CHAPTER 5

Part 1. Elliptic modular functions mod p and $\Gamma = PSL_2(\mathbf{Z}^{(p)})$.

Our purpose in Part 1 of this chapter is to formulate and prove a fundamental relation between the classes mod $\mathfrak{P}$ ($\mathfrak{P}|p$) of the special values of elliptic modular functions $J(z)$ and the group $\Gamma = PSL_2(\mathbf{Z}^{(p)})$ (Theorems 1, 1′; §5). This is a fruit of

(i) Deuring' s work on complex multiplication of elliptic curves [4] [6] [7],
(ii) a new standpoint.

Roughly speaking, (ii) is of:
"A fixed p and variable imaginary quadratic fields and lattices",
instead of "a fixed imaginary quadratic field and variable p", which was the standpoint of classical complex multiplication theory. However, besides this new standpoint, nothing more is to be added to Deuring' s work. In fact, the proof of Theorems 1, 1′ based on Deuring's results is quite elementary.

As described in [**18**], our Theorems 1, 1′ give a starting point of our problems. Generalizations to congruence subgroups of Γ (announced in §10) will be given in Part 2 of this chapter.

Elliptic modular functions mod p and $\Gamma = PSL_2(\mathbf{Z}^{(p)})$.

§1. Throughout this chapter, p is a fixed prime number and Π is the cyclic subgroup of $\mathbf{Q}^\times$ generated by p. Put $\mathbf{Z}^{(p)} = \Pi \cdot \mathbf{Z} = \cup_{n=0}^{\infty} p^{-n}\mathbf{Z}$, and put

(1) $$\Gamma = PSL_2(\mathbf{Z}^{(p)}).$$

It is a discrete subgroup of

$$G = G_{\mathbf{R}} \times G_p = PSL_2(\mathbf{R}) \times PSL_2(\mathbf{Q}_p).$$

We already know that the quotient G/Γ has finite invariant volume and that $\Gamma_{\mathbf{R}}, \Gamma_p$ are dense in $G_{\mathbf{R}}, G_p$ respectively (see Chapter 1, §1, §2). Put

(1*) $$\Gamma^* = \{x \in GL_2(\mathbf{Z}^{(p)}) | \det x \in \Pi\} / \pm \Pi.$$

Then this is a discrete subgroup of $G^* = G_{\mathbf{R}} \times G_p^*$, where

(2) $$G_p^* = \{x \in GL_2(\mathbf{Q}_p) | \det x \in \Pi\}/ \pm \Pi.$$

Since Γ is isomorphic to $\{x \in GL_2(\mathbf{Z}^{(p)}) \mid \det x \in \Pi^2\}/ \pm \Pi$, Γ can be considered as a subgroup of Γ^* of index two, and in the same manner, G_p and G can be considered as subgroups of G_p^* and G^* respectively with index two. So, it is clear that G^*/Γ^* has finite invariant volume, the projections $\Gamma_{\mathbf{R}}^*$, Γ_p^* of Γ^* are dense in $G_{\mathbf{R}}, G_p^*$ respectively, and that $\Gamma^* \cap G = \Gamma$.

§2. $\wp(\Gamma)$ and $\wp(\Gamma^*)$. Now let $\wp(\Gamma)$ be as in §3 of Chapter 1. So, it is the set of all Γ-equivalence classes of all Γ-fixed points on $\mathfrak{H} = \{z \in \mathbf{C} | \operatorname{Im} z > 0\}$. Recall that a point $z \in \mathfrak{H}$ is called a Γ -fixed point if its stabilizer in Γ (identified with $\Gamma_{\mathbf{R}}$) is *infinite*. Since $\Gamma^* \cong \Gamma_{\mathbf{R}}^* \subset G_{\mathbf{R}}$, this definition also carries over at once to the group Γ^*;

(3) $$\wp(\Gamma^*) = \{\Gamma^*\text{-fixed points on } \mathfrak{H}\}/\Gamma^*\text{-equivalence}.$$

Note that a point $z \in \mathfrak{H}$ is a Γ^*-fixed point if and only if it is a Γ-fixed point. In fact, if the stabilizer Γ_z^* of $z \in \mathfrak{H}$ in Γ^* is infinite, then $\Gamma_z = \Gamma \cap \Gamma_z^*$ is also infinite, for $(\Gamma_z^* : \Gamma_z) \leq (\Gamma^* : \Gamma) = 2$. It is also easy to see that if z is a Γ^*-fixed point, then the Γ^*-equivalence class containing z consists of either one or two Γ-equivalence classes, and that it is the latter if and only if Γ_z^* is contained in Γ. Such relations will be expressed as:

