HILBERT’S IRREDUCIBILITY, MODULAR FORMS, AND COMPUTATION OF CERTAIN GALOIS GROUPS

IVA KODRNJA AND GORAN MUIĆ

Abstract. In this paper we discuss applications of our earlier work in studying certain Galois groups and splitting fields of rational functions in $\mathbb{Q}(X_0(N))$ using Hilbert’s irreducibility theorem and modular forms. We also consider computational aspect of the problem using MAGMA and SAGE.

1. Introduction

In this paper we consider congruence subgroups $\Gamma_0(N)$, $N \geq 1$, and the corresponding compact Riemann surface $X_0(N)$ which we initially consider as a complex irreducible smooth projective curve. The $\mathbb{Q}$–structure on $X_0(N)$ is defined in a standard way using $j$–function i.e., the field of rational functions over $\mathbb{Q}$ on $X_0(N)$ is given by $\mathbb{Q}(X_0(N)) = \mathbb{Q}(j, j(N \cdot))$. We elaborate on equivalent ways of defining the $\mathbb{Q}$–structure in Section 3 (see Lemma 3-3 and its proof). This should be well–known but it is hard to find a convenient reference. These are technical results used in the proof of the main results below. In our earlier paper [18] we gave fairly general study of complex holomorphic maps $X_0(N) \to \mathbb{P}^2$ and developed the test for birationality in terms of modular forms of various even weights. The methods of that paper are further extended and combined with techniques of explicit computations in SAGE in our paper [19]. The paper [19] constructs various models over $\mathbb{C}$ of $X_0(N)$ complementing previous works such as [1], [2], [7], [5], [10], [15], [17], [23] and [27]. In the present paper we describe another application of [18] and [19] where we justify why it is interesting to study plane models of $X_0(N)$ of various type not necessarily of smallest possible degree or one with smallest possible coefficients. By Eichler–Shimura theory [22, Theorem 3.5.2] and explicit determination of certain Eisenstein series in [13, Chapter 7], we know that $S_m(\Gamma_0(N))$, and $M_m(\Gamma_0(N))$, for $m \geq 2$ even, have basis consisting of forms with integral $q$–expansions. So, if we take that $f, g, h$ are linearly independent modular forms with rational $q$–expansions for $\Gamma_0(N)$, we can construct an irreducible over $\mathbb{Z}$ homogeneous polynomial with integral coefficients $P_{f,g,h}$ such that $P_{f,g,h}(f, g, h) = 0$ in $\mathbb{Q}(X_0(N))$. Let $Q_{f,g,h}$ be its dehomogenization with respect to the last variable. Again, we obtain an irreducible over $\mathbb{Z}$ polynomial with integral coefficients. By means of Hilbert’s irreducibility theorem (see [26], summarized in Lemma [2-4]), we obtain a family of irreducible over $\mathbb{Z}$ polynomials with integral coefficients $Q_{f,g,h}(\lambda, \cdot)$, where $\lambda$ ranges over a certain thin set (see [26] Proposition 3.3.5 and page 26, part 3) or Lemma [2-1] here). In this way we obtain a family of number
fields determined as splitting fields of these polynomials all of them have the same Galois group $G_{f,g,h}$ which is the Galois group of the splitting field of $Q_{f,g,h}(g/f, \cdot)$ over $\mathbb{Q}(g/f)$. The goal of present paper is to study these objects as an application of the theory developed in [18] and [19]. We should observe that the field $\mathbb{Q}(g/f)$ is just the field of rational functions one variable over $\mathbb{Q}$, so the reader might wonder how the study of Galois groups in the present paper differ for example from that in [26]. The reason is that modular forms are great source of concrete irreducible polynomials $Q_{f,g,h}(\lambda, \cdot)$ that are more restrictive than general polynomials over the field $\mathbb{Q}(\lambda)$ ($\lambda$ is a variable here). The reader should consult Section 5 about many results for $\Gamma_0(72)$ which shows that.

We describe the content of the paper. In Section 2 we explain how to use Hilbert’s irreducibility (see Lemma 2-4) and a technique of Frobenius on reducing modulo various primes (see Theorem 2-5) in order to compute $G_{f,g,h}$. In Section 3, we adapt the results of paper [19] (see Lemmas 3-3, 3-5, and 2-2) in order to study how the Galois group $G_{f,g,h}$ behaves when we fix $f$ and $g$ and let $h$ vary under certain assumptions on $m$ and $N$. The main result is contained in Theorems 3-13 and 3-14. They are of general nature and they are illustrated by more concrete results in Section 5 for $\Gamma_0(63)$, $\Gamma_0(64)$, and especially for $\Gamma_0(72)$. In the Section 4, we improve on Theorem 3-14 in the case of hyperelliptic modular curves over $\mathbb{Q}$ (see Theorem 4-1). The section ends with an interesting example for $\Gamma_0(30)$. In Section 5, we discuss non–hyperelliptic modular curves (see Theorem 5-1). We give several elegant computations of Galois groups $G_{f,g,h}$ based on methods and results of Section 2. The results are contained in Proposition 5-2 (the case $\Gamma_0(63)$), Proposition 5-5 (the case $\Gamma_0(64)$), and in Propositions 5-6, 5-8, and 5-9 (the case $\Gamma_0(72)$). The key result of that section is also Remark 5-10 related to $\Gamma_0(72)$. The Galois groups of polynomials $\tilde{Q}(\lambda, \cdot)$ (a normalized version of $Q(\lambda, \cdot)$, see Section 2) over $\mathbb{Q}(\lambda)$ can also be computed using MAGMA system and a routine $\text{GaloisGroup}$. It is also interesting to use new MAGMA routine $\text{GeometricGaloisGroup}$ (see [6] for implementation) which give the Galois groups of polynomials $\tilde{Q}(\lambda, \cdot)$ over $\mathbb{C}(\lambda)$ and compare the two. (For MAGMA implementations (and background) the reader should consult papers [1], [6], [5], and [9].) They are not directly used in the paper. Nevertheless, we have made many experiments in MAGMA and SAGE related to the results of the present paper. In the final Section 6 we reprove [23, Lemma 2] (needed in the proof of Theorem 4-1) using more elegant approach based on [18] combined with certain simple computations in SAGE.

We would like to thank Nicole Sutherland for several useful conversations regarding the implementation in MAGMA of routines for computing Galois groups of polynomials with coefficients in the function fields over $\mathbb{Q}$ and $\mathbb{C}$.

2. An Application of Hilbert’s Irreducibility Theorem

The goal of the present section is to set-up the notation for the rest of the paper and to prove Theorem 2-5.

For an even integer $m \geq 2$, let $M_m(\Gamma_0(N))$ (resp., $S_m(\Gamma_0(N))$) be the space of (resp., cuspidal) modular forms of weight $m$ for $\Gamma_0(N)$. Assume $\dim M_m(\Gamma_0(N)) \geq 3$. Let $f, g, h$ be three linearly independent modular forms in $M_m(\Gamma_0(N))$. Then, we define a holomorphic
map $X_0(N) \to \mathbb{P}^2$ uniquely determined by
\begin{equation}
\mathbf{a}_z \longmapsto (f(z) : g(z) : h(z)), \quad z \in \mathbb{H}.
\end{equation}

Since $X_0(N)$ has a canonical structure of complex projective irreducible algebraic curve, this map can be regarded as a regular map between projective varieties. Consequently, the image is an irreducible projective curve which we denote by $\mathcal{C}(f, g, h)$. Let $P$ be the reduced equation of $\mathcal{C}(f, g, h)$ i.e., an irreducible homogeneous polynomial in three variables with complex coefficients such that $P(f(z), g(z), h(z)) = 0$, for all $z \in \mathbb{H}$. It is unique up to multiplication with non–zero complex numbers. Its dehomogenization $Q \overset{\text{def}}{=} P(1, 1, 1)$ is also an irreducible polynomial over $\mathbb{C}$, and it satisfies $Q(g/f, h/f) = 0$ in the field of rational functions $\mathbb{C}(X_0(N))$. It is very easy to see that $P$ is homogenization of $Q$ i.e., $P$ is uniquely determined. The polynomial $Q$ must depend on both variables or otherwise linear independence of $f$, $g$, and $h$ is violated. We see also that $Q(g/f, h/f)$ is an irreducible polynomial of $h/f \in \mathbb{C}(X_0(N))$ over the subfield $\mathbb{C}(g/f)$ generated by $g/f$. Consequently, the field extensions satisfy $[\mathbb{C}(g/f, h/f) : \mathbb{C}(g/f)] = \deg(Q(g/f, h/f))$.

The next lemma is important for our considerations. We recall that by Eichler–Shimura theory [22, Theorem 3.5.2] and explicit determination of certain Eisenstein series in [13, Chapter 7], we know that $S_m(\Gamma_0(N))$, and $M_m(\Gamma_0(N))$, for $m \geq 2$ even, have basis consisting of forms with integral $q$–expansions.

**Lemma 2-2.** Let $f, g, h$ be three linearly independent modular forms in $M_m(\Gamma_0(N))$ having rational $q$–expansions. Then, we may select that the polynomial $P$ (and consequently $Q$) has rational coefficients. Moreover, $Q(g/f, h/f)$ is an irreducible polynomial of $h/f$ over $\mathbb{Q}(g/f)$. Consequently, we have $[\mathbb{Q}(g/f, h/f) : \mathbb{Q}(g/f)] = [\mathbb{C}(g/f, h/f) : \mathbb{C}(g/f)] = \deg(Q(g/f, h/f))$.

**Proof.** The proof of the first claim of the lemma is contained in the proof of [19, Corollary 1.5 (ii)]. The polynomial $P$ must be irreducible over $\mathbb{Q}$ since it is irreducible over $\mathbb{C}$. The second claim follows from this. □

**Definition 2-3.** Maintaining the assumptions of Lemma 2-2, we denote by $Q_h = Q_{f,g,h}$ an irreducible polynomial with relatively prime coefficients in $\mathbb{Z}$ such that $Q_{f,g,h}(g/f, h/f) = 0$. Let $L_h = L_{f,g,h}$ be the splitting field $Q_h(g/f, \cdot)$ containing $\mathbb{Q}(g/f, h/f)$, and $G_h = G_{f,g,h} \overset{\text{def}}{=} \text{Gal}(L_h/\mathbb{Q}(g/f))$. For $\lambda \in \mathbb{Z}$, we let $L_{h,\lambda} = L_{f,g,h,\lambda}$ be the splitting field $Q_h(\lambda, \cdot)$, and $G_{h,\lambda} = G_{f,g,h,\lambda} \overset{\text{def}}{=} \text{Gal}(L_{h,\lambda}/\mathbb{Q})$.

