CHAPTER 1

Part 1. The group Γ and its ζ-function.

In Part 1 of this chapter, we shall define the ζ-function

$$\zeta_\Gamma(u) = \prod_P (1 - u^{\deg P})^{-1}$$

of Γ, and prove that

$$(20) \qquad \begin{gathered} \zeta_\Gamma(u) = \frac{\prod_{i=1}^{g}(1 - \pi_i u)(1 - \pi_i' u)}{(1-u)(1-q^2 u)} \times (1-u)^{(q-1)(g-1)}; \\ q = N\mathfrak{p},\ g \geq 2,\ \pi_i\pi_i' = q^2\ (1 \leq i \leq g) \end{gathered}$$

holds, if G/Γ is compact and Γ is torsion-free. We shall also prove the inequality; $|\pi_i|$, $|\pi_i'| \leq q^2$, π_i, $\pi_i' \neq 1, q^2$, by applying Lemma 10 (M.Kuga), §21. These results, particularly the existence of the factor $(1-u)^{(q-1)(g-1)}$, give a starting point of our problems described in the introduction. Our formula (20) is, modulo some group theory of $PL_2(k_\mathfrak{p})$, a consequence of Eichler-Selberg trace formula for the Hecke operators in the space of certain automorphic forms of weight 2. However, the proof, starting at Eichler-Selberg formula and ending at (20), is by no means simple, mainly because we do not have a simple proof of Lemma 3 (§13).[1] Finally, we point out that there is also a difference in the standpoint; Eichler-Selberg's left side of the formula comes to the right side of ours; (20). For us, the subject is the set of "elliptic Γ-conjugacy classes", and not the Hecke operator.

We shall begin with the definition of the group Γ.

Discrete subgroup Γ.

§1. Let

$$(1) \qquad G = PSL_2(\mathbf{R}) \times PSL_2(k_\mathfrak{p})$$

be considered as a topological group, and for each subset S of G, we denote by $S_\mathbf{R}$ resp. $S_\mathfrak{p}$ the set-theoretical projections of S to $\mathbf{R}$-component (i.e. the first component) resp.

[1] We can also prove (20) (for $\mathfrak{p} \nmid 2$) by using the spectral decomposition of $L^2(G/\Gamma)$.

k_p-component (i.e. the second component) of G. In particular, we have

(2) $$G_{\mathbf{R}} = PSL_2(\mathbf{R}), \qquad G_p = PSL_2(k_p),$$

and for any element x of G, $x_{\mathbf{R}}$ resp. x_p denote the $\mathbf{R}$-component resp. the k_p-component of x;

(3) $$x = x_{\mathbf{R}} \times x_p.$$

§2. *The subject of our study is a discrete subgroup Γ of $G = G_{\mathbf{R}} \times G_p$, for which $\Gamma_{\mathbf{R}}$ and Γ_p are dense in $G_{\mathbf{R}}$ and G_p respectively.* So, throughout the following, Γ will always denote such a discrete subgroup of G.

Example. Let p be a prime number, and let $\mathbf{Z}^{(p)}$ be the ring of rational numbers whose denominators are powers of p;

(4) $$\mathbf{Z}^{(p)} = \{a/p^n \mid a, n \in \mathbf{Z}\}.$$

Put

(5) $$\Gamma = PSL_2(\mathbf{Z}^{(p)}) = SL_2(Z^{(p)})/ \pm I.$$

Let $\mathbf{Q}_p$ be the p-adic number field. Then, by the injections $\mathbf{Z}^{(p)} \to \mathbf{R}, \to \mathbf{Q}_p$, the group Γ can be regarded as a subgroup of $G = PSL_2(\mathbf{R}) \times PSL_2(\mathbf{Q}_p)$. It is discrete in G, since if $\gamma = \gamma_{\mathbf{R}} \times \gamma_p \in \Gamma$, and if γ_p is contained in $PSL_2(\mathbf{Z}_p)$ ($\mathbf{Z}_p$: the ring of p-adic integers), which is a neighborhood of the identity of $PSL_2(\mathbf{Q}_p)$, then $\gamma_{\mathbf{R}}$ is contained in $PSL_2(\mathbf{Z})$, which is discrete in $PSL_2(\mathbf{R})$. It is a simple exercise, in arithmetic of algebraic groups, to check that $\Gamma_{\mathbf{R}}$, Γ_p are dense in $G_{\mathbf{R}}, G_p$ respectively.

Now, for this particular Γ, the projection maps $\Gamma \to \Gamma_{\mathbf{R}}, \to \Gamma_p$ are injective, and the quotient G/Γ has a finite invariant volume. The former is true in general, as the following proposition shows; as for the latter, we do not know whether it is true in general, but, curious as it may look, we think that it is quite possible.

Proposition 1. *Let Γ be a discrete subgroup of G, for which $\Gamma_{\mathbf{R}}$, Γ_p are dense in $G_{\mathbf{R}}$, G_p respectively. Then the projection maps $\Gamma \to \Gamma_{\mathbf{R}}, \to \Gamma_p$ are injective.*

Proof. Let Δ be the kernel of the projection $\Gamma \to \Gamma_{\mathbf{R}}$.

(6) $$\Delta = \{\gamma = \gamma_{\mathbf{R}} \times \gamma_p \in \Gamma \mid \gamma_{\mathbf{R}} = 1\}.$$

So $\Delta_p \cong \Delta$ is discrete in G_p, and normal in Γ_p ; hence normal in G_p, the closure of Γ_p. So, Δ_p is a discrete normal subgroup of G_p. On the other hand. it is well-known that if K is any infinite field, then the group $PSL_2(K) = SL_2(K)/\pm 1$ is simple (as an abstract group). So, G_p is simple, and hence $\Delta_p = \{I\}$; hence $\Delta = \{I\}$. The injectivity of $\Gamma \to \Gamma_p$ follows exactly in the same manner, by using the simplicity of $G_{\mathbf{R}}$. □

So, we can identify the three canonically isomorphic groups:

$$\Gamma_{\mathbf{R}} \cong \Gamma \cong \Gamma_p.$$

Proposition 2. *Let Γ be a subgroup of G such that the projection maps $\Gamma \to \Gamma_{\mathbf{R}}, \to \Gamma_{\mathfrak{p}}$ are injective, and that $\Gamma_{\mathbf{R}}$, $\Gamma_{\mathfrak{p}}$, are dense in $G_{\mathbf{R}}$, $G_{\mathfrak{p}}$ respectively. Let $U_{\mathfrak{p}}$ be an open compact subgroup of $G_{\mathfrak{p}}$, and let $\Gamma^0_{\mathbf{R}}$ be the projection to* $\mathbf{R}$*-component of $\Gamma^0 = \Gamma \cap (G_{\mathbf{R}} \times U_{\mathfrak{p}})$. Then,* (i) *$\Gamma$ is discrete in G if and only if $\Gamma^0_{\mathbf{R}}$ is discrete in $G_{\mathbf{R}}$. Moreover, if* (i) *is satisfied, then,* (ii) *the quotient G/Γ is compact (resp. has a finite invariant volume) if and only if $G_{\mathbf{R}}/\Gamma^0_{\mathbf{R}}$ is compact (resp. has a finite invariant volume).*

Proof. The first assertion (i) is immediate. The "if" part is because $U_{\mathfrak{p}}$ is open, and the "only if" part is because $U_{\mathfrak{p}}$ is compact. As for (ii), if $G_{\mathbf{R}}/\Gamma^0_{\mathbf{R}}$ is compact (resp. has a finite invariant volume), then, there is a subspace $K_{\mathbf{R}}$ of $G_{\mathbf{R}}$ which is compact (resp. has a finite invariant volume) such that $G_{\mathbf{R}} = K_{\mathbf{R}} \cdot \Gamma^0_{\mathbf{R}}$. Since we have $G_{\mathfrak{p}} = U_{\mathfrak{p}} \cdot \Gamma_{\mathfrak{p}}$, it follows immediately that $G = (K_{\mathbf{R}} \times U_{\mathfrak{p}}) \cdot \Gamma$; which proves the "only if" part. Conversely, if $G_{\mathbf{R}}/\Gamma^0_{\mathbf{R}}$ is non-compact (resp. has an infinite volume), then there is an open subset $F_{\mathbf{R}}$ of $G_{\mathbf{R}}$ such that the restriction to $F_{\mathbf{R}}$ of the natural map $\varphi_R : G_{\mathbf{R}} \to G_{\mathbf{R}}/\Gamma^0_{\mathbf{R}}$ is injective, and that $F_{\mathbf{R}}$ is non-compact (resp. has an arbitrarily large volume). Put $F = F_{\mathbf{R}} \times U_{\mathfrak{p}}$. Then, the restriction to F of the natural map $\varphi : G \to G/\Gamma$ is injective, and F is non-compact (resp. has an arbitrarily large volume) ; which proves the "if" part of (ii). □

§3. Now, $G_{\mathbf{R}} = PSL_2(\mathbf{R})$ acts on the complex upper half plane $\mathfrak{H} = \{z \in \mathbf{C} \mid \operatorname{Im} z > 0\}$ as:

$$G_{\mathbf{R}} \ni g_{\mathbf{R}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \quad \mathfrak{H} \ni z \mapsto g_{\mathbf{R}} \cdot z = \frac{az+b}{cz+d} \in \mathfrak{H}. \tag{7}$$

As is well-known, $G_{\mathbf{R}}$ acts transitively on $\mathfrak{H}$, and is identified with the group $\operatorname{Aut}(\mathfrak{H})$ of all automorphisms of the complex Riemann surface $\mathfrak{H}$. Since Γ is identified with its projection $\Gamma_{\mathbf{R}} \subset G_{\mathbf{R}}$, Γ also acts on $\mathfrak{H}$. Two points $z, z' \in \mathfrak{H}$ will be called *equivalent* (or, more precisely, Γ-equivalent), if there is an element $\gamma \in \Gamma$ such that $\gamma_{\mathbf{R}} \cdot z = z'$. We note that, since $\Gamma_{\mathbf{R}}$ is dense in $G_{\mathbf{R}}$, each equivalence class $\Gamma_{\mathbf{R}} \cdot z$ is also dense on $\mathfrak{H}$. A point $z \in \mathfrak{H}$ will be called a *Γ-fixed point*, if its stabilizer in Γ is infinite. For each $z \in \mathfrak{H}$, we put

$$\begin{cases} G_{z,\mathbf{R}} &= \{g_{\mathbf{R}} \in G_{\mathbf{R}} \mid g_{\mathbf{R}} \cdot z = z\} \cong \mathbf{R}/\mathbf{Z} \\ \Gamma_{z,\mathbf{R}} &= \Gamma_{\mathbf{R}} \cap G_{z,\mathbf{R}} = \{\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}} \mid \gamma_{\mathbf{R}} \cdot z = z\}. \end{cases} \tag{8}$$

Let Γ_z, $\Gamma_{z,\mathfrak{p}}$ be the subgroup of Γ, $\Gamma_{\mathfrak{p}}$ respectively which correspond to $\Gamma_{z,\mathbf{R}}$ by the canonical isomorphism: $\Gamma_{z,\mathbf{R}} \cong \Gamma_z \cong \Gamma_{z,\mathfrak{p}}$.

$$\begin{cases} \Gamma_z &= \{\gamma \in \Gamma \mid \gamma_{\mathbf{R}} \cdot z = z\} \\ \Gamma_{z,\mathfrak{p}} &= \{\gamma_{\mathfrak{p}} \in \Gamma_{\mathfrak{p}} \mid \gamma \in \Gamma_z\} = \{\gamma_{\mathfrak{p}} \in \Gamma_{\mathfrak{p}} \mid \gamma_{\mathbf{R}} \cdot z = z\}. \end{cases} \tag{9}$$

So, $z \in \mathfrak{H}$ is a Γ-fixed point if and only if $\Gamma_{z,\mathbf{R}} \cong \Gamma_z \cong \Gamma_{z,\mathfrak{p}}$ are infinite. Let

$$\wp(\Gamma) \tag{10}$$

be the set of all Γ-equivalence classes of all Γ-fixed points on $\mathfrak{H}$. We shall see later, that $\wp(\Gamma)$ is analogous, in various sense, to the set of all prime divisors of an algebraic function field of one variable over the finite field $\mathbf{F}_{q^2}$, where $q = N\mathfrak{p}$.

An element $g_{\mathbf{R}} \in G_{\mathbf{R}}$, $g_{\mathbf{R}} \neq 1$ will be called *elliptic* if it has a fixed point on $\mathfrak{H}$. So, $g_{\mathbf{R}}$ is elliptic if and only if $g_{\mathbf{R}}$ has imaginary eigenvalues, and hence if and only if $|\operatorname{tr} g_{\mathbf{R}}| < 2$.

If $g_{\mathbf{R}}$ is elliptic, then the fixed point $z \in \mathfrak{H}$ of $g_{\mathbf{R}}$ (i.e. z such that $g_{\mathbf{R}} \cdot z = z$) is unique, and the centralizer of $g_{\mathbf{R}}$ in $G_{\mathbf{R}}$ coincides with $G_{z,\mathbf{R}}$. We shall call an element γ of Γ *elliptic*, if $\gamma_{\mathbf{R}}$ is elliptic. Thus $\gamma \in \Gamma$ is elliptic if and only if $\gamma \neq 1$, and $\gamma \in \Gamma_z$ for some (unique) $z \in \mathfrak{H}$. In this case, by the preceding remark, it is clear that the centralizer of γ in Γ is Γ_z.

To show that $\wp(\Gamma)$ is non-empty, we note the following. Let $g_{\mathfrak{p}}$ be any element of $G_{\mathfrak{p}}$ of finite order n. Then the eigenvalues of $g_{\mathfrak{p}}$ are contained in some quadratic extension of $k_{\mathfrak{p}}$, and are primitive n-th or $2n$-th root of unity. Since there exist at most finitely many quadratic extensions of $k_{\mathfrak{p}}$, and since each such field contains at most finitely many roots of unity, we see that n must be bounded. Since $\Gamma_{\mathfrak{p}} \cong \Gamma$ is a subgroup of $G_{\mathfrak{p}}$, this shows that there are only finitely many possibilities of orders n of elements γ of Γ. Therefore, the set

$$S = \{|\operatorname{tr}\gamma_{\mathbf{R}}|;\, \gamma \in \Gamma, \gamma \text{ is of finite order } \neq 1\}$$

is finite. Put $G' = \{g_{\mathbf{R}} \in G_{\mathbf{R}} \mid |\operatorname{tr} g_{\mathbf{R}}| < 2\}$. Then G' is open, and contains S, which is finite; and hence $G' - S$ is again an open subset of $G_{\mathbf{R}}$. Since $\Gamma_{\mathbf{R}}$ is dense in $G_{\mathbf{R}}$, there exists an element $\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}} \cap (G' - S)$. Then $\gamma_{\mathbf{R}}$ has a fixed point $z \in \mathfrak{H}$, and $\Gamma_{z,\mathbf{R}}$ is infinite, since it contains $\gamma_{\mathbf{R}}$. So, $\wp(\Gamma)$ is non-empty.

