Part 2. Non-abelian classfields attached to subgroups of $\Gamma = PSL_2(\mathbf{Z}^{(p)})$ with finite indices.

Put $\Gamma = PSL_2(\mathbf{Z}^{(p)})$ and $\Gamma^* = \{x \in GL_2(\mathbf{Z}^{(p)}) | \det x \in \Pi\}/\pm\Pi$, where $\mathbf{Z}^{(p)} = \Pi \cdot \mathbf{Z}$ and $\Pi = p^{\mathbf{Z}}$ (the infinite cyclic group generated by p), so that $\Gamma^* \supset \Gamma$, $(\Gamma^* : \Gamma) = 2$. Our main purpose in Part 2 of this chapter is to show that the group Γ^* (resp. Γ, or other related groups) describes a certain "non-abelian classfield theory" over the rational function field $K^* = \mathbf{F}_p(\bar{j})$ (resp. $\mathbf{F}_{p^2}(\bar{j})$, or other related algebraic function fields). Namely, for each normal subgroup Γ' of (say) Γ^* with finite index, a finite Galois extension K' of K^* called the Γ'-*classfield* is defined, and the following main theorems are proved:

(i) for each Γ', the Γ'-classfield exists and is unique;
(ii) there is a certain isomorphism $\iota_{\Gamma'} : G(K'/K^*) \cong \Gamma^*/\Gamma'$;
(iii) the law of decomposition of prime divisors of K^* in K' is completely described by the primitive elliptic conjugacy classes of Γ^* (and the isomorphism $\iota_{\Gamma'}$).

More precisely, let $\wp(\Gamma^*)$, $\wp(K^*)$ and the bijection $\mathcal{J}^* : \wp(\Gamma^*) \to \wp(K^*)$ be as in §10 (Part 1), $\mathcal{J}^*$ being defined with respect to a fixed prime factor $\mathfrak{p}$ of p in $\mathbf{Q}^a$ (the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$). Then a finite Galois extension K' over K is called a Γ'-classfield if the following condition (♯) (§29) is satisfied:

(♯) An ordinary prime divisor $\mathfrak{P}^0$ of K^* (i.e., those $\mathfrak{P}^0$ contained in $\wp(K^*)$) is decomposed completely [5] in K' if and only if Γ_z^* is contained in Γ'; where $z (\in \mathfrak{H})$ is a representative of the Γ^*-equivalence class $\mathcal{J}^{*-1}(\mathfrak{P}^0)$, and Γ_z^* denotes its stabilizer in Γ^*.

With this definition, we have the following main theorems (§30):

Main Theorem (Γ^*-1). *For each Γ', Γ'-classfield exists and is unique.*

Main Theorem (Γ^*-2). *Let $\mathfrak{K}$ be the composite of all Γ'-classfields, where Γ' runs over all normal subgroups of Γ^* with finite indices. Then there is a dense injection $\iota : \Gamma^* \to G(\mathfrak{K}/K^*)$ satisfying the following conditions:*

(i) *ι induces an isomorphism of the completion of Γ^* with respect to "subgroups with finite indices topology" and $G(\mathfrak{K}/K^*)$; hence subgroups of Γ^* with finite indices and finite extensions of K^* contained in $\mathfrak{K}$ correspond in a one-to-one manner. Moreover, if Γ' is any normal subgroup of Γ^* with finite index, then the corresponding finite extension of K^* is nothing but the Γ'-classfield.*
(ii) *Let $\mathfrak{P}^0$ be any ordinary prime divisor of K^*, let z be a representative of $\mathcal{J}^{*-1}(\mathfrak{P}^0)$, and let Γ_z^* be the stabilizer of z in Γ^*. Let E_z^* be the torsion subgroup of Γ_z^*, and let γ be a positive generator of Γ_z^** mod *E_z^* with respect to $\mathfrak{p}$ (see §23). Then $\mathfrak{P}^0$ has an extension $\mathfrak{P}_z$ to $\mathfrak{K}$ whose inertia group is $\iota(E_z^*)$ and whose Frobenius substitution is* $\iota(\gamma)$ (mod $\iota(E_z^*)$).

[5] i.e., the relative degree is one.

(iii) *Let $\mathfrak{P}^0$ be the infinite prime divisor of K^* (i.e., $\mathfrak{P}^0(\bar{j}) = \infty$; see §22). Then $\mathfrak{P}^0$ has an extension $\mathfrak{P}_{i\infty}$ to $\mathfrak{K}$ whose inertia group is generated by $\iota\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)$ and whose Frobenius substitution (modulo the inertia group) is given by $\iota\left(\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\right)$.*

Main Theorem (Γ^*-3). *Let $\mathfrak{K}$ be as in Main Theorem* (Γ^*-2). *Then, $\mathfrak{K} \subset \widehat{\mathfrak{K}}$.*

Here, under the assumption[6] $p \neq 2, 3$, the field $\widehat{\mathfrak{K}}$ is defined to be the maximum Galois extension of $\mathbf{F}_{p^2}K^*$ such that

(i) if $\mathfrak{P}^0(\bar{j}) \neq 0, 12^3, \infty$, then $\mathfrak{P}^0$ is unramified in $\widehat{\mathfrak{K}}$;
(ii) if $\mathfrak{P}^0(\bar{j}) = 0, 12^3, \infty$, then $\mathfrak{P}^0$ is at most tamely ramified in $\widehat{\mathfrak{K}}$ with the ramification indices dividing $3, 2, \infty$ respectively.
(iii) if $\mathfrak{P}^0$ is supersingular (i.e., $\mathfrak{P}^0 \notin \wp(K^*)$ and $\mathfrak{P}^0(\bar{j}) \neq \infty$), then the relative degree of $\mathfrak{P}^0$ in $\widehat{\mathfrak{K}}/\mathbf{F}_{p^2}K^*$ is one.

On the other hand, whether $\mathfrak{K}$ coincides with $\widehat{\mathfrak{K}}$ is an open problem (our main conjecture for the group Γ^*; see §30).

Now, in the above formulation, Γ' was *any* normal subgroup of Γ^* with finite index. By Mennicke [23], however, the group $SL_2(\mathbf{Z}^{(p)})$ and hence also the group Γ^* have the congruence subgroup property; hence such Γ' is actually a congruence subgroup (i.e., contains some principal congruence subgroup). This fact is used essentially in the proof of Main Theorem (Γ^*-1). (Without Mennicke's result, we had to assume in our Main Theorems that Γ' is (or runs over) a congruence subgroup(s).) Apart from this, the proofs of our Main Theorems are based exclusively on a detailed study on the connection between the group Γ^* and the Shimura's and Igusa's modular function fields (i.e., certain fields obtained by division of elliptic curves whose modulus is a variable over the prime field of characteristic 0 and p respectively). Thus, although our main theorems are formulated without using elliptic curves at all,[7] their proofs are based on full applications of modern theory of elliptic curves. In fact, e.g., the existence of Γ'-classfield is shown by its explicit construction, using division points of elliptic curves.

Here, we note that since the bijection $\mathcal{J}^* : \wp(\Gamma^*) \to \wp(K^*)$ is not "absolutely well-defined" but depends on the choice of a prime factor $\mathfrak{p}$ of p in $\mathbf{Q}^a$, the definition of the Γ'-classfield also depends on the choice of $\mathfrak{p}$. This dependency, which is of quite a subtle nature (possibly reflecting some basic character of this theory), is studied in §32. We shall show that the composite $\mathfrak{K}$ of all Γ'-classfields is independent of $\mathfrak{p}$, and then determine what change on the injection ι of Main Theorem (Γ^*-2) (and hence also on the definition of Γ'-classfield) should be made when $\mathfrak{p}$ is replaced by $\mathfrak{p}^\sigma$ ($\sigma \in G(\mathbf{Q}^a/\mathbf{Q})$).

§11 ~ §14 are preliminaries; in §15 ~ §16, the connections between Γ^* and the Shimura's and Igusa's modular function fields are established; §17 ~ §28 are for the study of arithmetic of Igusa's modular function field, using our group Γ^*. The main theorems are formulated and proved in §29 ~ §30, and some supplements (including the effect of

[6] See §30 for the definition of $\widehat{\mathfrak{K}}$ for $p = 2, 3$.

[7] Supersingular prime divisors of K^* can also be defined without using elliptic curves. See [4].

changing $\mathfrak{p}$) are given in §31∼ §32. The final section §33 is for the remarks and numerical evidences for the conjecture $\mathfrak{K} = \widehat{\mathfrak{K}}$?

Examples of two simple facts obtained as applications of our results:

(i) For any given integer N, there is an example of algebraic curves over $\mathbf{F}_{p^2}$, which has *no* $\mathbf{F}_{p^2}$-birational *non-singular* projective model in $\mathbf{P}^N$. See §26, Remark 2.

(ii) Examples of elements of the group Γ^* that are not conjugate in Γ^* but are conjugate in all finite factor groups of Γ^* (Note that Γ^* is residually finite and that all non-trivial factor groups of Γ^* are finite.).[8] See §31, Remark 2

[An Indication]. For the proof of the announcement of §10 (Part 1), see §24.

Preliminaries on elliptic curves; results of Igusa and Shimura.

§11. Fields $k(E(n)), k(E(n))^0$. Let E be an elliptic curve over a field k. Let $k(E)$ be the field of all k-rational functions on E, and $k(E)^0$ the subfield of all $f \in k(E)$ satisfying $f(-u) = f(u)$ (for all $u \in E$). Let n be a positive integer not divisible by the characteristic of k, and let $E(n)$ be the group of all points $u \in E$ with $nu = 0$. Put

$$\text{(20)} \qquad \begin{cases} k(E(n)) = k(f(u) \mid u \in E(n), f \in k(E)), \\ k(E(n))^0 = k(f(u) \mid u \in E(n), f \in k(E)^0). \end{cases}$$

Fix any isomorphism $E(n) \cong (\mathbf{Z}/n\mathbf{Z})^2$. Then $k(E(n))$ is a finite Galois extension of k, and by the action of its Galois group G on $E(n)$, we can regard G as a subgroup of $GL_2(\mathbf{Z}/n\mathbf{Z})$. Let G^0 be the subgroup of G that corresponds to $k(E(n))^0$. Then $G^0 = G \cap \{\pm 1\}$. In fact, if $\sigma \in G^0$, then $f(u^\sigma) = f(u)$ for all $u \in E(n)$, $f \in k(E)^0$. But then $u^\sigma = \pm u$ for all $u \in E(n)$; hence in particular, for $u = (1,0), (0,1)$ and $(1,1)$. From this follows immediately that $\sigma = \pm 1$; hence $G^0 \subset \{\pm 1\}$. On the other hand, $G \cap \{\pm 1\} \subset G^0$ is obvious; hence $G^0 = G \cap \{\pm 1\}$.

Remark 1. The fact that $u^\sigma = \pm u$ for each $u \in E(n)$ implies $\sigma = \pm 1$ is used throughout the following without any remarks.

It is known that $k(E(n))$ always contains a primitive n-th root of unity ζ_n, and that for each $\sigma \in G$, we have

$$\text{(21)} \qquad \zeta_n^\sigma = \zeta_n^{\det \sigma} \qquad \text{(see Igusa [14], §3).}$$

[8]This last fact is due to Mennicke [23].

Hence $k(\zeta_n) \subset k(E(n))^0$, and the Galois group of $k(E(n))/k(\zeta_n)$ is $G \cap SL_2(\mathbf{Z}/n\mathbf{Z})$.

$$\begin{array}{ccc} k(E(n)) & \cdots & \{1\} \\ | & & | \\ k(E(n))^0 & \cdots & G \cap \{\pm 1\} \\ | & & | \\ k(\zeta_n) & \cdots & G \cap SL_2(\mathbf{Z}/n\mathbf{Z}) \\ | & & | \\ k & \cdots & G \subset GL_2(\mathbf{Z}/n\mathbf{Z}). \end{array} \tag{22}$$

Now let j be the absolute invariant of E (hence $j \in k$).

PROPOSITION 1. (i) *If $j \neq 0, 12^3$, the automorphism group of E is $\{\pm 1\}$;*
(ii) *if ch. $k \neq 2$, an automorphism of E which leaves fixed all elements of $E(2)$ is ± 1;*
(iii) *if ch. $k \neq 3$, an automorphism of E which leaves fixed all elements of $E(3)$ is 1.*

REMARK 2. In (ii), (iii), there is no condition on j. The important cases are (ii) $j = 12^3$, (iii) $j = 0$.

PROPOSITION 2. *If $j \neq 0, 12^3$, the field $k(E(n))^0$ depends only on k, j and n.*

PROOF OF PROPOSITION 1. (i) is rather well-known, and is indicated in J. Igusa [**14**].

(ii) Let σ be such an automorphism of E, and let ρ_2 be the 2-adic representation of the endomorphism ring of E. Then $\det \rho_2(\sigma) = \nu(\sigma) = 1$;[9] hence $\rho_2(\sigma)$ is contained in the group $X = \{x \in SL_2(\mathbf{Z}_2) \mid x \equiv 1 \pmod 2\}$. Since the automorphism group of E is always finite and since ρ_2 is faithful, it is enough to prove that the only elements of X of finite orders are ± 1. Since X is 2-primary, all finite subgroups of X are 2-groups; hence it is enough to show that no element of $X/\{\pm 1\}$ is of order two. Suppose that $x = \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ were such an element. Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. If the last sign is +, then $x = \pm 1$; hence a contradiction; if it is $-$, then $d = -a$, $a^2 + bc = -1$; but $a \equiv 1$, $b \equiv c \equiv 0 \pmod 2$; hence $-1 = a^2 + bc \equiv 1 \pmod 4$, which is also a contradiction.

(iii) In the same manner, it is enough to prove that the group $X = \{x \in SL_2(\mathbf{Z}_3) \mid x \equiv 1 \pmod 3\}$ has no elements of order 3. Suppose that $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ were such an element. Then $a + d = -1$, $ad - bc = 1$; hence $a(-1-a) = ad = 1 + bc \equiv 1 \pmod 9$; hence $a^2 + a + 1 \equiv 0 \pmod 9$, which is a contradiction.

This completes the proof of Proposition 1. □

PROOF OF PROPOSITION 2. Let E, E' be two elliptic curves over k with the same absolute invariant $j \neq 0, 12^3$. Then there is an isomorphism ρ of E onto E' defined over the algebraic closure of k. But by Chow's theorem [**3**], ρ is defined over the separable closure k^s of k. Let σ be any element of the Galois group $G(k^s/k)$. Then $\rho^{-1} \circ \rho^\sigma$ is an automorphism of E; hence $\rho^{-1} \circ \rho^\sigma = \pm 1$ (Proposition 1). Therefore, $\rho(u)^\sigma = \rho^\sigma(u^\sigma) = \varepsilon_\sigma \rho(u^\sigma)$ for all

[9] See Weil [35] for the symbol $\nu(\ )$.

$u \in E(n)$ with $\varepsilon_\sigma = \pm 1$. Therefore, $\rho(u)^\sigma = \pm\rho(u)$ (for $u \in E(n)$) holds if and only if $u^\sigma = \pm u$ (for $u \in E(n)$); which settles Proposition 2. □

Definition. In view of Proposition 2, we shall put

$$k_{j,n} = k(E(n))^0. \tag{23}$$

§12. Reduction of $k(E(n))^0$ mod $\tilde{v}$. Now let $j \in k$, with $j \neq 0, 12^3$. Then the following Tate's equation gives an elliptic curve over k with the absolute invariant j;

$$y^2 + xy = x^3 - \frac{36}{j - 12^3}x - \frac{1}{j - 12^3}, \tag{24}$$

the neutral element being $(x, y) = (\infty, \infty)$. An advantage of this over Weierstrass' equation $y^2 = 4x^3 - g_2x - g_3$ ($j = 12^3 g_2^3/(g_2^3 - 27g_3^2)$) is that (24) gives an elliptic curve (with absolute invariant j) for *any* characteristic including 2 and 3. We shall call this elliptic curve (24)

$$E_j, \tag{25}$$

throughout the following. Its addition theorem is given by

$$\text{(i)} \quad -(x, y) = (x, -x - y);$$

$$\text{(ii)} \quad \begin{cases} (x_1, y_1) + (x_2, y_2) = (x, y), \text{ with} \\ x \ = m + m^2 - x_1 - x_2, \\ y \ = (m+1)(x_1 + x_2 - m - m^2) - \frac{x_1y_2 - x_2y_1}{x_1 - x_2}, \end{cases} \tag{26}$$

where $m = \frac{y_1 - y_2}{x_1 - x_2}$. Thus, it is clear that

$$\begin{cases} \qquad k(E_j(n)) = k(x(u), y(u) \mid u \in E_j(n)), \\ k_{j,n} = \ k(E_j(n))^0 = k(x(u) \mid u \in E_j(n)). \end{cases} \tag{27}$$

Let v be an additive discrete valuation of k such that $v(j) = v(j - 12^3) = 0$. Let O_v and $\bar{k}$ be the valuation ring and the residue class field of v respectively; and for each $a \in k$, let $\bar{a}$ denote its residue class mod v, so that $\bar{a} \in \bar{k}$ ($a \in O_v$), $\bar{a} = \infty$ ($a \notin O_v$). In particular, $\bar{j} \neq 0, 12^3, \infty$.

Now $E_j \to E_{\bar{j}}$ is a good reduction of elliptic curves, and the addition theorem for $E_{\bar{j}}$ is also given by (26); hence the general theory of good reduction of abelian varieties (cf. e.g., Shimura [**29**]) can be applied, and we obtain:

Proposition 3. *The notations being as above, let $v(j) = v(j - 12^3) = v(n) = 0$, and let $\tilde{v}$ be any extension of v to $k(E_j(n))$. Then,*

$$(x(u), y(u)) \underset{\text{mod } \tilde{v}}{\longmapsto} (\overline{x(u)}, \overline{y(u)}) \quad (u \in E_j(n)) \tag{28}$$

gives an isomorphism of $E_j(n)$ onto $E_{\bar{j}}(n)$. ($(\overline{x(u)}, \overline{y(u)})$ are the (x, y)-coordinates of points of $E_{\bar{j}}(n)$.)

In particular, $\overline{x(u)}, \overline{y(u)}$ are finite for $u \neq 0$ for all extensions $\tilde{v}$ of v; hence $x(u)$ and $y(u)$ for $u \neq 0$ must be integral over O_v.

Corollary. *The notations and assumptions being as above and as in Proposition 3, express by* $\bar{\ }$ *the residue class or residue field modulo* $\bar{v}$. *Then*

(i) $\overline{k_{j,n}} \supset \bar{k}_{\bar{j},n}$;

(ii) *if the two fields of (i) coincide, then* $\bar{v}$ *is unramified in* $k_{j,n}/k$.

Remark. *The two fields* $\overline{k_{j,n}}$ *and* $\bar{k}_{\bar{j},n}$ *always coincide if* $\bar{k}$ *is perfect.* In fact, $\overline{k_{j,n}}/\bar{k}$ is then a Galois extension, and hence the homomorphism $\sigma \mapsto \bar{\sigma}$ (defined below) is surjective. Moreover the argument below shows that $\bar{\sigma}|_{\bar{k}_{\bar{j},n}} = 1$ implies $\sigma = 1$. Therefore, $\bar{k}_{\bar{j},n}$ must coincide with $\overline{k_{j,n}}$.

Proof of the Corollary. (i) is an immediate consequence of Proposition 3. To prove (ii), let G' be the decomposition group of $\bar{v}$ in $k_{j,n}/k$, so that there is a natural *onto* homomorphism $G' \ni \sigma \mapsto \bar{\sigma} \in G(\overline{k_{j,n}}/\bar{k})$ (since $\overline{k_{j,n}} = \bar{k}_{\bar{j},n}$ and hence it is a Galois extension over $\bar{k}$). Let σ be such that $\bar{\sigma} = 1$. Then for each $u \in E_j(n)$, $x(u)^\sigma$ and $x(u)$ have the same residue classes. But then it follows directly from Proposition 3 that $x(u)^\sigma = x(u)$ for all $u \in E_j(n)$; hence $\sigma = 1$. Therefore, the inertia group of $\bar{v}$ in $k_{j,n}/k$ is trivial. Since $\overline{k_{j,n}} = \bar{k}_{\bar{j},n}$ is separable over $\bar{k}$, this settles (ii). □

§13. $k(E(n))^0$ **when** k **is a rational function field over a prime field.** Now let F be a *prime field,* j a variable over F, and $k = F(j)$. For each $n \not\equiv 0 \pmod{\mathrm{ch}.F}$, put $k_n = k_{j,n}$ and let ζ_n be a primitive n-th root of unity. So by §11, the Galois group $G(k_n/k)$ can be considered as a subgroup of $GL_2(\mathbf{Z}/n\mathbf{Z})/\pm 1$. Now by G. Shimura **[30]** (ch $F = 0$) and J. Igusa **[14]** (ch $F > 0$), we have the following:

Theorem A. *The notations being as above,* $k(\zeta_n)$ *is algebraically closed in* k_n, *and the Galois group* $G(k_n/k)$ *is given by*

$$(29)\quad \begin{aligned} G(k_n/k) &= GL_2(\mathbf{Z}/n\mathbf{Z})/\pm 1 \cdots \mathrm{ch}.F = 0,\\ &= \{\sigma \in GL_2(\mathbf{Z}/n\mathbf{Z}) \mid \det\sigma \in \Pi_n\}/\pm 1 \cdots \mathrm{ch}.F > 0,^{10} \end{aligned}$$

where if $\mathrm{ch}.F = p > 0$, Π_n *denotes the cyclic subgroup of* $(\mathbf{Z}/n\mathbf{Z})^\times$ *generated by* p. *In particular, we have* $G(k_n/k(\zeta_n)) = SL_2(\mathbf{Z}/n\mathbf{Z})/\pm 1$ *in both cases (see §11).*

Examples (Igusa **[14]**, §3). We have

$$(30)\quad k_2 = k(\lambda), \quad \text{with} \quad j = 2^8\frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2} \quad (\mathrm{ch}.F \neq 2),$$

$$(31)\quad k_3 = k(\mu, \zeta_3), \quad \text{with} \quad j = \left\{\frac{3\mu(\mu^3+2^3)}{\mu^3-1}\right\}^3 \quad (\mathrm{ch}.F \neq 3).$$

Since $G(k_2/k) = SL_2(\mathbf{Z}/2\mathbf{Z}) \cong \mathfrak{S}_3$, k_2 contains a quadratic extension of k, which is generated by $\sqrt{j-12^3} = \frac{2^3(\lambda-2)(\lambda+1)(2\lambda-1)}{\lambda(1-\lambda)}$. Since $G(k_3/k(\zeta_3)) = SL_2(\mathbf{Z}/3\mathbf{Z})/\pm 1 \cong \mathfrak{A}_4$, k_3

[10] In Igusa **[14]**, it is proved that if $k = F^a(j)$ (F : the prime field of characteristic $p > 0$, F^a : the algebraic closure), then $G(k_n/k) = SL_2(\mathbf{Z}/n\mathbf{Z})/\pm 1$ for $n \not\equiv 0 \pmod p$. Our formulation follows immediately from this by using (21), (22). Actually, this Igusa's theorem can also be proved by our method; i.e., by using the decomposition law of prime divisors of k in k_n.

contains a cubic cyclic extension of $k(\zeta_3)$ (corresponding to the Klein's four group in $\mathfrak{A}_4$), which is generated by $\sqrt[3]{j}$. Thus,

$$k_2 \ni \sqrt{j-12^3}, \quad k_3 \ni \sqrt[3]{j}. \tag{32}$$

§14. $k(E(n))^0$ when k is a rational function field over Q; modular functions of level n. We denote by $\mathfrak{z}$ the *variable* of the complex upper half plane $\mathfrak{H}$, and by z special points of $\mathfrak{H}$. Let $j(\mathfrak{z})$ be the elliptic modular function, and put $k = \mathbf{Q}(j(\mathfrak{z}))$. For each n, put $k_n = k_{j(\mathfrak{z}),n}$. Then by G. Shimura [30], k_n can be realized as a subfield of the field of automorphic functions of level n. This is done as follows.