The polynomial $Q_{f,g,h}$ is determined up to a multiplication by $\pm 1$. The corresponding $P$ is denoted by $P_h = P_{f,g,h}$. Next, we can combine the above considerations with the celebrated Hilbert’s irreducibility theorem. Following Serre [26], we call a subset $A \subset \mathbb{Z}$ thin if the number of elements in the intersection of $A$ with a segment $[-n, n]$ is $O(n^{1/2})$ as $n \to \infty$.

**Lemma 2-4.** There exists a thin subset $A_{f,g,h} \subset \mathbb{Z}$ such that $G_{f,g,h}$ is isomorphic to $G_{f,g,h,\lambda}$, for $\lambda \in \mathbb{Z} - A_{f,g,h}$.

**Proof.** Since $g/f$ is transcendental over $\mathbb{Q}$ in sense of field theory, the field $\mathbb{Q}(g/f)$ is just a field of rational functions in one variable over $\mathbb{Q}$. Now, the claim follows from the Hilbert’s irreducibility (see for example [26, Proposition 3.3.5 and page 26, part 3]). □
We write $Q_{f,g,h}(\lambda, \cdot)$ in the form
\[ Q_{f,g,h}(\lambda, T) = \sum_{i=1}^{n} a_i(\lambda)T^i \in \mathbb{Z}[\lambda, T]. \]

We remark that $\lambda$ and $T$ are variables here. By Definition 2-3 the polynomial is irreducible over $\mathbb{Z}$ (not just over $\mathbb{Q}$). For the present purpose this form of the polynomial is not good. We use standard trick
\[ \tilde{Q}_{f,g,h}(\lambda, T) \stackrel{\text{def}}{=} a_n(\lambda)^{-1}Q(\lambda, T/a_n(\lambda)) = T^n + a_{n-1}(\lambda)T^{n-1} + \sum_{i=1}^{n-2} a_n(\lambda)^{n-1-i}a_i(\lambda)T^i \in \mathbb{Z}[\lambda, T]. \]

This polynomial is also irreducible over $\mathbb{Z}$ (and over $\mathbb{Q}$) as it is easy to check. Recall that in the present notation we have $\sum_{i=1}^{n} a_i(g/f)(h/f)^i = Q_{f,g,h}(g/f, h/f) = 0$ in $\mathbb{Q}(g/f, h/f)$. We fix an algebraic closure $\mathbb{Q}(g/f)$ containing $\mathbb{Q}(g,f,h,f)$. By Definition 2-3 we may regard $G_{f,g,h}$ as the Galois group of the splitting field $L_{f,g,h}$ inside $\mathbb{Q}(g/f)$. It is obvious that $L_{f,g,h}$ is the splitting field of $Q_{f,g,h}(g/f, T)$ in $\mathbb{Q}(g/f)$. We decompose into linear factors in $L_{f,g,h}$
\[ \tilde{Q}_{f,g,h}(g/f, T) = (T - \alpha_1)(T - \alpha_2) \cdots (T - \alpha_n), \text{ say, } \alpha_1 = a_n(g/f)h/f. \]

The group $G_{f,g,h}$ permutes the fixed sequence $\alpha_1, \cdots, \alpha_n$. In this way, we may regard $G_{f,g,h}$ as a subgroup of the symmetric group $S(n)$ of $n$–letters.

Let $\Lambda_{f,g,h}$ be the integral closure of $\mathbb{Q}[\lambda]$ in $L_{f,g,h}$. Let $\lambda \in \mathbb{Z} - A_{f,g,h}$. We select a point $a \in X_0(N)$ such that $a$ gets mapped by $g/f$ onto $\lambda$. Let $m_\lambda$ be the maximal ideal in $\mathbb{Q}[g/f]$ consisting of all that map $a$ onto zero. We fix a maximal ideal $M_{f,g,h,\lambda}$ in $\Lambda_{f,g,h}$ lying over $m_\lambda$. Then, $\Lambda_{f,g,h}/M_{f,g,h,\lambda}$ is a splitting field of $\tilde{Q}_{f,g,h}(\lambda, T)$, and we have
\[ \tilde{Q}_{f,g,h}(\lambda, T) = (T - \overline{\alpha}_1)(T - \overline{\alpha}_2) \cdots (T - \overline{\alpha}_n), \]

where $\overline{\alpha}_i = \alpha_i + M_{f,g,h,\lambda}$. We may let $L_{f,g,h,\lambda} = \Lambda_{f,g,h}/M_{f,g,h,\lambda}$ since both $\tilde{Q}_{f,g,h}(\lambda, T)$ and $\tilde{Q}_{f,g,h}(\lambda, T)$ have the same splitting field. Thus, $G_{f,g,h,\lambda}$ permutes the fixed sequence $\overline{\alpha}_1, \cdots, \overline{\alpha}_n$ (see Lemma 2-3). In this way, we may regard $G_{f,g,h,\lambda}$ as a transitive subgroup of the symmetric group $S(n)$ of $n$–letters. The isomorphism $G_{f,g,h}$ with $G_{f,g,h,\lambda}$ (see Lemma 2-4) can be taken to be compatible with the action on above fixed sequences of roots. After all preparations, classical Frobenius theory (generalized later by Chebotarev) easily implies the following theorem which we use for explicit computations.

**Theorem 2-5.** Maintaining above assumptions, $G_{f,g,h}$ contains a permutation with a cycle pattern $n_1, n_2, \ldots, n_t$ if and only if there exists a prime number $p$ and and $r \in \{0, 1, \ldots, p-1\}$ such that $\tilde{Q}_{f,g,h}(r, T) = T^n + a_{n-1}(r)T^{n-1} + \sum_{i=1}^{n-2} a_n(r)^{n-1-i}a_i(r)T^i \pmod{p}$ can be decomposed into a product of different irreducible factors of degrees $n_1, n_2, \ldots, n_t$.

**Proof.** First, for each $r \in \{0, 1, \ldots, p-1\}$, the number of integers $\leq n$ of the the form $kp + r$ is $O(n)$ is $n \rightarrow \infty$. So, this set can not be thin. Next, let $\lambda \in \mathbb{Z} - A_{f,g,h}$. By Frobenius theorem, the density of all primes $p$ such that $\tilde{Q}_{f,g,h}(\lambda, T) \pmod{p}$ can be decomposed into a product of different irreducible factors of degrees $n_1, n_2, \ldots, n_t$ is equal to the number number of elements in $G_{f,g,h,\lambda}$ with a cycle pattern $n_1, n_2, \ldots, n_t$ divided by the number of elements in $G_{f,g,h,\lambda}$.  


After these preliminaries, we prove the theorem. First, assume that for \( r \in \{0, 1, \ldots, p - 1\} \) \( \tilde{Q}_{f,g,h}(r, T) \) can be decomposed into a product of different irreducible factors of degrees \( n_1, n_2, \ldots, n_t \). Then, we select \( \lambda \in \mathbb{Z} - A_{f,g,h} \) such that \( \lambda \equiv r \pmod{p} \). By Frobenius theorem and Lemma 2-4, we obtain that \( G_{f,g,h} \) contains a permutation with a cycle pattern \( n_1, n_2, \ldots, n_t \).

Conversely, assume that \( G_{f,g,h} \) contains a permutation with a cycle pattern \( n_1, n_2, \ldots, n_t \). Then, the same is true for \( G_{f,g,h,\lambda} \) for any \( \lambda \in \mathbb{Z} - A_{f,g,h} \). We fix any such \( \lambda \). By Frobenius theorem, there exists a prime number \( p \) such that \( \tilde{Q}_{f,g,h}(\lambda, T) \pmod{p} \) can be decomposed into a product of different irreducible factors of degrees \( n_1, n_2, \ldots, n_t \). Finally, let \( r \) be the residue of division of \( \lambda \) by \( p \). We have \( \tilde{Q}_{f,g,h}(\lambda, T) \equiv \tilde{Q}_{f,g,h}(r, T) \pmod{p} \) proving the claim. \( \square \)

3. Proof of Theorems 3-14 and 3-13

The goal of the present section is to prove Theorems 3-13 and 3-14. We start by preliminary definitions and results. Let

\[
E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n
\]

be the usual Eisenstein series, and let

\[
\Delta(z) = q + \sum_{n=2}^{\infty} \tau(n)q^n
\]

be the Ramanujan delta function. Then, \( j = E_4^3/\Delta \). Since \( E_4^3(N \cdot), \Delta(N \cdot) \in M_{12}(\Gamma_0(N)) \), the fact that the function field over \( \mathbb{C} \) is generated by \( j \) and \( j(N \cdot) \) means that the holomorphic map

\[
(3-1) \quad a_z \mapsto (1 : j(z) : j(Nz)) = (\Delta(z)\Delta(Nz) : E_4^3(z)\Delta(Nz) : E_4^3(Nz)\Delta(z))
\]

is a birational uniformization by \( S_{24}(\Gamma_0(N)) \). The \( \mathbb{Q} \)-structure on the curve \( X_0(N) \) is introduced by considering its field of rational function defined over \( \mathbb{Q} \):

\[
(3-2) \quad \mathbb{Q}(X_0(N)) \overset{def}{=} \mathbb{Q}(j, j(N \cdot)).
\]

Now, we are ready to prove the following lemma. The lemma must be well–known but we could not find appropriate reference.

**Lemma 3-3.** Assume that \( m \geq 2 \) is an even integer. Suppose that \( f, g, h \in M_m(\Gamma_0(N)) \) have integral (or rational) \( q \)-expansions. Then, the map (2-1) is birational over \( \mathbb{C} \) if and only if it is birational over \( \mathbb{Q} \).