(4) $$\wp(\Gamma^*) \ni P^* \Rightarrow \begin{cases} P^* = P; & P \in \wp(\Gamma) \\ \quad \text{or} & \\ P^* = P_1 P_2; & P_1, P_2 \in \wp(\Gamma), P_1 \neq P_2. \end{cases}$$

(Such relations between $\wp(\Gamma^*)$ and $\wp(\Gamma')$ for normal subgroups Γ' of Γ^* with nonabelian quotients, and their arithmetic meanings will be the main subject of our study in Part 2 of this chapter.)

§3. Let $P^* \in \wp(\Gamma^*)$ and let z be a Γ^*-fixed point contained in the class P^*. Let Γ_z^* be the stabilizer of z in Γ^*. Then the argument of §4 of Chapter 1 can be applied to Γ_z^*, which asserts that $\Gamma_{z,p}^*$ is an infinite discrete abelian subgroup of G_p^* and that there exists $x \in G_p^*$ such that $x^{-1}\Gamma_{z,p}^* x \subset T_p^*$, where T_p^* is the diagonal subgroup of G_p^*. For each $\gamma^* \in \Gamma_z^*$, put $x^{-1}\gamma_p^* x = \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix}$ and $t = t_1 t_2^{-1} \in \mathbf{Q}_p^\times$. Then the map $\gamma^* \mapsto \operatorname{ord}_p t$ is a homomorphism of Γ_z^* into $\mathbf{Z}$, and since $\Gamma_{z,p}^*$ is infinite and discrete in G_p^*, the image of this homomorphism is not $\{0\}$. Denote the image by $a\mathbf{Z}$ ($a > 0$) and the kernel by Γ_z^{*0}. Then, since $\Gamma_{\gamma^* z}^* = \gamma^* \Gamma_z^* \gamma^{*-1}$ holds for all $\gamma^* \in \Gamma^*$ and since $t_1 : t_2$ is the ratio of two eigenvalues of γ_p^* for every $\gamma^* \in \Gamma_z^*$, the positive integer a is independent of the choice of z. So, we shall denote it by $\operatorname{Deg} P^*$. Also, for each $\gamma^* \in \Gamma_z^*$ we put $\operatorname{Deg} \gamma^* = |\operatorname{ord}_p t|$. Then it is clear that Γ_z^{*0} is the torsion subgroup of Γ_z^* and that $\operatorname{Deg} P^* = \operatorname{Deg} \gamma^*$ holds if γ^* is a generator of Γ_z^* modulo Γ_z^{*0}. Now recall Chapter 1 (§4, §5) for the definition of $\deg P$ ($P \in \wp(\Gamma)$). Then we can check easily that

$$(5) \qquad \operatorname{Deg} P^* = \begin{cases} \deg P & \cdots P^* = P,\ P \in \wp(\Gamma), \\ 2 \deg P_i \ (i = 1,2) & \cdots P^* = P_1 P_2,\ P_1,\ P_2 \in \wp(\Gamma). \end{cases}$$

holds for all $P^* \in \wp(\Gamma^*)$. Moreover, $\operatorname{Deg} P^*$ is odd in the former case.

§4. Let k be an algebraically closed field. Then, for each elliptic curve E over k, a number $j \in k$ called the absolute invariant of E is defined, and the map $E \to j$ gives a one-to-one correspondence between the set of all (k-isomorphism classes of) elliptic curves over k and that of all elements of the field k. If the characteristic of k is neither 2 nor 3, then E is k-isomorphic to an elliptic curve defined by the equation $y^2 = 4x^3 - g_2 x - g_3$ ($g_2, g_3 \in k$; $g_2^3 - 27g_3^2 \neq 0$), and j is given by $j = 12^3 \frac{g_2^3}{g_2^3 - 27g_3^2}$. In the case of characteristic 2 or 3, j is also defined, and the bijectivity of the map $E \mapsto j$ is proved in M. Deuring [**5**].

