Math. Ann. 207, 99–120 (1974)

On the Construction of Galois Extensions of Function Fields and Number Fields

Kuang-yen Shih

This paper consists of two parts and an appendix. In Part 1, we investigate Galois converings and consider the problem of reducing their fields of definition. We restrict ourselves to $PSL_2(\mathbf{Z}/p\mathbf{Z})$-coverings in Part 2. The results of Part 1 are applied to obtain Galois extensions with $PSL_2(\mathbf{Z}/p\mathbf{Z})$ as Galois group. We show that if p is an odd prime such that 2, 3 or 7 is a quadratic non-residue modulo p, then $PSL_2(\mathbf{Z}/p\mathbf{Z})$ occurs as Galois groups over the rationals. To prove this, Shimura's theory of canonical system of models is used to reduce the fields of definition of certain Galois coverings. Previously, our result is only known for $p=3$, 5 and 7.

In the appendix, we discuss the classification of Galois coverings, which is necessary in verifying Weil's criterion in certain cases. We also indicate how to use the theory developed in Part 1 to show Hilbert's result that alternating groups can be realized as Galois groups over $\boldsymbol{Q}$.

This paper is based on the author's doctoral dissertation. He would like to thank Professor Goro Shimura for several valuable suggestion during the course of the research.

Notation. For an associative ring S with an identity element, we denote by $S^\times$ the group of all invertible elements of S.

Part 1. Generalities

1. Definitions

Let G be a finite group. A *G-covering* Λ is a quadruple (W, V, π, φ) consisting of two projective non-singular algebraic curves W, V defined over $\boldsymbol{C}$, a surjective rational map $\pi: W \to V$ and an isomorphism φ of G into $\mathrm{Aut}(W)$, the group of automorphisms of W, such that the function field $\boldsymbol{C}(W)$ is a Galois extension of $\boldsymbol{C}(V)$ and $\varphi(G)$ coincides with the group of covering transformations of the covering $\pi: W \to V$.

Let $\Lambda = (W, V, \pi, \varphi)$ and $\Lambda' = (W', V', \pi', \varphi')$ be two G-coverings. A pair (Φ, Ψ) is called an *isomorphism* of Λ to Λ' if Φ (resp. Ψ) is a biregular birational map of W onto W' (resp. V onto V') such that $\pi' \circ \Phi = \Psi \circ \pi$

and $\varphi'(g) \circ \Phi = \Phi \circ \varphi(g)$ for all $g \in G$. We say that Λ and Λ' are *isomorphic* if there is an isomorphism from Λ to Λ'.

Let k be a subfield of $\mathbf{C}$. A G-covering $\Lambda = (W, V, \pi, \varphi)$ is *defined over* k if W, V, π and $\varphi(g)$ $(g \in G)$ are defined over k. Suppose Λ and Λ' are two G-coverings defined over k, then an isomorphism (Φ, Ψ) of Λ to Λ' is *defined over* k if Φ is defined over k. It is easy to see that this implies Ψ is also defined over k.

Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering defined over k. For an isomorphism σ of k into $\mathbf{C}$, define an isomorphism φ^σ of G into $\mathrm{Aut}(W^\sigma)$ by $\varphi^\sigma(g) = \varphi(g)^\sigma$, $g \in G$. Then $(W^\sigma, V^\sigma, \pi^\sigma, \varphi^\sigma)$ is a G-covering defined over k. We denote this covering by Λ^σ.

Let Λ be a G-covering and k a subfield of $\mathbf{C}$. A *model of* Λ *over* k is a G-covering defined over k which is isomorphic to Λ.

2. *Weil's Criterion*

Theorem 1. *Let G be a finite group and k_0, k subfields of $\mathbf{C}$ such that $k_0 \subset k$. Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering defined over k. For every $\sigma \in \mathrm{Aut}(\mathbf{C}/k_0)$, let $(\Phi_\sigma, \Psi_\sigma)$ be an isomorphism of Λ to Λ^σ defined over kk^σ. Then the following* (A) *and* (B) *are equivalent:*

(A) *There exist a G-covering Λ_0 defined over k_0 and an isomorphism (Φ, Ψ) of Λ_0 to Λ defined over k such that $\Phi^\sigma \circ \Phi^{-1} = \Phi_\sigma$ (therefore $\Psi^\sigma \circ \Psi^{-1} = \Psi_\sigma$) for all $\sigma \in \mathrm{Aut}(\mathbf{C}/k_0)$.*

(B) $\Phi_\sigma^\tau \circ \Phi_\tau = \Phi_{\sigma\tau}$ *(therefore $\Psi_\sigma^\tau \circ \Psi_\tau = \Psi_{\sigma\tau}$) for all $\sigma, \tau \in \mathrm{Aut}(\mathbf{C}/k_0)$.*

Proof. That (A) implies (B) is trivial. Assume (B). By Weil's criterion [12] there are two curves W_0, V_0 defined over k_0 and two biregular birational maps $\Phi : W_0 \to W$, $\Psi : V_0 \to V$ defined over k such that $\Phi^\sigma \circ \Phi^{-1} = \Phi_\sigma$, $\Psi^\sigma \circ \Psi^{-1} = \Psi_\sigma$ for all $\sigma \in \mathrm{Aut}(\mathbf{C}/k_0)$. Define $\pi_0 : W_0 \to V_0$ by $\pi_0 = \Psi^{-1} \circ \pi \circ \Phi$ and $\varphi_0 : G \to \mathrm{Aut}(W_0)$ by $\varphi_0(g) = \Phi^{-1} \circ \varphi(g) \circ \Phi$ for $g \in G$. Then $\Lambda_0 = (W_0, V_0, \pi_0, \varphi_0)$ is a G-covering defined over k_0, and (Φ, Ψ) is an isomorphism of Λ_0 to Λ defined over k.

Corollary 2. *Let G be a finite group and k_0, k two subfields of $\mathbf{C}$ such that $k_0 \subset k$. Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering defined over k. Then Λ has a model over k_0 which is isomorphic to Λ over k if and only if for every $\sigma \in \mathrm{Aut}(\mathbf{C}/k_0)$, there is a biregular birational map $\Phi_\sigma : W \to W^\sigma$ defined over kk^σ such that*

(a) $\Phi_\sigma^\tau \circ \Phi_\tau = \Phi_{\sigma\tau}$ *for all $\sigma, \tau \in \mathrm{Aut}(\mathbf{C}/k_0)$*

and

(b) $\varphi(g)^\sigma \circ \Phi_\sigma = \Phi_\sigma \circ \varphi(g)$ *for all $\sigma \in \mathrm{Aut}(\mathbf{C}/k_0)$ and $g \in G$.*

Proof. That Λ has a model over k_0 implies the existence of Φ_σ's is trivial. Conversely, assume for every $\sigma \in \mathrm{Aut}(\mathbf{C}/k_0)$ there is a biregular birational map $\Phi_\sigma : W \to W^\sigma$ defined over kk^σ satisfying (a) and (b). By (b),

there is a biregular birational map $\Psi_\sigma : V \to V^\sigma$ defined over kk^σ such that $(\Phi_\sigma, \Psi_\sigma)$ is an isomorphism of Λ to Λ^σ. Hence by Theorem 1, condition (a) implies the existence of a model of Λ over k_0 which is isomorphic to Λ over k.

Recall that a finite group G is said to be *complete* if the center of G is 1 and every automorphism of G is an inner automorphism [1].

Theorem 3. *Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering and k a subfield of $\boldsymbol{C}$. Suppose*

(1) *For all $\sigma \in \mathrm{Aut}(\boldsymbol{C}/k)$, there is a biregular birational map from W onto W^σ;*

(2) *The group $\mathrm{Aut}(W)$ is a complete finite group.*

Then Λ has a model over k.

Proof. Let $K \supset k$ be a subfield of $\boldsymbol{C}$ over which Λ and all elements of $\mathrm{Aut}(W)$ are defined. For $\sigma \in \mathrm{Aut}(\boldsymbol{C}/k)$, let F_σ be a biregular birational map from W to W^σ. Consider the automorphism of $\mathrm{Aut}(W)$ defined by $\alpha \mapsto F_\sigma^{-1} \circ \alpha^\sigma \circ F_\sigma$. By (2) there is a unique γ in $\mathrm{Aut}(W)$ such that $F_\sigma^{-1} \circ \alpha^\sigma \circ F_\sigma = \gamma \circ \alpha \circ \gamma^{-1}$ for all α in $\mathrm{Aut}(W)$. Set $\Phi_\sigma = F_\sigma \circ \gamma$. Then Φ_σ is a biregular birational map from W onto W^σ such that

$$\Phi_\sigma^{-1} \circ \alpha^\sigma \circ \Phi_\sigma = \alpha \tag{2.1}$$

for all $\sigma \in \mathrm{Aut}(\boldsymbol{C}/k)$ and $\alpha \in \mathrm{Aut}(W)$.

Note that Φ_σ is defined over KK^σ for $\sigma \in \mathrm{Aut}(\boldsymbol{C}/k)$. In fact, for $\tau \in \mathrm{Aut}(\boldsymbol{C}/KK^\sigma)$ and $\alpha \in \mathrm{Aut}(W)$ we have $(\Phi_\sigma^\tau)^{-1} \circ \alpha^\sigma \circ \Phi_\sigma^\tau = \alpha$ by (2.1). It follows that $\Phi_\sigma^{-1} \circ \Phi_\sigma^\tau$ is in the center of $\mathrm{Aut}(W)$. Hence $\Phi_\sigma^\tau = \Phi_\sigma$. This being true for all $\tau \in \mathrm{Aut}(\boldsymbol{C}/KK^\sigma)$, Φ_σ is defined over KK^σ.

