Part 2. Full $G_\mathfrak{p}$-subfields over algebraic number fields.

The readers are suggested to recall the definitions of full $G_\mathfrak{p}$-subfield (§4) and quasi-irreducibility (§16) of a $G_\mathfrak{p}$-field over **C**. Throughout the following, an algebraic number field always means a *finite* algebraic extension of the field of rational numbers **Q**.

Main results.

§18. Our main purpose in Part 2 of this chapter is to prove the following two theorems, Theorem 4 and Theorem 5. Later, we shall give some supplementary results (see §32 ~ §36).

THEOREM 4. *Every $G_\mathfrak{p}$-field over* **C** *contains a full $G_\mathfrak{p}$-subfield over an algebraic number field.*

If we impose quasi-irreducibility condition on a $G_\mathfrak{p}$-field over **C**, then we get an essentially stronger result, as follows.

THEOREM 5. *Every quasi-irreducible $G_\mathfrak{p}$-field L over* **C** *contains a unique full $G_\mathfrak{p}$-subfield L_{k_0} over an algebraic number field k_0 satisfying the following properties; namely, if k is any subfield of* **C***, then there is a full $G_\mathfrak{p}$-subfield L_k over k if and only if k contains k_0, and moreover if k is such a field, then L_k is unique and is given by $L_k = L_{k_0} \cdot k$.*

In short, every quasi-irreducible $G_\mathfrak{p}$-field over **C** contains a smallest full $G_\mathfrak{p}$-subfield over an algebraic number field, and all other full $G_\mathfrak{p}$-subfields are its constant field extensions. This will be referred to as *the existence and essential uniqueness of a full $G_\mathfrak{p}$-subfield over an algebraic number field* of a quasi-irreducible $G_\mathfrak{p}$-field over **C**. Some variations of Theorem 5 will be given in §32, §33.

Although Theorem 5 is essentially stronger (and hence more noteworthy) than Theorem 4, it is almost a formal consequence of Theorem 4. Thus, our first task is to show this.

Reducing Theorem 5 to Theorem 4.

§19. In general, if $L \supset K_1, K_2$ are overfields of a field k such that $L = K_1K_2$ and that K_1, K_2 are linearly disjoint over k, and if σ_1, σ_2 are automorphisms of K_1, K_2 respectively such that $\sigma_1|k = \sigma_2|k$, then there is a unique automorphism of L whose restrictions to K_1, K_2 coincide with σ_1, σ_2 respectively. This automorphism of L will be denoted by $\sigma_1 \otimes \sigma_2$. The identity automorphism of a field K will be denoted by 1_K.

Lemma 2. *Let L be a $G_{\mathfrak{p}}$-field over $\mathbf{C}$, and let L_k be a full $G_{\mathfrak{p}}$-subfield of L over a field k ($\subset \mathbf{C}$). Then L_k is the fixed field of the group of all automorphisms of L of the form $1_{L_k} \otimes \sigma$ ($\sigma \in \mathrm{Aut}_k \mathbf{C}$).*

Proof. Put $\mathcal{G} = \{1_{L_k} \otimes \sigma | \sigma \in \mathrm{Aut}_k \mathbf{C}\}$, and let L' be the fixed field of $\mathcal{G}$. Then it is clear that $L' \supset L_k$ and $L' \cap \mathbf{C} = k$. Moreover, since L_k is $G_{\mathfrak{p}}$-invariant, elements $g_{\mathfrak{p}}$ of $G_{\mathfrak{p}}$ acting on L are of the form $g_{\mathfrak{p}}|_{L_k} \otimes 1_{\mathbf{C}}$. Therefore, elements of $\mathcal{G}$ commute with all elements of $G_{\mathfrak{p}}$. Therefore, L' is $G_{\mathfrak{p}}$-invariant. Hence by Proposition 2, L' and $\mathbf{C}$ are linearly disjoint over k. Therefore, L' and $L_k \cdot \mathbf{C}$ must be linearly disjoint over L_k. But $L_k \cdot \mathbf{C} = L$. Therefore we get $L' = L_k$. □

$$
\begin{tikzcd}
L' \arrow[r, dash] \arrow[d, dash] & L = L_k \cdot \mathbf{C} \arrow[dd, dash] \\
L_k \arrow[ur, dash] \arrow[d, dash] & \\
k \arrow[r, dash] & \mathbf{C}
\end{tikzcd}
$$

Let L be a $G_{\mathfrak{p}}$-field over $\mathbf{C}$, and let σ be any automorphism of $\mathbf{C}$. An automorphism $\widetilde{\sigma}$ of L will be called a *$G_{\mathfrak{p}}$-extension of σ* if $\widetilde{\sigma}|_{\mathbf{C}} = \sigma$ and if $\widetilde{\sigma}$ commutes with the actions of all elements of $G_{\mathfrak{p}}$. We shall say that σ has a $G_{\mathfrak{p}}$-extension when such $\widetilde{\sigma}$ exists. In this case, all $G_{\mathfrak{p}}$-extensions of σ are given by $\widetilde{\sigma} \cdot z$ with $z \in \mathfrak{Z}$, where $\mathfrak{Z}$ is the centralizer of $G_{\mathfrak{p}}$ in $\mathrm{Aut}_{\mathbf{C}} L$. Recall that $\mathfrak{Z}$ is always finite and $\mathfrak{Z} = \{1\}$ if and only if L is quasi-irreducible (Corollary 3 of Theorem 3).

Now, *let L be quasi-irreducible. Then if $\sigma \in \mathrm{Aut}\,\mathbf{C}$ has a $G_{\mathfrak{p}}$-extension $\widetilde{\sigma}$, it is the unique $G_{\mathfrak{p}}$-extension of σ; hence $\widetilde{\sigma}$ always has a unique meaning.* By this it is clear that if $\sigma, \tau \in \mathrm{Aut}\,\mathbf{C}$ have $G_{\mathfrak{p}}$-extensions, then $\sigma\tau$ and σ^{-1} also have $G_{\mathfrak{p}}$-extensions given by

$$
\widetilde{\sigma\tau} = \widetilde{\sigma}\widetilde{\tau}, \quad \widetilde{\sigma^{-1}} = \widetilde{\sigma}^{-1}. \tag{41}
$$

Now let us look at Lemma 2 again, assuming now that L is quasi-irreducible. Then we see that for each $\sigma \in \mathrm{Aut}_k \mathbf{C}$, $1_{L_k} \otimes \sigma$ gives *the* unique $G_{\mathfrak{p}}$-extension of σ. In fact, as has been shown before, $1_{L_k} \otimes \sigma$ commutes with all elements of $G_{\mathfrak{p}}$. Put, therefore, $\widetilde{\sigma} = 1_{L_k} \otimes \sigma$ for each $\sigma \in \mathrm{Aut}_k \mathbf{C}$. Then by this lemma, L_k is the fixed field of the group of all $\widetilde{\sigma}$ with $\sigma \in \mathrm{Aut}_k \mathbf{C}$. But since the group of $\widetilde{\sigma}$ depends only on k and does not depend on L_k, we conclude that L_k is uniquely determined by k. We have therefore proved:

Proposition 5. *Let L be a quasi-irreducible $G_{\mathfrak{p}}$-field over $\mathbf{C}$, and let k be a subfield of $\mathbf{C}$. If L contains a full $G_{\mathfrak{p}}$-subfield L_k over k, then it is unique; moreover, every $\sigma \in \mathrm{Aut}_k \mathbf{C}$ has a unique $G_{\mathfrak{p}}$-extension $\widetilde{\sigma}$, and L_k is the fixed field of the group of all $\widetilde{\sigma}$ with $\sigma \in \mathrm{Aut}_k \mathbf{C}$.*

§20. Now we shall prove that Theorem 5 is reduced to Theorem 4. Let L be a quasi-irreducible $G_{\mathfrak{p}}$-field over $\mathbf{C}$, and assume that L contains a full $G_{\mathfrak{p}}$-subfield L_k over an algebraic number field k. Then every element of $\mathrm{Aut}_k \mathbf{C}$ has a unique $G_{\mathfrak{p}}$-extension. Therefore, if we denote by H the group [9] of all $\sigma \in \mathrm{Aut}\,\mathbf{C}$ which have $G_{\mathfrak{p}}$-extensions $\widetilde{\sigma}$, we have $\mathrm{Aut}\,\mathbf{C} \supset H \supset \mathrm{Aut}_k \mathbf{C}$. But $[k : \mathbf{Q}]$ is finite, and hence H is of the form $H = \mathrm{Aut}_{k_0} \mathbf{C}$ with some intermediate field k_0; $\mathbf{Q} \subset k_0 \subset k$. Put

$$
\mathcal{G}_{k_0} = \{\widetilde{\sigma} | \sigma \in \mathrm{Aut}_{k_0} \mathbf{C}\}, \tag{42}
$$

[9] See (41).

and let L_{k_0} be the fixed field of the group $\mathcal{G}_{k_0}$. We shall prove that L_{k_0} is the desired smallest full $G_{\mathfrak{p}}$-subfield of L over k_0. First, it is clear that L_{k_0} is $G_{\mathfrak{p}}$-invariant and that $L_{k_0} \cap \mathbf{C} = k_0$. Secondly, $\mathcal{G}_{k_0}$ contains

$$\mathcal{G}_k = \{\widetilde{\sigma} | \sigma \in \mathrm{Aut}_k \mathbf{C}\}, \text{ and } (\mathcal{G}_{k_0} : \mathcal{G}_k) = [k : k_0] < \infty.$$

Moreover, L_k is the fixed field of $\mathcal{G}_k$ (Proposition 5). Therefore, if we put

$$\mathcal{G}_{k_0} = \sum_{i=1}^{d} \widetilde{\sigma}_i \mathcal{G}_k \quad (d = (\mathcal{G}_{k_0} : \mathcal{G}_k) = [k : k_0]),$$

then for every $x \in L_k$, the elementary symmetric functions of $\widetilde{\sigma}_1(x), \cdots, \widetilde{\sigma}_d(x)$ are contained in L_{k_0}. Therefore we get $[L_{k_0}(x) : L_{k_0}] \leq d$ for all $x \in L_k$, and hence $[L_k : L_{k_0}] \leq d$. But by Proposition 2, L_{k_0} and $\mathbf{C}$ are linearly disjoint over k_0; hence $[L_{k_0} \cdot k : L_{k_0}] = [k : k_0] = d$. Therefore, $L_{k_0} \cdot k = L_k$, and hence $L_{k_0} \cdot \mathbf{C} = L$. Therefore, L_{k_0} is a full $G_{\mathfrak{p}}$-subfield of L over k_0. Now let $L_{k'}$ be an arbitrary full $G_{\mathfrak{p}}$-subfield of L over a field $k' \subset \mathbf{C}$. Then by Proposition 5, every element of $\mathrm{Aut}_{k'} \mathbf{C}$ has a $G_{\mathfrak{p}}$-extension, and hence $k' \supset k_0$. Moreover, by the same proposition, $L_{k'}$ is unique, and hence it must coincide with $L_{k_0} \cdot k'$. Conversely, if k' is a subfield of $\mathbf{C}$ containing k_0, then $L_{k_0} \cdot k'$ gives the (unique) full $G_{\mathfrak{p}}$-subfield of L over k'. Therefore, L_{k_0} has all the properties stated in Theorem 5. That such L_{k_0} is unique is obvious. *So, Theorem 5 is reduced to Theorem 4.*

REMARK. Consider the group of all automorphisms of L that commute with the actions of all elements of $G_{\mathfrak{p}}$. Then since $\mathbf{C}$ is the fixed field of $G_{\mathfrak{p}}$, such automorphisms leave $\mathbf{C}$ invariant (as a whole). Therefore, by the definitions of k_0 and $\mathcal{G}_{k_0}$, this group coincides with $\mathcal{G}_{k_0}$. Therefore, L_{k_0} is the fixed field of the centralizer of $G_{\mathfrak{p}}$ in $\mathrm{Aut}\, L$. (The centralizer of $G_{\mathfrak{p}}$ in $\mathrm{Aut}_{\mathbf{C}}\, L$ is trivial because of the quasi-irreducibility assumption on L.)

Preliminaries for the proof of Theorem 4.

§21. Before describing the method for the proof of Theorem 4, we need some definitions. Let L be a $G_{\mathfrak{p}}$-field over $\mathbf{C}$. Let $V_1, \cdots, V_n$ be any finite set of open compact subgroups of $G_{\mathfrak{p}}$ which generate $G_{\mathfrak{p}}$. Put $V_0 = \bigcap_{i=1}^{n} V_i$, and let L_i $(0 \leq i \leq n)$ be the fixed field of V_i in L. Then it is clear that L_0 contains $L_1, \cdots, L_n$ and is generated by them. Moreover,

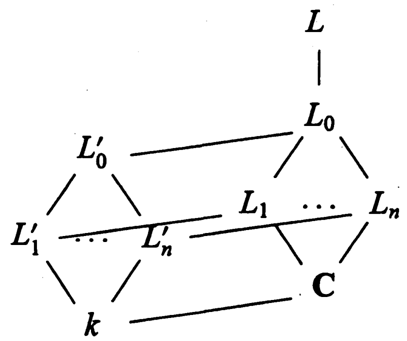
(#) *L is the smallest algebraic extension of L_0 that is normal over all L_i $(1 \leq i \leq n)$.*

In fact, if M is any algebraic extension of L_0 with this property, then $M \cap L$ also satisfies this property. But since $L \supset M \cap L \supset L_0$, $M \cap L$ corresponds to a compact subgroup Δ of V_0. Since $M \cap L/L_i$ are normal, Δ is a normal subgroup of V_i for all i. But V_i $(0 \leq i \leq n)$ generate $G_{\mathfrak{p}}$. Therefore, Δ is a normal subgroup of $G_{\mathfrak{p}}$. But Δ is compact and $G_{\mathfrak{p}}$ is simple. Hence $\Delta = \{1\}$, so that $M \cap L = L$, hence $M \supset L$. Therefore, L is characterized as the smallest algebraic extension of L_0 which is normal over all L_i $(0 \leq i \leq n)$. This characterization will be used later.

$$\begin{tikzcd}
 & L \arrow[d, dash] \arrow[rrrr, leftrightarrow] & & & & \{I\} \arrow[d, dash] & \\
 & M \cap L \arrow[d, dash] \arrow[rrrr, leftrightarrow] & & & & \Delta \arrow[d, dash] & \\
 & L_0 \arrow[dl, dash] \arrow[dr, dash] \arrow[rrrr, leftrightarrow] & & & & V_0 \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & \cdots & L_n \arrow[dl, dash] & \Longleftrightarrow & V_1 \arrow[dr, dash] & \cdots & V_n \arrow[dl, dash] \\
 & \mathbf{C} & & & & G_p &
\end{tikzcd}$$

Let V_i and L_i $(0 \leq i \leq n)$ be as above, and let k be a subfield of $\mathbf{C}$. We shall call a system $\{L_i' | 0 \leq i \leq n\}$ of subfields of L_0 *a k-form* of $\{L_i | 0 \leq i \leq n\}$ if the following conditions are satisfied:

(i) $L_i' \cdot \mathbf{C} = L_i$, $L_i' \cap \mathbf{C} = k \, (0 \leq i \leq n)$
(ii) $L_0' \supset L_i' \; (1 \leq i \leq n)$
(iii) L_0' and $\mathbf{C}$ are linearly disjoint over k.