§4.

Proposition 3. *Let $z \in \mathfrak{H}$, and let Γ_z be infinite. Then, $\Gamma_{z,\mathfrak{p}}$ is a discrete abelian subgroup of $G_{\mathfrak{p}}$. Moreover, if we put*

$$T_{\mathfrak{p}} = \left\{ \begin{pmatrix} t_{\mathfrak{p}} & 0 \\ 0 & t_{\mathfrak{p}}^{-1} \end{pmatrix} \middle|\, t_{\mathfrak{p}} \in k_{\mathfrak{p}}^{\times} \right\} / \{\pm 1\} \subset G_{\mathfrak{p}},$$

then there is an element $x_{\mathfrak{p}} \in G_{\mathfrak{p}}$ such that $x_{\mathfrak{p}}^{-1}\Gamma_{z,\mathfrak{p}}x_{\mathfrak{p}} \subset T_{\mathfrak{p}}$.

Proof. We have $\Gamma_{z,\mathbf{R}} \cong \Gamma_z \cong \Gamma_{z,\mathfrak{p}}$ canonically, and $\Gamma_{z,\mathbf{R}}$ is a subgroup of $G_{z,\mathbf{R}} \cong \mathbf{R}/\mathbf{Z}$ which is compact abelian. Therefore, Γ_z is abelian. Since $\Gamma_z \subset \Gamma$ is discrete in G, and since $\Gamma_{z,\mathbf{R}}$ is an infinite subgroup of a compact subgroup of $G_{\mathbf{R}}$, we see immediately that $\Gamma_{z,\mathfrak{p}}$ must be discrete in $G_{\mathfrak{p}}$.

Now let $\gamma \in \Gamma_z$ be of infinite order, and let $\pm\{\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{p}}^{-1}\}$ be the eigenvalues of $\gamma_{\mathfrak{p}}$.

We shall show that $\lambda_{\mathfrak{p}}^{-1} \neq \lambda_{\mathfrak{p}}$ and that $\lambda_{\mathfrak{p}} \in k_{\mathfrak{p}}$. In fact, if $\lambda_{\mathfrak{p}}^{-1} = \lambda_{\mathfrak{p}}$, then we can assume that $\lambda_{\mathfrak{p}}^{-1} = \lambda_{\mathfrak{p}} = 1$, and hence $\gamma_{\mathfrak{p}} = x_{\mathfrak{p}}^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}x_{\mathfrak{p}}$ with some $x_{\mathfrak{p}} \in GL_2(k_{\mathfrak{p}})$. If p is the characteristic of the residue field $O/\mathfrak{p}$, then $\lim_{n\to\infty}\begin{pmatrix} 1 & p^n \\ 0 & 1 \end{pmatrix} = 1$; hence $\lim_{n\to\infty}\gamma_{\mathfrak{p}}^{p^n} = 1$, which contradicts the discreteness of $\Gamma_{z,\mathfrak{p}}$ in $G_{\mathfrak{p}}$. Therefore, $\lambda_{\mathfrak{p}}^{-1}, \lambda_{\mathfrak{p}}$ must be distinct. Suppose now that $\lambda_{\mathfrak{p}}^{-1} \neq \lambda_{\mathfrak{p}}$, but $\lambda_{\mathfrak{p}} \notin k_{\mathfrak{p}}$. Put $K_{\mathfrak{p}} = k_{\mathfrak{p}}(\lambda_{\mathfrak{p}})$. Then, since $\lambda_{\mathfrak{p}}^{-1}, \lambda_{\mathfrak{p}}$ are conjugate of each other over $k_{\mathfrak{p}}$, we have $\lambda_{\mathfrak{p}} \in K_{\mathfrak{p}}^1 = \{x \in K_{\mathfrak{p}} \mid N_{K_{\mathfrak{p}}/k_{\mathfrak{p}}}(x) = 1\}$. Since $K_{\mathfrak{p}}^1$ is a subgroup of the group of units of $K_{\mathfrak{p}}$, $K_{\mathfrak{p}}^1$ is compact. Now if we ignore the sign and consider $\gamma_{\mathfrak{p}}$ as an element of $SL_2(k_{\mathfrak{p}})$ (choose either one of two), there is a unique isomorphism φ over $k_{\mathfrak{p}}$ of $K_{\mathfrak{p}}$ into $M_2(k_{\mathfrak{p}})$ which sends $\lambda_{\mathfrak{p}}$ to $\gamma_{\mathfrak{p}}$. So, $\gamma_{\mathfrak{p}}$ is contained in a compact subgroup $\varphi(K_{\mathfrak{p}}^1)$ of $G_{\mathfrak{p}}$. Since $\gamma_{\mathfrak{p}}$ is of infinite order by assumption, this also contradicts the discreteness of $\Gamma_{z,\mathfrak{p}}$ in $G_{\mathfrak{p}}$. So we have shown that $\lambda_{\mathfrak{p}}^{-1} \neq \lambda_{\mathfrak{p}}$ and that $\lambda_{\mathfrak{p}} \in k_{\mathfrak{p}}$.

Take $\tilde{x}_{\mathfrak{p}} \in GL_2(k_{\mathfrak{p}})$ such that $\tilde{x}_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p}}\tilde{x}_{\mathfrak{p}} = \pm\begin{pmatrix}\lambda_{\mathfrak{p}} & 0\\ 0 & \lambda_{\mathfrak{p}}^{-1}\end{pmatrix}$. By putting $x_{\mathfrak{p}} = \tilde{x}_{\mathfrak{p}}\begin{pmatrix}1 & 0\\ 0 & \det\tilde{x}_{\mathfrak{p}}^{-1}\end{pmatrix}$, we get $x_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p}}x_{\mathfrak{p}} = \pm\begin{pmatrix}\lambda_{\mathfrak{p}} & 0\\ 0 & \lambda_{\mathfrak{p}}^{-1}\end{pmatrix}$ with $x_{\mathfrak{p}} \in G_{\mathfrak{p}}$. If $\gamma'_{\mathfrak{p}}$ is any element of $\Gamma_{z,\mathfrak{p}}$, it commutes with $\gamma_{\mathfrak{p}}$, and hence $x_{\mathfrak{p}}^{-1}\gamma'_{\mathfrak{p}}x_{\mathfrak{p}}$ is of the form $\pm\begin{pmatrix}\lambda'_{\mathfrak{p}} & 0\\ 0 & \lambda'^{-1}_{\mathfrak{p}}\end{pmatrix}$ with some $\lambda'_{\mathfrak{p}} \in k_{\mathfrak{p}}^{\times}$. So, we get $x_{\mathfrak{p}}^{-1}\Gamma_{\mathfrak{p}}x_{\mathfrak{p}} \subset T_{\mathfrak{p}}$, which proves our Proposition. □

Corollary. *Let Γ_z be of infinite order. Then,*

$$\Gamma_z \cong (\textit{a finite cyclic group}) \times (\textit{infinite cyclic group}).$$

If $\gamma \in \Gamma_z$ is of infinite order, then the eigenvalues $\pm\{\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{p}}^{-1}\}$ of $\gamma_{\mathfrak{p}}$ are contained in $k_{\mathfrak{p}}$, and not contained in $\mathcal{U}_{\mathfrak{p}}$, $\mathcal{U}_{\mathfrak{p}}$ being the group of $\mathfrak{p}$-adic units of $k_{\mathfrak{p}}$.

Proof. Take $x_{\mathfrak{p}} \in G_{\mathfrak{p}}$ such that $x_{\mathfrak{p}}^{-1}\Gamma_{z,\mathfrak{p}}x_{\mathfrak{p}} \subset T_{\mathfrak{p}}$. For each $\gamma \in \Gamma_z$, put $x_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p}}x_{\mathfrak{p}} = \pm\begin{pmatrix}t_{\mathfrak{p}} & 0\\ 0 & t_{\mathfrak{p}}^{-1}\end{pmatrix}$, and put $t_{\mathfrak{p}} = \varphi(\gamma_{\mathfrak{p}})$. Then φ gives an isomorphism of Γ_z into $k_{\mathfrak{p}}^{\times}/\pm 1$, and since $\Gamma_{z,\mathfrak{p}}$ is discrete in $G_{\mathfrak{p}}$, $\varphi(\Gamma_z)$ is discrete in $k_{\mathfrak{p}}^{\times}/\pm 1$. So, $\varphi(\Gamma_z) \cap \mathcal{U}_{\mathfrak{p}}/\pm 1$ must be finite, and $\varphi(\Gamma_z)$ is the direct product of $\varphi(\Gamma_z) \cap \mathcal{U}_{\mathfrak{p}}/\pm 1$ and an infinite cyclic subgroup. □

§5. Let $P \in \wp(\Gamma)$, and let $z \in \mathfrak{H}$ be a Γ-fixed point contained in the class P. By Proposition 3, the set of eigenvalues $\pm\lambda_{\mathfrak{p}}^{\pm 1}$ of all elements $\gamma_{\mathfrak{p}}$ of $\Gamma_{z,\mathfrak{p}}$ forms a discrete subgroup $\varphi(\Gamma_z)$ of $k_{\mathfrak{p}}^{\times}/\pm 1$. Let $\mathrm{ord}_{\mathfrak{p}}$ be the normalized additive valuation of $k_{\mathfrak{p}}$, and put

$$\mathrm{ord}_{\mathfrak{p}}\,\varphi_{\mathfrak{p}}(\Gamma_z) = \{\mathrm{ord}_{\mathfrak{p}}(\lambda_{\mathfrak{p}}^{\pm 1}) \mid \gamma_{\mathfrak{p}} \in \Gamma_{z,\mathfrak{p}}\}. \tag{11}$$

Then, this is an infinite subgroup of $\mathbf{Z}$, and hence is of the form $a \cdot \mathbf{Z}$ with some positive integer a. If z is replaced by a Γ-equivalent point $z' = \gamma'_{\mathbf{R}} \cdot z$ ($\gamma' \in \Gamma$), then $\Gamma_{z'} = \gamma' \cdot \Gamma_z \cdot \gamma'^{-1}$, and hence we have $\varphi(\Gamma_{z'}) = \varphi(\Gamma_z)$. So, this positive integer a is determined uniquely by P. We shall call this number a, the *degree* of P, and denote it by

$$\deg P. \tag{12}$$

It is clear that if $\gamma \in \Gamma_z$ is such that, together with some finite group, γ generates Γ_z, and if $\pm\{\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{p}}^{-1}\}$ are the eigenvalues of $\gamma_{\mathfrak{p}}$, then

$$\deg P = |\,\mathrm{ord}_{\mathfrak{p}}(\lambda_{\mathfrak{p}})|. \tag{13}$$

The ζ function of Γ.

§6. We shall define the ζ function $\zeta_\Gamma(u)$ of Γ to be the following formal infinite product;

$$\zeta_\Gamma(u) = \prod_{P \in \wp(\Gamma)} (1 - u^{\deg P})^{-1}, \tag{14}$$

or, equivalently,

$$(15) \qquad \zeta_\Gamma(u) = \exp \sum_{m=1}^{\infty} \frac{N_m}{m} u^m$$

with

$$(16) \qquad N_m = \sum_{\substack{P \in \wp(\Gamma), \\ \deg P | m}} \deg P \qquad (m \geq 1).$$

That N_m are finite will be shown later.

§7. Example.[2] Let $\Gamma = PSL_2(\mathbf{Z}^{(p)})$ (see §2). Then, we can compute $\zeta_\Gamma(u)$ directly, by using a full knowledge of complex multiplication theory. Thus, let $J(z) = 12^3 g_2(z)^3 / \left[g_2(z)^3 - 27 g_3(z)^2\right]$ be the elliptic modular function, and let $\mathfrak{p}$ be a divisor of p in the algebraic closure $\overline{\mathbf{Q}}$ of the field of rational numbers $\mathbf{Q}$. We consider $\overline{\mathbf{Q}}$ as a subfield of the complex number field $\mathbf{C}$, and we denote by O the ring of all algebraic integers of $\overline{\mathbf{Q}}$. Moreover, we denote by $\mathbf{F}_p$ the finite field with p elements, and by $\overline{\mathbf{F}}_p$ its algebraic closure. We fix an isomorphism $O/\mathfrak{p} \cong \overline{\mathbf{F}}_p$ and identify them. Let S be the subset of $\overline{\mathbf{F}}_p$ formed of all $\overline{j} \in \overline{\mathbf{F}}_p$ such that the elliptic curve with modulus $\overline{j}$ has no points of order p, or equivalently, the elliptic curve with modulus $\overline{j}$ has Hasse invariant 0. Then, it is well-known that S is finite, and that S is contained in $\mathbf{F}_{p^2}$. The number of elements of S is given by

$$(17) \qquad H = 1 \ (p = 2,3), \quad H = \frac{p-1}{12}, \frac{p+7}{12}, \frac{p+5}{12}, \frac{p+13}{12}$$
$$(p \equiv 1, 5, 7, 11 (\mathrm{mod}\, 12) \text{ respectively}).$$

We shall call two elements $x, y \in \overline{\mathbf{F}}_p$ equivalent, and denote it by $x \sim y$, if x, y are conjugate of each other over $\mathbf{F}_{p^2}$. So, the number of distinct y with $y \sim x$ (x: given) is equal to the degree of x over $\mathbf{F}_{p^2}$, which will be called the degree of the equivalence class. Since $S \subset \mathbf{F}_{p^2}$, we can consider S also as a subset of $\overline{\mathbf{F}}_p/\!\sim$.

Now, for each $P \in \wp(\Gamma)$, let z_P be a Γ-fixed point contained in the class P, and let $J(z_P)$ be the value of J at $z = z_P$. Then, by using complex multiplication theory, we can check that $J(z_P) \in O$, and that the map $\mathcal{J}$ of $\wp(\Gamma)$ into $\overline{\mathbf{F}}_p/\sim$ defined by

$$(18) \qquad \mathcal{J} : \wp(\Gamma) \ni P \mapsto J(z_P) \mod \mathfrak{p} \in \overline{\mathbf{F}}_p/\sim$$

is well-defined (the congruence relation!), injective, and degree preserving. Moreover, the image of $\mathcal{J}$ coincides with $\overline{\mathbf{F}}_p/\!\sim - S$. Thus, $\mathcal{J}$ gives a degree-preserving one-to-one correspondence between $\wp(\Gamma)$ and $\overline{\mathbf{F}}_p/\!\sim - S$. Since a straightforward computation shows that

$$\prod_{\bar{x} \in \overline{\mathbf{F}}_p/\sim - S} (1 - u^{\deg \bar{x}})^{-1} = \frac{1}{(1-u)(1-p^2u)} \times (1-u)^{1+H},$$

[2] See Chapter 5 for the proof.

we get

$$\zeta_\Gamma(u) = \frac{1}{(1-u)(1-p^2u)} \times (1-u)^{1+H}, \tag{19}$$

where H is given by (17).