**Proof.** Assume that the map (2-1) is birational over \( \mathbb{C} \). Then, we have

\[
\mathbb{C}(g/f, h/f) = \mathbb{C}(j, j(N \cdot)).
\]
This implies that there exist homogeneous polynomials $P$ and $Q$ of the same degree with complex coefficients such that

$$j = \frac{P(f, g, h)}{Q(f, g, h)}.$$

Equivalently, we have the following:

$$E_4^3 \cdot Q(f, g, h) - \Delta \cdot P(f, g, h) = 0.$$

Inserting rational $q$--expansions of $E_4^3 \cdot \Delta$, $f$, $g$, and $h$, we obtain a $q$--expansion of the modular form $E_4^3 \cdot Q(f, g, h) - \Delta \cdot P(f, g, h)$. But, by the assumption, this modular form is identically equal to zero. Therefore, all its coefficients in the $q$--expansion are equal to zero. (Enough to choose first few depending on its weight.) Each of these coefficients is a linear homogeneous function in coefficients of $P$ and $Q$. Thus, we obtain the homogeneous linear system in coefficients of $Q$ and $P$ with coefficients in $Q$. This homogeneous system has a non--zero solution over $\mathbb{C}$. Therefore, it has a non--zero solution over $\mathbb{Q}$. Thus, we can take that the coefficients of $P$ and $Q$ are in $\mathbb{Q}$. This proves $j \in \mathbb{Q}(g/f, h/f)$. Similarly, we also prove $j(N \cdot) \in \mathbb{Q}(g/f, h/f)$. This implies

$$(3-4) \quad \mathbb{Q}(X_0(N)) = \mathbb{Q}(j, j(N \cdot)) \subset \mathbb{Q}(g/f, h/f).$$

Conversely, we can write

$$j = \frac{E_4^3}{\Delta} = \frac{E_4^3 \cdot \Delta(N \cdot)}{\Delta \cdot \Delta(N \cdot)}, \quad \text{and} \quad j(N \cdot) = \frac{E_4^3(N \cdot)}{\Delta(N \cdot)} = \frac{E_4^3(N \cdot) \cdot \Delta}{\Delta \cdot \Delta(N \cdot)}.$$

Now, we can argue as before to prove

$$g/f, h/f \in \mathbb{Q} \left( \frac{E_4^3 \cdot \Delta(N \cdot)}{\Delta \cdot \Delta(N \cdot)}, \frac{E_4^3(N \cdot) \cdot \Delta}{\Delta \cdot \Delta(N \cdot)} \right) = \mathbb{Q}(j, j(N \cdot)).$$

Hence, we obtain

$$\mathbb{Q}(g/f, h/f) \subset \mathbb{Q}(X_0(N)).$$

This means that the map (2-1) is birational over $\mathbb{Q}$.

Conversely, we have

$$\mathbb{Q}(g/f, h/f) = \mathbb{Q}(X_0(N)).$$

Taking the composite fields (with $\mathbb{C}$) we obtain

$$\mathbb{C}(g/f, h/f) = (\mathbb{C}) (\mathbb{Q}(g/f, h/f)) = (\mathbb{C}) (\mathbb{Q}(X_0(N))) = \mathbb{C}(X_0(N)).$$

In the last equality we use (3-2). This means that the map (2-1) is birational over $\mathbb{C}$. □

By Eichler–Shimura theory (22 Theorem 3.5.2), for each even integer $m \geq 2$ the space of cusp forms $S_m(\Gamma_0(N))$ is defined over $\mathbb{Q}$. Let $S_m(\Gamma_0(N))_Q$ be the $\mathbb{Q}$--span of all cusp forms in $S_m(\Gamma_0(N))$ having rational $q$--expansions. Obviously, $S_m(\Gamma_0(N)) = S_m(\Gamma_0(N))_Q \otimes_{\mathbb{Q}} \mathbb{C}$.

**Lemma 3-5.** Assume that either $m = 2$ and $X_0(N)$ is not hyperelliptic (implies $g(\Gamma_0(N)) \geq 3$) or $m \geq 4$ is an even integer such that $\dim S_m(\Gamma_0(N)) \geq \max (g(\Gamma_0(N)) + 2, 3)$. Then, we have the following:

(i) Let $f_0, \ldots, f_{s-1}$ be a basis of $S_m(\Gamma_0(N))_Q$. Then, $\mathbb{Q}(X_0(N))$ is generated over $\mathbb{Q}$ by the quotients $f_i/f_0$, $1 \leq i \leq s - 1$. 
(ii) Assume that \( f, g \in S_m(\Gamma_0(N))_\mathbb{Q} \) are linearly independent over \( \mathbb{Q} \). Then, there exists a non-empty Zariski open set \( U_{f,g} \subset S_m(\Gamma_0(N))_\mathbb{Q} \) such that \( X_0(N) \) is birationally equivalent over \( \mathbb{Q} \) to \( C(f, g, h) \) via the map (2.1), i.e., \( Q(g/f, h/f) = Q(X_0(N)) \) for any \( h \in U_{f,g} \).

(iii) Assume that \( f, g \in S_m(\Gamma_0(N))_\mathbb{Q} \) are linearly independent over \( \mathbb{Q} \). Then, the degree of the field extension \([Q(X_0(N)) : Q(g/f)]\) is equal to the degree of the divisor of zeroes of \( g/f \).

**Proof.** The proof of (i) is analogous to that of Lemma 3-3. The details are left to the reader. We just note that under assumption of the lemma we have \( C(f_1/f_0, \ldots, f_{k-1}/f_0) = C(X_0(N)) \). This is obvious when \( m = 2 \), and we use [19, Corollary 3.4] for the case \( m \geq 4 \). For the proof of the first claim in (ii), one can adjust the proofs of [19, Theorem 1.4]. We sketch the argument. First, we select a basis of \( S_m(\Gamma_0(N))_\mathbb{Q} \) such that \( f = f_0 \) and \( g = f_1 \). Then, by (i), we have that

\[
Q(X_0(N)) = Q(g/f, f_2/f, \ldots, f_{s-1}/f) = Q(g/f) (f_2/f, \ldots, f_{s-1}/f) \supset Q(g/f)
\]

is a finite algebraic extension. The set of all \( (\lambda_2, \ldots, \lambda_{s-1}) \in \mathbb{Q}^{s-2} \) such that \( \lambda_2 f_2 + \cdots + \lambda_{s-1} f_{s-1} \) generates \( Q(X_0(N)) \) over \( Q(g/f) \) is not empty (by an argument of [19, Lemma 3.2]) and it is determined by \( R(\lambda_2, \ldots, \lambda_{s-1}) \neq 0 \). Here, \( R \) is the discriminant of the characteristic polynomial of the endomorphism of the vector space \( Q(X_0(N)) \) over \( Q(g/f) \) determined by the multiplication by \( (\lambda_2 f_2 + \cdots + \lambda_{s-1} f_{s-1})/f \) (exactly as in the proof of [19, Lemma 3.4]). The discriminant \( R \) is a polynomial in variables \( \lambda_2, \ldots, \lambda_{s-1} \) with coefficients in \( Q(g/f) \). By above considerations, \( R \) is a non-zero polynomial. We select \( \lambda \in \mathbb{Q} \) and \( a \in X_0(N) \) such that \( g/f \) maps \( a \) onto \( \lambda \), and all non-zero coefficients of \( R \) when evaluated at \( a \), are non-zero numbers in \( \mathbb{Q} \). Then, \( R(\lambda_2, \ldots, \lambda_{s-1})(a) \) is a non-zero polynomial with rational coefficients. Then, for the Zariski open set \( U_{f,g} \subset S_m(\Gamma_0(N))_\mathbb{Q} \) can be taken the set of all \( h = \lambda_0 f + \lambda_1 g + \lambda_2 f_2 + \cdots + \lambda_{s-1} f_{s-1} \), such that \( R(\lambda_2, \ldots, \lambda_{s-1})(a) \neq 0 \).

Now, we prove (iii). First of all, by (ii), there exists \( S_m(\Gamma_0(N))_\mathbb{Q} \) such that \( Q(g/f, h/f) = Q(X_0(N)) \). By Lemma 3-3 we have \( C(g/f, h/f) = C(X_0(N)) \). Now, Lemma 2-2 we have that \([Q(X_0(N)) : Q(g/f)]\) is equal to \([C(X_0(N)) : C(g/f)]\). Finally, it is a well-known that \([C(X_0(N)) : C(g/f)]\) is equal to the degree of the divisor of zeroes of \( g/f \).

We generalize the last claim in (iii) in the following corollary:

**Corollary 3-6.** Let \( m \geq 2 \) be an even integer such that \( S_m(\Gamma_0(N))_\mathbb{Q} \geq 2 \). Assume that \( f, g \in S_m(\Gamma_0(N))_\mathbb{Q} \) are linearly independent over \( \mathbb{Q} \). Then, the degree of the field extension \([Q(X_0(N)) : Q(g/f)]\) is equal to the degree of the divisor of zeroes of \( g/f \). Moreover, if we let

\[
(3-7) \quad l_{m,N} \overset{\text{def}}{=} \dim S_m(\Gamma_0(N)) + g(\Gamma_0(N)) - 1 - \epsilon_m, \quad \epsilon_2 = 1 \text{ and } \epsilon_m = 0 \text{ for } m \geq 4,
\]

then \([Q(X_0(N)) : Q(g/f)] \leq l_{m,N} \) (a bound independent of \( f \) and \( g \)).

**Proof.** Select sufficiently large \( k \) such that \( \dim S_{km}(\Gamma_0) \geq \max (g(\Gamma_0(N)) + 2, 3) \) (which is easy to see using explicit formula for the dimension (see for example [19, Lemma 2.2])). For

\footnote{By definition, the intersection of a Zariski dense subset of \( S_m(\Gamma_0(N)) \) defined over \( \mathbb{Q} \) with \( S_m(\Gamma_0(N))_\mathbb{Q} \).}
such $k$, $f^k$ and $f^{k-1}g$ are $\mathbb{Q}$–linearly independent cuspidal forms in $\dim S_{km}(\Gamma_0)$. Now, the first claim of the corollary follows from Lemma 3-5 (iii) since $f^{k-1}g/f^k = g/f$.

For the bound, we estimate the degree of the divisor of zeroes of $g/f$ applying [18, Lemma 2.1]. We obtain

$$\text{div}(g/f) = \text{div}(g) - \text{div}(f) = c_g - c_f,$$

where for non–zero $h \in S_m(\Gamma_0(N))$ the divisor $c_h$ is an effective integral divisors of the degree $\deg (c_h) = l_{m,N}$. Hence, (3-8) implies that the degree of the divisor of zeroes of $g/f$ is $\leq l_{m,N}$.