Let $\wp(u|\omega_1,\omega_2)$ be the Weierstrass $\wp$-function with periods ω_1,ω_2, and let $g_i(\omega_1,\omega_2)$ ($i=2,3$) denote $60\sum'(m\omega_1+n\omega_2)^{-4}$ and $140\sum'(m\omega_1+n\omega_2)^{-6}$ respectively, where (m,n) runs over $\mathbf{Z}^2-(0,0)$. Put $g_i(\mathfrak{z}) = g_i(\mathfrak{z},1)$ ($i=2,3$), so that $j(\mathfrak{z}) = 12^3 g_2(\mathfrak{z})^3/(g_2(\mathfrak{z})^3 - 27g_3(\mathfrak{z})^2)$. For each positive integer n, consider $\mathbf{Z}/n\mathbf{Z}$ as a subgroup of $\mathbf{Q}/\mathbf{Z}$, so that the elements of $\mathbf{Z}/n\mathbf{Z}$ are i/n ($i\in\mathbf{Z}$, considered mod n). For each $\alpha,\beta\in\mathbf{Z}/n\mathbf{Z}$ with $(\alpha,\beta)\neq(0,0)$, put

$$\begin{cases} x'_{\alpha\beta}(\mathfrak{z}) &= \frac{g_2(\mathfrak{z})}{g_3(\mathfrak{z})}\wp(\alpha\mathfrak{z}+\beta|\mathfrak{z},1),\\ x_{\alpha\beta}(\mathfrak{z}) &= -\frac{1}{18}x'_{\alpha\beta}(\mathfrak{z})-\frac{1}{12}. \end{cases} \tag{33}$$

Then, by Shimura [30] (§4), we have the following propositions:

PROPOSITION 4. *For each $\sigma\in PSL_2(\mathbf{Z})$, we have $x_{(\alpha\beta)\sigma}(\mathfrak{z}) = x_{\alpha\beta}(\sigma\mathfrak{z})$ (in particular, $x_{\alpha\beta}(\sigma\mathfrak{z}) = x_{\alpha\beta}(\mathfrak{z})$ if $\sigma\equiv\pm1$ (mod n)). Moreover, the field $\mathbf{C}(j(\mathfrak{z}); x_{\alpha\beta}(\mathfrak{z})\mid\alpha,\beta\in\mathbf{Z}/n\mathbf{Z})$ coincides with the field of modular functions of level n.*

PROPOSITION 5. *The notations being as above, we have*

$$k_n = k(x_{\alpha\beta}(\mathfrak{z})\mid\alpha,\beta\in\mathbf{Z}/n\mathbf{Z}).^{11} \tag{34}$$

Moreover, there is an isomorphism $\iota: E_{j(\mathfrak{z})}(n)\cong(\mathbf{Z}/n\mathbf{Z})^2$, unique up to ±1, such that for any $\alpha,\beta\in\mathbf{Z}/n\mathbf{Z}$ with $(\alpha,\beta)\neq(0,0)$, $x_{\alpha\beta}(\mathfrak{z})$ coincides with the x-coordinate of the point $\iota^{-1}(\alpha,\beta)$ of $E_{j(\mathfrak{z})}$.

Proposition 4 is rather well-known, and is easily proved. Here, we shall reproduce the proof of Proposition 5 (in our notations). Put

$$x'(u,\mathfrak{z}) = \frac{g_2(\mathfrak{z})}{g_3(\mathfrak{z})}\wp(u|\mathfrak{z},1);\quad y'(u,\mathfrak{z}) = \left(\frac{g_2(\mathfrak{z})}{g_3(\mathfrak{z})}\right)^{3/2}\frac{\partial}{\partial u}\wp(u|\mathfrak{z},1). \tag{35}$$

Then we have $y'(u,\mathfrak{z})^2 = 4x'(u,\mathfrak{z})^3 - t(\mathfrak{z})x'(u,\mathfrak{z}) - t(\mathfrak{z})$, with $t(\mathfrak{z}) = \frac{g_2(\mathfrak{z})^3}{g_3(\mathfrak{z})^2}$. Hence if we put

$$\begin{cases} x(u,\mathfrak{z}) &= -\frac{1}{18}x'(u,\mathfrak{z})-\frac{1}{12},\\ y(u,\mathfrak{z}) &= \frac{1}{108\sqrt{2}}y'(u,\mathfrak{z})+\frac{1}{36}x'(u,\mathfrak{z})+\frac{1}{24}, \end{cases} \tag{36}$$

then we see that $x = x(u,\mathfrak{z})$, $y = y(u,\mathfrak{z})$ satisfy (24) for $j = j(\mathfrak{z})$. Now put $K = \mathbf{C}\cap\mathbf{Q}(j(\mathfrak{z}); x_{\alpha\beta}(\mathfrak{z})\mid\alpha,\beta\in\mathbf{Z}/n\mathbf{Z})$, so that K is finitely generated over $\mathbf{Q}$, and

[11] Shimura used this to prove Theorem A for $F = \mathbf{Q}$.

$\mathbf{Q}(j(\mathfrak{z});\ x_{\alpha\beta}(\mathfrak{z}) \mid \alpha,\beta \in \mathbf{Z}/n\mathbf{Z})$ is of dimension one over K (by Proposition 4). Let $z \in \mathfrak{H}$ be such that $j(z)$ is transcendental over K. Then

(37) $$(j(\mathfrak{z});\ x_{\alpha\beta}(\mathfrak{z}))_{\alpha,\beta} \longmapsto (j(z);\ x_{\alpha\beta}(z))_{\alpha,\beta}$$

is a specialization over $\mathbf{C}$ and hence also over K. By comparing the dimensions of both sides over K, we see that (37) is a generic specialization over K, and hence also over $\mathbf{Q}$. Therefore, there is an isomorphism σ of $\mathbf{Q}(j(\mathfrak{z});\ x_{\alpha\beta}(\mathfrak{z}) \mid \alpha,\beta \in \mathbf{Z}/n\mathbf{Z})$ onto $\mathbf{Q}(j(z);\ x_{\alpha\beta}(z) \mid \alpha,\beta \in \mathbf{Z}/n\mathbf{Z})$, sending $j(\mathfrak{z})$ to $j(z)$ and $x_{\alpha\beta}(\mathfrak{z})$ to $x_{\alpha\beta}(z)$ for all α,β. But, on the other hand, $x(u,z)$, $y(u,z)$ are generators of elliptic functions on $\mathbf{C}/[z,1]$, and they satisfy (24) with $j = j(z)$; hence we can identify $E_{j(z)}$ with $\mathbf{C}/[z,1]$ by $(x(u,z), y(u,z)) \leftrightarrow u$. Moreover, there is an isomorphism $\iota_z : E_{j(z)}(n) \cong (\mathbf{Z}/n\mathbf{Z})^2$ given by $\alpha z + \beta \leftrightarrow (\alpha,\beta)$. Therefore, $x_{\alpha\beta}(z) = x(\alpha z + \beta; z)$ is nothing but the x-coordinate of $\iota_z^{-1}(\alpha,\beta)$. This fact pulled back by σ gives Proposition 5. □

The group Γ^* and the extension $\mathfrak{K}/\bar{k}$.

Throughout the following, p is a fixed prime number, and $\mathfrak{p}$ is a fixed prime factor of p in the algebraic closure $\mathbf{Q}^a$ of $\mathbf{Q}$. The residue field of $\mathbf{Q}^a$ mod $\mathfrak{p}$ will be identified, once and for all, with the algebraic closure $\mathbf{F}_p^a$ of $\mathbf{F}_p$. Sometimes $\mathfrak{p}$ is considered as a place $\mathbf{Q}^a \to \mathbf{F}_p^a$,[12] and sometimes identified with its kernel, i.e., the maximal ideal of the ring of all $\mathfrak{p}$-integers in $\mathbf{Q}^a$. By n, we always denote a positive integer not divisible by p.

§15. The place $\wp$. Let $j(\mathfrak{z})$ be the elliptic modular function, abbreviated simply as j; $j = j(\mathfrak{z})$. Put

(38) $$k = \mathbf{Q}(j),$$

and for each $n \not\equiv 0 \pmod p$, consider the *Shimura's modular function field*, i.e.,

(39) $$k_n = k_{j,n} = k(x_{\alpha\beta} \mid \alpha,\beta \in \mathbf{Z}/n\mathbf{Z}),$$

where $x_{\alpha\beta} = x_{\alpha\beta}(\mathfrak{z})$ are as in §14. Put

(40) $$M\{k\} = \bigcup_{n \not\equiv 0 \bmod p} k_n,$$

which is an infinite Galois extension of k. Let G be the Galois group of $M\{k\}$ over k. Then by Theorem A, G is isomorphic to the group

(41) $$\left\{\prod_{l \neq p} GL_2(\mathbf{Z}_l)\right\} / \pm 1,$$

[12] Of course, some elements of $\mathbf{Q}^a$ go to infinity by $\mathfrak{p}$, but we shall always write in this way.

the isomorphism depending on the "n-adic" coordinate system (injective system for all $n \not\equiv 0 \pmod p$) on E_j. Take *the* coordinate system defined by Proposition 5, and by the corresponding isomorphism, identify G with the group (41); thus

$$G = \left\{ \prod_{l \neq p} GL_2(\mathbf{Z}_l) \right\} / \pm 1, \tag{42}$$

$$\sigma(x_{\alpha\beta}) = x_{(\alpha\beta)\sigma}; \quad \text{for} \quad \sigma \in G; \quad \alpha, \beta \in \mathbf{Z}/n\mathbf{Z}. \tag{43}$$

On the other hand, let $\bar{j}$ be a variable over $\mathbf{F}_p$, put

$$\bar{k} = \mathbf{F}_p(\bar{j}), \tag{44}$$

and for each $n \not\equiv 0 \pmod p$, consider the *Igusa's modular function field*, i.e.,

$$\bar{k}_n = \bar{k}_{\bar{j},n} \quad \text{(see §11, (23))}. \tag{45}$$

Put

$$M\{\bar{k}\} = \bigcup_{n \not\equiv 0 \bmod p} \bar{k}_n, \tag{46}$$

which is an infinite Galois extension of $\bar{k}$. Let $\overline{G}$ be the Galois group of $M\{\bar{k}\}$ over $\bar{k}$. Let Σ be an "n-adic" coordinate system (injective system for all $n \not\equiv 0 \pmod p$) on $E_{\bar{j}}$, and let φ_Σ be the corresponding "n-adic" representation of $\overline{G}$. Then by Theorem A, $\overline{G}$ is isomorphic by φ_Σ to

$$\left\{ \bar{\sigma} \in \prod_{l \neq p} GL_2(\mathbf{Z}_l) \;\middle|\; \det \bar{\sigma} \in \overline{\Pi} \right\} / \pm 1, \tag{47}$$

where $\overline{\Pi}$ denotes the subgroup of $\prod_{l \neq p} \mathbf{Z}_l^\times$ topologically generated by the diagonal p. (As is easily seen, the group $\overline{\Pi}$ is topologically isomorphic to the group $\sum_l \mathbf{Z}_l$, the direct sum being taken over *all* prime numbers l *including* p.) An important remark is that by a change of our n-adic coordinate system Σ, φ_Σ is changed by an inner automorphism of the group

$$\left\{ \prod_{l \neq p} GL_2(\mathbf{Z}_l) \right\} / \pm 1,$$

which may be an *outer* automorphism of the group (47). *Thus φ_Σ is not unique even up to inner automorphisms of G. But, on the other hand, some important automorphisms of $M\{\bar{k}\}/\bar{k}$, such as the Frobenius substitutions of prime divisors, are well-defined up to inner automorphisms of $\overline{G}$; hence to describe them definitively by the group* (47), *we need to find and fix a "special" coordinate system Σ, which must be well-defined up to $\overline{G}$.*

Thus, we shall proceed to define such a "special" $\overline{G}$-class of Σ.[13] For this purpose, we need the following proposition, which is an easy consequence of Theorem A.

[13] As the readers will see, this class is not "absolutely well-defined", but depends on the special choice of $\mathfrak{p}$. At any rate, once $\mathfrak{p}$ is fixed, it is well-defined.

PROPOSITION 6. *There exists a place*

$$\wp : M\{k\} \to M\{\bar{k}\}, \tag{48}$$

unique up to $\overline{G}$, *such that*

(i) $\wp$ *coincides with* $\mathfrak{p}$ *on* $M\{k\} \cap \mathbf{Q}^{\mathrm{a}} = \bigcup_{n \not\equiv 0 \pmod p} \mathbf{Q}(\zeta_n)$*;*

(ii) $\wp(j) = \bar{j}$.

Moreover, if $\wp$ *is such a place, then we have*

$$\wp(k_n) = \bar{k}_n. \tag{49}$$

PROOF. Put $\mathbf{Q}' = \bigcup_{n \not\equiv 0 \pmod p} \mathbf{Q}(\zeta_n)$. Let $\wp'$ be the unique place of $\mathbf{Q}'(j)$ that coincides with $\mathfrak{p}$ on $\mathbf{Q}'$ and that sends j to $\bar{j}$; hence $\wp'$ corresponds to the following discrete valuation[14] V of $\mathbf{Q}'(j)$:

$$V\left(p^m \frac{h(j)}{g(j)}\right) = m; \quad \text{for} \quad g(j),\ h(j) \in O'[j],\ \notin pO'[j]; \tag{50}$$

where O' is the ring of $\mathfrak{p}$-integers in $\mathbf{Q}'$. Let $\wp$ be any extension of $\wp'$ to a place of $M\{k\}$. Then it follows directly from Proposition 3 that $\wp(k_n) \supset \bar{k}_n$. But by Theorem A, $[\bar{k}_n : \bar{k}(\bar{\zeta}_n)] = [k_n : k(\zeta_n)]$, where $\bar{\zeta}_n = \wp(\zeta_n)$. Therefore, $\wp(k_n) = \bar{k}_n$; hence $\wp[M\{k\}] = M\{\bar{k}\}$; hence $\wp$ is a desired place.

On the other hand, if $\wp_1$ is another place satisfying (i), (ii), then $\wp_1 = \wp$ on $\mathbf{Q}'(j)$; hence there is some $\sigma \in G(M\{k\}/\mathbf{Q}'(j))$ with $\wp_1 = \wp^\sigma$. So, it is enough to show that the decomposition group of $\wp$ in $M\{k\}/\mathbf{Q}'(j)$ is the full Galois group of this extension; or equivalently, that the decomposition group of $\wp$ in $k_n/k(\zeta_n)$ is the full Galois group for all $n \not\equiv 0 \pmod p$. But this is in fact so, since by Theorem A, the relative degree $[\wp(k_n) : \wp(k(\zeta_n))] = [\bar{k}_n : \bar{k}(\bar{\zeta}_n)]$ is equal to $[k_n : k(\zeta_n)]$. □

We have also proved:

COROLLARY 1. $\wp$ *corresponds to a discrete valuation of* $M\{k\}$ *having* p *as a prime element;* $\wp$ *is unramified and remains träge in* $M\{k\}/\mathbf{Q}'(j)$*, where* $\mathbf{Q}' = \bigcup_{n \not\equiv 0 \pmod p} \mathbf{Q}(\zeta_n)$*, and also in* $k_n/k(\zeta_n)$ *for all* $n \not\equiv 0 \pmod p$.

By Propositions 3, 6, it is clear that:

COROLLARY 2. $\bar{k}_n = \bar{k}(\bar{x}_{\alpha\beta} \mid \alpha, \beta \in \mathbf{Z}/n\mathbf{Z})$*, where* $\bar{x}_{\alpha\beta} = \wp(x_{\alpha\beta})$.

Now we shall define the special ($\overline{G}$-)class of Σ on $E_{\bar{j}}$. Take any $\wp$ satisfying Proposition 6, and let $\Sigma = \Sigma_\wp$ be the unique (up to ± 1) coordinate system on $E_{\bar{j}}$ by which $\bar{x}_{\alpha\beta}$ corresponds to (α, β) for all α, β. Then by Proposition 6, any change of $\Sigma_\wp$ by a different choice of $\wp$ is merely a change by an action of an element of $\overline{G}$; hence the $\overline{G}$-class of $\Sigma_\wp$ is well-defined. *Now fix any* $\wp$ *once and for all, and identify* $\overline{G}$ *with the group* (47) *by* $\Sigma_\wp$*; thus, we have*

$$\overline{G} = \left\{ \bar{\sigma} \in \prod_{l \neq p} GL_2(\mathbf{Z}_l) \;\middle|\; \det \bar{\sigma} \in \overline{\Pi} \right\} / \pm 1, \tag{51}$$

[14] Note that p is unramified in $\mathbf{Q}'$, and hence p is a prime element of $\mathbf{Q}' \cap \mathfrak{p}$.

(52) $$\overline{\sigma}(\overline{x}_{\alpha\beta}) = \overline{x}_{(\alpha\beta)\overline{\sigma}}; \quad \text{for} \quad \overline{\sigma} \in \overline{G}; \quad \alpha,\beta \in \mathbf{Z}/n\mathbf{Z}.$$

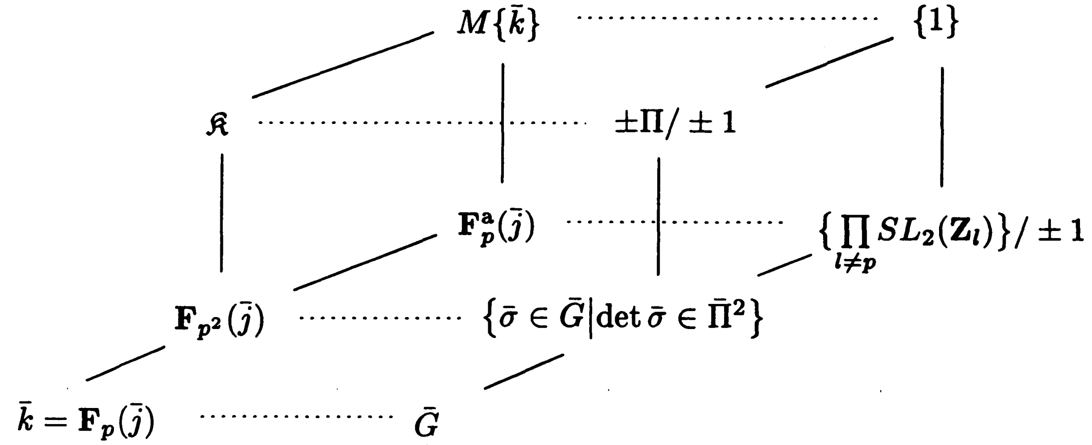
Obviously, the natural injection of the right side of (51) into the right of (42) corresponds to the injection $\overline{G} \to G$ defined by the natural identification of $\overline{G}$ with the decomposition group of $\wp$ in $M\{k\}/k$.

Now let

(53) $$\mathfrak{K}$$

be the subfield of $M\{k\}$ that corresponds to the subgroup $\pm\overline{\Pi}/\pm 1$ of $\overline{G}$. This is the field in which we are most interested. We have the following figure;

(54)



Here, $\square$ is "parallellogram"; i.e.,

(55) $$\mathfrak{K} \cap \mathbf{F}_p^{\mathrm{a}}(\bar{j}) = \mathbf{F}_{p^2}(\bar{j}), \quad \mathfrak{K}\cdot\mathbf{F}_p^{\mathrm{a}}(\bar{j}) = M\{\bar{k}\}.$$

Thus, the Galois groups of $\mathfrak{K}/\bar{k}$, $\mathfrak{K}/\mathbf{F}_{p^2}\bar{k}$, are given by

(56) $$\begin{cases} G(\mathfrak{K}/\bar{k}) = \left\{\overline{\sigma} \in \prod_{l\neq p} GL_2(\mathbf{Z}_l) \mid \det\overline{\sigma} \in \overline{\Pi}\right\} / \pm\overline{\Pi}, \\ G(\mathfrak{K}/\mathbf{F}_{p^2}\bar{k}) = \left\{\overline{\sigma} \in \prod_{l\neq p} GL_2(\mathbf{Z}_l) \mid \det\overline{\sigma} \in \overline{\Pi}^2\right\} / \pm\overline{\Pi}, \\ \qquad\qquad \overset{15}{=} \left\{\prod_{l\neq p} SL_2(\mathbf{Z}_l)\right\} / \pm 1. \end{cases}$$

Remark . Since the subgroup $\pm\overline{\Pi}/\pm 1$ is invariant by the inner automorphisms of $\left\{\prod_{l\neq p} GL_2(\mathbf{Z}_l)\right\} / \pm 1$, *the field* $\mathfrak{K}$ *is absolutely well-defined* (*in particular, it does not depend on the choice of* $\mathfrak{p}$).

§16. Now the groups

(57) $$\begin{cases} \Gamma^* = \left\{\gamma \in GL_2(\mathbf{Z}^{(p)}) \mid \det\gamma \in \Pi\right\} / \pm\Pi, \\ \Gamma = SL_2(\mathbf{Z}^{(p)})/\pm 1, \end{cases}$$

---

[15]Identify.

are going to play the central roles! Here, as in §1, Π is the infinite cyclic subgroup of $\mathbf{Q}^\times$ generated by p, and $\mathbf{Z}^{(p)} = \Pi \cdot \mathbf{Z}$. By (56), Γ^* can be regarded as a (dense) subgroup of the Galois group $G(\mathfrak{K}/\bar{k})$ by the diagonal embedding

$$\Gamma^* \to G(\mathfrak{K}/\bar{k}) = \left\{ \bar{\sigma} \in \prod_{l \neq p} GL_2(\mathbf{Z}_l) \mid \det \bar{\sigma} \in \bar{\Pi} \right\} / \pm \bar{\Pi},$$

and we have $\Gamma = \Gamma^* \cap G(\mathfrak{K}/\mathbf{F}_{p^2}\bar{k})$. Thus, Γ^* *acts, on one hand, on* $\mathfrak{H}$ *as a group of analytic transformations, and on the other hand, on* $\mathfrak{K}$ *as a (dense subgroup of the) Galois group.*

We note here that the *finite extensions* K *of* $\bar{k}$ *in* $\mathfrak{K}$ *and subgroups* Γ_K^* *of* Γ^* *with finite indices correspond in a one-to-one manner.* In fact, each K corresponds to an open subgroup $G_K = G(\mathfrak{K}/K)$ of $G(\mathfrak{K}/\bar{k})$ by the Galois theory, and by the congruence subgroup property of the group $SL_2(\mathbf{Z}^{(p)})$ (proved by Mennicke [23]), G_K and $\Gamma_K^* = G_K \cap \Gamma^*$ correspond in a one-to-one manner. Since Γ^* is dense in $G(\mathfrak{K}/\bar{k})$, K is nothing but the fixed field of Γ_K^* in $\mathfrak{K}$.