§8. Now let us compute $\zeta_\Gamma(u)$ for more general Γ. We shall restrict ourselves to the case where Γ is torsion-free (i.e. Γ has no elements of finite order) and where the quotient G/Γ is compact. Our purpose is to prove the following theorem.

THEOREM 1. *Let Γ be a torsion-free discrete subgroup of G with compact quotient, and with dense images of projections $\Gamma_{\mathbf{R}}$, $\Gamma_{\mathfrak{p}}$ in $G_{\mathbf{R}}$, $G_{\mathfrak{p}}$ respectively. Then we have;*

$$\zeta_\Gamma(u) = \frac{\prod_{i=1}^{g}(1-\pi_i u)(1-\pi_i' u)}{(1-u)(1-q^2u)} \times (1-u)^{(q-1)(g-1)}, \tag{20}$$

where $q = N\mathfrak{p}$, and g is the genus of $\Gamma_{\mathbf{R}}^0\backslash\mathfrak{H}$, with $\Gamma^0 = \Gamma \cap (G_{\mathbf{R}} \times U_{\mathfrak{p}})$, $U_{\mathfrak{p}} = PSL_2(O_{\mathfrak{p}})$. The numbers π_i, π_i' $(1 \le i \le g)$ are algebraic integers satisfying $\pi_i\pi_i' = q^2$ $(1 \le i \le g)$.

REMARK . Since $\Gamma_{\mathbf{R}}^0$ is a torsion-free discrete subgroup of $G_{\mathbf{R}}$ with compact quotient (see §2, Proposition 2), we have $g \ge 2$. The formula (20) is equivalent to saying that N_m defined by (16) is finite and is given by:

$$N_m = q^{2m} + 1 - \sum_{i=1}^{g}(\pi_i^m + \pi_i'^m) - (q-1)(g-1) \quad (m \ge 1). \tag{20'}$$

This formula for $\zeta_\Gamma(u)$ is one of the starting point of our study of Γ.

Lemmas for the proof of Theorem 1.

§9. The proof of Theorem 1 is based on three basic lemmas; Lemmas 1, 2 and 3. We shall begin by describing Lemma 1.

Let Δ be a torsion-free discrete subgroup of $G_{\mathbf{R}} = PSL_2(\mathbf{R})$ with compact quotient, and let $\tilde{\Delta}$ be a subgroup of $G_{\mathbf{R}}$ containing Δ such that, for any $\gamma \in \tilde{\Delta}$, the subgroups Δ, $\gamma\Delta\gamma^{-1}$ of $\tilde{\Delta}$ are commensurable with each other. Let $\mathcal{H}(\tilde{\Delta}, \Delta)$ be the Hecke ring [3] defined with respect to $\tilde{\Delta}$ and Δ . For each double coset $\Delta\gamma\Delta \in \mathcal{H}(\tilde{\Delta}, \Delta)$, we put

$$d(\Delta\gamma\Delta) = (\Delta : \gamma^{-1}\Delta\gamma \cap \Delta) = |\Delta\backslash\Delta\gamma\Delta|, \tag{21}$$

and define $d(X)$ for arbitrary $X \in \mathcal{H}(\tilde{\Delta}, \Delta)$ by (21) and by linearity. Thus $\mathcal{H}(\tilde{\Delta}, \Delta) \ni X \mapsto d(X)$ gives a linear representation of the ring $\mathcal{H}(\tilde{\Delta}, \Delta)$.

On the other hand, let $\mathfrak{M}_k$ be the space of all holomorphic automorphic forms of weight k $(k = 2, 4, 6, \cdots)$ with respect to Δ. For each $\Delta\gamma\Delta \in \mathcal{H}(\tilde{\Delta}, \Delta)$, put $\Delta\gamma\Delta = \sum_{i=1}^{d} \Delta\gamma_i$ $(d =$

[3] Defined with respect to the left Δ-cosets.

$d(\Delta\gamma\Delta)$), and let $\rho_k(\Delta\gamma\Delta)$ be the Hecke operator; i.e. the linear endomorphism of $\mathfrak{M}_k$ defined by:

$$\rho_k(\Delta\gamma\Delta) : \mathfrak{M}_k \ni f(z) \mapsto \sum_{i=1}^{d} f\left(\frac{a_i z + b_i}{c_i z + d_i}\right)(c_i z + d_i)^{-k} \in \mathfrak{M}_k, \tag{22}$$

where $\gamma_i = \pm\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$ $(1 \le i \le d)$. This is independent of the choice of representatives $\gamma_1, \cdots, \gamma_d$. Define $\rho_k(X)$ for arbitrary $X \in \mathcal{H}(\tilde{\Delta}, \Delta)$ by (22) and by linearity. Then, it is also easy to check (and is well-known) that ρ_k gives an representation of the ring $\mathcal{H}(\tilde{\Delta}, \Delta)$ in the ring of all linear endomorphisms of $\mathfrak{M}_k$. Now, by Petersson,

$$(f, g) = \int_{\Delta\backslash\mathfrak{H}} f(z)\overline{g(z)}y^{k-2}dxdy \quad (z = x + iy)$$

gives a positive hermitian form on $\mathfrak{M}_k$, and the adjoint of $\rho_k(\Delta\gamma\Delta)$ with respect to this hermitian form is $\rho_k(\Delta\gamma^{-1}\Delta)$. Therefore, if $\Delta\gamma^{-1}\Delta = \Delta\gamma\Delta$ is satisfied for all $\gamma \in \tilde{\Delta}$, then the Hecke operators $\rho_k(\Delta\gamma\Delta)$ are all hermitian. Moreover, $\Delta\gamma^{-1}\Delta = \Delta\gamma\Delta$ $(\forall\gamma \in \tilde{\Delta})$ implies the commutativity of the ring $\mathcal{H}(\tilde{\Delta}, \Delta)$. Therefore, under this condition, ρ_k is a direct sum of real *linear* representations of $\mathcal{H}(\tilde{\Delta}, \Delta)$.

Recall now that an element $g_{\mathbf{R}} \in G_{\mathbf{R}}$ is called elliptic if it has a fixed point on $\mathfrak{H}$. It is clear that if $g_{\mathbf{R}} \in \Delta\gamma\Delta$ $(\gamma \in \tilde{\Delta})$ is elliptic, and if $\delta \in \Delta$, then $\delta^{-1}g_{\mathbf{R}}\delta$ is also elliptic and contained in $\Delta\gamma\Delta$. Let $A(\Delta\gamma\Delta)$ be the number of all elliptic Δ-conjugacy classes contained in $\Delta\gamma\Delta$. Then, if $\Delta\gamma\Delta \neq \Delta$, Eichler-Selberg's trace formula for the Hecke operators asserts that [4]:

$$A(\Delta\gamma\Delta) = d(\Delta\gamma\Delta) + d(\Delta\gamma^{-1}\Delta) - \operatorname{tr}\rho_2(\Delta\gamma\Delta) - \operatorname{tr}\rho_2(\Delta\gamma^{-1}\Delta). \tag{23'}$$

(cf. Eichler [**12**]). As a summary (for $k = 2$), we get:

Lemma 1. *Let $\Delta, \tilde{\Delta}$ be as in the beginning of* §9, *and assume that we have $\Delta\gamma^{-1}\Delta = \Delta\gamma\Delta$ for all $\gamma \in \tilde{\Delta}$. Let $\rho = \rho_2$ be the representation* (22) *of $\mathcal{H}(\tilde{\Delta}, \Delta)$; the Hecke operators in the space of automorphic forms of weight* 2 *with respect to Δ. Then, ρ is a direct sum of g linear real representations $\chi_1, \cdots, \chi_g$, where g is the genus of $\Delta\backslash\mathfrak{H}$. Moreover, if $\gamma \in \tilde{\Delta}, \gamma \notin \Delta$, then the number $A(\Delta\gamma\Delta)$ of elliptic Δ-conjugacy classes contained in $\Delta\gamma\Delta$ is given by*

$$A(\Delta\gamma\Delta) = 2(d(\Delta\gamma\Delta) - \operatorname{tr}\rho(\Delta\gamma\Delta)), \tag{23}$$

where $d(\Delta\gamma\Delta)$ is defined by (21).

We remark that, in Eichler-Selberg, $\operatorname{tr}\rho(\Delta\gamma\Delta)$ comes on the left side; while in our point-view, $A(\Delta\gamma\Delta)$ is "wanted" and comes on the left side.

---

[4]This can also be proved by Lefschetz' fixed point Theorem.

§10. The second basic lemma is concerned with the Hecke ring $\mathcal{H}(G_\mathfrak{p}, U_\mathfrak{p})$, where $G_\mathfrak{p} = PSL_2(k_\mathfrak{p})$ and

(24) $$U_\mathfrak{p} = PSL_2(O_\mathfrak{p}) = SL_2(O_\mathfrak{p})/\pm 1.$$

It is clear that $\mathcal{H}(G_\mathfrak{p}, U_\mathfrak{p})$ is defined, since $g_\mathfrak{p}^{-1}U_\mathfrak{p}g_\mathfrak{p}$ and $U_\mathfrak{p}$, for any $g_\mathfrak{p} \in G_\mathfrak{p}$, are commensurable with each other. Let p be a prime element of $k_\mathfrak{p}$ (i.e. $pO_\mathfrak{p} = \mathfrak{p}$). Then, by elementary divisor theory, it is well-known that

(25) $$Y_l = U_\mathfrak{p}\begin{pmatrix} p^l & 0 \\ 0 & p^{-l}\end{pmatrix}U_\mathfrak{p} \quad (l = 0, 1, 2, \cdots)$$

gives all distinct $U_\mathfrak{p}$ double cosets contained in $G_\mathfrak{p}$, and that we have

(26) $$Y_l^{-1} = Y_l \quad (l = 0, 1, 2, \cdots); \; Y_0 = U_\mathfrak{p}.$$

Lemma 2. *We have*

(27) $$|Y_0\backslash Y_l| = q^{2l} + q^{2l-1} \; (l \geq 1),$$

and

(28) $$\sum_{l=0}^{\infty} Y_l u^l = \frac{(1-u)(1+qu)}{1-(Y_1-q+1)u+q^2u^2},$$

where the second formula implies the identity between two power series of u with coefficients in $\mathcal{H}(G_\mathfrak{p}, U_\mathfrak{p})$.

The proof of Lemma 2 will be given later, in §17.

Now, let Γ be a discrete subgroup of $G = G_\mathbf{R} \times G_\mathfrak{p}$ such that $\Gamma_\mathbf{R}$ and $\Gamma_\mathfrak{p}$ are dense in $G_\mathbf{R}$ and $G_\mathfrak{p}$ respectively. For each $l = 0, 1, 2, \cdots$, we put

(29) $$\Gamma^l = \{\gamma \in \Gamma \mid \gamma_\mathfrak{p} \in Y_l\}.$$

In particular, $\Gamma^0 = \Gamma \cap (G_\mathbf{R} \times U_\mathfrak{p})$ forms a subgroup of Γ;. and for any $\gamma \in \Gamma, \gamma^{-1}\Gamma^0\gamma$ and Γ^0 are commensurable with each other. It is obvious that we have $\Gamma^0 \cdot \Gamma^l \cdot \Gamma^0 = \Gamma^l$ for each $l \geq 0$, because $Y_0Y_lY_0 = Y_l$ $(l \geq 0)$ holds; and moreover, each Γ^l consists of a single Γ^0-double-coset. In fact, let $\gamma, \gamma' \in \Gamma^l$. Then $\gamma_\mathfrak{p}, \gamma'_\mathfrak{p} \in Y_l = U_\mathfrak{p}\begin{pmatrix} p^l & 0 \\ 0 & p^{-l}\end{pmatrix}U_\mathfrak{p}$; hence there exist $u_\mathfrak{p}, u'_\mathfrak{p} \in Y_0 = U_\mathfrak{p}$ such that $\gamma'_\mathfrak{p} = u_\mathfrak{p}\gamma_\mathfrak{p}u'_\mathfrak{p}$. Recall that $\Gamma_\mathfrak{p}$ is dense in $G_\mathfrak{p}$, and take $\delta_\mathfrak{p} \in \Gamma_\mathfrak{p}^0$ which is sufficiently near $u_\mathfrak{p}$. Then $\delta'_\mathfrak{p} = \gamma'^{-1}_\mathfrak{p}\delta_\mathfrak{p}\gamma_\mathfrak{p}$ is sufficiently near $u'^{-1}_\mathfrak{p}$ and hence is contained in $U_\mathfrak{p}$. On the other hand, $\delta'_\mathfrak{p}$ is in $\Gamma_\mathfrak{p}$; hence we have $\delta_\mathfrak{p}\gamma_\mathfrak{p}\delta'^{-1}_\mathfrak{p} = \gamma'_\mathfrak{p}$ with $\delta_\mathfrak{p}, \delta'_\mathfrak{p} \in \Gamma_\mathfrak{p}^0$. Therefore, each Γ^l consists of a single Γ^0-double coset. Now, since we have $U_\mathfrak{p}\Gamma_\mathfrak{p} = G_\mathfrak{p}$ and $U_\mathfrak{p} \cap \Gamma_\mathfrak{p} = \Gamma_\mathfrak{p}^0$, it is now clear that the projection $\Gamma \to \Gamma_\mathfrak{p} \subset G_\mathfrak{p}$ induces a canonical isomorphism of $\mathcal{H}(\Gamma, \Gamma^0)$ and $\mathcal{H}(G_\mathfrak{p}, U_\mathfrak{p})$, which sends to Γ^l to Y_l $(l \geq 0)$. So, by Lemma 2, we get:

Lemma 2′. *We have*

(30) $$|\Gamma^0\backslash\Gamma^l| = q^{2l} + q^{2l-1} \quad (l \geq 1),$$

and

(31) $$\sum_{l=0}^{\infty} \Gamma^l u^l = \frac{(1-u)(1+qu)}{1-(\Gamma^1-q+1)u+q^2u^2},$$

where the second formula implies the identity between two power series of u with coefficients in $\mathcal{H}(\Gamma,\Gamma^0)$. Moreover, each Γ^l is self-inverse (and hence $\mathcal{H}(\Gamma,\Gamma^0)$ is commutative).