§22. Now our method for the proof of Theorem 4 is as follows. First, we shall prove that if k is a subfield of $\mathbf{C}$ such that $\{L_i | 0 \leq i \leq n\}$ has a k-form, then L contains a full G_p-subfield over a finite extension of k. The method is algebraic, and is applicable to G_p-fields over any constant field. Secondly, we put

$$n = 2, \quad V_1 = PSL_2(O_p), \quad V_2 = \omega^{-1} V_1 \omega \quad \text{where } \omega = \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}$$

and π is a prime element of k_p, and prove that the corresponding $\{L_i | 0 \leq i \leq 2\}$ has a k-form for some algebraic number field k. Here, the method is analytic, i.e., it is based on the one-to-one correspondence between L and Γ (Theorem 1, §9). The reason for this particular choice of V_1 and V_2 is that G_p is a free product of V_1 and V_2 with amalgamated subgroup $V_1 \cap V_2$ (see Lemma 7, §28). This fact is an essential point in our proof.

§23. Thus, our first step is to prove the following proposition.

PROPOSITION 6. *Let L be a G_p-field over $\mathbf{C}$, and let k be a subfield of $\mathbf{C}$. Let V_i $(1 \leq i \leq n)$ be a set of open compact subgroups of G_p which generate G_p, and put $V_0 = \bigcap_{i=1}^n V_i$. Let L_i $(0 \leq i \leq n)$ be the fixed fields of V_i in L. Then if $\{L_i | 0 \leq i \leq n\}$ has a k-form, L contains a full G_p-subfield over a finite extension of k.*

To prove this, we need several lemmas.

§24.

LEMMA 3. *Let V be an open compact subgroup of $G_{\mathfrak{p}} = PSL_2(k_{\mathfrak{p}})$, and let $\mathcal{V}$ be the set of all subgroups of $G_{\mathfrak{p}}$ of the form $\bigcap_{i=1}^n x_i^{-1}Vx_i$ with $n \geq 1$ and $x_1, \cdots, x_n \in G_{\mathfrak{p}}$. Then $\mathcal{V}$ forms a basis of neighborhoods of the identity of $G_{\mathfrak{p}}$.*

PROOF. Let $y_1, y_2, \cdots, y_n, \cdots$ be a set of representatives of the coset space $V\backslash G_{\mathfrak{p}}$ (which is clearly countable). Put $V_n = \bigcap_{i=1}^n y_i^{-1}Vy_i$ $(n \geq 1)$. Then we get a descending sequence of open compact subgroups $V_1 \supset V_2 \supset \cdots$. Since $\bigcap_{n=1}^\infty V_n = \bigcap_{x \in G_{\mathfrak{p}}} x^{-1}Vx$ is a compact normal subgroup of $G_{\mathfrak{p}}$ and since $G_{\mathfrak{p}}$ is a simple group, we get $\bigcap_{n=1}^\infty V_n = \{1\}$. Since all V_n are compact, this implies that for any open subset U of $G_{\mathfrak{p}}$ containing 1, there exists some n such that $V_n \subset U$. □

COROLLARY . *Let φ be an automorphism, as an abstract group, of $G_{\mathfrak{p}}$. If there is an open compact subgroup V of $G_{\mathfrak{p}}$ such that $V^\varphi = V$, then φ is bicontinuous.*

PROOF. Let $\mathcal{V}$ be as in Lemma 3. Then φ and φ^{-1} leave $\mathcal{V}$ invariant. □

LEMMA 4. *There exists a finite set of open compact subgroups $V_1, \cdots, V_n$ of $G_{\mathfrak{p}}$ such that $V_1, \cdots, V_n$ generate $G_{\mathfrak{p}}$ and that every automorphism φ of $G_{\mathfrak{p}}$ satisfying $V_i^\varphi = V_i$ for all i $(1 \leq i \leq n)$ is an inner automorphism by some element of $\bigcap_{i=1}^n V_i$.*

PROOF. Let $\sigma \in \mathrm{Aut}_{\mathbf{Q}_p} k_{\mathfrak{p}}$. Then σ acts on $PL_2(k_{\mathfrak{p}})$ in a natural manner, and leaves $G_{\mathfrak{p}} = PSL_2(k_{\mathfrak{p}})$, $U_{\mathfrak{p}} = PL_2(O_{\mathfrak{p}})$ and $G_{\mathfrak{p}} \cap U_{\mathfrak{p}} = PSL_2(O_{\mathfrak{p}})$ invariant. First, let us check:

$$\bigcap_{x \in G_{\mathfrak{p}}} x^{-1}U_{\mathfrak{p}}x^\sigma = \begin{cases} \{1\} & \cdots \sigma = 1, \\ \phi & \cdots \sigma \neq 1. \end{cases} \tag{43}$$

Let p be the characteristic of $O_{\mathfrak{p}}/\mathfrak{p}$, and put $z_m = \begin{pmatrix} p^m & 0 \\ 0 & p^{-m} \end{pmatrix}$ $(m \in \mathbf{Z})$. So, $z_m^\sigma = z_m$, and

$$z_m^{-1}U_{\mathfrak{p}}z_m \cap U_{\mathfrak{p}} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_{\mathfrak{p}} \,\middle|\, bp^{2m}, cp^{-2m} \in O_{\mathfrak{p}} \right\}.$$

Hence

$$\bigcap_{m=-\infty}^{\infty} z_m^{-1}U_{\mathfrak{p}}z_m^\sigma = \bigcap_{m=-\infty}^{\infty} z_m^{-1}U_{\mathfrak{p}}z_m = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in U_{\mathfrak{p}} \right\}.$$

Let this last group be denoted by W, and put $y_m = \begin{pmatrix} p^{-m} & p^{-m} \\ 0 & p^m \end{pmatrix}$ for $m \geq 0$. Then

$$W \cap \bigcap_{m=0}^{\infty} y_m^{-1}U_{\mathfrak{p}}y_m^\sigma = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in U_{\mathfrak{p}} \right\} = \{1\}.$$

Hence $\bigcap_{x \in G_{\mathfrak{p}}} x^{-1}U_{\mathfrak{p}}x^\sigma$ is either $\{1\}$ or ϕ. If $\sigma = 1$, then 1 is contained in the intersection; hence $\bigcap_{x \in G_{\mathfrak{p}}} x^{-1}U_{\mathfrak{p}}x^\sigma = \{1\}$ for $\sigma = 1$. If $\sigma \neq 1$, take $\alpha \in O_{\mathfrak{p}}$ such that $\alpha^\sigma \neq \alpha$. Then, there exists $m \geq 0$ such that $\alpha^\sigma - \alpha \not\equiv 0 \pmod{p^m}$. Put $z = \begin{pmatrix} p^{-m} & \alpha \\ 0 & p^{-m} \end{pmatrix}$. Then

$z^\sigma \cdot z^{-1} = \begin{pmatrix} 1 & \frac{\alpha^\sigma-\alpha}{p^m} \\ 0 & 1 \end{pmatrix} \notin U_p$; hence $z^{-1}U_p z^\sigma \not\ni 1$. Hence $\bigcap_{x\in G_p} x^{-1}U_p x^\sigma = \phi$ for $\sigma \neq 1$; which settles (43).

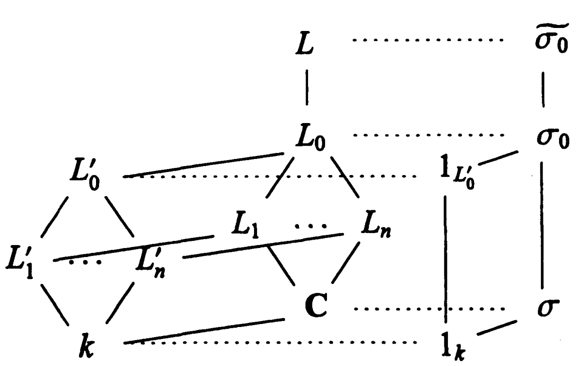
Now since $x^{-1}U_p x^\sigma$ are compact, and since $\mathrm{Aut}_{\mathbf{Q}_p} k_p$ is finite and $PSL_2(O_p)$ is an open set of $PL_2(k_p)$ containing 1, (43) implies that we can choose a finite set of elements $1 = x_1, \cdots, x_n$ of G_p such that

$$(44) \qquad \begin{cases} \bigcap_{i=1}^n x_i^{-1}U_p x_i^\sigma = \phi \ \text{ for all } \sigma \in \mathrm{Aut}_{\mathbf{Q}_p} k_p \ \text{ with } \sigma \neq 1, \text{ and} \\ \bigcap_{i=1}^n x_i^{-1}U_p x_i \subset PSL_2(O_p). \end{cases}$$

Put $V_1 = PSL_2(O_p) = x_1^{-1}PSL_2(O_p)x_1$, and $V_i = x_i^{-1}PSL_2(O_p)x_i = x_i^{-1}V_1 x_i$ $(1 \le i \le n)$. They are open compact subgroups of G_p. Now let φ be an automorphism of G_p satisfying $V_i^\varphi = V_i$ for all i $(1 \le i \le n)$. By the Corollary of Lemma 3, φ is a topological automorphism of G_p; hence by Lemma 1 (ii) (iii), φ is of the form $\sigma \cdot \varphi_x = \varphi_x \circ \sigma$, with $\sigma \in \mathrm{Aut}_{\mathbf{Q}_p} k_p$, $x \in PL_2(k_p)$, where $\varphi_x(y) = x^{-1}yx$ for all $y \in G_p$. Since $V_1^\sigma = V_1$, and since the normalizer of $V_1 = PSL_2(O_p)$ in $PL_2(k_p)$ is $U_p = PL_2(O_p)$ (as can be easily checked), $V_1^\varphi = V_1$ implies $x \in U_p$. Now since $V_i^\varphi = V_i$, we get $x^{-1}(x_i^\sigma)^{-1}V_1 x_i^\sigma x = x_i^{-1}V_1 x_i$; hence $x_i x^{-1}(x_i^\sigma)^{-1} \in U_p$; hence $x^{-1} \in x_i^{-1}U_p x_i^\sigma$ for all i $(1 \le i \le n)$. Therefore, by (44) we get $\sigma = 1$ and $x \in \bigcap_{i=1}^n x_i^{-1}U_p x_i \subset V_1$. Since $V_1 \cap x^{-1}U_p x \subset x^{-1}V_1 x$ for any $x \in G_p$, we get $x \in \bigcap_{i=1}^n x_i^{-1}V_1 x_i = \bigcap_{i=1}^n V_i$. Hence $\varphi = \varphi_x$ with $x \in \bigcap_{i=1}^n V_i$. Finally, it is clear by (44) that $x_i \notin U_p$ for some i; hence $V_i \neq V_1$ for some i. Hence the subgroup of G_p generated by $V_1, \cdots, V_n$ contains $V_1 = PSL_2(O_p)$ as a proper subgroup. But by Lemma 11 of Chapter 1, V_1 is a maximal subgroup of G_p. Therefore, $V_1, \cdots, V_n$ generate G_p; which completes the proof of Lemma 4. □

§25. The following lemma gives a criterion for the existence of a full G_p-subfield (of a G_p-field) over a given field $k \subset \mathbf{C}$.

LEMMA 5. *Let $V_1, \cdots, V_n$ be as in Lemma 4, and put $V_0 = \bigcap_{i=1}^n V_i$. Let L be a G_p-field over $\mathbf{C}$, let L_i $(0 \le i \le n)$ be the fixed field of V_i in L, and let k be a subfield of $\mathbf{C}$. Suppose that $\{L_i | 0 \le i \le n\}$ has a k-form $\{L_i' | 0 \le i \le n\}$. Then L contains a full G_p-subfield L' over k, satisfying $L' \cap L_i = L_i'$ for all i $(0 \le i \le n)$.*



PROOF. For each $\sigma \in \mathrm{Aut}_k \mathbf{C}$, put $\sigma_0 = 1_{L'_0} \otimes \sigma$. Then σ_0 is an automorphism of L_0, and we have $\sigma_0(L_i) = L_i$ for all i $(0 \leq i \leq n)$. Let $\widetilde{\sigma}_0$ be any extension of σ_0 to an *iso*morphism of L. Then, since L is the smallest algebraic extension of L_0 which is normal over $L_1, \cdots, L_n$ (see §21), the field $\widetilde{\sigma}_0(L)$ is the smallest algebraic extension of $\sigma_0(L_0) = L_0$ which is normal over $\sigma_0(L_i) = L_i$ for all i. Therefore, we get $\widetilde{\sigma}_0(L) = L$; hence $\widetilde{\sigma}_0$ is an *auto*morphism of L. Now $\widetilde{\sigma}_0$ defines an automorphism of the group $\mathrm{Aut}_{\mathbf{C}} L$ by

$$\mathrm{Aut}_{\mathbf{C}} L \ni \tau \mapsto \widetilde{\sigma}_0^{-1} \tau \widetilde{\sigma}_0 \in \mathrm{Aut}_{\mathbf{C}} L. \tag{45}$$