Suppose $\sigma, \tau \in \mathrm{Aut}(\boldsymbol{C}/k)$. By (2.1) we have

$$(\Phi_\tau^{-1} \circ (\Phi_\sigma^\tau)^{-1} \circ \Phi_{\sigma\tau}) \circ \alpha \circ (\Phi_\tau^{-1} \circ (\Phi_\sigma^\tau)^{-1} \circ \Phi_{\sigma\tau})^{-1} = \alpha$$

for all $\alpha \in \mathrm{Aut}(W)$. Therefore $\Phi_\sigma^\tau \circ \Phi_\tau = \Phi_{\sigma\tau}$. Hence Λ has a model over k by Corollary 2.

Remark. We can replace (1) and (2) of Theorem 3 by a somewhat weaker condition, namely, $\mathrm{Aut}(W)$ has trivial center and for all $\sigma \in \mathrm{Aut}(\boldsymbol{C}/k)$, there is a biregular birational map Φ_σ from W to W^σ satisfying (2.1).

3. A Necessary Condition

Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering. For $\mathfrak{P} \in W$, let $G_\mathfrak{P}$ be the isotropy subgroup $\{g \in G : \varphi(g)(\mathfrak{P}) = \mathfrak{P}\}$ and $\mathfrak{o}_\mathfrak{P} \subset \boldsymbol{C}(W)$ the valuation ring at the point $\mathfrak{P}$. Choose a local uniformizing parameter $t \in \mathfrak{o}_\mathfrak{P}$ at $\mathfrak{P}$. Then for $g \in G_\mathfrak{P}$, $t \circ \varphi(g)$ is also a uniformizing parameter at $\mathfrak{P}$. Therefore we have

$$t \circ \varphi(g) \equiv \zeta \cdot t \pmod{t^2 \mathfrak{o}_\mathfrak{P}},$$

where ζ is a root of unity independent of the choice of the parameter t. Denote ζ by $\zeta_{\mathfrak{P}}(g)$. Assigning $\zeta_{\mathfrak{P}}(g)$ to $g \in G_{\mathfrak{P}}$, we get a map $\zeta_{\mathfrak{P}}$ from $G_{\mathfrak{P}}$ into the circle group. It is easy to see that $\zeta_{\mathfrak{P}}$ is an injective group homomorphism.

Let $e_{\mathfrak{P}}$ denote the ramification index at $\mathfrak{P}$. From the above discussion, we know that $G_{\mathfrak{P}}$ is a cyclic group of order $e_{\mathfrak{P}}$. For $\mathfrak{p} \in V$, define $e_{\mathfrak{p}}$ to be $e_{\mathfrak{P}}$ for any $\mathfrak{P} \in \pi^{-1}(\mathfrak{p})$. This is well-defined because $\pi : W \to V$ is a Galois covering.

Let $\zeta = \exp(2\pi\sqrt{-1}/e_{\mathfrak{P}})$. Denote by $g_{\mathfrak{P}}$ the unique $g \in G_{\mathfrak{P}}$ such that $\zeta_{\mathfrak{P}}(g) = \zeta$. Then we have:

$$\textit{If } \pi(\mathfrak{P}) = \pi(\mathfrak{P}'), \textit{ then } g_{\mathfrak{P}} \textit{ and } g_{\mathfrak{P}'} \textit{ are conjugate in } G. \tag{3.1}$$

Let $\mathfrak{p} \in V$. From (3.1) we know that the set $\{g_{\mathfrak{P}} : \pi(\mathfrak{P}) = \mathfrak{p}\}$ is a conjugacy class in G. Denote this conjugacy class by $C_{\mathfrak{p}}$. Let $C_0 = \{1\}, C_1, \ldots, C_s$ be the conjugacy classes of G. We call $\mathfrak{p}$ *a point of type* C_i if $C_{\mathfrak{p}} = C_i$. Obviously, $\mathfrak{p}$ is unramified in W if and only if $\mathfrak{p}$ is of type C_0. For i: $1 \leqq i \leqq s$, the number of points of type C_i on V is finite. We denote this number by $\mu_i(\Lambda)$.

We call two points $\mathfrak{p}$ and $\mathfrak{p}'$ on V *equivalent* if there is an automorphism (Φ, Ψ) of Λ such that $\mathfrak{p}' = \Psi(\mathfrak{p})$.

Proposition 4. *Let* $\Lambda = (W, V, \pi, \varphi)$ *and* $\Lambda' = (W', V', \pi', \varphi')$ *be two* G*-coverings and* (Φ, Ψ) *an isomorphism of* Λ *to* Λ'. *Then* $C_{\mathfrak{p}} = C_{\Psi(\mathfrak{p})}$ *for all* $\mathfrak{p} \in V$. *Especially, equivalent points on* V *are of the same type.*

For $i : 0 \leqq i \leqq s$, let e_i be the order of any element of C_i and $\zeta_i = \exp(2\pi\sqrt{-1}/e_i)$. Let k be a subfield of $\boldsymbol{C}$. Define

$$Z(k; C_i) = \{m \in \boldsymbol{Z} : \zeta_i^m \text{ is conjugate to } \zeta_i \text{ over } k\}.$$

Let g be any element of C_i. Call $m_1, m_2 \in Z(k; C_i)$ equivalent if g^{m_1} and g^{m_2} are conjugate in G. It is easy to see that this definition is independent of the choice of $g \in C_i$. The relation thus defined is an equivalence relation on $Z(k; C_i)$. Denote the number of equivalence classes of this relation by $z(k; C_i)$. Obviously, $z(k; C_i) \leqq [k(\zeta_i) : k]$.

Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering defined over k, $\mathfrak{P}$ a point on W and $\mathfrak{p} = \pi(\mathfrak{P})$. For an automorphism α of $\boldsymbol{C}$ over k, $\mathfrak{P}^\alpha \in W$, $\mathfrak{p}^\alpha \in V$ and $\mathfrak{p}^\alpha = \pi(\mathfrak{P}^\alpha)$. Since W is defined over k, α can be extended to an automorphism of $\boldsymbol{C}(W)$, which is denoted by the same letter α. We have $(\mathfrak{o}_{\mathfrak{P}})^\alpha = \mathfrak{o}_{\mathfrak{P}^\alpha}$. Fix a local uniformizing parameter t at $\mathfrak{P}$. Let $\zeta = \exp(2\pi\sqrt{-1}/e_{\mathfrak{P}})$ and $m(\alpha)$ an integer satisfying

$$(\zeta^\alpha)^{m(\alpha)} = \zeta. \tag{3.2}$$

Then we have

$$t^\alpha \circ (g_{\mathfrak{P}}^{m(\alpha)}) \equiv \zeta \cdot t^\alpha \pmod{(t^\alpha)^2 \mathfrak{o}_{\mathfrak{P}^\alpha}}.$$

Therefore $g_{\mathfrak{P}^\alpha} = g_{\mathfrak{P}}^{m(\alpha)}$. Hence we have the following

Proposition 5. *Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering defined over a subfield k of $\boldsymbol{C}$ and $\mathfrak{p}$ a point on V. Set $\zeta = \exp(2\pi\sqrt{-1}/e_{\mathfrak{p}})$. For $\alpha \in \mathrm{Aut}(\boldsymbol{C}/k)$, let $m(\alpha)$ be an integer satisfying (3.2). Then for $\alpha, \beta \in \mathrm{Aut}(\boldsymbol{C}/k)$, $\mathfrak{p}^\alpha$ and $\mathfrak{p}^\beta$ are of the same type if and only if $m(\alpha)$ and $m(\beta)$ are equivalent in $Z(k; C_{\mathfrak{p}})$.*

Corollary 6. *Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering and k a subfield of $\boldsymbol{C}$. Suppose V is defined over k. If V has a rational point $\mathfrak{p}$ over k such that $z(k; C_{\mathfrak{p}}) > 1$, then Λ is not defined over k.*

Define $z_0(k; \mathfrak{p})$ to be the cardinality of the set
$\{i : 0 \leqq i \leqq s, \mathfrak{p}^\alpha$ is of type C_i for some $\alpha \in \mathrm{Aut}(\boldsymbol{C}/k)\}$.
By Proposition 5, we have

Proposition 7. *Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering defined over a subfield k of $\boldsymbol{C}$. Then $z(k; C_{\mathfrak{p}}) = z_0(k; \mathfrak{p})$ for all $\mathfrak{p} \in V$.*

Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering and e a positive integer. Denote by $z(e; \Lambda)$ the cardinality of the set

$$\{i : 0 \leqq i \leqq s, e_i = e \quad \text{and} \quad \mu_i(\Lambda) > 0\}.$$

Suppose Λ has a model $\Lambda_0 = (W_0, V_0, \pi_0, \varphi_0)$ over k. Let (Φ, Ψ) be an isomorphism to Λ to Λ_0. For $\mathfrak{p} \in V$ and $\mathfrak{p}' = \Psi(\mathfrak{p})$ we have $e_{\mathfrak{p}'} = e_{\mathfrak{p}}$, $C_{\mathfrak{p}'} = C_{\mathfrak{p}}$ (see Proposition 4). Therefore $z(e_{\mathfrak{p}'}; \Lambda_0) = z(e_{\mathfrak{p}}; \Lambda)$ and $z(k; C_{\mathfrak{p}'}) = z(k; C_{\mathfrak{p}})$. By Proposition 7, $z(k; C_{\mathfrak{p}'}) = z_0(k; \mathfrak{p}') \leqq z(e_{\mathfrak{p}'}; \Lambda_0)$. Hence we have $z(k; C_{\mathfrak{p}}) \leqq z(e_{\mathfrak{p}}; \Lambda)$.