§11. Before stating the third lemma, we need some alternative definition of $\zeta_\Gamma(u)$, which is simple in our case where Γ is torsion-free. Now, Γ being assumed torsion-free, each $\Gamma_z \neq \{1\}$ is isomorphic to the infinite cyclic group. We recall that $\gamma \in \Gamma$ is called elliptic if $\gamma_{\mathbf{R}}$ is elliptic, and hence equivalently, if $\gamma \neq 1$ and $\gamma \in \Gamma_z$ for some z. Such z is unique; hence we may write $\gamma = \gamma_z$. An elliptic element $\gamma \in \Gamma$ will be called *primitive*, if $\gamma = \gamma_z$ generates Γ_z. Thus it is clear that an elliptic element can be expressed uniquely as a positive integral power of a primitive elliptic element of Γ. If $\gamma = \gamma_z$ is elliptic, and if $\delta \in \Gamma$, then $\delta\gamma\delta^{-1}$ is elliptic, being contained in $\Gamma_{\delta_{\mathbf{R}}z}$. If moreover γ is primitive, then $\delta\gamma\delta^{-1}$ is also primitive, since it generates $\Gamma_{\delta_{\mathbf{R}}z} = \delta\Gamma_z\delta^{-1}$. So, we shall call a Γ-conjugacy class $\{\gamma\}_\Gamma$ *elliptic*, if γ is so, and *primitive*, if γ is moreover primitive. Since Γ is torsion-free, it is clear by Proposition 3 (§4) that, if γ is elliptic, then the eigenvalues $\pm\{\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{p}}^{-1}\}$ of $\gamma_{\mathfrak{p}}$ are contained in $k_{\mathfrak{p}}$, and are not in $\mathcal{U}_{\mathfrak{p}}$.

Proposition 4. *Let $\{\gamma\}_\Gamma$ be an elliptic Γ-conjugacy class. Then, $\{\gamma\}_\Gamma \neq \{\gamma^{-1}\}_\Gamma$.*

Proof. It is enough to show that $\gamma_{\mathbf{R}}^{-1}$ and $\gamma_{\mathbf{R}}$ are not conjugate in $G_{\mathbf{R}}$. Suppose, on the contrary, that we had $\gamma_{\mathbf{R}}^{-1} = g_{\mathbf{R}} \cdot \gamma_{\mathbf{R}} \cdot g_{\mathbf{R}}^{-1}$ with some $g_{\mathbf{R}} \in G_{\mathbf{R}}$. Let z be the fixed point of $\gamma_{\mathbf{R}}, \gamma_{\mathbf{R}}^{-1}$. Then $\gamma_{\mathbf{R}}^{-1}(g_{\mathbf{R}} \cdot z) = g_{\mathbf{R}} \cdot \gamma_{\mathbf{R}} \cdot z = g_{\mathbf{R}} \cdot z$; hence $g_{\mathbf{R}} \cdot z$ is also fixed by $\gamma_{\mathbf{R}}^{-1}$. Therefore we have $g_{\mathbf{R}} \cdot z = z$; hence $g_{\mathbf{R}} \in G_{z,\mathbf{R}}$. Since $G_{z,\mathbf{R}}$ is abelian, this implies $g_{\mathbf{R}}\gamma_{\mathbf{R}}g_{\mathbf{R}}^{-1} = \gamma_{\mathbf{R}}$, hence $\gamma_{\mathbf{R}}^{-1} = \gamma_{\mathbf{R}}$. But this is a contradiction, since $\gamma_{\mathbf{R}} \neq 1$ and, by assumption, Γ has no elements of finite order. □

Proposition 5. *$\wp(\Gamma)$ is in one-to-one correspondence with the set of all mutually inverse pairs $\{\gamma^{\pm 1}\}_\Gamma$ of primitive elliptic Γ-conjugacy classes.*

Proof. This is immediate, if we recall the definitions of $\wp(\Gamma)$ (§3) and of primitive elliptic Γ-conjugacy classes. The one-to-one correspondence is defined as follows. Take any $P \in \wp(\Gamma)$ and a Γ-fixed point $z \in \mathfrak{H}$ contained in the Γ-equivalence class P. Then Γ_z is the infinite cyclic group. Let γ, γ^{-1} be its generators. Then $P \mapsto \{\gamma^{\pm 1}\}_\Gamma$ gives the desired one-to-one correspondence. □

§12. Let $\{\gamma\}_\Gamma$ be any elliptic Γ-conjugacy class, and let $\pm\{\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{p}}^{-1}\}$ be the eigenvalues of $\gamma_{\mathfrak{p}}$. We know that $\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{p}}^{-1}$ are in $k_{\mathfrak{p}}$ and not in $\mathcal{U}_{\mathfrak{p}}$. Put

(32) $$\deg\{\gamma\}_\Gamma = |\operatorname{ord}_{\mathfrak{p}} \lambda_{\mathfrak{p}}|.$$

It is clear that this is a well-defined *positive* integer, and that for any $r \in \mathbf{Z}$, we have $\deg\{\gamma^r\}_\Gamma = |r| \deg\{\gamma\}_\Gamma$. Moreover, if a pair $\{\gamma^{\pm 1}\}_\Gamma$ of mutually inverse primitive elliptic conjugacy classes corresponds to $P \in \wp(\Gamma)$, then, $\deg P = \deg\{\gamma\}_\Gamma$ holds. (Recall the definition of $\deg P$ for $P \in \wp(\Gamma)$).

$$(33) \qquad \wp(\Gamma) \ni P \leftrightarrow \{\gamma^{\pm 1}\}_\Gamma\text{: primitive elliptic } \Rightarrow \deg P = \deg\{\gamma\}_\Gamma.$$

So, our ζ function $\zeta_\Gamma(u)$ can also be defined as

$$(34) \qquad \zeta_\Gamma(u) = \prod_{\{\gamma^{\pm 1}\}_\Gamma} (1 - u^{\deg\{\gamma^{\pm 1}\}_\Gamma})^{-1},$$

where $\{\gamma^{\pm 1}\}_\Gamma$ runs over all pairs of mutually inverse primitive elliptic Γ-conjugacy classes. We shall need the following alternative definition of $\deg\{\gamma\}_\Gamma$;

Proposition 6. *For each $\gamma \in \Gamma^l$, we put $l(\gamma) = l$. Let $\{\gamma\}_\Gamma$ be an elliptic Γ-conjugacy class. Then we have:*

$$(35) \qquad \deg\{\gamma\}_\Gamma = \mathrm{Min}_{x \in \{\gamma\}_\Gamma} l(x).$$

Proof. Since γ is elliptic (and γ is of infinite order, since Γ is assumed torsion-free), by Proposition 3, there is an element $g_\mathfrak{p} \in G_\mathfrak{p}$ such that $g_\mathfrak{p}^{-1}\gamma_\mathfrak{p} g_\mathfrak{p} = \begin{pmatrix} \lambda_\mathfrak{p} & 0 \\ 0 & \lambda_\mathfrak{p}^{-1} \end{pmatrix}$ with $\lambda_\mathfrak{p} \in k_\mathfrak{p}$; and we have $\deg\{\gamma\}_\Gamma = |\mathrm{ord}_\mathfrak{p}(\lambda_\mathfrak{p})|$. Put $d = \deg\{\gamma\}_\Gamma$. Then, $g_\mathfrak{p}^{-1}\gamma_\mathfrak{p} g_\mathfrak{p} = \begin{pmatrix} \lambda_\mathfrak{p} & 0 \\ 0 & \lambda_\mathfrak{p}^{-l} \end{pmatrix} \in U_\mathfrak{p}\begin{pmatrix} p^d & 0 \\ 0 & p^{-d} \end{pmatrix} U_\mathfrak{p} = Y_d$; where $U_\mathfrak{p} = PSL(O_\mathfrak{p})$ and p is a prime element of $k_\mathfrak{p}$. Let $\delta_\mathfrak{p} \in \Gamma_\mathfrak{p}$ be sufficiently near $g_\mathfrak{p}$. Then $\delta_\mathfrak{p}^{-1}\gamma_\mathfrak{p}\delta_\mathfrak{p} \in Y_d$. So, if $\delta \in \Gamma$ corresponds to $\delta_\mathfrak{p}$, we have $l(\delta^{-1}\gamma\delta) = d$; hence we have $d \geq \mathrm{Min}_{x \in \{\gamma\}_\Gamma} l(x)$. Now let γ' be any element of $\{\gamma\}_\Gamma$, and put $\gamma'_\mathfrak{p} = \pm\begin{pmatrix} a_\mathfrak{p} & b_\mathfrak{p} \\ c_\mathfrak{p} & d_\mathfrak{p} \end{pmatrix} \in G_\mathfrak{p}$. Put $l' = l(\gamma')$; hence $\gamma'_\mathfrak{p} \in Y_{l'}$. This implies that the entries of $p^{l'}\begin{pmatrix} a_\mathfrak{p} & b_\mathfrak{p} \\ c_\mathfrak{p} & d_\mathfrak{p} \end{pmatrix}$ are integers. Therefore, its eigenvalues $\pm\{p^{l'}\lambda_\mathfrak{p}, p^{l'}\lambda_\mathfrak{p}^{-1}\}$, must also be integers; which implies $l' \geq |\mathrm{ord}_\mathfrak{p}\lambda_\mathfrak{p}| = d$; hence we get $d \leq \mathrm{Min}_{x \in \{\gamma\}_\Gamma} l(x)$. □

§13. Now, the third lemma is on a relation between Γ- and Γ^0-conjugacy classes. By Proposition 6, if $\{\gamma\}_\Gamma$ is elliptic, then $\{\gamma\}_\Gamma \cap \Gamma^l = \phi$ for $l < \deg\{\gamma\}_\Gamma$. We have:

Lemma 3. *Let $\{\gamma\}_\Gamma$ be a primitive elliptic Γ-conjugacy class, put $d = \deg\{\gamma\}_\Gamma$, and let $r \geq 1$. Then,* (i) *$\{\gamma^r\}_\Gamma \cap \Gamma^{dr}$ consists of exactly d distinct Γ^0-conjugacy classes.* (ii) *If $k \geq 1$, then $\{\gamma^r\}_\Gamma \cap \Gamma^{dr+k}$ consists of exactly $dq^{k-1}(q-1)$ distinct Γ^0-conjugacy classes.*

The proof, which requires some preliminary studies on the structure of $PL_2(k_\mathfrak{p})$, will be given later, in §19.[5]

Corollary . *Let $A_m (m \geq 1)$ be the one-half of the number of elliptic Γ^0-conjugacy classes contained in Γ^m, and let N_m $(m \geq 1)$ be, as in §6 (16), the sum of all $\deg P$ for all*

[5]An alternative and easier proof is given in Part 2, §30, in the proof of Corollary of Theorem 4.

$P \in \wp(\Gamma)$ with $\deg P | m$*:*

$$A_m = \frac{1}{2}\#\{\textit{elliptic } \Gamma^0\textit{-conjugacy classes in } \Gamma^m\}$$

$$N_m = \sum_{\substack{P \in \wp(\Gamma), \\ \deg P | m}} \deg P.$$

Then, they are both finite, and we have:

$$A_m = N_m + (q-1)\sum_{k=1}^{m-1} q^{k-1} N_{m-k} \qquad (m \geq 1) \tag{36}$$

$$N_m = A_m - (q-1)\sum_{k=1}^{m-1} A_{m-k} \qquad (m \geq 1). \tag{37}$$

Proof. The finiteness of A_m is a special case of Lemma 1, applied to $\tilde{\Delta} = \Gamma_{\mathbf{R}}, \Delta = \Gamma^0_{\mathbf{R}}$. To show the finiteness of N_m, it is enough to show that there are at most finitely many elliptic Γ-conjugacy classes $\{\gamma\}_\Gamma$ with a given degree d. But, by Proposition 6, such $\{\gamma\}_\Gamma$ intersects Γ^d and the intersection $\{\gamma\}_\Gamma \cap \Gamma^d$ is a union of (several) elliptic Γ^0-conjugacy classes. Therefore, the finiteness of N_m follows immediately from that of A_d for $d|m$.

Now, (36) is a direct consequence of Proposition 6 and Lemma 3. In fact, each elliptic Γ^0-conjugacy class contained in Γ^m defines an elliptic Γ-conjugacy class, which can be written as $\{\gamma^r\}_\Gamma$, where $\{\gamma\}_\Gamma$ is primitive and $r \geq 1$. If we put $d = \deg\{\gamma\}_\Gamma$, then, by Proposition 6, we have $rd \leq m$. So, fix k $(0 \leq k \leq m-1)$, and for each $d|m-k$, consider all primitive elliptic Γ-conjugacy classes $\{\gamma\}_\Gamma$ of degree d. Put $rd = m - k$. Then, $\{\gamma^r\}_\Gamma \cap \Gamma^m = \{\gamma^r\}_\Gamma \cap \Gamma^{rd+k}$ consists of d $(k = 0)$ or $dq^{k-1}(q-1)$ $(k > 0)$ distinct Γ^0-conjugacy classes (Lemma 3). Therefore, we have:

$$2A_m = \sum_{k=0}^{m-1}\sum_{d|m-k} \#\{\{\gamma\}_\Gamma;\ \text{primitive, elliptic, degree } d\} \times \begin{cases} d & \cdots k = 0, \\ dq^{k-1}(q-1) & \cdots k > 0. \end{cases}$$

$$= \sum_{k=0}^{m-1} \sum_{\substack{\{\gamma\}_\Gamma;\ \text{primitive elliptic} \\ \deg\{\gamma\}_\Gamma | m-k}} \deg\{\gamma\}_\Gamma \times \begin{cases} 1 & \cdots k = 0, \\ q^{k-1}(q-1) & \cdots k > 0. \end{cases}$$

So, by Proposition 5 and (33), we get

$$A_m = N_m + (q-1)\sum_{k=1}^{m-1} q^{k-1} N_{m-k},$$

which settles (36). Now, (37) is a formal consequence of (36). In fact, it can be checked directly, by substituting (36) on the right side of (37). □

The proof of Theorem 1 assuming Lemmas 2, 3.