Since $G_{\mathfrak{p}}$ is a characteristic subgroup of $\mathrm{Aut}_{\mathbf{C}} L$ (Corollary 2 of Theorem 3), $G_{\mathfrak{p}}$ is invariant by this action of $\widetilde{\sigma}_0$. Moreover, since $\sigma_0(L_i) = L_i$ holds for all i, we get $\widetilde{\sigma}_0 V_i \widetilde{\sigma}_0^{-1} = V_i$ for all i (this also shows that $G_{\mathfrak{p}}$ is $\widetilde{\sigma}_0$-invariant). Therefore, $\widetilde{\sigma}_0$ induces an automorphism φ of $G_{\mathfrak{p}}$ which leaves all V_i invariant. Therefore, by Lemma 4, φ must be an inner automorphism by some element ρ of $V_0 = \bigcap_{i=1}^{\infty} V_i$. Therefore, $\widetilde{\sigma}_0^{-1} \tau \widetilde{\sigma}_0 = \rho^{-1} \tau \rho$ for all $\tau \in G_{\mathfrak{p}}$. Now put $\widetilde{\sigma} = \widetilde{\sigma}_0 \rho^{-1}$. Then $\widetilde{\sigma}$ is an automorphism of L which commutes with all elements of $G_{\mathfrak{p}}$ and whose restriction to L_0 coincides with σ_0. Since the centralizer of $G_{\mathfrak{p}}$ in $\mathrm{Aut}(L/L_0) = V_0$ is trivial, such $\widetilde{\sigma}$ is uniquely determined by σ_0, and hence also by σ (and L'_0). Therefore, we have $\widetilde{\sigma\tau} = \widetilde{\sigma}\widetilde{\tau}$ and $\widetilde{\sigma^{-1}} = \widetilde{\sigma}^{-1}$ for all $\sigma, \tau \in \mathrm{Aut}_k \mathbf{C}$. Let $\mathcal{G}$ be the group of all $\widetilde{\sigma}$ $(\sigma \in \mathrm{Aut}_k \mathbf{C})$, and let L' be the fixed field of $\mathcal{G}$ in L;

$$\begin{cases} \mathcal{G} = \{\widetilde{\sigma} \mid \sigma \in \mathrm{Aut}_k \mathbf{C}\} \\ L' = \{x \in L \mid \widetilde{\sigma}(x) = x, \ \forall \widetilde{\sigma} \in \mathcal{G}\}. \end{cases} \tag{46}$$

Then (since $\widetilde{\sigma}$ commutes with all elements of $G_{\mathfrak{p}}$) it is clear that L' is $G_{\mathfrak{p}}$-invariant, $L' \cap \mathbf{C} = k$, and that L' contains all L'_i $(0 \leq i \leq n)$. Put $M = L' \cdot \mathbf{C}$. Then M is $G_{\mathfrak{p}}$-invariant, and $M \supset L'_0 \cdot \mathbf{C} = L_0$. Therefore, M is the fixed field of some compact subgroup U of V_0. But since M is $G_{\mathfrak{p}}$-invariant, U must be a normal subgroup of $G_{\mathfrak{p}}$; hence $U = \{1\}$; hence $M = L$. Therefore, L' is a full $G_{\mathfrak{p}}$-subfield of L over k.

Finally, since L' contains L'_i, the inclusion $L' \cap L_i \supset L'_i$ is obvious. But L' and $\mathbf{C}$ are linearly disjoint over k; hence $L' \cap L_i$ and $\mathbf{C}$ are also linearly disjoint over k. Therefore, by $L'_i \cdot \mathbf{C} = L_i$, we get $L' \cap L_i = L'_i$; which completes the proof of Lemma 5. □

REMARK . A full $G_{\mathfrak{p}}$-subfield L' over k satisfying $L' \cap L_i = L'_i$ for all i $(0 \leq i \leq n)$ is moreover unique. In fact, if L'' is another such field, then it is the fixed field of the group of all $1_{L''} \otimes \sigma$ with $\sigma \in \mathrm{Aut}_k \mathbf{C}$ (Lemma 2). But since such $1_{L''} \otimes \sigma$ commute with all elements of $G_{\mathfrak{p}}$, and since the restriction to L_0 of such $1_{L''} \otimes \sigma$ is obviously $1_{L'_0} \otimes \sigma$, we get $\widetilde{\sigma} = 1_{L''} \otimes \sigma$, $\widetilde{\sigma}$ being as in the proof of the above Lemma. Therefore, L'' must be the fixed field of $\mathcal{G}$; hence $L'' = L'$. Therefore, L' is uniquely determined by $\{L'_i \mid 0 \leq i \leq n\}$.

Conversely, if L' is any full $G_{\mathfrak{p}}$-subfield of L over k, then by the Corollary of Proposition 2, it is clear that $\{L' \cap L_i | 0 \leq i \leq n\}$ gives a k-form of $\{L_i | 0 \leq i \leq n\}$. Therefore, *$k$-forms $\{L'_i | 0 \leq i \leq n\}$ of $\{L_i | 0 \leq i \leq n\}$ and full $G_{\mathfrak{p}}$-subfields L' of L over k correspond in a one-to-one manner by $L'_i = L' \cap L_i$ $(0 \leq i \leq n)$.* In particular, if L is quasi-irreducible, then L' is unique (if exists at all) by Proposition 5; hence $\{L'_i | 0 \leq i \leq n\}$ is also unique (if exists at all). Of course, we must not forget that these are under the assumption that the subgroups V_i $(1 \leq i \leq n)$ of $G_{\mathfrak{p}}$ satisfy the properties stated in Lemma 4.

§26.

Proof of Proposition 6. Now we shall prove Proposition 6 (§23). Let L_i $(0 \le i \le n)$ be as in Proposition 6, and let $\{L'_i | 0 \le i \le n\}$ be a k-form of $\{L_i | 0 \le i \le n\}$. Let M be the algebraic closure of L'_0 in L. We shall show that M is a full $G_{\mathfrak{p}}$-subfield of L over the algebraic closure $\bar{k}$ of k. First, let i be any index with $1 \le i \le n$, and let $x \in M$. Take any $v_i \in V_i$. Then since x is algebraic over L'_i, $v_i(x)$ is also algebraic over $v_i(L'_i) = L'_i$. Therefore, M is invariant by V_i. But since $G_{\mathfrak{p}}$ is generated by V_i $(1 \le i \le n)$, M is invariant by $G_{\mathfrak{p}}$. Secondly, since L'_0 and $\mathbf{C}$ are linearly disjoint over k, we get $M \cap \mathbf{C} = \bar{k}$. Finally, $M \cdot \mathbf{C}$ is a $G_{\mathfrak{p}}$-subfield of L over $\mathbf{C}$, and $M \cdot \mathbf{C}$ contains L_0. Therefore, $M \cdot \mathbf{C} = L$; so that M is a full $G_{\mathfrak{p}}$-subfield of L over $\bar{k}$.

Now take (a set of) open compact subgroups of $G_{\mathfrak{p}}$ *satisfying the properties stated in Lemma 4*, and call them $W_1, \cdots, W_m$. Put $W_0 = \bigcap_{j=1}^{m} W_j$, and let M_j $(0 \le j \le m)$ be the fixed field of W_j in M. Then by the Corollary of Proposition 2 (§3), $M_j\mathbf{C}$ is the fixed field of W_j in L, and $\{M_j \mid 0 \le j \le m\}$ is a $\bar{k}$-form of $\{M_j\mathbf{C} \mid 0 \le j \le m\}$. Now let C_j $(0 \le j \le m)$ be some affine models of M_j defined over $\bar{k}$, and let f_j $(1 \le j \le m)$ be the rational maps of C_0 onto C_j defined by the inclusion $M_0 \supset M_j$. Thus f_j are also defined over $\bar{k}$. Now, C_j and f_j are all defined over a subfield of $\bar{k}$ which is finitely generated over $\mathbf{Q}$, and therefore, they are defined over a finite extension k' of k. Let M'_j $(0 \le j \le m)$ be the field of k'-rational functions on C_j. Then it is clear that $\{M'_j \mid 0 \le j \le m\}$ is a k'-form of $\{M_j\mathbf{C} \mid 0 \le j \le m\}$, and hence by Lemma 5 there is a full $G_{\mathfrak{p}}$-subfield of L over k'. This proves Proposition 6. □

More lemmas.

§27. Now by Proposition 6, Theorem 4 is reduced [10] to the following:

Lemma 6 (Main lemma). *Put* $V_1 = PSL_2(O_{\mathfrak{p}})$, $V_2 = \omega^{-1}V_1\omega$ *and* $V_0 = V_1 \cap V_2$, *where* $\omega = \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}$ *and* π *is a prime element of* $k_{\mathfrak{p}}$. *Let* L *be a* $G_{\mathfrak{p}}$*-field over* $\mathbf{C}$, *and let* L_i $(0 \le i \le 2)$ *be the fixed field of* V_i. *Then* $\{L_i | 0 \le i \le 2\}$ *has a k-form for some algebraic number field k.*

For the proof of this, the following two lemmas, Lemma 7 (§28) and Lemma 8 (§29), are basic.

§28.

Lemma 7. *Let* V_i $(0 \le i \le 2)$ *be as in Lemma 6. Then* $G_{\mathfrak{p}}$ *is the free product of* V_1 *and* V_2 *with amalgamated subgroup* V_0.

[10] It is clear that V_1 and V_2 generate $G_{\mathfrak{p}}$, since V_1 is a maximal subgroup of $G_{\mathfrak{p}}$ (see Chapter 1, Lemma 11).

PROOF. Since V_2 consists of all elements of $G_\mathfrak{p}$ that are contained in $\begin{pmatrix} O_\mathfrak{p} & \mathfrak{p}^{-1} \\ \mathfrak{p} & O_\mathfrak{p} \end{pmatrix}$, we have

$$V_0 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in V_1 \;\middle|\; c \equiv 0 \pmod{\mathfrak{p}} \right\}.$$

Therefore, $(V_1 : V_0) = (V_2 : V_0) = q + 1$ (note that $\omega^{-1} V_2 \omega = V_1$, since $\omega^2 = \begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix}$). Put $X = PL_2(k_\mathfrak{p})$, $U_\mathfrak{p} = PL_2(O_\mathfrak{p})$ and

$$B_\mathfrak{p} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_\mathfrak{p} \;\middle|\; c \equiv 0 \pmod{\mathfrak{p}} \right\}.$$

Then $(U_\mathfrak{p} : B_\mathfrak{p}) = q+1$ and $B_\mathfrak{p} \cap V_1 = V_0$, and hence we have $U_\mathfrak{p} = B_\mathfrak{p} V_1$. Therefore, if $M_0 = 1, M_1, \cdots, M_q$ is a set of representatives of $V_0 \backslash V_1$, then it is also a set of representatives of $B_\mathfrak{p} \backslash U_\mathfrak{p}$. But since $B_\mathfrak{p} = U_\mathfrak{p} \cap \omega^{-1} U_\mathfrak{p} \omega$, we see immediately that $\omega M_0 = \omega, \omega M_1, \cdots, \omega M_q$ is a set of representatives of $U_\mathfrak{p} \backslash U_\mathfrak{p} \omega U_\mathfrak{p}$. Now for each $x \in X$, let $l(x)$ be the length of x (see Chapter 1, §15), and let X_l ($l = 0, 1, 2, \cdots$) be the set of all elements of X with length l. Then $X_0 = U_\mathfrak{p}$, $X_1 = U_\mathfrak{p} \omega U_\mathfrak{p}$, and therefore, $\omega M_0 = \omega, \omega M_1, \cdots, \omega M_q$ is a set of representatives of $X_0 \backslash X_1$. Put $\pi_i = \omega M_i$ ($0 \le i \le q$), and look at Lemma 5 of Chapter 1, §16. Then since $\pi_0 \pi_i = M_i \in U_\mathfrak{p} = X_0$ for all i, we see immediately by this Lemma that elements x of X are expressed *uniquely* in the form

$$x = u_\mathfrak{p} \omega M_{i_1} \omega M_{i_2} \cdots \omega M_{i_l},$$

with $u_\mathfrak{p} \in U_\mathfrak{p}$ and $i_\nu \neq 0$ for $\nu = 1, 2, \cdots, l-1$. But since $U_\mathfrak{p} = \sum_{i=0}^{q} B_\mathfrak{p} M_i$, this shows that *every element x of X is expressed uniquely in the form :*

$$x = b_\mathfrak{p} M_{i_0} \omega M_{i_1} \omega M_{i_2} \cdots \omega M_{i_l}, \quad b_\mathfrak{p} \in B_\mathfrak{p},\ i_\nu \neq 0\ (1 \le \nu \le l-1). \tag{47}$$

In this situation, moreover, l is the length of x (see Lemma 5 of Chapter 1). It is clear that x is contained in $G_\mathfrak{p} = PSL_2(k_\mathfrak{p})$ if and only if $l \equiv 0 \pmod 2$ and $b_\mathfrak{p} \in V_0$.

Now let $G'_\mathfrak{p}$ be the free product of V_1 and V_2 with amalgamated subgroup V_0. Then since $M_0 = 1, M_1, \cdots, M_q$ resp. $\omega^{-1} M_0 \omega = 1, \omega^{-1} M_1 \omega, \cdots, \omega^{-1} M_q \omega$ are the sets of representatives of $V_0 \backslash V_1$ resp. $V_0 \backslash V_2$, every element x' of $G'_\mathfrak{p}$ is expressed uniquely in the form

$$x' = v_0 M_{i_0} (\omega^{-1} M_{i_1} \omega) M_{i_2} (\omega^{-1} M_{i_3} \omega) M_{i_4} \cdots (\omega^{-1} M_{i_{l-1}} \omega) M_{i_l},$$

with $v_0 \in V_0$ and $i_\nu \neq 0$ for $\nu = 1, 2, \cdots, l-1$.[11] But since $\omega^2 = 1$ (when ω is considered as an element of X) *and since the expression* (47) *of the element of X is unique,* the natural homomorphism of $G'_\mathfrak{p}$ onto $G_\mathfrak{p}$ is injective. Therefore, $G_\mathfrak{p}$ is the free product of V_1 and V_2 with amalgamated subgroup V_0. □

REMARK . In the same manner by using the uniqueness of the expression (47), we can prove that $X = PL_2(k_\mathfrak{p})$ is the free product of $U_\mathfrak{p}$ and $B_\mathfrak{p} \cup B_\mathfrak{p} \omega$ with amalgamated subgroup $B_\mathfrak{p}$.

[11] Cf. Kurosh [**22**].