Theorem 8. *Let $\Lambda = (W, V, \pi, \varphi)$ be a G-covering and k a subfield of $\boldsymbol{C}$. If there is a point $\mathfrak{p}$ on V for which $z(e_{\mathfrak{p}}; \Lambda) < z(k; C_{\mathfrak{p}})$, then Λ has no model over k.*

When $z(e_{\mathfrak{p}}; \Lambda) = 1$, we can actually determine an algebraic number field which is contained in every field of definition of any model of Λ. To do this, for $i : 1 \leqq i \leqq s$ define

$$I(i) = \{m \in Z(\boldsymbol{Q}; C_i) : 1 \leqq m \leqq e_i - 1 \quad \text{and } g^m \text{ is conjugate to } g\}$$

and

$$\xi_i = \sum_{m \in I(i)} \zeta^m, \tag{3.3}$$

where $\zeta = \exp(2\pi\sqrt{-1}/e_i)$. Then $\xi_i \in k$ if $z(k; C_i) = 1$. In fact, suppose $\sigma \in \mathrm{Gal}(k(\zeta)/k)$. Then $\zeta^\sigma = \zeta^j$ for some j in $Z(k; C_i)$. Since $z(k; C_i) = 1$, g^j is conjugate to g. Hence $m \in I(i)$ if and only if g^{mj} is conjugate to g. Therefore

$$\xi_i^\sigma = \sum_{m \in I(i)} \zeta^{mj} = \xi_i.$$

Proposition 9. *Let Λ be a G-covering. Suppose Λ has a model over k and $z(e_i; \Lambda)=1$. Then k contains the algebraic integer ξ_i defined by* (3.3).

Proof. By Theorem 8, $z(k; C_i)=1$. Therefore by the above argument, ξ_i belongs to k.

4. *Eichler-Selberg's Trace Formula*

Let $\Lambda=(W, V, \pi, \varphi)$ be a G-covering. Then G acts naturally on the space of holomorphic differential forms of the first kind on W. Denote this representation of G by ϱ. Then we have the trace formula

$$\operatorname{tr}(\varrho(\sigma))=1+\sum_{i=1}^{s}\mu_i S_{ij}, \quad \text{if} \quad \sigma\in C_j(j\neq 0), \tag{4.1}$$

where $\mu_i=\mu_i(\Lambda)$ and S_{ij}'s are algebraic numbers associated with G defined as follows.

Let $\sigma\in C_j$. Suppose there is $g\in C_i$ such that σ is a power of g. Let H be the subgroup generated by g. Denote the set of all cosets xH such that $x^{-1}\sigma x\in H$ by M. For $xH\in M$, $x^{-1}\sigma x=g^m$ for a unique integer m mod e_i. Obviously, m mod e_i depends only on the coset xH, not on the choice of the representative x. We denote m by $m(xH)$. Let $\zeta=\exp(2\pi\sqrt{-1}/e_i)$. Define

$$S(g,\sigma)=\sum_{X\in M}\frac{\zeta^{m(X)}}{1-\zeta^{m(X)}}. \tag{4.2}$$

It is easy to see that if σ is also a power of $g'\in C_i$, then $S(g,\sigma)=S(g',\sigma)$. Therefore, we can define $S_i(\sigma)$ to be $S(g,\sigma)$ for any $g\in C_i$ such that σ is a power of g. If there is no g in C_i such that σ is a power of g, define $S_i(\sigma)=0$. Observe that $S_i(\sigma)$ depends only on C_j, the conjugacy class to which σ belongs. We define $S_{ij}=S_i(\sigma)$ for any $\sigma\in C_j$.

Let $\chi_0, \chi_1, \ldots, \chi_s$ be the characters of G, where χ_0 denotes the trivial character. Set $\chi_{ij}=\chi_i(\sigma)$ for any $\sigma\in C_j$. Let $\Lambda=(W, V, \pi, \varphi)$ be a G-covering and ϱ the representation of G in the space of holomorphic differential forms on W. Denote the multiplicity of χ_i in ϱ by λ_i and the number of points of type C_i on V by μ_i. Then from (4.1) we have

$$\sum_{i=0}^{s}\lambda_i\chi_{ij}=1+\sum_{i=1}^{s}\mu_i S_{ij}, \quad j=1,\ldots,s. \tag{4.3}$$

These formulas relate the numbers of points of different types to the multiplicities of irreducible representations of G in ϱ.

5. *Galois Coverings Constructed from Fuchsian Groups*

Let $\Gamma \subset SL_2(\boldsymbol{R})$ be a Fuchsian group of the first kind [10, p. 19]. Denote by $\mathfrak{H}^*$ the union of the upper half plane $\mathfrak{H}$ and the cusps of Γ. Then $\Gamma\backslash\mathfrak{H}^*$ has the structure of a compact Riemann surface. Hence there exist a projective non-singular algebraic curve V and a Γ-invariant holomorphic map φ from $\mathfrak{H}^*$ onto V which gives a biregular birational map from $\Gamma\backslash\mathfrak{H}^*$ onto V. We call (V, φ) a *model* of $\Gamma\backslash\mathfrak{H}^*$ [10, p. 152].

Let Δ be a normal subgroup of finite index of the Fuchsian group Γ. Let $(V_\Gamma, \varphi_\Gamma)$ [resp. $(V_\Delta, \varphi_\Delta)$] be a model of $\Gamma\backslash\mathfrak{H}^*$ (resp. $\Delta\backslash\mathfrak{H}^*$). Then there is a rational map $J: V_\Delta \to V_\Gamma$ such that $J \circ \varphi_\Delta = \varphi_\Gamma$. Denote the images of Γ, Δ in $SL_2(\boldsymbol{R})/\{\pm 1\}$ by $\bar{\Gamma}$, $\bar{\Delta}$, respectively. Then $\bar{\Gamma}/\bar{\Delta}$ acts on $\Delta\backslash\mathfrak{H}^*$ faithfully. Via φ_Δ, let this action be given by an isomorphism φ of $\bar{\Gamma}/\bar{\Delta}$ into $\mathrm{Aut}(V_\Delta)$. Then $(V_\Delta, V_\Gamma, J, \varphi)$ is a $(\bar{\Gamma}/\bar{\Delta})$-covering. By Shimura's theory, this covering has a model over an abelian extension of a totally real number field if Γ and Δ are "arithmetically defined". (See [10, Chapter 9], generalizations of this theory have been treated by Shimura and Miyake.)

Part 2. $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$-Coverings and the Realisation of $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$ as Galois Groups

From Shimura's result [9], one derives easily that $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$ can be realized as Galois groups over the cyclotomic field $\boldsymbol{Q}(\exp(2\pi\sqrt{-1}/p))$. A closer examination shows that this in fact gives us extensions over the quadratic number field $\boldsymbol{Q}(\sqrt{\varepsilon p})$, where $\varepsilon = (-1)^{(p-1)/2}$. Unfortunately, this can't be used to produce such extensions over the rationals, as we shall see in § 2. However, Shimura's recent result on the canonical system of models provides the necessary tool to construct Galois extensions over the rationals with Galois groups isomorphic to $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$ for certain prime numbers p (Theorem 12).

1. *Generalities on $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$-Coverings*

Let p be an odd prime. Set

$$P = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix},$$

where n is a quadratic non-residue modulo p. Then P and Q represent two different conjugacy classes of $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$. In the following, we use C_1 (resp. C_2) to denote the conjugacy class to which P (resp. Q) belongs. It is well-known that every element of order p belongs to either P or Q. Therefore

$$z(\boldsymbol{Q}; C_1) = z(\boldsymbol{Q}; C_2) = 2. \tag{1.1}$$

(For notation, see Part 1, § 3.) By Proposition 4 and Theorem 8 of Part 1, we have

Proposition 1. *Let $\Lambda=(W, V, \pi, \varphi)$ be a $PSL_2(\mathbf{Z}/p\mathbf{Z})$-covering. Consider the points $\mathfrak{p}$ on V such that $e_{\mathfrak{p}}=p$. Suppose all these $\mathfrak{p}$'s are equivalent, then Λ has no model over $\boldsymbol{Q}$. In fact, every field of definition of a model of Λ contains $\sqrt{\varepsilon p}$, where $\varepsilon=(-1)^{(p-1)/2}$.*

The last statement follows from Proposition 9, Part 1, and the identity

$$\sum_{\substack{m=1 \\ \left(\frac{m}{p}\right)=1}}^{p-1} \zeta^m=\frac{-1+\sqrt{\varepsilon p}}{2}, \qquad \zeta=\exp(2\pi\sqrt{-1}/p).$$

Let χ_1, χ_2 be the characters of $PSL_2(\mathbf{Z}/p\mathbf{Z})$ for which

$$\chi_1(P)=\chi_2(Q)=\frac{\varepsilon+\sqrt{\varepsilon p}}{2},$$

$$\chi_2(P)=\chi_1(Q)=\frac{\varepsilon-\sqrt{\varepsilon p}}{2}.$$

Here and throughout the rest of the paper ε will denote $\left(\frac{-1}{p}\right)$ $=(-1)^{(p-1)/2}$. By Eichler-Selberg's trace formula we can prove the following generalization of Hecke's result [3, 4].

Proposition 2. *Let $\Lambda=(W, V, \pi, \varphi)$ be a $PSL_2(\mathbf{Z}/p\mathbf{Z})$-covering. Denote the multiplicity of $\chi_i(i=1,2)$ in the representation ϱ of $PSL_2(\mathbf{Z}/p\mathbf{Z})$ in the space of holomorphic differential forms on W by λ_i, and the number of points of type C_i on V by μ_i. Then*

$$\lambda_1=\lambda_2 \qquad \text{if} \quad p\equiv 1 \pmod 4,$$

$$\lambda_1-\lambda_2=h(\mu_1-\mu_2) \qquad \text{if} \quad p\equiv 3 \pmod 4,$$

where h is the class number of $\boldsymbol{Q}(\sqrt{-p})$.