Let $k = \mathbf{C}$. Then, elliptic curves over $\mathbf{C}$ are given by complex tori $\mathbf{C}/[\omega_1, \omega_2]$. For each $z \in \mathfrak{H}$, we shall denote by $J(z)$ the absolute invariant of the elliptic curve given by the torus $\mathbf{C}/[1, z]$. It is well-known that $J(z)$, called elliptic modular function, is an automorphic function with respect to $PSL_2(\mathbf{Z})$.

Now let k be of characteristic $p \neq 0$, let $\mathbf{F}_p$ be the prime field, and let $\overline{\mathbf{F}}_p$ be the algebraic closure of $\mathbf{F}_p$ (hence $\overline{\mathbf{F}}_p \subset k$). For each elliptic curve E over k, we denote by $\mathcal{A}(E)$ the endomorphism ring of E. Then, (i) if $j \notin \overline{\mathbf{F}}_p$, $\mathcal{A}(E) \cong \mathbf{Z}$; (ii) if $j \in \overline{\mathbf{F}}_p$, $\notin S$, then $\mathcal{A}(E)$ is an order of an imaginary quadratic field; (iii) if $j \in S$, then $\mathcal{A}(E)$ is a maximal order of a certain quaternion algebra over $\mathbf{Q}$. Here, S is a certain finite set contained in $\mathbf{F}_{p^2}$, and elements of S are called *supersingular* (cf. Deuring [**4**]). Put $S = S_1 \cup S_2$ with $S_1 = S \cap \mathbf{F}_p, S_2 = S - S_1 = S \cap (\mathbf{F}_{p^2} - \mathbf{F}_p)$. Then S_2 (and hence also S) is invariant by the automorphisms of $\mathbf{F}_{p^2}$ over $\mathbf{F}_p$, and we have the following formulae for the cardinalities of S and S_1 (cf. [**4**] [1]).

$$(6) \qquad |S| = \begin{cases} 1 & \cdots p = 2, 3, \\ \frac{p-1}{12}, \frac{p+7}{12}, \frac{p+5}{12}, \frac{p+13}{12} & \cdots p \equiv 1, 5, -5, -1 (\mathrm{mod}\, 12) \end{cases}$$

respectively;

$$(7) \qquad |S_1| = \begin{cases} 1 & \cdots \quad p = 2, 3, \\ \varepsilon h & \cdots \quad p \neq 2, 3; \end{cases}$$

where h is the class number of $\mathbf{Q}(\sqrt{-p})$ and $\varepsilon = 1/2, 2, 1$ for $p \equiv 1 (\mathrm{mod}\ 4), 3 (\mathrm{mod}\ 8), 7 (\mathrm{mod}\ 8)$ respectively.

§5. Now we are going to state our Theorem. We use the following notations:

$\overline{\mathbf{Q}}$: the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$.

$\overline{\mathbf{Z}}$: the ring of integers of $\overline{\mathbf{Q}}$

$\mathfrak{P}$: a prime divisor of p in $\overline{\mathbf{Q}}$, and fix an isomorphism $\overline{\mathbf{Z}}/\mathfrak{P} \cong \overline{\mathbf{F}}_p$.

[1] A table of S for $p < 100$ is given in [**4**].

$j_1 \sim j_2$ (j_1, $j_2 \in \bar{\mathbf{F}}_p$) $\leftrightarrow$ j_1, j_2 are conjugate over $\mathbf{F}_p$,
$j_1 \approx j_2$ (j_1, $j_2 \in \bar{\mathbf{F}}_p$) $\leftrightarrow$ j_1, j_2 are conjugate over $\mathbf{F}_{p^2}$,
The degree of $\sim$-class of j_1 = the degree of j_1 over $\mathbf{F}_p$, denoted by $\mathrm{Deg}\{j_1\}$,
The degree of $\approx$-class of j_2 = the degree of j_2 over $\mathbf{F}_{p^2}$, denoted by $\deg\{j_2\}$.

THEOREM 1. *Let P^* be an element of $\wp(\Gamma^*)$, and let z be a Γ^*-fixed point which defines the class P^*. Then $J(z)$ is contained in $\bar{\mathbf{Z}}$, and the map*

$$\mathcal{J}^* : P^* \mapsto J(z) \mod \mathfrak{P} \tag{8}$$

gives a one-to-one correspondence between $\wp(\Gamma^*)$ and $(\bar{\mathbf{F}}_p - S)/\sim$. Moreover,

$$\mathrm{Deg}\,\mathcal{J}^*(P^*) = \mathrm{Deg}(P^*) \tag{9}$$

holds for all $P^* \in \wp(\Gamma^*)$.