COROLLARY. *Let Γ_p be a dense subgroup of G_p and put $\Gamma_p^{(i)} = V_i \cap \Gamma_p$ $(i = 0, 1, 2)$, where V_i are as in Lemmas 6, 7. Then Γ_p is the free product of $\Gamma_p^{(1)}$ and $\Gamma_p^{(2)}$ with amalgamated subgroup $\Gamma_p^{(0)}$.*

PROOF. Since Γ_p is dense in G_p, it is clear that $\Gamma_p^{(1)}$ and $\Gamma_p^{(2)}$ generate Γ_p. Let $M_0 = 1, M_1, \cdots, M_q$ resp. $N_0 = 1, N_1, \cdots, N_q$ be sets of representatives of $\Gamma_p^{(0)}\backslash\Gamma_p^{(1)}$ resp. $\Gamma_p^{(0)}\backslash\Gamma_p^{(2)}$. Then they are at the same time sets of representatives of $V_0\backslash V_1$ resp. $V_0\backslash V_2$, and hence by Lemma 7, every element x of G_p is expressed uniquely in the form $x = v_0 M_{i_0} N_{i_1} M_{i_2} N_{i_3} \cdots N_{i_{l-1}} M_{i_l}$ with $v_0 \in V_0$ and $i_\nu \neq 0$ for $\nu = 1, 2, \cdots, l-1$. It is clear that $x \in \Gamma_p$ if and only if $v_0 \in \Gamma_p^{(0)}$. Therefore, Γ_p is the free product of $\Gamma_p^{(1)}$ and $\Gamma_p^{(2)}$ with amalgamated subgroup $\Gamma_p^{(0)}$. □

§29. This is the most crucial lemma in the proof of Theorem 4.

LEMMA 8.[12] *Let Γ be a discrete subgroup of $G = G_{\mathbf{R}} \times G_p$ whose quotient G/Γ is of finite invariant volume and whose projections $\Gamma_{\mathbf{R}}$, Γ_p are dense in $G_{\mathbf{R}}$, G_p respectively. Let φ be a homomorphism (as abstract groups) of $\Gamma_{\mathbf{R}}$ into $G_{\mathbf{R}}$ such that for some open compact subgroup V of G_p, $\varphi|_{\Gamma_{\mathbf{R}}^V}$ is injective, $\varphi(\Gamma_{\mathbf{R}}^V)$ is discrete in $G_{\mathbf{R}}$, and the quotient $G_{\mathbf{R}}/\varphi(\Gamma_{\mathbf{R}}^V)$ is of finite invariant volume. Then, there is an element $x \in G'_{\mathbf{R}} = PL_2(\mathbf{R})$ such that $\varphi(\gamma_{\mathbf{R}}) = x^{-1}\gamma_{\mathbf{R}}x$ for all $\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}}$.*

PROOF. The proof of Lemma 8 is divided into four steps, as follows.

(i) To prove that φ is injective, and that if we put

$$\Gamma' = \{\varphi(\gamma_{\mathbf{R}}) \times \gamma_p \in G \mid \gamma_{\mathbf{R}} \times \gamma_p = \gamma \in \Gamma\}, \tag{48}$$

then Γ' is also a discrete subgroup of G satisfying the same conditions as Γ.

(ii) To prove that $\varphi(\gamma_{\mathbf{R}})$ is elliptic [13] if and only if $\gamma_{\mathbf{R}}$ is elliptic.

(iii) To prove that if φ is any injective homomorphism (as abstract groups) of $\Gamma_{\mathbf{R}}$ into $G_{\mathbf{R}}$ satisfying the property (ii), then $\varphi : \Gamma_{\mathbf{R}} \to \varphi(\Gamma_{\mathbf{R}})$ is bicontinuous.

(iv) To show that such φ as in (iii) are induced by some inner automorphisms of $G'_{\mathbf{R}} = PL_2(\mathbf{R})$.

Proof of (i). Let $\Delta_{\mathbf{R}}$ be the kernel of φ. Then $\Delta_{\mathbf{R}}$ is normal in $\Gamma_{\mathbf{R}}$, and since $\varphi|_{\Gamma_{\mathbf{R}}^V}$ is injective, $\Delta_{\mathbf{R}} \cap \Gamma_{\mathbf{R}}^V = \{I\}$. Let Δ_p be the subgroup of Γ_p corresponding to $\Delta_{\mathbf{R}}$ by the canonical identification $\Gamma_{\mathbf{R}} \cong \Gamma_p$. Then Δ_p is normal in Γ_p and $\Delta_p \cap V = \{I\}$; hence Δ_p is a discrete normal subgroup of the topological closure of Γ_p, i.e., G_p. But G_p is simple. Therefore, $\Delta_p = \{I\}$; hence $\Delta_{\mathbf{R}} = \{I\}$, so that φ is injective. Since $(\Gamma_{\mathbf{R}} : \Gamma_{\mathbf{R}}^V) = (G_p : V) = \infty$, we get $(\varphi(\Gamma_{\mathbf{R}}) : \varphi(\Gamma_{\mathbf{R}}^V)) = \infty$; and since $\varphi(\Gamma_{\mathbf{R}}^V)$ is a discrete subgroup of $G_{\mathbf{R}}$ whose quotient has finite invariant volume, $\varphi(\Gamma_{\mathbf{R}})$ must be dense [14] in $G_{\mathbf{R}}$. Now (i) is a direct consequence of Proposition 2 (Chapter 1, §2).

Proof of (ii). This is a direct consequence of the following lemma.

[12]As is shown later (§30), if the quotient G/Γ is compact, then all small deformations φ of $\Gamma_{\mathbf{R}}$ in $G_{\mathbf{R}}$ satisfy the conditions given in the lemma.

[13]As in Chapter 1, an element $g_{\mathbf{R}}$ of $G_{\mathbf{R}}$ is called elliptic if $|\operatorname{tr} g_{\mathbf{R}}| < 2$.

[14]See Supplement §1.

LEMMA 9. *Let Γ be as in Lemma 8, and let $\gamma = \gamma_{\mathbf{R}} \times \gamma_{\mathfrak{p}} \in \Gamma$. Then $\gamma_{\mathbf{R}}$ is elliptic if and only if the centralizer of $\gamma_{\mathfrak{p}}$ in $\Gamma_{\mathfrak{p}}$ is discrete in $G_{\mathfrak{p}}$.*

It is clear that Lemma 9 implies (ii) at once. In fact, by applying Lemma 9 to Γ and Γ', we see immediately that $\gamma_{\mathbf{R}}$ or $\varphi(\gamma_{\mathbf{R}})$ is elliptic if and only if the centralizer of $\gamma_{\mathfrak{p}}$ in $\Gamma_{\mathfrak{p}}$ is discrete in $G_{\mathfrak{p}}$ (note that $\Gamma'_{\mathfrak{p}} = \Gamma_{\mathfrak{p}}$). Therefore, $\varphi(\gamma_{\mathbf{R}})$ is elliptic if and only if $\gamma_{\mathbf{R}}$ is so.

PROOF OF LEMMA 9. In general, for any element x of any group X, we denote by X_x the centralizer of x in X. Let $\gamma' = \gamma'_{\mathbf{R}} \times \gamma'_{\mathfrak{p}}$ be any element of Γ. Then since the projections $\Gamma \to \Gamma_{\mathbf{R}}$ and $\Gamma \to \Gamma_{\mathfrak{p}}$ are injective (Proposition 1 of Chapter 1, §2), we see that γ' commutes with γ if and only if $\gamma'_{\mathbf{R}}$ commutes with $\gamma_{\mathbf{R}}$, and if and only if $\gamma'_{\mathfrak{p}}$ commutes with $\gamma_{\mathfrak{p}}$. Hence we get

$$(\Gamma_{\mathbf{R}})_{\gamma_{\mathbf{R}}} = (\Gamma_\gamma)_{\mathbf{R}} \cong \Gamma_\gamma \cong (\Gamma_\gamma)_{\mathfrak{p}} = (\Gamma_{\mathfrak{p}})_{\gamma_{\mathfrak{p}}} \quad \text{(canonically)}.$$

Now let $\gamma_{\mathbf{R}}$ be elliptic. Then $(G_{\mathbf{R}})_{\gamma_{\mathbf{R}}}$ is compact; hence $(\Gamma_\gamma)_{\mathbf{R}}$ is relatively compact in $G_{\mathbf{R}}$. Therefore, by the discreteness of Γ_γ in G, $(\Gamma_\gamma)_{\mathfrak{p}}$ must be discrete in $G_{\mathfrak{p}}$.

To prove the converse, we need the following assertion:
(b) *If $\gamma \in \Gamma$, then G_γ/Γ_γ has finite invariant volume. Moreover, if $\gamma \neq 1$, then G_γ/Γ_γ is compact.*

The second assertion follows immediately from the first because of the special simple structure of G_γ. The proof of (b) is simple if G/Γ is compact. In fact, put $G = K \cdot \Gamma$ with some compact subset K of G. Let $\gamma_0 \in \Gamma$ and $g \in G_{\gamma_0}$. Put $g = k \cdot \gamma$ with $k \in K$, $\gamma \in \Gamma$. Then, by $g\gamma_0 = \gamma_0 g$ we get $k^{-1}\gamma_0 k = \gamma\gamma_0\gamma^{-1} \in K^{-1}\gamma_0 K$. Since $K^{-1}\gamma_0 K$ is compact, the intersection $\Gamma \cap K^{-1}\gamma_0 K$ is finite, and hence the intersection $\{\gamma_0\}_\Gamma \cap K^{-1}\gamma_0 K$ is also finite. Put

$$\{\gamma_0\}_\Gamma \cap K^{-1}\gamma_0 K = \{\gamma_i\gamma_0\gamma_i^{-1} \mid \gamma_i \in \Gamma,\ i = 1, 2, \cdots, n\}.$$

Then $\gamma\gamma_0\gamma^{-1} = \gamma_i\gamma_0\gamma_i^{-1}$ for some i $(1 \le i \le n)$, and hence γ is contained in $\gamma_i\Gamma\gamma_0$. Therefore, $g \in K\gamma_i\Gamma\gamma_0$. Hence we get $G\gamma_0 \subset \bigcup_{i=1}^n K\gamma_i\Gamma\gamma_0$; hence $G_{\gamma_0}/\Gamma_{\gamma_0}$ is compact. On the other hand, if G/Γ is non-compact, the proof of (b) is not so simple (but it is elementary, because we know much about discrete subgroups of $G_{\mathbf{R}}$ whose quotients are of finite invariant volume). This is left to the readers.

Now suppose that $(\Gamma_\gamma)_{\mathfrak{p}}$ is discrete in $G_{\mathfrak{p}}$. Then $\gamma \neq 1$, and hence G_γ/Γ_γ is compact. Put, therefore, $G_\gamma = X \cdot \Gamma_\gamma$ with some compact subset X of G_γ. Take any $g_{\gamma,\mathbf{R}} \in (G_\gamma)_{\mathbf{R}} = (G_{\mathbf{R}})_{\gamma_{\mathbf{R}}}$, and put $g_{\gamma,\mathbf{R}} \times 1_{\mathfrak{p}} = x \cdot \delta$ with $x \in X$ and $\delta \in \Gamma_\gamma$, where $1_{\mathfrak{p}}$ is the identity element of $G_{\mathfrak{p}}$. Then we have $x_{\mathfrak{p}}\delta_{\mathfrak{p}} = 1_{\mathfrak{p}}$, and hence $\delta_{\mathfrak{p}} \in X_{\mathfrak{p}}^{-1}$. But since $(\Gamma_\gamma)_{\mathfrak{p}}$ is discrete, the intersection $X_{\mathfrak{p}}^{-1} \cap (\Gamma_\gamma)_{\mathfrak{p}}$ must be finite, so that we can put

$$X_{\mathfrak{p}}^{-1} \cap (\Gamma_\gamma)_{\mathfrak{p}} = \{\delta_{1\mathfrak{p}}, \cdots, \delta_{n\mathfrak{p}}\}$$

with some $\delta_i \in \Gamma_\gamma$ $(1 \le i \le n)$. Then $g_{\gamma,\mathbf{R}} = x_{\mathbf{R}}\delta_{i\mathbf{R}}$ with some i $(1 \le i \le n)$, and hence $(G_\gamma)_{\mathbf{R}} \subset \bigcup_{i=1}^n X_{\mathbf{R}}\delta_{i\mathbf{R}}$. Therefore, $(G_\gamma)_{\mathbf{R}}$ is compact, and hence $\gamma_{\mathbf{R}}$ is elliptic. □

Proof of (iii). This is a direct consequence of the following lemma.

LEMMA 10. *Let $\gamma_1, \gamma_2, \gamma_3, \cdots$ be any sequence in $\Gamma_{\mathbf{R}}$. Then, it converges to 1 if and only if for any elliptic element $\delta \in \Gamma_{\mathbf{R}}$, $\gamma_n \cdot \delta$ are elliptic for all sufficiently large n.*

It is clear that Lemma 10 implies (iii), *since the convergence of sequence is characterized in terms of ellipticity of elements, which is invariant by φ.*

Proof of Lemma 10. Since $g_{\mathbf{R}} \in G_{\mathbf{R}}$ is elliptic if and only if $|\operatorname{tr} g_{\mathbf{R}}| < 2$, the set of all elliptic elements of $G_{\mathbf{R}}$ forms an open set. Therefore, if $\delta \in \Gamma_{\mathbf{R}}$ is elliptic and if $\gamma_1, \gamma_2, \cdots$ converges to 1, then $\gamma_n\delta$ are elliptic for all sufficiently large n. This proves that the condition is necessary.

To prove the sufficiency, we first remark that there exist $\delta_1, \delta_2, \delta_3, \delta_4 \in \Gamma_{\mathbf{R}}$ such that δ_i $(1 \le i \le 4)$ are elliptic and that they are additively linearly independent over $\mathbf{R}$. In fact, put

$$g_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, g_2 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, g_3 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, g_4 = \begin{pmatrix} 0 & -2 \\ \frac{1}{2} & 0 \end{pmatrix}. \tag{49}$$

Then $g_1, g_2, g_3, g_4 \in G_{\mathbf{R}}$ are elliptic and are linearly independent over $\mathbf{R}$. Since $\Gamma_{\mathbf{R}}$ is dense in $G_{\mathbf{R}}$, we can take $\delta_1, \delta_2, \delta_3, \delta_4 \in \Gamma_{\mathbf{R}}$ sufficiently near g_1, g_2, g_3, g_4 respectively. Then, it is clear that δ_i $(1 \le i \le 4)$ satisfy the desired conditions. Put

$$\Pi = \{x \in G_{\mathbf{R}} \mid |\operatorname{tr}(x\delta_i)| < 2 \text{ for } i = 1, 2, 3, 4\}. \tag{50}$$

Then, since the map

$$M_2(\mathbf{R}) \ni x \mapsto (\operatorname{tr}(x\delta_1), \cdots, \operatorname{tr}(x\delta_4)) \in \mathbf{R}^4 \tag{51}$$

gives an isomorphism of the two vector spaces over $\mathbf{R}$, it is clear that Π is relatively compact in $G_{\mathbf{R}}$.