Let us fix an even integer $m \geq 2$ such that $\dim S_m(\Gamma_0(N))_{\mathbb{Q}} \geq 3$. Assume that $f, g \in S_m(\Gamma_0(N))_{\mathbb{Q}}$ are $\mathbb{Q}$–linearly independent. Then, for each $h \in S_m(\Gamma_0(N))_{\mathbb{Q}}$, $h \notin \mathbb{Q}f + \mathbb{Q}g$, we may construct irreducible polynomials $P_h$ and $Q_h$ with integral coefficients, define splitting fields $L_h$, and define Galois groups $G_h$ (see Definition 2-3).

**Definition 3-9.** Let $\mathcal{G} = \mathcal{G}_{f,g}$ be the set consisting of all representatives of groups $G_h$, $h \in S_m(\Gamma_0(N))_{\mathbb{Q}} - (\mathbb{Q}f + \mathbb{Q}g)$ up to isomorphism. For $G \in \mathcal{G}$, let $\Xi_G$ be the set of all $h \in S_m(\Gamma_0(N))_{\mathbb{Q}} - (\mathbb{Q}f + \mathbb{Q}g)$ such that $G_h \simeq G$. We denote by $\Xi'_{\mathcal{G}}$ the set of all $h \in \Xi_G$ such that the degree of $Q_{f,g,h}(g/f, \cdot)$ is $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)]$.

We explain Definition 3-9 in the following lemma:

**Lemma 3-10.** Let $G \in \mathcal{G}$. Then, the order of $G$ is divisible by $[\mathbb{Q}(g/f,h/f) : \mathbb{Q}(g/f)]$ for any $h \in \Xi_G$. Moreover, $G$ can be regarded as a subgroup of the symmetric group of $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)]$–letters (non–uniquely). In particular, $\mathcal{G}$ is finite. Moreover, assume that $\Xi'_{\mathcal{G}} \neq \emptyset$. Then, the order of $G$ is divisible by $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)]$, $\mathbb{Q}(g/f,h/f) = \mathbb{Q}(X_0(N))$, the splitting field $L_{f,g,h}$ is a finite extension of $\mathbb{Q}(X_0(N))$, and $G$ can be regarded as a transitive subgroup of the symmetric group of $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)]$–letters (uniquely up to conjugation).

**Proof.** The first claim is obvious since we have the chain of field extensions (see Definition 2-3)

$$\mathbb{Q}(g/f) \subset \mathbb{Q}(g/f,h/f) \subset L_h,$$

and $G \simeq G_h = \text{Gal}(L_h/\mathbb{Q}(g/f))$. Basic elementary estimate for $[L_h : \mathbb{Q}(g/f)]$ implies

$$\#G_h = [L_h : \mathbb{Q}(g/f)] \leq ([\mathbb{Q}(g/f,h/f) : \mathbb{Q}(g/f)])! \leq ([\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)])!.$$

Hence, $G$ can be regarded as a subgroup of the symmetric group of $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)]$–letters. Thus, $\mathcal{G}$ is finite.

Assume that $\Xi'_{\mathcal{G}} \neq \emptyset$. Then, by Lemma 2-2 and Definition 3-9 for $h \in \Xi'_{\mathcal{G}}$, we obtain

$$[\mathbb{Q}(g/f,h/f) : \mathbb{Q}(g/f)] = \deg (Q_{f,g,h}(g/f, \cdot)) = [\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)].$$

This is equivalent with $\mathbb{Q}(g/f,h/f) = \mathbb{Q}(X_0(N))$. Now, it is obvious that $L_{f,g,h}$ is a finite extension of $\mathbb{Q}(X_0(N))$. Other two claims in the last part of the lemma follow from Galois theory.

In the next lemma we give a bound independent of choice of $f$ and $g$. The bound might not be optimal but it is needed in the theorem below.
Lemma 3-11. The order of every group $G \in \mathcal{G}$ is less than or equal to $l_{m,N}! = 1 \cdot 2 \cdots l_{m,N}$ where $l_{m,N}$ is defined by (3-7).

Proof. We argue as in Lemma 3-10 using the estimate $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)] \leq l_{m,N}$ (see Corollary 3-6).

Finally, we need the following lemma:

Lemma 3-12. Assume that $f, g \in S_m(\Gamma_0(N)g)\mathbb{Q}$ are $\mathbb{Q}$–linearly independent. Then, there exists a subgroup $G \in \mathcal{G}$ such that $\Xi_G$ is Zariski dense in $S_m(\Gamma_0(N))\mathbb{Q}$.

Proof. The Zariski open set $S_m(\Gamma_0(N))\mathbb{Q} - (\mathbb{Q}f + \mathbb{Q}g)$ is a union of finite number of sets $\Xi_G$ parameterized by subgroups $G \in \mathcal{G}$. Taking the Zariski closure we find that 

$$S_m(\Gamma_0(N))\mathbb{Q} = \cup_G \Xi_G.$$ 

But the space $S_m(\Gamma_0(N))\mathbb{Q}$ is irreducible in sense of algebraic geometry. So, there exists a subgroup $G \in \mathcal{G}$ such that 

$$\Xi_G = S_m(\Gamma_0(N))\mathbb{Q}.$$ 

This means that $\Xi_G$ is Zariski dense in $S_m(\Gamma_0(N))\mathbb{Q}$.

Now, after all of these preparations, we are ready to state and prove the main results of the present section.

Theorem 3-13. Let $m \geq 2$ be an even integer such that $\dim S_m(\Gamma_0(N))\mathbb{Q} \geq 3$. Then, there exists a thin subset $A_{m,N} \subset \mathbb{Z}$, and triples of linearly independent forms $f_i, g_i, h_i \in S_m(\Gamma_0(N)), 1 \leq i \leq k$, such that for any $f, g, h \in S_m(\Gamma_0(N))$ which are linearly independent, there exists $i$ such that $G_{f,g,h} \simeq G_{f_i,g_i,h_i,\lambda}$, $\lambda \in \mathbb{Z} - A_{m,N}$.

Proof. By Lemma 3-11 when $f, g$ ranges over pairs of linearly independent forms in $S_m(\Gamma_0(N))\mathbb{Q}$, the groups in $\mathcal{G}_{f,g}$ are isomorphic to the subgroups of the symmetric group of $l_{m,N}$–letters. Thus, in the corresponding union $\cup_{f,g} \mathcal{G}_{f,g}$, there are only finitely many groups up to isomorphism. Let us call the representatives $G_{f_i,g_i,h_i}$, $1 \leq i \leq k$. Next, we select thin subsets $A_{f_i,g_i,h_i}$ as in Lemma 2-4. Then, the union 

$$A_{m,N} \overset{def}{=} \cup_{i=1}^{k} A_{f_i,g_i,h_i}$$

is a thin subset (see the paragraph before the statement of Lemma 2-4). For $\lambda \in \mathbb{Z} - A_{m,N}$, we have $G_{f_i,g_i,h_i,\lambda} \simeq G_{f_i,g_i,h_i,\lambda}$, $1 \leq i \leq k$. The theorem follows.

Theorem 3-14. Assume that either $m = 2$ and $X_0(N)$ is not hyperelliptic (implies $g(\Gamma_0(N)) \geq 3$) or $m \geq 4$ is an even integer such that $\dim S_m(\Gamma_0(N)) \geq \max (g(\Gamma_0(N)) + 2, 3)$. Assume that $f, g \in S_m(\Gamma_0(N))$ are linearly independent. Then, there exists a subgroup $G$ of the symmetric group of $l_{m,N}$–letters (see (3-7)) such that $\Xi_G'$ is Zariski dense in $S_m(\Gamma_0(N))\mathbb{Q}$ (see Definition 3-9).

Proof. First, by Lemma 3-11 every group $G \in \mathcal{G}$ can be isomorphically embedded into the symmetric group of $l_{m,N}$–letters. Next, there exists $G \in \mathcal{G}$ such that $\Xi_G$ is Zariski dense in $S_m(\Gamma_0(N))\mathbb{Q}$ (see Lemma 3-12). We fix such $G$. 


By Lemma [3-5], there exists a non-empty Zariski open set \( \mathcal{U} \subset S_m(\Gamma_0(N))_Q \) such that \( Q(g/f, h/f) = Q(X_0(N)) \) for \( h \in \mathcal{U} \). Since \( \Xi_G \) is Zariski dense in \( S_m(\Gamma_0(N))_Q \), the intersection \( \Xi_G \cap \mathcal{U} \) is also Zariski dense in \( S_m(\Gamma_0(N))_Q \). Moreover, since for \( h \in \Xi_G \cap \mathcal{U} \), we have \( Q(g/f, h/f) = Q(X_0(N)) \), we obtain that the degree of \( Q_{f, g, h}(g/f, \cdot) \) is \( [Q(X_0(N)) : Q(g/f)] \) (see Lemma [2-2]). Hence, \( \Xi_G \cap \mathcal{U} \subset \Xi_G' \) by Definition 3-9. 

4. The Case of Hyperelliptic Modular Curves

The goal of the present section is to prove Theorem 4-1. The reader should review Definitions 2-3 and 3-9 and Theorem 3-14.

Recall from [20] that \( X_0(N) \) is a hyperelliptic curve if and only if \( N \) belongs to the set \{22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59, 71\}. Select \( f, g \in S_2(\Gamma_0(N))_Q \) such that their orders at \( a_\infty \) (a cusp corresponding to \( \infty \)) satisfy that \( \nu_{a_\infty}(g) \) is largest possible, and \( \nu_{a_\infty}(f) = \nu_{a_\infty}(g) - 1 \). The existence of \( f \) and \( g \) is easy to check using SAGE system.

**Theorem 4-1.** Assume that \( X_0(N) \) is a hyperelliptic curve, and \( f, g \in S_2(\Gamma_0(N))_Q \) as above. Then, we have the following:

(i) The extension \( Q(g/f) \subset Q(X_0(N)) \) has the degree two, and therefore the Galois group is \( \mathbb{Z}/2\mathbb{Z} \).

(ii) For all even integers \( m \geq 4 \) there exists a non-empty Zariski open set \( \mathcal{U}_m \subset S_m(\Gamma_0(N))_Q \) such that \( L_{f, g, h} = Q(X_0(N)) = Q(g/f, h/f^{m/2}, h \in \mathcal{U}_m) \). We have \( \mathcal{U}_m \subset \Xi'_{\mathbb{Z}/2\mathbb{Z}} \) (see Definition 3-9). Moreover, \( G_{f, g, h} \) consists of \( \mathbb{Z}/2\mathbb{Z} \) and the trivial group.