(58)
$$\begin{array}{ccc} K & \underset{1:1}{\longleftrightarrow} & \Gamma_K^*; \\ \text{finite extensions} & & \text{subgroups of } \Gamma^* \\ \text{of } \bar{k} \text{ in } \mathfrak{K} & & \text{of finite indices.} \end{array} \quad \left(\begin{array}{c} K\text{: the fixed field of } \Gamma_K^*, \\ \Gamma_K^* = \Gamma^* \cap G(\mathfrak{K}/K). \end{array} \right)$$

A fundamental theorem.

Throughout the following, $\wp$ is a fixed place $M\{k\} \to M\{\bar{k}\}$ satisfying Proposition 6. We shall denote as $\bar{x} = \wp(x)$ (for $x \in M\{k\}$), $= \mathfrak{p}(x)$ (for $x \in \mathbf{Q}^a$).

§17. Let ψ be any place $\psi : M\{k\} \to \mathbf{Q}^a$, which is an identity on $M\{k\} \cap \mathbf{Q}^a = \bigcup_{n \not\equiv 0 \pmod p} \mathbf{Q}(\zeta_n) \underset{\text{put}}{=} \mathbf{Q}'$. We are going to attach to each such ψ, a unique place $\bar{\psi}$: $M\{\bar{k}\} \to \mathbf{F}_p^a$, which is an identity on $\mathbf{F}_p^a$ and for which the following diagram (59) is "almost commutative", i.e., it is commutative on a certain subring Θ_ψ of $M\{k\}$ defined below;

(59)
$$\begin{array}{ccc} M\{k\} & \xrightarrow{\wp} & M\{\bar{k}\} \\ \psi \downarrow & & \downarrow \bar{\psi} \\ \mathbf{Q}^a & \xrightarrow{\mathfrak{p}} & \mathbf{F}_p^a \end{array}$$

namely, we shall prove the following:

PROPOSITION 7. *Let ψ be any place $M\{k\} \rightarrow \mathbf{Q}^{a}$, identity on $M\{k\} \cap \mathbf{Q}^{a} = \bigcup_{n \not\equiv 0 \pmod{p}} \mathbf{Q}(\zeta_n) \underset{(\text{put})}{=} \mathbf{Q}'$. Let $\mathfrak{o}_{\psi}$ be the subring of $\mathbf{Q}'(j)$ given by*

$$(60)\qquad \begin{aligned} \mathfrak{o}_{\psi} &= \left\{ \tfrac{h(j)}{g(j)} \;\middle|\; g(j),\ h(j) \in O'[j],\ \overline{g(\psi(j))} \neq 0 \right\} \cdots \overline{\psi(j)} \neq \infty; \\ &= \left\{ \tfrac{h(j)}{g(j)} \;\middle|\; g(j),\ h(j) \in O'[j],\ \deg \overline{g} = \deg g \geq \deg h \right\} \cdots \overline{\psi(j)} = \infty, \end{aligned}$$

where O' is the ring of $\mathfrak{p}$-integers in $\mathbf{Q}'$. Let Θ_{ψ} be the integral closure of $\mathfrak{o}_{\psi}$ in $M\{k\}$. Then for each ψ, there exists a unique place $\overline{\psi} : M\{\overline{k}\} \rightarrow \mathbf{F}_{p}^{a}$ such that the diagram (59) *is commutative on Θ_{ψ}. Moreover, this $\overline{\psi}$ is an identity on $\mathbf{F}_{p}^{a}$.*

REMARK . The last assertion of Proposition 7 is obvious.

DEFINITION . Put $\widetilde{\mathfrak{H}} = \mathfrak{H} \cup \mathbf{Q} \cup \{i\infty\}$, and let $z \in \widetilde{\mathfrak{H}}$ be such that $j(z)$ is either algebraic or infinite (e.g., if z is a Γ^{*}-fixed point, $j(z)$ is an algebraic integer; if $z \in \mathbf{Q} \cup \{i\infty\}$, $j(z) = \infty$). Then z defines a place $\psi = \psi_z : M\{k\} \rightarrow \mathbf{Q}^{a}$ by the substitution $M\{k\} \ni F(\mathfrak{z}) \mapsto F(z)$ (which is obviously identical on $\mathbf{Q}'$); hence we obtain, by the above proposition, a place $\overline{\psi}_z : M\{\overline{k}\} \rightarrow \mathbf{F}_{p}^{a}$, and hence by its restriction to $\mathfrak{K}$, a place $\mathfrak{K} \rightarrow \mathbf{F}_{p}^{a}$, which we denote by

$$(61)\qquad \mathfrak{P}_z$$

(Thus, the restriction of $\mathfrak{P}_z$ to $\overline{k}$ is given by $\overline{j} \mapsto \overline{j(z)} = j(z) \mod \mathfrak{p}$.)

Now, since Γ^{*} acts on $\mathfrak{K}$, it also acts on the set of all places of $\mathfrak{K}$; namely, for each $\gamma \in \Gamma^{*}$ and a place $\mathfrak{P}$ of $\mathfrak{K}$, define $\gamma\mathfrak{P}$ by

$$(62)\qquad \gamma\mathfrak{P} \underset{\text{def.}}{=} \mathfrak{P} \circ \gamma.$$

Then it is clear that $\gamma'(\gamma\mathfrak{P}) = (\gamma'\gamma)\mathfrak{P}$ holds for all $\gamma, \gamma' \in \Gamma^{*}$, and that in this manner, Γ^{*} also acts on the set of *all equivalence classes of places* of $\mathfrak{K}$. Recall that the two places are called equivalent if they have the same valuation rings; hence if $\mathfrak{P}_1, \mathfrak{P}_2$ are two places $\mathfrak{K} \rightarrow \mathbf{F}_{p}^{a}$, they are equivalent if and only if there is some automorphism σ of $\mathbf{F}_{p}^{a}$ (not of $\mathfrak{K}$) such that $\mathfrak{P}_2 = \sigma \circ \mathfrak{P}_1$. To express the equivalence of two places, we shall use the notation:

$$(63)\qquad \mathfrak{P}_1 \equiv \mathfrak{P}_2 \quad \text{(equivalence of two places)}.$$

Now our fundamental theorem is as follows:

THEOREM 2. *Let $z \in \mathfrak{H}$ be such that $j(z)$ is algebraic and $\mathfrak{p}$-integral. Let $\gamma \in \Gamma^{*}$. Then γz is also such a point of $\mathfrak{H}$, and we have*

$$(64)\qquad \gamma\mathfrak{P}_z \equiv \mathfrak{P}_{\gamma z}.$$

REMARK . (64) is trivial if $\gamma \in PSL_2(\mathbf{Z})$, but highly non-trivial if $\gamma \notin PSL_2(\mathbf{Z})$. In fact, then, it is essentially based on the Kronecker's congruence relation (modernized by Shimura).

§18. Lemmas. To prove Proposition 7, we need the following two lemmas.

LEMMA 1. $\wp \cap \Theta_\psi = p\Theta_\psi$.

LEMMA 2. *Put* $\overline{\Theta}_\psi = \{\overline{b} \mid b \in \Theta_\psi\}$. *Then* $\overline{\Theta}_\psi$ *is the integral closure in* $M\{\overline{k}\}$ *of the valuation ring* $\mathfrak{v}$ ($\subset \mathbf{F}_p^{\mathrm{a}}(\overline{j})$), *attached to the place* $\overline{j} \mapsto \overline{\psi(j)}$ *of* $\mathbf{F}_p^{\mathrm{a}}(\overline{j})$ *which is identical on* $\mathbf{F}_p^{\mathrm{a}}$.

PROOF OF LEMMA 1. Put $\mathfrak{o} = \mathfrak{o}_\psi$, $\Theta = \Theta_\psi$. Then it is clear that $\mathfrak{o}$ and hence also Θ are contained in the valuation ring of $\wp$. Hence the inclusion $p\Theta \subset \wp \cap \Theta$ is obvious. Conversely, let $\xi \in \wp \cap \Theta$. Since $\xi \in \wp$, and p is a prime element of $\wp$, $\eta := p^{-1}\xi$ is $\wp$-integral. But since $\wp$ remains träge in $M\{k\}/\mathbf{Q}'(j)$, η is integral over the valuation ring of $\wp' = \wp \cap \mathbf{Q}'(j)$. Let $\eta^m + a_1\eta^{m-1} + \cdots + a_m = 0$ be the irreducible equation for η over $\mathbf{Q}'(j)$. Then all a_ν belong to the valuation ring of $\wp'$; hence are of the forms $a_\nu = \frac{h_\nu(j)}{g_\nu(j)}$; $g_\nu(j), h_\nu(j) \in O'[j]$, $g_\nu(j) \notin pO'[j]$ (see (50)). But then, the irreducible equation for ξ over $\mathbf{Q}'(j)$ is $\xi^m + pa_1\xi^{m-1} + \cdots + p^m a_m = 0$, and ξ is integral over $\mathfrak{o}$. Therefore, $p^\nu a_\nu \in \mathfrak{o}$ for all ν. Putting these together, we obtain immediately by the definition of $\mathfrak{o} = \mathfrak{o}_\psi$ that $a_\nu \in \mathfrak{o}$ for all ν; hence η is also integral over $\mathfrak{o}$; hence $\eta \in \Theta$; therefore, $\xi \in p\Theta$. Therefore, $p\Theta \supset \wp \cap \Theta$; hence the proof is completed. □

PROOF OF LEMMA 2. Again, put $\mathfrak{o} = \mathfrak{o}_\psi$, $\Theta = \Theta_\psi$. Let $\mathfrak{v}^{\mathrm{i}}$ be the integral closure of $\mathfrak{v}$ in $M\{\overline{k}\}$, and put $\overline{\mathfrak{o}} = \{\overline{b} \mid b \in \mathfrak{o}\}$. Then it is clear that $\overline{\mathfrak{o}} = \mathfrak{v}$; hence it follows immediately that $\overline{\Theta} \subset \mathfrak{v}^{\mathrm{i}}$. Now to prove the converse, let $\overline{\xi} \in \mathfrak{v}^{\mathrm{i}}$, and let $\overline{\xi}^m + \overline{a}_1\overline{\xi}^{m-1} + \cdots + \overline{a}_m = 0$ be the irreducible equation for $\overline{\xi}$ over $\mathbf{F}_p^{\mathrm{a}}(\overline{j})$. Then since $\overline{\xi}$ is integral over $\mathfrak{v}$, all $\overline{a}_\nu$ are contained in $\mathfrak{v}$. Now take any $a_\nu \in \mathfrak{o}$ such that the residue class of a_ν mod $\wp$ coincides with $\overline{a}_\nu$, and consider the equation ($\sharp$) : $X^m + a_1X^{m-1} + \cdots + a_m = 0$. Then since its reduction mod $\mathfrak{p}$ is irreducible, it is irreducible over $\mathfrak{o}$; hence also over $\mathbf{Q}'(j)$. Let ξ be any root of ($\sharp$). Then $\mathbf{Q}'(j,\xi)/\mathbf{Q}'(j)$ is unramified with the residue field $\mathbf{F}_p^{\mathrm{a}}(\overline{j},\overline{\xi})$. But on the other hand, since $M\{k\}/\mathbf{Q}'(j)$ is unramified with the residue field $M\{\overline{k}\} \supset \mathbf{F}_p^{\mathrm{a}}(\overline{j},\overline{\xi})$, there is some intermediate field k' of $M\{k\}/\mathbf{Q}'(j)$ with the residue field $\mathbf{F}_p^{\mathrm{a}}(\overline{j},\overline{\xi})$. Now since unramified extensions are in one-to-one correspondence with the separable extensions of the residue field, we may assume that $\xi \in k'$ and that the residue class of ξ is $\overline{\xi}$. But since $a_\nu \in \mathfrak{o}$ for all ν, ξ is contained in Θ; hence $\overline{\xi} \in \overline{\Theta}$. Therefore, $\mathfrak{v}^{\mathrm{i}} \subset \overline{\Theta}$, which completes the proof. □

§19. Proof of Proposition 7. Put $\psi_\mathfrak{p} = \mathfrak{p} \circ \psi$ (the composite place). Then $\psi_\mathfrak{p}$ is finite on $\mathfrak{o} = \mathfrak{o}_\psi$; hence is also finite on $\Theta = \Theta_\psi$. Then $\psi_\mathfrak{p}$ induces a ring homomorphism $\psi_\mathfrak{p}^0$ of Θ into $\mathbf{F}_p^{\mathrm{a}}$. On the other hand, let $\psi_\wp$ be the place of $M\{k\}$ given by $\wp$. Then $\psi_\wp$ is also finite on Θ, and hence induces a ring homomorphism $\psi_\wp^0$ of Θ into $M\{\overline{k}\}$. Now, by Lemma 1, we have $\operatorname{Ker}\psi_\wp^0 = \Theta \cap \wp = p\Theta$, and hence

$$\operatorname{Ker}\psi_\wp^0 \subset \operatorname{Ker}\psi_\mathfrak{p}^0. \tag{65}$$

Therefore, there is a unique homomorphism $\overline{\psi}^0$ of $\overline{\Theta} = \psi_\wp^0(\Theta)$ into $\mathbf{F}_p^{\mathrm{a}}$ such that $\overline{\psi}^0 \circ \psi_\wp^0 = \psi_\mathfrak{p}^0$. Extend this ring homomorphism $\overline{\psi}^0$ of $\overline{\Theta}$ to a place $\overline{\psi}$ of $M\{\overline{k}\}$. Then by its definition, it is clear that $\overline{\psi}$ satisfies the condition of Proposition 7; hence the existence.

To prove the uniqueness, let χ be any place of $M\{\bar{k}\}$ satisfying the condition of Proposition 7. It is obvious that χ must coincide with $\bar{\psi}$ on $\bar{\Theta}$. But by Lemma 2, $\bar{\Theta}$ is the integral closure of the valuation ring $\mathfrak{v}$ of $\mathbf{F}_p^a(\bar{j})$ attached to the place $\bar{j} \to \overline{\psi(j)}$ (identical on $\mathbf{F}_p^a$) of $\mathbf{F}_p^a(\bar{j})$, and this place is nothing but the restriction of χ and $\bar{\psi}$ to $\mathbf{F}_p^a(\bar{j})$. Therefore, χ and $\bar{\psi}$ must be equivalent, i.e., they must be equal up to an automorphism of $\mathbf{F}_p^a$. But since χ and $\bar{\psi}$ must be identical on $\mathbf{F}_p^a$ (as follows immediately), we have $\chi = \bar{\psi}$, which proves the uniqueness. □

§20. A lemma for the proof of Theorem 2. Consider the subring $O'[j, j^{-1}, (j - 12^3)^{-1}]$ of $\mathbf{Q}'(j)$. It is easy to see that this ring is nothing but the intersection of the valuation rings O_v of v, where v runs over all discrete valuations of $\mathbf{Q}'(j)$ such that $v(j) = v(j - 12^3) = v(b) = 0$ for all p-units $b \in \mathbf{Q}'$. In particular, $v(n) = 0$ for all $n \not\equiv 0 \pmod p$ for such v. But by §12 and Proposition 4, $x_{\alpha\beta}$ are $\tilde{v}$-finite for any extensions $\tilde{v}$ of such v; hence all $x_{\alpha\beta}$ are integral over O_v; hence the elementary symmetric functions of all conjugates of $x_{\alpha\beta}$ over $\mathbf{Q}'(j)$ are contained in $\bigcap_v O_v = O'[j, j^{-1}, (j - 12^3)^{-1}]$; hence

(66) $\qquad x_{\alpha\beta}$ are integral over $O'[j, j^{-1}, (j - 12^3)^{-1}]$ for all $(\alpha, \beta) \neq (0, 0)$.

Actually, we can prove more; namely,

LEMMA 3. *$x_{\alpha\beta}$ are integral over $O'[(j - 12^3)^{-1}]$.*

PROOF. With (66) on hand, it is enough to prove the existence of two places ψ_ω, $\psi_{i\infty}$ of $M\{k\}$ such that $\psi_\omega(j) = 0$, $\psi_{i\infty}(j) = \infty$, and that $\psi_\omega(x_{\alpha\beta})$, $\psi_{i\infty}(x_{\alpha\beta})$ are finite for all α, β. Define ψ_ω by $M(k) \ni F(\mathfrak{z}) \mapsto F(\omega)$, $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. Then $\psi_\omega(j) = j(\omega) = 0$, $g_2(\omega) = 0$; hence $x'_{\alpha\beta}(\omega) = 0$; hence $\psi_\omega(x_{\alpha\beta}) = x_{\alpha\beta}(\omega) = -\frac{1}{12}$ for all α, β. On the other hand, define $\psi_{i\infty}$ by $M(k) \ni F(\mathfrak{z}) \mapsto F(i\infty)$. Then $\psi_{i\infty}(j) = j(i\infty) = \infty$, $g_2(i\infty) = \frac{\pi^4}{12}$, $g_3(i\infty) = \frac{\pi^6}{216}$, $\lim_{z\to i\infty} \wp(\alpha z + \beta | z, 1) = -\frac{\pi^2}{12}$ $(\alpha \neq 0)$, $= \left(\frac{\pi}{2}\right)^2 \left\{\frac{1}{\sin^2(\pi\beta)} - \frac{1}{3}\right\}$ $(\alpha = 0, \beta \neq 0)$. Hence

$$\psi_{i\infty}(x_{\alpha\beta}) = \begin{cases} 0 & \cdots \alpha \neq 0, \\ -\frac{1}{(2\sin\pi\beta)^2} & \cdots \alpha = 0, \beta \neq 0. \end{cases} \tag{67}$$

Since $\psi_\omega(x_{\alpha\beta})$, $\psi_{i\infty}(x_{\alpha\beta})$ are all finite, we obtain our lemma. □

REMARK. Note that we have actually proved that for $\alpha, \beta \in \mathbf{Z}/n\mathbf{Z}$, $(\alpha, \beta) \neq (0, 0)$,

(68) $\qquad x_{\alpha\beta}$ are integral over $\mathbf{Z}[n^{-1}, (j - 12^3)^{-1}]$.

COROLLARY. *In the situation of Proposition 7, if $\psi(j) \not\equiv 12^3 \pmod{\mathfrak{p}}$, then all $x_{\alpha\beta}$ are contained in Θ_ψ.*

§21. Proof of Theorem 2. First, we note the following. As noted in §15, the Galois group $\bar{G}$ can be considered as a subgroup of G in a natural manner, and hence the (dense) subgroup:

$$\tilde{\Gamma}^* = \{\gamma \in GL_2(\mathbf{Z}^{(p)}) \mid \det\gamma \in \Pi\}/\pm 1 \tag{69}$$

of $\overline{G}$ acts both on $M\{k\}$ and on $M\{\overline{k}\}$ in a natural manner. Namely, $\gamma \in \widetilde{\Gamma}^*$ acts as $\gamma x_{\alpha\beta} = x_{(\alpha\beta)\gamma}$ (on $M\{k\}$), $\gamma\overline{x}_{\alpha\beta} = \overline{x}_{(\alpha\beta)\gamma}$ (on $M\{\overline{k}\}$). On the other hand, if γ is moreover contained in the subgroup $PSL_2(\mathbf{Z})$ of $\widetilde{\Gamma}^*$, then γ acts on $M\{k\}$ in another way; namely, as $\gamma : M\{k\} \ni F(\mathfrak{z}) \mapsto F(\gamma\mathfrak{z}) \in M\{k\}$. But by the definition of $x_{\alpha\beta} = x_{\alpha\beta}(\mathfrak{z})$, it follows immediately that $x_{(\alpha\beta)\gamma}(\mathfrak{z}) = x_{\alpha\beta}(\gamma\mathfrak{z})$ for all (α, β) and all $\gamma \in PSL_2(\mathbf{Z})$; hence the above two ways of actions of $PSL_2(\mathbf{Z})$ on $M\{k\}$ are the same. Now, (64) *for* $\gamma \in PSL_2(\mathbf{Z})$ is a trivial consequence of this (in fact, we have the equality $\gamma \cdot \mathfrak{P}_z = \mathfrak{P}_{\gamma z}$ instead of the equivalence $\equiv$ for such a γ, and the "restriction to $\mathfrak{K}$" is not essential here).

For the general case, i.e., for $\gamma \in \Gamma^*$ with $\gamma \notin PSL_2(\mathbf{Z})$, this argument does not apply. (For such γ, (64) is the strongest result; $\equiv$ cannot be replaced by $=$, and the restriction to $\mathfrak{K}$ is essential.) But since it is enough to prove (64) for the generators of Γ^*, it is enough to prove it for one element $\gamma \in \Gamma^*$ of the form $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbf{Z}$, $ad - bc = p$. Sometimes, this element $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ will be considered as an element of $\widetilde{\Gamma}^*$.

(I) The case $j(z) \not\equiv 0, 12^3 \pmod{\mathfrak{p}}$. For the sake of later necessity, let us only assume $ad - bc = p^n$ ($n \geq 1$), and put $z' = \gamma z$, $j_0 = j(z)$, $j_0' = j(z')$. Let $E = E_{j_0}$ be identified with the complex torus $\mathbf{C}/[z, 1]$ by the elliptic functions $x(u, z), y(u, z)$ (see (36)). Thus, for each $n \not\equiv 0 \pmod{p}$, $\alpha z + \beta \leftrightarrow (\alpha, \beta)$ gives an "n-adic" coordinate system on E, and the x-coordinate of $\alpha z + \beta$ is nothing but $x_{\alpha\beta}(z)$. Define $E' = E_{j_0'} \cong \mathbf{C}/[z', 1]$ and its coordinate system in the same manner. Then, there is an isogeny $\varphi : E' \to E$ which transforms the n-adic coordinates as $(\alpha', \beta') \mapsto (\alpha'\beta')\gamma$; in fact, the linear map $u \mapsto (cz + d)u$ of $\mathbf{C}$ induces such φ.

