Part 2.[10] Detailed study of elements of Γ with parabolic and elliptic real parts; the general formula for $\zeta_\Gamma(u)$.

Let Γ be a discrete subgroup of $G = G_{\mathbf{R}} \times G_{\mathfrak{p}} = PSL_2(\mathbf{R}) \times PSL_2(k_{\mathfrak{p}})$ with finite volume quotient G/Γ and with dense image of projection in each component of G. In the previous part of this chapter, we defined the ζ-function

$$\zeta_\Gamma(u) = \prod_{P \in \mathfrak{p}(\Gamma)} (1 - u^{\deg P})^{-1}$$

for such a group Γ (§6) and carried out its computation under the two assumptions: (a) G/Γ is compact, (b) Γ is torsion-free. (See Theorems 1, 2).

In the following Part 2, *we shall drop the above two assumptions* (a), (b), and after studying in detail the elements of Γ with parabolic real parts (§25 ~ §28, Theorem 3) and those with elliptic real parts (including in particular the torsion elements of Γ; §29~ §34, Theorems 4 ~ 6), we shall proceed to *prove a general formula for* $\zeta_\Gamma(u)$ by generalizing the previous computations (§35 ~ §38, Theorem 7). The main results are as follows:

1. Let $\gamma \in \Gamma$ be such that $\gamma_{\mathbf{R}}$ is parabolic.[11] Let H^0 be the centralizer of γ and let H be the normalizer of H^0 (both considered in Γ). Then (i) $k_{\mathfrak{p}} = \mathbf{Q}_p$ holds, (ii) H is conjugate in $G_{\mathbf{R}} \times PL_2(\mathbf{Z}_p)$ to the group

$$B^{(d)} = \left\{ \begin{pmatrix} p^{dk} & b \\ 0 & p^{-dk} \end{pmatrix} \middle| \, k \in \mathbf{Z}, b \in \mathbf{Z}^{(p)} \right\} \tag{102}$$

(where d is a positive integer well-defined by H), and by this, H^0 corresponds to the subgroup $\begin{pmatrix} 1 & \mathbf{Z}^{(p)} \\ 0 & 1 \end{pmatrix}$ of $B^{(d)}$ (Theorem 3, §25). By this theorem we can derive everything we need about such elements γ.

2. Let $\gamma \in \Gamma$ be such that $\gamma_{\mathbf{R}}$ is elliptic.[12] Put $\Gamma^0 = \Gamma \cap (G_{\mathbf{R}} \times V)$ with $V = PSL_2(O_{\mathfrak{p}})$, and for each $l \geq 0$ put $T^l = \Gamma \cap \left\{ G_{\mathbf{R}} \times V \begin{pmatrix} \pi^l & 0 \\ 0 & \pi^{-l} \end{pmatrix} V \right\}$, π being a prime element of $k_{\mathfrak{p}}$. Then our results here are the following:

(i) we parametrize the set of all Γ^0-conjugacy classes contained in $\{\gamma\}_\Gamma$ in a nice way as, say,

$$\{\gamma\}_\Gamma = \bigcup_{k,\,\mu} \{\gamma_{k\mu}\}_{\Gamma^0}; \quad k = 0, 1, 2, \cdots; \quad \mu = 1, \cdots, n_k;$$

[10] The author regrets that, despite his promise, he has failed to give a computation of L-functions $L_\Gamma(u, \chi)$ here. The reason is that when χ is not a real character, his definition of $L_\Gamma(u, \chi)$ was not adequate, and it still remains for him to find its best definition.

[11] An element $x \in G_{\mathbf{R}}$ is called parabolic if its eigenvalues are $\pm\{1, 1\}$ and $x \neq 1$.

[12] An element $x \in G_{\mathbf{R}}$ is called elliptic if its eigenvalues are imaginary.

(ii) for each $\{\gamma_{k\mu}\}_{\Gamma^0}$, we express its length $l(\gamma_{k\mu})$ (i.e., the number l for which $\gamma_{k\mu} \in T^l$) by means of its major parameter k and by some invariants of $\{\gamma\}_\Gamma$ (such as the order of the centralizer of γ in Γ, or $\deg\{\gamma\}_\Gamma$ when it is defined, etc.).

As a corollary, we shall compute the following quantity $A_l\{\gamma\}_\Gamma$ for each $l \geq 1$, which are used later in the computation of $\zeta_\Gamma(u)$:

$$A_l\{\gamma\}_\Gamma = \sum_{k,\mu} e\{\gamma_{k\mu}\}_{\Gamma^0}^{-1}, \tag{118}$$

where the summation is over all k, μ with $l(\gamma_{k\mu}) = l$, and $e\{\gamma_{k\mu}\}_{\Gamma^0}$ denotes the order of the group $\Gamma^0 \cap \Gamma_{\gamma_{k\mu}}$, $\Gamma_{\gamma_{k\mu}}$ being the centralizer of $\gamma_{k\mu}$ in Γ. These are given in Theorems 4, 5, 6 (and their corollaries), separated according to the difference in the types of $\{\gamma\}_\Gamma$. Namely, in Theorem 4 (§30), we deal with the case where the centralizer Γ_γ of γ is infinite, and in Theorem 5 (§31) (resp. Theorem 6 (§32)), we deal with the cases where Γ_γ is finite and the quadratic extension $k_\mathfrak{p}(\gamma_\mathfrak{p})$ of $k_\mathfrak{p}$ is ramified (resp. unramified). We note here that the corollary of Theorem 4 generalizes Lemma 3 (§13, Part 1) with a much simpler proof; hence eliminates previous complicated and tedious sections (§18, §19) needed for the proof of Lemma 3. On the other hand, the proofs of Theorems 5, 6 are again complicated, chiefly because of the p-power torsions of Γ_γ, where $\mathfrak{p}|p$.

3. The formula for $\zeta_\Gamma(u)$ in the general cases is given in Theorem 7 (§35). It reads as:

$$\zeta_\Gamma(u) \times \prod_{P \in \wp_\infty(\Gamma)} (1 - u^{\deg P})^{-1} = \frac{P(u)(1+qu)^{g'-g}}{(1-u)(1-q^2u)} \times (1-u)^H, \tag{169}$$

where $\wp_\infty(\Gamma)$ is a certain finite set defined from parabolic elements of $\Gamma_\mathbf{R}$, g is the genus of $\Gamma_\mathbf{R}^0$,

$$P(u) = \prod_{i=1}^{g} (1 - \pi_i u)(1 - \pi_i' u) \in \mathbf{Z}[u]$$

with some equalities and inequalities between π_i, π_i' and q, and H is a *positive* integer given explicitly. This number H is proportional to the volume of G/Γ if Γ has no second-type torsions (i.e., if for every $\gamma \in \Gamma$ its centralizer Γ_γ is infinite). For some examples of Γ, H is equal to the class number of some definite quaternion algebra (see §38). Finally g' is the genus of a certain fuchsian group "twisted" from $\Gamma_\mathbf{R}^0$. We have $g' = g$ if Γ has no second type torsions, and conjecturally, always so.

Study of elements of Γ with parabolic real parts.

§25. Let Γ be a discrete subgroup of $G = G_\mathbf{R} \times G_\mathfrak{p}$ such that $\Gamma_\mathbf{R}, \Gamma_\mathfrak{p}$ are dense in $G_\mathbf{R}, G_\mathfrak{p}$ respectively and that the quotient G/Γ has finite invariant volume. Let p be the characteristic of the residue class field of $k_\mathfrak{p}$. We shall study here those elements $\varepsilon \in \Gamma$ for which $\varepsilon_\mathbf{R} \in G_\mathbf{R} = PSL_2(\mathbf{R})$ is parabolic. For each such ε, denote by z the fixed point

($\in \mathbf{R} \cup \{i\infty\}$) of $\varepsilon_{\mathbf{R}}$ and define the two groups H^0, H by

$$H^0 = \{\gamma \in \Gamma \mid \gamma_{\mathbf{R}} z = z, \gamma_{\mathbf{R}} : \text{parabolic}\} \cup \{1\} \tag{99}$$
$$= \text{the centralizer of } \varepsilon \text{ in } \Gamma,$$

$$H = \{\gamma \in \Gamma \mid \gamma_{\mathbf{R}} z = z\} = \text{the normalizer of } H^0 \text{ in } \Gamma. \tag{100}$$

Now our main result here is the following theorem:

THEOREM 3. *Let $\varepsilon \in \Gamma$ be such that $\varepsilon_{\mathbf{R}}$ is parabolic. Then* (i) $k_{\mathfrak{p}} = \mathbf{Q}_p$, (ii) H^0, H *being as above, there is a positive integer d and an element $t \in G_{\mathbf{R}} \times PL_2(\mathbf{Z}_p)$ such that*

$$H = t^{-1} B^{(d)} t, \tag{101}$$

where

$$B^{(d)} = \left\{ \begin{pmatrix} p^{dk} & b \\ 0 & p^{-dk} \end{pmatrix} \middle| \, k \in \mathbf{Z},\ b \in \mathbf{Z}^{(p)} \right\} \tag{102}$$

(considered as a subgroup of G by the diagonal embedding). In particular, it follows that

$$H^0 = t^{-1} \begin{pmatrix} 1 & \mathbf{Z}^{(p)} \\ 0 & 1 \end{pmatrix} t. \tag{103}$$

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

COROLLARY 1. *G/Γ is non-compact if and only if $\Gamma_{\mathbf{R}}$ contains a parabolic element, and in this case $k_{\mathfrak{p}} = \mathbf{Q}_p$.*

PROOF. In fact, let V be any open compact subgroup of $G_{\mathfrak{p}}$ and put $\Gamma^V = \Gamma \cap (G_{\mathbf{R}} \times V)$. Then $\Gamma^V_{\mathbf{R}}$ is a fuchsian group, and G/Γ is compact if and only if $G_{\mathbf{R}}/\Gamma^V_{\mathbf{R}}$ is so (Prop.2, §2). Hence, if G/Γ is non-compact, $\Gamma^V_{\mathbf{R}}$ contains a parabolic element. Conversely, if Γ contains ε for which $\varepsilon_{\mathbf{R}}$ is parabolic, we see immediately by Theorem 3 that $\varepsilon^{p^N} \in G_{\mathbf{R}} \times V$ for some $N > 0$; hence $\varepsilon^{p^N}_{\mathbf{R}} \in \Gamma^V_{\mathbf{R}}$. But then $G_{\mathbf{R}}/\Gamma^V_{\mathbf{R}}$ is non-compact; hence G/Γ is non-compact. That $k_{\mathfrak{p}} = \mathbf{Q}_p$ is contained in Theorem 3. □

COROLLARY 2.[13] *If $\varepsilon \in \Gamma$ is such that $\varepsilon_{\mathbf{R}}$ is parabolic, there is a positive integer m and an element $\delta \in \Gamma$ such that $\delta^{-1}\varepsilon\delta = \varepsilon^{p^m}$.*

PROOF. This follows immediately from Theorem 3. □

COROLLARY 3. *The notations being as in Theorem 3, let Γ' be any subgroup of Γ of finite index, and put $H^{0\prime} = H^0 \cap \Gamma'$. Then the group index $(H^0 : H^{0\prime})$ is not divisible by p.*

PROOF. By Theorem 3, $H^0 \cong \mathbf{Z}^{(p)}$; hence $(H^0 : H^{0\prime})$ cannot be divisible by p. □

[13] This fact will be used in the proof of the Theorem given in Supplement §6.

§26. The definition of $\wp_\infty(\Gamma)$. A point $z \in \mathbf{R} \cup \{i\infty\}$ is called a *cusp* of Γ if there is some $\varepsilon \in \Gamma$ such that $\varepsilon_{\mathbf{R}}$ is parabolic and $\varepsilon_{\mathbf{R}} z = z$. Two cusps z, z' will be called (Γ-)equivalent if there is some $\gamma \in \Gamma$ such that $\gamma_{\mathbf{R}} z = z'$. By

(104) $$\wp_\infty(\Gamma)$$

we shall denote the set of all Γ-equivalence classes of all cusps of Γ. For each $P \in \wp_\infty(\Gamma)$, we shall define its *degree*, $\deg P$, as follows. Let z be a cusp representing P, and let H be the group defined by (100), for this z. Then by Theorem 3, we have $H = t^{-1}B^{(d)}t$ for some t and some positive integer d. It is clear that this integer d is well-defined by P, which we shall call the degree of P. Thus $\deg P$ is always a positive integer.

On the other hand, put $G_p = PSL_2(\mathbf{Q}_p)$, $V = PSL_2(\mathbf{Z}_p)$, let x be any element of $G'_p = PL_2(\mathbf{Q}_p)$, and put $\Delta = \Gamma \cap (G_{\mathbf{R}} \times x^{-1}Vx)$. Then $\Delta_{\mathbf{R}}$ is a fuchsian group, and by Theorem 3, a point $z \in \mathbf{R} \cup \{i\infty\}$ is a cusp of Γ if and only if it is a cusp of $\Delta_{\mathbf{R}}$ (see the proof of Corollary 1). Since the number of $\Delta_{\mathbf{R}}$-equivalence classes of cusps of $\Delta_{\mathbf{R}}$ is finite, the set $\wp_\infty(\Gamma)$ is a priori finite, and each $P \in \wp_\infty(\Gamma)$ consists of finitely many $\Delta_{\mathbf{R}}$-equvalence classes. We shall prove:

PROPOSITION 7. *The set $\wp_\infty(\Gamma)$ is finite, and each $P \in \wp_\infty(\Gamma)$ consists of exactly $\deg P$ distinct $\Delta_{\mathbf{R}}$-equivalence classes.*

PROOF. The first assertion is already proved above. To prove the second assertion, let z be a cusp representing P, put $d = \deg P$, and let H be the group (100) defined for this z. Then $\Delta_{\mathbf{R}}$-equivalence classes contained in P are in one-to-one correspondence with the double coset $\Delta\backslash\Gamma/H$; hence it is enough to prove $|\Delta\backslash\Gamma/H| = d$; or equivalently $|x^{-1}Vx\backslash G_p/H_p| = d$. But by Theorem 3, $H_p = t_p^{-1}B^{(d)}t_p$ with $t_p \in PL_2(\mathbf{Z}_p)$; hence $|x^{-1}Vx\backslash G_p/H_p| = |V\backslash G_p/y^{-1}B^{(d)}y|$ with $y = t_p x^{-1}$. Thus our proposition is reduced to the following lemma: □

LEMMA 12. *Let d be a positive integer, and put*

$$B^{(d)} = \left\{ \begin{pmatrix} p^{dk} & b \\ 0 & p^{-dk} \end{pmatrix} \middle| \, k \in \mathbf{Z},\ b \in \mathbf{Z}^{(p)} \right\}.$$

Put $G_p = PSL_2(\mathbf{Q}_p)$, $V = PSL_2(\mathbf{Z}_p)$, and let y be any element of $G'_p = PL_2(\mathbf{Q}_p)$. Then

(105) $$|V\backslash G_p/y^{-1}B^{(d)}y| = d.$$

PROOF. Let $\bar{B}^{(d)}$ be the closure of $B^{(d)}$ in G_p, so that

$$\bar{B}^{(d)} = \left\{ \begin{pmatrix} p^{dk} & b \\ 0 & p^{-dk} \end{pmatrix} \middle| \, k \in \mathbf{Z},\ b \in \mathbf{Q}_p \right\}.$$

Put $\bar{B} = \bar{B}^{(1)}$. We shall first check $G_p = V \cdot y^{-1}\bar{B}y$. It is well-known that $G_p = V \cdot \bar{B}$ and $G'_p = V' \cdot \bar{B}'$, where $V' = PL_2(\mathbf{Z}_p)$ and $\bar{B}'$ is the upper triangular subgroup of G'_p. Put $y^{-1} = v'b'$ with $v' \in V'$, $b' \in \bar{B}'$. Then

$$G_p = V \cdot \bar{B} = v'V\bar{B}v'^{-1} = Vv'b'\bar{B}b'^{-1}v'^{-1} = Vy^{-1}\bar{B}y.$$

Since $\bar{B}$ is the closure of $B^{(1)}$ and V is open, we obtain $G_p = V \cdot y^{-1}B^{(1)}y$. Therefore by $(B^{(1)} : B^{(d)}) = d$, we obtain $|V\backslash G_p/y^{-1}B^{(d)}y| \leq d$.

To prove the opposite inequality, put $\pi = \begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}$, and suppose that $\pi^j \in (yVy^{-1})\pi^i B^{(d)}$, with $i, j \in \mathbf{Z}$. Put $\pi^j = yvy^{-1}\pi^i b$, with $v \in V$, $b \in B^{(d)}$. Then we obtain $yvy^{-1} = \pi^j b^{-1}\pi^{-i}$; hence by comparing the eigenvalues of both sides, we obtain $i \equiv j \pmod{d}$. Therefore, $1, \pi, \cdots, \pi^{d-1}$ belong to the distinct $yVy^{-1}\backslash G_p / B^{(d)}$ double cosets. Therefore, $|V\backslash G_p / y^{-1}B^{(d)}y| = |yVy^{-1}\backslash G_p / B^{(d)}| \geq d$; hence the proof is completed. □

COROLLARY (of Proposition 7). *Let* $\Delta = \Gamma \cap (G_{\mathbf{R}} \times x^{-1}Vx)$, *with* $x \in PL_2(\mathbf{Q}_p)$, $V = PSL_2(\mathbf{Z}_p)$. *Then the number of* $\Delta_{\mathbf{R}}$*-equivalence classes of cusps of* $\Delta_{\mathbf{R}}$ *is given by* $\sum_{P \in \wp_\infty(\Gamma)} \deg P$. *In particular, this number is independent of* x.

REMARK . This second assertion is non-trivial because of the following circumstance. Put $\Delta^{(x)} = \Gamma \cap (G_{\mathbf{R}} \times x^{-1}Vx)$. Then $\Delta_{\mathbf{R}}^{(x)}$ and $\Delta_{\mathbf{R}}^{(x')}$ are conjugate in $\Gamma_{\mathbf{R}}$ (and hence in $G_{\mathbf{R}}$) provided $x^{-1}x' \in PSL_2(\mathbf{Q}_p) \cdot PL_2(\mathbf{Z}_p)$, but in general, they are not conjugate in $G_{\mathbf{R}}$. So, it does not follow trivially that they have the equal number of non-equivalent cusps.

These facts are used later in the computation of $\zeta_\Gamma(u)$.

§27. Lemmas for the proof of Theorem 3. The following Lemma 13 is for the proof of Lemma 14.

LEMMA 13. *Let* Δ *be a fuchsian group and let* $\delta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *run over all elements of* Δ. *Then the following two conditions are equivalent:*

(i) $(0, 0)$ *is not an accumulating point of* (c, d);
(ii) Δ *contains a translation.*

REMARK . In the following, we need only the implication (i) ⇒ (ii), and this proof is the less easier; so here we shall prove only this, and leave the other (which is easier and rather well-known) to the readers.

