J. Math. Soc. Japan
Vol. 18, No. 3, 1966

On discrete subgroups of the two by two projective linear group over $\mathfrak{p}$-adic fields

By Yasutaka IHARA*

(Received March 11, 1966)

Introduction. In the present paper we shall prove some properties of torsion-free discrete subgroups Γ of the title which were announced in our previous note [2], and then we shall show a method for the construction of all such Γ. Those properties are possessed by subgroups Γ of more general abstract groups G (defined in § 1), e. g. free product of two groups with some amalgamated subgroups, and so we shall treat them together in an abstract manner. In § 2, we shall show that Γ is isomorphic to a *free group* with some explicitly given set of generators. In § 3, we shall compute the number of primitive conjugacy classes of Γ with given " degree " or, what is the same, evaluate certain " ζ function " attached to $\Gamma \subset G$. This is based on the results of § 2. § 4 is for the *construction of all* Γ. The problem is nothing but a purely combinatorial one. There are many Γ and they have many non-trivial deformations. In the case where $G = PL(2)$ over $\mathfrak{p}$-adic fields, these, together with the remarks on spectral decompositions of $L^2(G/\Gamma)$ given at the end of § 3, show that although some Γ (with G/Γ compact) are arithmetically defined, their arithmetical properties are not preserved by taking subgroups with finite indices (cf. also [2] § 4) ; here everything is algebraic and, in general, not arithmetic. For example, Ramanujan's conjecture for some type of modular cusp forms is equivalent with some conjecture for arithmetically defined Γ, but the latter fails to be true if we take some subgroups of Γ with finite indices instead of Γ. Finally in § 5, a remark on the structure of " $\mathfrak{p}$-unit groups " of totally definite quaternion algebras, which is a direct application of Theorem 1 (§2), is given.

Throughout the followings, for any set S, $|S|$ will denote its cardinal number ; and the summation symbol Σ over some subsets of a set implies disjoint union. For any ring A and positive integer n, $M(n, A)$ will denote the ring of all n by n matrices whose entries are elements of A.

* This work was supported by the National Science Foundation Grant.

§ 1. Definition of (G, l) and Γ.

Let G be an abstract group. Assume that for each element x of G we are given some non-negative rational integer $l(x)$, called *the length of* x, satisfying the following conditions (G, l, I), (G, l, II); where G_l denotes the set of all elements of G with length l $(l=0, 1, 2, \cdots)$ and U denotes G_0 (once and for all).

(G, l, I) For any $l=0, 1, 2, \cdots$, G_l is non-empty, $U=G_0$ forms a subgroup of G and

$$G_l^{-1}=G_l, \quad UG_lU=G_l, \quad |U\backslash G_l|<\infty \quad \text{for all} \quad l=0, 1, 2, \cdots.$$

According to this we can define the double coset ring $\mathfrak{R}(G, U)$ with respect to U and G. Since each G_l is a union of finite number of U-double-cosets, it can be considered as an element of $\mathfrak{R}(G, U)$ (by taking formal sum instead of disjoint union).

(G, l, II) Put $|U\backslash G_1|=q+1$. Then, as elements of $\mathfrak{R}(G, U)$,

$$G_1^2=G_2+(q+1)U \tag{1}$$

$$G_1G_l=G_{l+1}+qG_{l-1} \qquad (l\geqq 2). \tag{2}$$

From this it follows directly that $|U\backslash G_l|=q^l+q^{l-1}$ for $l\geqq 1$.

EXAMPLE 1. Let G be the free group with n generators $x_1, \cdots, x_n$. For any $x\in G$, let $l(x)$ be the sum of absolute values of exponents of $x_1, \cdots, x_n$ in the reduced expression of x. Then G, l satisfies (G, l, I, II), and $U=\{1\}$, $q=2n-1$.

EXAMPLE 2. $G=PL(2, k)=GL(2, k)/k^*$ where k is a locally compact field under a discrete valuation. Let $\mathfrak{o}$ (resp. $\mathfrak{p}$) be the ring of integers (resp. prime ideal) of k. As a representative modulo k^* of any element x of G, we can choose a matrix $((a_{ij}))$ $(1\leqq i, j\leqq 2)$ such that $a_{ij}\in\mathfrak{o}$ $(1\leqq i, j\leqq 2)$ and $\sum_{i,j=1}^{2} a_{ij}\mathfrak{o}=\mathfrak{o}$. Put $\det.((a_{ij}))\mathfrak{o}=\mathfrak{p}^{l(x)}$. Then, $l(x)$ depends only on x. Now G, l satisfies (G, l, I, II) with $q=N\mathfrak{p}$, and $U=PL(2, \mathfrak{o})=GL(2, \mathfrak{o})/\mathfrak{o}^*$.

