GALOIS GROUP $PGL_2(\mathbb{Z}_n)$

MICHAEL TSIANG
UNIVERSITY OF BRITISH COLUMBIA
MATH 509

Abstract. A well known open problem is the Inverse Galois Theory Problem, which asks which groups can be realized as a Galois group over a given field k, in particular, when $k = \mathbb{Q}$. Due to Hilbert's irreducibility theorem, it suffices to consider Galois groups over a function field $\mathbb{Q}(z)$.

In this paper, I will show that the projective general linear group $PGL_2(\mathbb{Z}_n)$ over the group of integers mod n can be realized as a Galois group over $\mathbb{Q}(j)$, where j is the elliptic modular function. The approach taken in this paper follows the proof given by A.M. Macbeath [4].

1. Elliptic Modular Functions

We begin with some background on lattices and modular functions. Let $\mathbb{C}$ denote the complex plane, and $\mathbb{H}^2 = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ denote the upper half plane.

1.1 Definition. A *lattice* Ω is a discrete subgroup of $\mathbb{C}$ such that

$$\Omega = \Omega(\omega_1, \omega_2) = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\},$$

for fixed $\omega_1, \omega_2 \in \mathbb{C}$, where ω_1, ω_2 are linearly independent over $\mathbb{R}$. We say $\{\omega_1, \omega_2\}$ is a *basis* for Ω.

1.2 Remark. One can show[2] that if $\{\omega_1, \omega_2\}$ is a basis for a lattice Ω, then $\{c\omega_2 + d\omega_1, a\omega_2 + b\omega_1\}$, where $a, b, c, d \in \mathbb{Z}$, is also a basis for Ω if and only if $ad - bc = \pm 1$.

1.3 Definition. Let Ω be a lattice. Then the *Eisenstein series* for Ω is

$$E_k = E_k(\Omega) = \sum_{\omega \in \Omega}{}' \omega^{-k}.$$

1.4 Remark. (a) Note that E_k converges absolutely if and only if $k \geq 3$.
(b) Let Ω be a lattice. Define

$$g_2 = g_2(\Omega) = 60E_4 = 60\sum_{\omega \in \Omega}{}' \omega^{-4},$$

$$g_3 = g_3(\Omega) = 140E_6 = 140\sum_{\omega \in \Omega}{}' \omega^{-6}.$$

The notation for g_2 and g_3 arises from the differential equation for the Weierstrass $\wp$-function, $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$. The *discriminant* of the cubic polynomial $p(z) = 4z^3 - g_2 z - g_3$ is $\Delta = g_2^3 - 27g_3^2$.

Date: April 11, 2005.

1.5 Definition. Let Ω be a lattice. We define the *elliptic modular function* j by

$$j(\Omega) = \frac{(12g_2(\Omega))^3}{\Delta(\Omega)} = \frac{(12g_2)^3}{g_2^3 - 27g_3^2}.$$

1.6 Remark.[2] By considering the zeros of $\wp'$, for any lattice Ω, one can show that the roots of the polynomial $p(z) = 4z^3 - g_2 z - g_3$ are distinct, which implies the discriminant $\Delta = g_2^3 - 27g_3^2$ is never zero. Thus the denominator of j never vanishes.

1.7 Definition. Let $\mu \in \mathbb{C}$. Two lattices Ω, Ω' are *similar* if $\Omega' = \mu\Omega$ for some $\mu \neq 0$. This is clearly an equivalence relation.

1.8 Remark. (a) For any lattice Ω with basis $\{\omega_1, \omega_2\}$, there is a similar lattice Ω' with basis $\{1, \omega_2/\omega_1\}$, where $\mu = 1/\omega_1$. Since ω_1 and ω_2 are linearly independent over $\mathbb{R}$, then $\mathrm{Im}(\omega_2/\omega_1) \neq 0$. Thus we can assume $\mathrm{Im}(\omega_2/\omega_1) > 0$, as we can always switch the roles of ω_1 and ω_2.
(b) If Ω is a lattice with basis $\{\omega_1, \omega_2\}$, we define the *modulus* of the basis $\{\omega_1, \omega_2\}$ to be $\tau = \omega_2/\omega_1$, where ω_1, ω_2 are chosen so that $\mathrm{Im}(\tau) > 0$, i.e., $\tau \in \mathbb{H}^2$. Each lattice Ω determines a set of moduli, the moduli of different bases. By Remark 1.2 and Definition 1.7, if Ω' is similar to Ω, then basis elements ω_1', ω_2' of Ω' are of the form