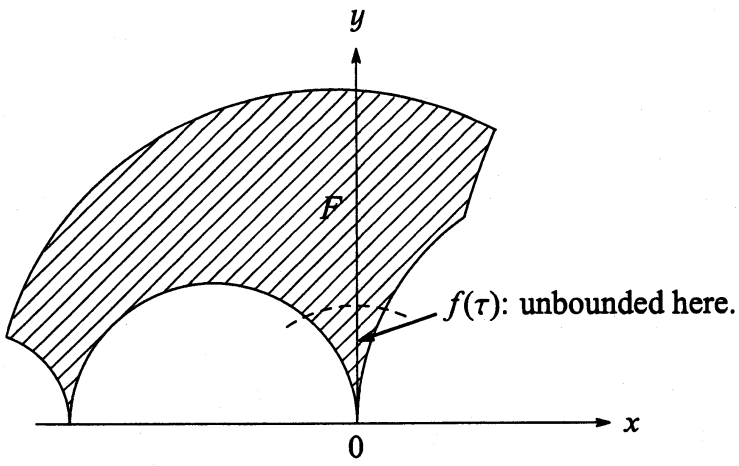
PROOF OF (i) ⇒ (ii). Let $\mathfrak{H}$ be the complex upper half plane, let $\tau \in \mathfrak{H}$, and put $f_0(\tau) = \inf_\delta |c\tau + d|^2$. Then $|c\tau + d|^2 > \varepsilon_\tau(c^2 + d^2)$, where ε_τ is a positive number depending only on τ and not on c, d; hence (i) implies $f_0(\tau) > 0$. Since $\mathrm{Im}\,(\delta\tau) = \frac{\mathrm{Im}\,(\tau)}{|c\tau+d|^2}$, we have $f(\tau) \underset{\text{def.}}{=} \sup_\delta \mathrm{Im}\,(\delta\tau) = \frac{\mathrm{Im}\,(\tau)}{f_0(\tau)} < \infty$. Moreover, $f(\tau)$ is a continuous function of τ. In fact, since $f(\tau)$ is the supremum of the continuous functions $\mathrm{Im}\,(\delta\tau)$, it is lower semi-continuous. On the other hand, if δ runs over Δ and τ runs over any compact subset K of $\mathfrak{H}$, then $|c\tau + d|^2$ has a positive lower bound (by (i)); hence $\mathrm{Im}\,(\delta\tau)$ has a finite upper bound. But then there is a positive constant C such that if $d(\tau, \tau_1)$ is the geodesic distance of τ, τ_1 by an invariant metric of $\mathfrak{H}$, we have

$$|\mathrm{Im}\,(\delta\tau_1) - \mathrm{Im}\,(\delta\tau)| \leq C \cdot d(\delta\tau_1, \delta\tau) = C \cdot d(\tau_1, \tau)$$

for all $\delta \in \Delta$ and $\tau, \tau_1 \in K$ (recall that an invariant metric of $\mathfrak{H}$ is given by $ds^2 = \frac{dx^2+dy^2}{y^2}$ for $x + yi \in \mathfrak{H}$). Therefore, the functions $\mathrm{Im}\,(\delta\tau)$ ($\delta \in \Delta$) are equicontinuous on K; hence $f(\tau)$ is also upper semi-continuous. Therefore, $f(\tau)$ is a continuous function which is

obviously Δ-invariant. On the other hand, since $f(\tau) \geq \mathrm{Im}\,(\tau)$, $f(\tau)$ is unbounded (on $\mathfrak{H}$). Thus we conclude first, that the quotient $\mathfrak{H}/\Delta$ cannot be compact.

Now let F be a fundamental domain of Δ. Then since $f(\tau)$ is unbounded in F and is bounded in any compact subset of F, we conclude that F has a cusp: $\tau = \alpha \in \mathbf{R} \cup \{i\infty\}$ *at which* $f(\tau)$ *is unbounded.* Now if $\alpha = i\infty$, there is nothing more to be proved. So let us assume $\alpha \in \mathbf{R}$ and prove that α is Δ-equivalent to $i\infty$. We may also assume without loss of generality, that $\alpha = 0$ (since we may conjugate Δ by a translation, if necessary).



Now put $\inf_{\delta}(c^2 + d^2) = m$ (> 0 by (i)), and let $\tau = x + yi \in F$ with $|x| \leq |y|$. Then

$$|c\tau + d|^2 = (cx + d)^2 + c^2y^2 = (x^2 + y^2)c^2 + 2cdx + d^2$$

$$= (x^2 + y^2)(c + \frac{x}{x^2 + y^2}d)^2 + \frac{y^2d^2}{x^2 + y^2} \geq \frac{y^2d^2}{x^2 + y^2} \geq \frac{d^2}{2}.$$

Hence $f_0(\tau) \geq \frac{1}{2}\inf_{\delta}(d^2)$. But since $f(\tau) = \frac{\mathrm{Im}\,(\tau)}{f_0(\tau)}$ is unbounded in this region (near $\tau = 0$ in F), we obtain

$$\inf_{\delta} |d| = 0. \tag{106}$$

Now suppose that there is no $\delta \in \Delta$ with $d = 0$. Then by (106) there must be a sequence $\{\delta_n\}_{n=1}^{\infty}$ in Δ with $\delta_n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$, $d_n \neq 0$, and $\lim_{n\to\infty} d_n = 0$. On the other hand since $\tau = 0$ is a cusp, Δ contains an element $\delta_0 = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$ with some $r > 0$. Put $\delta_n^{(k)} = \delta_n\delta_0^k = \begin{pmatrix} a_n^{(k)} & b_n^{(k)} \\ c_n^{(k)} & d_n^{(k)} \end{pmatrix}$ for each $k \in \mathbf{Z}$; so that $c_n^{(k)} = c_n + d_nrk$, $d_n^{(k)} = d_n$. Now for each n, choose $k = k_n$ so that $|c_n^{(k_n)}| < |d_n|r$, and put $\delta_n' = \delta_n^{(k_n)} = \begin{pmatrix} a_n' & b_n' \\ c_n' & d_n' \end{pmatrix}$. Then $d_n' = d_n$, $|c_n'| < |d_n|r$. But then $\lim_{n\to\infty} c_n' = \lim_{n\to\infty} d_n' = 0$, which is a contradiction to (i). Therefore, by (106) there must be some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta$ with $d = 0$. But then $\gamma(0) = i\infty$; hence $i\infty$ is a cusp of Δ; hence Δ contains a translation (namely, $\gamma\delta_0\gamma^{-1} = \begin{pmatrix} 1 & -b^2r \\ 0 & 1 \end{pmatrix}$). □

LEMMA 14. *Let Δ be a fuchsian group and let $\gamma \in G_{\mathbf{R}}$ be a parabolic element such that $\gamma^{-1}\Delta\gamma \sim \Delta$ (commensurable). Then the fixed point of γ (on $\mathbf{R} \cup \{i\infty\}$) is a cusp of Δ.*

PROOF. We may assume without loss of generality that $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, so that the fixed point of γ is $i\infty$. Suppose on the contrary that $i\infty$ is not a cusp of Δ, or equivalently that Δ contains no translation. Then by Lemma 13 applied for the fuchsian group $\Delta \cap \gamma^{-1}\Delta\gamma$, we can find a sequence $\{\xi_n\}_{n=1}^{\infty}$ in $\Delta \cap \gamma^{-1}\Delta\gamma$ such that $\lim_{n\to\infty} c_n = \lim_{n\to\infty} d_n = 0$, where $\xi_n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$. Put $\eta_n = \xi_n^{-1}\gamma\xi_n\gamma^{-1} = \begin{pmatrix} 1 + c_n d_n & d_n^2 - c_n d_n - 1 \\ -c_n^2 & c_n^2 - c_n d_n + 1 \end{pmatrix}$. Then $\eta_n \in \Delta$, and $\lim_{n\to\infty} \eta_n = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$. But since Δ is discrete, this implies $\eta_n = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \gamma^{-1}$ for all sufficiently large n. But this is impossible since this would imply $\xi_n^{-1}\gamma\xi_n\gamma^{-1} = \gamma^{-1}$ (for such n); hence $\gamma = 1$, which is a contradiction. Therefore, $i\infty$ must be a cusp of Δ. □

The following two lemmas are also needed for the proof of Theorem 3.

LEMMA 15. *The quotient $G_{\mathfrak{p}}/A_{\mathfrak{p}}$ by an abelian closed subgroup $A_{\mathfrak{p}}$ is non-compact.*

PROOF. If $A_{\mathfrak{p}} = \{1\}$, our assertion is trivial; so assume $A_{\mathfrak{p}} \neq \{1\}$. Let $1 \neq x \in A_{\mathfrak{p}}$ and let $T_{\mathfrak{p}}$ be the centralizer of x in $G_{\mathfrak{p}}$, so that $A_{\mathfrak{p}} \subset T_{\mathfrak{p}}$. Then $T_{\mathfrak{p}}$ is conjugate in $PL_2(k_{\mathfrak{p}})$ to either (i) the diagonal subgroup of $G_{\mathfrak{p}}$, or (ii) a compact torus in $G_{\mathfrak{p}}$, or (iii) the group $\begin{pmatrix} 1 & k_{\mathfrak{p}} \\ 0 & 1 \end{pmatrix}$. But in any case, it can be checked easily that $G_{\mathfrak{p}}/T_{\mathfrak{p}}$ is non-compact. Therefore, $G_{\mathfrak{p}}/A_{\mathfrak{p}}$ is non-compact. □

LEMMA 16. *Consider the group*

$$\mathcal{B}_p = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \,\middle|\, a \in \mathbf{Q}_p^{\times},\ b \in \mathbf{Q}_p \right\} / \pm 1 \tag{107}$$

as a subgroup of $G_{\mathfrak{p}} = PSL_2(k_{\mathfrak{p}})$. Then if $k_{\mathfrak{p}} \neq \mathbf{Q}_p$, $G_{\mathfrak{p}}/\mathcal{B}_p$ is non-compact.

PROOF. Put

$$\mathcal{B}_{\mathfrak{p}} = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} \,\middle|\, \alpha \in k_{\mathfrak{p}}^{\times},\ \beta \in k_{\mathfrak{p}} \right\} / \pm 1.$$

It is enough to show that if $k_{\mathfrak{p}} \neq \mathbf{Q}_p$, $\mathcal{B}_{\mathfrak{p}}/\mathcal{B}_p$ is non-compact. Put $V_{\mathfrak{p}} = \mathcal{B}_{\mathfrak{p}} \cap PSL_2(O_{\mathfrak{p}})$. Then since $V_{\mathfrak{p}}$ is an open compact subgroup of $\mathcal{B}_{\mathfrak{p}}$, $\mathcal{B}_{\mathfrak{p}}/\mathcal{B}_p$ is non-compact if and only if $V_{\mathfrak{p}}\backslash\mathcal{B}_{\mathfrak{p}}/\mathcal{B}_p$ is infinite. We shall show that $|V_{\mathfrak{p}}\backslash\mathcal{B}_{\mathfrak{p}}/\mathcal{B}_p| = \infty$ if $k_{\mathfrak{p}} \neq \mathbf{Q}_p$. Let $k_{\mathfrak{p}} \neq \mathbf{Q}_p$ and let e resp. f be the ramification index resp. the relative degree of the extension $k_{\mathfrak{p}}/\mathbf{Q}_p$, so that by $ef = [k_{\mathfrak{p}} : \mathbf{Q}_p] > 1$, either $e > 1$ or $f > 1$. If $e > 1$, let π be a prime element of $k_{\mathfrak{p}}$ and put $\omega_i = \pi^{-(ie+1)}$ $(i \geq 1)$; if $e = 1$ and $f > 1$, let ω be any element of $O_{\mathfrak{p}}$ outside $\mathfrak{p} + \mathbf{Z}_p$, and put $\omega_i = \omega p^{-i}$ $(i \geq 1)$. Then in either case the series ω_i $(i \geq 1)$ has the property: if $\omega_i - u\omega_j \in O_{\mathfrak{p}} + \mathbf{Q}_p$ for some $u \in U_p$, then $i = j$. From this follows immediately that the elements $\begin{pmatrix} 1 & \omega_i \\ 0 & 1 \end{pmatrix}$ $(i \geq 1)$ belong to the different double cosets $V_{\mathfrak{p}}\backslash\mathcal{B}_{\mathfrak{p}}/\mathcal{B}_p$; hence $|V_{\mathfrak{p}}\backslash\mathcal{B}_{\mathfrak{p}}/\mathcal{B}_p| = \infty$. □

§28. Proof of Theorem 3. The notations being as in §25, let $G_{\mathbf{R},z}$ be the parabolic stabilizer of z in $G_{\mathbf{R}}$. Then $G_{\mathbf{R},z} \cong \mathbf{R}$ and $H^0 = \{\gamma \in \Gamma \mid \gamma_{\mathbf{R}} \in G_{\mathbf{R},z}\}$; hence H^0 is abelian, and if ξ is any element of H^0 with $\xi \neq 1$, then H^0 is the centralizer of ξ in Γ. We shall prove

$$(H : H^0) = \infty. \tag{108}$$

For this purpose, let V be an open compact subgroup of $G_{\mathfrak{p}}$ and put $\Gamma^V = \Gamma \cap (G_{\mathbf{R}} \times V)$. Then by Lemma 14 applied to $\Delta = \Gamma^V_{\mathbf{R}}$ and $\gamma = \varepsilon_{\mathbf{R}}$, we conclude that z is a cusp of $\Gamma^V_{\mathbf{R}}$; hence for any $\gamma \in \Gamma$, $\gamma_{\mathbf{R}} z$ is also a cusp of $\Gamma^V_{\mathbf{R}}$. But since there are only finitely many non-equivalent cusps of $\Gamma^V_{\mathbf{R}}$, we have

$$|\Gamma^V \backslash \Gamma / H| < \infty. \tag{109}$$

Suppose that, contrary to (108), we had $(H : H^0) < \infty$. Then by (109), $|\Gamma^V \backslash \Gamma / H^0| < \infty$; hence $|V \backslash G_{\mathfrak{p}} / H^0| < \infty$. Let $A_{\mathfrak{p}}$ be the closure of $H^0_{\mathfrak{p}}$ in $G_{\mathfrak{p}}$. Then $A_{\mathfrak{p}}$ is abelian and $|V \backslash G_{\mathfrak{p}} / A_{\mathfrak{p}}| < \infty$; hence $G_{\mathfrak{p}}/A_{\mathfrak{p}}$ is compact. But this is impossible by Lemma 15. Therefore $(H : H^0) = \infty$.

Now put $H^{0V} = H^0 \cap \Gamma^V = H^0 \cap (G_{\mathbf{R}} \times V)$. Since z is a cusp of $\Gamma^V_{\mathbf{R}}$, and $H^{0V}_{\mathbf{R}}$ is the (parabolic) stabilizer group of z in $\Gamma^V_{\mathbf{R}}$, we have $H^{0V} \cong \mathbf{Z}$. Let ξ be a generator of H^{0V}. Then the centralizer of ξ in Γ is H^0, and hence by (108) there is an element $\delta \in H$ such that $\delta^{-1}\xi\delta \neq \xi^{\pm 1}$. But since $\delta^{-1}\xi\delta \in H^0 \cap (G_{\mathbf{R}} \times \delta_{\mathfrak{p}}^{-1} V \delta_{\mathfrak{p}})$, there is a positive integer m such that $\delta^{-1}\xi^m\delta \in H^{0V}$. Put $\delta^{-1}\xi^m\delta = \xi^n$ $(n \in \mathbf{Z})$. Now since $H^0_{\mathbf{R}} \subset G_{\mathbf{R},z} \cong \mathbf{R}$, H^0 can be considered as a subgroup of $\mathbf{R}$, and in this sense we have $\delta^{-1}\xi\delta = \xi^{n/m}$; hence $m \neq \pm n$. Therefore, $\delta_{\mathfrak{p}}^{-1}\xi_{\mathfrak{p}}^m\delta_{\mathfrak{p}} = \xi_{\mathfrak{p}}^n$ with $m \neq \pm n$; $m,\ n \neq 0$. Let $\pm\{\lambda_{\mathfrak{p}}, \lambda_{\mathfrak{p}}^{-1}\}$ be the eigenvalues of $\xi_{\mathfrak{p}}$. Then $\pm\lambda_{\mathfrak{p}}^{\pm m} = \pm\lambda_{\mathfrak{p}}^{\pm n}$; hence $\lambda_{\mathfrak{p}}$ is a root of unity. But since ξ is of infinite order, we conclude $\lambda_{\mathfrak{p}} = \pm 1$; hence there is an element $t_{\mathfrak{p}} \in PL_2(k_{\mathfrak{p}})$ such that $t_{\mathfrak{p}}^{-1}\xi_{\mathfrak{p}}t_{\mathfrak{p}} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (up to the sign). But $H^0_{\mathfrak{p}}$ centralizes $\xi_{\mathfrak{p}}$; hence $t_{\mathfrak{p}}^{-1}H^0_{\mathfrak{p}}t_{\mathfrak{p}} \subset \begin{pmatrix} 1 & k_{\mathfrak{p}} \\ 0 & 1 \end{pmatrix}$. Since $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in t_{\mathfrak{p}}^{-1} V t_{\mathfrak{p}}$ if b is sufficiently near 0, we conclude that for any $\gamma \in H^0$ there is a positive integer m such that $\gamma^{p^m} \in H^{0V}$. But since H^{0V} is generated by ξ, we see now that

$$t_{\mathfrak{p}}^{-1}H^0_{\mathfrak{p}}t_{\mathfrak{p}} \subset \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \,\middle|\, b \in \mathbf{Z}^{(p)} \right\}. \tag{110}$$

But since the centralizer of H^0 in H is H^0 itself, H/H^0 acts effectively on H^0, and by $(H : H^0) = \infty$, the automorphism group of H^0 is infinite. In particular, $H^0 \not\cong \mathbf{Z}$. But this and (110) show at once that the two groups in (110) must be equal;

$$t_{\mathfrak{p}}^{-1}H^0_{\mathfrak{p}}t_{\mathfrak{p}} = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \,\middle|\, b \in \mathbf{Z}^{(p)} \right\}. \tag{111}$$

Therefore $t_{\mathfrak{p}}^{-1}H_{\mathfrak{p}}t_{\mathfrak{p}}$ normalizes $\begin{pmatrix}1 & \mathbf{Z}^{(p)}\\ 0 & 1\end{pmatrix}$, and on the other hand, the centralizer of $\begin{pmatrix}1 & \mathbf{Z}^{(p)}\\ 0 & 1\end{pmatrix}$ in $t_{\mathfrak{p}}^{-1}H_{\mathfrak{p}}t_{\mathfrak{p}}$ coincides with $\begin{pmatrix}1 & \mathbf{Z}^{(p)}\\ 0 & 1\end{pmatrix}$. From this follows immediately that $t_{\mathfrak{p}}^{-1}H_{\mathfrak{p}}t_{\mathfrak{p}}$ is generated by $\begin{pmatrix}1 & \mathbf{Z}^{(p)}\\ 0 & 1\end{pmatrix}$ and an element of the form $\begin{pmatrix}p^d & \beta\\ 0 & p^{-d}\end{pmatrix}$, with some positive integer d and some $\beta \in k_{\mathfrak{p}}$. Now replace $t_{\mathfrak{p}}$ by $t_{\mathfrak{p}}\begin{pmatrix}1 & c\\ 0 & 1\end{pmatrix}$, with $c = \frac{-\beta}{p^d - p^{-d}}$. Then (110) remains valid, and $t_{\mathfrak{p}}^{-1}H_{\mathfrak{p}}t_{\mathfrak{p}}$ is generated by $\begin{pmatrix}1 & \mathbf{Z}^{(p)}\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}p^d & 0\\ 0 & p^{-d}\end{pmatrix}$; hence

$$t_{\mathfrak{p}}^{-1}H_{\mathfrak{p}}t_{\mathfrak{p}} = \left\{\begin{pmatrix}p^{dk} & b\\ 0 & p^{-dk}\end{pmatrix} \,\middle|\, k \in \mathbf{Z},\ b \in \mathbf{Z}^{(p)}\right\}. \tag{112}$$