Now j_0 is an algebraic integer with $j_0 \not\equiv 0, 12^3 \pmod{\mathfrak{p}}$ by assumption; hence as is well-known, its p-power transform j_0' has the same properties. Hence, E, E' and $\varphi \in \mathrm{Hom}(E', E)$ have good reductions $\overline{E}, \overline{E}', \overline{\varphi}$. Now let $n = 1$. Then since $\nu(\overline{\varphi}) = \nu(\varphi) = p$, we have either $\nu_s(\overline{\varphi}) = 1$ or $= p$. In the first case, we have $\overline{j}_0 = \overline{j}_0'^{\,p}$, $\overline{E} = \overline{E}'^{\,p}$, and $\overline{\varphi}\,\overline{u}' = \pm\overline{u}'^{\,p}$ for all $\overline{u}' \in \overline{E}'$; whereas in the second case, we have $\overline{j}_0 = \overline{j}_0'^{\,1/p}$, $\overline{E} = \overline{E}'^{\,1/p}$, and $\overline{\varphi}\,\overline{u}' = \pm(p\overline{u}')^{1/p}$ (The Kronecker's congruence relation modernized by Shimura; see **[30]** §3). Moreover, if the n-adic coordinates of $\overline{E}, \overline{E}'$ are taken to be the reductions mod $\mathfrak{p}$ of those of E, E', then $\overline{\varphi}$ induces the same transformation of n-adic coordinates as φ; hence $\overline{\varphi}$ induces $(\alpha', \beta') \mapsto (\alpha'\beta')\gamma$. Therefore, by looking at the $\overline{x}$-coordinates of n-th division points (which are finite by §12), and denoting always by $^{-}$ the residue classes mod $\mathfrak{p}$, we obtain

$$(70) \qquad \begin{aligned} \overline{x_{(\alpha'\beta')\gamma}(z)} &= \overline{x_{\alpha'\beta'}(\gamma z)}^{\,p} \quad \text{(the first case)}, \\ &= \overline{x_{p(\alpha'\beta')}(\gamma z)}^{\,1/p} \quad \text{(the second case)}. \end{aligned}$$

Now the rest follows almost formally. In fact, let ψ_z be the place of $M\{k\}$ defined by $F(\mathfrak{z}) \mapsto F(z)$. Then since $\overline{j(z)} \neq 0, 12^3$, all $x_{\alpha\beta}$ are contained in Θ_{ψ_z} (Corollary of Lemma 3). Hence $\overline{\psi}_z(\overline{x}_{\alpha\beta}) = \overline{x_{\alpha\beta}(z)}$ for all $(\alpha, \beta) \neq (0, 0)$. Therefore, $\overline{\psi}_{\gamma z}(\overline{x}_{\alpha\beta}) = \overline{x_{\alpha\beta}(\gamma z)}$, and $(\overline{\psi}_z \circ \gamma)(\overline{x}_{\alpha\beta}) = \overline{x_{(\alpha\beta)\gamma}(z)}$. Now let ρ be the Frobenius automorphism $b \mapsto b^p$ of $\mathbf{F}_p^{\mathrm{a}}$. In the first case of (70), put $\chi_1 = \rho^{-1} \circ \psi_z \circ \gamma$, $\chi_2 = \overline{\psi}_{\gamma z}$. Then by (70) and by $\overline{j}_0 = \overline{j}_0'^{\,p}$, we have $\chi_1(\bar{j}) = \chi_2(\bar{j})$ and $\chi_1(\bar{x}_{\alpha\beta}) = \chi_2(\bar{x}_{\alpha\beta})$ for all $(\alpha,\beta) \neq (0,0)$. Moreover, since the restriction of γ to $\mathbf{F}_p^a$ coincides with ρ (because $ad-bc = p$), χ_1 and χ_2 are identities on $\mathbf{F}_p^a$. Since χ_1, χ_2 coincide on $\mathbf{F}_p^a(\bar{j})$, there is an automorphism $\bar{\sigma}$ of $M\{\bar{k}\}$ over $\mathbf{F}_p^a(\bar{j})$ such that $\chi_1 = \chi_2 \circ \bar{\sigma}$. But then, $\overline{x_{(\alpha\beta)\bar{\sigma}}(\gamma z)} = \overline{x_{\alpha\beta}(\gamma z)}$ for all α, β; which, by §12, implies $\bar{\sigma} = 1$ (as an automorphism). Therefore, $\chi_1 = \chi_2$; i.e., $\rho \circ \bar{\psi}_{\gamma z} = \bar{\psi}_z \circ \gamma$; hence $\gamma \cdot \mathfrak{P}_z = \rho \circ \mathfrak{P}_{\gamma z} \equiv \mathfrak{P}_{\gamma z}$. In the second case of (70), we obtain, in the same manner, the equality $\rho^{-1} \circ \bar{\psi}_{\gamma z} = \bar{\psi}_z \circ (p^{-1}\gamma)$; hence by the restriction to $\mathfrak{K}$ (and now by considering γ as an element of Γ^* instead of $\widetilde{\Gamma}^*$), we obtain $\gamma \cdot \mathfrak{P}_z = \rho^{-1} \circ \mathfrak{P}_{\gamma z} \equiv \mathfrak{P}_{\gamma z}$. This settles the proof of the case $j(z) \not\equiv 0, 12^3$ (mod $\mathfrak{p}$).

(II) The case $j(z) \equiv 12^3$ (mod $\mathfrak{p}$)[16]; $p \neq 2$. Let $x'(u,\mathfrak{z})$, $y'(u,\mathfrak{z})$, and $x'_{\alpha\beta} = x'_{\alpha\beta}(\mathfrak{z})$ be as in §14, and put $e_1 = x'_{0,1/2}$, $e_2 = x'_{1/2,1/2}$, $e_3 = x'_{1/2,0}$; $\lambda = \frac{e_1-e_2}{e_3-e_2}$. Then we have $k_2 = k(\lambda)$, $j = 2^8 \frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}$ (as well-known)[17], and e_i $(i = 1,2,3)$ are contained in k_2. Let E^*_λ be the elliptic curve

$$\eta^2 = \xi(\xi-1)(\xi-\lambda), \tag{71}$$

with the neutral element $(\xi,\eta) = (\infty,\infty)$. Then E^*_λ is defined over k_2, and its absolute invariant is j. In general, (71) is an elliptic curve as long as $\lambda \neq 0, 1, \infty$ and the characteristic is not 2. Therefore, if v is any discrete valuation of k_2 such that $v(2) = v(\lambda) = v(\lambda-1) = 0$, then we obtain an elliptic curve $E^*_{\bar{\lambda}}$ by passing to the residue class (which is a good reduction of E^*_λ). Put

$$\begin{aligned} \xi(u;\mathfrak{z}) &= \frac{x'(u;\mathfrak{z}) - e_2(\mathfrak{z})}{e_3(\mathfrak{z}) - e_2(\mathfrak{z})}, \\ \eta(u;\mathfrak{z}) &= \frac{1}{2}\frac{y'(u;\mathfrak{z})}{(e_3(\mathfrak{z}) - e_2(\mathfrak{z}))^{3/2}}; \end{aligned} \tag{72}$$

and for each α,β, put $\xi_{\alpha\beta} = \xi_{\alpha\beta}(\mathfrak{z}) = \xi(\alpha\mathfrak{z}+\beta;\mathfrak{z}) = \frac{x'_{\alpha\beta}-e_2}{e_3-e_2}$. (In particular, $\xi_{0,1/2} = \lambda$, $\xi_{1/2,1/2} = 0$, $\xi_{1/2,0} = 1$.) Then, $(\xi(u;\mathfrak{z}), \eta(u;\mathfrak{z}))$ satisfies (71) for any $u \in \mathbf{C}$; hence for each $z \in \mathfrak{H}$, $E^*_{\lambda(z)}$ is naturally identified with the complex torus $\mathbf{C}/[z,1]$ by $(\xi,\eta) = (\xi(u;\mathfrak{z}), \eta(u;\mathfrak{z})) \Leftrightarrow u$, and $\xi_{\alpha\beta}(z)$ is nothing but the ξ-coordinate of the point $\alpha z + \beta$.

Now the proof goes parallel to the cases of $j(z) \not\equiv 0, 12^3$ (mod $\mathfrak{p}$) by using E^*_λ instead of E_j. The following are the points to be specifically noted here.

(i) Instead of Lemma 3, we have:

$$\xi_{\alpha\beta} \textit{ are integral over } \mathcal{O}'[j]. \tag{73}$$

In fact, by the argument parallel to that of §20, we see that $\xi_{\alpha\beta}$ are integral over $\mathcal{O}'[\lambda, \lambda^{-1}, (\lambda-1)^{-1}]$ (since 2 is a $\mathfrak{p}$-unit, by $p \neq 2$). But $\lambda, \lambda^{-1}, (\lambda-1)^{-1}$ are integral

[16] Actually, this proof (of II) also covers all cases of I for $p \neq 2$, and III also covers all cases of I for $p \neq 3$. In this sense, (I) is unnecessary. However, (I) deals with the typical cases for all characteristics, and the proof requires no specific technical cares. So we preferred to give (I) with a full proof, and to give (II), (III) with only remarks on what should be added and what specific cares should be taken.

[17] In particular, by the substitution of special values, we have the following correspondences: $j = \infty \Leftrightarrow \lambda = 0, 1, \infty$; $j = 12^3 \Leftrightarrow \lambda = 1/2, 2, -1$; $j = 0 \Leftrightarrow \lambda = -\omega, -\omega^2$; where $\omega = \frac{1}{2}(-1 \pm \sqrt{-3})$.

over $\mathcal{O}'[\mathfrak{z}]$ as can be seen directly from the equation $(1-\lambda+\lambda^2)^3 - 2^8 j\lambda^2(1-\lambda)^2 = 0$; hence (73).

(ii) Since it is enough to prove (64) for one generator γ of Γ^* over $PSL_2(\mathbf{Z})$, we may put $\gamma = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. But then, $\gamma \equiv 1 \pmod 2$; hence γ acts trivially on k_2; hence leaves e_2, e_3 invariant; hence we have

$$\gamma\xi_{\alpha\beta} = \gamma\left(\frac{x'_{\alpha\beta} - e_2}{e_3 - e_2}\right) = \frac{\gamma x'_{\alpha\beta} - e_2}{e_3 - e_2} = \xi_{(\alpha\beta)\gamma}.$$

(iii) Here, the automorphisms of $\overline{E}^* = E^*_{\overline{\lambda(z)}}$ are not necessarily $\{\pm 1\}$. Hence we only have

$$\text{(74)}\qquad \begin{aligned} &\overline{\lambda}_0 = \overline{\lambda}_0'^{\,p},\ \overline{E}^* = \overline{E}^{*\prime p},\ \overline{\varphi}\,\overline{u}' = \varepsilon\overline{u}'^{\,p}, \cdots \text{the case } \nu_s(\overline{\varphi}) = 1,\\ &\overline{\lambda}_0 = \overline{\lambda}'_0{}^{1/p},\ \overline{E}^* = \overline{E}^{*\prime 1/p},\ \overline{\varphi}\,\overline{u}' = \varepsilon(p\overline{u}')^{1/p}, \cdots \text{the case } \nu_s(\overline{\varphi}) = p,\end{aligned}$$

with the corresponding notations and with some automorphism ε of $\overline{E}^*$. However, $\overline{\lambda}_0 = 1/2$ or 2 or -1 by assumption (since $\overline{j}_0 = 12^3$), and $\overline{\lambda}'_0 = \overline{\lambda}_0^{\,p^{\pm 1}}$; hence $\overline{\lambda}'_0 = \overline{\lambda}_0$. On the other hand, if $(\alpha,\beta) = (0,1/2), (1/2,1/2)$, or $(1/2,0)$, then $\overline{\xi_{\alpha\beta}(z)} = \overline{\lambda}_0, 0$, or 1, and $\overline{\xi_{\alpha\beta}(\gamma z)} = \overline{\lambda}'_0, 0$, or 1 respectively; hence $\overline{\xi_{\alpha\beta}(z)} = \overline{\xi_{\alpha\beta}(\gamma z)} \in \mathbf{F}_p$. But by $\gamma \equiv 1 \pmod 2$, we have $(\alpha,\beta)\gamma = (\alpha,\beta)$ for such α,β. Hence we have $\overline{\xi_{(\alpha\beta)\gamma}(z)} = \overline{\xi_{\alpha\beta}(\gamma z)}^{\,p} = \overline{\xi_{\alpha\beta}(\gamma z)}^{\,1/p}$; hence by applying (74) for the second division points $\overline{u}'$ of $\overline{E}^{*\prime}$, we see that ε leaves all such division points invariant; hence by Proposition 1 (ii), we conclude $\varepsilon = \pm 1$.

(III) The case $j(z) \equiv 0 \pmod{\mathfrak{p}}$[18]**;** $p \neq 3$**.** As in the Examples in §13, let μ be any root of

$$\text{(75)}\qquad j = \left\{\frac{3\mu(\mu^3 + 2^3)}{\mu^3 - 1}\right\}^3,$$

so that $\mu \in k_3$, and $k_3 = k(\mu, \omega)$ where $\omega = \frac{1}{2}(-1 + \sqrt{-3})$. Put $k'_3 = k(\mu)$, and let E^*_μ be an elliptic curve over k'_3 given by the projective coordinates as

$$\text{(76)}\qquad X^3 + Y^3 + Z^3 = 3\mu XYZ \quad \text{(cf. Igusa [14])},$$

with the neutral element $(X, Y, Z) = (-1, 1, 0)$. Then E^*_μ has the absolute invariant j, and in general, (76) is an elliptic curve as long as $\mu^3 \neq 1$ and the characteristic is not 3. Therefore, if v is any discrete valuation of k'_3 with $v(3) = v(\mu^3 - 1) = 0$, then we obtain an elliptic curve $E^*_{\overline{\mu}}$ over the residue field by a good reduction of E^*_μ. Now put $\xi = \frac{Z}{X+Y+\mu Z}$. Then ξ is of order two on E^*_μ (as a rational function), and $\xi = \infty$ only at its origin. Since E^*_μ and E_j are defined over k'_3 and $E^*_\mu \cong E_j$, we can identify the two fields $k'_3(\xi)$ $(= k'_3(E^*_\mu)^0)$ (with the notations of §11) and $k'_3(x)$ $(= k'_3(E_j)^0)$, x being the function on E_j giving the x-coordinate (see the argument in the proof of Proposition 2, noting that j, μ are transcendental over $\mathbf{Q}$, and hence that E^*_μ, E_j have no automorphisms other than ± 1). Hence ξ can be considered as a rational (and moreover linear) function $f(x)$ of x over k'_3. Put $\xi(u;\mathfrak{z}) = f(x(u;\mathfrak{z}))$, $\xi_{\alpha\beta}(\mathfrak{z}) = \xi(\alpha\mathfrak{z} + \beta;\mathfrak{z})$. Then for each $z \in \mathfrak{H}$, $E^*_{\mu(z)}$ can be naturally identified with the

[18] See the footnote given w.r.t. (the beginning of) (II). Note that $12^3 \equiv 0 \pmod{\mathfrak{p}}$ for $p = 2, 3$; hence (I) (II) (III) cover all cases.

complex torus $\mathbf{C}/[z,1]$ (up to $\pm$) by $\xi(u;z) \leftrightarrow u$, and $\xi_{\alpha\beta}(z)$ is the ξ-coordinate of the point $\alpha z+\beta$. Now the proof will be completed if we look at the proof in (I), remarks in (II), and if we further note the following:

(i) $\xi_{\alpha\beta}$ are integral over $\mathcal{O}'[j]$; (this can be proved in the same manner as in (II)).

(ii) Take $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ as γ. Then there exists a solution μ of (75) that is invariant by γ. (In fact, for each solution μ of (75), the automorphism $\rho \neq 1$ of $k_3/k(\mu)$ is of order two and satisfies $\det\rho = -1$. Moreover, the involutions $\rho \in G(k_3/k) \cong GL_2(\mathbf{Z}/3\mathbf{Z})$ with $\det\rho = -1$ are all conjugate with each other. Hence each such involution ρ fixes some solution μ. Hence if $p \equiv -1 \pmod 3$, there exists some μ which is invariant by $\gamma \equiv \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 3$. If, on the other hand, $p \equiv 1 \pmod 3$, γ acts trivially on k_3; hence there is no problem.) Take such μ. Then by the relation between ξ and x, we conclude $\gamma\xi_{\alpha\beta} = \xi_{(\alpha\beta)\gamma}$.

(iii) In Igusa [14], p.456, the (X, Y, Z) coordinates of third division points of E_μ^* are given. From this, we obtain the values of $\xi_{\alpha\beta}$ for the third division points; they are 0, $\frac{1}{\mu-1}, \frac{1}{\mu-\omega}, \frac{1}{\mu-\omega^2}$. Among them, the first two are invariant by γ, and the latter two are not. Hence the first two are the values of $\xi_{0,1/3}, \xi_{1/3,0}$, and the latter two are of $\xi_{1/3,1/3}$, $\xi_{1/3,-1/3}$. On the other hand, the values of μ for $j = 0$ are $\mu = 0, -2, -2\omega, -2\omega^2$ by (75). These, together with Proposition 1 (iii), give all the necessary tools for the proof that a certain automorphism of $E_{\bar{\mu}_0}^*$ must be ± 1 (see (II) (iii)).

Decomposition of ordinary prime divisors of $\bar{k}$ in $\mathfrak{K}$.

§22. Prime divisors of $\bar{k}$. Let $\mathfrak{P}^0$ be a prime divisor, i.e., an equivalence class of non-trivial places, of $\bar{k} = \mathbf{F}_p(\bar{j})$. Then $\mathfrak{P}^0$ is determined by $\mathfrak{P}^0(\bar{j})$ (the residue class of $\bar{j}$ mod $\mathfrak{P}^0$), and by this, the set of all $\mathfrak{P}^0$ is in one-to-one correspondence with $\mathbf{F}_p^{\mathrm{a}}/\sim \cup\{\infty\}$. Here, $\sim$ denotes the conjugacy of elements of $\mathbf{F}_p^{\mathrm{a}}$ over $\mathbf{F}_p$. We shall call

(77)
$\mathfrak{P}^0$: *infinite,* if $\mathfrak{P}^0(\bar{j}) = \infty$;
: *supersingular,* if $\mathfrak{P}^0(\bar{j})$ is supersingular;
: *ordinary,* if otherwise.

(See §4 for the definition of supersingularity of elements of $\mathbf{F}_p^{\mathrm{a}}$). Recall that the set of all supersingular elements of $\mathbf{F}_p^{\mathrm{a}}$ is finite, contained in $\mathbf{F}_{p^2}$, and is self-conjugate over $\mathbf{F}_p$.

Now we are going to determine the law of decomposition of $\mathfrak{P}^0$ in $\mathfrak{K}/\bar{k}$. First, we shall deal with the case where $\mathfrak{P}^0$ is an ordinary prime divisor. This is the case where our fundamental theorems (Theorems 1, 2) are directly applied. Roughly speaking, such $\mathfrak{P}^0$ has an extension (to $\mathfrak{K}$) of the form $\mathfrak{P}_z$ ($z \in \mathfrak{H}$; see §17), and the decomposition group of $\mathfrak{P}_z$ (in $\mathfrak{K}/\bar{k}$) is the topological closure (in $G(\mathfrak{K}/\bar{k})$) of the stabilizer Γ_z^* of z in Γ^*. Moreover, the Frobenius automorphism of $\mathfrak{P}_z$ is given by the "positive generator" of Γ_z^*. Thus, our first task is to define the positive generator of Γ_z^*.

§23. Positive elements of Γ_z^*. Let z be a Γ^*-fixed point and let Γ_z^* be its stabilizer, so that by the definition of Γ^*-fixed point, Γ_z^* is infinite. Let $\gamma \in \Gamma_z^*$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z})$; $(a, b, c, d) = 1$. Put $D = \operatorname{Deg}\gamma$ (see §3). Let Ω be the imaginary quadratic field generated by z (so, $\left(\frac{\Omega}{p}\right) = 1$; see §3), and let O_f be the order of the lattice $[z, 1]$; f being the conductor. Put $f = f_0p^k$ with $f_0 \not\equiv 0 \pmod p$, and $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z \\ 1 \end{pmatrix} = \pi\begin{pmatrix} z \\ 1 \end{pmatrix}$, so that $\pi = cz + d \in O_f$, $\pi \notin pO_f$. Let O_1 be the maximal order of Ω.

Lemma 4. *We have $\pi O_1 = p^k\mathfrak{p}_1^D$ with a prime factor $\mathfrak{p}_1$ of p in Ω, where k and D are as above.*

Proof. Put $\pi O_1 = p^{k'}\mathfrak{p}_1^{D'}$ $(k', D' \geq 0)$, and $\pi_0 = \pi p^{-k'}$. Then $\pi_0 \in O_{f_0}$, but $\pi_0 \notin O_{pf_0}$. (In fact, if $D' > 0$, i.e., $\pi_0 \equiv 0 \pmod{\mathfrak{p}_1}$, then $\pi_0 \in O_{pf_0}$ would imply a contradiction $\pi_0 \in pO_1$; and if $D' = 0$, then π_0 is a root of unity and hence $[1, \pi_0] = O_1$; hence $\pi_0 \notin O_{pf_0}$). Therefore, $\pi \in O_{f_0p^{k'}}$ but $\notin O_{f_0p^{k'+1}}$; hence $k' \geq k$. On the other hand, $\pi \notin pO_f$; hence $\pi \notin p^{k+1}O_{f_0}$; hence $k' = k$. That $D' = D$ follows immediately from the definition of $\operatorname{Deg}\gamma$. □

In particular, if we put $ad - bc = p^n$, then $n = D + 2k$.

Definition . With respect to a fixed prime divisor $\mathfrak{p}$ of p in $\mathbf{Q}^a$, we shall call $\gamma \in \Gamma_z^*$ (with $\operatorname{Deg}\gamma > 0$) *positive* if $\mathfrak{p}_1$ coincides with the restriction of $\mathfrak{p}$ to Ω.

By the definition of positivity and by §3, there exists an injective homomorphism φ of Γ_z^* into $\mathbf{Q}_p^\times$, sending each $\gamma \in \Gamma_z^*$ to a ratio of the eigenvalues of γ_p, such that γ is positive if and only if $\operatorname{ord}_p \varphi(\gamma) > 0$. Let $E = E_z^*$ be the torsion subgroup of Γ_z^*. An element $\gamma_0 \in \Gamma_z^*$ will be called *a positive generator of* Γ_z^* mod E, if γ_0 is positive and generates Γ_z^* mod E. Thus, if γ_0 is such an element, elements γ of Γ_z^* are expressed uniquely in the form $\gamma = \varepsilon\gamma_0^m$ with $\varepsilon \in E$, $m \in \mathbf{Z}$. It is clear then that $\operatorname{Deg}\gamma = |m|D$, and that γ is positive if and only if $m > 0$. Thus, γ is a positive generator of Γ_z^* mod E if and only if $m = 1$. It is also clear that if γ is positive and $\delta \in \Gamma^*$, then $\delta^{-1}\gamma\delta$ $(\in \Gamma^*_{\delta^{-1}z})$ is also positive. Hence we may speak of positive elliptic Γ^*-conjugacy classes (w.r.t. $\mathfrak{p}$, of course).

§24.

Theorem 3. *Let z be a Γ^*-fixed point, let Γ_z^* be its stabilizer in Γ^*, and let E_z^* be the torsion subgroup of Γ_z^*. Let γ be a positive generator of Γ_z^* mod E_z^*. Then,*

(i) *the decomposition group of $\mathfrak{P}_z$ in $\mathfrak{K}/\bar{k}$ is the topological closure of Γ_z^* in $G(\mathfrak{K}/\bar{k})$;*
(ii) *the inertia group of $\mathfrak{P}_z$ in $\mathfrak{K}/\bar{k}$ is E_z^*;*
(iii) *the Frobenius substitution is given by γ.*

Before proving this, we shall give some of its direct corollaries.