**Proof.** First, (i) follows from Corollary 3-6 and Lemma 6-1 (see Section 6). Next, we prove that \( G_{f, g, h} \) contains a trivial group. Indeed, note that \( f^2, g f^2, g^2 f^2 \) are \( Q \)-linearly independent cuspidal modular forms in \( S_m(\Gamma_0(N))_Q \). We have

\[
Q(gf^{2m}/f^{m}, g^2f^{2m}/f^{m}) = Q(g/f, (g/f)^2) = Q(g/f) = Q(gf^{2m}/f^{m}).
\]

This implies that \( G_{f, g, h} \) contains the trivial group. Next, by (i),

\[
Q(gf^{2m}/f^m) = Q(g/f) \subset Q(X_0(N))
\]

is a degree two extension. Thus, all groups in \( G_{f, g, h} \) are isomorphically contained in \( S'(2) = \mathbb{Z}/2\mathbb{Z} \). Now, we prove the first claim (ii) which also completes the proof of the last. Since \( g(\Gamma_0(N)) \geq 2 \), for \( m \geq 4 \), by the well–known dimension formula (see for example preliminary [19] Lemma 2.2) we have that

\[
\dim S_m(\Gamma_0(N)) \geq (m - 1)(g(\Gamma_0(N)) - 1) + \left( \frac{m}{2} - 1 \right) \cdot \#\text{ (the number of non–equivalent cusps for } \Gamma_0(N)\text{)} \geq (m - 1)(g(\Gamma_0(N)) - 1) + \left( \frac{m}{2} - 1 \right) \geq g(\Gamma_0(N)) + 2.
\]

Thus, by Lemma [3-5] (ii), there exists a non-empty Zariski open set \( \mathcal{U}_m \) in \( S_m(\Gamma_0(N))_Q \) such that \( Q(X_0(N)) = Q(g/f, h/f^{m/2}) \), for \( h \in \mathcal{U}_m \). We obtain that the degree of
We let $f$ are elements of $S$ new base as follows:

\[ P \leq Q \]

\[ \text{combining with Lemma 3-3, we obtain} \]

\[ \text{in view of notation introduced in Theorem 4-1, we may let} \]

\[ \text{We obtain} \]

\[ \text{(i). Next, we apply methods of Section 2 (see Theorem 2-5). We easily see that} \]

\[ Q \]

\[ \text{We consider an example to Theorem 4-1. Let} \]

\[ N = 30. \text{ Then,} g(\Gamma_0(30)) = 3. \text{ Using SAGE we find the following base of} \]

\[ S_2(\Gamma_0(30)):\]

\[ f_0 = q - q^4 - q^6 - 2q^7 + q^9 + q^{10} + \cdots \]

\[ f_1 = q^2 - q^4 - q^6 - q^8 + q^{10} + \cdots \]

\[ f_2 = q^3 + q^4 - q^5 - q^6 - 2q^7 - 2q^8 + q^{10} + \cdots \]

We let $f = f_1$ and $g = f_2$. Now, we have that

\[ f^2 = q^4 - 2q^6 - q^8 + 5q^{12} + \cdots \]

\[ fg = q^5 + q^6 - 2q^7 - 2q^8 - 2q^9 - 2q^{10} + 2q^{11} + 3q^{12} \ldots \]

are elements of $S_4(\Gamma_0(30))$. By listing the basis of $S_4(\Gamma_0(30))$ using SAGE, we construct a new base as follows: $F = F_0 = f^2$, $G = F_1 = fg$, $F_i = q^{i-1} + \ldots$, $2 \leq i \leq 4$, $F_i = q^{i+1} + \ldots$, $5 \leq i \leq 14$.

Now, we use the Trial method for $(F, G, H)$ (see [19] Section 7]) where $H = \sum_{i=2}^{13} a_i F_i$, $a_i \in \mathbb{Z}$, is to be determined. This method is very simple. Given $H$, we compute the polynomial $P_{F,G,H}$ using SAGE. When

\[ \text{deg} P_{F,G,H} > (\dim S_4(\Gamma_0(30)) + g(\Gamma_0(30)) - 1)/2 = (14 + 3 - 1)/2 = 8, \]

combining with Lemma 3-3, we obtain $Q(X_0(N)) = Q(G/F, H/F) = Q(g/f, H/f^2)$. Thus, in view of notation introduced in Theorem 4-1, we may let $h = H$.

Applying the algorithm, we may obtain $h = H = F_3$. The corresponding polynomial $Q_{f^2, g, h}(\lambda, T)$ (a dehomogenization of $P_{f^2, g, h}$ (see Definition 2-3)) is given by

\[ 225 \lambda^6 (1 - \lambda - \lambda^2 + \lambda^3) T^2 - \lambda^3 (237 - 370\lambda + 319\lambda^2 + 341\lambda^3 - 310\lambda^4 - 101\lambda^5 + 400\lambda^6 - 10\lambda^7 - 64\lambda^8 + 32\lambda^9) T + 12 - 44\lambda - 85\lambda^2 + 153\lambda^3 + 1073\lambda^4 + 1375\lambda^5 - 420\lambda^6 - 660\lambda^7 - 30\lambda^8 + 162\lambda^9 - 26\lambda^{10} - 118\lambda^{11} + 84\lambda^{12} + 20\lambda^{13} + 12\lambda^{14} - 4\lambda^{15}. \]

We see that $Q(f/g) \subset Q(X_0(N))$ is a quadratic extension as it should be by Theorem 4-1 (i). Next, we apply methods of Section 2 (see Theorem 2-5). We easily see that $\tilde{Q}_{f^2, g, h}(\lambda, T)$ is given by

\[ T^2 - \lambda^3 (237 - 370\lambda + 319\lambda^2 + 341\lambda^3 - 310\lambda^4 - 101\lambda^5 + 400\lambda^6 - 10\lambda^7 - 64\lambda^8 + 32\lambda^9) T + 225 \lambda^6 (1 - \lambda - \lambda^2 + \lambda^3) \cdot (12 - 44\lambda - 85\lambda^2 + 153\lambda^3 + 1073\lambda^4 + 1375\lambda^5 - 420\lambda^6 - 660\lambda^7 - 30\lambda^8 + 162\lambda^9 - 26\lambda^{10} - 118\lambda^{11} + 84\lambda^{12} + 20\lambda^{13} + 12\lambda^{14} - 4\lambda^{15}). \]

We let $\lambda \in \mathbb{Z} - A_{f,g,h}$ and reduce polynomial (mod 5). We obtain $T^2 - \lambda^3 (2 - \lambda^2 + \lambda^3 - \lambda^5 + \lambda^8 + 2\lambda^9) T$. Letting $\lambda \equiv 1 \pmod{5}$ (possible as explained in the proof Theorem 2-5) we obtain $T^2 = T(T - 1)$. Considered $G_{f^2, g, h, \lambda}$ as a subgroup of the symmetric group $S(2)$,
we see that it contains a transposition. Hence, $G_{f^2,fg,H} = S(2)$. This recovers the Galois group of the original polynomial $G_{f^2,fg,H}$ by using Hilbert’s irreducibility. More interesting examples are given in Section 5.

5. The Case of Non–Hyperelliptic Modular Curves

By [20], $X_0(N)$ is non–hyperelliptic for $N \in \{34, 38, 42, 43, 44, 45, 51 – 58, 60 – 70\}$ or $N \geq 72$. This implies $g(\Gamma_0(N)) \geq 3$. We assume that in this section. The main result of the present section is the following theorem. The reader should compare to Theorem 4-1. The bound for $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)]$ in the theorem below is far more better than the generic bound $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)] \leq 2g(\Gamma_0(N)) – 2$ given by Corollary 3-6.

**Theorem 5-1.** Maintaining above assumptions, we select $f$ and $g$ in $S_m(\Gamma_0(N))_\mathbb{Q}$ with largest possible orders of vanishing at $a_\infty$ (as in Theorem 4-1 but they are not necessarily consecutive here), $\nu_\infty(f) < \nu_\infty(g)$. Then, $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)] \leq g(\Gamma_0(N))$. Consequently, for $h \in S_2(\Gamma_0(N))_\mathbb{Q} – (\mathbb{Q}f + \mathbb{Q}g)$, $G_{f,g,h}$ can be embedded as a subgroup of the symmetric group of $g(\Gamma_0(N))$–letters $S_{g(\Gamma_0(N))}$ (non–uniquely). Moreover, there exists a subgroup $G$ of $S_{g(\Gamma_0(N))}$ such that $\Xi'_G$ is Zariski dense in (see Definition 3-4).

**Proof.** We let $W_i = \{f \in S_2(\Gamma_0(N)) : f = 0 \text{ or } \nu_{a_\infty}(f) \geq i\}$. Then, by the proof of [19 Corollary 5.6], $\dim W_{g(\Gamma_0(N)) – 2} \geq 3$. This implies $\dim W_{g(\Gamma_0(N)) – 1} \geq 2$. Obviously, we have $f, g \in W_{g(\Gamma_0(N)) – 1}$. Now, in (3-38) there are a lot more cancellations. Namely, $q$–expansions satisfy

$$\begin{align*}
f &= a_l q^l + \cdots, & a_l \neq 0, & l = \nu_\infty(f), \\
g &= b_k q^k + \cdots, & b_k \neq 0, & k = \nu_\infty(g),
\end{align*}$$

where $k > l \geq g(\Gamma_0(N)) – 1$. This implies that

$$\begin{align*}
\epsilon_f &= (l - 1)a_\infty + \cdots, \\
\epsilon_g &= (k - 1)a_\infty + \cdots,
\end{align*}$$

by definition of these divisors [18 Lemma 2.1]. Thus, by (3-38), the divisor of zeroes of $g/f$ has degree

$$2(g(\Gamma_0(N)) – 1) – (l - 1) \leq 2(g(\Gamma_0(N)) – 1) – (g(\Gamma_0(N)) – 2) = g(\Gamma_0(N)).$$

By Lemma 3-5 and Corollary 3-6 we obtain $[\mathbb{Q}(X_0(N)) : \mathbb{Q}(g/f)] \leq g(\Gamma_0(N))$. The rest of claims follow from Lemma 3-10 and Theorem 3-13. 