On the other hand, since $\xi_{\mathbf{R}}$ is parabolic, there is an element $t_{\mathbf{R}} \in G_{\mathbf{R}}$ such that $t_{\mathbf{R}}^{-1}\xi_{\mathbf{R}}t_{\mathbf{R}} = \begin{pmatrix}1 & \pm 1\\ 0 & 1\end{pmatrix}$. By taking ξ^{-1} instead of ξ if necessary, we may assume that $t_{\mathbf{R}}^{-1}\xi_{\mathbf{R}}t_{\mathbf{R}} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. Let γ be any element of H^0 and put $t_{\mathfrak{p}}^{-1}\gamma_{\mathfrak{p}}t_{\mathfrak{p}} = \pm\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$ with $b \in \mathbf{Z}^{(p)}$. Then $t_{\mathbf{R}}^{-1}\gamma_{\mathbf{R}}t_{\mathbf{R}} = \pm\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}$. In fact, since H^0 is abelian, $t_{\mathbf{R}}^{-1}\gamma_{\mathbf{R}}t_{\mathbf{R}}$ commutes with $t_{\mathbf{R}}^{-1}\xi_{\mathbf{R}}t_{\mathbf{R}} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, and hence is of the form $\begin{pmatrix}1 & b'\\ 0 & 1\end{pmatrix}$ ($b' \in \mathbf{R}$). But since $\gamma_{\mathfrak{p}}^{p^m} = \xi_{\mathfrak{p}}^{b'}$, where $b = b'/p^m$ ($b' \in \mathbf{Z}$, $m > 0$), we get the same relation on the real part; hence $b' = b$. Therefore,

$$H^0 = \left\{t\delta t^{-1} \,\middle|\, \delta \in \begin{pmatrix}1 & \mathbf{Z}^{(p)}\\ 0 & 1\end{pmatrix}\right\}, \text{ with } t = t_{\mathbf{R}} \times t_{\mathfrak{p}}.$$

Now take $\eta \in H$ such that $t_{\mathfrak{p}}^{-1}\eta_{\mathfrak{p}}t_{\mathfrak{p}} = \begin{pmatrix}p^d & 0\\ 0 & p^{-d}\end{pmatrix}$, so that H^0 and η generate H. Then $t_{\mathbf{R}}^{-1}\eta_{\mathbf{R}}t_{\mathbf{R}}$ normalizes $\begin{pmatrix}1 & \mathbf{Z}^{(p)}\\ 0 & 1\end{pmatrix}$, and hence is of the form $\begin{pmatrix}p^l & \beta\\ 0 & p^{-l}\end{pmatrix}$ ($l \in \mathbf{Z}, \beta \in \mathbf{R}$). But by $\eta_{\mathfrak{p}}\xi_{\mathfrak{p}}\eta_{\mathfrak{p}}^{-1} = \xi_{\mathfrak{p}}^{p^{2d}}$, we get the same relation on the real part, and hence $l = d$. Now replace $t_{\mathbf{R}}$ by $t_{\mathbf{R}}\begin{pmatrix}1 & c\\ 0 & 1\end{pmatrix}$, with $c = -\frac{\beta}{p^d - p^{-d}}$. Then since

$$\begin{pmatrix}1 & -c\\ 0 & 1\end{pmatrix}\begin{pmatrix}p^d & \beta\\ 0 & p^{-d}\end{pmatrix}\begin{pmatrix}1 & c\\ 0 & 1\end{pmatrix} = \begin{pmatrix}p^d & 0\\ 0 & p^{-d}\end{pmatrix},$$

and since H^0 and η generate H, we obtain

$$H = tB^{(d)}t^{-1}, \quad H^0 = t\begin{pmatrix}1 & \mathbf{Z}^{(p)}\\ 0 & 1\end{pmatrix}t^{-1}, \tag{113}$$

with $t = t_{\mathbf{R}} \times t_{\mathfrak{p}}$, $B^{(d)} = \left\{\begin{pmatrix}p^{dk} & b\\ 0 & p^{-dk}\end{pmatrix} \,\middle|\, k \in \mathbf{Z},\ b \in \mathbf{Z}^{(p)}\right\}$.

Now we shall prove $k_\mathfrak{p} = \mathbf{Q}_p$. By (109), we have $|V\backslash G_\mathfrak{p}/H_\mathfrak{p}| < \infty$; hence by (112), $|V\backslash G_\mathfrak{p}/t_\mathfrak{p}\mathcal{B}_p t_\mathfrak{p}^{-1}| < \infty$, where $\mathcal{B}_p = \left\{\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \middle| \, a \in \mathbf{Q}_p^\times,\ b \in \mathbf{Q}_p \right\}$. But then $G_\mathfrak{p}/t_\mathfrak{p}\mathcal{B}_p t_\mathfrak{p}^{-1}$, and hence $G_\mathfrak{p}/\mathcal{B}_p$ is also compact. Therefore by Lemma 16, we obtain $k_\mathfrak{p} = \mathbf{Q}_p$.

Finally, put

$$B' = \left\{\begin{pmatrix} p^k & b \\ 0 & p^l \end{pmatrix} \middle| \, k,\ l \in \mathbf{Z},\ b \in \mathbf{Z}^{(p)} \right\} \Big/ p\text{-powers}. \tag{114}$$

Then $B^{(d)}$ is a normal subgroup of B', and $PL_2(\mathbf{Q}_p) = PL_2(\mathbf{Z}_p) \cdot B'$. Put $t_\mathfrak{p} = \tilde{t}_\mathfrak{p} b'$ with $\tilde{t}_\mathfrak{p} \in PL_2(\mathbf{Z}_p)$, $b' \in B'$, and put $t_\mathbf{R} = \tilde{t}_\mathbf{R} b'$ ($\tilde{t}_\mathbf{R} \in G_\mathbf{R}$). Then $H = tB^{(d)}t^{-1} = \tilde{t}B^{(d)}\tilde{t}^{-1}$, where $\tilde{t} = \tilde{t}_\mathbf{R} \times \tilde{t}_\mathfrak{p} \in G_\mathbf{R} \times PL_2(\mathbf{Z}_p)$. This completes the proof of Theorem 3. □

Study of elements of Γ with elliptic real parts.

§29. In the following, we shall study in detail such element $\gamma \in \Gamma$ that $\gamma_\mathbf{R}$ is elliptic, i.e., $\gamma_\mathbf{R}$ has imaginary eigenvalues, or equivalently, has a fixed point on $\mathfrak{H}$. Let $z \in \mathfrak{H}$, and put $\Gamma_z = \{\gamma \in \Gamma \mid \gamma_\mathbf{R} z = z\}$. Call $z, z' \in \mathfrak{H}$ "Γ-equivalent" if there exists $\gamma \in \Gamma$ with $z' = \gamma_\mathbf{R} z$. As before, let $\wp(\Gamma)$ be the set of all Γ-equivalence classes of points $z \in \mathfrak{H}$ with $|\Gamma_z| = \infty$ (§3); on the other hand, denote by

$$Q(\Gamma) \tag{115}$$

the set of all Γ-equivalence classes of z with $1 < |\Gamma_z| < \infty$. Put

$$\begin{cases} V = PSL_2(O_\mathfrak{p}), \quad T_\mathfrak{p}^l = V\begin{pmatrix} \pi^l & 0 \\ 0 & \pi^{-l} \end{pmatrix} V \ (l \geq 0), \quad l(x) = l \text{ for } x \in T_\mathfrak{p}^l; \\ \Gamma^0 = \Gamma \cap (G_\mathbf{R} \times V), \ T^l = \Gamma \cap (G_\mathbf{R} \times T_\mathfrak{p}^l), \quad l(\gamma) = l \text{ for } \gamma \in T^l, \end{cases} \tag{116}$$

where π is a prime element of $k_\mathfrak{p}$. For each $P \in \wp(\Gamma)$ (resp. $Q \in Q(\Gamma)$), denote by

$$P/\Gamma^0 \quad (\text{resp. } Q/\Gamma^0) \tag{117}$$

the set of all Γ^0-equivalence classes contained in P (resp. Q). Then our purpose is to parametrize the set P/Γ^0 (resp. Q/Γ^0) in a nice way, and for each element of P/Γ^0 (resp. Q/Γ^0) with a representative $z \in \mathfrak{H}$, to compute $l(\gamma)$ for each $\gamma \in \Gamma_z$ (expressed by $\deg\{\gamma\}_\Gamma$, the parameters of P/Γ^0 (resp. Q/Γ^0), etc.) (Theorems 4, 5, 6). This will enable us to compute, for each $\gamma \in \Gamma$ with elliptic $\gamma_\mathbf{R}$, the following quantity;

$$A_l\{\gamma\}_\Gamma = \sum_{\{\delta\}_{\Gamma^0}} \frac{1}{e\{\delta\}_{\Gamma^0}} \qquad (l \geq 1), \tag{118}$$

where $\{\delta\}_{\Gamma^0}$ runs over all Γ^0-conjugacy classes contained in $\{\gamma\}_\Gamma \cap T^l$, and $e\{\delta\}_{\Gamma^0}$ is the order of the group $\Gamma_\delta \cap \Gamma^0$, Γ_δ being the centralizer of δ in Γ. This computation is used essentially in the succeeding part of our study: the computation of $\zeta_\Gamma(u)$ for the general Γ (without the assumptions that Γ is torsion-free or G/Γ is compact).

$\wp(\Gamma)$ **and** $Q(\Gamma)$. Let $z \in \mathfrak{H}$ and put $\Gamma_z = \{\gamma \in \Gamma \mid \gamma_{\mathbf{R}} z = z\}$. Then Γ_z is abelian (§3). Moreover,

PROPOSITION 8. *Let $\gamma \in \Gamma_z$ with $\gamma \neq 1$, and $\delta \in \Gamma$. If $\delta^{-1}\gamma\delta \in \Gamma_z$ then $\delta \in \Gamma_z$.*

PROOF. We have $(\delta_{\mathbf{R}}^{-1}\gamma_{\mathbf{R}}\delta_{\mathbf{R}})z = z$; hence $\delta_{\mathbf{R}}z$ is also fixed by $\gamma_{\mathbf{R}}$, and $\delta_{\mathbf{R}}z \in \mathfrak{H}$. Hence $\delta_{\mathbf{R}}z = z$; hence $\delta \in \Gamma_z$. □

COROLLARY . *Let $\gamma \in \Gamma_z$ with $\gamma \neq 1$. Then*

(i) *Γ_z is the centralizer of γ in Γ.*
(ii) *γ is not Γ-conjugate to any other element of Γ_z.*

(I) Γ_z **for** $P_z \in \wp(\Gamma)$. Let $P \in \wp(\Gamma)$ be represented by z (hence we may denote $P = P_z$), so that $|\Gamma_z| = \infty$. We denote by Γ_z^e the torsion subgroup of Γ_z, and by $e(P) = e_0(P)p^{r(P)}$ its order [14] where $e_0(P) \not\equiv 0 \pmod{p}$.

PROPOSITION 9. *Let $W(k_\mathfrak{p})$ be the group of all roots of unity contained in $k_\mathfrak{p}$. Then Γ_z^e is isomorphic to a subgroup of $W(k_\mathfrak{p})/\pm 1$.*

PROOF. By Proposition 3 (§4), there is some $x_\mathfrak{p} \in G_\mathfrak{p}$ such that $x_\mathfrak{p}^{-1}\Gamma_{z,\mathfrak{p}}x_\mathfrak{p}$ is diagonal. Therefore, Γ_z is isomorphic to a subgroup of $k_\mathfrak{p}^\times/\pm 1$. □

COROLLARY . *Γ_z^e is finite cyclic, and $e_0(P)$ divides $\frac{q-1}{2}$ (if $\mathfrak{p} \nmid 2$) or $q-1$ (if $\mathfrak{p}|2$). Moreover $k_\mathfrak{p}$ contains primitive $2e(P)$-th roots of unity.*

We shall show later (§34) that $e(P) = 1$ holds for almost all $P \in \wp(\Gamma)$.

(II) Γ_z **for** $Q_z \in Q(\Gamma)$. Let $Q(\Gamma)$ be the set of all Γ-equivalence classes $Q = Q_z$ of points $z \in \mathfrak{H}$ for which Γ_z is finite but $\neq \{1\}$. For each $Q = Q_z \in Q(\Gamma)$, let $e(Q) = e_0(Q)p^{r(Q)}$ be the order of Γ_z, with $e_0(Q) \not\equiv 0 \pmod{p}$.

PROPOSITION 10. *Let $Q = Q_z \in Q(\Gamma)$ and let $\gamma \in \Gamma_z$ with $\gamma \neq 1$. Let $\pm\{\zeta, \zeta^{-1}\}$ be the eigenvalues of $\gamma_\mathfrak{p}$. Then*

(i) *$K_\mathfrak{p} = k_\mathfrak{p}(\zeta)$ is a quadratic extension which depends only on Q.*
(ii) *Γ_z is isomorphic to a subgroup of $W(K_\mathfrak{p}^1)/\pm 1$, where $W(K_\mathfrak{p}^1)$ is the group of all roots of unity contained in $K_\mathfrak{p}^1 = \{x \in K_\mathfrak{p} \mid N_{K_\mathfrak{p}/k_\mathfrak{p}}x = 1\}$. In particular, $e_0(Q)$ divides $\frac{1}{2}(q+1)$ (if $\mathfrak{p} \nmid 2$), or $q+1$ (if $\mathfrak{p}|2$).*
(iii) *If $K_\mathfrak{p}/k_\mathfrak{p}$ is ramified, $e_0(Q) = 1$; i.e., $e(Q)$ is a power of p.*

REMARK . On the other hand, $r(Q)$ may not be zero even if $K_\mathfrak{p}/k_\mathfrak{p}$ is unramified.

PROOF. Let $G_\gamma = G_{\gamma\mathbf{R}} \times G_{\gamma\mathfrak{p}}$ be the centralizer of γ in G. Then by the assertion (b) (§29 of Chapter 2, Part 2), G_γ/Γ_γ is compact. Since Γ_z is finite, this implies that G_γ is compact; hence $G_{\gamma\mathfrak{p}}$ is also compact. But $G_{\gamma\mathfrak{p}}$ is the centralizer of $\gamma_\mathfrak{p}$ in $G_\mathfrak{p}$; hence ζ cannot be contained in $k_\mathfrak{p}$ (see the proof of Proposition 3 (§4)). Now since $\Gamma_z \cong \Gamma_{z\mathbf{R}} \subset G_{\gamma\mathbf{R}} \cong \mathbf{R}/\mathbf{Z}$, Γ_z is cyclic. Let δ be a generator of Γ_z and let $\pm\{\eta, \eta^{-1}\}$ be the eigenvalues of $\delta_\mathfrak{p}$. Put $K_\mathfrak{p} = k_\mathfrak{p}(\eta)$. Then $[K_\mathfrak{p} : k_\mathfrak{p}] = 2$, and since ζ is a positive power of $\pm\eta$, we have $\zeta \in K_\mathfrak{p}$. But since $\zeta \notin k_\mathfrak{p}$, we have $K_\mathfrak{p} = k_\mathfrak{p}(\zeta)$. The second assertion follows immediately from

[14] By the corollary below, $e(P)$ is finite.

this. Now suppose that $e_0(Q) \neq 1$, and assume that γ is of order $e_0(Q)$. Then $K_\mathfrak{p} = k_\mathfrak{p}(\zeta)$ is unramified; hence (iii). □

By Proposition 10, to each $Q \in \mathcal{Q}(\Gamma)$, we can attach a quadratic extension $K_\mathfrak{p}/k_\mathfrak{p}$. Put

$$\begin{cases} \mathcal{Q}_u(\Gamma) = \{Q \in \mathcal{Q}(\Gamma) \mid K_\mathfrak{p}/k_\mathfrak{p} \text{ is unramified } \}, \\ \mathcal{Q}_r(\Gamma) = \{Q \in \mathcal{Q}(\Gamma) \mid K_\mathfrak{p}/k_\mathfrak{p} \text{ is ramified } \}, \end{cases} \tag{119}$$

so that $\mathcal{Q}(\Gamma) = \mathcal{Q}_u(\Gamma) \cup \mathcal{Q}_r(\Gamma)$ (disjoint), and we have $e_0(Q) = 1$ (hence $e(Q) = p^{r(Q)}$) for $Q \in \mathcal{Q}_r(\Gamma)$.

The finiteness of the set $\mathcal{Q}(\Gamma)$ will be shown in §34.

REMARK . In each case $Q \in \mathcal{Q}_u(\Gamma)$ or $\in \mathcal{Q}_r(\Gamma)$, the field $K_\mathfrak{p}$ does not (even) depend on Q. In fact, if $Q \in \mathcal{Q}_u(\Gamma)$, $K_\mathfrak{p}$ must be the unique unramified quadratic extension and if $Q \in \mathcal{Q}_r(\Gamma)$, it is clear by Proposition 10 that $K_\mathfrak{p}$ must coincide with the field obtained by adjoining primitive p-th roots of unity to $k_\mathfrak{p}$. (Even then, $K_\mathfrak{p}$ may contain higher p-powerth roots of unity.)

§30. P/Γ^0 for $P \in \wp(\Gamma)$. Let $P = P_z \in \wp(\Gamma)$. For each $\gamma \in \Gamma_z$, put

$$\deg\{\gamma\}_\Gamma = |\operatorname{ord}_\mathfrak{p} \lambda_\mathfrak{p}|, \tag{120}$$

where $\pm\{\lambda_\mathfrak{p}, \lambda_\mathfrak{p}^{-1}\}$ denote the eigenvalues of $\gamma_\mathfrak{p}$. Thus, $\deg\{\gamma\}_\Gamma$ is a multiple of $\deg P$, they are equal if and only if γ generates Γ_z modulo Γ_z^e, and $\deg\{\gamma\}_\Gamma = 0$ if and only if $\gamma \in \Gamma_z^e$ (see §5). As defined in §29, let P/Γ^0 be the set of all Γ^0-equivalence classes of points on $\mathfrak{H}$ that are Γ-equivalent to z. The following theorem (and its corollary) generalizes Lemma 3 (§13) (with a considerably simpler proof).

THEOREM 4. *Let $P \in \wp(\Gamma)$, and put $d = \deg P$, $e = e(P)$, $e_0 = e_0(P)$, $r = r(P)$ (hence $e = e_0 p^r$), and $c(p^r - p^{r-1}) = \operatorname{ord}_\mathfrak{p} p$.*[15] *Then*

(i) *the set P/Γ^0 is described as follows;*

(a) *P/Γ^0 contains special d elements;*

$$R_1, \cdots, R_d. \tag{121}$$

(b) *All other elements of P/Γ^0 are parametrized as*

$$R_{k\mu} \quad \begin{cases} k = 1, 2, 3 \cdots; \\ 1 \leq \mu \leq d\frac{q^k - q^{k-1}}{e_0 p^{\nu_k}}; \end{cases} \tag{122}$$

where ν_k is an integer defined by [16]

$$\nu_k = \begin{cases} 0 & \cdots 0 < k \leq c, \\ \nu & \cdots cp^{\nu-1} < k \leq cp^\nu \quad (1 \leq \nu \leq r-1), \\ r & \cdots cp^{r-1} < k. \end{cases}$$

[15] Since $k_\mathfrak{p}$ contains primitive p^r-th root of unity, c is a positive integer.

[16] Thus for $r = 0$, $\nu_k = 0$.

(ii)

(a) *Let $z_i \in \mathfrak{H}$ represent R_i $(1 \le i \le d)$, and let $\delta \in \Gamma_{z_i}$ $(\delta \ne 1)$. Then*

$$l(\delta) = \deg\{\delta\}_\Gamma. \tag{123}$$

(b) *Let $z_{k\mu} \in \mathfrak{H}$ represent $R_{k\mu}$ and let $\delta \in \Gamma_{z_{k\mu}}$ with $\delta \ne 1$. Then*

$$l(\delta) = \begin{cases} \deg\{\delta\}_\Gamma + k & \cdots \begin{cases} \text{if } \deg\{\delta\}_\Gamma > 0; \text{ or} \\ \text{if } \deg\{\delta\}_\Gamma = 0, \\ \quad \text{but the order of } \delta \text{ is not a power of } p. \end{cases} \\ \operatorname{Max}(0, k - cp^\nu) & \cdots \text{if the order of } \delta \text{ is } p^{r-\nu} \ (0 \le \nu \le r-1). \end{cases} \tag{124}$$

In particular, the order of $\Gamma_{z_{k\mu}} \cap \Gamma^0$ is given by $p^{r-\nu_k}$, and the order of $\Gamma_{z_i} \cap \Gamma^0$ $(1 \le i \le d)$ is always e; i.e., $\Gamma_{z_i} \cap \Gamma^0$ (coincides with) the torsion subgroup of Γ_{z_i}.