Remark. Suppose $p\equiv 3 \pmod 4$ and $\mu_1 \neq \mu_2$. Then $\lambda_1 \neq \lambda_2$ by the above Proposition. Hence $\operatorname{tr}(\varrho(P))$ is not rational in this case. Therefore Λ can not have a model over $\boldsymbol{Q}$.

To prove Proposition 2, first observe that

$$\begin{aligned} S(P,P) &= \frac{1}{2}\sum_{n=1}^{p-1}\left(1+\left(\frac{n}{p}\right)\right)\frac{\zeta^n}{1-\zeta^n} \\ &= -\frac{p-1}{4}+\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\frac{1}{1-\zeta^n}, \end{aligned} \tag{1.1}$$

where $\zeta=\exp(2\pi\sqrt{-1}/p)$. [For the definition of $S(P, P)$, see Part 1, § 4.]

Lemma 3. *We have*

$$\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\frac{1}{1-\zeta^n}=\begin{cases}0 & \text{if} \quad p\equiv 1\,(\mathrm{mod}\,4)\\ \sqrt{-p}\cdot h & \text{if} \quad p\equiv 3\,(\mathrm{mod}\,4),\end{cases}$$

where h is the class number of $\boldsymbol{Q}(\sqrt{-p})$.

Proof. If $p\equiv 1\,(\mathrm{mod}\,4)$, then the assertion follows from the fact that $\left(\frac{n}{p}\right)=\left(\frac{-n}{p}\right)$. Suppose $p\equiv 3\,(\mathrm{mod}\,4)$. Then

$$\begin{aligned}\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\frac{1}{1-\zeta^n}&=\frac{1}{p}\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\prod_{j\neq n}(1-\zeta^j)\\&=\frac{1}{p}\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\sum_{k=1}^{p-1}k\zeta^{-n(k+1)}\\&=\frac{1}{p}\sum_{k=2}^{p}(k-1)\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\zeta^{-nk}\\&=-\frac{1}{p}\sum_{k=2}^{p}(k-1)\sum_{n=1}^{p-1}\left(\frac{n}{p}\right)\zeta^{nk}\\&=-\frac{1}{p}\sum_{k=2}^{p-1}(k-1)\left(\frac{k}{p}\right)\sqrt{-p}\\&=-\frac{1}{p}\sqrt{-p}\left[\sum_{k=2}^{p-1}\left(\frac{k}{p}\right)k-\sum_{k=2}^{p-1}\left(\frac{k}{p}\right)\right]\\&=-\frac{1}{p}\sqrt{-p}\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)k\\&=\sqrt{-p}\cdot h\qquad\text{q.e.d.}\end{aligned}$$

By (1.1) and the above Lemma we have

$$\begin{aligned}S_1(P)=S_2(Q)&=S(P,P)\\&=\begin{cases}-\dfrac{p-1}{4} & \text{if} \quad p\equiv 1\,(\mathrm{mod}\,4)\\ -\dfrac{p-1}{4}+\dfrac{1}{2}\sqrt{-p}\cdot h & \text{if} \quad p\equiv 3\,(\mathrm{mod}\,4)\end{cases}\end{aligned}\tag{1.2}$$

$$\begin{aligned}S_2(P)=S_1(Q)&=S(Q,P)\\&=\begin{cases}-\dfrac{p-1}{4} & \text{if} \quad p\equiv 1\,(\mathrm{mod}\,4)\\ -\dfrac{p-1}{4}-\dfrac{1}{2}\sqrt{-p}\cdot h & \text{if} \quad p\equiv 3\,(\mathrm{mod}\,4).\end{cases}\end{aligned}\tag{1.3}$$

Proof of Proposition 2. By the trace formula (4.3), Part 1, we have

$$\lambda_1(\chi_1(P)-\chi_1(Q))+\lambda_2(\chi_2(P)-\chi_2(Q)) = \mu_1(S_1(P)-S_1(Q))+\mu_2(S_2(P)-S_2(Q)). \tag{1.4}$$

Suppose $p\equiv 1 \pmod 4$, then $\varepsilon=1$. So $\chi_1(P)=\chi_2(Q)=\dfrac{1+\sqrt{p}}{2}$ and $\chi_2(P)=\chi_1(Q)=\dfrac{1-\sqrt{p}}{2}$. Hence by (1.2), (1.3) and (1.4), $\lambda_1=\lambda_2$.

Suppose $p\equiv 3 \pmod 4$, then $\varepsilon=-1$. So $\chi_1(P)=\chi_2(Q)=\dfrac{-1+\sqrt{-p}}{2}$ and $\chi_2(P)=\chi_1(Q)=\dfrac{-1-\sqrt{-p}}{2}$. Hence by (1.2), (1.3) and (1.4) we have $\lambda_1-\lambda_2=h(\mu_1-\mu_2)$.

2. $PSL_2(\mathbf{Z}/p\mathbf{Z})$-Coverings Associated with Subgroups of $SL_2(\mathbf{Z})$

Let Δ be a subgroup of $SL_2(\mathbf{Z})$ of finite index such that $\overline{\Delta}\cdot\overline{\Gamma(p)}=\overline{SL_2(\mathbf{Z})}$, where

$$\Gamma(p)=\left\{\begin{bmatrix} a & b \\ c & d\end{bmatrix}\in SL_2(\mathbf{Z}) : a\equiv d\equiv 1,\ b\equiv c\equiv 0 \pmod p\right\}.$$

Denote $\Delta\cap\Gamma(p)$ by Δ'. Then $\overline{\Delta}/\overline{\Delta'}$ is isomorphic to $PSL_2(\mathbf{Z}/p\mathbf{Z})$. Therefore by § 5, Part 1, we can construct a $PSL_2(\mathbf{Z}/p\mathbf{Z})$-covering from Δ, Δ' in a natural way. We call this convering *the $PSL_2(\mathbf{Z}/p\mathbf{Z})$-covering associated with Δ*. Note that ramifications occur only at the cusps and the elliptic points of Δ'. The ramification index at a cusp is p and the ramification index at an elliptic point is 2 or 3.

Proposition 4. *Let Δ be a normal subgroup of $SL_2(\mathbf{Z})$ of finite index such that $\overline{\Delta}\cdot\overline{\Gamma(p)}=\overline{SL_2(\mathbf{Z})}$. Then the $PSL_2(\mathbf{Z}/p\mathbf{Z})$-covering $\Lambda=(W, V, \pi, \varphi)$ associated with Δ can not have a model over $\mathbf{Q}$. In fact, every field of definition of a model of Λ contains $\sqrt{\varepsilon p}$.*

Proof. By Proposition 1, it suffices to prove that the points on V corresponding to the cusps of Δ are equivalent. Since Δ and $\Gamma(p)$ are normal in $SL_2(\mathbf{Z})$, $\overline{\Gamma(p)}/\overline{\Delta}$ is contained in the centralizer of $\varphi(PSL_2(\mathbf{Z}/p\mathbf{Z}))$ in $\mathrm{Aut}(W)$. It follows that $\overline{\Gamma(p)}/\overline{\Delta}$ can be identified with a subgroup of the group of automorphisms of Λ. Being canonically isomorphic to $\overline{SL_2(\mathbf{Z})}/\overline{\Delta}$, $\overline{\Gamma(p)}/\overline{\Delta}$ permutes the cusps of Δ transitively. Therefore the points on V corresponding to the cusps of Δ are equivalent.

Especially the covering Λ associated with $SL_2(\mathbf{Z})$ has no model over $\mathbf{Q}$. We show that it does have a model over $\mathbf{Q}(\sqrt{\varepsilon p})$. To prove this

we need the following Theorem of Shimura [9]: Let j be the classical modular function and $\zeta = \exp(2\pi\sqrt{-1}/p)$.

Theorem 5. *There is a field F with the following properties:*

(1) *F is a Galois extension of $\boldsymbol{Q}(j)$.*

(2) *$\boldsymbol{C} \cdot F$ is the field of modular functions of level p.*

(3) *There is a homomorphism τ from $\mathrm{GL}_2(\boldsymbol{Z}/p\boldsymbol{Z})$ onto $\mathrm{Gal}(F/\boldsymbol{Q}(j))$ whose kernel is $\{\pm 1\}$.*

(4) *$\zeta \in F$, and $\zeta^{\tau(\beta)} = \zeta^{\det(\beta)}$ for all $\beta \in \mathrm{GL}_2(\boldsymbol{Z}/p\boldsymbol{Z})$.*

(5) *$\boldsymbol{Q}(\zeta)$ is algebraically closed in F.*

From this Theorem, we see that the extension $F/k(j)$, where $k = \boldsymbol{Q}(\zeta)$, gives us a model of Λ over k. To construct a model over $k' = \boldsymbol{Q}(\sqrt{\varepsilon p})$, let

$$H = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \in \mathrm{GL}_2(\boldsymbol{Z}/p\boldsymbol{Z}) : a \in (\boldsymbol{Z}/p\boldsymbol{Z})^{\times} \right\}$$

and

$$H' = H \cdot SL_2(\boldsymbol{Z}/p\boldsymbol{Z})$$
$$= \left\{ x \in \mathrm{GL}_2(\boldsymbol{Z}/p\boldsymbol{Z}) : \left(\frac{\det(x)}{p} \right) = 1 \right\}.$$

Then H'/H is isomorphic to $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$.