We continue with an example related to [19, Corollary 5.8] which shows that the result in Theorem 5-1 is optimal. Consider three basis elements of 5–dimensional space $S_2(\Gamma_0(63))$ having highest order of zero at $a_\infty$:

$$f \overset{\text{def}}{=} q^4 + q^7 - 4q^{10} + 2q^{13} - 2q^{16} - 4q^{19} + 5q^{22} + \cdots,$$

$$g \overset{\text{def}}{=} 2q^5 - q^8 - 3q^{11} - q^{14} + 2q^{17} + q^{23} + \cdots,$$

$$h \overset{\text{def}}{=} q^3 - q^6 + q^9 - q^{12} - 2q^{15} - q^{18} - q^{21} + 3q^{24} + \cdots.$$
The reader should observe that \( f \) and \( g \) are chosen as in the hyperelliptic case (see Theorem 4-1). We apply methods of Section 2 (see Theorem 2-5).

**Proposition 5-2.** Maintaining above assumptions, we have \( G_{f,g,h} \simeq S(5) \). Moreover, \( h \in \Xi'_{S(5)} \), and \( Q(g/f, h/f) = Q(X_0(63)) \).

**Proof.** The reduced equation of the curve \( C(f, g, h) \) is computed in SAGE. It is given by the polynomial

\[
P_{f,g,h}(f, g, h) = 2h^4f^2 - hf^5 + h^5g + 2h^2f^3g + h^3fg^2 - f^4g^2 + 3hf^2g^3 - 3h^2g^4 = 0.
\]

This implies

\[
Q_{f,g,h}(\lambda, T) = \lambda T^5 - 2T^4 + \lambda^2 T^3 + (2\lambda - 3\lambda^4) T^2 + (3\lambda^3 - 1) T - \lambda^2.
\]

We have (see Section 2)

\[
\tilde{Q}_{f,g,h}(\lambda, T) = T^5 - 2T^4 + \lambda^3 T^3 + (2\lambda - 3\lambda^4) \lambda^2 T^2 + (3\lambda^3 - 1) \lambda^3 T - \lambda^6.
\]

For \( \lambda \equiv -1 \pmod{3} \), reducing \( \equiv \pmod{3} \), the polynomial (5-3) becomes \( T^5 + T^4 - T^3 + T^2 + T + 1 \) which is irreducible over \( \mathbb{Z}/3\mathbb{Z} \). Since 5 is a prime number, we see that that group \( G_{f,g,h} \) must contain a 5-cycle (see Theorem 2-5). Similarly, for \( \lambda \equiv -1 \pmod{7} \), the polynomial (5-3) becomes a product of two irreducible polynomials

\[
T^5 - 2T^4 - T^3 + 2T^2 + 3T - 1 = (T^2 - T + 3) \cdot (T^3 - T^2 + 4T + 2).
\]

This shows that the Galois group \( G_{f,g,h} \) contains a permutation which is a product of commuting 2-cycle and 3-cycle. Its cube is a transposition. Now, since \( G_{f,g,h} \) is a subgroup of \( S(5) \) (and 5 is a prime number) which contains a 5-cycle and a transposition, by the standard argument, the group is \( S(5) \) (see [11]). Next, by Definition 3-9 to prove \( h \in \Xi'_{S(5)} \), we need to show that \( Q(X_0(N)) : Q(g/f) = g(\Gamma_0(63)) = 5 \). Indeed, by above considerations and Lemma 2-2 we have that

\[
[Q(g/f, h/f) : Q(g/f)] = \deg Q_{f,g,h}(g/f, \cdot) = 5.
\]

But, since by Theorem 5-1 we have

\[
[Q(X_0(63)) : Q(g/f)] \leq g(\Gamma_0(63)) = 5,
\]

we obtain \( Q(g/f, h/f) = Q(X_0(63)) \). The claim follows. Finally, the last claim of the proposition is also proved.

**Remark 5-4.** Keeping \( f \) and \( g \) fixed and letting \( h \) we have computed a considerable number of examples using MAGMA routines mentioned in the introduction. We always obtained \( G_{f,g,h} \simeq S(5) \).

\[\footnote{This also follows by methods of [18] from [19, Corollary 5.8] using Lemma 3-3.}\]
Let $N = 64$. Then, $g(\Gamma_0(64)) = 3$. The basis of $S_2(\Gamma_0(63))$ is

$$f \overset{\text{def}}{=} q^2 - 2q^{10} - 3q^{18} + 6q^{26} + 2q^{34} + \cdots,$$
$$g \overset{\text{def}}{=} q^5 - 3q^{13} + 5q^{29} + q^{37} + \cdots,$$
$$h \overset{\text{def}}{=} q - 3q^9 + 2q^{17} - q^{25} + \cdots,$$

Using SAGE we check that $-f^4 + h^3g + 4hg^3 = 0$. This implies that $Q_{f,g,h}(\lambda, T) = \lambda T^3 + 4\lambda^3T - 1$. Arguing as in Proposition 5.2 but reducing (mod 2) and (mod 5) we easily establish.

**Proposition 5.5.** Maintaining above assumptions, we have $G_{f,g,h} \simeq S(3)$ and $Q(\pi, \kappa)/f, g/f) = Q(X_0(64))$.

The last set of examples is for $N = 72$. We have $g(\Gamma_0(72)) = 5$. Using SAGE, the basis of 5–dimensional space $S_2(\Gamma_0(72))$ is given by

$$f \overset{\text{def}}{=} f_0 \overset{\text{def}}{=} q^5 - 2q^{11} - q^{17} + 4q^{23} - 3q^{29} + \cdots,$$
$$g \overset{\text{def}}{=} f_1 \overset{\text{def}}{=} q^7 - q^{13} - 3q^{19} + q^{25} + 3q^{31} + 4q^{37} + \cdots,$$
$$f_2 \overset{\text{def}}{=} q^3 - q^9 - 2q^{15} + q^{27} + 4q^{33} - 2q^{39} + \cdots,$$
$$f_3 \overset{\text{def}}{=} q^2 - 4q^{14} + 2q^{26} + 8q^{38} + \cdots,$$
$$f_4 \overset{\text{def}}{=} q - 2q^{13} - 4q^{19} - q^{25} + 8q^{31} + 6q^{37} + \cdots.$$

In the following proposition, among other things, we show that $[Q(X_0(72)) : Q(\pi,f)] = 4$ (which is $< g(\Gamma_0(72)) = 5$, see Theorem 5.1).

**Proposition 5.6.** Let $h = f_3$. Then, we have that $G_{f,g,h} \simeq D(4)$ a dihedral group of order $2 \cdot 4 = 8$. Moreover, $Q(\pi, f, g)/f) = Q(X_0(72))$, $[Q(X_0(72)) : Q(\pi,f)] = 4$, and $h \in \Xi'_D(4)$. Moreover, the Galois group of the extension $Q(X_0(72)) \subset L_{f,g,h}$ is generated by a transposition in $D(4)$.

**Proof.** The polynomial $P_{f,g,h}$ is given by

$$f^7 + 7f^4g^3 - 8fg^6 - f^5h^2 - 8f^2g^3h^2 + g^3h^4.$$

This implies

$$\tilde{Q}_{f,g,h}(\lambda, T) = T^4 - \lambda^3(1 + 8\lambda^3)T^2 + \lambda^9(1 + 7\lambda^3 - 8\lambda^6).$$

For $\lambda \equiv -1 \pmod{3}$, reducing $\equiv (\pmod{3})$, the polynomial $\tilde{Q}_{f,g,h}(\lambda, T)$ becomes $T^4 - T^2 - 1$ which is irreducible over $\mathbb{Z}/3\mathbb{Z}$. Thus, $G_{f,g,h}$ must contain a 4–cycle (see Theorem 25). Next, for $\lambda \equiv -1 \pmod{3}$, reducing $\equiv (\pmod{5})$, the polynomial $\tilde{Q}_{f,g,h}(\lambda, T)$ becomes $T^4 - 2T^2 - 1$ which is product of irreducible polynomials $T^2 - T + 2$ and $T^2 + T + 2$ over $\mathbb{Z}/5\mathbb{Z}$. This shows that the Galois group $G_{f,g,h}$ contains a permutation with a cycle pattern 2, 2. Now, we list all transitive groups in $S(4)$ (see [http://galoisdb.math.upb.de/groups?deg=4](http://galoisdb.math.upb.de/groups?deg=4) and [3](#) for notation). They are cyclic group $C(4)$, the Klein group $E(4)$ (order 4 all non–trivial
elements have order 2), the dihedral group $D(4)$ (order 8), the alternating group $A(4)$, and the symmetric group $S(4)$. Clearly, $G_{f,g,h}$ cannot be $C(4)$. It is not also $E(4)$ since it contains a four cycle which has order 4. Also, a four cycle is a product of three transpositions, for example $(1, 2, 3, 4) = (1, 2)(1, 3)(4, 1)$. Thus, $G_{f,g,h}$ cannot be $A(4)$. Thus, $G_{f,g,h}$ is either $D(4)$ or $S(4)$. If it would be $S(4)$, the it would contain a permutation with a cycle pattern 1, 3. Then, by Theorem 2-5, there would exist a prime number $p > 2$ and $\lambda \in \mathbb{Z}$ such that reducing $\equiv \pmod{p}$ the polynomial $\tilde{Q}_{f,g,h}(\lambda, T)$ would be a product of a normalized linear polynomial, say $P_1$, and a cubic normalized irreducible polynomial, say $P_2$, over $\mathbb{Z}/p\mathbb{Z}$. Clearly, $P_1$ is of the form $T - a$, $a \neq 0 \pmod{p}$. Then, $a$ is a zero of $\tilde{Q}_{f,g,h}(\lambda, T) \pmod{p}$. Clearly, $-a$ is also a zero, and since $p > 2$ we have $a \neq -a \pmod{p}$. This is a contradiction since $P_2$ cannot have zeroes in $\mathbb{Z}/p\mathbb{Z}$.