EXAMPLE 3. Let U be any (abstract) group with a proper subgroup H_1 such that $(U:H_1)<\infty$. Let H be another group with a subgroup H_2 with index two, where H_2 is isomorphic to H_1. Then the free product G of U and H with "amalgamated subgroups" H_1 and H_2 satisfies (G, l, I, II) with some length l. (G, l) satisfying (G, l, I, II) can be obtained in this manner if and only if G_1 consists of a single U-double-coset. (Detailed explanation is given in § 5, Supplement 1.) E. g. $G=PL(2, k)$, U, etc. being as in example 2, G is the free product of U and $\tilde{U}_B$ with amalgamated subgroup U_B, where U_B is the group of all matrices $((a_{ij}))$ $(1\leqq i, j\leqq 2)$ in $GL(2, \mathfrak{o})$ with $a_{21}\equiv 0 \pmod{\mathfrak{p}}$ divided by the center, and $\tilde{U}_B$ is the normalizor of U_B in G; namely $\tilde{U}_B=U_B \cup U_B\omega$, where $\omega=\begin{pmatrix}0 & 1\\ \pi & 0\end{pmatrix}$, $\mathfrak{p}=\pi\mathfrak{o}$.

Throughout the followings we shall fix once and for all any pair $(G, l(x))$ satisfying the conditions (G, l, I, II) (as well as the above notations), and consider subgroups Γ of G satisfying either (ΓI) alone or both (ΓI) and (ΓII) which are stated as follows.

(ΓI). Γ is torsion-free, and $\Gamma \cap x^{-1}Ux = \{1\}$ for any $x \in G$.

(ΓII). $|U\backslash G/\Gamma| < \infty$.

In example 1, (ΓI) is satisfied by any subgroup of G and (ΓII) is equivalent with $(G : \Gamma) < \infty$. In example 2, (ΓI) is equivalent with torsion-freeness and discreteness of Γ in G, and (ΓI), (ΓII) is equivalent with torsion-freeness, discreteness of Γ in G and compactness of G/Γ. In example 3, (ΓI) is equivalent with the condition that no element of Γ other than the identity is conjugate to the elements of U or H.

Our purpose is, given any $(G, l(x))$ satisfying (G, l, I, II) and Γ satisfying $(\Gamma I\text{-}II)$ (or sometimes only (ΓI)) to study the structure, method for construction, and to see how conjugacy classes of Γ are embedded in those of G.

§ 2. The structure of Γ.

2-1. In this section, we shall prove Theorems 1 and 1'.

THEOREM 1. *Let Γ be a subgroup of G satisfying (ΓI). Then Γ is isomorphic to a free group (over a set of at most countable generators). If moreover (ΓII) is satisfied, the number of generators of Γ is finite and is equal to $\frac{1}{2}(q-1)h+1$, where $q+1 = |U\backslash G_1|$, $h = |U\backslash G/\Gamma|$. (When q is even, h must also be even.)*

COROLLARY. *Any torsion-free discrete subgroup Γ of $PL(2, k)$, k being as in the example 2, is isomorphic to a free group (over a set of at most countable generators). If moreover $PL(2, k)/\Gamma$ is compact, the number of free generators of Γ is equal to $\frac{1}{2}(q-1)h+1$, where $q = N\mathfrak{p}$ and $h = |PL(2, \mathfrak{o})\backslash PL(2, k)/\Gamma|$.*

As for applications to "$\mathfrak{p}$-unit groups" of totally definite quaternion algebras, cf. § 5, Supplement 2.

Before going into the proof of Theorem 1, we need a few elementary lemmas on (G, l). The proof of Theorem 1 will be based on Lemma 1, Lemma 5 and on the particular choice of representatives of $U\backslash G/\Gamma$.

2-2. LEMMA 1. *Let $\pi_0, \pi_1, \cdots, \pi_q$ be a set of representatives of $U\backslash G_1$. Then for any $l = 0, 1, 2, \cdots$, the product $\pi_{i_1}\pi_{i_2}\cdots\pi_{i_l}$ has length l if and only if $\pi_{i_n}\pi_{i_{n+1}} \notin U$ holds for all $n = 1, 2, \cdots, l-1$; and conversely any element $x \in G$ with length l has a unique factorization of the form:*

$$x = u\pi_{i_1}\pi_{i_2}\cdots\pi_{i_l} \tag{3}$$

where $u \in U$ and $\pi_{i_n}\pi_{i_{n+1}} \notin U$ for all $n = 1, 2, \cdots, l-1$.