The corresponding Theorem for $\Gamma = PSL_2(\mathbf{Z}^{(p)})$ is the following:

THEOREM 1′. *Let P be an element of $\wp(\Gamma)$, and let z be a Γ-fixed point which defines the class P. Then $J(z)$ is contained in $\bar{\mathbf{Z}}$, and the map*

$$\mathcal{J} : P \to J(z) \mod \mathfrak{P} \tag{8′}$$

gives a one-to-one correspondence between $\wp(\Gamma)$ and $(\bar{\mathbf{F}}_p - S)/\approx$.
Moreover,

$$\deg \mathcal{J}(P) \doteq \deg P \tag{9′}$$

holds for all $P \in \wp(\Gamma)$.

These results are entirely based on the theory of complex multiplication of elliptic curves mainly by M. Deuring [4] [6] [7]. So, before the proof, we shall give a summary of the main results of Deuring.

Deuring's results.[2]

§6. Let Q' be an imaginary quadratic field. Then, a lattice $\mathfrak{A}$ in Q' is a free $\mathbf{Z}$-module in Q' with rank two, and two lattices $\mathfrak{A}$, $\mathfrak{A}'$ are equivalent (or belong to the same class) if $\mathfrak{A}' = \rho\mathfrak{A}$ holds with some $\rho \in Q'^{\times}$. An order O in Q' is a subring of Q' containing 1 which is at the same time a lattice in Q'. The ring of all algebraic integers is an order, denoted by O_1. Then all orders O are contained in O_1, and for every positive integer f, there is one and only one order O such that $(O_1 : O) = f$. So, $O \leftrightarrow f$ is one-to-one. We shall denote as $O = O_f$ and call f the conductor of O. If $\mathfrak{A}$ is a lattice, then $O_{\mathfrak{A}} = \{x \in Q' | x\mathfrak{A} \subset \mathfrak{A}\}$ is an order, called the order of $\mathfrak{A}$. In this case, $\mathfrak{A}$ is called a proper $O_{\mathfrak{A}}$-ideal. It is clear

[2] Cf. [4] for H. Hasse's contribution which precedes Deuring's.

that equivalent lattices have a common order. Given an order O, the set of all proper O-ideal classes form a finite multiplicative group, denoted by G_O. Therefore, we have the following one-to-one correspondence:

$$\text{All lattice classes in } Q' \underset{1:1}{\longleftrightarrow} \bigcup_{f=1}^{\infty} G_{O_f}. \tag{10}$$

§7. Let $O = O_f$ be an order of an imaginary quadratic field Q'. By $\left(\frac{O}{p}\right) = 1$, we mean that both $\left(\frac{Q'}{p}\right) = 1$ and $f \not\equiv 0 \pmod p$ hold;

$$\left(\frac{O}{p}\right) = 1 \longleftrightarrow \begin{cases} \left(\frac{Q'}{p}\right) = 1, \text{ and} \\ f \not\equiv 0 \pmod{p}. \end{cases} \tag{11}$$

For each O with $\left(\frac{O}{p}\right) = 1$, put $\mathfrak{p} = \mathfrak{P} \cap Q'$ and $\mathfrak{p}_O = \mathfrak{p} \cap O$, where $\mathfrak{P}$ is the fixed prime divisor of p in $\overline{\mathbf{Q}}$. Denote by $\{\mathfrak{p}_O\}$ the class of $\mathfrak{p}_O$ in G_O, by P_O the cyclic subgroup of G_O generated by $\{\mathfrak{p}_O\}$, and by d_O the number of elements of P_O;

$$G_O \supset P_O = \{\, \{O\}, \{\mathfrak{p}_O\}, \cdots, \{\mathfrak{p}_O^{d_O - 1}\}\,\}. \tag{12}$$

Finally, for any lattice $\mathfrak{A}$ in any imaginary quadratic field, we denote by $j(\mathfrak{A})$ the absolute invariant of the elliptic curve given by the complex torus $\mathbf{C}/\mathfrak{A}$. Then it is well-known that $j(\mathfrak{A}) \in \overline{\mathbf{Z}}$. Now, denoting by $\tilde{j}(\mathfrak{A})$ the element of $\overline{\mathbf{F}}_p$ ($\cong \overline{\mathbf{Z}}/\mathfrak{P}$) defined by $j(\mathfrak{A}) \mod \mathfrak{P}$, we can formulate a main result of Deuring [6] [7] as follows:

Theorem D (M. Deuring). *Let O run over all orders of all imaginary quadratic fields such that $\left(\frac{O}{p}\right) = 1$. Then the map*

$$\{\mathfrak{A}\} \to \tilde{j}(\mathfrak{A}) \tag{13}$$

gives a one-to-one correspondence between $\bigcup_{\left(\frac{O}{p}\right)=1} G_O$ and $\overline{\mathbf{F}}_p - S$.