After renumeration, the group $D(4)$ is generated by a 4-cycle $r = (1234)$ and a transposition $s = (13)$ subject to the relation $srs = r^{-1}$. The elements of $D(4)$ are $1, r, r^2, r^3, r^4, sr = (23)(14), s r^2 = (24)$ and $sr^3 = (12)(34)$. Thus, in the chain of field extensions $Q(g/f) \subset Q(g/f, h/f) \subset L_{f,g,h}$, we see that $\text{Gal}(L_{f,g,h}/Q(g/f, h/f))$ must be generated either by $s = (13)$ or $sr^2 = (2, 4)$ since other permutations do not have fixed points and a root $h/f$ of $Q_{f,g,h}(g/f, T)$ must be fixed by elements of $\text{Gal}(L_{f,g,h}/Q(g/f, h/f))$.

Finally, since the deg $P_{f,g,h} = 7 > g(\Gamma_0(72)) - 1 = 4$, the Trial method [19], Section 7 and Lemma 3-3 imply $\tilde{Q}(g/f, h/f) = Q(X_0(72))$. Hence, $[Q(X_0(72)) : Q(g/f)] = 4$. In particular, by Definition 3-9, $h \in \Xi_{D(4)}$.

**Remark 5-7.** By the method described in Section 2 (see Theorem 2-5), a transposition in $G_{f,g,h} = D(4)$ can be seen by taking $\lambda \equiv -1 \pmod{79}$ and reducing $\tilde{Q}_{f,g,h}(\lambda, T) \pmod{79}$. We obtain the polynomial $T^4 - 7T^2 + 14$ which is a product of two linear polynomials $T \pm 4$ and an irreducible quadratic polynomial $T^2 + 9$. By Theorem 2-5, $G_{f,g,h}$ must contain a permutation with a cyclic pattern 1, 1, 2 i.e., a transposition.

**Proposition 5-8.** Let $h = f_3 + f_4$. Then, we have $G_{f,g,h} \simeq S(4)$. Moreover, $h \in \Xi_{S(4)}$, and $Q(g/f, h/f) = Q(X_0(72))$.

**Proof.** The proof is very similar to the proof of Proposition 5-6 but easier. So, we sketch the argument. First, using SAGE, we find that $P_{f,g,h}$ is given by

$$f^8 - f^7g + 8f^5g^3 - 7f^4g^4 + 8f^3g^7 - 16g^6 - 2f^5g^2h + 8f^3g^4h - 16f^2g^5h +$$

$$32g^7h - f^6h^2 + f^5gh^2 - 8f^3g^3h^2 + 8f^2g^4h^2 - 24g^6h^2 + 2f^3g^2h^3 + 8g^5h^3 - 4g^4h^4.$$

Hence, $\tilde{Q}_{f,g,h}(\lambda, T)$ is given by

$$-\lambda^{12}(1 - \lambda + 8\lambda^3 - 7\lambda^4 + 8\lambda^7 - 16\lambda^8) + \lambda^8(2\lambda^2 + 8\lambda^4 - 16\lambda^5 + 32\lambda^7)T -$$

$$-\lambda^5(-1 + \lambda - 8\lambda^3 + 8\lambda^4 - 24\lambda^6)T^2 + (2\lambda^2 + 8\lambda^5)T^3 + T^4$$

For $\lambda \equiv 1 \pmod{3}$, reducing $\equiv \pmod{3}$, the polynomial $\tilde{Q}_{f,g,h}(\lambda, T)$ becomes $1 - T + T^3 + T^4$. This polynomial is irreducible over $\mathbb{Z}/3\mathbb{Z}$. Hence, by Theorem 2-5, the group $G_{f,g,h}$ contains a four cycle. Similarly for $\lambda \equiv 1 \pmod{7}$, reducing $\equiv \pmod{7}$, the polynomial $\tilde{Q}_{f,g,h}(\lambda, T)$ becomes $(-2 + 3T + 3T^2 + T^3)T$ a product of two irreducible polynomials. Hence, $G_{f,g,h}$ contains a permutation with a cycle pattern 1, 3, 3. Now, as in the proof of Proposition
Proposition 5-9. Maintaining above assumptions, let \( h = f_2 \). Then, we have \( G_{f,g,h} \simeq \mathbb{Z}/2\mathbb{Z} \). Next, let \( h \in \Xi_{\mathbb{Z}/2\mathbb{Z}} \) but \( \Xi_{\mathbb{Z}/2\mathbb{Z}}' = \emptyset \).

Proof. As before, using SAGE, we find that \( Q_{f,g,h}(\lambda, T) = \lambda T^2 - T - 2\lambda^2 \). Hence, \( \tilde{Q}_{f,g,h}(\lambda, T) = T^2 - T - 2\lambda^3 \). The result easily follows. For example, for \( \lambda \equiv 0 \pmod{2} \), reducing \( \equiv \pmod{2} \), the polynomial \( \tilde{Q}_{f,g,h}(\lambda, T) \) becomes a product \( T \cdot (T - 1) \). Hence, \( G_{f,g,h} \simeq S(2) \simeq \mathbb{Z}/2\mathbb{Z} \). In particular, \( h \in \Xi_{\mathbb{Z}/2\mathbb{Z}} \).

Finally, for \( h' \in \Xi_{\mathbb{Z}/2\mathbb{Z}} \), the degree of the extension \( \mathbb{Q}(g/f) \subset \mathbb{Q}(g/f, h'/f) \) is two while \( \mathbb{Q}(g/f) \subset \mathbb{Q}(X_0(72)) \) has degree four by Proposition 5-6. Hence, \( \Xi_{\mathbb{Z}/2\mathbb{Z}}' = \emptyset \) (see Definition 5-9).

Remark 5-10. Using [http://galoisdb.math.upb.de/groups?deg=4](http://galoisdb.math.upb.de/groups?deg=4) (see [8] for notation), we may conclude that \( \Xi_{C(4)} = \Xi_{E(4)} = \emptyset \) (see Definition 5-9). Indeed, let \( h' \in \Xi_{C(4)} \) or \( h' \in \Xi_{E(4)} \). Then, the degree \( [\mathbb{Q}(g/f, h'/f) : \mathbb{Q}(g/f)] \) obviously must divide \( [\mathbb{Q}(X_0(72)) : \mathbb{Q}(f/g)] = 4 \) (see Proposition 5-4). Thus, \( [\mathbb{Q}(g/f, h'/f) : \mathbb{Q}(f/g)] = 4 \) (or otherwise \( L_{f,g,h'} = \mathbb{Q}(g/f, h'/f) \) contradicting that it must be a degree four extension of \( \mathbb{Q}(f/g) \)).

We obtain that \( \mathbb{Q}(g/f, h'/f) = \mathbb{Q}(X_0(72)) \) is a Galois extension of \( \mathbb{Q}(f/g) \) with the Galois group \( C(4) \). On the other hand, using \( h \) from Proposition 5-8 we have the Galois extension \( L_{f,g,h} \) of \( \mathbb{Q}(f/g) \) with the Galois group \( S(4) \) containing \( \mathbb{Q}(X_0(72)) \). Now, by Galois theory we conclude that \( S(4) \) has normal subgroup with a quotient of order four. But this is a contradiction since \( S(4) \) has no normal subgroup of order \( 4!/4 = 6 \).

6. The Proof of Lemma 5-1

In this section we prove the following lemma used in the proof of Theorem 4-1:

Lemma 6-1. Maintaining the assumptions of Theorem 4-1, we have that \( C \subset C(N) \) is a degree two extension.

Proof. This claim is contained in [23, Lemma 2] but we give different proof using our previous work [18] combined with certain simple computations in SAGE.

First, we assume that we have \( g(\Gamma_0(N)) = 2 \) i.e., \( N = 22, 23, 26, 28, 29, 31, 37, 50 \). We use results recalled in the proof of Theorem 3-13 up to the formula in (3-7). The divisor of zeroes must be \( e_0 \) since otherwise the divisor of zeroes would have degree one, and we would obtain \( C(X_0(N)) = C(g/f) \). Hence, \( X_0(N) \) would have a genus 0 which is a contradiction. This proves (6-1) when \( g(\Gamma_0(N)) = 2 \). Next, we assume that \( g(\Gamma_0(N)) \geq 3 \) i.e.,

\[
N = 30, 33, 35, 39, 40, 41, 46, 47, 48, 59, 71.
\]

Then, above method does not work since the degree of divisors \( e_0 \) and \( e_0 \) is \( 2(g(\Gamma_0(N)) - 1) \geq 4 \). We need to dig deeper into the geometry and computations in SAGE. We write \( f_0, \ldots, f_{g(\Gamma_0(N)) - 1} \) for the basis of \( S_2(\Gamma_0(N)) \). By Eichler–Shimura theory [22, Theorem 3.5.2] we see that they have integral \( q \)-expansions, and using SAGE system we can easily check that their \( q \)-expansions are of the form

\[
f_i = a_i q^{i+1} + \cdots, \quad 0 \leq i \leq g(\Gamma_0(N)) - 1.
\]
where $a_i \neq 0$. By definition of $f$ and $g$, we see that $g = \lambda f_{\gamma_0(N)-1}$ and $f = \mu f_{\gamma_0(N)-2} + \nu f_{\gamma_0(N)-1}$, for some $\lambda, \mu, \nu \in \mathbb{Q}$, $\lambda, \mu \neq 0$. So, in order to prove (6-5), we may assume $f = f_{\gamma_0(N)-2}$, and $\gamma = f_{\gamma_0(N)-1}$.

In what follows we do not need letter $\gamma$ to denote a cuspidal form, so we may put $\gamma = \gamma(\Gamma_0(N))$. We consider the analogue of the map (2-1) given by

$$a_z \mapsto (f_{\gamma-3}(z) : f_{\gamma-2}(z) : f_{\gamma-1}(z)), \quad z \in \mathbb{H}.$$  

(6-4)

Let $d(f_{\gamma-3}, f_{\gamma-2}, f_{\gamma-1})$ be the degree of that map (it is explained in detail in [18]). We recall that $d(f_{\gamma-3}, f_{\gamma-2}, f_{\gamma-1})$ is a degree of the field extension $\mathbb{C}(\mathcal{C}(f_{\gamma-3}, f_{\gamma-2}, f_{\gamma-1})) \subset \mathbb{C}(X_0(N))$. This means that the map (6-4) is generically $d$–to–1 map (see [18, Lemma 3.4]). We prove (6-5)

$$d(f_{\gamma-3}, f_{\gamma-2}, f_{\gamma-1})$$

is an even integer.