Now let $\gamma_1, \gamma_2, \cdots$ be a sequence in $\Gamma_{\mathbf{R}}$ such that for any elliptic element $\delta \in \Gamma_{\mathbf{R}}$, $\gamma_n\delta$ are elliptic for all sufficiently large n. Since δ_i $(1 \le i \le 4)$ are elliptic, this implies that γ_n are contained in Π for all large n. Since the closure $\overline{\Pi}$ of Π in $G_{\mathbf{R}}$ is compact, the sequence $\gamma_1, \gamma_2, \cdots$ must have at least one accumulating point in $\overline{\Pi}$. Let $\xi \in G_{\mathbf{R}}$ be any accumulating point of $\gamma_1, \gamma_2, \cdots$. If we can show $\xi = 1$, the proof will be completed. Let $\delta \in \Gamma_{\mathbf{R}}$ be any elliptic element. Then $\gamma_n\delta$ are elliptic for all large n, and $\xi\delta$ is an accumulating point of $\gamma_1\delta, \gamma_2\delta, \cdots$. Therefore we get $|\operatorname{tr}(\xi\delta)| \le 2$. Since $\Gamma_{\mathbf{R}}$ is dense in $G_{\mathbf{R}}$, this implies that $|\operatorname{tr}(\xi g_{\mathbf{R}})| \le 2$ for any elliptic element $g_{\mathbf{R}}$ of $G_{\mathbf{R}}$. Put

$$\xi = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \ g_{\mathbf{R}} = \begin{pmatrix} 0 & -y \\ \frac{1}{y} & 0 \end{pmatrix} \text{ with } y \in \mathbf{R}^{\times}.$$

Then $g_{\mathbf{R}}$ is elliptic, and $\operatorname{tr}(\xi g_{\mathbf{R}}) = \frac{b}{y} - cy$. If $b \neq 0$, let $|y|$ be sufficiently small, and if $c \neq 0$, let $|y|$ be sufficiently large. Then in either case, we get a contradiction to $|\operatorname{tr}(\xi g_{\mathbf{R}})| \le 2$. Therefore $b = c = 0$; hence $\xi = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. Now, since $|\operatorname{tr}(\xi g_{\mathbf{R}})| \le 2$ holds for all elliptic elements $g_{\mathbf{R}}$ which are sufficiently near 1, we get $|a + a^{-1}| \le 2$. But this is impossible unless $a = a^{-1} = \pm 1$, since a, a^{-1} are real. Hence we get $\xi = 1$ (as an element of $G_{\mathbf{R}}$), which completes the proof of Lemma 10. □

Proof of (iv). Now, φ is a bicontinuous map of $\Gamma_{\mathbf{R}}$ onto $\varphi(\Gamma_{\mathbf{R}})$. Therefore, φ can be extended to a bicontinuous map $\overline{\varphi}$ of $\overline{\Gamma_{\mathbf{R}}} = G_{\mathbf{R}}$ onto $\overline{\varphi(\Gamma_{\mathbf{R}})} \subset G_{\mathbf{R}}$. Since every homomorphism of a Lie group into another is analytic, so is $\overline{\varphi}$; and since $\overline{\varphi}$ has no kernel (since $G_{\mathbf{R}}$

is simple) and $G_{\mathbf{R}}$ is connected, $\widetilde{\varphi}$ must be surjective. Therefore, $\widetilde{\varphi}$ is an analytic automorphism of $G_{\mathbf{R}}$; hence it is an inner automorphism by some element of $G'_{\mathbf{R}} = PL_2(\mathbf{R})$. This completes the proof of Lemma 8. □

§30. We remark here that in the case where G/Γ is compact, Lemma 8 has a direct consequence, "the triviality of deformation of $\Gamma_{\mathbf{R}}$ in $G_{\mathbf{R}}$". This fact, however, is not necessary for our present purpose.

Corollary of Lemma 8 . *Let Γ be as in Lemma 8, and assume moreover that the quotient G/Γ is compact. Then $\Gamma_{\mathbf{R}}$ has no non-trivial deformation in $G_{\mathbf{R}}$.*

Here, by "$\Gamma_{\mathbf{R}}$ has no non-trivial deformation in $G_{\mathbf{R}}$", we mean the following. In general, let X be any topological group, and let Δ be a finitely generated subgroup of X with a set of generators $\delta_1, \cdots, \delta_r$. By "small deformation of Δ in X", we mean any homomorphism φ of the *abstract group* Δ into X, such that $\varphi(\delta_1), \cdots, \varphi(\delta_r)$ are sufficiently near $\delta_1, \cdots, \delta_r$ respectively. We use this terminology only in the form: "if φ is a small deformation of Δ in X, then $\cdots$ holds;" which implies that there exist some neighborhoods $U_1, \cdots, U_r$ of $\delta_1, \cdots, \delta_r$ respectively such that if $\varphi(\delta_i) \in U_i$ $(1 \le i \le r)$, then $\cdots$ holds. It is clear that this definition is independent of the choice of the set of generators $\delta_1, \cdots, \delta_r$. We shall say that Δ has no non-trivial deformation in X if every small deformation φ of Δ in X is induced by some inner automorphism of X; i.e., if there exists some neighborhood $U_1, \cdots, U_r$ of $\delta_1, \cdots, \delta_r$ respectively such that every homomorphism φ of the abstract group Δ into X satisfying $\varphi(\delta_i) \in U_i$ for all i $(1 \le i \le r)$ is given by $\varphi(\delta) = t_\varphi^{-1}\delta t_\varphi$ (for all $\delta \in \Delta$) with some $t_\varphi \in X$.

We must check that $\Gamma_{\mathbf{R}}$ is finitely generated before we can speak of the deformation of $\Gamma_{\mathbf{R}}$. Put $\Gamma^0 = \Gamma \cap (G_{\mathbf{R}} \times V_1)$, where $V_1 = PSL_2(O_{\mathfrak{p}})$. Then $\Gamma^0_{\mathbf{R}}$ is a discrete subgroup of $G_{\mathbf{R}}$ and the quotient $G_{\mathbf{R}}/\Gamma^0_{\mathbf{R}}$ has finite invariant volume; hence $\Gamma^0 \cong \Gamma^0_{\mathbf{R}}$ is finitely generated. On the other hand, since Γ^0 is maximal in Γ (Corollary of Lemma 11 in Chapter 1), Γ is generated by Γ^0 and γ, where γ is any element of Γ not contained in Γ^0. Therefore, by the isomorphisms $\Gamma \cong \Gamma_{\mathbf{R}}$ and $\Gamma^0 \cong \Gamma^0_{\mathbf{R}}$ (canonically), we get the finite generatedness of $\Gamma_{\mathbf{R}}$.

Proof of the Corollary of Lemma 8. In general, it is known that if X is a connected real Lie group and Δ is a finitely generated discrete subgroup of X with compact quotient, and if φ is a small deformation of Δ in X, then φ is injective, $\varphi(\Delta)$ is discrete in X, and the quotient $X/\varphi(\Delta)$ is compact (cf. A. Weil [**36**]). Let Γ be as in Lemma 8, and apply this for $X = G_{\mathbf{R}}$ and $\Delta = \Gamma^V_{\mathbf{R}}$ (note that since G/Γ is compact, $G_{\mathbf{R}}/\Gamma^V_{\mathbf{R}}$ is also compact by Proposition 2 of Chapter 1), where V is any open compact subgroup of $G_{\mathfrak{p}}$ and $\Gamma^V = \Gamma \cap (G_{\mathbf{R}} \times V)$. Let φ be any small deformation of $\Gamma_{\mathbf{R}}$ in $G_{\mathbf{R}}$. Then $\varphi|_{\Gamma^V_{\mathbf{R}}}$ is also a small deformation of $\Gamma^V_{\mathbf{R}}$ in $G_{\mathbf{R}}$; hence $\varphi|_{\Gamma^V_{\mathbf{R}}}$ is injective, $\varphi(\Gamma^V_{\mathbf{R}})$ is discrete in $G_{\mathbf{R}}$, and the quotient $G_{\mathbf{R}}/\varphi(\Gamma^V_{\mathbf{R}})$ is compact. Therefore, by Lemma 8 there exists $x \in G'_{\mathbf{R}}$ such that $\varphi(\gamma_{\mathbf{R}}) = x^{-1}\gamma_{\mathbf{R}}x$ for all $\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}}$. But since φ is a small deformation, x must be near 1; hence $x \in G_{\mathbf{R}}$, and hence φ is a trivial deformation. □

Proof of Theorem 4 (Conclusion).

§31. Now we have come to the final stage of the proof of Theorem 4. It is enough to prove the Main lemma (§27). Let

$$V_1 = PSL_2(O_{\mathfrak{p}}),\ V_2 = \omega^{-1}V_1\omega\ \left(\omega = \begin{pmatrix} 0 & 1 \\ \pi & 0 \end{pmatrix}, O_{\mathfrak{p}}\pi = \mathfrak{p}\right),$$

and put $V_0 = V_1 \cap V_2$. Let L be a $G_{\mathfrak{p}}$-field over $\mathbf{C}$ and let L_i $(0 \le i \le 2)$ be the fixed field of V_i in L. Let $\mathfrak{R}_i$ $(0 \le i \le 2)$ be a complete non-singular model of L_i, and let f_i $(i = 1, 2)$ be the rational map of $\mathfrak{R}_0$ onto $\mathfrak{R}_i$ defined by the inclusion $L_0 \supset L_i$. Thus we get an algebraico-geometric object:

$$(52) \qquad \mathfrak{R}: \begin{array}{ccc} & \mathfrak{R}_0 & \\ {\scriptstyle f_1}\swarrow & & \searrow{\scriptstyle f_2} \\ \mathfrak{R}_1 & & \mathfrak{R}_2 \end{array}.$$

Let Γ be the discrete subgroup of $G = G_{\mathbf{R}} \times G_{\mathfrak{p}}$ which corresponds to L by Theorem 1 (§9). Put $\Gamma^i = \Gamma \cap (G_{\mathbf{R}} \times V_i)$ $(0 \le i \le 2)$. Then for each i, $\mathfrak{R}_i$ can be identified with the normalized and compactified quotient $\mathfrak{H}/\Gamma^i_{\mathbf{R}}$, where $\mathfrak{H}$ is the complex upper half plane. To show the idea of proof in a primitive form, let us assume for the time being that $\Gamma^0_{\mathbf{R}}$ is torsion-free and $G_{\mathbf{R}}/\Gamma^0_{\mathbf{R}}$ (or equivalently G/Γ) is compact. So, the natural covering map $\mathfrak{H} \to \mathfrak{R}_0$ (with the covering group $\Gamma^0_{\mathbf{R}}$) is surjective and unramified.

Now let F be a field of definition for $\mathfrak{R}$, i.e., a common field of definition for all $\mathfrak{R}_i$ and f_i. We can assume that F is finitely generated over $\mathbf{Q}$. Let k be the algebraic closure of $\mathbf{Q}$ in F, so that k is an algebraic number field and F is a regular extension of k. Put $F = k((t))$ with $(t) = (t_1, \cdots, t_r)$, and let W be the locus of (t) over k, so that W is an irreducible affine algebraic variety in $\mathbf{C}^r$.

Let (t') be a point on W which is sufficiently near (t). Then the following geometric intuition is in fact valid :

(♮) *The specialization*

$$(52') \qquad \mathfrak{R}': \begin{array}{ccc} & \mathfrak{R}'_0 & \\ {\scriptstyle f'_1}\swarrow & & \searrow{\scriptstyle f'_2} \\ \mathfrak{R}'_1 & & \mathfrak{R}'_2 \end{array}$$

of $\mathfrak{R}$ *over* $(t) \mapsto (t')/k$ *is well-defined,* $\mathfrak{R}'_i$ $(0 \le i \le 2)$ *are complete non-singular algebraic curves with the same genus as* $\mathfrak{R}_i$ *(respectively), and the rational maps* f'_i $(1 \le i \le 2)$ *have the same types of ramifications as* f_i *(respectively). Moreover, there exist topological isomorphisms* φ_{01} *and* φ_{02} *of* $\mathfrak{R}_0$ *onto* $\mathfrak{R}'_0$, *and* φ_1 *resp.* φ_2 *of* $\mathfrak{R}_1$ *onto* $\mathfrak{R}'_1$ *resp.* $\mathfrak{R}_2$ *onto* $\mathfrak{R}'_2$ *such that :*

(i) *the diagrams*

$$
\begin{array}{ccc} \mathfrak{R}_0 & \xrightarrow{\varphi_{01}} & \mathfrak{R}'_0 \\ f_1 \downarrow & & \downarrow f'_1 \\ \mathfrak{R}_1 & \xrightarrow{\varphi_1} & \mathfrak{R}'_1 \end{array}, \quad \begin{array}{ccc} \mathfrak{R}_0 & \xrightarrow{\varphi_{02}} & \mathfrak{R}'_0 \\ f_2 \downarrow & & \downarrow f'_2 \\ \mathfrak{R}_2 & \xrightarrow{\varphi_2} & \mathfrak{R}'_2 \end{array} \tag{53}
$$

are commutative, and that

(ii) *the topological automorphism $\varphi_{02} \circ \varphi_{01}^{-1}$ of $\mathfrak{R}'_0$ is "small", and hence is homotopic to the identity map.*

Now let π be the natural covering map $\mathfrak{H} \to \mathfrak{R}_0$ defined before, and let $\pi' : \mathfrak{H} \to \mathfrak{R}'_0$ be the universal covering map. Moreover, call $\Delta^0_{\mathbf{R}}$ the covering group of π', and call $\Delta^i_{\mathbf{R}}$ $(i = 1, 2)$ the covering group of $f'_i \circ \pi'$. Thus we have $\Delta^0_{\mathbf{R}} \subset \Delta^i_{\mathbf{R}} \subset G_{\mathbf{R}} = \operatorname{Aut}\mathfrak{H}$. Let $\Delta_{\mathbf{R}}$ be the subgroup of $G_{\mathbf{R}}$ generated by $\Delta^1_{\mathbf{R}}$ and $\Delta^2_{\mathbf{R}}$.