Remark 1. Deuring has also proved that if $\mathfrak{A}$ is a lattice in Q' such that $\left(\frac{Q'}{p}\right) \neq 1$, then $\tilde{j}(\mathfrak{A}) \in S$ (cf. [4]).

Moreover, by the congruence relation for the modular equation of degree p, we have the following Theorem (cf. e.g., [4]).

Theorem C. *Let $\mathfrak{A}$ be a lattice in an imaginary quadratic field, and let $\mathfrak{A}'$ be another lattice contained in $\mathfrak{A}$ such that $(\mathfrak{A} : \mathfrak{A}') = p$. Then we have*

$$\tilde{j}(\mathfrak{A}') = \tilde{j}(\mathfrak{A})^{p^{\pm 1}}. \tag{14}$$

Corollary. *Let $\mathfrak{A}, \mathfrak{A}'$ be two lattices in an imaginary quadratic field such that $\mathfrak{A}' \subset \mathfrak{A}$ and $(\mathfrak{A} : \mathfrak{A}') = p^n$ with some n. Then $\tilde{j}(\mathfrak{A})$ and $\tilde{j}(\mathfrak{A}')$ are conjugate over $\mathbf{F}_p$. If moreover n is even, then they are conjugate over $\mathbf{F}_{p^2}$.*

Now, by Theorem C, if $\left(\frac{O}{p}\right) = 1$, $\{\mathfrak{A}\} \in G_O$, and $\mathfrak{A}' = \mathfrak{p}_O\mathfrak{A}$ so that $\mathfrak{A}' \subset \mathfrak{A}$ and $(\mathfrak{A} : \mathfrak{A}') = p$ hold, then $\tilde{j}(\mathfrak{p}_O\mathfrak{A}) = \tilde{j}(\mathfrak{A})^{p^{\pm 1}}$. But in such a special case, we have a more precise result, which is well-known in complex multiplication theory (cf. e.g., [7]); namely,

$$\tilde{j}(\mathfrak{p}_O\mathfrak{A}) = \tilde{j}(\mathfrak{A})^{p^{-1}}. \tag{15}$$

Therefore, by (15) and by the injectivity of the map (13), the complete set of conjugates of $\tilde{j}(\mathfrak{A})$ over $\mathbf{F}_p$ is given by

$$\tilde{j}(\mathfrak{A}), \tilde{j}(\mathfrak{p}_O\mathfrak{A}), \cdots, \tilde{j}(\mathfrak{p}_O^{d_O-1}\mathfrak{A}). \tag{16}$$

In particular, its degree over $\mathbf{F}_p$ is equal to d_O,

$$\operatorname{Deg}\tilde{j}(\mathfrak{A}) = d_O. \tag{17}$$

Remark . By the same reason, the degree of $\tilde{j}(\mathfrak{A})$ over $\mathbf{F}_{p^2}$ is the cardinality of P_O^2; hence it is equal to d_O (if d_O is odd) or to $\frac{1}{2}d_O$ (if d_O is even).

Proof of Theorems 1, 1′.

§8. Here, we shall prove Theorem 1. Then, the proof will show that Theorem 1′ is an immediate consequence of Theorem 1 and the corollary of Theorem C.