$$\omega_2' = \mu(a\omega_2 + b\omega_1)$$
$$\omega_1' = \mu(c\omega_2 + d\omega_1),$$

where $\mu \in \mathbb{C}, \mu \neq 0$, $a, b, c, d \in \mathbb{Z}, ad - bc = \pm 1$. So the modulus of $\{\omega_1', \omega_2'\}$ is

$$\tau' = \frac{\mu(a\omega_2 + b\omega_1)}{\mu(c\omega_2 + d\omega_1)} = \frac{a\omega_2 + b\omega_1}{c\omega_2 + d\omega_1} = \frac{a\frac{\omega_2}{\omega_1} + b\frac{\omega_1}{\omega_1}}{c\frac{\omega_2}{\omega_1} + d\frac{\omega_1}{\omega_1}} = \frac{a\tau + b}{c\tau + d}$$

Remark 1.2 and the second equality imply similar lattices determine the same set of moduli. We know $\tau, \tau' \in \mathbb{H}^2$ and $ad - bc = \pm 1$; if $ad - bc = -1$, then the linear fractional transformation $T : z \mapsto (az + b)/(cz + d)$ sends the upper half plane $\mathbb{H}^2$ to the lower half plane. But since $\tau' = T(\tau) \in \mathbb{H}^2$, then $ad - bc \neq -1$. Therefore $ad - bc = 1$. We can conclude then that Ω and Ω' are similar if and only if $\tau' = T(\tau)$, where T is an element of the *modular group* Γ, defined by

$$\Gamma = \left\{ T : z \mapsto \frac{az + b}{cz + d} \;\middle|\; a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

We can think of Γ as the group $PSL_2(\mathbb{Z})$ acting on $\mathbb{H}^2$ by linear fractional transformations. For convenience, we will consider the transformation and the matrix corresponding to the transformation as equivalent, and thus say $\Gamma = PSL_2(\mathbb{Z})$.

1.9 Proposition. *Let $\mu \in \mathbb{C}, \mu \neq 0$. Then $j(\mu\Omega) = j(\Omega)$.*
Proof.
For a similar lattice $\mu\Omega$, we have

$$g_2(\mu\Omega) = 60 \sum_{\omega \in \Omega}{}' (\mu\omega)^{-4} = \mu^{-4} 60 \sum_{\omega \in \Omega}{}' \omega^{-4} = \mu^{-4} g_2(\Omega),$$
$$g_3(\mu\Omega) = 140 \sum_{\omega \in \Omega}{}' (\mu\omega)^{-6} = \mu^{-6} 140 \sum_{\omega \in \Omega}{}' \omega^{-6} = \mu^{-6} g_3(\Omega),$$

which yields

$$\begin{aligned} j(\mu\Omega) &= \frac{(12\mu^{-4}g_2(\Omega))^3}{(\mu^{-4}g_2(\Omega))^3 - 27(\mu^{-6}g_3(\Omega))^2} \\ &= \frac{\mu^{-12}(12g_2(\Omega))^3}{\mu^{-12}(g_2(\Omega)^3 - 27g_3(\Omega)^2)} \\ &= \frac{(12g_2(\Omega))^3}{g_2(\Omega)^3 - 27g_3(\Omega)^2} \\ &= j(\Omega). \ \square \end{aligned}$$

1.10 Remark. The previous proposition states that similar lattices yield the same value of j. Remark 1.8(a) then implies that we can consider j on the lattice $\Omega(1,\tau)$, where τ is a modulus of one of the bases of Ω. So we can think of g_2, g_3, Δ, and j as functions of one complex variable $\tau \in \mathbb{H}^2$. In an abuse of notation, we will write $j(\tau)$ to mean $j(\Omega(1,\tau))$.

1.11 Proposition. *$j(T(\tau)) = j(\tau)$ for all $\tau \in \mathbb{H}^2, T \in \Gamma$.*
Proof.
If $\tau' = T(\tau)$ for some $T \in \Gamma$, then Remark 1.8(b) implies $\Omega(1,\tau)$ and $\Omega' = \Omega(1,\tau')$ are similar. Then by Proposition 1.9, $j(T(\tau)) = j(\tau') = j(\tau)$. $\square$

1.12 Remark. The converse of Proposition 1.11 is also true, i.e., if $j(\tau_1) = j(\tau_2)$, then $\tau_1 = T(\tau_2)$ for some $T \in \Gamma$. This result is a corollary of a larger theorem which we will state next.