§14. We have

$$N_m = A_m - (q-1)\sum_{k=1}^{m-1} A_{m-k}. \tag{37}$$

Apply Lemma 1 for $\tilde{\Delta} = \Gamma_{\mathbf{R}}, \Delta = \Gamma^0_{\mathbf{R}}$. Since we can identify $\mathcal{H}(\Gamma, \Gamma^0)$ with $\mathcal{H}(\Gamma_{\mathbf{R}}, \Gamma^0_{\mathbf{R}})$, we consider d, ρ as representations of $\mathcal{H}(\Gamma, \Gamma^0)$. Since, by (30), we have $d(\Gamma^m) = |\Gamma^0\backslash\Gamma^m| = q^{2m} + q^{2m-1}$, we get

$$A_m = q^{2m} + q^{2m-1} - \operatorname{tr}\rho(\Gamma^m) \qquad (m \geqq 1). \tag{38}$$

By substituting (38) in (37), we get

$$N_m = q^{2m} + q - \operatorname{tr}\rho\{\Gamma^m - (q-1)\sum_{k=1}^{m-1}\Gamma^{m-k}\}. \tag{39}$$

Since $\operatorname{tr}\rho(I) = g$, the genus of $\Gamma^0_{\mathbf{R}}\backslash\mathfrak{H}$, we get

$$N_m = q^{2m} + 1 - (q-1)(g-1) - \operatorname{tr}\rho\{\Gamma^m - (q-1)\sum_{k=1}^{m}\Gamma^{m-k}\}. \tag{40}$$

On the other hand, by (31) (Lemma 2′) we get

$$\frac{1-qu}{1-u}\sum_{m=0}^{\infty}\Gamma^m u^m = \frac{1-q^2u^2}{1-(\Gamma^1 - q + 1)u + q^2u^2}; \tag{41}$$

and by a simple computation, we see that the left side of (41) is equal to

$$\sum_{m=1}^{\infty}\left\{\Gamma^m - (q-1)\sum_{k=1}^{m}\Gamma^{m-k}\right\}u^m. \tag{42}$$

Put

$$1 - (\Gamma^1 - q + 1)u + q^2u^2 = (1-\pi u)(1-\pi' u) \tag{43}$$

formally, with $\pi\pi' = \pi'\pi = q^2$. Then,

$$\begin{aligned}\frac{1}{(1-\pi u)(1-\pi' u)} &= \sum_{m=0}^{\infty}(\pi^m + \pi^{m-1}\pi' + \cdots + \pi'^m)u^m \\ &= 1 + \sum_{m=1}^{\infty}(\pi^m + \pi'^m)u^m + q^2u^2\frac{1}{(1-\pi u)(1-\pi' u)};\end{aligned} \tag{44}$$

hence we get

$$\frac{1-q^2u^2}{(1-\pi u)(1-\pi' u)} = 1 + \sum_{m=1}^{\infty}(\pi^m + \pi'^m)u^m. \tag{45}$$

Therefore, by (41), we get

$$\Gamma^m - (q-1)\sum_{k=1}^{m}\Gamma^{m-k} = \pi^m + \pi'^m \qquad (m \geq 1). \tag{46}$$

This is a formal computation, but this shows that if χ is a linear representation of the ring $\mathcal{H}(\Gamma,\Gamma^0)$, and if we put

$$1-(\chi(\Gamma^1)-q+1)u+q^2u^2=(1-\pi u)(1-\pi' u),$$

then

$$\chi(\Gamma^m)-(q-1)\sum_{k=1}^{m}\chi(\Gamma^{m-k})=\pi^m+\pi'^m \qquad (m\geq 1) \tag{47}$$

holds. Now, by Lemma 1, ρ is a direct sum of g linear representations:

$$\rho=\chi_1\oplus\cdots\oplus\chi_g;$$

so, by putting

$$1-(\chi_i(\Gamma^1)-q+1)u+q^2u^2=(1-\pi_i u)(1-\pi_i' u) \quad (1\leq i\leq g, \pi_i\pi_i'=q^2) \tag{48}$$

we get

$$\chi_i(\Gamma^m)-(q-1)\sum_{k=1}^{m}\chi_i(\Gamma^{m-k})=\pi_i^m+\pi_i'^m \quad (1\leq i\leq g,\ m\geq 1). \tag{49}$$

So, by summing over i $(1\leq i\leq g)$, we obtain:

$$\mathrm{tr}\,\rho\{\Gamma^m-(q-1)\sum_{k=1}^{m}\Gamma^{m-k}\}=\sum_{i=1}^{g}(\pi_i^m+\pi_i'^m); \tag{50}$$

and hence, by (40), we get

$$N_m=q^{2m}+1-(q-1)(g-1)-\sum_{i=1}^{g}(\pi_i^m+\pi_i'^m) \quad (m\geq 1); \tag{51}$$

and hence we get

$$\zeta_\Gamma(u)=\exp\sum_{m=1}^{\infty}\frac{N_m}{m}u^m=\frac{\prod_{i=1}^{g}(1-\pi_i u)(1-\pi_i' u)}{(1-u)(1-q^2u)}\times(1-u)^{(q-1)(g-1)}. \tag{52}$$

Since (48) are the eigenvalues of $1-(\rho(\Gamma^1)-q+1)u+q^2u^2$, we have

$$\zeta_\Gamma(u)=\frac{\det\{1-(\rho(\Gamma^1)-q+1)u+q^2u^2\}}{(1-u)(1-q^2u)}\times(1-u)^{(q-1)(g-1)}. \tag{53}$$

That π_i,π_i' $(1\leq i\leq g)$ are algebraic integers follows immediately from (51) (for $m=1,\cdots,2g$). □

So, we have also shown:

A SUPPLEMENT TO THEOREM 1. *The numerator of the main factor of $\zeta_\Gamma(u)$ is given by:*

$$\prod_{i=1}^{g}(1-\pi_i u)(l-\pi_i' u)=\det\{1-(\rho(\Gamma^1)-q+1)u+q^2u^2\}. \tag{54}$$

Proofs of Lemmas 2, 3.

§15. Put

$$X = PL_2(k_\mathfrak{p}) = GL_2(k_\mathfrak{p})/k_\mathfrak{p}^\times. \tag{55}$$

Then, for any element $x \in X$, we can take its representative $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mod $k_\mathfrak{p}^\times$ such that a, b, c, d are all contained in $O_\mathfrak{p}$, but not all are in $\mathfrak{p}$. Put $(ad - bc)O_\mathfrak{p} = \mathfrak{p}^{l(x)}$. Then, $l(x)$ is a non-negative integer, well-defined by x. We shall call it the *length* of x. It is clear that we have

$$\begin{aligned} l(x_1 x_2 \cdots x_n) &\le l(x_1) + \cdots + l(x_n) \\ &\equiv l(x_1) + \cdots + l(x_n) \pmod 2, \end{aligned} \tag{56}$$

for any $x_1, \cdots, x_n \in X$. Put

$$X_l = \{x \in X \mid l(x) = l\}. \tag{57}$$

In particular,

$$X_0 = PL_2(O_\mathfrak{p}) = GL_2(O_\mathfrak{p})/\mathcal{U}_\mathfrak{p} \tag{58}$$

is an open compact subgroup of X; and it is well-known by elementary divisor theory, that each X_l consists of a single X_0-double-coset;

$$X_l = X_0 \begin{pmatrix} p^l & 0 \\ 0 & 1 \end{pmatrix} X_0, \text{ where } p \text{ is any prime element of } k_\mathfrak{p}. \tag{59}$$

Since X_0 is open compact, for any $x \in X$, the subgroups $x^{-1}X_0 x$ and X_0 are commensurable with each other; hence $|X_0 \backslash X_l|$ for each $l \ge 0$ is finite, and the Hecke ring $\mathcal{H}(X, X_0)$ can be defined. Moreover, since $l(x^{-1}) = l(x)$ for each $x \in X$, each X_l is self-inverse, and hence $\mathcal{H}(X, X_0)$ is commutative. Now, the following lemma is a very well-known one:

LEMMA 4. *Let p be a prime element of $k_\mathfrak{p}$, and let $l \ge 1$. Then the following set of matrices mod $k_\mathfrak{p}^\times$ forms a set of representatives of $X_0 \backslash X_l$;*

$$\left\{ \begin{pmatrix} p^m & \alpha \\ 0 & p^n \end{pmatrix}; \begin{array}{c} m, n \ge 0, m + n = l \\ \alpha : \textit{representatives of } O_\mathfrak{p} \pmod{\mathfrak{p}^n} \\ \textit{If } m, n \textit{ are both} > 0, \textit{ then } \alpha \not\equiv 0 \pmod{\mathfrak{p}} \end{array} \right\}. \tag{60}$$

In particular, we have

$$X_1 = X_0 \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_{\alpha \bmod \mathfrak{p}} X_0 \begin{pmatrix} 1 & \alpha \\ 0 & p \end{pmatrix} \quad \text{(disjoint)}; \tag{61}$$

hence we have $|X_0 \backslash X_1| = 1 + q$.

§16. Now we shall prove the following two equivalent lemmas; Lemmas 5, 5′.

LEMMA 5. *Put* $X_1 = \sum_{i=0}^{q} X_0\pi_i$ *(disjoint). Then,*

(i) *For each* i $(0 \le i \le q)$*, there exists a unique suffix* j $(0 \le j \le q)$ *such that* $\pi_j\pi_i \in X_0$. *We shall put* $j = \rho(i)$ $(0 \le i \le q)$.

(ii) *Any element* $x \in X_l$ $(l \ge 0)$ *can be expressed uniquely in the form:*

$$x = u\pi_{i_1}\pi_{i_2}\cdots\pi_{i_l},\ \text{with}\ u \in X_0,\ i_n \ne \rho(i_{n+1})\ (1 \le \forall n \le l-1). \tag{62}$$

Conversely, an element $x \in X$ *of the form* (62) *is contained in* X_l. *In short, we have*

$$X_l = \sum\nolimits' X_0\pi_{i_1}\cdots\pi_{i_l}, \tag{63}$$

where the disjoint union $\sum'$ *is over all* $\{i_1, \cdots, i_l\}$ *such that* $i_n \ne \rho(i_{n+1})$ *for all* n $(1 \le n \le l)$.

We note that (i) is trivial, since $j = \rho(i)$ is uniquely determined by $X_0\pi_j = X_0\pi_i^{-1}$. This is merely for a better understanding of (ii).

LEMMA 5′. *As elements of* $\mathcal{H}(X, X_0)$*, we have*

$$X_1^2 = X_2 + (q+1)X_0, \tag{64}$$

$$X_1X_l = X_lX_1 = X_{l+1} + qX_{l-1} \quad (l \ge 2). \tag{65}$$

This Lemma 5′ is more or less well-known. We shall prove Lemma 5 (ii) and Lemma 5′ in the following order;
Lemma 5 (ii) for a particular $\pi_0, \cdots, \pi_q \Rightarrow$ Lemma 5′ $\Rightarrow$ Lemma 5 (ii) for any $\pi_0, \cdots, \pi_q$.

PROOF. Let p be a prime element of $k_\mathfrak{p}$, and let $\alpha_1 = 0, \alpha_2, \cdots, \alpha_q$ be a set of representatives of $O_\mathfrak{p}$ mod $\mathfrak{p}$. Put

$$\pi_0 = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \pi_i = \begin{pmatrix} 1 & \alpha_i \\ 0 & p \end{pmatrix} \quad (1 \le i \le q). \tag{66}$$

By (61), we have $X_1 = \sum_{i=0}^{q} X_0\pi_i$ (disjoint). Since

$$\pi_0\pi_i = \begin{pmatrix} p & p\alpha_i \\ 0 & p \end{pmatrix} \equiv \begin{pmatrix} 1 & \alpha_i \\ 0 & 1 \end{pmatrix} \quad (\text{mod } k_\mathfrak{p}^\times),$$

we have $\pi_0\pi_i \in X_0$ for $1 \le i \le q$, and hence $\rho(i) = 0$ $(1 \le i \le q)$. Since

$$\pi_1\pi_0 = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (\text{mod } k_\mathfrak{p}^\times),$$

we have $\pi_1\pi_0 \in X_0$; hence $\rho(0) = 1$. So, to show Lemma 5 (ii), it is enough to show that:

$$X_l = \sum_{s=0}^{l} \sum_{\substack{i_1,\cdots,i_{l-s} \ge 1, \\ i_{l-s} > 1 \text{ if } s > 0}} X_0\pi_{i_1}\cdots\pi_{i_{l-s}}\pi_0^s \quad (\text{disjoint}). \tag{67}$$

But we have

$$\pi_{i_1}\cdots\pi_{i_{l-s}}\pi_0^s = \begin{pmatrix} p^s & \alpha_{i_{l-s}} + \alpha_{i_{l-s-1}}p + \cdots + \alpha_{i_1}p^{l-s-1} \\ 0 & p^{l-s} \end{pmatrix}.$$

Hence, (67) follows immediately from Lemma 4. So, Lemma 5 (ii) is proved for the particular $\pi_0, \cdots, \pi_q$ given by (66). This also shows $|X_0\backslash X_l| = q^l + q^{l-1}$ $(l \geq 1)$.

Now let us prove Lemma 5′. Let $\pi_0, \cdots, \pi_q$ be as in (66). Then we have $X_1 = \sum_{i=0}^q X_0\pi_i$; hence $X_1^2 = \sum_{i,j} X_0\pi_j\pi_i$, multiplicity being taken into account. Hence

$$X_1^2 = \sum_{i,j\ j\neq\rho(i)} X_0\pi_j\pi_i + \sum_{i,j\ j=\rho(i)} X_0\pi_j\pi_i = X_2 + \sum_{j=\rho(i)} X_0 = X_2 + (q+1)X_0.$$

By Lemma 5 (ii) for these $\pi_0, \cdots, \pi_q$, we have $X_l = \sum_{i_n\neq\rho(i_{n+1}),\ \forall n} X_0\pi_{i_1}\cdots\pi_{i_l}$. So,

$$\begin{aligned}
X_1X_l &= \sum_{i=0}^{q} \sum_{i_n\neq\rho(i_{n+1})} X_0\pi_i\pi_{i_1}\cdots\pi_{i_l} \\
&= \sum_{\substack{i_n\neq\rho(i_{n+1}),\\ i\neq\rho(i_1)}} X_0\pi_i\pi_{i_1}\cdots\pi_{i_l} + \sum_{\substack{i_n\neq\rho(i_{n+1}),\\ i=\rho(i_1)}} X_0\pi_i\pi_{i_1}\cdots\pi_{i_l} \\
&= X_{l+1} + \sum_{\substack{i_n\neq\rho(i_{n+1}),\\ 1\leq n\leq l-1}} X_0\pi_{i_2}\cdots\pi_{i_l} \\
&= X_{l+1} + \sum_{i_1\neq\rho(i_2)} \sum_{\substack{i_n\neq\rho(i_{n+1}),\\ 2\leq n\leq l-1}} X_0\pi_{i_2}\cdots\pi_{i_l} \\
&= X_{l+1} + qX_{l-1} \quad (\geq 2).
\end{aligned}$$

Since $\mathcal{H}(X, X_0)$ is commutative, we have $X_lX_1 = X_1X_l = X_{l+1} + qX_{l-1}$; hence Lemma 5′ is proved.

Finally, let us prove Lemma 5 (ii) for an arbitrary set $\pi_0, \pi_1, \cdots, \pi_q$ of representatives of $X_0\backslash X_1$; $X_1 = \sum_{i=0}^q X_0\pi_i$. By (65), we obtain

$$X_1^l = X_l + cX_{l-2} + c'X_{l-4} + \cdots \quad (l \geq 1), \tag{68}$$

where $c, c', \cdots$ are non-negative integers. In fact, it is trivial for $l = 1$; so, assume that (68) is true for some $l \geq 1$, and multiply X_1 on both sides. Then from (65) follows directly that (68) is also true for $l + 1$. Now, the expression of X_1^l by the formal sum of left X_0-cosets, multiplicities being taken into account, will be

$$\sum X_0\pi_{i_1}\cdots\pi_{i_l} = \sum{}' X_0\pi_{i_1}\cdots\pi_{i_l} + \text{ lower length terms },\tag{69}$$

where the first formal sum $\sum$ is over all $0 \leq i_1, \cdots, i_l \leq q$, and the second one, $\sum'$, is over all $0 \leq i_1, \cdots, i_l \leq q$, with $i_n \neq \rho(i_{n+1})$ for all n $(1 \leq n \leq l-1)$. On the other hand, the number of terms under $\sum'$ in (69) is $q^l + q^{l-1}$, which is equal to $|X_0\backslash X_l|$. Thus, by comparing (68) and (69), we see that all left X_0 cosets under $\sum'$ in (69) must be mutually distinct, elements of such left X_0 cosets have length l, and that

$$X_l = \sum{}' X_0\pi_{i_1}\cdots\pi_{i_l} \quad \text{(disjoint)};$$

which proves Lemma 5 (ii). □

Corollary 1. *We have*

$$|X_0\backslash X_l| = |X_l/X_0| = q^l + q^{l-1} \quad \textit{for } l \geq 1. \tag{70}$$

Remark. Since $X_l^{-1} = X_l$, we have $|X_l/X_0| = |X_0\backslash X_l|$.