Proof. It is enough to parametrize the double coset $\Gamma^0 \backslash \Gamma / \Gamma_z$ and for each $\Gamma^0 g \Gamma_z$, to compute $l(\delta)$ for each $\delta \in g\Gamma_z g^{-1}$. By the embedding into $G_\mathfrak{p}$, it is the same thing to do it for $V \backslash G_\mathfrak{p} / \Gamma_{z\mathfrak{p}}$. Take $x \in G_\mathfrak{p}$ such that $T = x^{-1}\Gamma_{z\mathfrak{p}} x$ is diagonal, and for each $\delta \in \Gamma_z$ $(\delta \ne 1)$ put

$$x^{-1}\delta_\mathfrak{p} x = t = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \qquad (a \in k_\mathfrak{p}^\times), \tag{125}$$

so that $\deg\{\delta\}_\Gamma = |\operatorname{ord}_\mathfrak{p} a|$. Now $g \mapsto g' = gx$ induces a bijection of $V \backslash G_\mathfrak{p} / \Gamma_{z\mathfrak{p}}$ onto $V \backslash G_\mathfrak{p} / T$, and for each $Vg\Gamma_{z\mathfrak{p}}$, we have $l(g\delta_\mathfrak{p} g^{-1}) = l(g' t g'^{-1})$; hence *it is enough to parametrize $V \backslash G_\mathfrak{p} / T$* and for each $Vg'T$, to compute $l(g' t g'^{-1})$.

Now we shall use the following set of representatives of $V \backslash G_\mathfrak{p}$;

$$x_{n\alpha} = \begin{pmatrix} \pi^{-n} & \alpha \\ 0 & \pi^n \end{pmatrix}; \quad \begin{array}{l} n = 0, \pm 1, \pm 2, \cdots; \\ \alpha : \text{representatives of } k_\mathfrak{p} \mod \mathfrak{p}^n; \\ \text{Choose } \alpha = 0 \text{ for } \alpha \equiv 0 \mod \mathfrak{p}^n. \end{array} \tag{126}$$

Since T is generated by two elements $\begin{pmatrix} b & 0 \\ 0 & b^{-1} \end{pmatrix}, \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$ where $b \in k_\mathfrak{p}$ with $\operatorname{ord}_\mathfrak{p} b = d$ and where ζ is a primitive $2e$-th root of unity in $k_\mathfrak{p}^\times$, we can choose the following set of representatives for $V \backslash G_\mathfrak{p} / T$;

$$\begin{cases} \sigma^\mu = \begin{pmatrix} \pi^{-\mu} & 0 \\ 0 & \pi^\mu \end{pmatrix}; & \mu = 0, 1, 2, \cdots, d-1; \\ \tau_{k\rho}^\mu = \begin{pmatrix} \pi^{-\mu} & \alpha_{k\rho}\pi^{\mu-k} \\ 0 & \pi^\mu \end{pmatrix}; & \begin{array}{l} \mu = 0, 1, 2, \cdots, d-1; \\ k = 1, 2, 3, \cdots; \\ \rho = 1, 2, 3, \cdots, n_k', \end{array} \end{cases} \tag{127}$$

where $\alpha_{k\rho}$ runs over a set of representatives of $\mathcal{U}_\mathfrak{p} / E(1 + \mathfrak{p}^k)$, and where E is the group of all e-th roots of unity contained in $k_\mathfrak{p}$; hence $n_k' = (\mathcal{U}_\mathfrak{p} : E(1 + \mathfrak{p}^k))$. Now let us compute $l(\sigma^\mu t \sigma^{-\mu})$ and $l(\tau_{k\rho}^\mu t (\tau_{k\rho}^\mu)^{-1})$. We have $\sigma^\mu t \sigma^{-\mu} = t$; hence $l(\sigma^\mu t \sigma^{-\mu}) = l(t)$; hence for these

d elements σ^μ, $l(\sigma^\mu t\sigma^{-\mu}) = \deg\{\delta\}_\Gamma$. Therefore if we denote by R_μ $(1 \le \mu \le d)$ the elements of P/Γ^0 corresponding to σ^μ, we have (i)(a) and (ii)(a). As for $\tau^\mu_{k\rho}$, we have

$$y = \tau^\mu_{k\rho} t (\tau^\mu_{k\rho})^{-1} = \begin{pmatrix} a & \alpha_{k\rho}(a^{-1} - a)\pi^{-k} \\ 0 & a^{-1} \end{pmatrix}; \tag{128}$$

hence if $\deg\{\delta\}_\Gamma = |\operatorname{ord}_\mathfrak{p} a| > 0$, we have $l(y) = |\operatorname{ord}_\mathfrak{p} a| + k = \deg\{\delta\}_\Gamma + k$. Also if $\deg\{\delta\}_\Gamma = 0$ but the order of δ (i.e., the order of a^2 as a root of unity) is not a power of p, we have $\operatorname{ord}_\mathfrak{p}(a^{-1} - a) = 0$; hence $l(y) = k = \deg\{\delta\}_\Gamma + k$. Finally if δ is of p-power order, then $l(y) = \operatorname{Max}(0, k - \operatorname{ord}_\mathfrak{p}(1 - a^2))$. So there only remains to compute n'_k and $\operatorname{ord}_\mathfrak{p}(1 - a^2)$. For this purpose let $\eta_\nu \in k_\mathfrak{p}$ $(0 \le \nu \le r - 1)$ be a primitive $p^{r-\nu}$-th root of unity. Then

$$\operatorname{ord}_\mathfrak{p}(1 - \eta_\nu) = \operatorname{ord}_\mathfrak{p} p \cdot \operatorname{ord}_p(1 - \eta_\nu) = c\frac{p^r - p^{r-1}}{p^{r-\nu} - p^{r-\nu-1}} = cp^\nu.$$

This shows that

$$n'_k = (\mathcal{U}_\mathfrak{p} : E(1 + \mathfrak{p}^k)) = (\mathcal{U}_\mathfrak{p} : (1 + \mathfrak{p}^k))|E \cap (1 + \mathfrak{p}^k)|/e = \frac{q^k - q^{k-1}}{e_0 p^\nu}$$

for $cp^{\nu-1} < k \le cp^\nu$, and $n'_k = (q^k - q^{k-1})/e$ for $cp^{r-1} < k$.[17] Therefore, by using one index μ' instead of μ and ρ, and by denoting $R_{k\mu'}$ the element of P/Γ^0 corresponding to $\tau^{\mu'}_k = \tau^\mu_{k\rho}$, we arrive at the end of the proof. □

COROLLARY . *Let $\gamma \in \Gamma$ be such that $\gamma_\mathbf{R}$ is elliptic and that the centralizer Γ_γ is infinite. Let $A_l\{\gamma\}_\Gamma$ $(l \ge 1)$ be as defined by* (118). *Then*

$$A_l\{\gamma\}_\Gamma = \begin{cases} 0 & l < \deg\{\gamma\}_\Gamma, \\ d/e & l = \deg\{\gamma\}_\Gamma, \\ d(q^k - q^{k-1})/e \quad \cdots & l = \deg\{\gamma\}_\Gamma + k,\ k \ge 1; \\ & \deg\{\gamma\}_\Gamma > 0 \\ & \text{or if } = 0, \gamma \text{ is not of } p\text{-power order.} \\ dq^{cp^\nu}(q^l - q^{l-1})/e \quad \cdots & \deg\{\gamma\}_\Gamma = 0, \\ & \gamma \text{ is of order } p^{r-\nu}\ (0 \le \nu \le r - 1). \end{cases} \tag{129}$$

where P is the element of $\wp(\Gamma)$ defined by the fixed point of $\gamma_\mathbf{R}$, and $d = \deg P$, $e = e(P)$, $r = r(P)$, and c is as in Theorem 4.

REMARK . This generalizes Lemma 3 (§13), since in Lemma 3, Γ is assumed to be torsion-free; hence $e\{\delta\}_{\Gamma^0} = 1$.

PROOF. By the Corollary (ii) of Proposition 8, the set of all Γ^0-conjugacy classes contained in $\{\gamma\}_\Gamma$ is in one-to-one correspondence with the set P/Γ^0. Now our corollary is a direct consequence of Theorem 4. □

[17] Here, for $\nu = 0$, $cp^{\nu-1}$ should be replaced by 0.

§31. Q/Γ^0 for $Q \in Q_r(\Gamma)$. Now we are going to study in detail the elements Q of $Q(\Gamma)$. For convenience' sake, we shall first deal with $Q \in Q_r(\Gamma)$, i.e., $Q \in Q(\Gamma)$ for which $K_\mathfrak{p}/k_\mathfrak{p}$ is ramified. Thus, let $Q = Q_z \in Q_r(\Gamma)$, put $e(Q) = p^{r(Q)}$, and let Q/Γ^0 be, as before, the set of all Γ^0-equivalence classes of points on $\mathfrak{H}$ that are Γ-equivalent to z. We shall treat the two cases $p \neq 2$ and $p = 2$ separately;

The case $p \neq 2$.

THEOREM 5 ($p \neq 2$). *Let $p \neq 2$, $Q = Q_z \in Q_r(\Gamma)$, and put $e = e(Q)$, $r = r(Q)$, so that $|\Gamma_z| = e = p^r$. Put $\frac{1}{2}c(p^r - p^{r-1}) = \operatorname{ord}_\mathfrak{p} p$. Then c is an odd integer, and*

(i) *we can parametrize the elements of Q/Γ^0 in the following way;*

$$R_{k\mu} \qquad \left(k = 0, 1, 2, \cdots;\ 1 \leq \mu \leq \frac{q^k}{p^{\nu_k}}\right) \tag{130}$$

where ν_k is an integer defined by

$$\nu_k = \begin{cases} 0 & \cdots 0 \leq k \leq \frac{1}{2}(c-1) \\ \nu & \cdots \frac{1}{2}(cp^{\nu-1} - 1) < k \leq \frac{1}{2}(cp^\nu - 1) \quad (1 \leq \nu \leq r-1) \\ r & \cdots \frac{1}{2}(cp^{r-1} - 1) < k. \end{cases} \tag{131}$$

(ii) *Let $z_{k\mu} \in \mathfrak{H}$ represent $R_{k\mu}$, and let $\delta \in \Gamma_{z_{k\mu}}$ with $\delta \neq 1$. Let $p^{r-\nu}$ be the order of δ. Then*

$$l(\delta) = \operatorname{Max}(0, k - \frac{1}{2}(cp^\nu - 1)). \tag{132}$$

In particular, the order of the group $\Gamma_{z_{k\mu}} \cap \Gamma^0$ is given by $p^{r-\nu_k}$.

PROOF. Let ζ be a primitive p^r-th root of unity, and put $K_\mathfrak{p} = k_\mathfrak{p}(\zeta)$. Then $K_\mathfrak{p}$ is a ramified quadratic extension of $k_\mathfrak{p}$ (see §29). Since $k_\mathfrak{p} \cap \mathbf{Q}_p(\zeta) = \mathbf{Q}_p(\zeta + \zeta^{-1})$, we have $(\zeta - \zeta^{-1})^2 \in k_\mathfrak{p}$ and $K_\mathfrak{p} = k_\mathfrak{p}(\sqrt{(\zeta - \zeta^{-1})^2})$. Since $K_\mathfrak{p}/k_\mathfrak{p}$ is ramified and $\mathfrak{p} \nmid 2$,

$$\operatorname{ord}_\mathfrak{p}(\zeta - \zeta^{-1})^2 = \operatorname{ord}_\mathfrak{p} p \times \operatorname{ord}_p(\zeta - \zeta^{-1})^2 = \frac{2 \operatorname{ord}_\mathfrak{p} p}{p^r - p^{r-1}} = c$$

must be an odd integer. Now let π be a prime element of $k_\mathfrak{p}$ such that $K_\mathfrak{p} = k_\mathfrak{p}(\sqrt{\pi})$. Then $a + b\sqrt{\pi}$ ($a, b \in k_\mathfrak{p}$) is integral if and only if $a, b \in O_\mathfrak{p}$. Let γ be an element of Γ_z such that the eigenvalues of $\gamma_\mathfrak{p}$ are $\pm(\zeta, \zeta^{-1})$, and let $\delta = \gamma^n$ ($1 \leq n \leq p^r - 1$) be any element ($\neq 1$) of Γ_z. Let $\pm(\eta, \eta^{-1})$ be the eigenvalues of $\delta_\mathfrak{p}$, so that we may assume $\eta = \zeta^n$. Put $\eta = a + b\sqrt{\pi}$ ($a, b \in O_\mathfrak{p}$) and $t' = \begin{pmatrix} a & b \\ \pi b & a \end{pmatrix}$. Then there is some $x' \in GL_2(k_\mathfrak{p})$ such that $x'^{-1}\delta_\mathfrak{p}x' = t'$ for all $\delta \in \Gamma_z$ ($\delta \neq 1$). Since $K_\mathfrak{p}/k_\mathfrak{p}$ is ramified, $\operatorname{ord}_\mathfrak{p}(N_{K_\mathfrak{p}/k_\mathfrak{p}}K_\mathfrak{p}^\times) = \mathbf{Z}$; hence if $X_{t'}$ is the centralizer of t' in $GL_2(k_\mathfrak{p})$, we have $(\det X_{t'})\mathcal{U}_\mathfrak{p} = k_\mathfrak{p}^\times$; hence there is some $y \in X_{t'}$ such that $\det y \in \mathcal{U}_\mathfrak{p} \det x'$. Put $\varepsilon = \det(x'y^{-1}) \in \mathcal{U}_\mathfrak{p}$, $\omega = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix}$, and $x = x'y^{-1}\omega^{-1}$, so that $x \in G_\mathfrak{p}$ and $x^{-1}\gamma_\mathfrak{p}x = \omega t'\omega^{-1} = \begin{pmatrix} a & b\varepsilon \\ \pi b\varepsilon^{-1} & a \end{pmatrix}$. Call this element t and put $T = x^{-1}\Gamma_{z\mathfrak{p}}x = \{t\}$.

Now by the same argument as in the beginning of the proof of Theorem 4, we see immediately that it is enough to parametrize $V\backslash G_\mathfrak{p}/T$ and for each VgT, to compute $l(gtg^{-1})$. Let $x_{n\alpha}$ be as in (126). Then

$$y = x_{n\alpha}tx_{n\alpha}^{-1} = \begin{pmatrix} a + b\varepsilon^{-1}\alpha\pi^{n+1}, & \pi b\varepsilon(\pi^{-2n-1} - \alpha^2\varepsilon^{-2}) \\ b\varepsilon^{-1}\pi^{2n+1}, & a - b\varepsilon^{-1}\alpha\pi^{n+1} \end{pmatrix}. \tag{133}$$

Hence

$$l(y) = \begin{cases} \mathrm{Max}(0, 2l - \mathrm{ord}_\mathfrak{p} b) & \cdots n \geq 0, \mathrm{ord}_\mathfrak{p} b \geq -n; \\ \mathrm{Max}(0, 2l - 1 - \mathrm{ord}_\mathfrak{p} b) & \cdots \text{otherwise}; \end{cases} \tag{134}$$

where $l = l(x_{n\alpha})$. Here note that

$$\mathrm{ord}_\mathfrak{p} b = \mathrm{ord}_\mathfrak{p} \frac{\eta - \eta^{-1}}{2\sqrt{\pi}} = \frac{1}{2}(cp^\nu - 1),$$

where $p^{r-\nu}$ is the order of δ. First (134) shows that if $x_{n\alpha}$, $x_{n'\alpha'}$ belong to the same $V\backslash G_\mathfrak{p}/T$-coset and if $n \geq 0$ and $\mathrm{ord}_\mathfrak{p}\alpha \geq -n$ hold, then we have $n' = n \geq 0$ and $\mathrm{ord}_\mathfrak{p}\alpha' \geq -n'$. In fact if $x_{n\alpha}tx_{n\alpha}^{-1} \in V$ for all $t \in T$, then $x_{n'\alpha'} = x_{n\alpha}$; hence there is no problem. On the other hand, if $l(x_{n\alpha}tx_{n\alpha}^{-1}) > 0$ for some t, then $l(x_{n\alpha}tx_{n\alpha}^{-1}) = 2l(x_{n\alpha}) - \mathrm{ord}_\mathfrak{p} b$, and $l(x_{n'\alpha'}tx_{n'\alpha'}^{-1}) = l(x_{n\alpha}tx_{n\alpha}^{-1}) > 0$. But since $T \subset V$, we have $l(x_{n\alpha}) = l(x_{n'\alpha'})$; hence $l(x_{n'\alpha'}tx_{n'\alpha'}^{-1}) = 2l(x_{n'\alpha'}) - \mathrm{ord}_\mathfrak{p} b > 0$. But by (134) this implies $n' \geq 0$ and $\mathrm{ord}_\mathfrak{p}\alpha' \geq -n'$. But then $n' = l(x_{n'\alpha'}) = l(x_{n\alpha}) = n$; hence our assertion.

Now for each $l \geq 0$, let $R_{2l,\mu}$ $(1 \leq \mu \leq n_{2l})$ be all the distinct double cosets $Vx_{n\alpha}T$ with $n = l \geq 0$ and $\mathrm{ord}_\mathfrak{p}\alpha \geq -n$; and for each $l \geq 1$, let $R_{2l-1,\mu}$ $(1 \leq \mu \leq n_{2l-1})$ be all the distinct double cosets $Vx_{n'\alpha'}T$ with $l(x_{n'\alpha'}) = l$ that are not any one of $R_{2l,\mu}$. Then by (134) and by the above formula for $\mathrm{ord}_\mathfrak{p} b$, it follows immediately that $n_0 = 1$, $n_k = \frac{q^k}{p^{\nu k}}$ $(k > 0)$, and that (132) holds. □

The case $p = 2$. This case is more delicate than the case $p \neq 2$. We begin with the following lemma.

LEMMA 17. *Let $\mathfrak{p}|2$, and let $\tau \in \mathcal{U}_\mathfrak{p}$. Suppose that $K_\mathfrak{p} = k_\mathfrak{p}(\sqrt{\tau})$ is a ramified quadratic extension, and put $\kappa = \underset{u\in\mathcal{U}_\mathfrak{p}}{\mathrm{Max}}\{\mathrm{ord}_\mathfrak{p}(u^2 - \tau)\}$. Then*

(i) *κ is an odd integer satisfying $1 \leq \kappa \leq \mathrm{ord}_\mathfrak{p} 4 - 1$;*

(ii) *If $0 \leq k < \kappa$, there is some $u \in \mathcal{U}_\mathfrak{p}$ with $\mathrm{ord}_\mathfrak{p}(u^2 - \tau) = k$ if and only if k is even.*

(iii) *For any $u \in \mathcal{U}_\mathfrak{p}$,*

$$\mathrm{ord}_\mathfrak{p}(u^2 - \tau) = \mathrm{ord}_\mathfrak{P}(u - \sqrt{\tau}) = \mathrm{ord}_\mathfrak{P}(u + \sqrt{\tau})$$

holds, where $\mathfrak{P}$ is the prime factor of $\mathfrak{p}$ in $K_\mathfrak{p}$.