Let z be a Γ^*-fixed point. Let γ be an element of Γ_z^* of infinite order represented by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z})$, $(a, b, c, d) = 1$, $ad - bc = p^n$. Then, by the ellipticity of γ, we have $c \neq 0$, and since γ is moreover of infinite order, n cannot be 0. Hence $n > 0$. Put $\lambda = cz + d$. Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z \\ 1 \end{pmatrix} = \lambda\begin{pmatrix} z \\ 1 \end{pmatrix}$; hence λ is a quadratic integer with $N(\lambda) = p^n$. Moreover, by $\lambda = cz + d$, λ is imaginary; hence, in particular, *irrational*. Let m be a positive integer and apply this result for γ^m. Then we see that λ^m is also irrational. Therefore, λ^m is *not* of the form (a power of p) $\times$ (a root of unity), for if λ^m were of such a form, its suitable (positive integral) power must be rational. In particular, the ideal (λ^2) cannot be a power of (p). But since (λ) is integral with p-power norm, it must be of the form $(\lambda) = \mathfrak{p}^a$ *if* $\left(\frac{\mathbf{Q}(\lambda)}{p}\right) \neq 1$, where $\mathfrak{p}$ is the unique prime factor of p in $\mathbf{Q}(\lambda)$. But then, we get $(\lambda^2) = \mathfrak{p}^{2a} = (p)^a$ or $(p)^{2a}$, which is impossible. Therefore, we get $\left(\frac{\mathbf{Q}(z)}{p}\right) = \left(\frac{\mathbf{Q}(\lambda)}{p}\right) = 1$.

Now let us prove that the map $\mathcal{J}^*$ is well-defined. First, $J(z) \in \bar{\mathbf{Z}}$ is trivial, for we have $J(z) = j([1, z])$. Let $\delta \in \Gamma^*$, and put

$$\delta = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_2(\mathbf{Z}),\ AD - BC = p^r.$$

Put $z' = \delta z$. Then $J(z') = j([1, z'])$ and $[1, z'] \sim [Az + B, Cz + D] \subset [1, z]$, and the group index is p^r. Therefore, by the Corollary of Theorem C, $\tilde{j}([1, z])$ and $\tilde{j}([1, z'])$ are conjugate over $\mathbf{F}_p$. Hence $J(z) \mod \mathfrak{P} \sim J(z') \mod \mathfrak{P}$. Moreover, if $\delta \in \Gamma$, then r is even; hence we get $J(z) \mod \mathfrak{P} \approx J(z') \mod \mathfrak{P}$ by the same corollary. Now, to show that $J(z) \mod \mathfrak{P} \in \bar{\mathbf{F}}_p - S$, put $\mathfrak{A} = [1, z]$ and let $O = O_f$ be the order of $\mathfrak{A}$. Put $f = f_0 p^\nu$

with $f_0 \not\equiv 0 \pmod p$, and put $O_0 = O_{f_0}$, $\mathfrak{A}_0 = O_0\mathfrak{A}$. Then $\mathfrak{A} \subset \mathfrak{A}_0$, and $(\mathfrak{A}_0 : \mathfrak{A}) = p^\nu$. Therefore, $\bar{j}(\mathfrak{A})$ is conjugate to $\bar{j}(\mathfrak{A}_0)$ over $\mathbf{F}_p$. But since $\mathfrak{A}_0$ is a proper O_0-ideal and since $f_0 \not\equiv 0 \pmod{\underline{p}}$, we get $\bar{j}(\mathfrak{A}_0) \in \bar{\mathbf{F}}_p - S$ (Theorem D). Therefore, $J(z) \mod \mathfrak{P} = \bar{j}(\mathfrak{A})$ is contained in $\bar{\mathbf{F}}_p - S$. Therefore, the map $\mathcal{J}^*$ is well-defined.

Surjectivity of $\mathcal{J}^*$. Let $\bar{j} \in \bar{\mathbf{F}}_p - S$. Then by Theorem D, $\bar{j} = \bar{j}(\mathfrak{A})$ with some $\{\mathfrak{A}\} \in G_O$, $\left(\frac{O}{p}\right) = 1$. By multiplying some scalar to $\mathfrak{A}$, we can assume that $\mathfrak{A} = [1, z]$ with $z \in \mathfrak{H}$. Put $\mathfrak{P} \cap O = \mathfrak{p}_O$, $\mathfrak{p}_O^{d_O} = \pi_O \cdot O$, and put

$$\pi_O \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \begin{pmatrix} z \\ 1 \end{pmatrix}$$

with $a_0, b_0, c_0, d_0 \in \mathbf{Q}$. Then, since $\pi_O \in O$ and O is the order of $\mathfrak{A}$, a_0, b_0, c_0, d_0 must be integral. Moreover, $a_0 d_0 - b_0 c_0 = \pi_O \bar{\pi}_O \in \Pi$. Therefore, $\gamma_0^* = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}$ is an element of Γ^*, and $\gamma_0^* \cdot z = z$. Since all positive integral powers of π_O are irrational, γ_0^* is of infinite order in Γ^*. Therefore, z is a Γ^*-fixed point. Therefore, by

$$J(z) \bmod \mathfrak{P} = \bar{j}(\mathfrak{A}) = \bar{j},$$

we get the surjectivity of $\mathfrak{J}^*$.