1.13 Theorem.[2] *For each $c \in \mathbb{C}$, there is exactly one orbit of Γ in $\mathbb{H}^2$ on which j takes the value c.*

1.14 Theorem.[1] *If $\tau \in \mathbb{H}^2$ and $q = e^{2\pi i\tau}$, we have the Fourier expansion*

$$j(\tau) = \frac{1}{q} + \sum_{k=0}^{\infty} c_k q^k,$$

where the c_k are integers.

1.15 Definition. Let $\tau \in \mathbb{H}^2$. A *modular function* f is a function such that

(i) f is meromorphic in $\mathbb{H}^2$,
(ii) $f(T(\tau)) = f(\tau)$ for all $T \in \Gamma$, and
(iii) f has a Fourier expansion of the form

$$f(\tau) = \sum_{k=-m}^{\infty} a_k q^k.$$

1.16 Theorem.[3] *Let f be a modular function which is analytic in $\mathbb{H}^2$ with a Fourier expansion*

$$f(\tau) = \sum_{k=0}^{\infty} a_k q^k,$$

where $q = e^{2\pi i\tau}$ for $\tau \in \mathbb{H}^2$. Then f is a polynomial in j with coefficients in the field generated by the Fourier coefficients a_k.

1.17 Corollary. *A modular function with rational Fourier series belongs to the field $\mathbb{Q}(j(\tau))$, for $\tau \in \mathbb{H}^2$.*

Proof.[4]
Let f be a modular function with rational Fourier series. Then by definition, f is meromorphic, so f has a finite number of poles. This implies there are only a finite number of orbits of Γ at which $f(\tau)$ has poles. Let F be a finite set of points in $\mathbb{H}^2$ including one point p from each orbit of Γ in which $f(\tau)$ has a pole. Let $\nu(p)$ denote the order of the pole at p. Then the function

$$\phi(\tau) = f(\tau) \prod_{p \in F} (j(\tau) - j(p))^{\nu(p)}$$

is analytic in $\mathbb{H}^2$. By Theorem 1, $\phi(\tau)$ is a polynomial in $j(\tau)$, so $f(\tau)$ is a rational function of $j(\tau)$ with coefficients in $\mathbb{C}$. This implies there is a linear dependence between a finite set of functions $[j(\tau)]^m, [j(\tau)]^n f(\tau)$. We can find the dependence by solving a set of linear equations whose coefficients are the Fourier coefficients of f. Since the coefficients are rational by assumption, then $f(\tau) \in \mathbb{Q}(j(\tau))$, as desired. □

2. Sublattices

To define the necessary fields and field extensions to construct our desired Galois group, we will consider sublattices of index n. For this section, let Ω be a lattice with basis $\{\omega_1, \omega_2\}$ so that its modulus $\tau = \omega_2/\omega_1$ is in $\mathbb{H}^2$, and let the modular group be denoted by $\Gamma = PSL_2(\mathbb{Z})$. Finally, let n be a positive integer.

2.1 Definition. If $a, b, c, d \in \mathbb{Z}$ and $ad - bc = n$, then the pair of periods $c\omega_1 + d\omega_2,\ a\omega_1 + b\omega_2$ generates a *sublattice* $\Omega_0 \subset \Omega$.

2.2 Proposition. *A sublattice $\Omega_0 \subset \Omega$ with basis $\{c\omega_1 + d\omega_2, a\omega_1 + b\omega_2\}$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = n$, has index n in Ω. Moreover, if $\gcd(a, b, c, d) = 1$, then $\Omega/\Omega_0 \cong \mathbb{Z}_n$.*

Proof.
Clearly Ω_0 is a subgroup of Ω. Since the basis of Ω_0 can be seen as an element of $GL_2(\mathbb{Z})$ with determinant n acting on the basis of Ω, we see that Ω_0 has index n in Ω. By definition, $\Omega \cong \mathbb{Z} \oplus \mathbb{Z}$. Since Ω is abelian, then Ω_0 is normal in Ω. By the Fundamental Theorem of Finitely Generated Abelian Groups, we have

$$\Omega/\Omega_0 \cong \mathbb{Z}/(c\omega_1 + d\omega_2) \oplus \mathbb{Z}/(a\omega_1 + b\omega_2) = \mathbb{Z}_\alpha \oplus \mathbb{Z}_\beta,$$

where $\alpha|\beta$ and $\alpha\beta = ad - bc = n$. If $\gcd(a, b, c, d) = 1$, then we can change the bases of Ω and Ω_0 so that

$$\Omega/\Omega_0 \cong \mathbb{Z}/(1) \oplus \mathbb{Z}/((a\omega_1 + b\omega_2)/(c\omega_1 + d\omega_2)) = \mathbb{Z}_n. \ \square$$