$$
\begin{tikzcd}[column sep=small]
\mathfrak{H} \arrow[d, "\pi"] & & & & \\
\mathfrak{R}_0 \arrow[r, dotted, no head] \arrow[d, "f_1"'] \arrow[dr, "f_2"] & \cdots & \Gamma^0_{\mathbf{R}} \arrow[dl, no head] \arrow[dr, no head] & & \\
\mathfrak{R}_1 \arrow[r, dotted, no head] & \mathfrak{R}_2 \cdots \Gamma^1_{\mathbf{R}} \arrow[dr, no head] & & \Gamma^2_{\mathbf{R}} \arrow[dl, no head] & \\
& & \Gamma_{\mathbf{R}} \subset G_{\mathbf{R}} & &
\end{tikzcd}
,\quad
\begin{tikzcd}[column sep=small]
\mathfrak{H} \arrow[d, "\pi'"] & & & & \\
\mathfrak{R}'_0 \arrow[r, dotted, no head] \arrow[d, "f'_1"'] \arrow[dr, "f'_2"] & \cdots & \Delta^0_{\mathbf{R}} \arrow[dl, no head] \arrow[dr, no head] & & \\
\mathfrak{R}'_1 \arrow[r, dotted, no head] & \mathfrak{R}'_2 \cdots \Delta^1_{\mathbf{R}} \arrow[dr, no head] & & \Delta^2_{\mathbf{R}} \arrow[dl, no head] & \\
& & \Delta_{\mathbf{R}} \subset G_{\mathbf{R}} & &
\end{tikzcd}. \tag{54}
$$

Now, extend the topological isomorphisms φ_{0i} $(i = 1, 2)$ of $\mathfrak{R}_0$ onto $\mathfrak{R}'_0$ to topological automorphisms Φ_i $(i = 1, 2)$ of $\mathfrak{H}$ so that the diagrams

$$
\begin{array}{ccc} \mathfrak{H} & \xrightarrow{\Phi_i} & \mathfrak{H} \\ \pi \downarrow & & \downarrow \pi' \\ \mathfrak{R}_0 & \xrightarrow{\varphi_{0i}} & \mathfrak{R}'_0 \end{array} \qquad (i = 1, 2) \tag{55}
$$

are commutative. Since $\varphi_{02} \circ \varphi_{01}^{-1}$ is homotope 0, we can take Φ_1 and Φ_2 such that $\Phi_2 \circ \Phi_1^{-1}$ commutes with the actions of $\Delta^0_{\mathbf{R}}$. By (53), Φ_i defines an isomorphism ρ_i of $\Gamma^i_{\mathbf{R}}$ onto $\Delta^i_{\mathbf{R}}$, and by the above remark ρ_1 *and* ρ_2 *coincide on* $\Gamma^0_{\mathbf{R}}$, and $\rho_1(\Gamma^0_{\mathbf{R}}) = \rho_2(\Gamma^0_{\mathbf{R}}) = \Delta^0_{\mathbf{R}}$. But by the canonical identification of $\Gamma_{\mathbf{R}}$ with $\Gamma_{\mathfrak{p}}$, $\Gamma^i_{\mathbf{R}}$ $(0 \leq i \leq 2)$ are identified with $\Gamma^i_{\mathfrak{p}}$ respectively, and hence by the Corollary of Lemma 7 (§28), $\Gamma_{\mathbf{R}}$ *is the free product of* $\Gamma^1_{\mathbf{R}}$ *and* $\Gamma^2_{\mathbf{R}}$ *with amalgamated subgroup* $\Gamma^0_{\mathbf{R}}$. Therefore, there is a homomorphism ρ of $\Gamma_{\mathbf{R}}$ onto $\Delta_{\mathbf{R}}$ such that $\rho|_{\Gamma^i_{\mathbf{R}}} = \rho_i$ $(i = 1, 2)$. But $\rho(\Gamma^0_{\mathbf{R}}) = \Delta^0_{\mathbf{R}}$ is discrete in $G_{\mathbf{R}}$, and the quotient $G_{\mathbf{R}}/\Delta^0_{\mathbf{R}}$ is compact. Moreover, $\rho|_{\Gamma^0_{\mathbf{R}}} = \rho_1|_{\Gamma^0_{\mathbf{R}}}$ is injective. Therefore by Lemma 8 (§29), there is an element $x \in G'_{\mathbf{R}} = PL_2(\mathbf{R})$ such that $\rho(\gamma_{\mathbf{R}}) = x^{-1}\gamma_{\mathbf{R}}x$ for all $\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}}$. In particular, we get $\Delta^i_{\mathbf{R}} = x^{-1}\Gamma^i_{\mathbf{R}}x$ for $0 \leq i \leq 2$. Therefore, if $x \in G_{\mathbf{R}} = PSL_2(\mathbf{R})$, then $\mathfrak{R}$ and $\mathfrak{R}'$ are isomorphic analytically (and hence algebraically); i.e., there are analytic (and hence algebraic) isomorphisms ψ_i of $\mathfrak{R}_i$ onto $\mathfrak{R}'_i$ $(0 \leq i \leq 2)$ such that the diagram:

$$(56)\qquad \begin{tikzcd} \mathfrak{R}_0 \arrow[rr, "\psi_0"] \arrow[dd, "f_1"'] \arrow[dr, "f_2"] & & \mathfrak{R}'_0 \arrow[dd, "f'_1"'] \arrow[dr, "f'_2"] & \\ & \mathfrak{R}_2 \arrow[rr, "\psi_2"] & & \mathfrak{R}'_2 \\ \mathfrak{R}_1 \arrow[rr, "\psi_1"'] & & \mathfrak{R}'_1 & \end{tikzcd}$$

is commutative. On the other hand, if $x \notin G_{\mathbf{R}}$, then $\mathfrak{R}$ and $\overline{\mathfrak{R}'}$ are isomorphic analytically, where $\overline{\mathfrak{R}'}$ is the complex conjugation of $\mathfrak{R}'$. But this is impossible (unless $\overline{\mathfrak{R}'} \cong \mathfrak{R}'$), since (t') is sufficiently near (t). *Therefore, $\mathfrak{R}$ and $\mathfrak{R}'$ are isomorphic algebraically.* Now since W is defined over k, algebraic points are dense on W, and hence we can *choose (t') to be algebraic over k* (and hence over $\mathbf{Q}$). Then $\mathfrak{R}'$ is defined over an algebraic number field k'. Now, by the isomorphism $\mathfrak{R}' \cong \mathfrak{R}$, we identify L_i with the field of $\mathbf{C}$-rational functions on $\mathfrak{R}'_i$ $(0 \leq i \leq 2)$. Now let L'_i be the field of k'-rational functions on $\mathfrak{R}'_i$ $(0 \leq i \leq 2)$. Then it is clear that $\{L'_i | 0 \leq i \leq 2\}$ is a k'-form of $\{L_i | 0 \leq i \leq 2\}$. But since k' is an algebraic number field, this proves the Main lemma (§27) (and hence Theorem 4), in the case where $\Gamma^0_{\mathbf{R}}$ is torsion-free and $G_{\mathbf{R}}/\Gamma^0_{\mathbf{R}}$ is compact.

In the general case, we need a slight modification. Let P_j $(1 \leq j \leq m)$ be the points on $\mathfrak{R}_0$ that are ramified in the covering $\pi : \mathfrak{H} \to \mathfrak{R}_0$, and let e_j $(1 \leq j \leq m;\ 1 \leq e_j \leq \infty)$ be the ramification index of P_j in this covering. Take F large enough so that all P_j are rational over F. Then if (t') is sufficiently near (t), we can check without any difficulty that in addition to the assertions $(\natural)$, the specialization P'_j of P_j over $(t) \mapsto (t')/k$ is defined for each j, and that we can take φ_{01} and φ_{02} such that $\varphi_{01}(P_j) = \varphi_{02}(P_j) = P'_j$ for all j. Now define $\pi' : \mathfrak{H} \to \mathfrak{R}'_0$ to be the maximal covering of $\mathfrak{R}'_0$ with the ramifications e_j at P'_j for all j (and unramified everywhere else). Then with these definitions, we can prove the general case exactly in the same manner as in the special case. Thus the proof of the Main lemma, and hence also the proof of Theorem 4, is completed. □

Variations of Theorems 4, 5.

§32.

Corollary of Theorem 5 . *Notations and assumptions being as in Theorem 5, L_{k_0} is the fixed field of the group of all automorphisms of L which commute with the actions of all elements of $G_{\mathfrak{p}}$. If $\sigma \in \mathrm{Aut}\,\mathbf{C}$, then σ has a $G_{\mathfrak{p}}$-extension if and only if $\sigma|_{k_0} = 1$.*

Proof. This follows immediately from Theorem 5 and §20. □

Now let L be any $G_{\mathfrak{p}}$-field over $\mathbf{C}$, and let $G'_{\mathfrak{p}}$ be any subgroup of $\mathrm{Aut}_{\mathbf{C}}\, L$ containing $G_{\mathfrak{p}}$. By *a full $G'_{\mathfrak{p}}$-subfield of L over a field k'* $(\subset \mathbf{C})$, we mean a $G'_{\mathfrak{p}}$-invariant subfield L' of L satisfying $L' \cdot \mathbf{C} = L$ and $L' \cap \mathbf{C} = k'$. Thus, if $G'_{\mathfrak{p}} = G_{\mathfrak{p}}$, this definition agrees with the previous one; and it is also clear that full $G'_{\mathfrak{p}}$-subfields are a priori full $G_{\mathfrak{p}}$-subfields.

THEOREM 6. *Let L be a $G_{\mathfrak{p}}$-field over $\mathbf{C}$, and let $G'_{\mathfrak{p}}$ be any group with $G_{\mathfrak{p}} \subset G'_{\mathfrak{p}} \subset$ $\mathrm{Aut}_{\mathbf{C}} L$. Then L contains a full $G'_{\mathfrak{p}}$-subfield over an algebraic number field. Moreover, if the centralizer of $G'_{\mathfrak{p}}$ in $\mathrm{Aut}_{\mathbf{C}} L$ is trivial, then full $G'_{\mathfrak{p}}$-subfields of L are essentially unique, in the sense that among them there is a smallest one over an algebraic number field playing the role completely parallel to that of L_{k_0} in Theorem 5. Finally, if L is quasi-irreducible, all full $G_{\mathfrak{p}}$-subfields of L are full $\mathrm{Aut}_{\mathbf{C}} L$-subfields.*

PROOF. Let L_k be a full $G_{\mathfrak{p}}$-subfield of L over an algebraic number field k. Let $\mathfrak{Z}$ be the centralizer of $G_{\mathfrak{p}}$ in $\mathrm{Aut}_{\mathbf{C}} L$, so that $\mathfrak{Z}$ is finite (§15, Corollary 3 of Theorem 3). Let M be the fixed field of $\mathfrak{Z}$ in L. For each $\sigma \in \mathrm{Aut}_k \mathbf{C}$, let $\tilde{\sigma}$ be the automorphism of L which is trivial on L_k and which coincides with σ on $\mathbf{C}$. Put $\mathcal{G} = \{\tilde{\sigma} | \sigma \in \mathrm{Aut}_k \mathbf{C}\}$. Then by Lemma 2 (§19), L_k is the fixed field of $\mathcal{G}$. Let $\widetilde{\mathcal{G}}$ be the group of all automorphisms of L which are trivial on k and which commute with all elements of $G_{\mathfrak{p}}$. Then $\widetilde{\mathcal{G}} = \mathcal{G} \cdot \mathcal{Z}$, $\widetilde{\mathcal{G}} \cap \mathcal{Z} = \{1\}$, and $M_k = M \cap L_k$ is the fixed field of $\widetilde{\mathcal{G}}$. Therefore, M_k depends only on k and does not depend on the choice of L_k; and since $(\widetilde{\mathcal{G}} : \mathcal{G}) = (\mathcal{Z} : 1) < \infty$, we get $[L_k : M_k] < \infty$.

Now let $\rho \in \mathrm{Aut}_{\mathbf{C}} L$. Then since $G_{\mathfrak{p}}$ is a characteristic subgroup of $\mathrm{Aut}_{\mathbf{C}} L$ (Corollary 2 of Theorem 3, §15), $\rho(L_k)$ is also $G_{\mathfrak{p}}$-invariant; hence it is a full $G_{\mathfrak{p}}$-subfield over k (hence if L is quasi-irreducible, then we get $\rho(L_k) = L_k$; which settles the last point of the Theorem). Therefore, by the above remark on M_k, we get $\rho(L_k) \cap M = M_k$ and $[\rho(L_k) : M_k] < \infty$.