PROOF. *That $\kappa \leq \mathrm{ord}_\mathfrak{p} 4 - 1$:* Let κ' be the critical exponent for the quadratic residues in $k_\mathfrak{p}$; i.e., the largest exponent such that $u \in \mathcal{U}_\mathfrak{p}$ is a square in $\mathcal{U}_\mathfrak{p}$ if and only if it is a square mod $\mathfrak{p}^{\kappa'}$. Then, by the general estimation formula for κ', we have

$$\kappa' \leq \left[\frac{\mathrm{ord}_\mathfrak{p} p}{p-1}\right] + \mathrm{ord}_\mathfrak{p} p + 1 = \mathrm{ord}_\mathfrak{p} 4 + 1.$$

Hence if $u \in \mathcal{U}_\mathfrak{p}$ is a square mod $4\mathfrak{p}$, then u is a square in $\mathcal{U}_\mathfrak{p}$. But since τ is not a square we have $\kappa < \kappa' \leq \mathrm{ord}_\mathfrak{p} 4 + 1$; hence $\kappa \leq \mathrm{ord}_\mathfrak{p} 4$. Now we shall show that there is no $u \in \mathcal{U}_\mathfrak{p}$ with $u^2 \equiv \tau \pmod 4$, which would prove $\kappa \leq \mathrm{ord}_\mathfrak{p} 4 - 1$. Suppose on the contrary that we had $u^2 \equiv \tau \pmod 4$ for some u. Put $u^{-2}\tau = 1 + 4a$ ($a \in O_\mathfrak{p}$). Then $a \not\equiv b^2 + b \pmod \mathfrak{p}$ for any $b \in O_\mathfrak{p}$. In fact $a \equiv b^2 + b \pmod \mathfrak{p}$ would imply $\tau \equiv u^2(1 + 2b)^2 \pmod{4\mathfrak{p}}$, which contradicts $\kappa \leq \mathrm{ord}_\mathfrak{p} 4$. Consider the equation $X^2 + X = a$. Then this is irreducible mod $\mathfrak{p}$; hence it is also irreducible on $k_\mathfrak{p}$ and its splitting field $k_\mathfrak{p}(\sqrt{1 + 4a}) = k_\mathfrak{p}(\sqrt{\tau}) = K_\mathfrak{p}$ must be unramified, which contradicts our assumption. Therefore, $u^2 \not\equiv \tau \pmod 4$; hence $\kappa \leq \mathrm{ord}_\mathfrak{p} 4 - 1$.

The rest of (i) *and* (iii). Let $u \in \mathcal{U}_\mathfrak{p}$ and put $k = \mathrm{ord}_\mathfrak{p}(u^2 - \tau)$. Let $\mathfrak{P}$ be the prime factor of $\mathfrak{p}$ in $K_\mathfrak{p}$, so that $\mathfrak{p} = \mathfrak{P}^2$. Then

$$\mathrm{ord}_\mathfrak{p}(u^2 - \tau) = \frac{1}{2}\{\mathrm{ord}_\mathfrak{P}(u - \sqrt{\tau}) + \mathrm{ord}_\mathfrak{P}(u + \sqrt{\tau})\} = k;$$

hence either (a) $\mathrm{ord}_\mathfrak{P}(u - \sqrt{\tau}) \geq k$ or (b) $\mathrm{ord}_\mathfrak{P}(u + \sqrt{\tau}) \geq k$. But $\mathrm{ord}_\mathfrak{P}(2\sqrt{\tau}) = \mathrm{ord}_\mathfrak{P} 2 = \mathrm{ord}_\mathfrak{p} 4 > \kappa \geq k$; hence (a) implies (b) and conversely. Therefore, $\mathrm{ord}_\mathfrak{P}(u - \sqrt{\tau}) = \mathrm{ord}_\mathfrak{P}(u + \sqrt{\tau}) = k$. (This settles (iii)). Now assume that k is even, and put $u' = u + \pi^{k/2} \cdot \alpha$ ($\alpha \in O_\mathfrak{p}$). Then $\frac{u' - \sqrt{\tau}}{\pi^{k/2}} = \frac{u - \sqrt{\tau}}{\pi^{k/2}} + \alpha$; hence if we choose α so that $\alpha \equiv -\frac{u - \sqrt{\tau}}{\pi^{k/2}} \mod \mathfrak{P}$ (this is possible since $K_\mathfrak{p}$ and $k_\mathfrak{p}$ have the same residue class field), we have $u' \equiv \sqrt{\tau} \mod \mathfrak{P}^{k+1}$. But by $k \leq \mathrm{ord}_\mathfrak{p} 4 - 1$, we have $2\sqrt{\tau} \equiv 0 \pmod{\mathfrak{P}^{k+1}}$; hence $u'^2 - \tau \equiv 0 \pmod{\mathfrak{p}^{k+1}}$; hence $\mathrm{ord}_\mathfrak{p}(u'^2 - \tau) \geq k + 1$. This shows that if $k = \mathrm{ord}_\mathfrak{p}(u^2 - \tau)$ is even, then $k < \kappa$. Therefore κ must be odd. In particular, $1 \leq \kappa$.

(ii) Take $u_0 \in u_\mathfrak{p}$ such that $\mathrm{ord}_\mathfrak{p}(u_0^2 - \tau) = \kappa$. Let $u \in \mathcal{U}_\mathfrak{p}$ with $k = \mathrm{ord}_\mathfrak{p}(u^2 - \tau) < \kappa$. Then

$$k = \mathrm{ord}_\mathfrak{p}(u^2 - u_0^2) = \mathrm{ord}_\mathfrak{p}(u - u_0) + \mathrm{ord}_\mathfrak{p}(u + u_0).$$

But since (say) $\mathrm{ord}_\mathfrak{p}(u - u_0) \leq \frac{k}{2} < \mathrm{ord}_\mathfrak{p} 2 = \mathrm{ord}_\mathfrak{p}(2u_0)$, we have $\mathrm{ord}_\mathfrak{p}(u + u_0) = \mathrm{ord}_\mathfrak{p}(u - u_0)$; hence $k = 2\,\mathrm{ord}_\mathfrak{p}(u - u_0) \equiv 0 \pmod 2$. Conversely, let k be even with $0 \leq k < \kappa$, and take $u \in \mathcal{U}_\mathfrak{p}$ such that $\mathrm{ord}_\mathfrak{p}(u - u_0) = \frac{k}{2}$. Then it follows immediately that $\mathrm{ord}_\mathfrak{p}(u^2 - \tau) = k$. □

Now let $\mathfrak{p}|2$, let $Q = Q_z \in Q_r(\Gamma)$, and let $K_\mathfrak{p}$ be the corresponding ramified quadratic extension of $k_\mathfrak{p}$. Let ξ be an element of Γ_z of order 2. Then $K_\mathfrak{p}$ is generated over $k_\mathfrak{p}$ by the eigenvalues of $\xi_\mathfrak{p}$; hence $K_\mathfrak{p} = k_\mathfrak{p}(\sqrt{-1})$. By the above lemma this shows that if $Q_r(\Gamma)$ is non-empty, the number $\kappa = \mathrm{Max}_{u \in \mathcal{U}_\mathfrak{p}} \mathrm{ord}_\mathfrak{p}(u^2 + 1)$ is a finite odd integer satisfying $\kappa \leq \mathrm{ord}_\mathfrak{p} 4 - 1$.

Now we shall prove the following Theorem 5 ($p = 2$);

THEOREM 5 ($p = 2$). *Let $p = 2$, $Q = Q_z \in Q_r(\Gamma)$, and put $e = e(Q)$, $r = r(Q)$, so that $|\Gamma_z| = e = 2^r$. Put $2^{r-2}c = \mathrm{ord}_\mathfrak{p} 2$, $\kappa = \mathrm{Max}_{u \in \mathcal{U}_\mathfrak{p}} \mathrm{ord}_\mathfrak{p}(u^2 + 1)$. Then c is an even integer, κ is odd, and* $\mathrm{ord}_\mathfrak{p} 4 - c + 1 \leq \kappa \leq \mathrm{ord}_\mathfrak{p} 4 - 1$. *Moreover,*

(i) *we can parametrize the elements of Q/Γ^0 in the following way;*

$$R_{k\mu} \qquad (k = 0, 1, 2, \cdots;\ 1 \leq \mu \leq \frac{q^k}{2^{\nu_k}}), \tag{135}$$

where ν_k is an integer defined by

$$(136)\qquad \nu_k = \begin{cases} 0 & \cdots 0 \le k \le (\frac{\kappa}{2} - \mathrm{ord}_\mathfrak{p} 2) + \frac{1}{2}(c-1), \\ \nu & \cdots (\frac{\kappa}{2} - \mathrm{ord}_\mathfrak{p} 2) + \frac{1}{2}(c2^{\nu-1} - 1) < k \le (\frac{\kappa}{2} - \mathrm{ord}_\mathfrak{p} 2) + \frac{1}{2}(c2^{\nu} - 1), \\ r & \cdots \frac{\kappa-1}{2} < k. \end{cases}$$

(ii) *Let $z_{k\mu} \in \mathfrak{H}$ represent $R_{k\mu}$, and let $\delta \in \Gamma_{z_{k\mu}}$ with $\delta \neq 1$. Let $2^{r-\nu}$ be the order of δ. Then*

$$(137)\qquad l(\delta) = \mathrm{Max}(0, \kappa - \frac{1}{2}(c2^{\nu} - 1) + \mathrm{ord}_\mathfrak{p} 2 - \frac{\kappa}{2}).$$

In particular, the order of the group $\Gamma_{z_{k\mu}} \cap \Gamma^0$ is given by $2^{r-\nu_k}$.

Proof. Let $K_\mathfrak{p}$ be the corresponding ramified extension of $k_\mathfrak{p}$. Then $K_\mathfrak{p} = k_\mathfrak{p}(\sqrt{-1})$, and $K_\mathfrak{p}$ contains the group E of 2^{r+1}-th roots of unity. This shows that c is an even integer. That κ is odd and $\kappa \le \mathrm{ord}_\mathfrak{p} 4 - 1$ is a direct consequence of Lemma 17. To prove $\kappa \ge \mathrm{ord}_\mathfrak{p} 4 - c + 1 = (2^{r-1} - 1)c + 1$, let $\zeta \in E$ be a primitive 2^{r+1}-th root of unity and put $\zeta = a_0 + b_0\sqrt{-1}$ $(a_0, b_0 \in k_\mathfrak{p})$. If $r = 1$, the assertion is trivial; so assume $r > 1$. Then

$$\mathrm{ord}_\mathfrak{p} b_0 = \mathrm{ord}_\mathfrak{p}(\zeta - \zeta^{-1}) - \mathrm{ord}_\mathfrak{p} 2 = -(2^{r-1} - 1)\frac{c}{2} < 0;$$

hence $\mathrm{ord}_\mathfrak{p} a_0 = \mathrm{ord}_\mathfrak{p} b_0$, and $\sqrt{-1} \equiv -\frac{a_0}{b_0} \pmod{\mathfrak{p}^{(2^{r-1}-1)\frac{c}{2}}}$. Therefore, by Lemma 17 (iii), $\kappa \ge (2^{r-1} - 1)c$. But since κ is odd, we obtain $\kappa \ge (2^{r-1} - 1)c + 1$; hence our assumption on κ.

Now there is an onto isomorphism $\Gamma_z \to E/\pm 1$ such that if $\delta \mapsto \pm\eta$, then $\pm\{\eta, \eta^{-1}\}$ are the eigenvalues of $\delta_\mathfrak{p}$. For each $\delta \in \Gamma_z$, put $\eta = a + b\sqrt{-1}$ $(a, b \in k_\mathfrak{p})$ and $t' = \pm\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G_\mathfrak{p}$. Then as in the case of $\mathfrak{p} \nmid 2$ we see easily that there exist some $\varepsilon \in \mathcal{U}_\mathfrak{p}$ and $x \in G_\mathfrak{p}$ such that $t = x^{-1}\delta_\mathfrak{p} x = \begin{pmatrix} a & b\varepsilon \\ -b\varepsilon^{-1} & a \end{pmatrix}$ for all $\delta \in \Gamma_z$. Put $T = x^{-1}\Gamma_{z\mathfrak{p}}x = \{t\}$. Then our problem is reduced to parametrizing $V\backslash G_\mathfrak{p}/T$, and for each VgT computing $l(gtg^{-1})$. Now let $x_{n\alpha}$ be as in (126). Then

$$(138)\qquad y = x_{n\alpha}tx_{n\alpha}^{-1} = \begin{pmatrix} a - \varepsilon^{-1}b\alpha\pi^{-n}, & \varepsilon b\pi^{-2n}(1 + \varepsilon^{-2}\alpha^2\pi^{2n}) \\ -\varepsilon^{-1}b\pi^{2n}, & a + \varepsilon^{-1}b\alpha\pi^{n} \end{pmatrix},$$

and $\mathrm{ord}_\mathfrak{p} b = 2^{\nu-1}c - \mathrm{ord}_\mathfrak{p} 2$, where $2^{r-\nu}$ is the order of δ. Put $l = l(x_{n\alpha})$, and $m = m(x_{n\alpha}) = 0$ (if $\mathrm{ord}_\mathfrak{p}\alpha \neq -n$), $= \mathrm{Min}(4l, \mathrm{ord}_\mathfrak{p}(u^2 + 1))$ (if $\mathrm{ord}_\mathfrak{p}\alpha = -n$ and $u = \varepsilon^{-1}\alpha\pi^n$).[18] Then by (138), we obtain directly

$$(139)\qquad l(y) = \mathrm{Max}(0, 2l - m - \mathrm{ord}_\mathfrak{p} b).$$

Moreover, by the definition of κ, we have $0 \le m \le \mathrm{Min}(4l, \kappa)$, and by Lemma 17 (ii), m must be even unless $m = \kappa$.

Now for each integer k, let n'_k be the number of $x_{n\alpha}$ such that $2l - m + \frac{\kappa-1}{2} = k$. Then by a straightforward computation, we obtain $n'_k = q^k$ $(k \ge 0)$, $= 0$ $(k < 0)$. Moreover if $x_{n\alpha}$, $x_{n'\alpha'}$ belong to the same $V\backslash G_\mathfrak{p}/T$-coset, then $k(x_{n\alpha}) = k(x_{n'\alpha'})$. In fact, if $l(x_{n\alpha}tx_{n\alpha}^{-1}) =$

[18] In this case, $n > 0$ and $l = n$.

0 for all $t \in T$, then $x_{n'\alpha'} = x_{n\alpha}$; hence there is no problem. If, on the other hand, $l(x_{n\alpha}tx_{n\alpha}^{-1}) > 0$ for some t, then by (139),

$$l(x_{n\alpha}tx_{n\alpha}^{-1}) = k(x_{n\alpha}) - \frac{\kappa - 1}{2} - \mathrm{ord}_{\mathfrak{p}}\, b > 0.$$

But $l(x_{n'\alpha'}tx_{n'\alpha'}^{-1}) = l(x_{n\alpha}tx_{n\alpha}^{-1}) > 0$; hence

$$l(x_{n'\alpha'}tx_{n'\alpha'}^{-1}) = k(x_{n'\alpha'}) - \frac{\kappa - 1}{2} - \mathrm{ord}_{\mathfrak{p}}\, b;$$

hence $k(x_{n\alpha}) = k(x_{n'\alpha'})$. So, let n_k be the number of distinct $Vx_{n\alpha}T$ such that $k(x_{n\alpha}) = k$. Then since the number of $t \in T$ such that $Vx_{n\alpha}t = Vx_{n\alpha}$ is $2^{t-\nu_k}$ by (139), we obtain $n_k = \frac{n'_k}{2^{\nu_k}} = \frac{q^k}{2^{\nu_k}}$ $(k \geq 0)$. Therefore, by putting $R_{k\mu}$ $(1 \leq \mu \leq n_k)$ all the double cosets $Vx_{n\alpha}T$ such that $k(x_{n\alpha}) = k$, we arrive at the end of the proof. □

By Theorem 5, we obtain immediately:

COROLLARY . *Let $Q = Q_z \in Q_r(\Gamma)$, put $|\Gamma_z| = p^r$, and let $\gamma \in \Gamma_z$ with $\gamma \neq 1$. Then*

$$A_l\{\gamma\}_\Gamma = \begin{cases} \frac{1}{p^r} q^{l+\frac{1}{2}(cp^\nu - 1)} & \cdots p \neq 2, \\ \frac{1}{2^r} q^{l+\frac{1}{2}(c2^\nu - 1)+\frac{\kappa}{2}-\mathrm{ord}_{\mathfrak{p}}2} & \cdots p = 2, \end{cases} \tag{140}$$

where $p^{r-\nu}$ is the order of γ, $c = \frac{2}{p^r - p^{r-1}}\,\mathrm{ord}_{\mathfrak{p}}\, p$, and κ is as in Theorem 5 $(p = 2)$.

§32. Q/Γ^0 for $Q \in Q_u(\Gamma)$.

THEOREM 6. *We can decompose the set $Q_u(\Gamma)$ into the disjoint union*

$$Q_u(\Gamma) = Q_u^+(\Gamma) \cup Q_u^-(\Gamma) \qquad (\textit{disjoint}) \tag{141}$$

in a unique way so that the following assertions (i) ~ (ii) *are satisfied.*

(i) *For each $Q \in Q_u(\Gamma)$, put $e(Q) = e = e_0 p^r$ with $e_0 \not\equiv 0 \pmod p$. Put $\mathrm{ord}_{\mathfrak{p}}\, p = c(p^r - p^{r-1})$, so that c is a positive integer and $c \equiv 0 \pmod 2$ if $\mathfrak{p}|2$.*[19] *Then we can parametrize the elements of Q/Γ^0 as*

$$R_{k\mu} \quad \begin{cases} k = 0, 2, 4, \cdots, & \text{if } Q \in Q_u^+(\Gamma), \\ \quad = 1, 3, 5, \cdots, & \text{if } Q \in Q_u^-(\Gamma); \\ 1 \leq \mu \leq \begin{cases} 1 & \cdots k = 0 \\ \frac{q^k + q^{k-1}}{e_0 p^{\nu_k}} & \cdots k > 0; \end{cases} \end{cases} \tag{142}$$

where ν_k is an integer defined by[20]

$$\nu_k = \begin{cases} 0 & \cdots 0 < k \leq c, \\ \nu & \cdots cp^{\nu-1} < k \leq cp^\nu \quad (1 \leq \nu \leq r-1) \\ r & \cdots cp^{r-1} < k. \end{cases} \tag{143}$$

[19] Since if $\mathfrak{p}|2$, then $K_{\mathfrak{p}}$ contains primitive 2^{r+1}-th root of unity.

[20] Thus if $r = 0$, then $\nu_k = 0$ for all $k > 0$.

(ii) *Let $z_{k\mu} \in \mathfrak{H}$ represent $R_{k\mu}$ and let $\delta \in \Gamma_{z_{k\mu}}$ with $\delta \neq 1$. Then*

$$(144) \qquad l(\delta) = \begin{cases} k & \cdots \text{if the order of } \delta \text{ is not a power of } p, \\ \mathrm{Max}(0, k - cp^{\nu}) & \cdots \text{if the order of } \delta \text{ is } p^{r-\nu} \quad (0 \leq \nu \leq r-1). \end{cases}$$

In particular, the order of the group $\Gamma_{z_{k\mu}} \cap \Gamma^0$ is given by e (if $k = 0$), and by $p^{r-\nu_k}$ (if $k > 0$).

PROOF. Put $K_{\mathfrak{p}} = k_{\mathfrak{p}}(\sqrt{\tau})$ $(\tau \in \mathcal{U}_{\mathfrak{p}})$. Then since $K_{\mathfrak{p}}/k_{\mathfrak{p}}$ is unramified, the basis $1, \sqrt{\tau}$ of $K_{\mathfrak{p}}/k_{\mathfrak{p}}$ has the following properties;

(i) if $\mathfrak{p} \nmid 2$, $a + b\sqrt{\tau}$ $(a, b \in k_{\mathfrak{p}})$ is integral if and only if a, b are so, and τ is a quadratic non-residue mod $\mathfrak{p}$;

(ii) if $\mathfrak{p}|2$, τ is a quadratic residue mod 4 but non-residue mod $4\mathfrak{p}$ (see the proof of Lemma 17) [21]; hence we may assume $\tau \equiv 1 \pmod 4$. Then $\frac{1}{2}(a + b\sqrt{\tau})$ $(a, b \in k_{\mathfrak{p}})$ is integral if and only if a, b are integral and $a \equiv b \pmod 2$.