2.3 Remark. (a) Let Ω_0 be a sublattice defined as above, with $\gcd(a, b, c, d) = 1$. Since $\Omega/\Omega_0 \cong \mathbb{Z}_n$ by Proposition 2.2, then $n\Omega \subset \Omega_0 \subset \Omega$. Let $\overline{\omega}$ denote the image of $\omega \in \Omega$ under the natural map $\Omega \to \Omega/n\Omega \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. We see then that $\alpha\overline{\omega}$ is the same for any α in the equivalence class $\bar{\alpha} \pmod n$, so we write $\bar{\alpha}\overline{\omega}$ for $\alpha\overline{\omega}$, for

all $\alpha \in \mathbb{Z}$. Thus $\overline{c\omega}_1 + \overline{d\omega}_2, \overline{a\omega}_1 + \overline{b\omega}_2$ generate $\overline{\Omega}_0$, the image of Ω_0.
(b) Let E_n denote the set of sublattices $\Omega_0 \subset \Omega$ such that $\Omega/\Omega_0 \cong \mathbb{Z}_n$, and let $\overline{E}_n$ denote the set of subgroups G of $\mathbb{Z}_n \oplus \mathbb{Z}_n$ such that $(\mathbb{Z}_n \oplus \mathbb{Z}_n)/G \cong \mathbb{Z}_n$. By the Correspondence Theorem[5], the correspondence $\Omega_0 \to \overline{\Omega}_0$ is an injective mapping between E_n and $\overline{E}_n$. Since $\overline{E}_n$ is finite, then E_n is finite. In fact,[4] the number N of elements in E_n is

$$N = n \prod_{p|n} \left(1 + \frac{1}{p}\right).$$

(c)[4] If $\Omega_0 \in E_n$, let d be the least positive integer such that $d\omega_1 \in \Omega_0$. Extending $d\omega_1$ to a basis of Ω_0, we obtain a basis of the form $\{d\omega_1, a\omega_2 + b\omega_1\}$, where $ad = n$ and $\gcd(a, b, d) = 1$. This means a is uniquely determined, but b is only determined modulo d, so we add the condition $0 \le b \le d - 1$. Then the set of functions of τ defined by

$$\{j(\Omega_0) \mid \Omega_0 \in E_n\}$$

is identical to the set of functions

$$j\left(\frac{a\tau + b}{d}\right), \ ad = n, \ \gcd(a, b, d) = 1, \ 0 \le b \le d - 1.$$

For notational convenience, we write the Fourier expansion of $j(\tau)$ given in Theorem 1.14 as

$$j(\tau) = \sum_{k=-\infty}^{\infty} c_k q^k$$

for $c_k = 0$ when $k \le -2$, where $q = e^{2\pi i \tau}$. By plugging in $(a\tau + b)/d$ in for τ, we have

$$\begin{aligned} j\left(\frac{a\tau + b}{d}\right) &= \sum_{k=-\infty}^{\infty} c_k \left(e^{2\pi i\left(\frac{a\tau+b}{d}\right)}\right)^k \\ &= \sum_{k=-\infty}^{\infty} c_k \left(e^{2\pi i a\tau/d} e^{2\pi i b/d}\right)^k \\ &= \sum_{k=-\infty}^{\infty} c_k \left(\left(e^{2\pi i\tau/n}\right)^{a^2} \left(e^{2\pi i/n}\right)^{ab}\right)^k \\ &= \sum_{k=-\infty}^{\infty} c_k \zeta^{abk} \left(q^{1/n}\right)^{a^2 k} \end{aligned}$$

using the fact that $ad = n$, with $\zeta = e^{2\pi i/n}$. This calculation shows that the Fourier expansion of $j(\Omega_0)$ is in powers of $q^{1/n}$ and all the Fourier coefficients belong to the field $\mathbb{Q}(\zeta)$, where ζ is a primitive nth root of unity.