Since moreover $(\mathrm{Aut}_{\mathbf{C}} L : G_{\mathfrak{p}}) < \infty$, the composite $L_{k'}$ of all $\rho(L_k)$ ($\rho \in \mathrm{Aut}_{\mathbf{C}} L$) is a finite extension of L_k; hence $L_{k'} \cdot \mathbf{C} \supset L_k \cdot \mathbf{C} = L$, $L_{k'} \cap \mathbf{C} = k'$ is a finite extension of k, and $L_{k'}$ is obviously $\mathrm{Aut}_{\mathbf{C}} L$-invariant. Therefore, $L_{k'}$ is a full $\mathrm{Aut}_{\mathbf{C}} L$-subfield of L over k'; which settles the first point of the Theorem.

$$\begin{tikzcd}
& & L \arrow[r, leftrightarrow] \arrow[dll, dash] \arrow[dl, dash] \arrow[dd, dash] & \{1\} \arrow[dd, dash] \\
\rho(L_k) \arrow[r, phantom, "\cdots"] \arrow[dd, dash] & L_k \arrow[ddl, dash] & & \\
& & M \arrow[r, leftrightarrow] \arrow[dd, dash] & \mathfrak{Z} \arrow[dd, dash] \\
M_k \arrow[urr, dash] \arrow[d, dash] & & & \\
k \arrow[rr, dash] & & \mathbf{C} & G_{\mathfrak{p}}
\end{tikzcd}$$

The proof of the second part is completely parallel to the argument given in §19, §20; and hence is omitted. The proof of the last point was given above. □

COROLLARY . *If the center of $\mathrm{Aut}_{\mathbf{C}} L$ is trivial, then full $\mathrm{Aut}_{\mathbf{C}} L$-subfields of L are essentially unique.*

§33. Full $G_{\mathfrak{p}}$-subfields over $\overline{\mathbf{Q}}$. Let L be an arbitrary $G_{\mathfrak{p}}$-field over $\mathbf{C}$. Then, by Theorem 6, L contains a full $\mathrm{Aut}_{\mathbf{C}} L$-subfield L_k over an algebraic number field k. Let $\overline{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$, considered as a subfield of $\mathbf{C}$. Then, $L_k \cdot \overline{\mathbf{Q}}$ is a full $\mathrm{Aut}_{\mathbf{C}} L$-subfield of L over $\overline{\mathbf{Q}}$; hence L contains a full $\mathrm{Aut}_{\mathbf{C}} L$-subfield over $\overline{\mathbf{Q}}$. We shall prove that full $G_{\mathfrak{p}}$-subfield of L over $\overline{\mathbf{Q}}$ is unique. Then, it is clear that the unique full $G_{\mathfrak{p}}$-subfield over $\overline{\mathbf{Q}}$ is also a full $\mathrm{Aut}_{\mathbf{C}} L$-subfield over $\overline{\mathbf{Q}}$. For that purpose, let $\wp$ be the set of all non-trivial (non-equivalent) discrete valuations v_P of L over $\mathbf{C}$ whose stabilizers in $G_{\mathfrak{p}}$ are infinite;

$$\wp = \{v_P \in \Sigma \mid \text{ the group } g_{\mathfrak{p}} \in G_{\mathfrak{p}},\ g_{\mathfrak{p}}(v_P) = v_P \text{ is infinite }\}. \tag{57}$$

We denote by P the place of L over $\mathbf{C}$ defined by v_P, and put

(58) $$L' = \{f \in L \mid P\{f\} \in \bar{\mathbf{Q}} \cup \{\infty\},\ \forall v_P \in \wp\}.$$

On the other hand, let Γ be the discrete subgroup of G which corresponds to L, and consider $L = \bigcup_V L_V$ as the union of the fields L_V of automorphic functions $f(z)$ with respect to $\Gamma_{\mathbf{R}}^V = [\Gamma \cap (G_{\mathbf{R}} \times V)]_{\mathbf{R}}$. Let L'' be the subset of L formed of all $f(z) \in L$ whose values at $\Gamma_{\mathbf{R}}$-fixed points [15] are all contained in $\bar{\mathbf{Q}} \cup \{\infty\}$;

(59) $$L'' = \{f(z) \in L \mid f(\forall \Gamma_{\mathbf{R}}\text{-fixed points}) \in \bar{\mathbf{Q}} \cup \{\infty\}\}.$$

Finally, let L''' be an arbitrary full $G_{\mathfrak{p}}$-subfield of L over $\bar{\mathbf{Q}}$. We shall prove that $L' = L'' = L'''$ holds; which, in particular, would prove the uniqueness of L'''.

First, to prove $L' \subset L''$, note that each point $z_0 \in \mathfrak{H}$ defines $v_P = v_{P_{z_0}} \in \Sigma$, and that, in this manner, $\mathfrak{H}$ can be considered as a connected component of Σ (see §5-§10). Moreover, if $f = f(z) \in L$, then $P_{z_0}\{f\} = f(z_0)$. Since $\Gamma_{\mathfrak{p}}$ is the stabilizer of the connected component $\mathfrak{H}$ in $G_{\mathfrak{p}}$, it is clear that $v_{P_{z_0}}$ is contained in $\wp$ if and only if z_0 is a $\Gamma_{\mathbf{R}}$-fixed point. This proves $L' \subset L''$.

Secondly, we shall prove $L''' \subset L'$. Let $v_P \in \wp$, and let $g_{\mathfrak{p}} \in G_{\mathfrak{p}}$, $g_{\mathfrak{p}} \neq 1$ with $g_{\mathfrak{p}}(v_P) = v_P$. Take $f \in L'''$ such that $g_{\mathfrak{p}}(f) \neq f$. If f is not v_P-integral, we replace f by f^{-1}, and assume from the beginning that f is v_P-integral. Since P is invariant by $g_{\mathfrak{p}}$, we get $P\{f\} = P\{g_{\mathfrak{p}}(f)\}$; hence $P\{f - g_{\mathfrak{p}}(f)\} = 0$; hence P is non-trivial on L'''. Hence $v_P|_{L'''}$ gives a non-trivial discrete valuation of L''' over $\bar{\mathbf{Q}}$; and since $\dim_{\bar{\mathbf{Q}}} L''' = 1$ and $\bar{\mathbf{Q}}$ is algebraically closed, we get $P\{f_1\} \in \bar{\mathbf{Q}} \cup \{\infty\}$ for all $f_1 \in L'''$; which proves $L''' \subset L'$.

(60)
$$\begin{tikzcd}[arrows=dash]
L'' \arrow[d] \arrow[dr] & \\
L' \arrow[d] \arrow[r] & L = L''' \cdot \mathbf{C} \arrow[dd] \\
L''' \arrow[d] \arrow[ur] & \\
\bar{\mathbf{Q}} \arrow[r] & \mathbf{C}
\end{tikzcd}$$

Finally, we shall prove $L'' \subset L'''$. Let $f(z)$ be any element of L''. Since $L = L''' \cdot \mathbf{C}$, we can put

$$f(z) = \sum_{i=1}^{n} \lambda_i f_i(z) / \sum_{i=1}^{n} \lambda_i f_i'(z)$$

where $f_i(z), f_i'(z) \in L'''$ $(1 \leq i \leq n)$, and $\lambda_1, \cdots, \lambda_n \in \mathbf{C}$ are linearly independent over $\bar{\mathbf{Q}}$. Take $i = i_0$ such that $f_{i_0}'(z) \not\equiv 0$. We shall show that $f_{i_0}(z) = f(z) f_{i_0}'(z)$. Suppose, on the contrary, that we have $f_{i_0}(z) \not\equiv f(z) f_{i_0}'(z)$. Since $\Gamma_{\mathbf{R}}$-fixed points are dense on $\mathfrak{H}$ (see

[15] As in Chapter 1, a point $z \in \mathfrak{H}$ is called a $\Gamma_{\mathbf{R}}$-fixed point (or Γ-fixed point) if its stabilizer in $\Gamma_{\mathbf{R}}$ is *infinite*.

Chapter 1, §3), there exists a $\Gamma_{\mathbf{R}}$-fixed point z_0 such that all $f(z_0)$, $f_i(z_0)$, $f_i'(z_0)$ $(1 \le i \le n)$ are finite and $f_{i_0}(z_0) \ne f(z_0)f_{i_0}'(z_0)$. Therefore, we get

$$\sum_{i=1}^{n} c_i\lambda_i = 0 \quad \text{with } c_i = f_i(z_0) - f(z_0)f_i'(z_0).$$

Since $f(z)$, $f_i(z)$, $f_i'(z)$ are in L'', we have $c_i \in \bar{\mathbf{Q}}$ $(1 \le i \le n)$, and by our choice of z_0, we also have $c_{i_0} \ne 0$. But this is a contradiction to linear independence of $c_1, \cdots, c_n$ over $\bar{\mathbf{Q}}$. Therefore, $f_{i_0}(z) = f(z)f_{i_0}'(z)$, and hence $f(z) \in L'''$, which proves $L'' \subset L'''$.

Therefore, we have proved $L' = L'' = L'''$.

THEOREM 7. *Let L be a $G_{\mathfrak{p}}$-field over $\mathbf{C}$. Then L contains a unique full $G_{\mathfrak{p}}$-subfield $L_{\bar{Q}}$ over $\bar{\mathbf{Q}}$, which is given by* (58) *and also by* (59). *Moreover, $L_{\bar{Q}}$ is invariant by* $\mathrm{Aut}_{\mathbf{C}}\, L$.

§34.

EXAMPLE .[16] Let $G_{\mathbf{R}} = PSL_2(\mathbf{R})$, $G_p = PSL_2(\mathbf{Q}_p)$, and let $\Gamma = PSL_2(\mathbf{Z}^{(p)})$ be considered as a discrete subgroup of $G = G_{\mathbf{R}} \times G_p$. Let L be the G_p-field over $\mathbf{C}$ which corresponds to Γ. So, if we denote as

$$(61)\quad \begin{cases} U_p^{(n)} = \{x \in SL_2(\mathbf{Z}_p) \mid x \equiv \pm 1 \pmod{p^n}\}/\pm 1 \\ \Gamma^{(n)} = \Gamma \cap (G_{\mathbf{R}} \times U_p^{(n)}) = \{x \in SL_2(\mathbf{Z}) \mid x \equiv \pm 1 \pmod{p^n}\}/\pm 1, \end{cases} \quad (n = 0, 1, 2, \cdots)$$

then L is nothing but the union $\bigcup_{n=0}^{\infty} L_n$ of the field L_n of automorphic functions with respect to $\Gamma_{\mathbf{R}}^{(n)}$ (see Example in §2). We have shown (§17) that L is irreducible; hence there is a unique full G_p-subfield L_{k_0} over k_0 enjoying the property stated in Theorem 5. *Let us find out k_0 and L_{k_0} for this L.*

Put

$$(62)\quad \begin{cases} G_p^* = \{x \in GL_2(\mathbf{Q}_p) \mid \det x = p\text{-powers}\}/\pm\{p\text{-powers}\} \\ \Gamma^* = \{x \in GL_2(\mathbf{Z}^{(p)}) \mid \det x = p\text{-powers}\}/\pm\{p\text{-powers}\}, \end{cases}$$

$$(63)\quad \begin{array}{ccc} & & G_p^* = G_p \cdot \Gamma^* \\ \Gamma^* & \diagup & \\ 2\,\Big| & & 2\,\Big| \\ & & G_p \\ G_p \cap \Gamma^* = \Gamma & \diagup & \end{array} \quad , \ \mathrm{Aut}_{\mathbf{C}}L = G_p^* \text{ (see §17).}$$

Let $J(z)$ be the elliptic modular function; so that $L_0 = \mathbf{C}(J(z))$, and $J(\sqrt{-1}) = 12^3$, $J(\frac{1}{2}(-1 + \sqrt{-3})) = 0$, $J(i\infty) = \infty$. Put[17]

$$(64)\quad L' = \mathbf{Q}(J(\gamma_{\mathbf{R}}^* z) \mid \gamma^* \in \Gamma^*).$$

Then L' is obviously Γ^*-invariant, and since the action of G_p^* on L is continuous and Γ^* is dense in G_p^*, L' is also G_p^*-invariant; hence *a priori* G_p-invariant. Therefore, $L' \cdot \mathbf{C}$ is

[16]See also §2 and §17.

[17]Here, $\Gamma^* \ni \gamma^* \mapsto \gamma_{\mathbf{R}}^*$ denotes the projection of Γ^* into $\{x \in GL_2(\mathbf{R}) \mid \det x > 0\}/\mathbf{R}^\times \cong G_{\mathbf{R}}$.

also G_p-invariant; but since L is irreducible, we get $L' \cdot \mathbf{C} = L$. Therefore, L' is a full G_p-subfield of L over $k' = L' \cap \mathbf{C}$. We shall prove, by using known results on elliptic modular functions, that $L_{k_0} = L'$, $k_0 = k' = \mathbf{Q}(\sqrt{\pm p})$ $(p \neq 2,\ \pm p \equiv 1 \pmod 4)$, $= \mathbf{Q}(\sqrt{-1}, \sqrt{2})$ $(p = 2)$.

For this purpose, we refer to G. Shimura [30]. Let E be the elliptic curve defined over $K_1 = \mathbf{Q}(J(z))$ given by the equation

$$Y^2 = 4X^3 - tX - t, \quad t = \frac{27J(z)}{J(z) - 12^3}. \tag{65}$$

For each positive integer N, let K_N be the Galois extension of K_1 generated over K_1 by X-coordinates of all N-th division points of E. Then by G. Shimura [30] (§2,§4), the Galois group of K_N/K_1 is (in some way) isomorphic to $G_N = GL_2(\mathbf{Z}/N\mathbf{Z})/\pm 1$, the algebraic closure of $\mathbf{Q}$ in K_N is the field $\mathbf{Q}(\zeta_N)$ of primitive N-th root of unity ζ_N, the action of $\sigma \in G_N$ on $K_1(\zeta_N)$ is $\zeta_N \mapsto \zeta_N^{\det\sigma}$, and finally;[18] if we put

$$K_N^* = K_1\left(J\left(\frac{az+b}{cz+d}\right) \,\middle|\, \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}),\ ad - bc = N\right), \tag{66}$$

then K_N^* is a subfield of K_N corresponding to the center of G_N:

$$\begin{array}{ccc} K_N & \longleftrightarrow & \{1\} \\ K_N^* & \longleftrightarrow & \left\{a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \,\middle|\, a \in (\mathbf{Z}/N\mathbf{Z})^*\right\} / \pm 1 \\ K_1(\zeta_N) & \longleftrightarrow & \{\sigma \in G_N \mid \det\sigma = 1\} \\ K_N^* \cap K_1(\zeta_N) & \longleftrightarrow & \{\sigma \in G_N \mid \det\sigma \in (\mathbf{Z}/N\mathbf{Z})^{*2}\} \\ K_1 & \longleftrightarrow & G_N = GL_2(\mathbf{Z}/N\mathbf{Z})/\pm 1. \end{array} \tag{67}$$

Therefore, the algebraic closure of $\mathbf{Q}$ in K_N^* is the maximum $(2, \cdots, 2)$ type extension of $\mathbf{Q}$ in $\mathbf{Q}(\zeta_N)$.