In short, $G_1=\sum_{i=0}^{q} U\pi_i$ *implies* $G_l=\sum' U\pi_{i_1}\cdots\pi_{i_l}$, *the disjoint union* Σ' *being taken over all* $0\leqq i_1,\cdots,i_l\leqq q$ *such that* $\pi_{i_n}\pi_{i_{n+1}}\notin U$ *for all* $n=1,2,\cdots,l-1$.

PROOF. By (2) we obtain

$$G_1^l=G_l+cG_{l-2}+c'G_{l-4}+\cdots \qquad (l\geqq 1) \tag{4}$$

where $c, c', \cdots$ are non-negative integers. In fact, it is trivial for $l=1$; so assume that (4) is true for some $l\geqq 1$, and multiply G_1 on both sides. Then from (2) follows directly that (4) is true also for $l+1$.

(4) implies in particular that the length of a product of l elements of G_1 is at most equal to l. Now, the expression of G_1^l by the formal sum of left U-cosets, multiplicity being taken into account, will be

$$\Sigma U\pi_{i_1}\cdots\pi_{i_l}=\Sigma' U\pi_{i_1}\cdots\pi_{i_l}+ \text{ lower length terms,} \tag{5}$$

the first formal sum Σ being taken over all $0\leqq i_1,\cdots,i_l\leqq q$, the second formal sum Σ' being taken over all $0\leqq i_1,\cdots,i_l\leqq q$ such that $\pi_{i_n}\pi_{i_{n+1}}\notin U$ for all $n=1,2,\cdots,l-1$, On the other hand, the number of terms under Σ' in (5) is q^l+q^{l-1} which is also equal to $|U\backslash G_l|$. Thus by comparing (4) and (5) we see that all left U-cosets under Σ' in (5) must be mutually distinct, elements of such left U-cosets must have length l, and that

$$G_l=\Sigma' U\pi_{i_1}\cdots\pi_{i_n} \qquad \text{(disjoint union)}$$

which proves Lemma 1.

REMARK. Moreover we can easily verify that under the condition (G, l, I) the statement of Lemma 1 is equivalent with the condition (G, l, II) for G and $l(x)$.

It is direct consequence of Lemma 1 that for any $x_1,\cdots,x_n\in G$ we have

$$l(x_1\cdots x_n)\leqq l(x_1)+\cdots+l(x_n)$$

and that

$$l(x_1\cdots x_n)\equiv l(x_1)+\cdots+l(x_n) \qquad (\text{mod } 2).$$

We say that the product $x_1\cdots x_n$ is *free* when the equality instead of the above inequality holds.

LEMMA 2. *Suppose* $x, y, z\in G, y\notin U$. *If the two products* xy, yz *are both free, then the product* xyz *is also free.*

PROOF. Let $\pi_0,\cdots,\pi_q$ be as in Lemma 1 and factorize $z=u\pi_{\lambda_1}\cdots\pi_{\lambda_l}$, $yu=u'\pi_{\mu_1}\cdots\pi_{\mu_m}$, $xu'=u''\pi_{\nu_1}\cdots\pi_{\nu_n}$, where $u, u', u''\in U$, $l=l(z)$, $m=l(y)>0$, $n=l(x)$ (cf. lemma 1). By the assumption, $y\cdot z$, $x\cdot y$ are free products; hence $\pi_{\mu_m}\pi_{\lambda_1}\notin U$, $\pi_{\nu_n}\pi_{\mu_1}\notin U$. Therefore by Lemma 1, $xyz=u''\pi_{\nu_1}\cdots\pi_{\nu_n}\pi_{\mu_1}\cdots\pi_{\mu_m}\pi_{\lambda_1}\cdots\pi_{\lambda_l}$ has length $l+m+n$. Q. E. D.

LEMMA 3. *Let* $x\cdot y$ *be a free product and let* $xy=u\pi_{i_1}\cdots\pi_{i_l}$ *be the factorization* (3) *of* xy. *Then* $x=u\pi_{i_1}\cdots\pi_{i_m}u'$, $y=u'^{-1}\pi_{i_{m+1}}\cdots\pi_{i_l}$ *with some* $u'\in U$

and $m=l(x)$.

PROOF. Let $y=u'\pi_{j_{m+1}}\cdots\pi_{j_l}$ be the factorization (3) for y. Since the factorization of xy can be obtained by factorizations of x, y and then by carrying the elements of U to the left (no influence to y-side), we see directly by the uniqueness of factorization (3) for xy that $j_{m+1}=i_{m+1}, \cdots, j_l=i_l$, and hence $y=u'\pi_{i_{m+1}}\cdots\pi_{i_l}$ for some $u'\in U$. Q. E. D.