Now let E be the group of all $2e$-th roots of 1 contained in $K_{\mathfrak{p}}$. Then there is an onto isomorphism $\Gamma_z \to E/\pm 1$ such that if $\delta \mapsto \pm\eta$, then $\pm\{\eta, \eta^{-1}\}$ are the eigenvalues of $\delta_{\mathfrak{p}}$. For each $\delta \in \Gamma_z$ put $\eta = a + b\sqrt{\tau}$ $(a, b \in k_{\mathfrak{p}})$ and $t = \begin{pmatrix} a & b \\ b\tau & a \end{pmatrix} \in G_{\mathfrak{p}}$. Then there is some $x' \in PL_2(k_{\mathfrak{p}})$ such that $x'^{-1}\delta_{\mathfrak{p}}x' = t$ (for all $\delta \in \Gamma_z$). Put $\omega = \begin{pmatrix} 0 & \pi \\ 1 & 0 \end{pmatrix}$ so that

$$PL_2(k_{\mathfrak{p}}) = G_{\mathfrak{p}} \cdot PL_2(O_{\mathfrak{p}}) \cup G_{\mathfrak{p}}\omega PL_2(O_{\mathfrak{p}}).$$

Since the centralizer X_t of t in $PL_2(k_{\mathfrak{p}})$ is identified with $K_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times}$ in a natural manner, and since $K_{\mathfrak{p}}/k_{\mathfrak{p}}$ is unramified and hence $N_{K_{\mathfrak{p}}/k_{\mathfrak{p}}}K_{\mathfrak{p}}^{\times} \supset \mathcal{U}_{\mathfrak{p}}$, we have $\det X_t \supset \det PL_2(O_{\mathfrak{p}})$; hence we can replace x' by either $x \in G_{\mathfrak{p}}$ or by $x\omega$ $(x \in G_{\mathfrak{p}})$. Therefore, either of the following two cases may happen:

$$(145) \qquad \begin{cases} \text{(Case 1)} & \exists x \in G_{\mathfrak{p}};\ x^{-1}\delta_{\mathfrak{p}}x = \begin{pmatrix} a & b \\ b\tau & a \end{pmatrix} = t & (\forall \delta \in \Gamma_z), \\ \text{(Case 2)} & \exists x \in G_{\mathfrak{p}};\ x^{-1}\delta_{\mathfrak{p}}x = \begin{pmatrix} a & b\tau\pi \\ b\pi^{-1} & a \end{pmatrix} \underset{\text{put}}{=} t' & (\forall \delta \in \Gamma_z). \end{cases}$$

However, since $\det X_t = N_{K_{\mathfrak{p}}/k_{\mathfrak{p}}}K_{\mathfrak{p}}^{\times}$ does not contain prime elements of $k_{\mathfrak{p}}$, only one of the two cases can happen.

Case 1. Put $T = x^{-1}\Gamma_{z\mathfrak{p}}x = \{t\}$. Then our problem is to parametrize $V\backslash G_{\mathfrak{p}}/T$, and for each VgT, to compute $l(gtg^{-1})$. Let $x_{n\alpha}$ be as in (126). Then,

$$(146) \qquad y = x_{n\alpha}tx_{n\alpha}^{-1} = \begin{pmatrix} a + b\tau\alpha\pi^n, & b\pi^{-2n}(1 - \alpha^2\pi^{2n}\tau) \\ b\tau\pi^{2n}, & a - b\tau\alpha\pi^n \end{pmatrix}.$$

[21] That τ is a quadratic residue mod 4 follows from the argument used in the proof of Lemma 17 combined with the fact that the unramified quadratic extension is unique.

Put $l = l(x_{n\alpha})$ and now assume that $t \neq 1$. Then we can check by a direct computation [22] that

$$l(y) = \mathrm{Max}(0,\ 2l - 2m - \mathrm{ord}_{\mathfrak{p}} b,\ 2l - \mathrm{ord}_{\mathfrak{p}} 4 - \mathrm{ord}_{\mathfrak{p}} b), \tag{147}$$

where $m = m(Vx_{n\alpha})$ is defined as follows:

(i) if $\mathrm{ord}_{\mathfrak{p}} \alpha \neq -n$, put $m = 0$;

(ii) if $\mathrm{ord}_{\mathfrak{p}} \alpha = -n$ (then $n > 0$, $l = n$), put $u = \alpha\pi^n$ (so that u runs over $\mathcal{U}_{\mathfrak{p}} \mod \mathfrak{p}^{2l}$) and put $m = \mathrm{ord}_{\mathfrak{p}}(u - 1)$.

Here we put $m = 2l$ when $u \equiv 1 \pmod{\mathfrak{p}^{2l}}$. (Note, in computing out (147), that we have $\mathrm{ord}_{\mathfrak{p}}(1 - u^2\tau) = 2m$ if $m \leq \mathrm{ord}_{\mathfrak{p}} 2$, and $= \mathrm{ord}_{\mathfrak{p}} 4$ if $m \geq \mathrm{ord}_{\mathfrak{p}} 2$.) Moreover, we have

$$\mathrm{ord}_{\mathfrak{p}}(2b) = \begin{cases} \mathrm{ord}_{\mathfrak{p}}(\eta - \eta^{-1}) = 0 & \text{(if the order of } \delta \text{ is not a power of } p), \\ cp^{\nu} & \text{(if the order of } \delta \text{ is } p^{r-\nu}, \text{ with } 0 \leq \nu \leq r-1). \end{cases}$$

Now put

$$k' = \mathrm{Max}(l - m, l - \mathrm{ord}_{\mathfrak{p}} 2), \qquad k = 2k' + \mathrm{ord}_{\mathfrak{p}} 2. \tag{148}$$

Then since $2k' \geq (l - m) + (l - \mathrm{ord}_{\mathfrak{p}} 2) \geq -\mathrm{ord}_{\mathfrak{p}} 2$, we have $k \geq 0$ and $k \equiv \mathrm{ord}_{\mathfrak{p}} 2 \pmod 2$. By (147), we have

$$\begin{aligned} l(y) &= \mathrm{Max}(0, k - \mathrm{ord}_{\mathfrak{p}}(2b)) \\ &= \begin{cases} k & \cdots \text{if the order of } \delta \text{ is not a power of } p, \\ \mathrm{Max}(0, k - cp^{\nu}) & \cdots \text{if the order of } \delta \text{ is } p^{r-\nu} \ (0 \leq \nu \leq r-1). \end{cases} \end{aligned} \tag{149}$$

Now for a given integer $k \geq 0$ with $k \equiv \mathrm{ord}_{\mathfrak{p}} 2 \pmod 2$, let n'_k be the number of distinct $Vx_{n\alpha}$ for which (148) (and hence also (149)) holds. Then by a straightforward computation we obtain $n'_0 = 1$ or 0 according to $\mathrm{ord}_{\mathfrak{p}} 2 \equiv 0$ or $\equiv 1 \pmod 2$, and $n'_k = q^k + q^{k-1}$ ($k > 0$, $k \equiv \mathrm{ord}_{\mathfrak{p}} 2 \pmod 2$). Now we can show exactly in the same manner as in the proof of Theorem 5 ($p = 2$) that k, a function of $x_{n\alpha}$, depends only on the double coset $Vx_{n\alpha}T$. So, let n_k be the number of distinct $Vx_{n\alpha}T$ for which (148) holds. Then since $Vx_{n\alpha}t = Vx_{n\alpha}$ if and only if $l(y) = 0$, we can obtain easily by (149) that $n_0 = n'_0$, $n_k = \frac{n'_k}{e_0 p^{\nu_k}}$ ($k > 0$), where ν_k is given by (143). Thus if we denote by

$$R_{k\mu} \quad \left(k \geq 0,\ k \equiv \mathrm{ord}_{\mathfrak{p}} 2 \pmod 2; \quad 1 \leq \mu \leq \begin{cases} 1 & (k = 0) \\ \frac{q^k + q^{k-1}}{e_0 p^{\nu_k}} & (k > 0) \end{cases} \right)$$

all the distinct $Vx_{n\alpha}T$ with $k(x_{n\alpha}) = k$, then we have (144) for such $R_{k\mu}$.

Case 2. This case is treated exactly in the same manner, and the result is as follows. Put $y' = x_{n\alpha} t' x_{n\alpha}^{-1}$. Then, for $t' \neq 1$, we have

$$l(y') = \mathrm{Max}(0, 2l - 2m' - 1 - \mathrm{ord}_{\mathfrak{p}} b, 2l - \mathrm{ord}_{\mathfrak{p}} 4 - 1 - \mathrm{ord}_{\mathfrak{p}} b)$$

where m' is given as follows:

(i) if $\mathrm{ord}_{\mathfrak{p}} \alpha + n - 1 < 0$, put $m' = -1$;

(ii) if $\mathrm{ord}_{\mathfrak{p}} \alpha + n - 1 > 0$, put $m' = 0$;

[22] Note that $a + b\tau\alpha\pi^n = \eta + b\tau(\alpha\pi^n - 1)$; hence $\mathrm{ord}_{\mathfrak{p}}(a + b\tau\alpha\pi^n)$ is either ≥ 0 or $= \mathrm{ord}_{\mathfrak{p}}\{b(\alpha\pi^n - 1)\}$.

(iii) and if $\mathrm{ord}_{\mathfrak{p}}\alpha + n - 1 = 0$ (then $n > 0$, $l = n$), then put $u = \alpha\pi^{n-1}$ (so that u runs over $\mathcal{U}_{\mathfrak{p}} \mod \mathfrak{p}^{2l-1}$) and put $m' = \mathrm{ord}_{\mathfrak{p}}(u-1)$.

Here we put $m = 2l - 1$ when $u \equiv 1 \mod \mathfrak{p}^{2l-1}$). Put

$$k' = \mathrm{Max}(l - m', l - \mathrm{ord}_{\mathfrak{p}} 2), \qquad k = 2k' + \mathrm{ord}_{\mathfrak{p}} 2 - 1 \geq 0,$$

so that $l(y') = \mathrm{Max}(0, k - \mathrm{ord}_{\mathfrak{p}}(2b))$. Then k depends only on $Vx_{n\alpha}T'$ (where $T' = \{t'\}$), and for each $k \geq 0$ with $k \equiv \mathrm{ord}_{\mathfrak{p}} 2 - 1 \pmod 2$, the number n_k of distinct $Vx_{n\alpha}T'$ such that $k(Vx_{n\alpha}T') = k$ is given by

$$n_0 = 1 \ (\text{if } \mathrm{ord}_{\mathfrak{p}} 2 \equiv 1 \pmod 2), \quad n_k = \frac{q^k + q^{k-1}}{e_0 p^{\nu_k}} \ (k > 0,\ k \equiv \mathrm{ord}_{\mathfrak{p}} 2 - 1 \pmod 2).$$

Thus denoting by

$$R_{k\mu} \quad \left(k \geq 0,\ k \equiv \mathrm{ord}_{\mathfrak{p}} 2 - 1 \pmod 2;\quad 1 \leq \mu \leq \begin{cases} 1 & (k=0) \\ \frac{q^k+q^{k-1}}{e_0 p^{\nu_k}} & (k>0) \end{cases}\right)$$

all the distinct $Vx_{n\alpha}T'$ with $k(x_{n\alpha}) = k$, we have (144) for such $R_{k\mu}$.

Now let $Q_u^+(\Gamma)$ be the set of all $Q \in Q_u(\Gamma)$ which belong to Case 1 (resp. Case 2) according to $\mathrm{ord}_{\mathfrak{p}} 2 \equiv 0 \pmod 2$ (resp. $\equiv 1 \pmod 2$), and let $Q_u^-(\Gamma)$ be that of all Q which belong to Case 2 (resp. Case 1) according to $\mathrm{ord}_{\mathfrak{p}} 2 \equiv 0 \pmod 2$ (resp. $\equiv 1 \pmod 2$).

(150)

	Case 1	Case 2
$\mathrm{ord}_{\mathfrak{p}} 2 \equiv 0 \pmod 2$	$Q_u^+(\Gamma)$	$Q_u^-(\Gamma)$
$\mathrm{ord}_{\mathfrak{p}} 2 \equiv 1 \pmod 2$	$Q_u^-(\Gamma)$	$Q_u^+(\Gamma)$

Then by what we have shown, Theorem 6 (i) (ii) holds for this definition of $Q_u^+(\Gamma)$ and $Q_u^-(\Gamma)$. On the other hand, it is clear that the decomposition (141) is characterized by the equality (144) (even if $e_0 = 1$). □

COROLLARY . *Let $Q = Q_z \in Q_u(\Gamma)$ and let $\gamma \in \Gamma_z$ with $\gamma \neq 1$. Put $e(Q) = e = e_0 p^r$ with $e_0 \not\equiv 0 \pmod p$, and let c be as in Theorem 6. Then*

(i) *if $Q \in Q_u^+(\Gamma)$,*

(151)
$$A_l\{\gamma\}_\Gamma = \begin{cases} \frac{1}{e}(q^l + q^{l-1}) & \cdots \text{the order of } \gamma \text{ is not a power of } p;\ l: \text{even}, \\ 0 & \cdots \text{the order of } \gamma \text{ is not a power of } p;\ l: \text{odd}, \\ \frac{1}{e}q^{cp^\nu}(q^l + q^{l-1}) & \cdots \text{the order of } \gamma \text{ is } p^{r-\nu};\ cp^\nu \equiv l \pmod 2, \\ 0 & \cdots \text{the order of } \gamma \text{ is } p^{r-\nu};\ cp^\nu \not\equiv l \pmod 2. \end{cases}$$

(ii) *if* $Q \in Q_u^-(\Gamma)$,

$$A_l\{\gamma\}_\Gamma = \begin{cases} 0 \\ \frac{1}{e}(q^l + q^{l-1}) \\ 0 \\ \frac{1}{e}q^{cp^\nu}(q^l + q^{l-1}) \end{cases} ; \begin{array}{l} \textit{the same condition} \\ \textit{(same order) as above.} \end{array} \tag{152}$$

§33. The results of §32 suggest us to consider not only the group Γ^0 and the length $l(\gamma)$ but also the following group $\Gamma^{0\prime}$ and the length $l'(\gamma)$. Fix any element $\omega \in V\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}V$, and put

$$\begin{cases} V' = \omega^{-1}V\omega, \quad T_{\mathfrak{p}}^{l\prime} = V'\begin{pmatrix} \pi^l & 0 \\ 0 & \pi^{-l} \end{pmatrix}V' = \omega^{-1}T_{\mathfrak{p}}^l\omega, \\ \Gamma^{0\prime} = \Gamma \cap (G_{\mathbf{R}} \times V'), \quad T^{l\prime} = \Gamma \cap (G_{\mathbf{R}} \times T_{\mathfrak{p}}^{l\prime}) \quad (l \geq 0). \end{cases} \tag{153}$$

Further, put $l'(x) = l$ for $x \in T_{\mathfrak{p}}^{l\prime}$, and $l'(\gamma) = l$ for $\gamma \in T^{l\prime}$. Note here that for any $x \in PL_2(k_{\mathfrak{p}})$, $x^{-1}Vx$ is conjugate in $G_{\mathfrak{p}}$ to either V or V'; hence up to Γ-conjugacy, it is enough to consider only the two functions $l(\gamma)$ and $l'(\gamma)$.

THEOREM 4′. *Theorem 4 is also valid if we replace* Γ^0 *by* $\Gamma^{0\prime}$ *and* $l(\delta)$ *by* $l'(\delta)$.

THEOREM 5′. *Theorem 5 is also valid if we replace* Γ^0 *by* $\Gamma^{0\prime}$ *and* $l(\delta)$ *by* $l'(\delta)$.

PROOF. They are reduced to the same problems (as Theorem 4 resp. 5) at the first steps of imitating the proofs of Theorem 4 resp. 5. Namely, they are also reduced to the problems of parametrizing $V\backslash G_{\mathfrak{p}}/T$ and for each VgT, computing $l(gtg^{-1})$ (*not* $l'(gtg^{-1})$). The reason is that if X_T is the centralizer of T in $PL_2(k_{\mathfrak{p}})$, then X_T contains an element ξ for which $\mathrm{ord}_{\mathfrak{p}}(\det \xi) \equiv 1 \pmod 2$. (This is in fact the case, since in the case of Theorem 4, X_T is the diagonal subgroup of $PL_2(k_{\mathfrak{p}})$, and in the case of Theorem 5, X_T is identified with $K_{\mathfrak{p}}^\times/k_{\mathfrak{p}}^\times$, but *since* $K_{\mathfrak{p}}/k_{\mathfrak{p}}$ *is ramified,* there is some $\xi \in K_{\mathfrak{p}}$ such that $\mathrm{ord}_{\mathfrak{p}} N_{K_{\mathfrak{p}}/k_{\mathfrak{p}}}(\xi) \equiv 1 \pmod 2$.) □

On the other hand, as for Theorem 6, the circumstance is quite different. In fact, we obtain an "opposite" result, as follows.

THEOREM 6′. *Theorem 6 is also valid if we replace* Γ^0 *by* $\Gamma^{0\prime}$, $l(\delta)$ *by* $l'(\delta)$ *and if we invert* $Q_u^+(\Gamma)$ *and* $Q_u^-(\Gamma)$.

PROOF. In the proof of Theorem 6, the two cases of (145) appear inverted for $l'(\delta)$. □

§34. The signatures of $\Gamma_{\mathbf{R}}^0$ and $\Gamma_{\mathbf{R}}^{0\prime}$. Let Δ be any fuchsian group, let g be the genus of $\mathfrak{H}/\Delta$, let s be the number of cusps of Δ (counted up to Δ-equivalence), and let $e_1, \cdots, e_t$

be the orders of the stabilizers of elliptic points of Δ (counted up to Δ-equivalence). In this situation, the data

$$\{g; \underbrace{\infty, \cdots, \infty}_{s}; e_1, \cdots, e_t\} \tag{154}$$

is called *the signature of* Δ. It is well-known that

$$v(\Delta) \underset{\text{def.}}{=} \frac{1}{2\pi} \int_{\Delta \backslash \mathfrak{H}} \frac{dxdy}{y^2} = 2g - 2 + s + \sum_{i=1}^{t} (1 - \frac{1}{e_i}) > 0, \tag{155}$$

where $x + iy \in \mathfrak{H}$ $(x, y \in \mathbf{R})$.

Now let us consider the signatures of $\Gamma_{\mathbf{R}}^0$ and $\Gamma_{\mathbf{R}}^{0\prime}$. First, since $(V : V \cap V') = (V' : V \cap V') = q + 1$, we have $(\Gamma_{\mathbf{R}}^0 : \Gamma_{\mathbf{R}}^0 \cap \Gamma_{\mathbf{R}}^{0\prime}) = (\Gamma_{\mathbf{R}}^{0\prime} : \Gamma_{\mathbf{R}}^0 \cap \Gamma_{\mathbf{R}}^{0\prime})$; hence

$$v(\Gamma_{\mathbf{R}}^0) = v(\Gamma_{\mathbf{R}}^{0\prime}). \tag{156}$$

Let

$$\{g; \underbrace{\infty, \cdots, \infty}_{s}; e_1, \cdots, e_a; e_{11}, \cdots, e_{1b}; e_{21}, \cdots, e_{2c}\} \tag{157}$$

be the signature of $\Gamma_{\mathbf{R}}^0$, where $\{e_1, \cdots, e_a\}$ resp. $\{e_{11}, \cdots, e_{1b}\}$ resp. $\{e_{21}, \cdots, e_{2c}\}$ are associated with those elliptic points z of $\Gamma_{\mathbf{R}}^0$ that belong to $\wp(\Gamma)$ resp. $Q_u(\Gamma)$ resp. $Q_r(\Gamma)$. In the same manner, denote by

$$\{g'; \underbrace{\infty, \cdots, \infty}_{s'}; e'_1, \cdots, e'_{a'}; e'_{11}, \cdots, e'_{1b'}; e'_{21}, \cdots, e'_{2c'}\} \tag{157'}$$

the signature of $\Gamma_{\mathbf{R}}^{0\prime}$.