Let L and L' be the subfields of F corresponding to the subgroups $H/\{\pm 1\}$ and $H'/\{\pm 1\}$, respectively. Then $\mathrm{Gal}(L/L')$ is isomorphic to $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$. It is easy to see that $L' = k'(j)$, $k' = L \cap k$ and $\boldsymbol{C} \cdot L = \boldsymbol{C} \cdot F$ is the field of modular functions of level p. Hence the extension L/L' gives us a model of Λ over k'.

Such a model over k' can also be obtained by using Shimura's theory of canonical system of models. We omit the construction here, because it is similar to the one we are going to give in the following section.

Since $L' = k'(j)$ is transcendental over k', by Hilbert's irreducibility Theorem, we have

Theorem 6. *Let p be an odd prime number. Then there exist Galois extensions of $\boldsymbol{Q}(\sqrt{\varepsilon p})$ with Galois groups isomorphic to $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$.*

3. *The $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$-Covering Associated with $\Gamma_0(N)$*

Let N be an integer relatively prime to p. Denote by $\Lambda(p; N)$ the $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$-covering associated with $\Gamma_0(N)$.

Proposition 7. *The $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$-covering $\Lambda(p; N)$ has a model over $\boldsymbol{Q}(\sqrt{\varepsilon p})$.*

We prove this by Shimura's theory of canonical system of models. For notation see [10, § 9.2].

Proof. Let $\{V_S, \varphi_S, J_{TS}(x)\}$ be a system associated with the matrix algebra $M_2(\boldsymbol{Q})$ over $\boldsymbol{Q}$ satisfying the conditions of [10, Theorem 9.6]. For every finite prime l of $\boldsymbol{Q}$, let

$$U_l = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\boldsymbol{Z}_l) : a \equiv d, b \equiv c \equiv 0 (\mathrm{mod}\, p\boldsymbol{Z}_l), c \equiv 0 (\mathrm{mod}\, N\boldsymbol{Z}_l) \right\},$$

$$U_l' = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\boldsymbol{Z}_l) : c \equiv 0 (\mathrm{mod}\, N\boldsymbol{Z}_l) \right\}.$$

Set

$$U = \left\{ x = (x_l) \in \prod_l \mathrm{GL}_2(\boldsymbol{Z}_l) \times \mathrm{GL}_2^+(\boldsymbol{R}) : x_l \in U_l \text{ for all finite } l \right\}, \tag{3.1}$$

$$U' = \left\{ x = (x_l) \in \prod_l \mathrm{GL}_2(\boldsymbol{Z}_l) \times \mathrm{GL}_2^+(\boldsymbol{R}) : x_l \in U_l' \text{ for all finite } l \right\}, \tag{3.2}$$

$$S = \boldsymbol{Q}^\times \cdot U, \tag{3.3}$$

$$T = \boldsymbol{Q}^\times \cdot U'. \tag{3.4}$$

Then $S, T \in \mathscr{Z}$, S is normal in T and

$$\begin{aligned} \Gamma_S &= S \cap G_{\boldsymbol{Q}^+} = \boldsymbol{Q}^\times \cdot (\Gamma_0(N) \cap \Gamma(p)), \\ \Gamma_T &= T \cap G_{\boldsymbol{Q}^+} = \boldsymbol{Q}^\times \cdot \Gamma_0(N), \\ k_S &= \boldsymbol{Q}(\sqrt{\varepsilon p}), \\ k_T &= \boldsymbol{Q}. \end{aligned}$$

Identify $\bar{\Gamma}_T/\bar{\Gamma}_S$ with $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$. For $g \in PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$ define $\varphi_0(g) = J_{SS}(x)$ for any $x \in \Gamma_T$ which is mapped to g under the canonical homomorphism. Then by [10, Theorem 9.6], $\Lambda_0 = (V_S, V_T, J_{TS}(1), \varphi_0)$ is a model of $\Lambda(p; N)$ over $k_S = \boldsymbol{Q}(\sqrt{\varepsilon p})$.

We call the above Λ_0 *the basic model of* $\Lambda(p; N)$ *over* $\boldsymbol{Q}(\sqrt{\varepsilon p})$.

Theorem 8. *If* $\left(\frac{N}{p}\right) = -1$, *then* $\Lambda(p; N)$ *has a model over* $\boldsymbol{Q}$.

Proof. Let the notation be as in the proof of the above Proposition. For a prime divisor l of $\boldsymbol{Q}$, let

$$\gamma_l = \begin{cases} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & \text{if } l \nmid N \text{ or } l = \infty \\ \begin{bmatrix} 0 & 1/N \\ -1 & 0 \end{bmatrix} & \text{if } l \mid N. \end{cases} \tag{3.5}$$

Set $\gamma=(\gamma_l)\in G_{A^+}$. Then we have:

$$\text{The restriction of } \sigma(\gamma) \text{ to } \boldsymbol{Q}(\sqrt{\varepsilon p}) \text{ generates } \mathrm{Gal}(\boldsymbol{Q}(\sqrt{\varepsilon p})/\boldsymbol{Q}), \tag{3.6}$$

$$x^{-1}\gamma^{-1}x\gamma\in S \quad \text{for all} \quad x\in T, \tag{3.7}$$

$$\gamma^2\in S. \tag{3.8}$$

The statement (3.7) can be checked easily by direct computation. To prove (3.6), note that $N\cdot\det(\gamma)\in\prod_l \boldsymbol{Z}_l^\times\times\boldsymbol{R}_+^\times$ and $N\cdot\det(\gamma_p)=N$. Hence (3.6) follows from the assumption $\left(\frac{N}{p}\right)=-1$. Since $(-N)\cdot\gamma^2\in U$ [see (3.1)], $\gamma^2\in S$ by definition (3.3).

Let $\Lambda_0=(V_S, V_T, J_{TS}(1), \varphi_0)$ be the basic model of $\Lambda(p;N)$ over $\boldsymbol{Q}(\sqrt{\varepsilon p})$ and σ the generator of $\mathrm{Gal}(\boldsymbol{Q}(\sqrt{\varepsilon p})/\boldsymbol{Q})$. Then (3.6) and (3.7) imply that $(J_{SS}(\gamma), J_{TT}(\gamma))$ is an isomorphism of Λ_0 to Λ_0^σ. By (3.8) and [10, Theorem 9.6], $J_{SS}(\gamma)^\sigma\cdot J_{SS}(\gamma)=J_{SS}(\gamma^2)=\mathrm{id}$. Hence Λ_0 has a model over $\boldsymbol{Q}$ by Theorem 1, Part 1.

Remark. The basic model Λ_0 itself *is not* defined over $\boldsymbol{Q}$. In fact, the curve V_T is defined over $\boldsymbol{Q}$ and the function field $\boldsymbol{Q}(V_T)$ is isomorphic to $\boldsymbol{Q}(j(z), j(Nz))$, where j is the classical modular function (cf. [10, p. 156]). Therefore $\mathfrak{p}=\varphi_T(\infty)$ is a rational point over $\boldsymbol{Q}$. Now $z(\boldsymbol{Q}; C_1)=z(\boldsymbol{Q}; C_2)=2$ [see (1.1)]. Hence Λ_0 is not defined over $\boldsymbol{Q}$ by Corollary 6, Part 1.

4. *The Rational Points over* $\boldsymbol{Q}$

Let the notation be as in § 3. Recall especially that we use σ to denote the generator of $\mathrm{Gal}(\boldsymbol{Q}(\sqrt{\varepsilon p})/\boldsymbol{Q})$. From the proof of Theorem 8, we see that there exist a $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$-covering $\Lambda=(W, V, \pi, \varphi)$ defined over $\boldsymbol{Q}$ and an isomorphism (Φ, Ψ) of Λ to Λ_0 rational over $\boldsymbol{Q}(\sqrt{\varepsilon p})$ such that $J_{SS}(\gamma)=\Phi^\sigma\circ\Phi^{-1}$ and $J_{TT}(\gamma)=\Psi^\sigma\circ\Psi^{-1}$ (cf. Theorem 1, Part 1). Our task in this section is to determine whether $V=V(p;N)$ has a rational point over $\boldsymbol{Q}$.

Lemma 9. *The curve V has a rational point over $\boldsymbol{Q}$ if and only if there is a point $z_0\in\mathfrak{H}^*$ such that $\varphi_T(z_0)\in V_T$ is rational over $\boldsymbol{Q}(\sqrt{\varepsilon p})$ and $\varphi_T(z_0)^\sigma=\varphi_T(-1/Nz_0)$.*

Proof. First observe that $J_{TT}(\gamma)(\varphi_T(z))=\varphi_T(-1/Nz)$ for all $z\in\mathfrak{H}^*$. Let $\alpha=\begin{bmatrix}0 & 1/N\\ -1 & 0\end{bmatrix}$ and $x=\alpha\circ\gamma^{-1}$. Then $\alpha\in G_{\boldsymbol{Q}^+}$ and $x\in T$. Therefore by [10, Theorem 9.6] we have

$$J_{TT}(\gamma)(\varphi_T(z))=J_{TT}(\alpha)(\varphi_T(z))=\varphi_T(\alpha(z))=\varphi_T(-1/Nz).$$

Now suppose $\mathfrak{p}$ is a point on V rational over $\boldsymbol{Q}$. Then for any automorphism τ of $\boldsymbol{C}$ such that $\tau = \sigma$ on $\boldsymbol{Q}(\sqrt{\varepsilon p})$ we have

$$\Psi(\mathfrak{p})^{\tau} = \Psi^{\tau}(\mathfrak{p}^{\tau}) = \Psi^{\tau}(\mathfrak{p}) = J_{TT}(\gamma)\,(\Psi(\mathfrak{p}))\,.$$

This shows that $\mathfrak{q} = \Psi(\mathfrak{p}) \in V_T$ is rational over $\boldsymbol{Q}(\sqrt{\varepsilon p})$ and $\mathfrak{q}^{\sigma} = J_{TT}(\gamma)\,(\mathfrak{q})$. Let z_0 be a point on $\mathfrak{H}^*$ such that $\varphi_T(z_0) = \mathfrak{q}$. Then

$$\varphi_T(z_0)^{\sigma} = J_{TT}(\gamma)\,(\varphi_T(z_0)) = \varphi_T(-1/N z_0)\,.$$

Conversely, suppose there is $z_0 \in \mathfrak{H}^*$ such that $\varphi_T(z_0)$ is rational over $\boldsymbol{Q}(\sqrt{\varepsilon p})$ and $\varphi_T(z_0)^{\sigma} = \varphi_T(-1/N z_0)$. Let $\mathfrak{q} = \varphi_T(z_0)$. Then $\mathfrak{q}$ is rational over $\boldsymbol{Q}(\sqrt{\varepsilon p})$ and $\mathfrak{q}^{\sigma} = J_{TT}(\gamma)\,(\mathfrak{q})$. From this it is easy to see that $\mathfrak{p} = \Psi^{-1}(\mathfrak{q})$ is rational over $\boldsymbol{Q}$.