Corollary 1. *Let z, z' be Γ^*-fixed points. Then $\mathfrak{P}_{z'} \equiv \mathfrak{P}_z$ if and only if $z' = z$.*

Proof (of Corollary 1). Let $z' \neq z$. If they are not Γ^*-conjugate with each other, then by Theorem 1 (§5), $\overline{j(z')}$ and $\overline{j(z)}$ are not conjugate over $\mathbf{F}_p$; hence the restrictions to $\bar{k}$ of $\mathfrak{P}_z$ and $\mathfrak{P}_{z'}$ are already distinct. On the other hand, if $z' = \delta z \neq z$ with some $\delta \in \Gamma^*$, then δ does not centralize Γ_z^*; hence δ is not contained in the topological closure of Γ_z^* in $G(\mathfrak{K}/\bar{k})$; hence by Theorem 3 (i), $\delta\mathfrak{P}_z \not\equiv \mathfrak{P}_z$; but by Theorem 2, $\mathfrak{P}_{\delta z} \equiv \delta\mathfrak{P}_z$; hence $\mathfrak{P}_{\delta z} \not\equiv \mathfrak{P}_z$. □

Let

$$\wp(\bar{k}) \tag{78}$$

be the set of all ordinary prime divisors of $\bar{k}$, and for each finite extension K of $\bar{k}$ contained in $\mathfrak{K}$, let

$$\wp(K) \tag{79}$$

be the set of all prime divisors of K which lie above $\wp(\bar{k})$. Let Γ_K^* be the subgroup of Γ^* corresponding to K (see §16). Then we have:

Corollary 2. *Let z, z' be Γ^*-fixed points. Then the restrictions $\mathfrak{P}_z|_K$, $\mathfrak{P}_{z'}|_K$ are contained in $\wp(K)$, and they are equal*[19] *if and only if z, z' are Γ_K^*-equivalent.*

Proof. $\mathfrak{P}_z$ sends $\bar{j}$ to $\overline{j(z)}$, and $\overline{j(z)}$ is finite and not supersingular by Theorem 1; hence $\mathfrak{P}_z|_K$, etc. are contained in $\wp(K)$. Moreover, by Theorem 1, our statement is true for $K = \bar{k}$. Now suppose that z, z' are Γ_K^*-equivalent, and put $z' = \gamma z$ ($\gamma \in \Gamma_K^*$). Then by Theorem 2, $\mathfrak{P}_{z'} \equiv \gamma \cdot \mathfrak{P}_z$; hence $\mathfrak{P}_{z'}|_K \equiv \mathfrak{P}_z|_K$. Conversely, if $\mathfrak{P}_{z'}|_K \equiv \mathfrak{P}_z|_K$, then a priori $\mathfrak{P}_{z'}|_{\bar{k}} \equiv \mathfrak{P}_z|_{\bar{k}}$; hence $z' = \gamma z$ with some $\gamma \in \Gamma^*$. But then, $\gamma\mathfrak{P}_z|_K \equiv \mathfrak{P}_z|_K$; hence $\gamma \in G(\mathfrak{K}/K)X$, where X is the decomposition group of $\mathfrak{P}_z$. But by Theorem 3, X is the topological closure of Γ_z^* in $G(\mathfrak{K}/\bar{k})$; hence $\gamma \in G(\mathfrak{K}/K)\Gamma_z^*$. Put $\gamma = \gamma'\gamma_1$, with $\gamma_1 \in \Gamma_z^*$, $\gamma' \in G(\mathfrak{K}/K) \cap \Gamma^* = \Gamma_K^*$. Then $z' = \gamma z = \gamma' z$; hence z' and z are Γ_K^*-equivalent. □

As in Part 1, let $\wp(\Gamma_K^*)$ be the set of Γ_K^*-equivalence classes of all Γ^*-fixed points (or equivalently, Γ_K^*-fixed points). Then by Corollary 2, $z \mapsto \mathfrak{P}_z|_K$ gives a one-to-one correspondence $\mathcal{J}_K : \wp(\Gamma_K^*) \to \wp(K)$, and by the definition of $\mathcal{J}_K$, the diagram

$$\begin{array}{ccccccc} \wp(\Gamma_K^*) & \ni & \{z\}_{\Gamma_K^*} & \xrightarrow{\mathcal{J}_K} & \mathfrak{P}_z|_K & \in & \wp(K) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \wp(\Gamma^*) & \ni & \{z\}_{\Gamma^*} & \xrightarrow{\mathcal{J}^*} & \mathfrak{P}_z|_{\bar{k}} & \in & \wp(\bar{k}) \end{array} \tag{80}$$

is commutative, *a fact announced in §10*. In particular, the law of decomposition of prime divisors of $\wp(\bar{k})$ in K is completely described by the corresponding elements of $\wp(\Gamma^*)$ (e.g., if $E_z^* = \{1\}$, it is described as in Conjecture 3, in the General Introduction).

Remark . That $\mathcal{J}_K$ is Degree-preserving follows easily. Define the Degree of each element of $\wp(\Gamma_K^*)$ (resp. $\wp(K)$) in the same manner as in the definition of the Degree of

[19]As prime divisors of K; thus if we regard $\mathfrak{P}_z|_K$, $\mathfrak{P}_{z'}|_K$ as places of K, then we should say "equivalent" instead of "equal".

elements of $\wp(\Gamma^*)$ (§3) (resp. $\wp(\bar{k})$; §5, §22).[20] Let γ be a positive generator of Γ_z^* modulo the torsion subgroup E_z^*, and let f be the smallest positive integer such that $\gamma^f \cdot \varepsilon \in \Gamma_K^*$ with some $\varepsilon \in E_z^*$. Put $\gamma_1 = \gamma^f \varepsilon$. Then it is clear that γ_1 is a generator of $(\Gamma_K^*)_z$ (modulo $E_z^* \cap \Gamma_K^*$); hence $\mathrm{Deg}\{z\}_{\Gamma_K^*} = f \cdot \mathrm{Deg}\{z\}_{\Gamma^*}$, and γ_1 generates (topologically) the decomposition group of $\mathfrak{P}_z$ in $\mathfrak{K}/K$ (modulo the inertia). Since γ and f are positive, this shows that γ_1 gives a Frobenius substitution of $\mathfrak{P}_z$ in $\mathfrak{K}/K$; hence

$$\mathrm{Deg}(\mathfrak{P}_z|_K) = f \cdot \mathrm{Deg}\left(\mathfrak{P}_z|_{\bar{k}}\right) = f \cdot \mathrm{Deg}\{z\}_{\Gamma^*} = \mathrm{Deg}\{z\}_{\Gamma_K^*}$$

by Theorem 1, i.e., $\mathcal{J}_K$ is Degree-preserving.

(In the case where the constant field of K is $\mathbf{F}_{p^2}$, or equivalently $\Gamma_K^* = \Gamma \subset PSL_2(\mathbf{Z}^{(p)})$, we may define degree $= \frac{1}{2}$(Degree) of elements of $\wp(\Gamma_K^*)$, which corresponds to the degrees of prime divisors of K over $\mathbf{F}_{p^2}$. Of course, with these definitions, $\mathcal{J}_K$ is also degree-preserving.)

§25. Proof of Theorem 3.

(I) The case $j(z) \not\equiv 0, 12^3 \pmod{\mathfrak{p}}$. In this case, z is not Γ^*-equivalent to $i = \sqrt{-1}$ or $\omega = \frac{1}{2}\left(-1+\sqrt{-3}\right)$[21]; hence Γ_z^* is infinite cyclic; hence $E_z^* = \{1\}$. Now by the Corollary of Proposition 3 and the Remark in §12 (applied for $k = \bar{k}$, $v : \bar{j} \to \overline{j(z)}$), $\overline{\psi}_z$ is unramified in all $\bar{k}_n$; hence also in $\mathfrak{K}$ (see §17 for $\overline{\psi}_z$). This settles (ii).

Now γ being as in Theorem 3, put $D = \mathrm{Deg}\,\gamma$. Then $\overline{j(z)}$ is of degree D over $\mathbf{F}_p$ (see Part 1), and hence the residue field of $\bar{k}$ with respect to $\mathfrak{P}_z$ is $\mathbf{F}_{p^D}$. By Theorem 2, we have $\delta\mathfrak{P}_z \equiv \mathfrak{P}_{\delta z}$ for all $\delta \in \Gamma_z^*$; hence the topological closure of Γ_z^* is contained in the decomposition group of $\mathfrak{P}_z$. On the other hand, the decomposition group is generated topologically by the Frobenius substitution; hence it is enough to show that γ gives the Frobenius substitution of $\mathfrak{P}_z$.

Now keep all the notations in §21, §23. Then since $\gamma z = z$, we have $E' = E$, and φ is a complex multiplication of E induced by the linear map $u \mapsto \pi u$ of $\mathbf{C}$. Moreover, O_f is the ring of endomorphisms of E, $\pi = cz + d \in O_f$, and $\pi O_1 = p^k \mathfrak{p}_1^D$ where $\mathfrak{p}_1 = \mathfrak{p} \cap \mathbf{Q}(z)$ (since γ is positive w.r.t. $\mathfrak{p}$). Now by M. Deuring [4] [7], the endomorphism ring of $\overline{E}$ is naturally identified with O_{f_0} (by reduction mod $\mathfrak{p}$). But we have $\pi O_{f_0} = p^k \mathfrak{p}_{f_0}^D = \mathfrak{p}_{f_0}^{D+k} \mathfrak{p}'^k_{f_0}$, with $\mathfrak{p}_{f_0} = \mathfrak{p}_1 \cap O_{f_0}$, $\mathfrak{p}'_{f_0} = \mathfrak{p}'_1 \cap O_{f_0}$, $\mathfrak{p}_1\mathfrak{p}'_1 = p$. Moreover, $\overline{\varphi}$ is nothing but π, considered as an element of O_{f_0}. Therefore, $\nu_s(\overline{\varphi}) = p^k$ and $\nu_i(\overline{\varphi}) = p^{D+k}$; hence $\overline{\varphi}\,\overline{u} = \pm(p^k\overline{u})^{p^D}$ holds for all $\overline{u} \in \overline{E}$ (see the argument in §21). Therefore,

$$\overline{x_{(\alpha\beta)\gamma}(z)} = \overline{x_{p^k(\alpha,\beta)}(z)}^{p^D} \tag{81}$$

holds for all α, β. Therefore by an argument similar to that in §21, we obtain $\chi_z = \rho^{-D} \circ \chi_z \circ (p^{-k}\gamma)$; hence $\mathfrak{P}_z \circ \gamma = \rho^D \circ \mathfrak{P}_z$. Therefore, γ is the Frobenius substitution of $\mathfrak{P}_z$ in $\mathfrak{K}/\bar{k}$.

[20]Thus, the Degree of the prime divisor of $\wp(K)$ is its *degree over* $\mathbf{F}_p$.

[21]By Theorem 1.

(II) The case $j(z) \equiv 12^3 \pmod{\mathfrak{p}}$**.** Since z is a Γ^*-fixed point, $\overline{j(z)} = 12^3 = \overline{j(i)}$ ($i = \sqrt{-1}$) is not supersingular; hence z is Γ^*-equivalent to i (Theorem 1), and p is decomposed completely in $\mathbf{Q}(i)$; hence $p \equiv 1 \pmod 4$ (in particular, $p \neq 2, 3$). Since z is Γ^*-equivalent to i, Γ_z^* is conjugate to Γ_i^* in Γ^*; hence E_z^* is of order 2. By Theorem 2, the topological closure of Γ_z^* in $G(\mathfrak{K}/\bar{k})$ is contained in the decomposition group of $\mathfrak{P}_z$, and since the automorphism group of $\mathbf{F}_p^a$ has no torsion (since it is isomorphic to $\bigoplus_l \mathbf{Z}_l$), E_z^* must act trivially on the residue field of $\mathfrak{P}_z$; hence E_z^* is contained in the inertia group of $\mathfrak{P}_z$. Now, consider the subfield $\bar{k}_2 = \bar{k}(\bar{\lambda}) = \mathbf{F}_p(\bar{\lambda})$ of $\mathfrak{K}$, λ being as in §21 (II). Then in $M\{\bar{k}\}/\bar{k}_2$, all discrete valuations v of $\bar{k}_2$ with $v(\bar{\lambda}) = v(\bar{\lambda} - 1) = 0$ are unramified (this is rather well-known, and can be seen by an argument exactly parallel to that in the proof of the Corollary of Proposition 3, by using the elliptic curve $\eta^2 = \xi(\xi - 1)(\xi - \bar{\lambda})$ and its good reductions). On the other hand, the decomposition of $\mathfrak{P}^0 = \mathfrak{P}_z|_{\bar{k}}$ in $\bar{k}_2$ is of the form $\mathfrak{P}^0 = (\mathfrak{P}^{(1)}\mathfrak{P}^{(2)}\mathfrak{P}^{(3)})^2$, where $\mathfrak{P}^{(1)}, \mathfrak{P}^{(2)}, \mathfrak{P}^{(3)}$ send $\bar{\lambda}$ to $2, \frac{1}{2}, -1$ respectively. Therefore, the ramification index of $\mathfrak{P}_z$ in $\mathfrak{K}/\bar{k}$ is 2. Therefore, by what we have seen, the inertia group of $\mathfrak{P}_z$ in $\mathfrak{K}/\bar{k}$ is E_z^*. Moreover, the above decomposition of $\mathfrak{P}^0$ shows that the relative degrees of $\mathfrak{P}^{(i)}$ are 1; hence the decomposition group of $\mathfrak{P}_z$ in $G(\mathfrak{K}/\bar{k})$ is the direct product of its intersection with $G(\mathfrak{K}/\bar{k}_2)$ and E_z^*. In particular, there is a positive generator γ of Γ_z^* mod E_z^* such that $\gamma \equiv 1 \pmod 2$. Now it is enough to prove that γ gives a Frobenius substitution. But this proof can be obtained exactly in the same manner as in the case of $j(z) \not\equiv 0, 12^3 \pmod{\mathfrak{p}}$, by applying the results of §21 (II) instead of §21 (I).

(III) The case $j(z) \equiv 0 \pmod{\mathfrak{p}}$**.** In this case, z is Γ^*-equivalent to $\omega = \frac{1}{2}\left(-1 + \sqrt{-3}\right)$, $p \equiv 1 \pmod 3$ (in particular, $p \neq 2, 3$), and E_z^* is of order 3. Consider $\bar{k}_3 = \bar{k}(\bar{\mu}, \bar{\omega})$, μ being as in §21 (III). Then $\bar{k}_3 \subset \mathfrak{K}$, and the decomposition of $\mathfrak{P}^0 = \mathfrak{P}_z|_{\bar{k}}$ in $\bar{k}_3$ is of the form $\mathfrak{P}^0 = (\mathfrak{P}^{(1)}\mathfrak{P}^{(2)}\mathfrak{P}^{(3)}\mathfrak{P}^{(4)})^3$, where $\mathfrak{P}^{(i)}$ ($i = 1, 2, 3, 4$) send $\bar{\mu}$ to $0, -2, -2\omega, -2\omega^2$ respectively. Note that $\bar{\omega} \in \mathbf{F}_p$, since $p \equiv 1 \pmod 3$. Now our proof proceeds exactly in the same manner as above, by using the results of §21 (III).

This completes the proof of Theorem 3. □

Decomposition of supersingular prime divisors of $\bar{k}$ in $\mathfrak{K}$.

§26. Now we are going to study the law of decomposition in $\mathfrak{K}/\bar{k}$ of *supersingular* prime divisors $\mathfrak{P}^0$ of $\bar{k}$ (see §22 for its definition). Recall that if $\mathfrak{P}^0$ is supersingular, then $\mathfrak{P}^0$ is of degree either one or two, i.e., either $\mathfrak{P}^0(\bar{k}) = \mathbf{F}_p$ or $= \mathbf{F}_{p^2}$.

Theorem 4. *Let $\mathfrak{P}^0$ be a supersingular prime divisor of $\bar{k}$, and let $\mathfrak{P}$ be any extension of $\mathfrak{P}^0$ to $\mathfrak{K}$. Then the residue field of $\mathfrak{K}$ mod $\mathfrak{P}$ is $\mathbf{F}_{p^2}$;*

$$\mathfrak{P}(\mathfrak{K}) = \mathbf{F}_{p^2}. \tag{82}$$

Corollary. *Let $\mathfrak{P}^0$ be as above. Then,*

(i) *if $\mathfrak{P}^0$ is of degree two, it is unramified and is decomposed completely in $\mathfrak{K}$;*

(ii) *if $\mathfrak{P}^0$ is of degree one, then $\mathfrak{P}^0$ remains inert ("träge") in the quadratic constant field extension $\mathbf{F}_{p^2}\bar{k}$, but in $\mathfrak{K}/\mathbf{F}_{p^2}\bar{k}$, the decomposition group of $\mathfrak{P}$ coincides with the inertia group.*

Proof of the Corollary. (ii) follows trivially from Theorem 4. As for (i), we need only check that $\mathfrak{P}^0$ is unramified. Put $\mathfrak{P}^0(\bar{j}) = \bar{j}_0$. Then since $\mathfrak{P}^0$ is of degree two, $\bar{j}_0$ is of degree two over $\mathbf{F}_p$; hence, in particular, $\bar{j}_0 \neq 0, 12^3$. Now the unramifiedness follows directly from the Corollary of Proposition 3 and Remark in §12. □

Remark 1. Put $\mathfrak{P}^0(\bar{j}) = \bar{j}_0$. Then, according to Igusa [14], the inertia group of $\mathfrak{P}$ in $\mathfrak{K}/\bar{k}$ is isomorphic to

(a) $\{1\}$	$\cdots \bar{j}_0 \neq 0, 12^3;$
(b) cyclic group of order 2	$\cdots \bar{j}_0 = 12^3,\ p \neq 2, 3;$[22]
(c) cyclic group of order 3	$\cdots \bar{j}_0 = 0,\ p \neq 2, 3;$
(d) $\mathfrak{S}_3$(symmetric group)	$\cdots \bar{j}_0 = 0 = 12^3,\ p = 3;$
(e) $\mathfrak{A}_4$(alternating group)	$\cdots \bar{j}_0 = 0 = 12^3,\ p = 2.$

On the other hand, $\mathfrak{P}$ is unramified in $\mathfrak{K}/\bar{k}_2$ $(p \neq 2)$ and also in $\mathfrak{K}/\bar{k}_3$ $(p \neq 3)$.

Remark 2. Let K be any finite extension of $\bar{k}$ contained in $\mathfrak{K}$, so that K is an algebraic function field whose (exact) constant field is either $\mathbf{F}_p$ or $\mathbf{F}_{p^2}$. Call a prime divisor $\mathfrak{P}$ of K supersingular if it lies above a supersingular prime divisor $\mathfrak{P}^0$ of $\bar{k}$, and suppose now that the constant field of K is $\mathbf{F}_{p^2}$. Then by Theorem 4, all supersingular $\mathfrak{P}$ of K are of degree one over $\mathbf{F}_{p^2}$, and moreover, if we put $n = [K : \mathbf{F}_{p^2} \cdot \bar{k}]$ and

$$(83) \qquad e = \begin{cases} 1 & \cdots \mathfrak{P}^0(\bar{j}) \neq 0, 12^3, \\ 2 & \cdots \mathfrak{P}^0(\bar{j}) = 12^3,\ p \neq 2, 3, \\ 3 & \cdots \mathfrak{P}^0(\bar{j}) = 0,\ p \neq 2, 3, \\ 6 & \cdots \mathfrak{P}^0(\bar{j}) = 0 = 12^3,\ p = 3, \\ 12 & \cdots \mathfrak{P}^0(\bar{j}) = 0 = 12^3,\ p = 2, \end{cases}$$

then the number of $\mathfrak{P}$ lying above $\mathfrak{P}^0$ is at least equal to n/e. Therefore, by the roughest estimation, the number of prime divisors of K of degree one is *at least* equal to $\frac{n}{12}$. On the other hand, let M be the smallest positive integer for which K has a non-singular model *over* $\mathbf{F}_{p^2}$ in the projective space $\mathbf{P}^M$. Then, since the number of $\mathbf{F}_{p^2}$-rational points of $\mathbf{P}^M$ is $\frac{p^{2M+2}-1}{p^2-1}$, the number of prime divisors of K of degree one is *at most* equal to $\frac{p^{2M+2}-1}{p^2-1}$. Therefore, we have $p^{2M+2} \geq 1 + \frac{n}{12}(p^2 - 1)$, which implies $\lim_{n\to\infty} M = \infty$; thus,

(84) *the smallest dimension of the projective space in which K has a non-singular model over $\mathbf{F}_{p^2}$ tends to infinity as $[K : \bar{k}] \to \infty$.*

[22] $\bar{j}_0 = 12^3$ (resp. $\bar{j}_0 = 0$) is supersingular if and only if $p \not\equiv 1 \pmod 4$ (resp. $p \not\equiv 1 \pmod 3$).

As an example, let $N \not\equiv 0 \pmod p$, put

$$(85) \qquad \Gamma(N) = \left\{\gamma \in SL_2(\mathbf{Z}^{(p)}) \mid \gamma \equiv \pm 1 (\mathrm{mod}\ N)\right\} / \pm 1,$$

and let K_N be the subfield of $\mathfrak{K}$ corresponding to $\Gamma(N)$ (so that $K_N \supset \mathbf{F}_{p^2}$). Then if $N > 1$, $\mathfrak{K}/K_N$ is unramified; hence by a simple computation, the number of supersingular prime divisors of K_N is $\frac{n}{12}(p-1)$, where $n = [K_N : \mathbf{F}_{p^2} \cdot \bar{k}] = (PSL_2(\mathbf{Z}^{(p)}) : \Gamma(N)) = 6$ $(N = 2), = \frac{N^3}{2}\prod_{l|N}\left(1 - \frac{1}{l^2}\right)$ $(N > 2)$; hence $p^{2M+2} \geq 1 + \frac{n}{12}(p-1)(p^2-1)$. For example, for $(p, N) = (2, 9)$ or $(3, 11)$, we have $M \geq 3$, and for $(p, N) = (2, 13)$ or $(3, 23)$, we have $M \geq 4$.

§27. Proof of Theorem 4. Put $\mathfrak{P}^0(\bar{j}) = \bar{j}_0$.

(I) The case $\bar{j}_0 \neq 0, 12^3$. Let $\tilde{\mathfrak{P}}$ be an extension of $\mathfrak{P}$ to $\bigcup_{n \not\equiv 0 \ (\mathrm{mod}\ p)} \bar{k}(E_{\bar{j}}(n))$. Since $\bar{j}_0 \neq 0, 12^3$, $\tilde{\mathfrak{P}}$ gives a good reduction $E_{\bar{j}} \to E_{\bar{j}_0}$, and hence induces an isomorphism $E_{\bar{j}}(n) \cong E_{\bar{j}_0}(n)$ for each $n \not\equiv 0 \pmod p$. On the other hand, we know that there is an isomorphism $E_{\bar{j}}(n) \cong (\mathbf{Z}/n\mathbf{Z})^2$ (unique up to ± 1) such that for any (α, β), $\bar{x}_{\alpha\beta}$ is the x-coordinate of the point of $E_{\bar{j}}(n)$ which corresponds to (α, β) (see §15). Thus the above two isomorphisms induce the isomorphism $E_{\bar{j}_0}(n) \cong (\mathbf{Z}/n\mathbf{Z})^2$, where the x-coordinate of the point of $E_{\bar{j}_0}(n)$ corresponding to (α, β) is the residue class of $\bar{x}_{\alpha\beta} \mod \tilde{\mathfrak{P}}$, which we denote by $\bar{x}^0_{\alpha\beta}$. So, $\bar{x}^0_{\alpha\beta}$ are finite, and $\bar{x}^0_{\alpha\beta} = \bar{x}^0_{\alpha'\beta'}$ if and only if $(\alpha, \beta) = \pm(\alpha', \beta')$ (see §12).