Then by the corollary of Proposition 7 (§26), we have

$$s = s' = \sum_{P \in \wp_\infty(\Gamma)} \deg P, \tag{158}$$

and by Theorems 4, 4′,

$$\begin{aligned} &a = a'; \\ &\{e_1, \cdots, e_a\} = \{e'_1, \cdots, e'_{a'}\} \\ &= \{\underbrace{e(P), \cdots, e(P)}_{\deg P}; \underbrace{p^{r(P)-\nu}, \cdots, p^{r(P)-\nu}}_{a(P,\nu)};\ (0 \le \nu \le r(P) - 1)\}_{P \in \wp(\Gamma),\ e(P) > 1} \end{aligned} \tag{159}$$

with

$$a(P, \nu) = \begin{cases} \frac{\deg P}{e_0(P) p^\nu} (q^{cp^\nu} - q^{cp^{\nu-1}}) & \cdots \nu > 0, \\ \frac{\deg P}{e_0(P)} (q^c - 1) & \cdots \nu = 0, \end{cases} \tag{160}$$

where $e(P) = e_0(P) p^{r(P)}$ $(e_0(P) \not\equiv 0 \pmod p)$, and $c = c(P)$ is as in Theorem 4. In particular, we see that $e(P) = 1$ holds for almost all $P \in \wp(\Gamma)$. Moreover, by Theorems 5, 5′, we obtain

$$\begin{aligned} &c = c'; \quad \{e_{21}, \cdots, e_{2c}\} = \{e'_{21}, \cdots, e'_{2c'}\} \\ &= \{\underbrace{p^{r(Q)-\nu}, \cdots, p^{r(Q)-\nu}}_{a(Q,\nu)}; (0 \le \nu \le r(Q) - 1)\}_{Q \in Q_r(\Gamma)} \end{aligned} \tag{161}$$

where $e(Q) = p^{r(Q)}$, and

$$a(Q,\nu) = \begin{cases} \frac{1}{p^\nu}\frac{q^{\frac{1}{2}(cp^\nu+1)}-q^{\frac{1}{2}(cp^{\nu-1}+1)}}{q-1} & \cdots \mathfrak{p} \nmid 2,\ \nu > 0, \\ \frac{q^{\frac{1}{2}(c+1)}-1}{q-1} & \cdots \mathfrak{p} \nmid 2,\ \nu = 0, \\ \frac{1}{2^\nu} q^{\frac{c}{2}-\mathrm{ord}_{\mathfrak{p}} 2}\frac{q^{\frac{1}{2}(c2^\nu+1)}-q^{\frac{1}{2}(c2^{\nu-1}+1)}}{q-1} & \cdots \mathfrak{p}|2,\ \nu > 0, \\ \frac{q^{\frac{c}{2}-\mathrm{ord}_{\mathfrak{p}} 2+\frac{1}{2}(c+1)}-1}{q-1} & \cdots \mathfrak{p}|2,\ \nu = 0. \end{cases} \tag{162}$$

Here, $c = c(Q)$ is as in Theorem 5. In particular, $Q_r(\Gamma)$ is finite. Therefore, by (156), (158), (159) and (161), we obtain

$$\frac{1}{2}\sum_{i=1}^{b}(1-\frac{1}{e_{1i}}) - \frac{1}{2}\sum_{j=1}^{b'}(1-\frac{1}{e'_{1j}}) = g' - g. \tag{163}$$

As for e_{1i} and e'_{1j}, we obtain by Theorems 6, 6′:

$$\begin{aligned} \{e_{11},\cdots,e_{1b}\} =& \{e(Q);\overbrace{p^{r(Q)-\nu},\cdots,p^{r(Q)-\nu}}^{a(Q,\nu)}\ (0\le\nu\le r(Q)-1)\}_{Q\in Q_u^+(\Gamma)} \\ & \cup \{\underbrace{p^{r(Q)-\nu},\cdots,p^{r(Q)-\nu}}_{b(Q,\nu)}\ (0\le\nu\le r(Q)-1)\}_{Q\in Q_u^-(\Gamma)} \\ \{e'_{11},\cdots,e'_{1b'}\} =& \{\overbrace{p^{r(Q)-\nu},\cdots,p^{r(Q)-\nu}}^{b(Q,\nu)}\ (0\le\nu\le r(Q)-1)\}_{Q\in Q_u^+(\Gamma)} \\ & \cup \{e(Q);\underbrace{p^{r(Q)-\nu},\cdots,p^{r(Q)-\nu}}_{a(Q,\nu)}\ (0\le\nu\le r(Q)-1)\}_{Q\in Q_u^-(\Gamma)}, \end{aligned} \tag{164}$$

where

$$a(Q,\nu) = \begin{cases} \frac{1}{e_0(Q)p^\nu}\frac{q^{2[\frac{cp^\nu}{2}]+1}-q^{2[\frac{cp^{\nu-1}}{2}]+1}}{q-1} & \cdots \nu > 0, \\ \frac{1}{e_0(Q)}\frac{q^{2[\frac{c}{2}]+1}-q}{q-1} & \cdots \nu = 0, \end{cases}$$

$$b(Q,\nu) = \begin{cases} \frac{1}{e_0(Q)p^\nu}\frac{q^{2[\frac{cp^\nu+1}{2}]}-q^{2[\frac{cp^{\nu-1}+1}{2}]}}{q-1} & \cdots \nu > 0, \\ \frac{1}{e_0(Q)}\frac{q^{2[\frac{c+1}{2}]}-1}{q-1} & \cdots \nu = 0. \end{cases} \tag{165}$$

Here, $c = c(Q)$ is as in Theorem 6. However, we do not know at present whether $\{e(Q)\}_{Q\in Q_u^+(\Gamma)}$ and $\{e(Q)\}_{Q\in Q_u^-(\Gamma)}$, or $\{e_{11},\cdots,e_{1b}\}$ and $\{e'_{11},\cdots,e'_{1b'}\}$, or g and g' are always equal. (We conjecture that they are equal. No counterexamples are known.)

At any rate, by (164), $Q_u(\Gamma) = Q_u^+(\Gamma) \cup Q_u^-(\Gamma)$ is finite; hence $Q(\Gamma) = Q_u(\Gamma) \cup Q_r(\Gamma)$ is also finite.

The following formulae, which are obtained directly by the above results, are used later.

$$\begin{aligned} \sigma &\underset{\text{def.}}{=} \sum_{i=1}^{a}(1-\frac{1}{e_i}) \\ &= \sum_{P\in\mathfrak{p}(\Gamma)} \deg P\left\{1-\frac{1}{e_0(P)}+\frac{1}{e(P)}\sum_{\nu=1}^{r(P)}(p^\nu-p^{\nu-1})q^{\frac{\mathrm{ord}_{\mathfrak{p}} p}{p^\nu-p^{\nu-1}}}\right\}, \end{aligned} \tag{166}$$

$$\tau_r \underset{\text{def.}}{=} (q-1)\sum_{i=1}^{c}(1-\frac{1}{e_{2i}}) + \sum_{Q\in Q_r(\Gamma)}(1-\frac{1}{e(Q)})$$

(167)

$$= \sum_{Q\in Q_r(\Gamma)}\frac{1}{e(Q)}\sum_{\nu=1}^{r(Q)}(p^\nu - p^{\nu-1})q^{\frac{\text{ord}_\mathfrak{p} p}{p^\nu - p^{\nu-1}}+\frac{1}{2}} \times \begin{cases} 1 & \cdots \mathfrak{p}\nmid 2, \\ q^{\frac{\kappa}{2}-\text{ord}_\mathfrak{p} 2} & \cdots \mathfrak{p}|2, \end{cases}$$

where $\kappa = \text{Max}_{u\in u_\mathfrak{p}} \text{ord}_\mathfrak{p}(u^2+1)$ (for $\mathfrak{p}|2$, if $Q_r(\Gamma)\neq\phi$).[23]

$$\tau_u \underset{\text{def.}}{=} (q-1)\sum_{i=1}^{b}(1-\frac{1}{e_{1i}}) + \sum_{Q\in Q_u(\Gamma)}(1-\frac{1}{e(Q)})$$

(168)

$$= q\sum_{Q\in Q_u^+(\Gamma)}\left\{1-\frac{1}{e_0(Q)}+\frac{1}{e(Q)}\sum_{\nu=1}^{r(Q)}(p^\nu-p^{\nu-1})q^{2[\frac{\text{ord}_\mathfrak{p} p}{2(p^\nu-p^{\nu-1})}]}\right\}$$

$$+\sum_{Q\in Q_u^-(\Gamma)}\left\{1-\frac{1}{e_0(Q)}+\frac{1}{e(Q)}\sum_{\nu=1}^{r(Q)}(p^\nu-p^{\nu-1})q^{2[\frac{1}{2}(\frac{\text{ord}_\mathfrak{p} p}{p^\nu-p^{\nu-1}}+1)]}\right\}.$$

Here, [ ] denotes the Gauss symbol.

(168′) Equation (168) remains valid if we replace $\sum_{i=1}^{b}(1-\frac{1}{e_{1i}})$ by $\sum_{i=1}^{b'}(1-\frac{1}{e'_{1i}})$ and invert $Q_u^+(\Gamma)$ and $Q_u^-(\Gamma)$.

Call this new number τ'_u.

The ζ function of Γ in the general case.

§35. The results. By our above results on parabolic elements and elliptic elements of Γ, we can extend Theorem 1 (§8) and Theorem 2 (§23) to the case of general Γ, as follows.

THEOREM 7. *Let Γ be any discrete subgroup of $G = G_\mathbf{R}\times G_\mathfrak{p}$ such that $\Gamma_\mathbf{R}$, $\Gamma_\mathfrak{p}$ are dense in $G_\mathbf{R}$, $G_\mathfrak{p}$ respectively and that G/Γ has finite invariant volume. Let $\zeta_\Gamma(u) = \prod_{P\in\wp(\Gamma)}(1-u^{\deg P})^{-1}$ be the ζ-function of Γ (see §6). Then we have the following formula for $\zeta_\Gamma(u)$:*

$$\zeta_\Gamma(u)\times\prod_{P\in\wp_\infty(\Gamma)}(1-u^{\deg P})^{-1} = \frac{P(u)(1+qu)^{g'-g}}{(1-u)(1-q^2u)}\times(1-u)^H, \tag{169}$$

where $\wp_\infty(\Gamma)$ is the (finite) set of all Γ-equivalence classes of cusps of Γ (see §26), $q = N\mathfrak{p}$, g and g' are the genus of $\Gamma^0_\mathbf{R}$ and $\Gamma^{0\prime}_\mathbf{R}$ respectively, where $\Gamma^0 = \Gamma\cap(G_\mathbf{R}\times V)$ and $\Gamma^{0\prime} = \Gamma\cap(G_\mathbf{R}\times\omega^{-1}V\omega)$, with $V = PSL_2(O_\mathfrak{p})$ and $\omega\in V\begin{pmatrix}\pi & 0\\ 0 & 1\end{pmatrix}V$ (π: a prime element of $k_\mathfrak{p}$).

[23] As can be checked, easily, the exponent $\frac{\text{ord}_\mathfrak{p} p}{p^\nu-p^{\nu-1}}+\frac{1}{2}$ ($+\frac{\kappa}{2}-\text{ord}_\mathfrak{p} 2$ for $\mathfrak{p}|2$) is an integer.

$P(u)$ is a polynomial of degree $2g$ with a form:

$$\begin{cases} P(u) = \prod_{i=1}^{g}(1-\pi_i u)(1-\pi_i^* u) \in \mathbf{Z}[u], \\ \pi_i\pi_i^* = q^2 \qquad (1 \le i \le g), \end{cases} \tag{170}$$

$$|\pi_i|,\ |\pi_i^*| \le q^2;\ \pi_i,\ \pi_i^* \ne 1,\ q^2. \tag{171}$$

Now, the positive integer H is given as follows:

$$\begin{aligned} H &= \frac{1}{2}(q-1)v(\Gamma_{\mathbf{R}}^0) + \frac{1}{2}\sum_{Q\in Q(\Gamma)}\left(1-\frac{1}{e(Q)}\right) \\ &= (q-1)(g-1+\frac{s}{2}+\frac{\sigma}{2})+\frac{\tau_u}{2}+\frac{\tau_r}{2}, \end{aligned} \tag{172}$$

where

$$\begin{aligned} v(\Gamma_{\mathbf{R}}^0) &= \frac{1}{2\pi}\int_{\Gamma_{\mathbf{R}}^0\backslash\mathfrak{H}}\frac{dxdy}{y^2} \\ &= 2g-2+s+\sum_{i=1}^{a}\left(1-\frac{1}{e_i}\right)+\sum_{j=1}^{b}\left(1-\frac{1}{e_{1j}}\right)+\sum_{k=1}^{c}\left(1-\frac{1}{e_{2k}}\right), \end{aligned} \tag{173}$$

$\{g; \underbrace{\infty, \cdots, \infty}_{s}; e_1, \cdots, e_a; e_{11}, \cdots, e_{1b}; e_{21}, \cdots, e_{2c}\}$ *being the signature of $\Gamma_{\mathbf{R}}^0$ in the way of notations given in §34. Thus, $s = \sum_{P\in\wp_\infty(\Gamma)} \deg P$, and the numbers σ, τ_u, τ_r are given by* (166), (168), (167) *respectively. In particular, if Γ has no elements of order p and $g' = g$, then we have*

$$\begin{aligned} &\zeta_\Gamma(u)\times\prod_{P\in\wp_\infty(\Gamma)}(1-u^{\deg P})^{-1} \\ &= \frac{P(u)}{(1-u)(1-q^2u)}\times(1-u)^{\frac{1}{2}(q-1)v(\Gamma_{\mathbf{R}}^0)+\sum_{j=1}^{b}(1-\frac{1}{e_{1j}})} \end{aligned} \tag{174}$$

(*see* (163), (164)).

Remarks. (i) We conjecture that $g' = g$; to which no counterexamples are known.

(ii) By (169), we see that $\zeta_\Gamma(u)$ was better defined with

$$\prod_{P\in\wp(\Gamma)\cup\wp_\infty(\Gamma)}(1-u^{\deg P})^{-1}.$$

But to avoid confusion, we shall keep the previous definition.

(iii) Finally, we note that if Γ is torsion-free, then we have $g' = g$ by (163); hence

$$\begin{aligned} &\zeta_\Gamma(u)\times\prod_{P\in\wp_\infty(\Gamma)}(1-u^{\deg P})^{-1} \\ &= \frac{P(u)}{(1-u)(1-q^2u)}\times(1-u)^{(q-1)(g-1+\frac{s}{2})} \end{aligned} \tag{175}$$

and if moreover G/Γ is compact, then $\wp_\infty(\Gamma) = \phi$ and $s = 0$; hence we have

$$\zeta_\Gamma(u) = \frac{P(u)}{(1-u)(1-q^2u)}\times(1-u)^{(q-1)(g-1)} \tag{176}$$

which is nothing but Theorem 1 (§8).

§36. The Eichler-Selberg trace-formula. Having Theorems 3 ~ 6 and their corollaries on hand, we can prove Theorem 7 exactly in the same manner as in the proof of Theorem 1. But, of course, we need here the Eichler-Selberg trace formula (for the Hecke operators acting on the space of holomorphic cusp forms of weight 2) with respect to fuchsian groups Δ, where $G_{\mathbf{R}}/\Delta$ *may not be compact and* Δ *may not be torsion-free.* Namely, we make use of the following generalization of Lemma 1 (§9):

LEMMA 18 (Eichler-Selberg, Petersson).[24] *Let* Δ *be a discrete subgroup of* $G_{\mathbf{R}}$ *such that* $G_{\mathbf{R}}/\Delta$ *has finite invariant volume, let* $\tilde{\Delta}$ *be a subgroup of* $G_{\mathbf{R}}$ *containing* Δ *such that* $\gamma^{-1}\Delta\gamma$ *is commensurable with* Δ *and* $\Delta\gamma^{-1}\Delta = \Delta\gamma\Delta$ *for all* $\gamma \in \tilde{\Delta}$. *Let* $\rho = \rho_2$ *be the representation* (22) (§9) *of the Hecke ring* $\mathcal{H}(\tilde{\Delta}, \Delta)$ *in the space of holomorphic cusp forms of weight* 2 *with respect to* Δ. *Then* ρ *is a direct sum of* g *linear real representations* $\chi_1, \cdots, \chi_g$ (g: *the genus of* Δ). *Moreover for each* $\gamma_0 \in \tilde{\Delta}$ *with* $\gamma_0 \notin \Delta$, *put*

$$A(\Delta\gamma_0\Delta) = \sum_{\nu} \frac{1}{n_\nu} + 2\sum_{S}\sum_{h} r_h, \tag{177}$$

where

(i) ν *runs over all elliptic* Δ*-conjugacy classes* $\{\gamma\}_\Delta$ *contained in* $\Delta\gamma_0\Delta$, *and* n_ν *is the order of the centralizer of* γ *in* Δ; *or equivalently,* n_ν *is the multiplicity of the fixed point of* γ *as an elliptic point of* Δ.

(ii) S *runs over all cusps of* Δ *up to* Δ*-equivalence;* $(\Delta\gamma_0\Delta)_S$ (*resp.* Δ_S) *is the set of all elements of* $\Delta\gamma_0\Delta$ (*resp.* Δ) *that stabilize* [25] S. *For each* S, h *runs over a set of representatives of* Δ_S*-double cosets in* $(\Delta\gamma_0\Delta)_S$, *and* r_h *is defined as follows. For each* S, *fix a generator* δ_S *of* Δ_S, *and define* r_h *by:*

(178)

h	r_h
h : *parabolic*, $h = \delta_S^b$ $(b \in \mathbf{R})$	$\frac{1}{1-e^{-2\pi i b}}$
h : *hyperbolic*, $h^{-1}\delta_S h = \delta_S^{\beta/\alpha}$, *where* $\alpha, \beta \in \mathbf{Z}, > 0$, *and* $(\alpha, \beta) = 1$.	$\begin{cases} 0 & (\text{if } \alpha > \beta) \\ \alpha & (\text{if } \alpha < \beta) \end{cases}$

Then, the summations on the right side of (177) *are finite, and we have*

$$A(\Delta\gamma_0\Delta) = 2(d(\Delta\gamma_0\Delta) - \operatorname{tr}\rho(\Delta\gamma_0\Delta)), \tag{179}$$

where $d(\Delta\gamma_0\Delta) = |\Delta\gamma_0\Delta/\Delta|$.

§37. Proof of Theorem 7. First we shall compute the right side of (177) for the case $\tilde{\Delta} = \Gamma_{\mathbf{R}}$, $\Delta = \Gamma_{\mathbf{R}}^0$, and $\Delta\gamma_0\Delta = T_m$ ($m \geq 1$).

(i) *The second term* (*contribution of parabolic elements*).

Fix any cusp S of $\Gamma_{\mathbf{R}}^0$ and let d be the degree of its Γ-equivalence class (see §26). Put

$$H^0 = \{\gamma \in \Gamma \mid \gamma_{\mathbf{R}} S = S,\ \gamma_{\mathbf{R}} : \text{parabolic}\} \cup \{1\},$$
$$H = \{\gamma \in \Gamma \mid \gamma_{\mathbf{R}} S = S\}.$$

[24] Cf. M. Eichler [12].

[25] Then elements of Δ_S are necessarily parabolic, but elements of $(\Delta\gamma_0\Delta)_S$ may not be so.