Corollary 2. *We have*

$$\sum_{l=0}^{\infty} X_l u^l = \frac{1-u^2}{1-X_1u+qu^2}, \tag{71}$$

as an identity between two formal power series of u with coefficients in $\mathcal{H}(X, X_0)$.

Proof. That $(1-X_1u+qu^2)\sum_{l=0}^{\infty} X_l u^l = 1-u^2$ follows directly from Lemma 5′. □

§17. The proof of Lemma 2. Put

$$\begin{aligned} X' &= \{x \in X \mid l(x) \equiv 0 \pmod 2\} \\ &= \bigcup_{l=0}^{\infty} X_{2l}. \end{aligned} \tag{72}$$

$$\begin{tikzcd}[column sep=small] & X = PL_2(k_\mathfrak{p}) \arrow[d, dash, "2"'] \\ PSL_2(k_\mathfrak{p}) = G_\mathfrak{p} \arrow[r, dash] \arrow[d, dash] & X' = G_\mathfrak{p} X_0 \arrow[d, dash] \\ PSL_2(O_\mathfrak{p}) = U_\mathfrak{p} \arrow[r, dash] & X_0 = PL_2(O_\mathfrak{p}) \end{tikzcd}$$

Then, X' forms a subgroup of X with index 2. It is easy to see that if $X \ni x \mapsto \det x \in k_\mathfrak{p}^\times / k_\mathfrak{p}^{\times 2}$ is the homomorphism of X onto $k_\mathfrak{p}^\times / k_\mathfrak{p}^{\times 2}$ induced from the determinant map: $GL_2(k_\mathfrak{p}) \ni x \mapsto \det x \in k_\mathfrak{p}^\times$, then we have

$$\begin{aligned} X' &= \{x \in X \mid \det x \in k_\mathfrak{p}^{\times 2}\mathcal{U}_\mathfrak{p} / k_\mathfrak{p}^{\times 2}\} \\ &= \{x \in X \mid \mathrm{ord}_\mathfrak{p}(\det x) \equiv 0 \pmod 2\} \\ &= PL_2(O_\mathfrak{p}) \cdot PSL_2(k_\mathfrak{p}) = X_0 \cdot G_\mathfrak{p}. \end{aligned} \tag{73}$$

On the other hand, (71) gives rise to

$$2\sum_{l=0}^{\infty} X_{2l}u^{2l} = \sum_{l=0}^{\infty} X_l u^l + \sum_{l=0}^{\infty} X_l(-u)^l = \frac{2(1-u^2)(1+qu^2)}{(1+qu^2)^2 - X_1^2u^2};$$

hence we get

$$\sum_{l=0}^{\infty} X_{2l}u^l = \frac{(1-u)(1+qu)}{1-(X_2-q+1)u+q^2u^2}. \tag{74}$$

So, to prove Lemma 2, it is enough to show that $\mathcal{H}(G_\mathfrak{p}, U_\mathfrak{p})$ and $\mathcal{H}(X', X_0)$ are canonically isomorphic, i.e. there is an isomorphism which maps Y_l on X_{2l} ($l \geq 1$). To see this, we remark that, in general, if $G_1 \supset G_2$, H_1 are three groups such that $G_1 = G_2H_1$; $x^{-1}G_2x \sim G_2$ ($\sim$: commensurability, $\forall x \in G_1$), $x^{-1}H_2x \sim H_2$ ($\forall x \in H_1$; $H_2 = H_1 \cap G_2$), and that $G_2h_1G_2 \cap H_1 = H_2h_1H_2$ ($\forall h_1 \in H_1$), then the two Hecke rings $\mathcal{H}(G_1, G_2)$, $\mathcal{H}(H_1, H_2)$ defined with respect to (say) left coset decompositions are canonically isomorphic; i.e., $H_2h_1H_2 \in \mathcal{H}(H_1, H_2)$ corresponds to $G_2h_1G_2 \in \mathcal{H}(G_1, G_2)$. This follows immediately from the definition of the Hecke rings. Thus, to show that $\mathcal{H}(G_\mathfrak{p}, U_\mathfrak{p})$ and $\mathcal{H}(X', X_0)$ are isomorphic by $Y_l \mapsto X_{2l}$ ($l \geq 0$), it is enough to check $X_{2l} \cap G_\mathfrak{p} = Y_l$ ($l \geq 0$), since we know that Y_l is a single $U_\mathfrak{p}$ double coset. But $Y_l = U_\mathfrak{p}\begin{pmatrix} p^l & 0 \\ 0 & p^{-l} \end{pmatrix}U_\mathfrak{p}$ consists of all elements $g_\mathfrak{p} \in G_\mathfrak{p} = PSL_2(k_\mathfrak{p})$ with elementary divisors p^{-l}, p^l; i.e., all elements $g_\mathfrak{p} \in G_\mathfrak{p} \cap X_{2l}$; hence the Lemma 2 is proved. □

§18. For the proof of Lemma 3, we need some more lemmas, which are direct consequences of Lemma 5.[6]

Let $x_1, \cdots, x_n \in X = PL_2(k_p)$. We shall say that the product $x_1 \cdot \cdots \cdot x_n$ is *free*, if

$$l(x_1 \cdot \cdots \cdot x_n) = l(x_1) + \cdots + l(x_n) \tag{75}$$

holds.

LEMMA 6. *Let $x, y, z \in X, y \notin X_0$. If the two products $x \cdot y, y \cdot z$ are free, then the product $x \cdot y \cdot z$ is also free.*

PROOF. Let $\pi_0, \cdots, \pi_q$ be as in Lemma 5, and factorize $z = u\pi_{\lambda_1} \cdots \pi_{\lambda_l}$, $yu = u'\pi_{\mu_1} \cdots \pi_{\mu_m}$, $xu' = u''\pi_{\nu_1} \cdots \pi_{\nu_n}$, where $u, u', u'' \in X_0, l = l(z), m = l(y) > 0, n = l(x)$ (see Lemma 5). By assumption, $y \cdot z, x \cdot y$ are free products; hence $\pi_{\mu_m}\pi_{\lambda_1} \notin X_0$, $\pi_{\nu_n}\pi_{\mu_1} \notin X_0$. Therefore, by Lemma 5, $xyz = u''\pi_{\nu_1} \cdots \pi_{\nu_n}\pi_{\mu_1} \cdots \pi_{\mu_m}\pi_{\lambda_1} \cdots \pi_{\lambda_l}$ has length $l + m + n$. □

LEMMA 7. *Let $x \cdot y$ be a free product, and let $xy = u\pi_{i_1} \cdots \pi_{i_l}$ be the factorization* (62) *of xy. Then, $x = u\pi_{i_1} \cdots \pi_{i_m}u'^{-1}$, $y = u'\pi_{i_{m+1}} \cdots \pi_{i_l}$ with some $u' \in X_0$, and with $m = l(x)$.*

PROOF. Let $y = u'\pi_{j_{m+1}} \cdots \pi_{j_l}$ be the factorization (62) for y. Since the factorization of xy can be obtained by factorizations of x and y, and then by carrying the elements of X_0 to the left (no influence to y-side!), we see directly by the uniqueness of factorization (62) for xy that $j_{m+1} = i_{m+1}, \cdots, j_l = i_l$, and hence $y = u'\pi_{i_{m+1}} \cdots \pi_{i_l}$ for some $u' \in X_0$. □

LEMMA 8. *Let $x, y \in X$, and put $l(xy) = l(x) + l(y) - 2d$. Then $d \leqq l(x), l(y)$; and if $x = x'' \cdot x'$, $y = y' \cdot y''$ are free products with $d \leqq l(x'), l(y')$, then $l(x'y') = l(x') + l(y') - 2d$.*

PROOF. The first assertion is clear.[7] Let

$$x = u\pi_{i_1} \cdots \pi_{i_l}, \quad y = u'\pi_{j_1} \cdots \pi_{j_m}$$

be the factorizations (62) for x, y. By Lemma 7,

$$x' = u''\pi_{i_s} \cdots \pi_{i_l}, \quad y' = u'\pi_{j_1} \cdots \pi_{j_t}u'''$$

with $u'', u''' \in X_0$, $l(x') = l - s + 1 \geq d$, $l(y') = t \geq d$. It is enough to prove that

$$l(\pi_{i_s} \cdots \pi_{i_l}u'\pi_{j_1} \cdots \pi_{j_t}) = (l - s + 1) + t - 2d.$$

This can be seen easily from the process of obtaining the factorization (62) for xy from that of x and y given above. □

LEMMA 9. *Let $x_1, \cdots, x_n$ be any elements of X and put*

$$l(x_ix_{i+1}) = l(x_i) + l(x_{i+1}) - 2d_i \quad (1 \leq i \leq n-1).$$

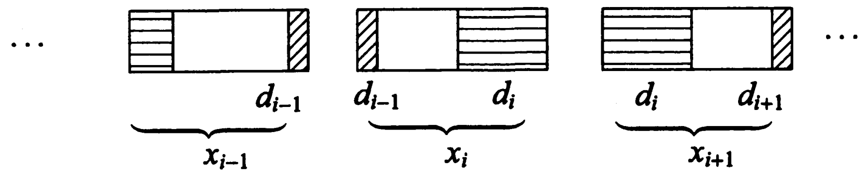
If $l(x_{i+1}) > d_i + d_{i+1}$ holds[8] *for all i $(1 \leq i \leq n-2)$, then*

$$l(x_1 \cdots x_n) = l(x_1) + \cdots + l(x_n) - 2(d_1 + \cdots + d_{n-1}). \tag{76}$$

[6] They are given in Y. Ihara [**16**].

[7] Since $x = xy \cdot y^{-1}$, we have $l(x) \leq l(xy) + l(y)$; thus we get $l(xy) \geq |l(x) - l(y)|$.

[8] Where we put $d_n = 0$.



PROOF. Factorize each x_i into free product $x_i = a_i b_i c_i$ with $l(a_i) = d_{i-1}, l(b_i) = l(x_i) - d_i - d_{i-1} > 0, l(c_i) = d_i$ (here we understand $a_1 = c_n = 1$). Lemma 8 shows that $c_i a_{i+1} \in X_0$ $(1 \leq i \leq n-1)$, and that $l(b_i c_i a_{i+1} b_{i+1}) = l(b_i) + l(b_{i+1})$, and hence the products $(b_i c_i a_{i+1}) \cdot b_{i+1}$, and hence also the product $(b_i c_i a_{i+1}) \cdot (b_{i+1} c_{i+1} a_{i+2})$ are free. Now our lemma follows directly from Lemma 6. □

COROLLARY . *Let $x_1, \cdots, x_n \in X$ with $l(x_2), \cdots, l(x_{n-1}) > 0$. Then, if the products $x_1 \cdot x_2, \cdots, x_{n-1} \cdot x_n$ are all free, the product $x_1 \cdots x_n$ is also free.*

§19. The proof of Lemma 3. Recall the definitions;

$$\Gamma^l = \left\{ \gamma \in \Gamma \,\middle|\, \gamma_\mathfrak{p} \in Y_l = U_\mathfrak{p} \begin{pmatrix} p^l & 0 \\ 0 & p^{-l} \end{pmatrix} U_\mathfrak{p} \right\} \quad (l \geqq 0),$$

where $U_\mathfrak{p} = PSL_2(O_\mathfrak{p})$, and p is a prime element of $k_\mathfrak{p}$. When $\gamma \in \Gamma$ belongs to Γ^l, we put $l = l(\gamma)$. To avoid unnecessary suffices, we shall not make distinction between Γ and $\Gamma_\mathfrak{p}$; and consider Γ as a (dense) subgroup of $G_\mathfrak{p}$. Also, we consider $G_\mathfrak{p} = PSL_2(k_\mathfrak{p})$ as a subgroup of $X = PL_2(k_\mathfrak{p})$. We note here, that the definitions of the functions $l(x)$ are different on $G_\mathfrak{p}$ and on X; in fact, we have $Y_l = G_\mathfrak{p} \cap X_{2l}$. We shall use the symbol $l(x)$ exclusively in the sense that $l(x) = l$ for $x \in Y_l$. We shall further put $L(x) = l$ for $x \in X_l$. Thus, we have

$$l(x) = 2L(x) \quad \text{for } x \in G_\mathfrak{p}. \tag{77}$$

The product $\gamma_1\gamma_2\cdots\gamma_n$ of $\gamma_1, \cdots, \gamma_n \in \Gamma$ is called *free*, if $l(\gamma_1 \cdots \gamma_n) = l(\gamma_1) + \cdots + l(\gamma_n)$ holds. We shall show that any element $\gamma \in \Gamma$ with $l(\gamma) = l$ $(l = 1, 2, \cdots)$ is a free product of elements of Γ^1;

$$\gamma = \gamma_1\gamma_2\cdots\gamma_l; \quad \gamma_1, \cdots, \gamma_l \in \Gamma^1. \tag{78}$$

In fact, it is trivial for $l = 1$. Assume that it is true for $l(\gamma) \leqq l - 1$, and prove it for $l(\gamma) = l$. By Lemma 5, we can put $\gamma = x_1 x_2 \cdots x_{2l}$ with $x_1, \cdots, x_{2l} \in X_1$. Since $PL_2(O_\mathfrak{p})\Gamma_\mathfrak{p} = PL_2(O_\mathfrak{p}) \cdot G_\mathfrak{p} = X'$, there is an element $\gamma_l \in \Gamma$ contained in $PL_2(O_\mathfrak{p})x_{2l-1}x_{2l}$. Then we have $l(\gamma_l) = 1$, $l(\gamma\gamma_l{}^{-1}) = l - 1$, and hence by the induction assumption, we have $\gamma\gamma_l{}^{-1} = \gamma_1 \cdots \gamma_{l-1}$ with $\gamma_1, \cdots, \gamma_{l-1} \in \Gamma^1$; hence we get $\gamma = \gamma_1\gamma_2\cdots\gamma_l$.