Now we claim that

$$(86) \qquad \bar{u}^{p^2} = \pm p\bar{u}; \quad \text{for } \bar{u} \in E_{\bar{j}_0}.$$

In fact, since $\bar{j}_0$ is supersingular, $\bar{u} \mapsto p \cdot \bar{u}$ is purely inseparable of degree p^2; hence $\bar{u} \mapsto (p\bar{u})^{1/p^2}$ is an automorphism of $E_{\bar{j}_0}$, which is ± 1 since $\bar{j}_0 \neq 0, 12^3$ (Proposition 1); hence (86). Hence $\bar{x}^0_{p(\alpha,\beta)} = (\bar{x}^0_{\alpha\beta})^{p^2}$ holds for all α, β. Now let σ be a Frobenius substitution of $\tilde{\mathfrak{P}}$ over $\mathbf{F}_{p^2}\bar{k}$. Then $\bar{x}^0_{(\alpha,\beta)\sigma} = \bar{x}^{0\ p^2}_{\alpha\beta}$; hence $\bar{x}^0_{(\alpha\beta)\sigma} = \bar{x}^0_{p(\alpha\beta)}$ for all α, β. Therefore, $(\alpha, \beta)\sigma = \pm p(\alpha, \beta)$ holds for all α, β; which implies $\sigma = \pm p \in \pm\overline{\Pi}$; hence $\sigma|_{\mathfrak{K}} = 1$. But this implies $\mathfrak{P}(\mathfrak{K}) = \mathbf{F}_{p^2}$; hence settles the proof for this case.

(II) The case $\bar{j}_0 = 12^3$, $p \neq 2$. Since $\mathfrak{P}$ sends $\bar{\lambda}$ to either $2, \frac{1}{2}$, or -1, the residue field of $\mathbf{F}_{p^2}\bar{k}_2 = \mathbf{F}_{p^2}(\bar{\lambda})$ is $\mathbf{F}_{p^2}$. Now by using the elliptic curve of §21 (II), we obtain, exactly in the same manner as above, that the relative degree of $\mathfrak{P}$ in $\mathfrak{K}/\mathbf{F}_{p^2}\bar{k}_2$ is one; i.e., $\mathfrak{P}(\mathfrak{K}) = \mathfrak{P}(\mathbf{F}_{p^2}\bar{k}_2) = \mathbf{F}_{p^2}$.

(III) The case $\bar{j}_0 = 0$, $p \neq 3$. Since $\mathfrak{P}$ sends $\bar{\mu}$ to either $0, -2, -2\bar{\omega}$, or $-2\bar{\omega}^2$ (where $\omega = \frac{1}{2}(-1 + \sqrt{-3})$), the residue field of $\mathbf{F}_{p^2}\bar{k}_3 = \mathbf{F}_{p^2}(\bar{\mu})$ is $\mathbf{F}_{p^2}$. Thus we obtain the theorem for this case by using the elliptic curve of §21 (III). Since $12^3 = 0$ if $p = 2$ or 3, this completes the proof of Theorem 4. □

Decomposition of the infinite prime divisor of $\bar{k}$ in $\mathfrak{K}$.

§28. Now it only remains to study the law of decomposition in $\mathfrak{K}$ of the *infinite* prime divisor $\mathfrak{P}^0$ of $\bar{k}$ (see §22 for its definition). Let $z \in \mathbf{Q} \cup \{i\infty\}$ be a cusp of $PSL_2(\mathbf{Z})$, let ψ_z be the place of $M\{k\}$ defined by $F(\mathfrak{z}) \to F(z)$, and let $\bar{\psi}_z$ be the place of $M\{\bar{k}\}$ associated to ψ_z by Proposition 7. Let $\mathfrak{P}_z$ be the restriction of $\bar{\psi}_z$ to $\mathfrak{K}$. Then $\mathfrak{P}_z|_{\bar{k}} = \mathfrak{P}^0$; hence it is enough to find out the inertia and the decomposition groups of $\mathfrak{P}_z$ in $\mathfrak{K}/\bar{k}$. The result is as follows:

THEOREM 5.[23] *Let z be a cusp of $PSL_2(\mathbf{Z})$. Then,*

(i) *we have*

$$\gamma\mathfrak{P}_z \equiv \mathfrak{P}_{\gamma z}, \quad \textit{for any } \gamma \in \Gamma^*; \tag{87}$$

(ii) *Put*

$$\begin{cases} H^0 = \{\gamma \in \Gamma^* \mid \gamma z = z,\ \gamma : \textit{parabolic}\} \cup \{1\}, \\ H \ = \{\gamma \in \Gamma^* \mid \gamma z = z\}. \end{cases} \tag{88}$$

Then the inertia and the decomposition groups of $\mathfrak{P}_z$ in $\mathfrak{K}/\bar{k}$ are the topological closures in $G(\mathfrak{K}/\bar{k})$ of H^0 and of H respectively.

REMARK . In particular, when $z = i\infty$, the groups H^0, H are given by

$$\begin{cases} H^0 &= \begin{pmatrix} 1 & \mathbf{Z}^{(p)} \\ 0 & 1 \end{pmatrix}, \\ H &= \left\{ \begin{pmatrix} p^m & b \\ 0 & p^n \end{pmatrix} \middle| \ m, n \in \mathbf{Z},\ b \in \mathbf{Z}^{(p)} \right\} \Big/ \Pi. \end{cases}$$

PROOF.

(I) The proof of (ii) for $z = i\infty$. Put $\psi = \psi_{i\infty}$, $\bar{\psi} = \bar{\psi}_{i\infty}$, and $\mathfrak{P} = \mathfrak{P}_{i\infty}$. Put $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. By Proposition 7, if $\mathfrak{o}_\psi$ is the second ring of (60) and if Θ_ψ is its integral closure in $M\{k\}$, then $\bar{\psi}$ is the *unique* place of $M\{\bar{k}\}$ that sends $\overline{F(\mathfrak{z})}$ to $\overline{F(i\infty)}$ for all $F(\mathfrak{z}) \in \Theta_\psi$. But since $\gamma \in PSL_2(\mathbf{Z})$, we have $\gamma(\overline{F(\mathfrak{z})}) = \overline{F(\gamma\mathfrak{z})}$, and since $\gamma(i\infty) = i\infty$, we see that the place $\bar{\psi} \circ \gamma$ (of $M\{\bar{k}\}$) also sends $\overline{F(\mathfrak{z})}$ to $\overline{F(i\infty)}$ for all $F(\mathfrak{z}) \in \Theta_\psi$. Therefore, $\bar{\psi} = \bar{\psi} \circ \gamma$; hence γ is contained in the inertia group of $\bar{\psi}$. This proves that the inertia group of $\mathfrak{P}$ contains the topological closure of H^0, i.e., $\prod_{l \neq p} \begin{pmatrix} 1 & \mathbf{Z}_l \\ 0 & 1 \end{pmatrix}$.

Conversely, let $\sigma \in G(M\{\bar{k}\}/\bar{k})$ be such that $\sigma = 1$ on $\mathbf{F}_p^{\mathrm{a}}$ and that $\overline{x_{(\alpha\beta)\sigma}(i\infty)} = \overline{x_{\alpha\beta}(i\infty)}$ for all α, β. We claim that such σ is contained in $\prod_{l \neq p} \begin{pmatrix} 1 & \mathbf{Z}_l \\ 0 & 1 \end{pmatrix}$. To see this, put $\sigma = \prod_{l \neq p} \sigma_l$, with $\sigma_l = \begin{pmatrix} a_l & b_l \\ c_l & d_l \end{pmatrix} \in GL_2(\mathbf{Z}_l)$. Since $\sigma = 1$ on $\mathbf{F}_p^{\mathrm{a}}$, we have $\det \sigma_l = 1$ $(l \neq p)$. But by (67), we have $x_{\alpha\beta}(i\infty) = 0$ $(\alpha \neq 0)$, $= -(2\sin\pi\beta)^{-2}$ $(\alpha = 0, \beta \neq 0)$; hence by

[23] See the Corollary below, for the Frobenius substitution.

$\overline{x_{(\alpha\beta)\sigma}(i\infty)} = \overline{x_{\alpha\beta}(i\infty)}$ (for all α, β), we obtain $c_l = 0$, $(d_l)_l = \pm 1$; hence $\sigma \in \prod_{l \neq p} \begin{pmatrix} 1 & \mathbf{Z}_l \\ 0 & 1 \end{pmatrix}$. Now if σ is an element of the inertia group of $\overline{\psi}$, we have $\overline{\psi} \circ \sigma(\overline{x}_{\alpha\beta}) = \overline{\psi}(\overline{x}_{\alpha\beta})$; but since $x_{\alpha\beta} \in \Theta_\psi$ (by the Corollary of Lemma 3), we have $\overline{\psi} \circ \sigma(\overline{x}_{\alpha\beta}) = \overline{x_{(\alpha\beta)\sigma}(i\infty)}$, $\overline{\psi}(\overline{x}_{\alpha\beta}) = \overline{x_{\alpha\beta}(i\infty)}$; hence σ satisfies the above conditions. Therefore, the inertia group of $\overline{\psi}$ is contained in $\prod_{l \neq p} \begin{pmatrix} 1 & \mathbf{Z}_l \\ 0 & 1 \end{pmatrix}$; hence together with what we have shown already, we conclude that the inertia group of $\mathfrak{P}$ in $\mathfrak{K}/\overline{k}$ is $\prod_{l \neq p} \begin{pmatrix} 1 & \mathbf{Z}_l \\ 0 & 1 \end{pmatrix}$.

Since the decomposition group is generated by a Frobenius substitution modulo the inertia group, it is now enough to show that $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ gives a Frobenius substitution. Put $\overline{\psi}' = \rho^{-1} \circ \overline{\psi} \circ \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, ρ being the Frobenius automorphism of $\mathbf{F}_p^{\mathrm{a}}$. Then $\overline{\psi}' = \overline{\psi}$ on $\mathbf{F}_p^{\mathrm{a}}(\overline{j})$; hence there is an automorphism $\sigma \in G\left(M\{\overline{k}\}/\mathbf{F}_p^{\mathrm{a}}\overline{k}\right)$ such that $\overline{\psi}' = \overline{\psi} \circ \sigma$. But $\overline{\psi}'$ and $\overline{\psi} \circ \sigma$ send $\overline{x}_{\alpha\beta}$ to $\overline{x_{\alpha,p\beta}(i\infty)}^{1/p} = \overline{x_{\alpha\beta}(i\infty)}$ and $\overline{x_{(\alpha\beta)\sigma}(i\infty)}$ respectively; hence $\overline{x_{\alpha\beta}(i\infty)} = \overline{x_{(\alpha\beta)\sigma}(i\infty)}$; hence by the above argument, σ is contained in the inertia group of $\overline{\psi}$; hence $\overline{\psi}' = \overline{\psi}$; hence $\overline{\psi} \circ \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} = \rho \circ \overline{\psi}$; hence $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ gives a Frobenius substitution for $\overline{\psi}$ and hence also for $\mathfrak{P}$. This settles (I).

(II) The proof of (i). Note first that $\gamma\mathfrak{P}_z = \mathfrak{P}_{\gamma z}$ holds if $\gamma \in PSL_2(\mathbf{Z})$. Note, moreover, that since $PSL_2(\mathbf{Z})$ acts transitively on the set of all cusps of $PSL_2(\mathbf{Z})$, it is enough to prove (87) only for the case $z = i\infty$. Thus, let $z = i\infty$, put $\gamma z = \delta z$ with $\delta \in PSL_2(\mathbf{Z})$, and put $\gamma = \delta\gamma_1$. Then γ_1 is upper triangular, and hence by (I), it is contained in the decomposition group of $\mathfrak{P}_{i\infty}$. Therefore, $\gamma\mathfrak{P}_{i\infty} = \delta\gamma_1\mathfrak{P}_{i\infty} \equiv \delta\mathfrak{P}_{i\infty} = \mathfrak{P}_{\delta(i\infty)} = \mathfrak{P}_{\gamma(i\infty)}$; hence (II) is settled.

(III) The proof of (ii) for the general z. Put $z = \delta(i\infty)$ ($\delta \in PSL_2(\mathbf{Z})$). Then $\mathfrak{P}_z = \mathfrak{P}_{\delta(i\infty)} = \delta\mathfrak{P}_{i\infty}$; hence the inertia (resp. the decomposition) group of $\mathfrak{P}_z$ is the transform by δ of the inertia (resp. the decomposition) group of $\mathfrak{P}_{i\infty}$. This settles (III), and hence completes the proof of Theorem 5. □

We have also proved:

COROLLARY. *The inertia and the decomposition groups of* $\mathfrak{P}_{i\infty}$ *are:*

$$(89)\quad \begin{cases} \text{the inertia group} = \left\{ \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \middle| \beta \in \prod_{l \neq p} Z_l \right\}, \\ \text{the decomposition group} = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \middle| \alpha, \delta \in \overline{\Pi},\ \beta \in \prod_{l \neq p} Z_l \right\} \Big/ \pm \overline{\Pi}. \end{cases}$$

Moreover, a Frobenius substitution is given by $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$.

Reformulation in terms of non-abelian classfields; Main Theorems (Γ^*-1) ~ (Γ^*-3), and Conjecture Γ^*.

Now we shall summarize our above results in terms of "non-abelian classfield theory".[24] In this formulation, elliptic curves are completely eliminated. Throughout §29 ~ §31, $\mathfrak{p}$ is a fixed prime factor of p in $\mathbf{Q}^a$.

§29. Definition of classfields. As before, put

$$\Gamma^* = \{\gamma \in GL_2(\mathbf{Z}^{(p)}) \mid \det\gamma \in \Pi\}/\pm\Pi,$$

and let $\wp(\Gamma^*)$ be the set of all Γ^*-equivalence classes of all Γ^*-fixed points z on $\mathfrak{H}$ (so that, by definition, Γ^*_z is infinite for such z; see §1 ~ §2). On the other hand, put now $K^* = \mathbf{F}_p(\bar{j})$, $\bar{j}$ being a variable over $\mathbf{F}_p$, and let $\wp(K^*)$ be the set of all ordinary prime divisors (cf. §22) of K^*, so that $\wp(K^*)$ is naturally identified with $\mathbf{F}_p^a - S/\sim$, where S ($\subset \mathbf{F}_{p^2}$) is the set of all supersingular elements and $\sim$ denotes the conjugacy over $\mathbf{F}_p$ (see §4, §5). In Part 1 (Theorem 1), we have proved that $z \mapsto j(z) \mod \mathfrak{p}$ induces a degree-preserving bijection $\mathcal{J}^* : \wp(\Gamma^*) \to \wp(K^*)$. Since $\mathcal{J}^*$ depends on the choice of $\mathfrak{p}$, we shall denote $\mathcal{J}^* = \mathcal{J}^*_{\mathfrak{p}}$ when necessary.

Now let Γ' be any normal subgroup of Γ^* with finite index. A finite Galois extension K' over K^* will be called *a Γ'-classfield* (over K^*), or *a classfield attached to* Γ' (over K^*), if the following condition (♯) is satisfied:

(♯) *An ordinary prime divisor $\mathfrak{P}^0$ of K^* is decomposed completely in K' if and only if Γ^*_z is contained in Γ'; where $z(\in \mathfrak{H})$ is a representative of the Γ^*-equivalence class $\mathcal{J}^{*-1}_{\mathfrak{p}}(\mathfrak{P}^0)$, and Γ^*_z denotes its stabilizer in Γ^*.*

Here, note that if we take another representative z_1 of $\mathcal{J}^{*-1}_{\mathfrak{p}}(\mathfrak{P}^0)$, then $z_1 = \delta z$ with some $\delta \in \Gamma^*$; hence $\Gamma^*_{z_1} = \delta\Gamma^*_z\delta^{-1}$; hence the above condition does not depend on the choice of z. The dependency of this condition on the choice of $\mathfrak{p}$ (which is of quite a subtle nature) will be studied in §32 (Proposition 13).

§30. Main theorems (Γ^*-1) ~ (Γ^*-3).

Main Theorem (Γ^*-1). *For each Γ', a Γ'-classfield exists, and is unique.*

Proof. By Mennicke [**23**], the group $SL_2(\mathbf{Z}^{(p)})$, and hence also the group Γ^*, have congruence subgroup property. Therefore, by (56), the Galois group $G(\mathfrak{K}/\bar{k})$ ($\bar{k} = \mathbf{F}_p(\bar{j}) = K^*$) is naturally identified with the completion of Γ^* with respect to "subgroups with finite indices topology". Therefore, subgroups of Γ^* with finite indices are in one-to-one correspondence with finite extensions of $\bar{k} = K^*$ contained in $\mathfrak{K}$. Let K' be the extension of K^* corresponding to Γ'. Then it is clear by Theorem 3 that K' is a Γ'-classfield. Uniqueness is an immediate consequence of Čebotarev's density theorem. □

[24] We shall formulate this only for the group Γ^*. Similar (and related) results for subgroups Γ_K of Γ^* with finite indices are obtained if we use $\mathcal{J}_K$ (§24) instead of $\mathcal{J}^*$. The fields $\mathfrak{K}$, $\widehat{\mathfrak{K}}$ are common for all Γ_K.

Main Theorem (Γ^*-2). *Let $\mathfrak{K}$ be the composite of all Γ'-classfields, where Γ' runs over all normal subgroups of Γ^* with finite indices*[25]. *Then there is a dense injection $\iota : \Gamma^* \to G(\mathfrak{K}/K^*)$ satisfying the following conditions.*[26]

(i) *ι induces an isomorphism of the completion of Γ^* with respect to "subgroups with finite indices topology" and $G(\mathfrak{K}/K^*)$; hence subgroups of Γ^* with finite indices and finite extensions of K^* contained in $\mathfrak{K}$ correspond in a one-to-one manner. Moreover, if Γ' is any normal subgroup of Γ^* with finite index, then the corresponding finite extension of K^* is nothing but the Γ'-classfield.*

(ii) *Let $\mathfrak{P}^0$ be any ordinary prime divisor of K^*, let z be a representative of $\mathcal{J}_{\mathfrak{p}}^{*-1}(\mathfrak{P}^0)$, and let Γ_z^* be the stabilizer of z in Γ^*. Let E_z^* be the torsion subgroup of Γ_z^* and let γ be a positive generator of $\Gamma_z^* \bmod E_z^*$ with respect to $\mathfrak{p}$ (see §23). Then $\mathfrak{P}^0$ has an extension $\mathfrak{P}_z$ to $\mathfrak{K}$ whose inertia group is $\iota(E_z^*)$ and whose Frobenius substitution is $\iota(\gamma) \pmod{\iota(E_z^*)}$.*

(iii) *Let $\mathfrak{P}^0$ be the infinite prime divisor of K^* (cf. §22). Then $\mathfrak{P}^0$ has an extension $\mathfrak{P}_{i\infty}$ to $\mathfrak{K}$ whose inertia group is generated by $\iota\left(\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\right)$ and whose Frobenius substitution (modulo the inertia group) is given by $\iota\left(\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\right)$.*

Proof. Immediate from our results above (esp. Theorems 3, 5). □

Some supplementary remarks to this theorem are given in §32 (esp. Propositions 9, 13).

Now, our third main theorem and our main conjecture on Γ^* are concerned with a characterization of the field $\mathfrak{K}$ defined in Main Theorem (Γ^*-2):

Main Theorem (Γ^*-3). *Let $\mathfrak{K}$ be as in Main Theorem (Γ^*-2), and let $\widehat{\mathfrak{K}}$ be another field defined below. Then we have*

$$\mathfrak{K} \subset \widehat{\mathfrak{K}} \tag{90}$$

Conjecture Γ^*. With the same notations as above, we have

$$\mathfrak{K} = \widehat{\mathfrak{K}}\ ?$$[27]

The definition of $\widehat{\mathfrak{K}}$ and proof of Main Theorem (Γ^*-3). The field $\widehat{\mathfrak{K}}$ is easily defined if $p \neq 2, 3$. Namely, in this case, $\widehat{\mathfrak{K}}$ is the union of all separable algebraic extensions K' over K^* (finite or infinite) satisfying the following conditions (i) ~ (iii). Here, for any prime divisor $\mathfrak{P}^0$ of K^*, we put $\mathfrak{P}^0(\bar{j}) = \bar{j}_0$.

(i) *If $\bar{j}_0 \neq 0, 12^3, \infty$, then $\mathfrak{P}^0$ is unramified in K';*

[25] Since this $\mathfrak{K}$ obviously coincides with the former $\mathfrak{K}$ (by the above proof of Main Theorem (Γ^*-1)), there is no fear of confusion.

[26] We can also check that ι is characterized by (i) and (ii) up to inner automorphisms of $G(\mathfrak{K}/K^*)$. But we shall not give this proof here.

[27] Some remarks and numerical evidences for this conjecture are given in §33.

(ii) *If* $\bar{j}_0 = 0, 12^3, \infty$, *then* $\mathfrak{P}^0$ *is at most tamely ramified in* K' *with the ramification index dividing* $3, 2, \infty$ *respectively;*[28]

(iii) *If* $\bar{j}_0$ *is supersingular,*[29] *then* $\mathfrak{P}^0$ *is decomposed "almost completely" in* K'; *namely, in* $\mathbf{F}_{p^2}K'/\mathbf{F}_{p^2}K^*$, *the relative degree of* $\mathfrak{P}^0$ *is equal to one.*

It is clear that if K' satisfies (i) ~ (iii), then all conjugates of K' over K^* and all intermediate fields of K'/K^* also satisfy (i) ~ (iii). Moreover, it is easy to see that if K', K'' both satisfy (i) ~ (iii), then so does the composite field $K' \cdot K''$.[30] Therefore, $\widehat{\mathfrak{K}}$ *is nothing but the maximum* (*Galois*) *extension of* K^* *satisfying* (i) ~ (iii). Now by Theorems 3, 4, 5, the field $\mathfrak{K}$ satisfies all (i) ~ (iii); hence $\mathfrak{K} \subset \widehat{\mathfrak{K}}$. In particular, the fields $\mathbf{F}_{p^2}(\bar{\lambda})$ and $\mathbf{F}_{p^2}(\bar{\mu})$ which are finite Galois extensions of $K^* = \mathbf{F}_p(\bar{j})$ defined by the equations:

$$\bar{j} = 2^8 \frac{(1 - \bar{\lambda} + \bar{\lambda}^2)^3}{\left\{\bar{\lambda}(1 - \bar{\lambda})\right\}^2}, \quad \text{and} \quad \bar{j} = \left\{\frac{3\bar{\mu}(\bar{\mu}^3 + 2)}{\bar{\mu}^3 - 1}\right\}^3 \tag{91}$$

respectively, are contained in $\widehat{\mathfrak{K}}$ (since by §13, they are $\mathbf{F}_{p^2}\bar{k}_2$ and $\mathbf{F}_{p^2}\bar{k}_3$ respectively). Since the ramification indices of $\mathfrak{P}^0$ with $\bar{j}_0 = 0$ or 12^3 in these two fields are 3 or 2 respectively, the prime factors of such $\mathfrak{P}^0$ in $\widehat{\mathfrak{K}}$ are unramified in $\widehat{\mathfrak{K}}/\mathbf{F}_{p^2}(\bar{\lambda})$ and in $\widehat{\mathfrak{K}}/\mathbf{F}_{p^2}(\bar{\mu})$. By this, we obtain *the following alternative definitions of* $\widehat{\mathfrak{K}}$ *for* $p \neq 2, 3$, *which also serve as the definition of* $\widehat{\mathfrak{K}}$ *for* $p = 2$, *or* 3. Here, we call a prime divisor of $\mathbf{F}_{p^2}(\bar{\lambda})$ or of $\mathbf{F}_{p^2}(\bar{\mu})$ *ordinary* resp. *supersingular* resp. *infinite* when its restriction to K^* is ordinary resp. supersingular resp. infinite.