LEMMA 4. *Let $x, y\in G$ and put $l(xy)=l(x)+l(y)-2d$. Then $d\leqq l(x), l(y)$; and if $x=x''\cdot x'$, $y=y'\cdot y''$ are free products with $d\leqq l(x'), l(y')$, then $l(x'y')=l(x')+l(y')-2d$.*

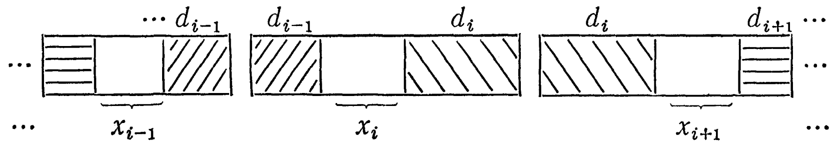
PROOF. The first assertion is clear. Let $x=u\pi_{i_1}\cdots\pi_{i_l}$, $y=u'\pi_{j_1}\cdots\pi_{j_m}$ be the factorization (3) of x, y. By Lemma 3, $x'=u''\pi_{i_s}\cdots\pi_{i_l}$, $y'=u'\pi_{j_1}\cdots\pi_{j_t}u'''$ with $u'', u'''\in U$, $l(x')=l-s+1\geqq d$, $l(y')=t\geqq d$. It is enough to prove that $l(\pi_{i_s}\cdots\pi_{i_l}u'\pi_{j_1}\cdots\pi_{j_t})=(l-s+1)+t-2d$. This can be seen easily from the process of obtaining the factorization (3) for xy from that of x and y above. Q. E. D.

LEMMA 5. *Let $x_1, \cdots, x_n$ be any elements of G and put*

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

If $l(x_{i+1})>d_i+d_{i+1}$ holds for all i $(1\leqq i\leqq n-1)$, then

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



PROOF. Factorize each x_i into free product $x_i=a_ib_ic_i$ with $l(a_i)=d_{i-1}$, $l(b_i)=l(x_i)-d_{i-1}-d_i>0$, $l(c_i)=d_i$ (here we understand $a_1=c_n=1$). Lemma 4 shows that $c_ia_{i+1}\in U$ $(1\leqq i\leqq n-1)$ and that $l(b_ic_ia_{i+1}b_{i+1})=l(b_i)+l(b_{i+1})$, and hence the product $(b_ic_ia_{i+1})\cdot b_{i+1}$ and hence also the product $(b_ic_ia_{i+1})\cdot(b_{i+1}c_{i+1}a_{i+2})$ are free. Now our lemma follows directly from Lemma 2. Q. E. D.

COROLLARY. *Let S be a subset of G such that $S\cap S^{-1}=\phi$. Assume that $l(y)>d_{xy}+d_{yz}$ holds for any three elements $x, y, z\in S\cup S^{-1}$ with $xy\neq 1$, $yz\neq 1$, where d_{xy}, d_{yz} are defined by $l(xy)=l(x)+l(y)-2d_{xy}$, $l(yz)=l(y)+l(z)-2d_{yz}$. Then the subgroup of G generated by S is the free group over S.*

PROOF. By Lemma 5, any reduced word $\neq 1$ over S has positive length, and hence cannot be the identity. Q. E. D.

2-3. Now let Γ be a subgroup of G satisfying (ΓI). Since $|U\backslash G_l|<\infty$ for $l=0, 1, 2, \cdots$, $|U\backslash G|$ is countable. Put $G=\sum_{i=1}^{h}Ux_i\Gamma$, $h=|U\backslash G/\Gamma|\leqq\infty$. Let $\mathfrak{R}(G, U)$ be the double coset ring with respect to U and G, and let $\mathfrak{T}$ be the subring of $\mathfrak{R}(G, U)$ generated by G_l $(l=0, 1, 2, \cdots)$. For each U-double-coset

UyU in G, we correspond an $h \times h$ matrix whose (i, j)-component is the element of the group ring $Z[\Gamma]$ of Γ over the ring of rational integers Z defined by the formal (finite) sum of all elements of $\Gamma \cap x_i^{-1}UyUx_j$. Then this gives a homomorphism φ of $\mathfrak{R}(G, U)$ into the ring M of all $h \times h$ matrices $((m_{ij}))$ over $Z[\Gamma]$ such that for each i (resp. j), $m_{ij}=0$ for almost all j (resp. i), and hence the restriction $\varphi|\mathfrak{T}$ of φ to $\mathfrak{T}$ gives that of $\mathfrak{T}$ into M. Put $T_l = \varphi(G_l)(l=0, 1, 2, \cdots)$. Then by (4)