In order to prove (6-5), let $K$ be the canonical divisor on $X_0(N)$ i.e., a divisor attached to a non–zero meromorphic differential form on $X_0(N)$. The regular map attached to $K$ is explicitly described in [7]:

$$X_0(N) \rightarrow \mathbb{P}^{g-1}, \quad a_z \mapsto (f_0(z) : f_1(z) : \cdots : f_{g-1}), \quad z \in \mathbb{H}.$$  

(6-6)

The image is an irreducible projective curve, say $C(f_0, \ldots, f_{g-1})$. It is well–known that this maps is generically two–to–one since our curve is hyperelliptic. This means that the degree of the field extension $\mathbb{C}(\mathcal{C}(f_0, \ldots, f_{g-1})) \subset \mathbb{C}(X_0(N))$ is equal to 2.

The map (6-4) can be considered as a rational map (i.e., defined on a open subset), and factored as a dominant rational map in a composition of the map (6-6) followed by the restriction of the projection $\mathbb{P}^{g-1} \rightarrow \mathbb{P}^2$ given by $(y_0 : y_1 : \cdots : y_{g-1}) \mapsto (y_{g-3} : y_{g-2} : y_{g-1})$ which is defined on a non–empty Zariski open set of the image $C(f_0, \ldots, f_{g-1})$. (For example, on the complement of the finite set of zeroes in $\mathbb{H}$ of the cuspidal modular form $f_{g-3} f_{g-2} f_{g-1}$ of weight 6.) Let $d$ be the degree of the projection restricted to the curve $C(f_0, \ldots, f_{g-1})$. By definition, this is a degree of the field extension $\mathbb{C}(\mathcal{C}(f_{g-3}, f_{g-2}, f_{g-1})) \subset \mathbb{C}(C(f_0, \ldots, f_{g-1}))$. Thus, considering chain field extensions $\mathbb{C}(\mathcal{C}(f_{g-3}, f_{g-2}, f_{g-1})) \subset \mathbb{C}(C(f_0, \ldots, f_{g-1})) \subset \mathbb{C}(X_0(N))$, we see that $d(f_{g-3}, f_{g-2}, f_{g-1}) = 2d$. This proves (6-5).

Next, by the main result of [18], the product $d(f_{g-3}, f_{g-2}, f_{g-1}) \cdot \deg P_{f_{g-3}, f_{g-2}, f_{g-1}}$ is given by

$$2(g - 1) - \sum_{a \in X_0(N)} \min \left( \epsilon_{f_{g-3}}(a), \epsilon_{f_{g-2}}(a), \epsilon_{f_{g-1}}(a) \right),$$

where effective divisors $\epsilon_{f_{g-3}}, \epsilon_{f_{g-2}}, \text{ and } \epsilon_{f_{g-1}}$ are defined by [18, Lemma 2.1]. By (6-3), we have

$$\sum_{a \in X_0(N)} \min \left( \epsilon_{f_{g-3}}(a), \epsilon_{f_{g-2}}(a), \epsilon_{f_{g-1}}(a) \right) \geq \min \left( \epsilon_{f_{g-3}}(a_\infty), \epsilon_{f_{g-2}}(a_\infty), \epsilon_{f_{g-1}}(a_\infty) \right) = g - 3.$$

Thus, we obtain the following:

$$d(f_{g-3}, f_{g-2}, f_{g-1}) \cdot \deg P_{f_{g-3}, f_{g-2}, f_{g-1}} \leq 2(g - 1) - (g - 3) = g + 1.$$  

(6-7)

Considering case by case analysis based on (6-2) (described below), we compute equations in SAGE, and find that $\deg P_{f_{g-3}, f_{g-2}, f_{g-1}} = 2$ for all $N$ in (6-2). Using (6-5) and (6-7), we obtain $d(f_{g-3}, f_{g-2}, f_{g-1}) = 2$ in all cases. This means that $\mathbb{C}(X_0(N))$ is a quadratic extension
of $\mathbb{C}(C(f_{g-3}, f_{g-2}, f_{g-1}))$. Since the explicit computations below show $\mathbb{C}(C(f_{g-3}, f_{g-2}, f_{g-1}))$ is equal to $\mathbb{C}(f_{g-1}/f_{g-2})$, the proof lemma is complete.

Now, we give case by case analysis mentioned above. Assume $N = 30$. We have $g = 3$. The equation of $C(f_{g-3}, f_{g-2}, f_{g-1})$ is given by the irreducible polynomial $-x_1^3 + x_0x_2 - x_1x_2$. We have

$$\mathbb{C}(C(f_{g-3}, f_{g-2}, f_{g-1})) = \mathbb{C}(f_{g-3}/f_{g-2}, f_{g-1}/f_{g-2}) = \mathbb{C}(f_{g-1}/f_{g-2})$$

since the equation of the curve implies $-f_{g-2}^2 + f_{g-3}f_{g-1} - f_{g-2}f_{g-1} = 0$. Analogously, we treat remaining cases. We leave details to the reader.

Assume that $N = 33, 35, 39, 40, 41,$ or $48$. We have $g = 3$. The equations of curves $C(f_{g-3}, f_{g-2}, f_{g-1})$ are given by the irreducible polynomials $-x_1^2 + x_0x_2 - 2x_2^2$, $-x_1^3 - x_0x_2 + 2x_1x_2 - x_2^2$, $-x_1^2 + x_0x_2 + x_1x_2$, $-x_1^2 + x_0x_2 + x_2^2$, $-x_1^2 + x_0x_2 + 2x_1x_2$, and $-x_1^2 + x_0x_2$, respectively.

Assume $N = 47$. Then, $g = 4$. The equation of $C(f_{g-3}, f_{g-2}, f_{g-1})$ is given by the irreducible polynomial $-x_1^3 + x_0x_2 + 2x_1x_2 - 3x_2^2$.

Assume that $N = 46$ or $59$. Then, $g = 5$. The equations of $C(f_{g-3}, f_{g-2}, f_{g-1})$ are given by the irreducible polynomials $-x_1^2 + x_0x_2 - x_1x_2$ and $-x_1^2 + x_0x_2 + 2x_1x_2 - 3x_2^2$, respectively.

Assume $N = 71$. Then, $g = 6$. The equation of $C(f_{g-3}, f_{g-2}, f_{g-1})$ is given by the irreducible polynomial $-x_1^3 + x_0x_2 + 2x_1x_2 - 3x_2^2$. \hfill \Box

References

[1] R. Bröker, K. Lauter, A. V. Sutherland, Modular polynomials via isogeny volcanoes, Mathematics of Computation 81, 1201–1231, (2012).

[2] B. Cho, N. M. Kim, J. K. Koo, Affine models of the modular curves $X(p)$ and its application, Ramanujan J. 24, no. 2, 235–257, (2011).

[3] J. H. Conway, A. Hulpke, J. McKay, On transitive permutation groups, LMS J. Computation and Mathematics, 1(1998), 1–8.

[4] C. Fieker, Galois groups of polynomials over $\mathbb{Q}(t)$ (2008), Magma implementation.

[5] C. Fieker, J. Klüners, Computation of Galois groups of rational polynomials, LMS J. Comput. Math. 17 (2014), no. 1, 141–158.

[6] C. Fieker, N. Sutherland, Constructions using Galois Theory, https://arxiv.org/abs/2010.01281, 2020.

[7] S. Galbraith, Equations for modular curves, Ph.D. thesis, Oxford (1996)

[8] N. Ishida, Generators and equations for modular function fields of principal congruence subgroups, Acta Arithmetica, 85 no 3, 197–207, (1998).

[9] D. Krumm, N. Sutherland, Galois groups over rational functional fields and explicit Hilbert irreducibility, J. Symbolic Comput. 103 (2021), 108–126.

[10] I. Kodrnja, On a simple model of $X_0(N)$, Monatsh. Math. 186 (2018), no. 4, 653–661.

[11] S. Lang, Algebra, Second edition., Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984.

[12] Magma Computational Algebra System (Version Magma V2.26), Computational Algebra Group at the University of Sydney, 2021, http://magma.maths.usyd.edu.au/magma/

[13] T. Miyake, Modular forms, Springer-Verlag, (2006).

[14] R. Miranda, Algebraic Curves and Riemann Surfaces, Graduate Studies in Mathematics 5, (1995).

[15] G. Muić, Modular curves and bases for the spaces of cuspidal modular forms, Ramanujan J. 27, 181–208, (2012)

[16] G. Muić, On embeddings of modular curves in projective spaces, Monatsh. Math. Vol. 173, No. 2, 239–256, (2014).
[17] G. Muić, D. Mikoč, Birational maps of $X(1)$ into $\mathbb{P}^2$, Glasnik Matematicki Vol. 48, No. 2, 301–312, (2013).

[18] G. Muić, On degrees and birationality of the maps $X_0(N) \to \mathbb{P}^2$ constructed via modular forms, Monatsh. Math. Vol. 180, No. 3, 607–629, (2016).

[19] G. Muić, I. Kodrnja On primitive elements of algebraic function fields and models of $X_0(N)$, The Ramanujan Journal, 55 No. 2 (2021), 393–420 doi:10.1007/s11139-021-00423-w.

[20] A. P. Ogg, Hyperelliptic modular curves. Bull. Soc. Math. France 102 (1974), 449–462.

[21] I. R. Shafarevich, Basic algebraic geometry I: Varieties in projective space 3rd edition, Springer, 2013.

[22] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Kanô Memorial Lectures, No. 1. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., (1971)

[23] M. Shimura, Defining Equations of Modular Curves $X_0(N)$, Tokyo J. Math. Vol. 18, No. 2, (1995)

[24] K. Ono, The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and $q$-Series, Conference Board of the Mathematical Sciences 102, American Mathematical Society (2004).

[25] Sage Mathematics Software (Version 8.8), The Sage Developers, 2019, http://www.sagemath.org

[26] J. P. Serre, Topics in Galois theory. Lecture notes prepared by Henri Darmon [Henri Darmon]. With a foreword by Darmon and the author. Research Notes in Mathematics, 1. Jones and Bartlett Publishers, Boston, MA, 1992.

[27] Y. Yifan, Defining equations of modular curves, Advances in Mathematics 204, 481–508, (2006)

Faculty of Geodesy, University of Zagreb, Kačićevo 26, 10000 Zagreb, Croatia
Email address: ikodrnja@geof.hr

Department of Mathematics, Faculty of Sciences, University of Zagreb, Bijenička 30, 10000 Zagreb, Croatia
Email address: gmuic@math.hr