If $p \neq 2$ (resp. $p \neq 3$) and $K_1 = \mathbf{F}_{p^2}(\bar{\lambda})$ (resp. $K_1 = \mathbf{F}_{p^2}(\bar{\mu})$), $\widehat{\mathfrak{K}}$ is the composite of all separable algebraic extensions K' over K_1 satisfying the following:

(i)' *ordinary or supersingular prime divisors of* K_1 *are unramified in* K';

(ii)' *infinite prime divisors of* K_1 *are at most tamely ramified in* K';

(iii)' *supersingular prime divisors of* K_1 *are decomposed completely in* K'.

Note that the conditions (i)' ~ (iii)' are "hereditary" with respect to taking composite fields, conjugate fields over K^* (not only over K_1), and subfields (containing K_1); hence $\widehat{\mathfrak{K}}$ is nothing but the maximum separable algebraic extension of K_1 satisfying (i)' ~ (iii)', and $\widehat{\mathfrak{K}}$ is a Galois extension of K^*. By (iii)', *the constant field of* $\widehat{\mathfrak{K}}$ *is* $\mathbf{F}_{p^2}$.

Now, by Theorems 3, 4, 5 and by Remark 1 in §26, we see immediately that $\mathfrak{K} \subset \widehat{\mathfrak{K}}$ holds for all p including 2 or 3.

REMARK 1. By Deuring [4], $\bar{j}_0$ is supersingular if and only if it is a zero of a certain polynomial $f_j(x)$; hence supersingularity can be defined without using elliptic curves.

REMARK 2. Let us determine infinite and supersingular prime divisors of $K_1 = \mathbf{F}_{p^2}(\bar{\lambda})$ or $\mathbf{F}_{p^2}(\bar{\mu})$ more explicitly. Let I_λ, S_λ be the set of all $\bar{\lambda}_0$ such that the prime divisor $\mathfrak{P}^0$ of

[28] I.e., if $\bar{j}_0 = \infty$, there is no condition on the ramification index (except that the ramification must be tame).

[29] We may define supersingularity without using elliptic curves; see Remark 1 below.

[30] See Supplement §5.

$\mathbf{F}_{p^2}(\overline{\lambda})$ with $\mathfrak{P}^0(\overline{\lambda}) = \overline{\lambda}_0$ is infinite or supersingular respectively. Then

$$(92)\quad \begin{cases} I_\lambda &= \{0, 1, \infty\}, \\ S_\lambda &= \left\{ \overline{\lambda}_0 \in \mathbf{F}_p^a \;\middle|\; \begin{array}{l} \text{the elliptic curve } Y^2 = X(X-1)(X-\overline{\lambda}_0) \\ \text{is supersingular} \end{array} \right\} \\ &= \left\{ \overline{\lambda}_0 \in \mathbf{F}_p^a \;\middle|\; \overline{\lambda}_0 \text{ is a zero of } f_\lambda(x) = \sum_{i=0}^{r} \binom{r}{i}^2 x^i \right\}, \end{cases}$$

[31]

where $r = \frac{p-1}{2}$. Moreover, by $\mathbf{F}_{p^2}(\overline{\lambda}) \subset \widehat{\mathfrak{R}}$, we see easily that

$$(93)\qquad S_\lambda \subset \mathbf{F}_{p^2}, \quad |S_\lambda| = \frac{p-1}{2};$$

for example, if $p = 3$, then $S_\lambda = \{-1\}$.

In the same manner, I_μ and S_μ (defined similarly) are given as follows:

$$(94)\quad \begin{cases} I_\mu &= \{1, \omega, \omega^2, \infty\}, \quad \omega = \frac{1}{2}\left(-1 + \sqrt{-3}\right), \\ S_\mu &= \left\{ \overline{\mu}_0 \in \mathbf{F}_p^a \;\middle|\; \begin{array}{l} \text{the elliptic curve } X^3 + Y^3 + Z^3 = 3\overline{\mu}_0 XYZ \\ \text{(in projective coordinates) is supersingular} \end{array} \right\} \\ &= \left\{ \overline{\mu}_0 \in \mathbf{F}_p^a \mid \overline{\mu}_0 \text{ is a zero of } f_\mu(x) \right\}, \end{cases}$$

where $f_\mu(x)$ is a certain polynomial of x of degree $p-1$. Moreover,

$$(95)\qquad S_\mu \subset \mathbf{F}_{p^2}, \quad |S_\mu| = p-1;$$

for example, if $p = 2$, then $S_\mu = \{0\}$.

Supplements to Main Theorems and to Conjecture Γ^*.

Here, we shall give some supplementary results and remarks to §29 ~ §30.

§31. Some equivalence relations in $\wp(\Gamma^*)$ and in $\wp(K^*)$.

(I) Equivalence relations in $\wp(\Gamma^*)$. We shall introduce the following two equivalence relations $\sim$ and $\approx$ in $\wp(\Gamma^*)$. Let $P = P_z \in \wp(\Gamma^*)$ ($z \in \mathfrak{H}$), and put $\Omega = \mathbf{Q}(z)$, so that Ω is an imaginary quadratic field with $\left(\frac{\Omega}{p}\right) = 1$ (see §8). Consider the $\mathbf{Z}^{(p)}$-lattice $\mathfrak{a} = \mathbf{Z}^{(p)} + \mathbf{Z}^{(p)}z$, and let O be its $\mathbf{Z}^{(p)}$-order; i.e., $O = \{x \in \Omega \mid x\mathfrak{a} \subset \mathfrak{a}\}$. Then the lattice class [32] of $\mathfrak{a}$ and hence also the order O are well-defined by P. Denote by C_P resp. O_P the lattice class of $\mathfrak{a}$ resp. the order O. Then it is easy to see (cf. §8) that $P \mapsto C_P$ gives a one-to-one correspondence between $\wp(\Gamma^*)$ and the set of all $\mathbf{Z}^{(p)}$-lattice classes in (all) imaginary quadratic fields Ω with $\left(\frac{\Omega}{p}\right) = 1$. In another words, this is a one-to-one correspondence

[31] See Igusa [13].

[32] Two lattices $\mathfrak{a}_1, \mathfrak{a}_2$ belong to the same class if and only if $\mathfrak{a}_1 = \rho\mathfrak{a}_2$ with some $\rho \in \Omega$.

between $\wp(\Gamma^*)$ and the (set-theoretic) union of the group G_O, where G_O is the group of all proper[33] O-ideal classes, and O runs over all $\mathbf{Z}^{(p)}$-orders in all Ω;

$$\wp(\Gamma^*) \ni P \underset{1:1}{\longleftrightarrow} C_P \in \left\{ \begin{array}{l} \mathbf{Z}^{(p)}\text{-lattice classes in all} \\ \text{imaginary quadratic fields } \Omega \\ \text{with } \left(\frac{\Omega}{p}\right) = 1 \end{array} \right\} \tag{96}$$

$$\underset{1:1}{\longleftrightarrow} C_P \in \bigcup_O G_O.$$

Now, the first equivalence relation $\sim$ in $\wp(\Gamma^*)$ is defined by

$$P \sim P' \underset{\text{def.}}{\longleftrightarrow} O_P = O_{P'}, \tag{97}$$

while the second, stronger relation $\approx$ is defined by

$$P \approx P' \underset{\text{def.}}{\longleftrightarrow} \begin{cases} \text{(i)} \quad O_P = O_{P'} \underset{\text{put}}{(=} O), \\ \text{(ii)} \quad C_P C_{P'}^{-1} \in \{G_O\}^2; \end{cases} \tag{98}$$

where $\{G_O\}^2$ is the subgroup of G_O formed of all square elements (of G_O).

Remark 1. If one desires to formulate these in terms of $\mathbf{Z}$-orders only, then he may do it as follows; instead of (96), one has:

$$\wp(\Gamma^*) \ni P \underset{1:1}{\longleftrightarrow} C_P^{(0)} \in \bigcup_{O_0} G_{O_0}/\{\mathfrak{p}_0\}, \tag{99}$$

where O_0 runs over all $\mathbf{Z}$-orders in all Ω such that $\left(\frac{\Omega}{p}\right) = 1$ and that the conductor of O_0 is not divisible by p, G_{O_0} is the group of all proper O_0-ideal classes, $\{\mathfrak{p}_0\}$ is the cyclic subgroup of G_{O_0} generated by the (O_0-ideal) class of $\mathfrak{p}_0 = \mathfrak{p} \cap O_0$, and $C_P^{(0)}$ denotes the unique element of $\bigcup_{O_0} G_{O_0}/\{\mathfrak{p}_0\}$ such that $C_P^{(0)} \otimes_{\mathbf{Z}} \mathbf{Z}^{(p)} = C_P$. (Note that $\{\mathfrak{p}_0\}$ does not depend on the choice of a prime factor of p in Ω.) Since G_{O_0} is a finite group, each $\sim$-class (hence a priori $\approx$-class) consists of a finite number of elements of $\wp(\Gamma^*)$. Finally, $\operatorname{Deg} P$ is nothing but the order of the group $\{\mathfrak{p}_0\}$.

Proposition 8. *Let X be the completion of Γ^* with respect to all subgroups with finite indices, so that*

$$X = \left\{ x \in \prod_{l \neq p} GL_2(\mathbf{Z}_l) \;\middle|\; \det x \in \overline{\Pi} \right\} \Big/ \pm \overline{\Pi},$$

where $\overline{\Pi}$ is the topological closure of Π in $\prod_{l \neq p} U_l$. Put

$$\widetilde{X} = \left\{ \prod_{l \neq p} GL_2(\mathbf{Z}_l) \right\} \Big/ \pm \overline{\Pi},$$

so that $\Gamma^* \underset{dense}{\subset} X \subset \widetilde{X}$. Let $P_z, P_{z'}$ be two elements of $\wp(\Gamma^*)$ not equal to P_i or P_ω ($i = \sqrt{-1}$, $\omega = \frac{1}{2}(-1 + \sqrt{-3})$), and let γ resp. γ' be the positive generator of Γ_z^* resp. $\Gamma_{z'}^*$ (w.r.t. $\mathfrak{p}$;

[33] $\mathbf{Z}^{(p)}$-lattice $\mathfrak{a}$ is a *proper* O-ideal if and only if the order of $\mathfrak{a}$ *coincides* with O.

see §23). Then

$$\text{(i)}\ \{\gamma\}_{\Gamma^*} = \{\gamma'\}_{\Gamma^*} \longleftrightarrow P_z = P_{z'},$$
$$\text{(ii)}\ \{\gamma\}_X = \{\gamma'\}_X \longleftrightarrow P_z \approx P_{z'},$$
$$\text{(iii)}\ \{\gamma\}_{\overline{X}} = \{\gamma'\}_{\overline{X}} \longleftrightarrow P_z \sim P_{z'}.$$

Moreover, $P_z \sim P_{z'}$ *implies* $\operatorname{Deg} P_z = \operatorname{Deg} P_{z'}$.

PROOF. Put $\mathfrak{a} = [z, 1]_{\mathbf{Z}^{(p)}}$, $\mathfrak{a}' = [z', 1]_{\mathbf{Z}^{(p)}}$, and let O resp. O' be the $\mathbf{Z}^{(p)}$-orders of $\mathfrak{a}$ resp. $\mathfrak{a}'$. For each prime number $l \neq p$, a quadratic field Ω, and a $\mathbf{Z}^{(p)}$-lattice $\mathfrak{a}$, we put $\Omega_l = \Omega \otimes_{\mathbf{Q}} \mathbf{Q}_l$ and $\mathfrak{a}_l = \mathfrak{a} \otimes_{\mathbf{Z}^{(p)}} \mathbf{Z}_l$. For each $a \in \Omega$ (or Ω_l), $\overline{a}$ will denote its conjugation over $\mathbf{Q}$ (or $\mathbf{Q}_l$).

(i) Trivial.

(iii) $\rightarrow$: Let $\widetilde{\gamma} \in GL_2(\mathbf{Z}^{(p)})$ be any representative of γ modulo $\pm\Pi$. Then from $\{\gamma'\}_{\overline{X}} = \{\gamma\}_{\overline{X}}$ follows easily that there is a representative $\widetilde{\gamma}' \in GL_2(\mathbf{Z}^{(p)})$ of γ', and $x = (x_l)_{l \neq p} \in \prod_{l \neq p} GL_2(\mathbf{Z}_l)$ such that $\widetilde{\gamma}' = x^{-1}\widetilde{\gamma}x$. Put $\widetilde{\gamma}\begin{pmatrix} z \\ 1 \end{pmatrix} = \pi\begin{pmatrix} z \\ 1 \end{pmatrix}$, $\widetilde{\gamma}'\begin{pmatrix} z' \\ 1 \end{pmatrix} = \pi'\begin{pmatrix} z' \\ 1 \end{pmatrix}$. Then since $\widetilde{\gamma}$ and $\widetilde{\gamma}'$ are conjugate, we have $\{\pi, \overline{\pi}\} = \{\pi', \overline{\pi}'\}$, and since γ, γ' are positive (w.r.t. $\mathfrak{p}$), we have $\operatorname{ord}_{\mathfrak{p}} \pi > \operatorname{ord}_{\mathfrak{p}} \overline{\pi}$ and $\operatorname{ord}_{\mathfrak{p}} \pi' > \operatorname{ord}_{\mathfrak{p}} \overline{\pi}'$. Therefore, $\pi' = \pi$. Put $\Omega = \mathbf{Q}(\pi)$ $(= \mathbf{Q}(z) = \mathbf{Q}(z'))$. Then, in Ω_l, we have two equalities $\widetilde{\gamma}\begin{pmatrix} z \\ 1 \end{pmatrix} = \pi\begin{pmatrix} z \\ 1 \end{pmatrix}$ and $\widetilde{\gamma}x_l\begin{pmatrix} z' \\ 1 \end{pmatrix} = \pi x_l\begin{pmatrix} z' \\ 1 \end{pmatrix}$; hence we have $x_l\begin{pmatrix} z' \\ 1 \end{pmatrix} = \alpha_l\begin{pmatrix} z \\ 1 \end{pmatrix}$ with some $\alpha_l \in \Omega_l$. But since $x_l \in GL_2(\mathbf{Z}_l)$, this implies $\mathfrak{a}'_l = \alpha_l\mathfrak{a}_l$; hence $O'_l = O_l$ for all $l \neq p$; which implies $O' = O$, i.e., $P_{z'} \sim P_z$.

(ii) $\rightarrow$: In this case, we can assume that $\det x \in \overline{\Pi}$. But since $\overline{\Pi} = \overline{\Pi}^2 \cup p\overline{\Pi}^2$, we can assume further that $\det x = p^n$ ($n = 0$ or 1). Now, from $x_l\begin{pmatrix} z' \\ 1 \end{pmatrix} = \alpha_l\begin{pmatrix} z \\ 1 \end{pmatrix}$ follows $x_l\begin{pmatrix} z' & \overline{z}' \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} \alpha_l z & \overline{\alpha_l z} \\ \alpha_l & \overline{\alpha_l} \end{pmatrix}$; hence by taking the determinants, we obtain $p^n\frac{z'-\overline{z}'}{z-\overline{z}} = N(\alpha_l)$. Put $c = p^n\frac{z'-\overline{z}'}{z-\overline{z}}$. Then $c \in \mathbf{Q}$, and *locally,* c is a norm of an element of Ω. In fact, $c = N(\alpha_l)$ for $l \neq p$, and c is also a norm at p and ∞ since $\left(\frac{\Omega}{p}\right) = 1$ and $c > 0$ (by $\operatorname{Im} z$, $\operatorname{Im} z' > 0$). Therefore,[34] $c = N(\alpha)$ with some $\alpha \in \Omega$. Now since $N(\alpha_l\alpha^{-1}) = 1$, we can choose $\beta_l \in \Omega_l$ ($l \neq p$) such that $\alpha_l\alpha^{-1} = \beta_l\overline{\beta}_l^{-1}$ holds for all $l \neq p$ and that $\beta_l O_l = O_l$ holds for almost all l. Let $\mathfrak{b}$ be the unique proper O-ideal such that $\mathfrak{b}_l = \beta_l O_l$ for all $l \neq p$. Then by $x_l\begin{pmatrix} z' \\ 1 \end{pmatrix} = \alpha_l\begin{pmatrix} z \\ 1 \end{pmatrix}$, we obtain $\mathfrak{a}'_l = (\alpha\mathfrak{a}\mathfrak{b}\overline{\mathfrak{b}}^{-1})_l$ for all $l \neq p$; hence $\mathfrak{a}' = \alpha\mathfrak{a}\mathfrak{b}\overline{\mathfrak{b}}^{-1}$; hence $\mathfrak{a}'\mathfrak{a}^{-1} = \alpha N(\mathfrak{b})^{-1} \cdot \mathfrak{b}^2$. Since $N(\mathfrak{b}) = \mathfrak{b}\overline{\mathfrak{b}}$ is a principal O-ideal,[35] this implies $P_{z'} \approx P_z$.

(iii) $\leftarrow$: An essential point in this proof is the fact that all proper O-ideals $\mathfrak{a}$ are *locally principal* (i.e., $\mathfrak{a}_l = \alpha_l O_l$ ($\alpha_l \in \Omega_l$) holds for each $l \neq p$). This fact is proved in [17], p.272. Now by assumption, we have $O' = O$. Let O_1 be the maximal $\mathbf{Z}$-order of $\Omega = \mathbf{Q}(z)$ $(= \mathbf{Q}(z'))$, and put $O_0 = O \cap O_1$. Further, put $\mathfrak{p}_0 = \mathfrak{p} \cap O_0$, and let d be the smallest

[34] As is well-known, this "Normensatz" holds for all cyclic extensions.

[35] In fact, we have $\mathfrak{b}\overline{\mathfrak{b}} = bO$, where $b = (O : \mathfrak{b})$ (this "group index" is well-defined naturally even if $\mathfrak{b} \not\subset O$). This is checked easily by using the fact that every proper O-ideal is locally principal (see (iii) $\leftarrow$: below).

positive integer such that $\mathfrak{p}_0^d$ is principal (O_0-ideal). Put $\mathfrak{p}_0^d = \pi O_0$. Then it is easily seen that $\operatorname{Deg} P_z = \operatorname{Deg} P_{z'} = d$ (*this settles the last point of Prop. 8*), and that there exist representatives $\widetilde{\gamma}, \widetilde{\gamma}' \in GL_2(\mathbf{Z}^{(p)})$ of γ, γ' such that $\widetilde{\gamma}\begin{pmatrix} z \\ 1 \end{pmatrix} = \pi\begin{pmatrix} z \\ 1 \end{pmatrix}$ and $\widetilde{\gamma}'\begin{pmatrix} z' \\ 1 \end{pmatrix} = \pi\begin{pmatrix} z' \\ 1 \end{pmatrix}$. On the other hand, since both $\mathfrak{a}, \mathfrak{a}'$ are proper O-ideals, the above remark shows that $\mathfrak{a}_l' = \alpha_l \mathfrak{a}_l$ ($\alpha_l \in \Omega_l$) for each $l \neq p$. Therefore, $\alpha_l\begin{pmatrix} z \\ 1 \end{pmatrix} = x_l\begin{pmatrix} z' \\ 1 \end{pmatrix}$ holds with some $x_l \in GL_2(\mathbf{Z}_l)$. Hence $(x_l\widetilde{\gamma}'x_l^{-1})\begin{pmatrix} z \\ 1 \end{pmatrix} = \pi\begin{pmatrix} z \\ 1 \end{pmatrix}$; hence $\widetilde{\gamma} = x_l\widetilde{\gamma}'x_l^{-1}$ for all $l \neq p$; hence $\{\gamma\}_{\widetilde{X}} = \{\gamma'\}_{\widetilde{X}}$.

(ii) $\leftarrow$: In this case, we have $\mathfrak{a}' = \alpha\mathfrak{b}\overline{\mathfrak{b}}^{-1}\mathfrak{a}$ with some $\alpha \in \Omega$ and some proper O-ideal $\mathfrak{b}$. Put $\mathfrak{b}_l = \beta_l O_l$ ($l \neq p$), so that we can take $\alpha_l = \alpha\beta_l\overline{\beta_l}^{-1}$. Since $\alpha_l\begin{pmatrix} z \\ 1 \end{pmatrix} = x_l\begin{pmatrix} z' \\ 1 \end{pmatrix}$, we obtain $\det(x_l) = N(\alpha_l)\frac{z-\bar{z}}{z'-\bar{z}'} = N(\alpha_l)([z,1]_{\mathbf{Z}} : [z':1]_{\mathbf{Z}})^{36} = N(\alpha_l)([z,1]_{\mathbf{Z}^{(p)}} : [z':1]_{\mathbf{Z}^{(p)}}) \times p^n = N(\alpha)N(\mathfrak{a})N(\mathfrak{a}')^{-1}p^n = p^n$ with some positive integer n (independent of l). Hence $\{\gamma\}_X = \{\gamma'\}_X$.

This completes the proof of Proposition 8. □

Example . Let $p = 2$. Then the table of O_P for all $P \in \wp(\Gamma^*)$ with $\operatorname{Deg} P \leq 7$ is given as follows. Here, the multiplicity indicates the number of P having the same O_P (i.e., the cardinality of the corresponding $\sim$-class), and each block indicates the $\approx$-class. Thus, when the discriminant of O_P is -431 or -503, the three elements of $\wp(\Gamma^*)$ belonging to the corresponding $\sim$-class are also $\approx$-equivalent, but all other P (with $\deg P \leq 7$) form single $\approx$-classes.

(100)

<table>
<tr><td>Deg P</td><td colspan="11">(−1)× (Discriminant[37] of $O_{\mathfrak{p}}$)</td></tr>
<tr><td>1</td><td>7</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>15</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>3</td><td>23</td><td>31</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>4</td><td>$3^2 \cdot 7$</td><td>39</td><td>55</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">47</td><td rowspan="2">79</td><td rowspan="2">103</td><td>119</td><td rowspan="2">127</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>119</td></tr>
<tr><td rowspan="2">6</td><td rowspan="2">$5^2 \cdot 7$</td><td rowspan="2">$3^2 \cdot 15$</td><td rowspan="2">$3^2 \cdot 23$</td><td rowspan="2">87</td><td>231</td><td rowspan="2">247</td><td>255</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>231</td><td>255</td></tr>
<tr><td rowspan="2">7</td><td rowspan="2">$7^2 \cdot 7$</td><td rowspan="2">71</td><td rowspan="2">151</td><td rowspan="2">223</td><td>287</td><td>391</td><td rowspan="2">431
431
431</td><td rowspan="2">463</td><td rowspan="2">487</td><td rowspan="2">503
503
503</td><td>511</td></tr>
<tr><td>287</td><td>391</td><td>511</td></tr>
</table>

Remark 2. By Proposition 8, we can give examples of elements of Γ^* which are not conjugate in Γ^* but are conjugate in all finite factor groups of Γ^*.[38] For example, let $p = 2$ and take three P with

$$O_P = \left[1, \frac{1}{2}(1 + \sqrt{-431})\right]_{\mathbf{Z}^{(p)}}.$$

[36]"Generalized group index". It is clear how to define $(\mathfrak{a} : \mathfrak{a}')$ when $\mathfrak{a} \not\supset \mathfrak{a}'$, since they are commensurable.