$$T_1^l = T_l + cT_{l-2} + c'T_{l-4} + \cdots \tag{6}$$

where $c, c', \cdots$ are *non-negative* integers. Since any element γ of Γ is contained in some G_l, and hence appears in (1,1) component of T_l, we see directly from (6) that Γ is generated by the set of elements of Γ which appear in some components of T_1, i. e. Γ is generated by $\Gamma \cap x_i^{-1}G_1x_j$ $(1 \leqq i, j \leqq h)$. It is also easy to see that if we put $A_l = ((a_{ij}^{(l)}))$, $a_{ij}^{(l)} = |\Gamma \cap x_i^{-1}G_lx_j|$, then

$$a_{ij}^{(l)} = a_{ji}^{(l)}, \ \sum_{j=1}^{h} a_{ij}^{(l)} = \sum_{i=1}^{h} a_{ij}^{(l)} = q^l + q^{l-1} \tag{7}$$

for any $l=1, 2, \cdots$, and $1 \leqq i, j \leqq h$.

2-4. THE PROOF OF THEOREM 1. (A) Put $G = \sum_{i=1}^{h} Ux_i'\Gamma$ (disjoint), and $S'_{ij} = x_i'^{-1}G_1x'_j \cap \Gamma$ $(1 \leqq i, j \leqq h)$. We have seen that these S'_{ij} $(1 \leqq i, j \leqq h)$ together generate Γ. To find a minimum set of generators, we need some special representatives of $U \backslash G/\Gamma$.

For that purpose, we fix once and for all a set of representatives $\pi_0, \pi_1, \cdots, \pi_q$ of $U \backslash G_1$, and consider the totality Π_l of all elements of G_l which have expressions of the form $\pi_{i_l} \cdots \pi_{i_1}$ where $\pi_{i_{n+1}}\pi_{i_n} \notin U$ for $n=1, 2, \cdots, l-1$. By Lemma 1, Π_l is a set of representatives of $U \backslash G_l$; hence $\Pi = \bigcup_{l=0}^{\infty} \Pi_l$ is that of $U \backslash G$. We shall introduce in Π a lexicographic ordering in the following manner.

1) $$x \in \Pi_l, \ y \in \Pi_{l'}, \ l > l' \Rightarrow x > y.$$

2) $$x, y \in \Pi_l, \ x = \pi_{i_l} \cdots \pi_{i_1}, \ y = \pi_{j_l} \cdots \pi_{j_1},$$
$$i_1 = j_1, \cdots, i_{m-1} = j_{m-1}, \ i_m > j_m \quad \text{for some} \quad m \geqq 1 \Rightarrow x > y.$$

Now let $Ux\Gamma$ be any $U \backslash G/\Gamma$ double-coset and let x_0 be the smallest element among $Ux\Gamma \cap \Pi (\neq 0)$. We shall call x_0 *the smallest representative* of $Ux\Gamma$, and denote by $\mathfrak{R}$ the set of all such smallest representatives of $U \backslash G/\Gamma$ double-cosets. Thus $G = U\mathfrak{R}\Gamma$, $|\mathfrak{R}| = h$, and $\mathfrak{R} \ni 1$.

Moreover $\mathfrak{R}$ has the following properties. *Let* $x \in \mathfrak{R}, x \neq 1$ *and put* $x = \pi_{i_l} \cdots \pi_{i_1}$ $(l = l(x) > 0)$. *Then* $y = \pi_{i_{l-1}} \cdots \pi_{i_1}$ *also belongs to* $\mathfrak{R}$, *and it is the only element in* $\mathfrak{R}$ *which is smaller than* x *and which satisfies* $x^{-1}G_1y \ni 1$. In fact, let us suppose that y were not smallest in $Uy\Gamma \cap \Pi$ and let y' be the smallest.

Put $y=uy'\gamma$, $u\in U$, $\gamma\in\Gamma$. Then $x\gamma^{-1}=\pi_{i_l}y\gamma^{-1}=\pi_{i_l}uy'$. Choose $u'\in U$ so that $u'x\gamma^{-1}=u'\pi_{i_l}uy'\in\Pi\frown Ux\Gamma$. If $l(y')<l(y)=l-1$, then $l(u'x\gamma^{-1})\leqq 1+l(y')<l=l(x)$; hence a contradiction. So $l(y')=l(y)=l-1$. But the uniqueness of factorization (cf. Lemma 1) shows that $y'<y$ implies $u'\pi_{i_l}uy'<\pi_{i_l}y$ i.e. $u'x\gamma^{-1}<x$; hence a contradiction. This proves that $y\in\mathfrak{R}$. Secondly assume that $z\in\mathfrak{R}$, $z<x$ and $x^{-1}G_1z\ni 1$. Thus $z=\pi x$ with $\pi\in G_1$. Since $l(z)\leqq l(x)$ by assumption we have $l(z)=l(\pi x)=l-1$ and hence $\pi=u\pi_{i_l}^{-1}$ with $u\in U$, i.e. $z=u\pi_{i_{l-1}}\cdots\pi_{i_1}$. Since $z\in\mathfrak{R}$, $u=1$ i.e. $z=y$; hence the second assertion is proved.