By Theorem 3, there exists $t \in G_{\mathbf{R}} \times PL_2(\mathbf{Z}_p)$ such that $H = t^{-1}B^{(d)}t$, where

$$B^{(d)} = \left\{ \begin{pmatrix} p^{-dk} & b \\ 0 & p^{dk} \end{pmatrix} \middle| \, k \in \mathbf{Z},\ b \in \mathbf{Z}^{(p)} \right\}.$$

Thus $H^0 = t^{-1}\begin{pmatrix} 1 & \mathbf{Z}^{(p)} \\ 0 & 1 \end{pmatrix}t$, and $H \cap \Gamma^0 = t^{-1}\begin{pmatrix} 1 & \mathbf{Z} \\ 0 & 1 \end{pmatrix}t$. Put $\xi = t^{-1}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}t$, so that ξ generates $H \cap \Gamma^0$. Let h be any element of H and put $h = t^{-1}\begin{pmatrix} p^{-kd} & b \\ 0 & p^{kd} \end{pmatrix}t$. Then

$$h \in T^m \leftrightarrow \begin{cases} |k| \cdot d \leq m, & b_0 \in \mathbf{Z}; \\ \text{when } |k| \cdot d < m, & b_0 \not\equiv 0 \pmod{p}; \end{cases} \tag{180}$$

where $b_0 = bp^m$. Moreover if k and b_0 run over such numbers as above, and b_0 runs only over a set of representatives modulo $p^{m-|k|\cdot d}$, then h runs over a set of representatives of the double coset space $H \cap \Gamma^0 \backslash H \cap T^m / H \cap \Gamma^0$. For each such representative h, let us compute r_h (defined in Lemma 18).[26] First, h is parabolic if and only if $k = 0$, and in this case $b_h = b = b_0/p^m$ ($b_0 \not\equiv 0 \pmod{p}$). Thus the summation $\sum r_h$ over such h is given by $\sum_\zeta (1-\zeta)^{-1}$, where ζ runs over all primitive p^m-th roots of unity; hence is equal to $\frac{1}{2}(p-1)p^{m-1}$ (use the equality $\sum_\zeta (x-\zeta)^{-1} = \frac{f'(x)}{f(x)}$, where $f(x) = (x^{p^m}-1)(x^{p^{m-1}}-1)^{-1}$). On the other hand, if h is hyperbolic, i.e., if $k \neq 0$, then the numbers α, β defined in (178) are given by $\alpha = 1, \beta = p^{2kd}$ ($k > 0$), and $\alpha = p^{-2kd}, \beta = 1$ ($k < 0$). Moreover for each $k > 0$ with $kd \leq m$, the number of $b_0 \mod p^{m-kd}$ satisfying (180) is equal to $(p-1)p^{m-kd-1}$ ($kd < m$), 1 ($kd = m$). Therefore, the summation $\sum r_h$ over the hyperbolic representatives h is given by

$$\begin{cases} (p-1)\sum_{k=1}^{\left[\frac{m}{d}\right]} p^{m-kd-1} & \cdots m \not\equiv 0 \pmod{d} \\ (p-1)\sum_{k=1}^{\frac{m}{d}-1} p^{m-kd-1} + 1 & \cdots m \equiv 0 \pmod{d}. \end{cases} \tag{181}$$

Call this number $c(m, d)$. Then, since each $P \in \wp_\infty(\Gamma)$ consists of exactly $\deg P$ distinct $\Gamma_{\mathbf{R}}^0$ equivalence classes (Proposition 7, §26), the second term of the right side of (177) is given by

$$s(p-1)p^{m-1} + 2\sum_{P \in \wp_\infty(\Gamma)} c(m, \deg P)\deg P, \tag{182}$$

where $s = \sum_{P \in \wp_\infty(\Gamma)} \deg P$ is the number of cusps of $\Gamma_{\mathbf{R}}^0$ (up to $\Gamma_{\mathbf{R}}^0$-equivalence).

(ii) *The first term (contribution of elliptic elements).*

This is obtained directly from the Corollaries of Theorems 4, 5, 6 (see (118) for the definition of $A_m\{\gamma\}_\Gamma$). In fact, $\sum_\nu n_\nu^{-1}$ is given by

$$\sum_{\{\gamma\}_\Gamma} A_m\{\gamma\}_\Gamma = \Big(\sum_{\{\gamma\}_\Gamma}^{\wp} + \sum_{\{\gamma\}_\Gamma}^{Q_u} + \sum_{\{\gamma\}_\Gamma}^{Q_r}\Big) A_m\{\gamma\}_\Gamma, \tag{183}$$

where the summation on the left side is over all Γ-conjugacy classes $\{\gamma\}_\Gamma$ such that $\gamma_{\mathbf{R}}$ is elliptic, and the summations on the right side are over such $\{\gamma\}_\Gamma$ that the fixed points z ($\in \mathfrak{H}$) of $\gamma_{\mathbf{R}}$ belong to the elements $\wp(\Gamma)$, $Q_u(\Gamma)$ and $Q_r(\Gamma)$ respectively.

[26] W. r. t. the generator ξ of $H \cap \Gamma^0$.

By the Corollary of Theorem 4, we have

$$\sum_{\{\gamma\}_\Gamma}^{\wp} A_m\{\gamma\}_\Gamma = \sum_{P=P_z\in\wp(\Gamma)} \sum_{\gamma\in\Gamma_z,\gamma\neq 1} A_m\{\gamma\}_\Gamma$$

(184)

$$= 2\{N_m + (q-1)\sum_{k=1}^{m-1} q^{k-1}N_{m-k}\} + (q-1)q^{m-1}\sigma,$$

where σ is given by (166) and

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

Note, in computing this out, that for each $n \geq 0$, the number of elements γ ($\gamma \neq 1$) of Γ_z with $\deg\{\gamma\}_\Gamma = n$ is given by

$$\begin{cases} 2e(P) & \cdots n > 0,\ n \equiv 0 \pmod{\deg P}, \\ 0 & \cdots n > 0,\ n \not\equiv 0 \pmod{\deg P}, \\ e(P) - 1 & \cdots n = 0. \end{cases}$$

Note also the Corollary ((ii)) of Proposition 8.

On the other hand, by the Corollary of Theorem 6, we obtain

(186) $$\sum_{\{\gamma\}_\Gamma}^{Q_u} A_m\{\gamma\}_\Gamma = \begin{cases} (q+1)q^{m-1}\mu & \cdots m:\ \text{even}, \\ (q+1)q^{m-1}\mu' & \cdots m:\ \text{odd}. \end{cases}$$

where μ, μ' are given by the following:

(187) $$\mu = \sum_{Q\in Q_u^+(\Gamma)}\left(1 - \frac{1}{e_0(Q)}\right) + \begin{cases} \sum_{Q\in Q_u^+(\Gamma)} e(Q)^{-1}\sum_{\nu=1}^{r(Q)}(p^\nu - p^{\nu-1})q^{cp^{r(Q)-\nu}} & \cdots c:\ \text{even}, \\ \sum_{Q\in Q_u^-(\Gamma)} e(Q)^{-1}\sum_{\nu=1}^{r(Q)}(p^\nu - p^{\nu-1})q^{cp^{r(Q)-\nu}} & \cdots c:\ \text{odd}. \end{cases}$$

(187′) *the formula for μ' is obtained by inverting $Q_u^+(\Gamma)$ and $Q_u^-(\Gamma)$ on the right side of* (187).

Here, c is defined by $\mathrm{ord}_\mathfrak{p} p = c(p^{r(Q)} - p^{r(Q)-1})$. Note, in computing this out, that since c is even when $\mathfrak{p}|2$ (see Theorem 6), we have c: even $\Leftrightarrow$ cp: even. Now we can check directly by (168) and (163) that

(188) $$q\mu + \mu' = \tau_u,$$

(189) $$\mu - \mu' = 2(g' - g).$$

Finally, we obtain immediately from the Corollary of Theorem 5 that

(190) $$\sum_{\{\gamma\}_\Gamma}^{Q_r} A_m\{\gamma\}_\Gamma = q^{m-1}\tau_r,$$

τ_r being as in (167). Thus by putting these together, we obtain

(191)[27] $$\frac{1}{2}A(T^m) = A_m + B_m,$$

with

(192) $$\begin{cases} A_m = N_m + (q-1)\sum_{k=1}^{m-1} N_{m-k}, \\ B_m = \frac{1}{2}(p-1)sp^{m-1} + \sum_{P\in\wp_\infty(\Gamma)} c(m, \deg P)\deg P \\ \qquad +(\frac{q-1}{2}\sigma + \frac{\tau_r}{2})q^{m-1} + \begin{cases} \frac{1}{2}(q+1)q^{m-1}\mu & \cdots m: \text{ even}, \\ \frac{1}{2}(q+1)q^{m-1}\mu' & \cdots m: \text{ odd}. \end{cases} \end{cases}$$

Now, in general, let $f(m)$, $F(m)$ be two functions defined for every positive integer m. Then the following two relations are equivalent:

(193) $$F(m) = f(m) - (q-1)\sum_{k=1}^{m-1} f(m-k) \qquad (m \geq 1),$$

(193′) $$f(m) = F(m) + (q-1)\sum_{k=1}^{m-1} q^{k-1}F(m-k) \qquad (m \geq 1),$$

(see §13). Moreover, we have the following table:[28]

(194)

	$f(m)$	$F(m)$	Notes
(i)	$c(m,d)$	$\begin{cases} 1 & \cdots m \equiv 0 \pmod d \\ 0 & \cdots m \not\equiv 0 \pmod d \end{cases}$	use (193′) to check
(ii)	q^{m-1}	1	put $d=1$ in (i)
(iii)	$\begin{cases} (q+1)q^{m-1}\mu & \cdots m: \text{even} \\ (q+1)q^{m-1}\mu' & \cdots m: \text{odd} \end{cases}$	$q\mu + \mu' + (-q)^m(\mu - \mu')$ $= \tau_u + 2(-q)^m(g' - g)$	
(iv)	A_m	N_m	by definition

Now define L_m and N'_m by :

	B_m	L_m
(v)		
(vi)	$\frac{1}{2}A(T^m)$	$N'_m = N_m + L_m$

Then by (194) (i) (ii), we obtain

(195) $$L_m = \frac{1}{2}(p-1)s + \sum_{\substack{P\in\wp_\infty(\Gamma), \\ \deg P \mid m}} \deg P + \frac{q-1}{2}\sigma + \frac{\tau_r}{2} + \frac{\tau_u}{2} + (-q)^m(g'-g),$$

and

(196) $$N_m = N'_m - L_m.$$

---

[27] $A(T^m)$ is the $A(\Delta\gamma\Delta)$ (of Lemma 18) for $\Delta\gamma\Delta = T^m$.

[28] Recall that if Γ has a cusp, then $k_\mathfrak{p} = \mathbf{Q}_p$; hence $q = p$.

Now, on the other hand, we can compute the right side of (179) for $\Delta\gamma_0\Delta = T^m$ by exactly the same computation as in §14. Namely, put

$$\det\{1-(\rho(T^1)-q+1)u+q^2u^2\} = \prod_{i=1}^{g}\{1-(\chi_i(T^1)-q+1)u+q^2u^2\}$$
$$= \prod_{i=1}^{g}(1-\pi_i u)(1-\pi_i^* u), \quad (\pi_i\pi_i^* = q^2;\ 1\le i\le g). \tag{197}$$

Then by the same computation as in §14, we obtain

$$N'_m = q^{2m}+1-(q-1)(g-1)-\sum_{i=1}^{g}(\pi_i^m+\pi_i^{*m}) \quad (m\ge 1). \tag{198}$$

Now by (195), (196) and (198), we immediately obtain the formula for $\zeta_\Gamma(u) = \prod_{P\in\wp(\Gamma)}(1-u^{\deg P})^{-1} = \exp(\sum_{m=1}^{\infty}\frac{N_m}{m}u^m)$; namely we obtain

$$\begin{aligned}\zeta_\Gamma(u) &= \exp\Big(\sum_{m=1}^{\infty}\frac{N'_m}{m}u^m\Big)\times\exp\Big(-\sum_{m=1}^{\infty}\frac{L_m}{m}u^m\Big)\\ &= \frac{\prod_{i=1}^{g}(1-\pi_i u)(1-\pi_i^* u)}{(1-u)(1-q^2u)}\times(1-u)^{(q-1)(g-1)}\\ &\quad\times\prod_{P\in\wp_\infty(\Gamma)}(1-u^{\deg P})\times(1-u)^{\frac{1}{2}(p-1)s+\frac{q-1}{2}\sigma+\frac{\tau_u}{2}+\frac{\tau_r}{2}}\\ &\quad\times(1+qu)^{g'-g}.\end{aligned} \tag{199}$$

Since $H = \frac{1}{2}(p-1)s+\frac{1}{2}(q-1)\sigma+\frac{1}{2}\tau_u+\frac{1}{2}\tau_r$, this proves (169).[29]

That $P(u)\in\mathbf{Z}[u]$ and $H\in\mathbf{Z}$. By (169), we have $P(u)(1-u)^H\in\mathbf{Z}[[u]]$, and by definition, $H\in\mathbf{Q}$.[30] Put $H=\frac{m}{n}$ $(m,n\in\mathbf{Z},>0)$. Then $P(u)^n\in\mathbf{Z}[u]$; hence [31] $P(u)\in\mathbf{Z}[u]$. But then $(1-u)^H\in\mathbf{Z}[[u]]$; hence $H\in\mathbf{Z}$.

That (171) *holds.* This follows exactly in the same manner as in the proof of Theorem 2 (§23), if we use the generalization of Lemma 10 of Chapter 1 given in Supplement §2 instead of Lemma 10. This completes the proof of Theorem 7. □

We have also proved:

COROLLARY. *With the notations of Theorem 7 and Lemma 18, we have*

$$P(u) = \det\{1-(\rho(T^1)-q+1)u+q^2u^2\}. \tag{200}$$

§38. Examples.

EXAMPLE 1. Let B be a quaternion algebra over $\mathbf{Q}$, in which p and ∞ are unramified. Let D be the discriminant of B (so, $D\not\equiv 0 \pmod p$). Let O be a maximal order of B, put $O^{(p)} = \bigcup_{n=0}^{\infty}p^{-n}O$, and put

$$\Gamma = \{x\in O^{(p)} \mid N_{B/\mathbf{Q}}(x)=1\}/\pm 1. \tag{201}$$

[29] Recall that $s\neq 0$ only if $q=p$.

[30] Hence $P(u)\in\mathbf{Q}[u]$.

[31] Use Gauss' lemma.

Then by Proposition 1 of Chapter 4, Γ can be considered as a discrete subgroup of $G = G_{\mathbf{R}} \times G_{\mathfrak{p}} = PSL_2(\mathbf{R}) \times PSL_2(\mathbf{Q}_p)$ (with dense image of projection in each component of G, and with finite volume quotient G/Γ). The quotient is compact if and only if $D \neq 1$. For $D = 1$, we have $B = M_2(\mathbf{Q})$, and $\Gamma = PSL_2(\mathbf{Z}^{(p)})$ up to conjugacy in G.

Now by Eichler's arithmetic of quaternion algebras [**11**], and by Shimizu [**28**] (for (203)), we can easily calculate the various invariants of these Γ defined in Theorem 7. The result is as follows:

$$g = g' = \frac{1}{12}\prod_{l|D}(l-1) - \frac{1}{4}\prod_{l|D}\left(1-\left(\frac{-4}{l}\right)\right) - \frac{1}{3}\prod_{l|D}\left(1-\left(\frac{-3}{l}\right)\right) + 1 - \begin{cases}\frac{1}{2} & \cdots D = 1,\\ 0 & \cdots D \neq 1;\end{cases} \tag{202}$$

$$v(\Gamma_{\mathbf{R}}^0) = \frac{1}{6}\prod_{l|D}(l-1), \tag{203}$$

$$\sum_{Q \in Q(\Gamma)}\left(1 - \frac{1}{e(Q)}\right) = \frac{1}{2}\prod_{l|Dp}\left(1-\left(\frac{-4}{l}\right)\right) + \frac{2}{3}\prod_{l|Dp}\left(1-\left(\frac{-3}{l}\right)\right). \tag{204}$$

Hence

$$H = \frac{1}{12}\prod_{l|Dp}(l-1) + \frac{1}{4}\prod_{l|Dp}\left(1-\left(\frac{-4}{l}\right)\right) + \frac{1}{3}\prod_{l|Dp}\left(1-\left(\frac{-3}{l}\right)\right). \tag{205}$$

Thus,

$$\zeta_\Gamma(u) \times \begin{cases}(1-u)^{-1} & \cdots D = 1\\ 1 & \cdots D \neq 1\end{cases} = \frac{P(u)}{(1-u)(1-p^2u)} \times (1-u)^H, \tag{206}$$

$P(u)$ being a polynomial of degree $2g$ of the form described in Theorem 7. In particular, if $D = 1$, 6, 10 or 22, then we have $g = 0$; hence $P(u) = 1$. For $D = 1$, i.e., $\Gamma = PSL_2(\mathbf{Z}^{(p)})$, this formula coincides with the one calculated in §7.

Here, we note a rather strange fact: if B^* denotes the quaternion algebra over $\mathbf{Q}$ with discriminant $D^* = Dp$ (hence D^* is *definite*), then by Eichler's formula for the class number of (definite) quaternion algebras (see Eichler [**10**] Satz 2), we obtain:

(207) *H is equal to the class number of B^*.*

However, we do not know what this really implies, except in the case of $D = 1$. (For $D = 1$, i.e., $\Gamma = PSL_2(\mathbf{Z}^{(p)})$, H is nothing but the number of supersingular moduli j (Corollary of Theorem 1′ in §9 of Chap.5), and if E_j denotes the elliptic curve with modulus j, then $j \mapsto \mathcal{A}(E_j)$ (the endomorphism ring of E_j) gives a bijection between the set of all supersingular moduli j and that of right orders of the (complete set of) representatives of left O^*-ideals of B^*, where O^* is a given maximal order of B^*.)

EXAMPLE 2 (See Chap. 5, Part 2 for the details and proofs). Let $\Gamma = PSL_2(\mathbf{Z}^{(p)})$ and let Γ' be a subgroup of Γ with finite index. Let K' be the finite extension of $K = \mathbf{F}_{p^2}(j)$ (j: a variable over $\mathbf{F}_p$) corresponding to Γ' in the sense of §16 of Chapter 5 Part 2. Let H' be the number of prime divisors of K' that lie on supersingular prime divisors of K. Then by the results of Chapter 5, Part 2 (esp. §30), we have

$$\zeta_{\Gamma'}(u) \times \prod_{P \in \mathfrak{p}_\infty(\Gamma')} (1 - u^{\deg P})^{-1} = \zeta_{K'}(u) \times (1-u)^{H'}, \tag{208}$$

where $\zeta_{K'}(u) = \frac{P'(u)}{(1-u)(1-p^2u)}$ is the congruence ζ-function of K' over $\mathbf{F}_{p^2}$. Thus we have

$$P'(u) = \prod_{i=1}^{g'} (1 - \pi_i u)(1 - \bar{\pi}_i u) \quad \text{with } |\pi_i| = |\bar{\pi}_i| = p \quad (1 \le i \le g'),$$

where g' is the genus of K' and is at the same time the genus of $(\Gamma'^0)_{\mathbf{R}}$.

As an example, let $N > 1$, $N \not\equiv 0 \pmod{p}$ be an integer, and let $\Gamma' = \Gamma(N)$ be the principal congruence subgroup of Γ;

$$\Gamma(N) = \{\gamma \in SL_2(\mathbf{Z}^{(p)}) \mid \gamma \equiv \pm 1 (\mathrm{mod} N)\} / \pm 1 \quad (N > 1). \tag{209}$$

Put

$$n = (\Gamma : \Gamma(N)) = \begin{cases} 6 & (N = 2), \\ \frac{N^3}{2} \prod_{l \mid N} (1 - \frac{1}{l^2}) & (N > 2); \end{cases}$$

put $s = n/N$, and let d be the smallest positive integer such that $p^d \equiv \pm 1 \pmod{N}$. Then we have

$$\prod_{P \in \mathfrak{p}_\infty(\Gamma')} (1 - u^{\deg P}) = (1 - u^d)^{s/d}. \tag{210}$$

The genus g' of $\Gamma(N)$ is given by $g' = \frac{N-6}{12N} n + 1$, and since $\Gamma(N)$ is torsion-free, we have $H' = (p-1)(g' - 1 + \frac{s}{2}) = \frac{n}{12}(p-1)$. Hence

$$\zeta_{\Gamma'}(u) \times (1 - u^d)^{-s/d} = \frac{P'(u)}{(1-u)(1-p^2u)} \times (1-u)^{\frac{n}{12}(p-1)}. \tag{211}$$