2.4 Definition. Let K denote the field $\mathbb{Q}(j(\Omega))$ consisting of all rational epxressions in $j(\Omega)$ with rational coefficients.
Let L denote the field $\mathbb{Q}(j(\Omega); j(\Omega_0), \Omega_0 \in E_n)$ obtained by adjoining to K the functions $j(\Omega_0)$ corresponding to all the lattices $\Omega_0 \in E_n$.
Let L_R denote the subfield consisting of all functions in L which have Fourier expansions in powers of $q^{1/n}$ with rational coefficients.
Let L_M denote the subfield consisting of all functions in L which are modular functions.

2.5 Remark. By Theorem 1.16 and Corollary 1.17, $K = L_R \cap L_M$.

3. The Galois Group of L over K

In this section, we consider the group $PGL_2(\mathbb{Z}_n)$ acting as a group of automorphisms on L. We will see the group permutes the sublattices $\Omega_0 \in E_n$. Then we will look at two subgroups of $PGL_2(\mathbb{Z}_n)$ and thus compute the Galois group of L over K. Let all notation be as in the previous section.

3.1 Proposition. *The group $PGL_2(\mathbb{Z}_n)$ permutes the sublattices in E_n transitively.*

Proof.
Clearly the group $GL_2(\mathbb{Z}_n)$ of matrices

$$A = \begin{bmatrix} \bar{f} & \bar{g} \\ \bar{h} & \bar{k} \end{bmatrix},$$

where $\bar{f}, \bar{g}, \bar{h}, \bar{k} \in \mathbb{Z}_n$ and determinant $\bar{f}\bar{k} - \bar{g}\bar{h}$ a unit, is the automorphism group of $\mathbb{Z}_n \oplus \mathbb{Z}_n$ and thus permutes the set of subgroups $\overline{E}_n$. If a group $G \in \overline{E}_n$ is generated by $r_i\overline{\omega}_1 + s_i\overline{\omega}_2$, then its image under $A \in GL_2(\mathbb{Z})$ is generated by $r_i(\bar{f}\overline{\omega}_1 + \bar{g}\overline{\omega}_2) + s_i(\bar{h}\overline{\omega}_1 + \bar{k}\overline{\omega}_2)$. If $\bar{k} \in \mathbb{Z}_n$ is a unit, then $\overline{\omega}$ and $\bar{k}\overline{\omega}$ generate the same subgroup, which implies that the scalar matrices $\bar{k}I$ map every element of $\overline{E}_n$ onto itself. Thus $GL_2(\mathbb{Z}_n)/\{\bar{k}I\} = PGL_2(\mathbb{Z}_n)$ permutes the subgroups in $\overline{E}_n$ transitively. Then by the correspondence $\Omega_0 \leftrightarrow \overline{\Omega}_0$, we have that $PGL_2(\mathbb{Z}_n)$ permutes the sublattices in E_n transitively. $\square$.

3.2 Definition. Let Δ_n denote the subgroup of $PGL_2(\mathbb{Z}_n)$ consisting of diagonal matrices

$$\begin{bmatrix} \bar{l} & 0 \\ 0 & \bar{k} \end{bmatrix},$$

and let $PSL_2(\mathbb{Z}_n)$ denote the subgroup of $PGL_2(\mathbb{Z}_n)$ of all matrices with determinant $\bar{1}$.

3.3 Theorem. *The group Δ_n acts as a group of automorphisms of L. Its fixed field is L_R.*

Proof.[4]
Consider the transformation

$$T = \begin{bmatrix} 1 & 0 \\ 0 & \bar{k}^{-1} \end{bmatrix}$$

applied to the lattice Ω_0 generated by the basis $\{d\omega_1, a\omega_2 + b\omega_1\}$. Then $\overline{\Omega}_0$ is generated by the basis $\{\bar{d}\omega_1, \bar{a}\overline{\omega}_2 + \bar{b}\overline{\omega}_1\}$ is mapped by T onto the subgroup generated by $\bar{d}\overline{\omega}_1$ and $\bar{k}^{-1}\bar{a}\overline{\omega}_2 + \bar{b}\overline{\omega}_1$. Since $\bar{k}$ is a unit, then the subgroup generated by $\bar{k}^{-1}\bar{a}\overline{\omega}_2 + \bar{b}\overline{\omega}_1$ is the same as that generated by $\bar{a}\overline{\omega}_2 + \bar{k}\bar{b}\overline{\omega}_1$, so T maps Ω_0 on the sublattice generated by the pair $d\omega_1, a\omega_2 + kb\omega_1$. So by Remark 2.3(c), the Fourier series for $j(T(\Omega_0))$ is obtained by replacing each ζ by ζ^k in $j(\Omega_0)$ (where they occur). This defines an automorphism on the field of Fourier series. But these are just automorphisms induced by the Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$. Thus the fixed field consists of the Fourier series with rational coefficients, as desired. $\square$