Now put $\mathfrak{R}=\{x_1, x_2, \cdots\}$, $1=x_1<x_2<\cdots$; so, $G=\sum_{i=1}^{h}Ux_i\Gamma$. Put $S_{ij}=x_i^{-1}G_1x_j\frown\Gamma$. The above argument shows that for each $j>1$ there exists unique suffix $i=\rho(j)<j$ such that $S_{ij}\ni 1$. *We shall show that the following subsets of* G:

$$(*)\qquad \begin{array}{c} S_{ij}\quad (1\leqq i<j\leqq h,\ i\neq\rho(j)),\\ S_{\rho(j)j}-\{1\}\quad (2\leqq j\leqq h)\end{array}$$

and

$$T_i\quad (1\leqq i\leqq h)$$

where T_i is subset of S_{ii} satisfying $S_{ii}=T_i\cup T_i^{-1}$, $T_i\frown T_i^{-1}=\phi$, *are mutually disjoint, and that* Γ *is the free group over their union* S. Since $\sum_{j=1}^{h}|S_{ij}|=\sum_{i=1}^{h}|S_{ij}|=q+1$ by (6), this would show that if (ΓII) is satisfied, i.e. if $h<\infty$, then Γ is a free group with $(q-1)h/2+1$ generators.

(B) First, let $\gamma\in S_{ij}$, $\gamma\neq 1$ and put $\gamma=x_i^{-1}\pi x_j$, $\pi\in G_1$. *Then, the product* $x_i^{-1}\cdot\pi\cdot x_j$ *is free*, i.e. $l(\gamma)=l(x_i)+l(\pi)+l(x_j)$. In fact, let us first show that the product $\pi\cdot x_j$ is free. Suppose $j\neq 1$ (i.e. $x_j\neq 1$), otherwise it is trivial. Let $x_j=\pi_{i_l}\cdots\pi_{i_1}$ ($l=l(x_j)$) be the factorization which we defined above. Suppose $\pi\cdot x_j$ were not free, then $\pi\pi_{i_l}\in U$, i.e. $\gamma=x_i^{-1}u\pi_{i_{l-1}}\cdots\pi_{i_1}$ with $u\in U$, but we have shown that $x_{j'}=\pi_{i_{l-1}}\cdots\pi_{i_1}\in\mathfrak{R}$. Thus $x_{j'}=u^{-1}x_i\gamma\in Ux_i\Gamma$, and hence $j'=i$, and hence $\gamma=x_i^{-1}ux_i\in x_i^{-1}Ux_i$. By (ΓI) this implies $\gamma=1$, which is a contradiction to our hypothesis, and so, the product $\pi\cdot x_j$ is free. If we apply the same argument for $\gamma^{-1}\in S_{ji}$, we see that the product $x_i^{-1}\cdot\pi$ is also free, and hence by Lemma 2, the product $x_i^{-1}\cdot\pi\cdot x_j$ is free.

(C) Now let $\gamma=x_i^{-1}\pi x_j\in S_{ij}$, $\gamma'=x_k^{-1}\pi' x_l\in S_{kl}$, $\pi, \pi'\in G_1$, $\gamma, \gamma'\neq 1$, and consider the product $\gamma\gamma'=x_i^{-1}\pi x_j x_k^{-1}\pi' x_l$. *We shall show that*

$$(8)\qquad l(\gamma\gamma')=l(\gamma)+l(\gamma')-2d\quad \textit{with}\quad d\leqq \mathrm{Min}\,(l(x_j), l(x_k))$$

unless $(l, k)=(i, j)$ *and* $\gamma\gamma'=1$.