Now let $\{\gamma\}_\Gamma$ be a primitive elliptic Γ-conjugacy class of degree d. By Proposition 6, we can assume, without loss of generality, that $l(\gamma) = d$. Put $\gamma = \gamma_1 \cdots \gamma_d$ with $\gamma_1, \cdots, \gamma_d \in \Gamma^1$. Then the products $\gamma_1 \cdot \gamma_2, \cdots, \gamma_{d-1} \cdot \gamma_d$ are free; but moreover, the product $\gamma_d \cdot \gamma_1$ must also be free. In fact, if not, then $l(\gamma_1{}^{-1}\gamma\gamma_1) = l(\gamma_2 \cdots \gamma_d\gamma_1) < d$, which is a contradiction, since by Lemma 6, we have $d = \mathrm{Min}_{x \in \{\gamma\}_\Gamma} l(x)$. Therefore, the products $\gamma \cdot \gamma$, $\gamma \cdot \gamma \cdot \gamma, \cdots$ etc. are also free, and we have $l(\gamma^r) = |r| l(\gamma) = |r| d$ for any $r \in \mathbf{Z}$. Another remark is that, if $\gamma_1^{-1} = u_1\pi_a\pi_b$, $\gamma_d = u_2\pi_e\pi_f$ are the factorizations (62) of γ_1^{-1}, γ_d, then, since $\gamma_d \cdot \gamma_1$ is a free product, we have $\pi_b \neq \pi_f$. On the other hand, if $x = u\pi_{i_1} \cdots \pi_{i_l}$ is the factorization for $x \in \Gamma$, then the product $x \cdot \gamma_1$ is free if and only if $\pi_{i_l} \neq \pi_b$; $\gamma_d \cdot x^{-1}$ is free if and only if $\pi_{i_l} \neq \pi_f$. In particular, it shows that at least one of the two products $x \cdot \gamma_1$, $\gamma_d \cdot x^{-1}$ must be free. Since $\gamma_i \cdot \gamma_{i+1}$ is a free product for any i, where the index is considered mod d, we see that the above remark is also valid, if we replace γ_d, γ_1 by γ_i, γ_{i+1} respectively.

Now the proof of Lemma 3 requires a separate treatment for the cases k: even or k: odd.

The case k is even. Let S be a set of representatives of $\Gamma^0\backslash\Gamma^{k/2}$. If $k = 0$, then we simply put $S = \{I\}$. If $k > 0$, then we have $|S| = q^{k-1}(q+1)$. In this case, for each i (mod d), let S_i be a subset of S formed of all $x \in S$ such that $x \cdot \gamma_i$ and $\gamma_{i-1} \cdot x^{-1}$ are free products. Then, by the previous remark, S_i consists of $q^{k-1}(q-1)$ elements (see Lemma 5). If $k = 0$, we simply put $S_i = S = \{I\}$ $(1 \leq i \leq d)$. We shall prove that the following set of $dq^{k-1}(q-1)$ $(k > 0)$ or d $(k = 0)$ elements of Γ forms a set of representatives of all Γ^0-conjugacy classes contained in $\{\gamma^r\}_\Gamma \cap \Gamma^{dr+k}$;

$$(79)\qquad \begin{cases} y_1(\gamma_1\gamma_2\cdots\gamma_d)^r y_1^{-1}; & y_1 \in S_1 \\ y_2(\gamma_2\gamma_3\cdots\gamma_1)^r y_2^{-1}; & y_2 \in S_2 \\ \quad\vdots & \quad\vdots \\ y_d(\gamma_d\gamma_1\cdots\gamma_{d-1})^r y_d^{-1}; & y_d \in S_d. \end{cases}$$

Since the products $y_i \cdot \gamma_i$, $\gamma_{i-1} \cdot y_i^{-1}$ are free, the product $y_i(\gamma_i\cdots\gamma_{i-1})^r y_i^{-1} = y_i \cdot \gamma_i \cdot \cdots \cdot \gamma_{i-1} \cdot y_i^{-1}$ is free (corollary of Lemma 9); hence they are contained in Γ^{dr+k}. On the other hand, since

$$(\gamma_i\gamma_{i+1}\cdots\gamma_{i-1})^r = (\gamma_1\cdots\gamma_{i-1})^{-1}\gamma^r(\gamma_1\cdots\gamma_{i-1}),$$

they are contained in $\{\gamma^r\}_\Gamma$.

First, let us prove that the distinct members of (79) are not Γ^0-conjugate with each other. Suppose that

$$y_i(\gamma_i\cdots\gamma_{i-1})^r y_i^{-1} = uy_j'(\gamma_j\cdots\gamma_{j-1})^r y_j'^{-1}u^{-1}$$

holds with $u \in \Gamma^0$, $1 \leq j \leq i \leq d$, and $y_i \in S_i$, $y_j' \in S_j$. Then, this implies that $y_i^{-1}uy_j'(\gamma_j\gamma_{j+1}\cdots\gamma_{i-1})$ commutes with $(\gamma_i\cdots\gamma_{i-1})^r$. Since $\gamma_i\cdots\gamma_{i-1}$ is primitive (it is Γ-conjugate to γ), its centralizer in Γ is the free cyclic group generated by itself. Hence, we get

$$y_i^{-1}uy_j'(\gamma_j\gamma_{j+1}\cdots\gamma_{i-1}) = (\gamma_i\cdots\gamma_{i-1})^s$$

with some $s \in \mathbf{Z}$; hence we get

$$(80)\qquad uy_j'(\gamma_j\gamma_{j+1}\cdots\gamma_{i-1}) = y_i(\gamma_i\gamma_{i+1}\cdots\gamma_{i-1})^s \quad (s \in \mathbf{Z}).$$

But the products $y_j' \cdot \gamma_j$, $y_i \cdot \gamma_i$, $y_i \cdot \gamma_{i-1}^{-1}$ (appears, if $s < 0$) are all free; hence by taking $l(\,)$ of both sides, we get $\frac{k}{2} + i - j = \frac{k}{2} + |s| \cdot d$; hence $i - j = |s|d$; hence $i = j$, $s = 0$. So, by (80), we get $uy_i' = y_i$; hence, by the definition of S, we get $y_j' = y_i' = y_i$, $u = 1$.

Now, we shall show that any element of $\{\gamma^r\}_\Gamma \cap \Gamma^{dr+k}$ is Γ^0-conjugate to a member of (79). Take any $z \in \{\gamma^r\}_\Gamma \cap \Gamma^{dr+k}$, and put

$$z = x(\gamma_i\gamma_{i+1}\cdots\gamma_{i-1})^r x^{-1}, \quad x \in \Gamma, \quad (1 \leq i \leq d). \tag{81}$$

We can assume, without loss of generality, that, among all expressions of the form (81) (where i can vary), we have chosen our particular (81) so that $l(x)$ is taken as small as possible. Now, by the previous remark, at least one of the two products $x \cdot \gamma_i$, $\gamma_{i-1} \cdot x^{-1}$ must be free. We shall show that the both must be free. In fact, if not, and say $x \cdot \gamma_i$ is free but $\gamma_{i-1} \cdot x^{-1}$ is not, then we have either $L(\gamma_{i-1} \cdot x^{-1}) = L(x)$ or $= L(x) - 2$ (by (56) and Lemma 8). But if $L(\gamma_{i-1} \cdot x^{-1}) = L(x)$, then, by Lemma 9 applied to the product

$$\{x(\gamma_i\cdots\gamma_{i-1})^{r-1}\gamma_i\cdots\gamma_{i-2}\} \cdot \gamma_{i-1} \cdot x^{-1},$$

we get $L(z) = 2dr + 2L(x) - 2$; hence $k = L(x) - 1 = 2l(x) - 1$, which is a contradiction, since k is even. On the other hand, if $L(\gamma_{i-1} \cdot x^{-1}) = L(x) - 2$, then if we put $y = x \cdot \gamma_{i-1}^{-1}$, then $l(y) = l(x \cdot \gamma_{i-1}^{-1}) = l(x) - 1 < l(x)$, and

$$z = z(\gamma_i\cdots\gamma_{i-1})^r x^{-1} = y(\gamma_{i-1}\gamma_i\cdots\gamma_{i-2})y^{-1}$$

with $l(y) < l(x)$; which is a contradiction to our assumption on the expression (81) of z. Exactly in the same manner, we can show that an assumption that $x \cdot \gamma_i$ is not free leads to a contradiction.

Therefore, the both of the products $x \cdot \gamma_i$, $\gamma_{i-1} \cdot x^{-1}$ must be free. So, by the corollary of Lemma 9, the product $z = x \cdot \gamma_i \cdot \cdots \cdot \gamma_{i-1} \cdot x^{-1}$ is free, hence $dr + k = l(z) = 2l(x) + rl(\gamma) = 2l(x) + rd$; hence $2l(x) = k$; hence $x \in \Gamma^{k/2}$. Since the products $x \cdot \gamma_i$, $\gamma_{i-1} \cdot x^{-1}$ are both free, we have $x = uy_i$ with $u \in \Gamma^0$, $y_i \in S_i$; hence $z = uy_i(\gamma_i\cdots\gamma_{i-1})^r y_i^{-1}u^{-1}$, and hence z is Γ^0-conjugate to $y_i(\gamma_i\cdots\gamma_{i-1})^r y_i^{-1}$, $y_i \in S_i$.

The case k is odd. Let S' be a set of representatives of $\Gamma^0\backslash\Gamma^{(k+1)/2}$, and let S_i' $(1 \leq i \leq d)$ be a subset of S' formed of all $x \in S'$ such that $l(x \cdot \gamma_i) = l(x)$. If $\gamma_i^{-1} = u_i\pi_a\pi_b$ is the factorization (62) of γ_i^{-1}, and $x = u\pi_{i_1}\cdots\pi_{i_{k+1}}$ is that of x, then, the condition $l(x \cdot \gamma_i) = l(x)$ is equivalent to $\pi_{i_{k+1}} = \pi_b$, $\pi_{i_k} \neq \pi_a$. So, by consulting Lemma 5, we see directly that the cardinality of S' is $(q-1)q^{k-1}$. Now, we shall show that the following set of $dq^{k-1}(q-1)$ elements of Γ forms a set of representatives of all Γ^0-conjugacy classes contained in $\{\gamma^r\}_\Gamma \cap \Gamma^{dr+k}$;

$$\begin{cases} y_1(\gamma_1\cdots\gamma_d)^r y_1^{-1} & y_1 \in S_1' \\ \quad\vdots & \vdots \\ y_d(\gamma_d\cdots\gamma_{d-1})^r y_d^{-1} & y_d \in S_d'. \end{cases} \tag{82}$$

Since $l(y_i\gamma_i) = l(y_i)$, and since $\gamma_{i-1} \cdot y_i^{-1}$ is free (recall that at least one of $y_i \cdot \gamma_i$, $\gamma_{i-1} \cdot y_i^{-1}$ must be free), Lemma 9 shows that

$$l(y_i(\gamma_i\cdots\gamma_{i-1})^r y_i^{-1}) = 2l(y_i) + dr - 1 = dr + k;$$

hence $y_i(\gamma_i\cdots\gamma_{i-1})^r y_i^{-1} \in \Gamma^{dr+k} \cap \{\gamma^r\}_\Gamma$.

Let us show that the distinct members of (82) are not Γ^0-conjugate with each other. If

$$y_i(\gamma_i\cdots\gamma_{i-1})^r y_i^{-1} = uy_j'(\gamma_j\cdots\gamma_{j-1})^r y_j'^{-1}u^{-1}$$

with $u \in \Gamma^0$, $1 \le j \le i \le d$, $y_i \in S'_i$, $y'_j \in S'_j$, then, by the same argument as in k: even case, we get

$$uy'_j(\gamma_j\gamma_{j+1}\cdots\gamma_{i-1}) = y_i(\gamma_i\gamma_{i+1}\cdots\gamma_{i-1})^s \quad (s \in \mathbf{Z}). \tag{83}$$

We shall show that $j = i$. Suppose on the contrary that we had $j < i$. Then, we have $l(uy'_j(\gamma_j\gamma_{j+1}\cdots\gamma_{i-1})) = l(y'_j) + (i-j) - 1$ (by Lemma 9). So, we get, by (83),

$$\frac{k+1}{2} + i - j - 1 = \begin{cases} \frac{k+1}{2} + sd - 1 & \text{if } s > 0 \\ \frac{k+1}{2} + |s|\cdot d & \text{if } s < 0\ (\because\ y_i\cdot\gamma_{i-1}^{-1} \text{ is free}) \\ \frac{k+1}{2} & \text{if } s = 0. \end{cases} \tag{84}$$

If $s \ne 0$, (84) implies $i-j \ge d$, which is a contradiction. If $s = 0$, then we get $i = j+1$, and hence by (83), we get $uy'_j\gamma_j = y_i$; hence $uy'_j\gamma_j\gamma_{j+1} = y_i\gamma_i$. But we have $l(y_i\gamma_i) = l(y_i) = \frac{k+1}{2}$, while

$$l(uy'_j\gamma_j\gamma_{j+1}) = l(y'_j) + l(\gamma_j) + l(\gamma_{j+1}) - 1 = \frac{k+1}{2} + 1,$$

since $l(y'_j\gamma_j) = l(y'_j)$ and since the product $\gamma_j \cdot \gamma_{j+1}$ is free (use Lemma 9). So, we get a contradiction $l(uy'_j\gamma_j\gamma_{j+1}) \ne l(y_i\gamma_i)$. Therefore we get $j = i$. So, by (83), we get

$$uy'_j = y_i(\gamma_i\cdots\gamma_{i-1})^s; \quad j = i, \tag{85}$$

hence

$$\frac{k+1}{2} = \begin{cases} \frac{k+1}{2} + sd - 1 & (\text{if } s > 0), \\ \frac{k+1}{2} + |s|d & (\text{if } s < 0). \end{cases}$$

But these are obviously contradictions; hence we get $s = 0$. Therefore $uy'_j = y_i \in S'_i = S'_j$. Therefore $u = 1$, $y_i = y'_j$.