3.4 Theorem. *The group $PSL_2(\mathbb{Z}_n)$ acts as a group of automorphisms of L. Its fixed field is L_M.*

Proof.[4]

Clearly the natural homomorphism which sends

$$T = \begin{bmatrix} s & r \\ q & p \end{bmatrix} \longrightarrow \begin{bmatrix} \bar{s} & \bar{r} \\ \bar{q} & \bar{p} \end{bmatrix} = \overline{T}$$

is surjective from $\Gamma = PSL_2(\mathbb{Z})$ onto $PSL_2(\mathbb{Z}_n)$. So since $\Omega_0' = T(\Omega_0)$ if and only if $\overline{\Omega}_0' = \overline{T}(\overline{\Omega}_0)$, then the action of Γ on E_n corresponds to the action of $PSL_2(\mathbb{Z}_n)$ on $\overline{E}_n$. Suppose

$$f(\tau) = F(j(\Omega); j(\Omega_0^1), \ldots, j(\Omega_0^N))$$

where the Ω_0^i are the elements of E_n and F is a rational function with rational coefficients in the $N+1$ variables. Then

$$f\left(\frac{p\tau + q}{r\tau + s}\right) = F(j(\Omega); j(T(\Omega_0^1)), \ldots, j(T(\Omega_0^N)))$$

where T is the restriction to L of the automorphisms of the field of all meromorphic functions in $\mathbb{H}^2$ given by

$$\tau' = \frac{p\tau + q}{r\tau + s}.$$

The fixed field thus consists of the f which are invariant under Γ. Consider a function f in the fixed field. Then f has a Fourier series in $q^{1/n}$ and f is invariant under elements in Γ. In particular, f is invariant under the map $\tau \mapsto \tau + 1$, so the Fourier series of f is invariant under the map $q^{1/n} = e^{2\pi i\tau/n} \mapsto e^{2\pi i(\tau+1)/n} = \zeta q^{1/n}$, for $\zeta = e^{2\pi i\tau/n}$. This implies that f must have coefficients of zero for all powers of $q^{1/n}$ which are not divisible by n. Thus f in fact has a Fourier series in $(q^{1/n})^n = q$, so f is a modular fuction. □

3.5 Corollary. *The Galois group of L over K is $PGL_2(\mathbb{Z}_n)$.*

Proof.

Since $PGL_2(\mathbb{Z}_n)$ is generated by Δ_n and $PSL_2(\mathbb{Z}_n)$, then from Theorems 3.3 and 3.4, we see the fixed field of $PGL_2(\mathbb{Z}_n)$ is $L_R \cap L_M = K$, by Remark 2.5. So all we need to show is that $PGL_2(\mathbb{Z}_n)$ acts transitively on L. If $T \in PGL_2(\mathbb{Z}_n)$ such that T fixes both the subgroups $< \overline{\omega}_1 >, < \overline{\omega}_2 >$, then T must clearly be a diagonal matrix. In the proof of Theorem 3.3, we showed that the only diagonal matrices which map every sublattice with basis $\{n\omega_1, \omega_2 + c\omega_1\}$ onto itself are the scalar matrices. Combining this with Theorem 1.13 implies $PGL_2(\mathbb{Z}_n)$ acts transitively, and thus is isomorphic to the Galois group of L over K. □

References

[1] Apostol, Tom M., *Modular Functions and Dirichlet Series in Number Theory*, Springer-Verlag, New York, 1976.

[2] Jones, Gareth A., and Singerman, David, *Complex Functions*, Cambridge University Press, Cambridge, 1987.

[3] Lang, Serge, *Elliptic Functions*, 2nd ed., Springer-Verlag, New York, 1987.

[4] Macbeath, A.M., "Extensions of the rationals with Galois group $PGL(2, Z_n)$", Bull. London Math Soc. **1** (1969), 332-338.

[5] Rotman, Joseph J. *Advanced Modern Algebra*, Prentice Hall, New Jersey, 2002.