Put $x_j=\pi_{j_l}\cdots\pi_{j_1}$, $x_k=\pi_{k_m}\cdots\pi_{k_1}$, $l=l(x_j)$, $m=l(x_k)$, and put $l(x_jx_k^{-1})=l+m-2d'$ ($d'\leqq\mathrm{Min}\,(l, m)$ by Lemma 4). If $d'<\mathrm{Min}\,(l, m)$ then $d=d'<\mathrm{Min}\,(l, m)$ by Lemma 5; so (8) holds. So let us suppose that $d'=\mathrm{Min}\,(l, m)$. This implies that either $l > m$, and $k_1 = j_1, \cdots, k_m = j_m$ or $l < m$ and $j_1 = k_1, \cdots, j_l = k_l$, or $j = k$. First, assume that $l > m$ is the case. Then $\gamma\gamma' = x_i^{-1}\pi\pi_{j_1} \cdots \pi_{j_{m+1}}\pi' x_l$, and hence to show (8), it suffices to show that $\pi_{j_{m+1}}\pi' \notin U$. Suppose on the contrary that $\pi_{j_{m+1}}\pi' \in U$, and put $\pi_{j_{m+1}}x_k = x_{k'}$. (Since it is a right free factor of x_j, it belongs to $\mathfrak{R}$.) Then $x_{k'}x_k^{-1}\pi' \in U$, which implies that $x_{k'}\gamma' x_l^{-1} \in U$, and hence $k' = l$, and hence $\gamma' = 1$, which is a contradiction. So we have $\pi_{j_{m+1}}\pi' \notin U$, and hence (8) is valid for the case $l > m$. Just by the same manner, we see that (8) holds for the case $l < m$. Finally if $j = k$, (8) is equivalent with $\pi\pi' \notin U$. Suppose on the contrary that $\pi\pi' \in U$. Then $x_i^{-1}\gamma\gamma' x_k \in U$, and hence $x_k \in Ux_i\Gamma$ i.e. $k = i$ and $\gamma\gamma' \in x_i U x_i^{-1}$, and hence $\gamma' = \gamma^{-1}$, and (8) is completely proved.

This shows that the sets $(*)$ are mutually disjoint, and assertions (B) and (C) together enable us to apply the Corollary of Lemma 5 for the set

$$S = \bigcup_{\substack{1 \leqq i < j \leqq h \\ i \neq \rho(j)}} S_{ij} \bigcup_{2 \leqq j \leqq h} (S_{\rho(j)j} - \{1\}) \bigcup_{1 \leqq i \leqq h} T_i$$

which proves the theorem. Q. E. D.

Thus the following theorem is obtained from the above proof of Theorem 1.

THEOREM 1'. *Γ, and other notations being as in Theorem* 1 *and as in the proof of Theorem* 1 *(part (A)), the subsets* $(*)$ *of* Γ *are mutually disjoint and their union* $S = S(\Gamma)$ *is a set of free generators of* Γ.

REMARK. For each j $(2 \leqq j \leqq h)$, $i = \rho(j)$ is the minimum suffix $(1 \leqq i \leqq h)$ such that $S_{ij} \neq \phi$, In fact, if $\gamma = x_i^{-1}\pi x_j \in S_{ij}$, we have (by the definition of $x_i \in \mathfrak{R}$), $u\pi^{-1}x_i \geqq x_j$ where $u \in U$ is chosen such that $u\pi^{-1}x_i \in \Pi$. This implies $x_i \geqq x_{\rho(j)}$, i. e. $i \geqq \rho(j)$,

§ 3. Conjugacy classes of $\Gamma \subset G$ with given degree.

Throughout this section we assume that Γ is a subgroup of G satisfying (ΓI) and (ΓII), and hence is isomorphic to a free group with finite number of generators. For any conjugacy class $\{\gamma\} \neq \{1\}$ of Γ, we define its *degree* by

$$\deg\{\gamma\} = \min_{x \in G} l(x^{-1}\gamma x) \qquad (> 0).$$

Any element $\gamma \neq 1$ of Γ or conjugacy class $\{\gamma\} \neq \{1\}$ in Γ is called *primitive* if γ generates its centralizer in Γ (which is always free cyclic group); hence any element (resp conjugacy class) $\neq \{1\}$ in Γ is a positive power of the uniquely determined primitive element (resp. conjugacy class). Our purpose in this section is to count the number of primitive conjugacy classes of Γ with given degree, or what is the same, to evaluate the following formal infinite product:

$$Z_\Gamma(u)=\prod_P(1-u^{\deg P})^{-1} \tag{9}$$

where P runs over all primitive conjugacy classes of Γ. Taking log. of both sides of (9), we have

$$\log Z_\Gamma(u)=\sum_{P,m\geqq 1}\frac{u^{m\deg P}}{m}=\sum_{m=1}^{\infty}\frac{N_m}{m}u^m \tag{9$'$}$$

where $N_m=\sum_{\deg P\mid m}\deg P$ is the sum of $\deg P$ for all P such that $\deg P$ divides m. More generally, let ρ be a finite dimensional representation of Γ over a field of characteristic 0, and let $\chi(\gamma)(\gamma\in\Gamma)$ be the trace of $\rho(\gamma)$. Let us define $Z_\Gamma(u,\chi)$ by:

