{m'})^6$, this polynomial satisfies Ore's condition. This proves the proposition. □

Proof of Theorem 4.2. As noted in the above, we need to consider the numerators and the denominators of t and the numerators of $t + 108$.

We start with the proof of (ii), and hence, assume $t = 7^7 n^3/m^7$. By Propositions 3.1, 3.2, and 3.3, we have $v_p(D_{K_t}) = 0$ or 3 for all p dividing $7n$. The equation $v_p(D_{K_t}) = 0$ or 3 holds also for all p dividing $7^7 n^3 + 108m^7$ by Proposition 4.3. Therefore, the primes of the quadratic subfield lying above such p are unramified by Lemma 4.1. The prime divisors of the denominator m are unramified in $\widetilde{K_t}/\mathbb{Q}$ from Proposition 4.8. Consequently, we have proved that $\widetilde{K_t}$ is unramified over the unique quadratic subfield.

Similar argument for $t = 7^7 n^6/m^7$ shows (i). □

Table 4: Examples of Theorem 4.2

Examples of (i)			Examples of (ii)		
n	m	$D_{K_{7^7n^6/m^7}}$	n	m	$D_{K_{7^7n^3/m^7}}$
1	-5	45053^3	1	-4	945929^3
1	-4	945929^3	1	-3	-1627^3
1	-3	-1627^3	1	-2	-809719^3
1	-2	-809719^3	1	-1	$-5^3 \cdot 37^3 \cdot 4451^3$
1	1	-823651^3	1	1	-823651^3
1	2	-837367^3	1	2	-837367^3
5	3	-12868095571^3	1	3	$-67^3 \cdot 15817^3$
5	6	-12898092463^3	1	4	$-5^3 \cdot 89^3 \cdot 5827^3$
5	8	-13094351791^3	5	-4	$-5^3 \cdot 317^3 \cdot 319159^3$
7	-6	-96858777319^3	5	-3	$-5^3 \cdot 397^3 \cdot 258707^3$
7	-2	-96888996583^3	5	-2	$-5^3 \cdot 73^3 \cdot 149^3 \cdot 9463^3$
7	3	-96889246603^3	5	-1	$-5^3 \cdot 79^3 \cdot 1303073^3$
7	4	-96890779879^3	5	1	$-5^3 \cdot 11^3 \cdot 13^3 \cdot 139^3 \cdot 5179^3$
7	8	-97115502823^3	5	2	$-5^3 \cdot 29^3 \cdot 41^3 \cdot 131^3 \cdot 661^3$
			5	3	$-5^3 \cdot 29^3 \cdot 293^3 \cdot 12143^3$
			5	4	$-5^3 \cdot 104712347^3$

We find 615 pairs of integers n and m with $1 \leq n \leq 100$, $-100 \leq m \leq 100$ satisfying conditions of Theorem 4.2 (i). For these pairs, the Galois group of $K_{7^7n^6/m^7}/\mathbb{Q}$ is isomorphic to $\mathrm{PGL}(2,7)$ and there is only one prime dividing the discriminant of $K_{7^7n^6/m^7}$. Similarly, we find 5252 pairs of n and m satisfying the conditions of Theorem 4.2 (ii) in the same range. For these pairs n and m, $\mathrm{Gal}(K_{7^7n^3/m^7}/\mathbb{Q}) \cong \mathrm{PGL}(2,7)$ holds and the valuations of $D_{K_{7^7n^3/m^7}}$ for prime divisors of $D_{K_{7^7n^3/m^7}}$ are 3. Table 4 consists of some such pairs (n,m) with small absolute values and the discriminants of the fields K_t.

References

[1] M. Aoki and M. Kida: *Constructing unramified extensions over quadratic fields*, Involve **15** (2022), no. 1, 55–68.

[2] W. Bosma, J. Cannon, and C. Playoust: *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[3] K.-S. Kim and J. König: On Galois extensions with prescribed decomposition groups. J. Number Theory **220** (2021), 266–294.

[4] J. König, D. Neftin, and J. Sonn: *Unramified extensions over low degree number fields*, J. Number Theory **212** (2020), 72–87.

[5] J. König, D. Rabayev, and J. Sonn: *Galois realizations with inertia groups of order two*, Int. J. Number Theory **14** (2018), no. 7, 1983–1994.

[6] P. Llorente, E. Nart, and N. Vila: *Decomposition of primes in number fields defined by trinomials*, Sém. Théor. Nombres Bordeaux (2) **3** (1991), no. 1, 27–41.

[7] P. Llorente and E. Nart: *Effective determination of the decomposition of the rational primes in a cubic field*, Proc. Amer. Math. Soc. **87** (1983), no. 4, 579–585.

[8] G. Malle and B. H. Matzat: *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.

[9] J. Neukirch: *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1999.

[10] T. Ogasawara and G. J. Schaeffer: *On* $\mathrm{PGL}_2(\mathbb{F}_7)$ *and* $\mathrm{PSL}_2(\mathbb{F}_7)$ *number fields ramified at a single prime*, preprint.

[11] O. Ore: Newtonsche Polygone in der Theorie der algebraischen Körper. Math. Ann. **99** (1928), no. 1, 84–117.

[12] D. P. Roberts and A. Venkatesh: *Hurwitz monodromy and full number fields*, Algebra Number Theory **9** (2015), no. 3, 511–545.

[13] B. L. van der Waerden: *Die Zerlegungs-und Trägheitsgruppe als Permutationsgruppen.* Math. Ann., **111** (1935), no. 1, 731–733.

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

[15] K. Yamamura: *On unramified Galois extensions of real quadratic number fields*, Osaka J. Math. **23** (1986), no. 2, 471–478.

Masanari Kida
e-mail: kida@rs.tus.ac.jp
Nozomu Suzuki
e-mail: 1123702@ed.tus.ac.jp
Department of Mathematics
Faculty of Science Division I
Tokyo University of Science
1-3 Kagurazaka Shinjuku Tokyo 162-8601 Japan