Now we restrict ourselves to the case where V is of genus zero, i.e. when N is one of

$$2, 3, 5, 6, 7, 8, 10, 12, 13, 18\,. \tag{4.1}$$

The squares 1, 4, 9, 16 and 25 are not included because we require $\left(\frac{N}{p}\right) = -1$.

As noted in the Remark at the end of § 3, V_T has a rational point over $\boldsymbol{Q}$. Let X be a $\boldsymbol{Q}$-rational function on V_T which generates the function field $\boldsymbol{Q}(V_T)$. Then $f = X \circ \varphi_T$ generates the field $\boldsymbol{Q}(j(z), j(Nz))$. Conversely, any generator of $\boldsymbol{Q}(j(z), j(Nz))$ is obtained in this way. From Lemma 9, we derive easily the following.

Proposition 10. *Suppose V is of genus zero. Then V has a rational point over $\boldsymbol{Q}$ if and only if there is a point z_0 in $\mathfrak{H}^*$ such that $f(z_0) \in \boldsymbol{Q}(\sqrt{\varepsilon p})$ and $f(z_0)^{\sigma} = f(-1/N z_0)$ for any generator f of the field $\boldsymbol{Q}(j(z), j(Nz))$.*

Now for each N in the list (4.1), there is a $\Gamma_0(N)$-automorphic function f_N which generates $\boldsymbol{Q}(j(z), j(Nz))$ and satisfies

$$f_N(z) \cdot f_N(-1/Nz) = c_N \quad \textit{for all} \quad z \in \mathfrak{H}^*\,, \tag{4.2}$$

where c_N is a constant specified in the following table:

N	2	3	5	6	7	8	10	12	13	18
c_N	1	1	125	18	49	8	5	12	13	6

(4.3)

These f_N, c_N were given by Klein for prime N [7], and by Gierster for composite N [2]. When N is prime, the function f_N is defined explicitly as

$$f_N(z) = \sqrt[N-1]{\frac{\Delta(z)}{\Delta(Nz)}}\,,$$

where $\Delta(z)$ is the cusp form of weight 12 with the expression

$$\Delta(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24} \qquad (q = \exp(2\pi\sqrt{-1}z)).$$

Proposition 11. *Let N be one of the integers in the list* (4.1). *Then $V(p; N)$ has a rational point over $\boldsymbol{Q}$ if and only if c_N is the norm of some element of $\boldsymbol{Q}(\sqrt{\varepsilon p})$.*

Proof. By Proposition 10, $V = V(p; N)$ has a rational point over $\boldsymbol{Q}$ if and only if there is a $z_0 \in \mathfrak{H}^*$ such that $f_N(z_0) \in \boldsymbol{Q}(\sqrt{\varepsilon p})$ and $f_N(z_0)^\sigma = f_N(-1/Nz_0)$. Assume such a point z_0 exists. Then

$$c_N = f_N(z_0) \cdot f_N(-1/Nz_0) = f_N(z_0) \cdot f_N(z_0)^\sigma = Nr(f_N(z_0)),$$

where Nr denotes the norm from $\boldsymbol{Q}(\sqrt{\varepsilon p})$ to $\boldsymbol{Q}$.

Conversely, suppose $c_N = Nr(a)$ for some $a \in \boldsymbol{Q}(\sqrt{\varepsilon p})$. Let z_0 be a point on $\mathfrak{H}^*$ such that $f_N(z_0) = a$. Then

$$f_N(z_0) \cdot f_N(z_0)^\sigma = a \cdot a^\sigma = Nr(a) = c_n = f_N(z_0) \cdot f_N(-1/Nz_0).$$

Hence $f_N(z_0)^\sigma = f_N(-1/Nz_0)$.

By the above Proposition and an easy computation of the Hilbert symbol, we obtain the following table:

N	2	3	5	6	7	8	10	12	13	18
$V(p; N)$	+	+	−	$\left(\frac{2}{p}\right)=1$	+	−	$\left(\frac{5}{p}\right)=1$	−	−	−

(4.4)

where "+" stands for "$V(p; N)$ has a rational point over $\boldsymbol{Q}$", "−" stands for "$V(p; N)$ has no rational point over $\boldsymbol{Q}$", and "$\left(\frac{m}{p}\right)=1$" means "$V(p; N)$ has a rational point over $\boldsymbol{Q}$ if and only if $\left(\frac{m}{P}\right)=1$".

5. *Realization of $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$ as Galois Groups*

Theorem 12. *Let p be an odd prime such that 2, 3 or 7 is a quadratic non-residue modulo p. Then the group $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$ can be realized as the Galois group of some Galois extension over $\boldsymbol{Q}$.*

Proof. Let N be one of 2, 3 and 7 such that $\left(\frac{N}{p}\right) = -1$. Then $\Lambda(p; N)$ has a model $\Lambda = (W, V, \pi, \varphi)$ over $\boldsymbol{Q}$ such that V has a rational point over $\boldsymbol{Q}$ [cf. Theorem 8 and Table (4.4)]. Therefore the function field $\boldsymbol{Q}(V)$ is pure transcendental over $\boldsymbol{Q}$ and the covering Λ gives a Galois extension of $\boldsymbol{Q}(V)$ with Galois group isomorphic to $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$.

By Hilbert's irreducibility Theorem [6], this is sufficient to prove our assertion.

6. Remarks

(A) We have the following partial converse to Theorem 8: *If N is a prime and $\left(\frac{N}{p}\right) = 1$, then $\Lambda(p; N)$ has no model over $\boldsymbol{Q}$.*

Proof. Suppose $\Lambda(p; N) = (W, V, \pi, \varphi)$. By assumption, there is an integer A such that $N \cdot A^2 \equiv 1 \pmod{p}$. By the approximation theorem, there is $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$ such that $a \equiv d \equiv 0$, $b \equiv A$, $c \cdot A \equiv -1 \pmod{p}$. Let

$$\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1/\sqrt{N} \\ -\sqrt{N} & 0 \end{bmatrix} \in SL_2(\boldsymbol{R}).$$

Now N is prime, so $\Gamma_0(N)$ has exactly two cusps. Let $\mathfrak{p}_1, \mathfrak{p}_2$ be the points on V corresponding to these two cusps. It is easy to see that $\alpha\beta\alpha^{-1}\beta^{-1} \in \Gamma_0(N) \cap \Gamma(p)$ for all $\beta \in \Gamma_0(N)$. Therefore α induces an automorphism (Φ, Ψ) of $\Lambda(p; N)$ such that $\Psi(\mathfrak{p}_1) = \mathfrak{p}_2$. By Proposition 1, $\Lambda(p; N)$ has no model over $\boldsymbol{Q}$.

(B) It is not necessarily true that $\Lambda(p; N)$ has no model over $\boldsymbol{Q}$ if $\left(\frac{N}{p}\right) = 1$. For example, using Lehner and Newman's result [8, Theorem 1], one can prove the following assertion: *Suppose N is square free. Then $\Lambda(p; N)$ has a model over $\boldsymbol{Q}$ if and only if there is a divisor d of N such that $\left(\frac{d}{p}\right) = -1$.*

If N is not square free, then the result will not always hold. For example, take $N = 25$ and $p \equiv 3 \pmod{4}$ such that $\left(\frac{5}{p}\right) = -1$. As in (A), there is an $\alpha \in SL_2(R)$ which normalizes $\Gamma_0(25)$ and $\Gamma_0(25) \cap \Gamma(p)$, and $\alpha\beta\alpha^{-1}\beta^{-1} \in \Gamma_0(25) \cap \Gamma(p)$ for all $\beta \in \Gamma_0(25)$. Therefore α induces an automorphism of $\Lambda(p; N)$ of order 2. Now $\Gamma_0(25)$ has exactly 6 cusps. The map α sorts these cusps into three groups, each contains 2 equivalent points. Therefore the number of points of type C_1 is 0, 2, 4 or 6. In each case $\mu_1 \neq \mu_2$. So by the Remark after Proposition 2, $\Lambda(p; 25)$ has no model over $\boldsymbol{Q}$.