[37]I.e., $-f^2 \cdot d$, where $-d$ is the discriminant of the quadratic field Ω, and f is the conductor of O_P (taken $f \not\equiv 0 \pmod{p}$).

[38]By Mennicke [23], all non-trivial factor groups of Γ^* are finite.

Then they are $P_z, P_{z'}, P_{z''}$ with $z = \frac{1}{2}(1+\sqrt{-431}), z' = \frac{1}{6}(1+\sqrt{-431})$ and $z'' = \frac{1}{6}(1-\sqrt{-431})$; and we have $\pi = \frac{1}{2}(9 \pm \sqrt{-431})$. Here the sign $\pm$ depends on $\mathfrak{p}$. Take $\mathfrak{p}$ such that it is (say) $+$. Then by putting $\pi\begin{pmatrix} z \\ 1 \end{pmatrix} = \gamma\begin{pmatrix} z \\ 1 \end{pmatrix}, \pi\begin{pmatrix} z' \\ 1 \end{pmatrix} = \gamma'\begin{pmatrix} z' \\ 1 \end{pmatrix}, \pi\begin{pmatrix} z'' \\ 1 \end{pmatrix} = \gamma''\begin{pmatrix} z'' \\ 1 \end{pmatrix}$, we obtain three elements $\gamma, \gamma', \gamma''$ of Γ^* which are not conjugate in Γ^* but are conjugate in X (and hence in all finite factor groups of Γ^*). They are:

$$(101) \qquad \begin{pmatrix} 5 & -108 \\ 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} 5 & -36 \\ 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 4 & 36 \\ -3 & 5 \end{pmatrix}.$$

This is an example for small p ($p = 2$) but large Degree ($\operatorname{Deg} P_z = 7$). An example of Degree one is obtained e.g., from the case $p = 59$; namely, for this p, the following three elements have the same properties in Γ^* as above;

$$(102) \qquad \begin{pmatrix} 7 & -12 \\ 2 & 5 \end{pmatrix}, \quad \begin{pmatrix} 7 & -6 \\ 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 5 & -6 \\ 4 & 7 \end{pmatrix}.$$

For these, $\pi = 6 + \sqrt{-23}$, and z, z', z'' are given by $\frac{1}{2}(1+\sqrt{-23})$, $\frac{1}{4}(1+\sqrt{-23})$ and $\frac{1}{4}(-1+\sqrt{-23})$ respectively.

REMARK 3. Let $G_O^{(1)}$ be the subgroup of G_O formed of all proper O-ideal classes that contain an ideal of norm 1. Then $G_O^{(1)} \supset \{G_O\}^2$ (since $\mathfrak{a}^2$ and $\mathfrak{a}/\bar{\mathfrak{a}}$ belong to the same class), and they are equal if O is maximal. However, in general, they are different subgroups of G_O.

REMARK 4. In Proposition 8, if we replace $\Gamma^*, X, \widetilde{X}$ by $\Gamma = PSL_2(\mathbf{Z}^{(p)})$, $\left\{\prod_{l \neq p} SL_2(\mathbf{Z}_l)\right\} / \pm 1$, and $\left\{\prod_{l \neq p} GL_2(\mathbf{Z}_l)\right\} / \pm 1$ respectively, then we should add the following condition (b) to the right sides of (ii) and (iii),

(b) $\operatorname{ord}_p([z,1]_{\mathbf{Z}} : [z',1]_{\mathbf{Z}})$ is even.

As above, (:) denotes the generalized group index.

(II) Equivalence relations in $\wp(K^*)$. Let $\wp(K^*)$ be the set of all ordinary prime divisors of K^*. By the bijection $\mathcal{J}_{\mathfrak{p}}^* : \wp(\Gamma^*) \to \wp(K^*)$, we shall map the two equivalence relations $\sim$ and $\approx$ of $\wp(\Gamma^*)$ onto $\wp(K^*)$. Thus, for $\mathfrak{P}, \mathfrak{P}' \in \wp(K^*)$, we define

$$(103) \qquad \begin{aligned} \mathfrak{P} \underset{\mathfrak{p}}{\sim} \mathfrak{P}' &\longleftrightarrow \mathcal{J}_{\mathfrak{p}}^{*-1}(\mathfrak{P}) \sim \mathcal{J}_{\mathfrak{p}}^{*-1}(\mathfrak{P}'), \\ \mathfrak{P} \underset{\mathfrak{p}}{\approx} \mathfrak{P}' &\longleftrightarrow \mathcal{J}_{\mathfrak{p}}^{*-1}(\mathfrak{P}) \approx \mathcal{J}_{\mathfrak{p}}^{*-1}(\mathfrak{P}'). \end{aligned}$$

We shall show in §32 that these two relations $\underset{\mathfrak{p}}{\sim}$ and $\underset{\mathfrak{p}}{\approx}$ of $\wp(K^*)$ do not depend on the choice of $\mathfrak{p}$.

§32. Effect of changing $\mathfrak{p}$. Now we shall study the effect of changing the prime factor $\mathfrak{p}$ of p in $\mathbf{Q}^{\mathrm{a}}$. First, we shall check the following two assertions.

PROPOSITION 9. *The field $\mathfrak{K}$ of Main Theorem* (Γ^*-2) *is independent of the choice of* $\mathfrak{p}$.

PROPOSITION 10. *The two equivalence relations* $\underset{\mathfrak{p}}{\sim}$ *and* $\underset{\mathfrak{p}}{\approx}$ *of* $\wp(K^*)$ *are independent of the choice of* $\mathfrak{p}$.

PROOF OF PROPOSITION 9. By the proof of Main Theorem (Γ^*-1), it is clear that the field $\mathfrak{K}$ of Main Theorem (Γ^*-1) must coincide with the "old" field $\mathfrak{K}$ of §15, which was independent of the choice of $\mathfrak{p}$ (see the Remark in §15). □

PROOF OF PROPOSITION 10. Put $P_z = \mathcal{J}_{\mathfrak{p}}^{*-1}(\mathfrak{P})$, so that $\mathfrak{P}(\bar{j}) = j(z) \mod \mathfrak{p}$. Let O be the order of $[z,1]_{\mathbf{Z}^{(p)}}$, let O_1 be the maximal $\mathbf{Z}$-order of $\Omega = \mathbf{Q}(z)$, and put $O_0 = O \cap O_1$ (so that $O = O_0 \otimes_{\mathbf{Z}} \mathbf{Z}^{(p)}$). Then since $O = \mathrm{End}(\mathbf{C}/[z,1]) \otimes_{\mathbf{Z}} \mathbf{Z}^{(p)}$, it follows immediately from Deuring [4] that $\mathrm{End}(E_{\mathfrak{P}(\bar{j})}) = O_0$, where $E_{\mathfrak{P}(\bar{j})}$ is an elliptic curve with the absolute invariant $\mathfrak{P}(\bar{j})$. Therefore,

$$\mathfrak{P} \underset{\mathfrak{p}}{\sim} \mathfrak{P}' \longleftrightarrow \mathrm{End}(E_{\mathfrak{P}(\bar{j})}) = \mathrm{End}(E_{\mathfrak{P}'(\bar{j})}). \tag{104}$$

But this implies that $\underset{\mathfrak{p}}{\sim}$ does not depend on $\mathfrak{p}$.

On the other hand, by Main Theorem (Γ^*-2) and Proposition 8, if we denote by $\left\{\frac{\mathfrak{K}/K^*}{\mathfrak{P}}\right\}$ the Frobenius substitution of $\mathfrak{P}$ in $\mathfrak{K}/K^*$ (thus it is a $G(\mathfrak{K}/K^*)$-conjugacy class);[39] we have

$$\mathfrak{P} \underset{\mathfrak{p}}{\approx} \mathfrak{P}' \longleftrightarrow \left\{\frac{\mathfrak{K}/K^*}{\mathfrak{P}}\right\} = \left\{\frac{\mathfrak{K}/K^*}{\mathfrak{P}'}\right\}. \tag{105}$$

Therefore, by Proposition 9, $\underset{\mathfrak{p}}{\approx}$ does not depend on $\mathfrak{p}$. □

In view of Proposition 10, we shall simply denote $\sim, \approx$ instead of $\underset{\mathfrak{p}}{\sim}, \underset{\mathfrak{p}}{\approx}$. Thus, for each $\mathfrak{p}$, $\mathcal{J}_{\mathfrak{p}}^*$ induces the bijections $\wp(\Gamma^*)/\sim \to \wp(K^*)/\sim$ and $\wp(\Gamma^*)/\approx \to \wp(K^*)/\approx$.

PROPOSITION 11. *The induced bijection* $\wp(\Gamma^*)/\sim \to \wp(K^*)/\sim$ *is independent of* $\mathfrak{p}$.

PROOF. This is clear by the proof of Proposition 10. □

On the other hand, the bijection $\wp(\Gamma^*)/\approx \to \wp(K^*)/\approx$ actually depends on $\mathfrak{p}$. To see how it depends, let F be the maximum $(2,2,\cdots)$-type abelian extension of $\mathbf{Q}$ in which p is decomposed completely. Then F is contained in $\mathbf{Q}' = \bigcup_{n \not\equiv 0 \pmod p} \mathbf{Q}(\zeta_n)$ (ζ_n : primitive n-th root of unity), and the canonical isomorphism $G(\mathbf{Q}'/\mathbf{Q}) \cong \prod_{l \neq p} U_l$ induces the isomorphism $G(F/\mathbf{Q}) \cong \left(\prod_{l\neq p} U_l\right) / \left(\prod_{l \neq p} U_l^2\right) \cdot \overline{\Pi}$. On the other hand, if X and $\widetilde{X}$ are as in Proposition 8, then the determinant map induces an isomorphism $\widetilde{X}/X \cdot \left(\text{center of } \widetilde{X}\right) \cong \left(\prod_{l\neq p} U_l\right) / \left(\prod_{l\neq p} U_l^2\right) \cdot \overline{\Pi}$. Therefore, there is a natural isomorphism

$$\widetilde{X}/X \cdot \left(\text{center of } \widetilde{X}\right) \cong G(F/\mathbf{Q}). \tag{106}$$

Now, for each $\sigma \in G(\mathbf{Q}^a/\mathbf{Q})$, identify $\mathcal{J}^*_{\mathfrak{p}^{\sigma^{-1}}}$ with the map $z \to j(z)^\sigma \mod \mathfrak{p}$, and let $\widetilde{x}_\sigma$ be any element of $\widetilde{X}$ whose residue class mod $\left\{X \cdot \left(\text{center of } \widetilde{X}\right)\right\}$ corresponds to $\sigma|_F$ by the above isomorphism (106). Then we have the following:

[39] If $\mathfrak{P}(\bar{j}) = 12^3$ or 0, the inertia group is non-trivial, and hence $\left\{\frac{\mathfrak{K}/K^*}{\mathfrak{P}}\right\}$ is not a single $G(\mathfrak{K}/K^*)$-conjugacy class. But such $\mathfrak{P}$ are not $\underset{\mathfrak{p}}{\sim}$ or $\underset{\mathfrak{p}}{\approx}$ equivalent to any other element; hence there is no problem.

Proposition 12. *The notations being as above, let P_z be any element of $\wp(\Gamma^*)$ not equal to P_i or P_ω, and let γ be the positive generator of Γ_z^* with respect to $\mathfrak{p}$. Let σ be any element of $G(\mathbf{Q}^a/\mathbf{Q})$, put ${\mathcal{J}_{\mathfrak{p}^\sigma}^*}^{-1}\mathcal{J}_{\mathfrak{p}}^*(P_z) = P_{z'}$, and let γ' be the positive generator of $\Gamma_{z'}^*$ with respect to $\mathfrak{p}^\sigma$.*[40] *Then*

$$\{\gamma'\}_X = \left\{\widetilde{x}_\sigma^{-1}\gamma\widetilde{x}_\sigma\right\}_X. \tag{107}$$

Proof. This is a simple exercise in (abelian) classfield theory. □

Corollary . *If $\sigma = 1$ on F, then ${\mathcal{J}_{\mathfrak{p}^\sigma}^*}^{-1}\mathcal{J}_{\mathfrak{p}}^*$ leaves each $\approx$-class invariant.*

Therefore,[41] we have proved the following:

Proposition 13. *In Main Theorem (Γ^*-2), if $\mathfrak{p}$ is replaced by $\mathfrak{p}^\sigma$ ($\sigma \in G(\mathbf{Q}^a/\mathbf{Q})$), then it is enough to replace ι by $\bar{\iota} \circ \mathrm{Inn}(\widetilde{x}_\sigma)$ to keep the validity of this theorem, where $\mathrm{Inn}(\widetilde{x}_\sigma)$ denotes the inner automorphism induced by $\widetilde{x}_\sigma$, and $\bar{\iota}$ is the isomorphism $X \cong G(\mathfrak{K}/K^*)$ induced by ι. Therefore, if Γ' is a normal subgroup of Γ^* with finite index, then the Γ'-classfield w.r.t. $\mathfrak{p}$ is the $\Gamma^* \cap \widetilde{x}_\sigma^{-1}\overline{\Gamma'}\widetilde{x}_\sigma$-classfield w.r.t. $\mathfrak{p}^\sigma$, where $\overline{\Gamma'}$ denotes the closure of Γ' in X. In particular, if $\overline{\Gamma'}$ is a characteristic subgroup of X (e.g., if Γ' is a principal congruence subgroup), then the definition of Γ'-classfield is independent of $\mathfrak{p}$.*

Remark 1. It can be immediately checked that this change of ι also keeps the validity of assertion (iii) of Main Theorem (Γ^*-2).

Remark 2. Since $\widetilde{X}/X\cdot\left(\text{center of }\widetilde{X}\right)$ is of $(2, 2, \cdots)$-type, one needs not worry about the sign of the power indices of σ or $\widetilde{x}_\sigma$.

§33. Here, we shall give some remarks and numerical evidences for Conjecture Γ^*.

Remark . For each $N \geq 1$ with $N \not\equiv 0 \pmod p$, let $\Gamma(N)$ be the principal congruence subgroup of Γ^* of level N;

$$\Gamma(N) = \left\{\gamma \in SL_2(\mathbf{Z}^{(p)}) \mid \gamma \equiv \pm 1 \pmod N\right\} / \pm 1. \tag{108}$$

Let K_N be the $\Gamma(N)$-classfield over K^*. Call a prime divisor $\mathfrak{P}$ of K_N supersingular when its restriction to K^* is so. Let $\widehat{K}_N$ be the maximum Galois extension of K_N such that

(i) $\widehat{K}_N/K_N$ is unramified,
(ii) all supersingular prime divisors of K_N are decomposed completely in $\widehat{K}_N$.

Then

(109) *Conjecture Γ^* is valid if and only if $\widehat{K}_N = K_N$ holds for all N.*

To prove (109), we need the following result of Mennicke [23]: *$\Gamma(N)$ is the smallest normal subgroup of $\Gamma = PSL_2(\mathbf{Z}^{(p)})$ containing $\begin{pmatrix}1 & N\\ 0 & 1\end{pmatrix}$.* From this, it follows directly that K_N is the maximum Galois extension of K^* such that (i) $K_N \subset \mathfrak{K}$, (ii) the ramification

[40] Since $P_z \sim P_{z'}$ by Proposition 11, $P_{z'} \neq P_i, P_\omega$.

[41] See also the Remarks 1, 2 below.

index in K_N/K^* of the infinite prime divisor of K^* divides N. Moreover, the last ramification index in K_N/K^* is exactly equal to N (by Main Theorem (Γ^*-2)). Hence it follows immediately that $\widehat{K}_N$ is the maximum Galois extension of K^* such that $\widehat{\text{(i)}}$ $\widehat{K}_N \subset \widehat{\mathfrak{K}}$, $\widehat{\text{(ii)}}$ the ramification index in $\widehat{K}_N/K^*$ of the infinite prime divisor of K^* divides N. Moreover, it is clear that $\widehat{\mathfrak{K}} = \bigcup_N \widehat{K}_N$; hence (109).

For $N \leq 5$, the genus of K_N is zero; hence $\widehat{K}_N = K_N$ $(N \leq 5)$. So, the first non-trivial example of $\widehat{K}_N = K_N$? is the case of $N = 6$, where the genus of K_N is one. Now K_6 has exactly $6(p-1)$ supersingular prime divisors, and is of degree one over $\mathbf{F}_{p^2}$. Choose any one as an origin, and let E be the corresponding elliptic curve (model of K_6). Let Δ be the group of all $\mathbf{F}_{p^2}$-rational points on E, and let $\widehat{\Delta}$ be the subgroup of Δ generated by all supersingular points on E (i.e., those points on E whose corresponding prime divisors of K_6 are supersingular). Then it is easy to see that $\widehat{K}_6$ is an abelian extension of K_6 with the Galois group isomorphic to $\Delta/\widehat{\Delta}$, and hence $\widehat{K}_6 = K_6$ *holds if and only if* $\widehat{\Delta} = \Delta$. However, the author has not tried to check this – it seems too laborious a work for large p.

Some numerical evidences. Another way of giving numerical evidences for Conjecture Γ^* is to take a finite extension K_1 of K^* in $\mathfrak{K}$ and to see whether

$$\mathfrak{K} \cap A_{K_1} = \widehat{\mathfrak{K}} \cap A_{K_1}?, \tag{110}$$

where A_{K_1} denotes the maximum *abelian* extension of K_1. Since we know one inclusion $\mathfrak{K} \cap A_{K_1} \subset \widehat{\mathfrak{K}} \cap A_{K_1}$, it is enough to compute and compare the degrees of both fields over K_1. By the abelian class field theory, it is easily shown that the degree of $\widehat{\mathfrak{K}} \cap A_{K_1}$ over K_1 is finite, and the degree can be computed if we know all supersingular prime divisors of K_1. On the other hand, if Γ_1 is the subgroup of Γ^* that corresponds to K_1, then the degree of $\mathfrak{K} \cap A_{K_1}$ over K_1 is nothing but $(\Gamma_1 : [\Gamma_1, \Gamma_1])$. Since the group Γ_1 has congruence subgroup property, this group index can be computed easily. Now we shall show the following:

Proposition 14. *If* $K_1 = \mathbf{F}_{p^2}(\bar{j})$, *then* (110) *holds, but almost trivially.*

Proof. It can be easily checked that

$$\begin{aligned} \widehat{\mathfrak{K}} \cap A_{K_1} = \mathfrak{K} \cap A_{K_1} &= \mathbf{F}_{p^2}\left(\sqrt{\bar{j} - 12^3}, \sqrt[3]{\bar{j}}\right) && \cdots\ p \neq 2, 3, \\ &= \mathbf{F}_{p^2}\left(\sqrt{\bar{j} - 12^3}\right) && \cdots\ p = 3, \\ &= \mathbf{F}_{p^2}\left(\sqrt[3]{\bar{j}}\right) && \cdots\ p = 2. \end{aligned} \tag{111}$$

(In this case, supersingular prime divisors do not play essential roles. The ramification condition already determines $\widehat{\mathfrak{K}} \cap A_{K_1}$ up to constant field extensions.) A non-trivial example comes from the case $K_1 = \mathbf{F}_{p^2}(\bar{\lambda})$, as follows. □

Proposition 15. *Let* $p \neq 2$ *and* $K_1 = \mathbf{F}_{p^2}(\bar{\lambda})$. *Put*

$$\begin{cases} \Delta = \left\{ (x, y) \in \mathbf{F}_{p^2}^{\times} \times \mathbf{F}_{p^2}^{\times} \;\middle|\; (xy)^{\frac{p^2-1}{3}} \overset{42}{=} x^{\frac{p^2-1}{8}} = y^{\frac{p^2-1}{8}} = 1 \right\} \\ \widehat{\Delta} = \text{the subgroup of } \mathbf{F}_{p^2}^{\times} \times \mathbf{F}_{p^2}^{\times} \text{ generated multiplicatively} \\ \qquad \text{by all elements of the form } \left(\frac{b}{a}, \frac{b-1}{a-1}\right), \text{ where } a, b \\ \qquad \text{run over all supersingular } \bar{\lambda}_0. \end{cases} \tag{112}$$

Then

(i) $\widehat{\Delta} \subset \Delta$,

(ii) *the Galois group* $G\left(\widehat{\mathfrak{R}} \cap A_{K_1}/K_1\right)$ *is isomorphic to* $\mathbf{F}_{p^2}^{\times} \times \mathbf{F}_{p^2}^{\times}/\widehat{\Delta}$, *and the fixed field of* $\Delta/\widehat{\Delta}$ *is* $\mathfrak{R} \cap A_{K_1}$*;*

(iii) *the field* $\mathfrak{R} \cap A_{K_1}$ *is given explicitly as:*

$$\mathfrak{R} \cap A_{K_1} = \mathbf{F}_{p^2}\left(\sqrt[8]{-\bar{\lambda}},\ \sqrt[8]{\bar{\lambda}-1},\ \sqrt[3]{\frac{1}{2}\bar{\lambda}(1-\bar{\lambda})}\ ^{[43]}\right). \tag{113}$$

In particular, (110) *holds for* $K_1 = \mathbf{F}_{p^2}(\bar{\lambda})$ *if and only if* $\widehat{\Delta} = \Delta$.

$$\begin{array}{llcc}
 & \widehat{\mathfrak{R}} \cap A_{K_1} & \cdots & \{1\} \\
 & \quad | & & | \\
(114) & \mathfrak{R} \cap A_{K_1} = \mathbf{F}_{p^2}\left(\sqrt[8]{-\bar{\lambda}},\ \sqrt[8]{\bar{\lambda}-1},\ \sqrt[3]{\tfrac{1}{2}\bar{\lambda}(1-\bar{\lambda})}\ ^{[44]}\right) & \cdots & \Delta/\widehat{\Delta} \\
 & \quad | & & | \\
 & K_1 = \mathbf{F}_{p^2}\left(\bar{\lambda}\right) & \cdots & \left(\mathbf{F}_{p^2}^{\times} \times \mathbf{F}_{p^2}^{\times}\right)/\widehat{\Delta}
\end{array}$$

COROLLARY . *Let* S_λ *be the set of all supersingular elements* $\bar{\lambda}_0$ *(see Remark 2 §30), and let* $a \in S_\lambda$*. Then* $-a, a-1$ *are* 8*-th powers, and*[44] $\frac{1}{2}a(1-a)$ *is a 3rd power in* $\mathbf{F}_{p^2}$.

Now by Proposition 15, we can check the validity of (110) for various p by the direct computation of $\widehat{\Delta}$, after the preparation of making S_λ's table.[45] For example, if $p = 3$, then $S_\lambda = \{-1\}$; hence $\widehat{\Delta} = \{1\} = \Delta$. If $p = 5$, then $S_\lambda = \{-\omega, -\omega^2\}$; hence $\widehat{\Delta} = \{(1,1), (\omega, \omega^2), (\omega^2, \omega)\} = \Delta$. In the same manner, we can check (110) (for $K_1 = \mathbf{F}_{p^2}(\bar{\lambda})$) for all $p \leq 41$.

[42] If $p = 3$, the equality (or element) should be taken away.

[43] If $p = 3$, this equality (or element) should be taken away.

[44] Only for $p \neq 3$

[45] It is convenient to use Deuring's table of supersingular $\bar{j}_0$ to make the table of S_λ.