Now we have $L' = \bigcup_{n=0}^{\infty} K_{p^n}^*$. Since $\dim_{\mathbf{Q}} K_N^* = \dim_{\mathbf{Q}} K_1 = 1$, we get $\dim_{\mathbf{Q}} L' = 1$. On the other hand, since L' is a full G_p-subfield over k', $\dim_{k'} L' = 1$. Therefore $\dim_Q k' = 0$; hence $k' \subset \overline{\mathbf{Q}}$; hence $k' = L' \cap \overline{\mathbf{Q}}$. Therefore, k' is the maximum $(2, \cdots, 2)$ type extension of $\mathbf{Q}$ in $\mathbf{Q}(\zeta_{p^n} | n = 0, 1, 2, \cdots)$; hence

$$k' = \begin{cases} \mathbf{Q}(\sqrt{p}) & (p \equiv 1 \pmod 4), \\ \mathbf{Q}(\sqrt{-p}) & (p \equiv -1 \pmod 4), \\ \mathbf{Q}(\sqrt{-1}, \sqrt{2}) & (p = 2). \end{cases}$$

[18] This part is not explicitly stated in G. Shimura [30], but it follows directly from the results stated explicitly.

Now since L' is a full $G_{\mathfrak{p}}$-subfield of L over k', we get $\mathbf{Q} \subseteq k_0 \subseteq k'$ and $L' = k' \cdot L_{k_0}$. To prove that $k_0 = k'$, we note that (by the above quoted results) $L'/\mathbf{Q}(J(z))$ is a Galois extension, its Galois group is $PL_2(\mathbf{Z}_p)$, and by $PL_2(\mathbf{Z}_p) \ni \sigma \mapsto \det\sigma \in U_p/U_p^2 \cong G(k'/\mathbf{Q})$ (where U_p is the p-adic unit group), all automorphisms of $k'/\mathbf{Q}$ are induced from $PL_2(\mathbf{Z}_p)$. Therefore, together with $\mathrm{Aut}_{k'} L' = \mathrm{Aut}_{\mathbf{C}} L = G_p^*$ (§17 and §32 Theorem 7 (the last assertion)), we see immediately that

$$\mathrm{Aut}_{\mathbf{Q}} L' = PL_2(\mathbf{Q}_p). \tag{68}$$

Since $\mathbf{Q} \subseteq k_0 \subseteq k'$ and since k' is as given above, k'/k_0 is abelian, and hence $L'/L_{k_0} = L_{k_0} \cdot k'/L_{k_0}$ is also abelian; hence, a priori, normal. Let $\mathfrak{Z}$ be the Galois group of L'/L_{k_0}. Then, $\mathfrak{Z}$ centralizes $\mathrm{Aut}_{k'} L' = G_p^*$, hence also $G_p = PSL_2(\mathbf{Q}_p)$. But it is clear that the centralizer of $PSL_2(\mathbf{Q}_p)$ in $PL_2(\mathbf{Q}_p)$ is trivial. Therefore $\mathfrak{Z} = \{1\}$; hence we finally get:

$$L_{k_0} = L' = \mathbf{Q}(J(\gamma_{\mathbf{R}}^* z)|\gamma^* \in \Gamma^*) = \mathbf{Q}(J(\gamma_{\mathbf{R}} z)|\gamma \in \Gamma), \tag{69}$$

$$k_0 = \begin{cases} \mathbf{Q}(\sqrt{\pm p}) \cdots\cdots & \pm p \equiv 1 (\mathrm{mod} 4), \\ \mathbf{Q}(\sqrt{-1}, \sqrt{2}) \cdots & p = 2. \end{cases} \tag{70}$$

The second formula for L' is clear by $L' = \bigcup_{n=0}^{\infty} K_{p^n}^* = \bigcup_{n=0}^{\infty} K_{p^{2n}}^*$.

$$\begin{tikzcd}[arrows=dash] & L_{k_0} \arrow[r] \arrow[d] & L' = L_{k_0} \cdot k' \arrow[d] \\ \mathbf{Q} \arrow[r] & k_0 \arrow[r] & k' \end{tikzcd}$$

The fields k_0 and $F = \mathbf{Q}((\mathrm{tr}\,\gamma_{\mathbf{R}})^2|\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}})$.

§35. By Theorem 5, if L is a quasi-irreducible $G_{\mathfrak{p}}$-field over $\mathbf{C}$, then L contains the smallest full $G_{\mathfrak{p}}$-subfield L_{k_0} over k_0. It is an important problem to determine this more explicitly. We particularly want to know the relation between k_0 and $k_{\mathfrak{p}}$. As a first step to this, we shall show that under a certain condition on Γ which is satisfied by all examples of Γ that we know at present (i.e., those Γ given in Chapter 4), *the field k_0 contains $F = \mathbf{Q}((\mathrm{tr}\,\gamma_{\mathbf{R}})^2|\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}})$.*

Let $g_{\mathbf{R}}$ be an elliptic element of $G_{\mathbf{R}}$. Then there is an element $t \in G_{\mathbf{R}}$ such that $t^{-1} g_{\mathbf{R}} t$ is of the form $\pm \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, and such θ is determined uniquely modulo π. Put $e^{i\theta} = \pm\lambda$. Then, up to the sign, λ is an eigenvalue of $g_{\mathbf{R}}$, which will be called *the first eigenvalue* of $g_{\mathbf{R}}$, while λ^{-1} will be called *the second eigenvalue* of $g_{\mathbf{R}}$. It is easy to check that 2θ is the argument of the rotation induced by $g_{\mathbf{R}}$ at its fixed point on $\mathfrak{H}$.

LEMMA 11. *Let L be a $G_{\mathfrak{p}}$-field over $\mathbf{C}$ with a fixed connected component Σ_0 of Σ and a fixed isomorphism $\Sigma_0 \cong \mathfrak{H}$, and let Γ be the corresponding discrete subgroup of $G = G_{\mathbf{R}} \times G_{\mathfrak{p}}$ (see §9). Let $\gamma = \gamma_{\mathbf{R}} \times \gamma_{\mathfrak{p}} \in \Gamma$ be such that $\gamma_{\mathbf{R}}$ is elliptic, and let $P_0 \in \Sigma_0$ be the fixed element of $\gamma_{\mathfrak{p}}$. Then for any prime element $x_0 \in L$ of P_0, we have*

$$\gamma_{\mathfrak{p}}^{-1}(x_0)/x_0 \equiv \lambda^2 \pmod{P_0}, \tag{71}$$

where $\pm\lambda$ is the first eigenvalue of $\gamma_{\mathbf{R}}$.

PROOF. Let z_0 be the point on $\mathfrak{H}$ corresponding to P_0 by the isomorphism $\Sigma_0 \cong \mathfrak{H}$. Then z_0 is the fixed point of $\gamma_{\mathbf{R}}$ on $\mathfrak{H}$. For each $z \in \mathfrak{H}$, let $P = P_z$ be the corresponding element of Σ_0, and let $f(z) \in \mathbf{C} \cup \{\infty\}$ be the residue class of x_0 at P;

$$x_0 \equiv f(z) \mod P; \quad \mathrm{ord}_{z_0} f(z) = 1. \tag{72}$$

Hence

$$\gamma_{\mathfrak{p}}^{-1}(x_0) \equiv f(\gamma_{\mathbf{R}} \cdot z) \qquad (\mathrm{mod}\ P). \tag{73}$$

Therefore, the residue class of $\gamma_{\mathfrak{p}}^{-1}(x_0)/x_0$ at $P = P_0$ is the value of $f(\gamma_{\mathbf{R}} \cdot z)/f(z)$ at $z = z_0$; hence is equal to $e^{2\theta i}$, where 2θ is the rotation argument of $\gamma_{\mathbf{R}}$ at $z = z_0$. Therefore, by the previous remark, it is equal to λ^2. □

§36.

LEMMA 12. *The notations being as in Lemma 11, assume now that Γ satisfies the following condition; if $\gamma', \gamma'' \in \Gamma$ are such that $\gamma'_{\mathfrak{p}}$ and $\gamma''_{\mathfrak{p}}$ are conjugate in $G_{\mathfrak{p}}$, then $\gamma'_{\mathbf{R}}$ and $\gamma''_{\mathbf{R}}$ are conjugate in $G'_{\mathbf{R}} = PL_2(\mathbf{R})$. Then, for every $P \in \Sigma$ which is fixed by $\gamma_{\mathfrak{p}}$, we have*

$$\gamma_{\mathfrak{p}}^{-1}(x)/x \equiv \lambda^{\pm 2} \quad (\mathrm{mod}\ P), \tag{74}$$

where x is any prime element of P.

REMARK . Here, P need not be an element of Σ_0.

PROOF. Let $g_{\mathfrak{p}}$ be an element of $G_{\mathfrak{p}}$ such that $g_{\mathfrak{p}} \cdot P$ is contained in Σ_0. Put $P'_0 = g_{\mathfrak{p}} \cdot P$, and $\gamma'_{\mathfrak{p}} = g_{\mathfrak{p}}\gamma_{\mathfrak{p}}g_{\mathfrak{p}}^{-1}$. Then $\gamma'_{\mathfrak{p}}$ fixes P'_0; hence $\gamma'_{\mathfrak{p}} \cdot \Sigma_0 = \Sigma_0$; hence $\gamma'_{\mathfrak{p}} \in \Gamma_{\mathfrak{p}}$, and the element $\gamma'_{\mathbf{R}} \in \Gamma_{\mathbf{R}}$ corresponding to $\gamma'_{\mathfrak{p}}$ is elliptic. Let $\pm\lambda'$ be the first eigenvalue of $\gamma'_{\mathbf{R}}$. Then, since $x'_0 = g_{\mathfrak{p}}(x)$ is a prime element of $P'_0 = g_{\mathfrak{p}}P$, we get (by Lemma 11)

$$\gamma'^{-1}_{\mathfrak{p}}(x'_0)/x'_0 \equiv \lambda'^2 \quad (\mathrm{mod}\ P'_0). \tag{75}$$

But since $\gamma'_{\mathfrak{p}}$ and $\gamma_{\mathfrak{p}}$ are conjugate in $G_{\mathfrak{p}}$, $\gamma'_{\mathbf{R}}$ and $\gamma_{\mathbf{R}}$ must be conjugate in $G'_{\mathbf{R}} = PL_2(\mathbf{R})$ by our assumption on Γ. Therefore, we have $\pm\lambda' = \pm\lambda^{\pm 1}$. Therefore, by (75) we get

$$\gamma'^{-1}_{\mathfrak{p}}(x'_0)/x'_0 \equiv \lambda^{\pm 2} \quad (\mathrm{mod}\ P'_0);$$

hence

$$g_{\mathfrak{p}}\gamma_{\mathfrak{p}}^{-1}(x)/g_{\mathfrak{p}}(x) \equiv \lambda^{\pm 2} \quad (\mathrm{mod}\ g_{\mathfrak{p}}P).$$

Therefore $\gamma_{\mathfrak{p}}^{-1}(x)/x \equiv \lambda^{\pm 2}$ (mod P), which proves our lemma. □

Now, it is easy to prove:

LEMMA 13. *Let L, Γ be as in Lemma 11, and assume that Γ satisfies the condition given in Lemma 12. Then, for every elliptic element $\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}}$ and for every automorphism σ of L which commutes with all elements of $G_{\mathfrak{p}}$, we have $\sigma((\mathrm{tr}\,\gamma_{\mathbf{R}})^2) = (\mathrm{tr}\,\gamma_{\mathbf{R}})^2$.*

PROOF. Let $\gamma_{\mathfrak{p}}$ be the element of $\Gamma_{\mathfrak{p}}$ corresponding to $\gamma_{\mathbf{R}}$, and let P_0, x_0, $\pm\lambda$ be as in Lemma 11. Thus, we have

$$\gamma_{\mathfrak{p}}^{-1}(x_0)/x_0 \equiv \lambda^2 \pmod{P_0}.$$

But since σ commutes with all elements of $G_{\mathfrak{p}}$ and hence in particular with $\gamma_{\mathfrak{p}}$, we get,

$$\gamma_{\mathfrak{p}}^{-1}\sigma(x_0)/\sigma(x_0) \equiv \sigma(\lambda)^2 \pmod{\sigma P_0}.$$

Now, σP_0 may not lie on Σ_0, but it is an element of Σ which is fixed by $\gamma_{\mathfrak{p}}$. Moreover, it is clear that $\sigma(x_0)$ is a prime element of σP_0. Therefore by Lemma 12, we get

$$\gamma_{\mathfrak{p}}^{-1}\sigma(x_0)/\sigma(x_0) \equiv \lambda^{\pm 2} \pmod{\sigma P_0}.$$

Therefore, $\sigma(\lambda)^2 = \lambda^{\pm 2}$; hence $\lambda^2 + \lambda^{-2} = (\operatorname{tr}\gamma_{\mathbf{R}})^2 - 2$ is invariant by σ. Therefore, $(\operatorname{tr}\gamma_{\mathbf{R}})^2$ is also invariant by σ. □

THEOREM 8. *Let L be a $G_{\mathfrak{p}}$-field over $\mathbf{C}$ such that the corresponding discrete subgroup Γ satisfies the condition given in Lemma 12. Let k be a subfield of $\mathbf{C}$ such that there exists a full $G_{\mathfrak{p}}$-subfield of L over k. Then k contains the field $F = \mathbf{Q}((\operatorname{tr}\gamma_{\mathbf{R}})^2 | \gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}})$. In particular, if L is moreover quasi-irreducible, then the field k_0 (defined by Theorem 5) contains F.*

PROOF. Let L_k be a full $G_{\mathfrak{p}}$-subfield of L over k, and for each $\sigma \in \operatorname{Aut}_k \mathbf{C}$, let $\tilde{\sigma}$ be the automorphism of L which is trivial on L_k and which coincides with σ on $\mathbf{C}$. Then $\tilde{\sigma}$ commutes with all elements of $G_{\mathfrak{p}}$. Therefore by Lemma 13, we have

$$\sigma((\operatorname{tr}\gamma_{\mathbf{R}})^2) = \tilde{\sigma}((\operatorname{tr}\gamma_{\mathbf{R}})^2) = (\operatorname{tr}\gamma_{\mathbf{R}})^2$$

for all $\sigma \in \operatorname{Aut}_k \mathbf{C}$ and for all elliptic elements $\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}}$. Therefore, k contains $(\operatorname{tr}\gamma_{\mathbf{R}})^2$ for any elliptic element $\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}}$. But by the Corollary of Proposition 4 (Chapter 3, §11) and by the Remark (Chapter 3, §14), F is generated over $\mathbf{Q}$ by $(\operatorname{tr}\gamma_{\mathbf{R}})^2$ of all elliptic elements $\gamma_{\mathbf{R}} \in \Gamma_{\mathbf{R}}$.

Therefore k contains F. □