(C) Using Theorem 3 of Part 1, we can prove Theorem 8 for the case $N = 2$ without arithmetic theory of modular functions. Let $\Lambda = \Lambda(p; 2) = (W, V, \pi, \varphi)$. Then we have:

If (W', V', π', φ') is a $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$-covering of type $(2, p, p)$ (see Appendix, § 1), *then W and W' are conformally equivalent;* (6.1)

Suppose $p \geqq 5$. *Then* $\mathrm{Aut}(W)$ *is isomorphic to* $PGL_2(\mathbf{Z}/p\mathbf{Z})$ *if* $\left(\frac{2}{p}\right) = -1$, *to* $PSL_2(\mathbf{Z}/p\mathbf{Z}) \times Z_2$ *if* $\left(\frac{2}{p}\right) = 1$. *Here* Z_2 *is a cyclic group of order* 2. (6.2)

To prove Theorem 8 for $N = 2$, let σ be any automorphism of $\boldsymbol{C}$. Then Λ^σ is of type $(2, p, p)$. Hence by (6.1), W and W^σ are conformally equivalent. By (6.2), $\mathrm{Aut}(W)$ is complete if $\left(\frac{2}{p}\right) = -1$. Hence Λ has a model over $\boldsymbol{Q}$ by Theorem 3, Part 1.

The proofs of (6.1) and (6.2) are modeled on Hecke's proof [5] of the following result: Let (W, V, π, φ) be the $PSL_2(\mathbf{Z}/p\mathbf{Z})$-covering associated with $SL_2(\mathbf{Z})$. Then we have:

If (W', V', π', φ') *is a* $PSL_2(\mathbf{Z}/p\mathbf{Z})$*-covering of type* $(2, 3, p)$, *then* W *and* W' *are conformally equivalent;* (6.3)

Suppose $p \geqq 7$. *Then* $\mathrm{Aut}(W)$ *is isomorphic to* $PSL_2(Z/pZ)$. (6.4)

By Proposition 2 of the appendix, (6.1) is a consequence of the following statement:

Any two admissible systems of generators of $PSL_2(\mathbf{Z}/p\mathbf{Z})$ *with respect to* $(2, p, p \mid 0)$ *are quasi-equivalent.* (6.5)

The proof of (6.5) is similar to that of [5, Hilfssatz].

As for the proof of (6.2), note that $p \geqq 5$ implies that W is of genus $\geqq 2$, hence $\mathrm{Aut}(W)$ is finite. Also observe that $\begin{bmatrix} 0 & 1 \\ -2 & 0 \end{bmatrix}$ induces an automorphism of W not contained in $\varphi(PSL_2(\mathbf{Z}/p\mathbf{Z}))$. Let V_0 be the quotient space $W/\mathrm{Aut}(W)$, and $\pi_0 : W \to V_0$ the natural map. Using the method Hecke employed in [5], one proves that the Galois covering $\pi_0 : W \to V_0$ is of type $(2, 4, p)$ and $\varphi(PSL_2(\mathbf{Z}/p\mathbf{Z}))$ is of index 2 in $\mathrm{Aut}(W)$. To determine the group structure of $\mathrm{Aut}(W)$, we prove that the centralizer of $\varphi(PSL_2(\mathbf{Z}/p\mathbf{Z}))$ in $\mathrm{Aut}(W)$ is trivial if and only if $\left(\frac{2}{p}\right) = -1$.

That $\left(\frac{2}{p}\right) = -1$ is necessary is essentially proved in (A). Conversely, suppose $\varphi(PSL_2(\mathbf{Z}/p\mathbf{Z}))$ has a nontrivial centralizer $\{\gamma, \mathrm{id.}\}$ in $\mathrm{Aut}(W)$. Then γ is induced by a matrix $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -2 & 0 \end{bmatrix}$, with $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(2)$. For this α, we have

$$\alpha\beta\alpha^{-1}\beta^{-1} \in \Gamma_0(2) \cap \Gamma(p) \quad \textit{for all} \quad \beta \in \Gamma_0(2). \tag{6.6}$$

Take $\beta = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$ in (6.6). Then we have $2 \equiv c^2 \pmod{p}$.

(D) *Condition* (2) *of* Theorem 3, Part 1, *is essential.* We know that the $PSL_2(\boldsymbol{Z}/p\boldsymbol{Z})$-covering associated with $SL_2(\boldsymbol{Z})$ has no model over $\boldsymbol{Q}$ (§ 2). For this covering, condition (1) of the Theorem is true by (6.3), while condition (2) is false by virtue of (6.4). In view of (A), (6.1) and (6.2), $\Lambda(p; 2)$ with $\left(\frac{2}{p}\right) = 1$ would give some other such examples.

Appendix

1. Classification of Galois Coverings

Let G be a finite group, g a non-negative integer and $n_1, n_2, \ldots, n_r$ integers $\geqq 2$. An ordered system of generators $(\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g, \gamma_1, \ldots, \gamma_r)$ of G is called *admissible with respect to* $(n_1, n_2, \ldots, n_r \mid g)$ if

$$\alpha_1 \beta_1 \alpha_1^{-1} \beta_1^{-1} \ldots \alpha_g \beta_g \alpha_g^{-1} \beta_g^{-1} \gamma_1 \ldots \gamma_r = 1 \tag{1.1}$$

and

$$\textit{the order of } \gamma_i \textit{ is } n_i . \tag{1.2}$$

Two admissible systems of generators $(\alpha_i, \beta_i, \gamma_k)$ and $(\alpha_i', \beta_i', \gamma_k')$ are called *equivalent* (resp. *quasi-equivalent*) if there is an inner automorphism (resp. automorphism) of G sending α_i to α_i', β_i to β_i', and γ_k to γ_k'.

Fix a non-singular projective algebraic curve V of genus g defined over $\boldsymbol{C}$ and r points $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ on V. Denote the space $V - \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r\}$ by V^*. Then the fundamental group $\pi_1(V^*)$ has a system of generators $(A_1, B_1, \ldots, A_g, B_g, C_1, \ldots, C_r)$ with the defining relation

$$A_1 B_1 A_1^{-1} B_1^{-1} \ldots A_g B_g A_g^{-1} B_g^{-1} C_1 \ldots C_r = 1 . \tag{1.3}$$

We fix such a system of generators in the following discussion.

We call a G-covering $\Lambda = (W, V, \pi, \varphi)$ with the above V as base space of type $\{(\mathfrak{p}_1, n_1), (\mathfrak{p}_2, n_2), \ldots, (\mathfrak{p}_r, n_r)\}$ if $\mathfrak{p}_i$'s are the only points on V ramified in W and $e_{\mathfrak{p}_i} = n_i$.

Now by [11] and the theory of covering spaces, φ gives rise to a surjective homomorphism θ from $\pi_1(V^*)$ onto G. By (1.3) we see that

$$(\theta(A_1), \theta(B_1), \ldots, \theta(A_g), \theta(B_g), \theta(C_1), \ldots, \theta(C_r))$$

is an admissible system of generators of G with respect to $(n_1, n_2, \ldots, n_r \mid g)$. Conversely, from an admissible system of generators of G with respect to $(n_1, n_2, \ldots, n_r \mid g)$, we get a surjective homomorphism θ from $\pi_1(V^*)$ onto G. The kernel of the homomorphism corresponds to a covering of V^* which we can close up easily to obtain a Galois covering of V. Then the homomorphism θ endows the covering a G-covering structure. Obviously, this G-covering is of type $\{(\mathfrak{p}_1, n_1), (\mathfrak{p}_2, n_2), \ldots, (\mathfrak{p}_r, n_r)\}$.

We call two G-coverings $\Lambda=(W, V, \pi, \varphi)$ and $\Lambda'=(W', V', \pi', \varphi')$ *equivalent* if there is a couple (Φ, Ψ) consisting of conformal mappings $\Phi: W \to W'$ and $\Psi: V \to V'$ such that $\Psi \circ \pi = \pi' \circ \Phi$. If $V = V'$ and $\Psi = \mathrm{id}$, then we say that Λ and Λ' are *V-equivalent*.

Two G-coverings Λ and Λ' with the same base space V are called *V-isomorphic* if there is an isomorphism from Λ to Λ' of the form $(\Phi, \mathrm{id.})$. From the above discussion and these definitions we have

Proposition 1. *Let the notation be as above. Then there is a one-to-one correspondence between the equivalence classes (resp. quasi-equivalence classes) of admissible systems of generators of G with respect to $(n_1, n_2, \ldots, n_r \mid g)$ and the V-isomorphism classes (resp. V-equivalence classes) of G-coverings of type $\{(\mathfrak{p}_1, n_1), (\mathfrak{p}_2, n_2), \ldots, (\mathfrak{p}_r, n_r)\}$.*

Let n_1, n_2, n_3 be three integers $\geqq 2$. We call a G-covering $\Lambda=(W, V, \pi, \varphi)$ *of type* (n_1, n_2, n_3) if V is of genus zero and Λ is of type $\{(\mathfrak{p}_1, n_1), (\mathfrak{p}_2, n_2), (\mathfrak{p}_3, n_3)\}$ for some $\mathfrak{p}_i$ on V.

Fix a curve V of genus zero and three points $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ on V. It is easy to see that the classification of G-coverings of type (n_1, n_2, n_3) into isomorphism classes (resp. equivalence classes) is the same as the classification of G-coverings of type $\{(\mathfrak{p}_1, n_1), (\mathfrak{p}_2, n_2), (\mathfrak{p}_3, n_3)\}$ into V-isomorphism classes (resp. V-equivalence classes). Therefore by Proposition 1, we have

Proposition 2. *Let G be a finite group and n_1, n_2, n_3 integers $\geqq 2$. Then there is a one-to-one correspondence between the equivalence classes (resp. quasi-equivalence classes) of admissible system of generators of G with respect to $(n_1, n_2, n_3 \mid 0)$ and the isomorphism classes (resp. equivalence classes) of G-coverings of type (n_1, n_2, n_3).*

Example. Classification of $PSL_2(\mathbf{Z}/5\mathbf{Z})$-coverings of types (n_1, n_2, n_3).