Finally, to show that any element $z \in \{\gamma^r\}_\Gamma \cap \Gamma^{dr+k}$ is Γ^0-conjugate to a member of (82), put

$$z = x(\gamma_i\gamma_{i+1}\cdots\gamma_{i-1})^r x^{-1}, \quad x \in \Gamma, \quad (1 \le i \le d). \tag{86}$$

As in the k: even case, we assume that among all expressions of the form (86) (where i can vary), we have chosen our particular expression (86) so that $l(x)$ is taken as small as possible. Now, at least one of the two products $x\cdot\gamma_i$, $\gamma_{i-1}\cdot x^{-1}$ must be free. We see that, in this case, both cannot be free. In fact, if it were so, we would have $dr+k = l(z) = 2l(x)+dr$, hence $2l(x) = k$; which is a contradiction, since k is odd. So, one of the two products $x\cdot\gamma_i$, $\gamma_{i-1}\cdot x^{-1}$ is free and the other is not. If $\gamma_{i-1}\cdot x^{-1}$ is free and $x\cdot\gamma_i$ is not, then either $l(x\cdot\gamma_i) = l(x)$ or $= l(x) - 1$. But if $l(x\cdot\gamma_i) = l(x) - 1$, then, if we put $y = x\cdot\gamma_i$, then $l(y) = l(x) - 1$ and we have $z = y(\gamma_{i+1}\cdots\gamma_i)^r y^{-1}$; which is a contradiction to our assumption. Therefore, $l(x\cdot\gamma_i) = l(x)$; hence, by Lemma 9, $l(z) = 2l(x) + dr - 1$; hence $l(x) = \frac{k+1}{2}$. Since $l(x\cdot\gamma_i) = l(x)$, we have $x = uy_i$ with $u \in \Gamma^0$, $y_i \in S'_i$; hence $z = uy_i(\gamma_i\cdots\gamma_{i-1})^r y_i^{-1}u^{-1}$. If, on the other hand, $x\cdot\gamma_i$ is free but $\gamma_{i-1}\cdot x^{-1}$ is not, again we get $l(\gamma_{i-1}\cdot x^{-1}) = l(x^{-1}) = l(x)$. Put $y'_{i-1} = x\cdot\gamma_{i-1}^{-1}$. Then, $z = y'_{i-1}(\gamma_{i-1}\gamma_i\cdots\gamma_{i-2})^r {y'_{i-1}}^{-1}$, and we have $l(y'_{i-1}) = l(x) = \frac{k+1}{2}$, $l(y'_{i-1}\gamma_{i-1}) = l(x) = l(y'_{i-1})$; hence we have $y'_{i-1} = uy_{i-1}$ with $u \in \Gamma^0$, $y_{i-1} \in S'_{i-1}$; and we have $z = uy_{i-1}(\gamma_{i-1}\gamma_i\cdots\gamma_{i-2})^r y_{i-1}^{-1}u^{-1}$; which proves our Lemma 3 completely. □

Regular cycles on $\Gamma_{\mathbf{R}}^0\backslash\mathfrak{H}$.

§20. The situations being as in Theorem 1, let $P \in \wp(\Gamma)$, $\deg P = d$; and let $\{\gamma^{\pm 1}\}_\Gamma$ be the pair of mutually inverse primitive elliptic Γ-conjugacy class that corresponds to P. By Lemma 3, $\{\gamma\}_\Gamma \cap \Gamma^d$ consists of d distinct Γ^0-conjugacy classes. Put

$$\{\gamma\}_\Gamma \cap \Gamma^d = \{\gamma_1\}_{\Gamma^0} \cup \cdots \cup \{\gamma_d\}_{\Gamma^0}; \tag{87}$$

and let $z_1, \cdots, z_d \in \mathfrak{H}$ be the fixed points of $(\gamma_1)_{\mathbf{R}}, \cdots, (\gamma_d)_{\mathbf{R}}$ respectively. Then, as a set of points on $\Gamma_{\mathbf{R}}^0\backslash\mathfrak{H}$, $z_1, \cdots, z_d$ are well-defined, and are distinct. So, to each $P \in \wp(\Gamma)$ with $\deg P = d$, we can correspond a set $\tilde{z}_1, \cdots, \tilde{z}_d$ of d distinct points on $\Gamma_{\mathbf{R}}^0\backslash\mathfrak{H}$. We call this $\{\tilde{z}_1, \cdots, \tilde{z}_d\}$ *the regular cycle* on $\Gamma_{\mathbf{R}}^0\backslash\mathfrak{H}$ which corresponds to $P \in \wp(\Gamma)$.

Estimation of the roots of $\zeta_\Gamma(u)$.

§21. Now we are going to give some estimation of the absolute values of the roots π_i, π_i' $(1 \le i \le g)$ of $\zeta_\Gamma(u)$. It is a direct consequence of the following lemma by M. Kuga.

LEMMA 10 (Kuga[9]). *Let Δ be a discrete subgroup of $G_{\mathbf{R}} = PSL_2(\mathbf{R})$ with compact quotient, and let $\gamma \in G_{\mathbf{R}}$ be such that $\Delta, \gamma^{-1}\Delta\gamma$ are commensurable with each other, that $\Delta\gamma^{-1}\Delta = \Delta\gamma\Delta$, and that Δ and γ generate a dense subgroup of $G_{\mathbf{R}}$. Put*

$$\Delta\gamma\Delta = \sum_{i=1}^{d} \Delta\gamma_i \quad (d = (\Delta : \Delta \cap \gamma^{-1}\Delta\gamma)),$$

and let $f(z) \not\equiv 0$ be a holomorphic automorphic form of weight k $(k = 2, 4, 6, \cdots)$ with respect to Δ, which is an eigenfunction of the following Hecke operator with an eigenvalue λ;

$$\sum_{i=1}^{d} f(\gamma_i z) j(\gamma_i, z) = \lambda \cdot f(z), \tag{88}$$

where, in general, we put $j(g, z) = (c_{\mathbf{R}} z + d_{\mathbf{R}})^{-k}$ for $g = \pm\begin{pmatrix} a_{\mathbf{R}} & b_{\mathbf{R}} \\ c_{\mathbf{R}} & d_{\mathbf{R}} \end{pmatrix} \in G_{\mathbf{R}}$. Then, we have

$$|\lambda| < d. \tag{89}$$

PROOF. Let F be the continuous function on $G_{\mathbf{R}}$ defined by

$$F(g) = f(g\sqrt{-1}) \cdot j(g, \sqrt{-1}) \qquad (g \in G_{\mathbf{R}}). \tag{90}$$

Since $f(z)$ is an automorphic form of weight k with respect to Δ, we have

$$\begin{aligned} F(\delta \cdot g) &= f(\delta g\sqrt{-1}) j(\delta g, \sqrt{-1}) = f(g\sqrt{-1}) j(\delta, g\sqrt{-1})^{-1} j(\delta g, \sqrt{-1}) \\ &= f(g\sqrt{-1}) j(g, \sqrt{-1}) = F(g) \end{aligned}$$

[9]Cf. M.Kuga [21]. The formulation and the method for proof are not exactly the same.

for any $\delta \in \Delta$. So, F is Δ-invariant from the left. Therefore, $|F|$, being a continuous function on the compact quotient $\Delta\backslash G_{\mathbf{R}}$, achieves the maximum value M

$$M = \mathrm{Max}_{g\in G_{\mathbf{R}}} |F(g)|. \tag{91}$$

Let D be the set of all elements $g \in G_{\mathbf{R}}$ such that $|F(g)| = M$. Then, obviously, D is Δ-invariant from the left; $D = \Delta \cdot D$. Now, (88) implies

$$\sum_{i=1}^{d} F(\gamma_i g) = \lambda \cdot F(g) \qquad (g \in G_{\mathbf{R}}). \tag{92}$$

So, if $g \in D$, we get $|\lambda| \cdot M \leq \sum_{i=1}^{d} |F(\gamma_i g)| \leq Md$; hence we get $|\lambda| \leq d$. Now, let us show that $|\lambda| \neq d$. Suppose, on the contrary, that we had $|\lambda| = d$. Then, in the above inequality, we must have $|F(\gamma_i g)| = M$ for all i $(1 \leq i \leq d)$. So, we have $|F(\xi g)| = M$ for any $g \in D$ and $\xi \in \bigcup_{i=1}^{d} \Delta\gamma_i = \Delta\gamma\Delta$. By $\Delta\gamma^{-1}\Delta = \Delta\gamma\Delta$, we also have $|F(\xi^{-1}g)| = M$. So, if we denote by Δ', the subgroup of $G_{\mathbf{R}}$ formed of all elements $g \in G_{\mathbf{R}}$ such that $gD = D$, then Δ' contains Δ and γ. So, by our assumption, Δ' is dense in $G_{\mathbf{R}}$; which implies that D is dense in $G_{\mathbf{R}}$. But since F is continuous, D is closed. Therefore $D = G_{\mathbf{R}}$; and hence we get

$$|F(g)| \equiv M \quad \text{for } g \in G_{\mathbf{R}}. \tag{93}$$

Now let us show that (93) is impossible. If $g = \begin{pmatrix} \sqrt{a} & \sqrt{a}^{-1}b \\ 0 & \sqrt{a}^{-1} \end{pmatrix}$, with $a, b \in \mathbf{R}, a > 0$, then $F(g) = f(a\sqrt{-1} + b)a^{k/2}$. Therefore, by (93), we get

$$|f(z)| = M(\mathrm{Im}\ z)^{-k/2} \quad \text{on } \mathfrak{H}. \tag{94}$$

Thus , Re $(\log f(z))$ depends only on the imaginary part of z, and hence the derivative of $\sqrt{-1}\log f(z)$ is always real; hence $\frac{d}{dz}\log f(z)$ must be a constant, and we get $f(z) = Ae^{Bz}$ with some constants A, B. But then (94) would be impossible. So, $|\lambda| = d$ is a contradiction; and we get $|\lambda| < d$. □

§22. To make it possible to apply Lemma 10 to our group, we need verify the following simple lemma.

LEMMA 11. *The subgroup $U_{\mathfrak{p}} = PSL_2(O_{\mathfrak{p}})$ is maximal in $G_{\mathfrak{p}} = PSL_2(k_{\mathfrak{p}})$.*

PROOF. Let H be a subgroup of $G_{\mathfrak{p}}$ with $H \supsetneq U_{\mathfrak{p}}$. Let $x \in H, \notin U_{\mathfrak{p}}$. Then

$$H \supset U_{\mathfrak{p}}xU_{\mathfrak{p}} = U_{\mathfrak{p}}\begin{pmatrix} p^l & 0 \\ 0 & p^{-l} \end{pmatrix}U_{\mathfrak{p}} = Y_l \quad (l > 0),$$

p being a prime element of $k_{\mathfrak{p}}$. Since $\begin{pmatrix} p^l & 0 \\ 0 & p^{-l} \end{pmatrix}, \begin{pmatrix} p^l & p^{l-1} \\ 0 & p^{-l} \end{pmatrix} \in Y_l \subset H$, we get

$$\begin{pmatrix} 1 & p^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} p^{-l} & 0 \\ 0 & p^l \end{pmatrix}\begin{pmatrix} p^l & p^{l-1} \\ 0 & p^{-l} \end{pmatrix} \in H.$$

Hence, $H \supset U_{\mathfrak{p}} \begin{pmatrix} 1 & p^{-1} \\ 0 & 1 \end{pmatrix} U_{\mathfrak{p}} \ni \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}$. Hence, H contains $\begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}^l$ for all $l \geq 0$; hence all $U_{\mathfrak{p}} \begin{pmatrix} p^l & 0 \\ 0 & p^{-l} \end{pmatrix} U_{\mathfrak{p}}$; hence $G_{\mathfrak{p}}$. Hence we get $H = G_{\mathfrak{p}}$. □

COROLLARY. *The subgroup Γ^0 is maximal in Γ. If $\gamma \in \Gamma$, $\notin \Gamma^0$, then $\Gamma^0_{\mathbf{R}}$ and $\gamma_{\mathbf{R}}$ generate a dense subgroup of $G_{\mathbf{R}}$.*

PROOF. In fact, $\Gamma^0_{\mathbf{R}}$ and $\gamma_{\mathbf{R}}$ generate $\Gamma_{\mathbf{R}}$. □

§23. Now we shall prove:

THEOREM 2. *The notations being as in Theorem 1, we have*

$$|\pi_i|,\ |\pi_i'| \leq q^2, \tag{95}$$

and

$$\pi_i,\ \pi_i' \neq 1,\ q^2. \tag{96}$$

PROOF. Recall that we have $\rho = \chi_1 \oplus \cdots \oplus \chi_g$ and

$$\chi_i(\Gamma^m) - (q-1)\sum_{k=1}^{m} \chi_i(\Gamma^{m-k}) = \pi_i^m + \pi_i'^m \quad (1 \leq i \leq g,\ m \geq 1), \tag{49}$$

where ρ is as defined in §9 for $\Delta = \Gamma^0_{\mathbf{R}}$, $\tilde{\Delta} = \Gamma_{\mathbf{R}}$ (see also §14). By the corollary of Lemma 11, we can apply Lemma 10 for $\Delta = \Gamma^0_{\mathbf{R}}$ and for any $\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}}$, $\notin \Gamma^0_{\mathbf{R}}$, and we get

$$|\chi_i(\Gamma^m)| < q^{2m} + q^{2m-1} \quad (1 \leq i \leq g,\ m \geq 1). \tag{97}$$

First, let us prove (95). Suppose that we had $|\pi_i| = q^a, a > 2$. Then, by $\pi_i\pi_i' = q^2$, we get $|\pi_i'| < 1$. By (49), we get

$$\begin{aligned} |\pi_i^m + \pi_i'^m| &\leq q^{2m} + q^{2m-1} + (q-1)\{q^{2m-2} + q^{2m-3} + \cdots + 1\} \\ &= q^{2m} + 2q^{2m-1} - 1 = O(q^{2m}). \end{aligned}$$

But this is impossible for $|\pi_i| = q^a$ $(a > 2)$ and $|\pi_i'| < 1$. Hence, we get $|\pi_i| \leq q^2$. In the same manner, we get $|\pi_i'| \leq q^2$.

To prove (96), suppose, on the contrary, that we had $\pi_i, \pi_i' = 1, q^2$. Then, by (49), we get

$$\sigma_m - q\sigma_{m-1} = q^{2m} + 1; \quad \sigma_m = \sum_{l=0}^{m} \chi_i(\Gamma^l) \quad (m \geq 1). \tag{98}$$

But this implies $\sigma_m = q^{2m} + q^{2m-1} + \cdots + 1$ $(m \geq 1)$; hence $\sigma_m - \sigma_{m-1} = q^{2m} + q^{2m-1}$ $(m \geq 1)$. But this implies $\chi_i(\Gamma) = q^{2m} + q^{2m-1}$, which is a contradiction to (97). So, we cannot have π_i, $\pi_i' = 1, q^2$. □

So far, Theorem 2, (95) (96) are the only estimation for the absolute values of π_i, π_i' which we could prove. Some application of Theorem 2 will be given later.

Concluding remarks on Chapter 1, Part 1.

§24.

Remark 1. All our results in this Chapter (Part 1) are valid also in the case where $k_\mathfrak{p}$ is the field of power series over a finite field $\mathbf{F}_q$. However, we do not know whether Γ exists at all in such a case.

Remark 2. In the computation of $\zeta_\Gamma(u)$, we assumed that Γ is torsion-free and G/Γ is compact. Among them, the former can be dropped easily, and we get a similar result. We plan to give its description in Part 2 of Chapter 1. Also, we are planning to give there a computation of "L-functions" attached to Γ, which has an interesting application to an analogue of "Tschebotarev's density Theorem" for the law of decomposition of elements of $\wp(\Gamma)$ in $\wp(\Gamma')$, where Γ' is a subgroup of finite index in Γ.