Injectivity of $\mathcal{J}^*$.[3] Let z, z' be two Γ^*-fixed points, put $\mathfrak{A} = [1, z]$, $\mathfrak{A}' = [1, z']$; put $O = O_{\mathfrak{A}} = O_f$, $O_0 = O_{f_0}$, $\mathfrak{A}_0 = O_0 \cdot \mathfrak{A}$ as above, and let $O', O_0', \mathfrak{A}_0'$ be the correspondings for $\mathfrak{A}'$. Suppose that $J(z) \mod \mathfrak{P}$ and $J(z') \mod \mathfrak{P}$ are conjugate over $\mathbf{F}_p$ so that $\bar{j}(\mathfrak{A}) \sim \bar{j}(\mathfrak{A}')$. Then, since we have $\bar{j}(\mathfrak{A}) \sim \bar{j}(\mathfrak{A}_0)$ and $\bar{j}(\mathfrak{A}') \sim \bar{j}(\mathfrak{A}_0')$, we get $\bar{j}(\mathfrak{A}_0) \sim \bar{j}(\mathfrak{A}_0')$. So, by the last part of §7, we obtain $\bar{j}(\mathfrak{A}_0') = \bar{j}(\mathfrak{A}_0 \mathfrak{p}_O^m)$ for some m. But then, by Theorem D, $\mathfrak{A}_0$ and $\mathfrak{A}_0'$ belong to the same field Q' and $\mathfrak{A}_0' = \rho \mathfrak{A}_0 \mathfrak{p}_O^m$ holds for some $\rho \in Q'$. Therefore,

$$\mathfrak{A}' \otimes_{\mathbf{Z}} \mathbf{Z}^{(p)} = \mathfrak{A}_0' \otimes_{\mathbf{Z}} \mathbf{Z}^{(p)} = \rho \mathfrak{A}_0 \otimes_{\mathbf{Z}} \mathbf{Z}^{(p)} = \rho \mathfrak{A} \otimes_{\mathbf{Z}} \mathbf{Z}^{(p)};$$

hence $[z', 1]_{\mathbf{Z}^{(p)}} = [\rho z, \rho]_{\mathbf{Z}^{(p)}}$. Therefore, we have

$$\rho \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} z' \\ 1 \end{pmatrix} \text{ with some } \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_2(\mathbf{Z}^{(p)}).$$

But since $\operatorname{Im} z$, $\operatorname{Im} z' > 0$, we get $AD - BC > 0$, and hence $AD - BC \in \Pi$. Therefore, z and z' are Γ^*-equivalent.

That $\mathcal{J}^*$ is Degree-preserving. Let the notations be as in the proof of the surjectivity of $\mathcal{J}^*$. By the definition of Deg, we have

$$\operatorname{Deg} \gamma_0^* = |\operatorname{ord}_{\mathfrak{P}} \pi_O \bar{\pi}_O^{-1}| = \operatorname{ord}_{\mathfrak{P}} \pi_O = d_O.$$

On the other hand, by (17), we have $\operatorname{Deg} \bar{j}(\mathfrak{A}) = d_O$. Therefore, it suffices to prove that γ_0^* generates Γ_z^* modulo the torsion subgroup Γ_z^{*0} of Γ_z^* (see §3). For this purpose, let $\gamma^* \in \Gamma_z^*$ be any element of infinite order and put

$$\gamma^* = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \text{ with } (a, b, c, d) = 1 \text{ and } ad - bc = p^n \ (n > 0).$$

[3] The injectivity of $\mathcal{J}$ follows easily by well-definedness and surjectivity of $\mathcal{J}$, and by the decomposition (4). Therefore, we need not worry about it here.