Let $\Lambda=(W, V, \pi, \varphi)$ be a $PSL_2(\mathbf{Z}/5\mathbf{Z})$-covering of type (n_1, n_2, n_3). Denote by C_0, C_1, C_2, C_3, C_4 the conjugacy classes of $PSL_2(\mathbf{Z}/5\mathbf{Z})$ represented by $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, $\begin{bmatrix}0 & 1\\ -1 & -1\end{bmatrix}$, $\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}$, $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$ and $\begin{bmatrix}1 & 2\\ 0 & 1\end{bmatrix}$, respectively. Denote the number of points of type C_i on V by μ_i. Then by the trace formula (4.3), Part 1, we have $\mu_3 + \mu_4 \geqq 1$ and $\mu_2 \leqq 1$. Hence the type of Λ must be one of the following: (2, 3, 5), (3, 3, 5), (2, 5, 5), (3, 5, 5) and (5, 5, 5). The numbers of equivalence classes of the corresponding admissible systems of generators can be determined by the method used by Hecke [5]. In fact, there are 2 (resp. 2, 2, 4, 2) equivalence classes of admissible systems of generators with respect to $(2, 3, 5 \mid 0)$ [resp. $(3, 3, 5 \mid 0)$, $(2, 5, 5 \mid 0)$, $(3, 5, 5 \mid 0)$, $(5, 5, 5 \mid 0)$]. So by Proposition 2, we conclude that *there are* 12 *non-isomorphic $PSL_2(\mathbf{Z}/p\mathbf{Z})$-coverings of types (n_1, n_2, n_3).*

2. *Realization of Alternating Groups as Galois Groups*

We give a sketchy proof of Hilbert's result [6] on realizing alternating groups as Galois groups over the rationals by using Theorem 3, Part 1. Let $n \geqq 5$, and S_n (resp. A_n) the symmetric group (resp. alternating group) of degree n. Denote the elements $(1\,2)$, $(1\,2\,3 \ldots n)$ and $(n\,n-1 \ldots 4\,3\,1)$ of S_n by α_1, α_2 and α_3, respectively.

Proposition 3. *Let $(\gamma_1, \gamma_2, \gamma_3)$ be an admissible system of generators of S_n with respect to $(2, n, n-1 \mid 0)$. Suppose γ_1 is a transposition. Then $(\gamma_1, \gamma_2, \gamma_3)$ is equivalent to $(\alpha_1, \alpha_2, \alpha_3)$.*

Proof. Since γ_1 is a transposition, we may assume that $\gamma_1 = \alpha_1$. Write $\gamma_2 = A \cdot B$, where A is a product of disjoint cycles in which 1 or 2 appears, and B is a product of cycles disjoint from A. Suppose B is of order m. Then m divides n, the order of γ_2. On the other hand $\gamma_3^{-1} = \gamma_1 \cdot A \cdot B$ is of order $n-1$, and $\gamma_1 \cdot A$ is disjoint from B. Therefore m also divides $n-1$. Hence $m = 1$ and γ_2 is a product of at most two disjoint cycles in which 1 or 2 appears. Suppose there are two cycles in this product. Then it has to be of the form $(1\,a_3 \ldots a_l)(2\,a_{l+1} \ldots a_n)$, because γ_1 and γ_2 generate S_n. It follows that $\gamma_3^{-1} = (1\,a_{l+1} \ldots a_n\,2\,a_3 \ldots a_l)$ is of order n, a contradiction. Therefore γ_2 is a cycle of order n, say $\gamma_2 = (1\,a_3 \ldots a_l\,2\,a_{l+1} \ldots a_n)$. We claim $l = 2$ or n, i.e. $\gamma_2 = (1\,2\,a_3 \ldots a_n)$ or $(2\,1\,a_3 \ldots a_n)$. In either case, there is an inner automorphism of S_n fixing $\gamma_1 = \alpha_1 = (1\,2)$ and sending γ_2 to α_2.

Coming back to the proof that $l = 2$ or n, we observe that $\gamma_3^{-1} = (1\,a_{l+1} \ldots a_n)(2\,a_3 \ldots a_l)$. The order of γ_3, $(1\,a_{l+1} \ldots a_n)$ and $(2\,a_3 \ldots a_l)$ is $n-1$, $n-(l-1)$ and $(l-1)$, respectively. Hence the least common multiple of $(l-1)$ and $n-(l-1)$ is $n-1$. So our assertion follows from

Lemma 4. *Let x, y and n be positive integers such that $x+y=n$. Suppose the least common multiple $[x, y]$ of x and y is $n-1$. Then $x=1$ or $y=1$.*

Proof. Let m be the greatest common divisor of x and y. Then we have $m \mid n$ since $x+y=n$, and also $m \mid (n-1)$ since $[x, y] = n-1$. Therefore $m = 1$. Hence $x \cdot y = [x, y] \cdot m = n-1 = x+y-1$. So $(x-1)(y-1) = 0$.

Let $\Lambda = (W, V, \pi, \varphi)$ be an S_n-covering of type $(2, n, n-1)$ corresponding to the admissible system of generators $(\alpha_1, \alpha_2, \alpha_3)$ of S_n. For $\sigma \in \mathrm{Aut}(C/Q)$, Λ^σ is also of type $(2, n, n-1)$. Let $(\gamma_1, \gamma_2, \gamma_3)$ be the admissible system of generators of S_n corresponding to Λ^σ (see Proposition 2). By looking at the intermediate covering of Λ corresponding to the subgroup $H = \{\gamma \in S_n : \gamma \text{ fixes } 1\}$, one can prove that γ_1 is a transposition. Hence Λ and Λ^σ are isomorphic by Proposition 2 and 3. Especially, W and W^σ are conformally equivalent. Now we can show that $\varphi(S_n) = \mathrm{Aut}(W)$ the same way Hecke proved (6.4), Part 2. Hence in case $n \neq 6$,

Λ has a model over $\boldsymbol{Q}$ by Theorem 3, Part 1, because $S_n (n \neq 6)$ is complete [1]. In general, we have to use the stronger version of the Theorem. Let $(\Phi_\sigma, \Psi_\sigma)$ be an isomorphism of Λ to Λ^σ for $\sigma \in \mathrm{Aut}(\boldsymbol{C}/\boldsymbol{Q})$. By definition, $\Phi_\sigma^{-1} \circ \varphi(\gamma)^\sigma \circ \Phi_\sigma = \varphi(\gamma)$ for all $\gamma \in S_n$. Since $\mathrm{Aut}(W) = \varphi(S_n)$, (2.1) of Part 1 holds. So Λ has a model over $\boldsymbol{Q}$ by the Remark after Theorem 3, Part 1.

Therefore we may assume that Λ is defined over $\boldsymbol{Q}$. By Galois theory, corresponding to the subgroup A_n of S_n there is an A_n-covering (W, V', π', φ') defined over $\boldsymbol{Q}$. We prove that V' is of genus zero. First note that a point $\mathfrak{p} = \pi(\mathfrak{P})$ is ramified in V' if and only if $g_{\mathfrak{P}} \notin A_n$. (See § 3, Part 1 for notation.) Hence there are always exactly two points of V ramified in V'. Being a two-sheeted covering of V, V' is of genus zero by Hurwitz formula.

Finally we show that V' has a rational point over $\boldsymbol{Q}$. Let $\mathfrak{p} \in V$ be the point which is ramified in W of ramification index 2. It is obvious that $\mathfrak{p}$ is rational over $\boldsymbol{Q}$. Since $\mathfrak{p}$ is ramified in V', the unique point on V' lying over $\mathfrak{p}$ is also rational over $\boldsymbol{Q}$. Therefore the covering (W, V', π', φ') gives a Galois extension of $\boldsymbol{Q}(V')$, which is pure transcendental over $\boldsymbol{Q}$, with Galois group isomorphic to A_n. So by Hilbert's irreducibility Theorem [6], we have

Proposition 5. *For $n \geqq 5$, there exist Galois extensions of $\boldsymbol{Q}$ with Galois groups isomorphic to A_n.*

References

1. Burnside, W.: Theory of groups of finite order (2nd ed.). Cambridge University Press, 1911
2. Gierster, J.: Notiz über Modulargleichungen bei zusammengesetztem Transformationsgrad. Math. Ann. **14**, 537—544 (1879)
3. Hecke, E.: Über ein Fundamentalproblem aus der Theorie der elliptischen Modulfunktionen. Abh. Math. Sem. Hamburg 6 (1928). (Math. Werke, 525—547)
4. Hecke, E.: Über das Verhalten der Integrale 1. Gattung bei Abbildungen, insbesondere in der Theorie der elliptischen Modulfunktionen. Abh. Math. Sem. Hamburg 8 (1930). (Math. Werke, 548—558)
5. Hecke, E.: Die Eindeutige Bestimmung der Modulfunktionen q-ter Stufe durch algebraische Eigenschaften. Math. Ann. **111** (1935). (Math. Werke, 568—576)
6. Hilbert, D.: Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. J. Reine Angew. Math. 110 (1892). (Ges. Abh. II. 264—286)
7. Klein, F., Fricke, R.: Vorlesungen über die Theorie der Modulfunktionen II. Leipzig, 1892
8. Lehner, J., Newman, M.: Weierstrass points of $\Gamma_0(n)$. Ann. of Math. **79**, 360—368 (1964)
9. Shimura, G.: Correspondances modulaires et les fonctions ζ de courbes algébriques. J. Math. Soc. Japan **10**, 1—28 (1958)

10. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan, no. 11, 1971
11. Weil, A.: Généralisation des fonctions abéliennes. J. Math. Pures Appl. 9 série **17**, 47—87 (1938)
12. Weil, A.: The field of definition of a variety. Amer. J. Math. **78**, 509—524 (1956)

Kuang-yen Shih
Department of Mathematics
Princeton University
Princeton, N.J. 08540, USA

Current address
Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48106, USA

(Received June 19, 1972)