Then, if we put $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} z \\ 1 \end{pmatrix} = \lambda\begin{pmatrix} z \\ 1 \end{pmatrix}$, we have $\lambda \in O$ and $\lambda \notin pO$. Therefore, λO is a positive power of either $\mathfrak{p}_O$ or $\bar{\mathfrak{p}}_O$. But d_O is the smallest positive integer, for which $\mathfrak{p}_O^{d_O}$ is principal. Therefore, we see that $d_O|n$, and that either $\lambda/\pi_O^{n/d_O}$ or $\lambda/\bar{\pi}_O^{n/d_O}$ is a root of unity. Therefore, $\lambda/\bar{\lambda}$ is a power of $\pi_O/\bar{\pi}_O$ modulo a root of unity. Therefore by §2, γ_0^* must be a generator of Γ_z^* modulo Γ_z^{*0}. □

A corollary and an announcement of generalizations.

§9.

COROLLARY. *Let $\zeta_{\Gamma^*}(u)$ and $\zeta_{\Gamma}(u)$ be defined by*

$$\prod_{P^* \in \wp(\Gamma^*)} (1 - u^{\mathrm{Deg}\, P^*})^{-1}, \text{ and } \prod_{P \in \wp(\Gamma)} (1 - u^{\deg P})^{-1}$$

respectively. Then we have

$$(18^*) \qquad \zeta_{\Gamma^*}(u) = \frac{1}{(1-u)(1-pu)} \times (1-u)^{1+|S_1|} \times (1-u^2)^{\frac{1}{2}|S_2|},$$

$$(18) \qquad \zeta_{\Gamma}(u) = \frac{1}{(1-u)(1-p^2u)} \times (1-u)^{1+|S|}.$$

PROOF. By Theorem 1, there is a Degree-preserving one-to-one correspondence between $\wp(\Gamma^*)$ and $(\bar{\mathbf{F}}_p - S)/\!\sim$. But there is also a Degree-preserving natural one-to-one correspondence between $\bar{\mathbf{F}}_p/\!\sim\cup\{\infty\}$ and the set of all prime divisors of the rational function field over $\mathbf{F}_p$. Therefore, the computation of $\zeta_{\Gamma^*}(u)$ reduces to the computation of the congruence ζ function of the rational function field over $\mathbf{F}_p$, which is nothing but $\frac{1}{(1-u)(1-pu)}$. This proves (18*). The formula (18) for $\zeta_{\Gamma}(u)$ is obtained exactly in the same manner, by using Theorem 1′. □

§10. As above, identify the set $\bar{\mathbf{F}}_p/\!\sim\cup\{\infty\}$ with the set of all prime divisors of the rational function field K^* over $\mathbf{F}_p$ and denote by $\mathfrak{p}(K^*)$ the set of all prime divisors of K^* *which do not belong to* $S \cup \{\infty\}$. Then by Theorem 1, $\mathcal{J}^*$ gives a one-to-one correspondence between $\wp(\Gamma^*)$ and $\wp(K^*)$. In Part 2 of this chapter, we shall generalize this and prove the following theorem.

Let Γ' be any congruence subgroup[4] *of Γ^* and let $\iota : \wp(\Gamma') \to \wp(\Gamma^*)$ be the natural map defined by the inclusion $\Gamma' \subset \Gamma^*$. Then there exists a finite extension K' of K^* whose constant field is either $\mathbf{F}_p$ (if $\Gamma' \not\subset \Gamma$) or $\mathbf{F}_{p^2}$ (if $\Gamma' \subset \Gamma$), and a degree preserving one-to-one correspondence $\mathcal{J}'$ between $\wp(\Gamma')$ and $\wp(K')$ such that the following diagram* (19)

[4] I.e. a subgroup of Γ^* containing some principal congruence subgroup. See Chapter 4 §3, and J. Mennicke [23].

is commutative. Here, $\wp(K')$ denotes the set of all prime divisors of K' which lie above $\wp(K^*)$.

$$\begin{array}{ccccl} \wp(\Gamma') & \overset{\mathcal{T}'}{\rightarrow} & \wp(K') & & \\ \downarrow \iota & & \downarrow & & \textit{the natural projection} \\ \wp(\Gamma^*) & \overset{\mathcal{T}^*}{\rightarrow} & \wp(K^*) & & \end{array} \tag{19}$$

Moreover, the prime divisors of K which belong to S are "essentially" decomposed completely in K' in a certain sense.

This theorem will give the law of decomposition of prime divisors of K^* in K' completely, and hence will solve our Congruence Monodromy Problems partly for the group $\Gamma = PSL_2(\mathbf{Z}^{(p)})$. Its relation with J. Igusa's work [**14**] will be explained.