$$\left\{\begin{aligned}&\log Z_\Gamma(u,\chi)=\sum_{P,m\geqq 1}\frac{\chi(P^m)u^{m\deg P}}{m}=\sum_{m=1}^{\infty}\frac{N_{m,\chi}}{m}u^m\\ &\log Z_\Gamma(0,\chi)=1\end{aligned}\right. \tag{9$''$}$$

where $\chi(Q)=\chi(\gamma)$ for any conjugacy class $Q=\{\gamma\}$ in Γ and

$$N_{m,\chi}=\sum_{d\mid m}d\sum_{\deg P=d}\chi(P^{m/d}).$$

When $G=PL(2,k)$, k being a locally compact field under a discrete valuation, our $Z_\Gamma(u,\chi)$ is an analogue of Selberg's ζ functions for discrete subgroups of $SL(2,R)$. According to the structure theorems (Theorem 1$'$) in § 2, we can evaluate our $Z_\Gamma(u,\chi)$ algebraically (for general G). Namely, put $G=\sum_{i=1}^{h}Ux_i\Gamma$ $(h=|U\backslash G/\Gamma|)$, $S_{ij}^{(l)}=x_i^{-1}G_lx_j\frown\Gamma$, $S_{ij}=S_{ij}^{(1)}$ $(l\geqq 0,\ 1\leqq i,j\leqq h)$. Let φ be as in § 2 the homomorphism of the subring $\mathfrak{T}$ of $\mathfrak{R}(G,U)$ generated by G_l $(l=0,1,2,\cdots)$ into $M(h,Z[\Gamma])$ defined by

$$\varphi(G_l)=((\sum_{\gamma\in S_{ij}^{(l)}}\gamma)).$$

ρ can be extended to the representation of the group ring $Z[\Gamma]$ of Γ in a natural manner, and hence also to that of $M(h,Z[\Gamma])$. Thus

$$G_l\to A_l^\chi=((\sum_{\gamma\in S_{ij}^{(l)}}\rho(\gamma)))\qquad(l\geqq 0)$$

gives a representation of $\mathfrak{T}$ with degree $\chi(1)h$. (These notations will be kept throughout this section.) Then we have:

THEOREM 2. *The notations being as above, we have*

$$Z_\Gamma(u,\chi)=(1-u^2)^{-g_\chi}\det(1-A_1^\chi u+qu^2)^{-1} \tag{10}$$

where $g_\chi=(q-1)h\chi(1)/2$.

The proof of this will be given after another lemma. Let $\pi_0,\pi_1,\cdots,\pi_q$ be a set of representatives of $U\backslash G_1$, and let Π and its lexicographic orderings be defined as before. Let $x_1,\cdots,x_h\in\Pi$ be the smallest representatives of

$U\backslash G/\Gamma$ with respect to our ordering. As before put $S_{ij}^{(l)}=x_i^{-1}G_l x_j$, $S_{ij}=S_{ij}^{(1)}$ $(l\geqq 1, 1\leqq i, j\leqq h)$ for such x_i. Thus the sets S_{ij} $(1\leqq i<j\leqq h, i\neq\rho(j))$, $S_{\rho(j)j}-\{1\}(2\leqq j\leqq h)$, $T_i(1\leqq i\leqq h)$, where $S_{ii}=T_i\cup T_i^{-1}$, $T_i\cap T_i^{-1}=\phi$, are mutually disjoint and their union S constitutes a set of free generators of Γ.

LEMMA 6. *The notations being as above,*

(i) *Let i, j $(1\leqq i, j\leqq h)$ and $l\geqq 1$ be given. Then $S_{ij}^{(l)}$ consist of all elements γ of the form:*

$$\gamma=\sigma_{ii_1}\sigma_{i_1i_2}\cdots\sigma_{i_{l-1}j}, \tag{11}$$

where $i_1, \cdots, i_{l-1}$ are any set of indices among $\{1, 2, \cdots, h\}$ such that $S_{i_{m-1}i_m}$ are non-empty $(m=1, 2, \cdots, l-1$; we understand that $i_0=i$, $i_m=j)$; $\sigma_{i_{m-1}i_m}$ are any elements of $S_{i_{m-1}i_m}$ $(m=1, 2, \cdots, l-1)$ such that if $i_{m-1}=i_{m+1}$ then $\sigma_{i_{m-1}i_m}\sigma_{i_mi_{m+1}}\neq 1$.

Moreover for any element of $S_{ij}^{(l)}$ the expression (11) *is unique.* (*Since S is a set of free generators of Γ, this expression* (11) *is nothing but the expression of γ by the given free generators of Γ—the only thing different is that some of $\sigma_{i_{m-1}i_m}$ can be the identity* 1.)

(ii) *For the sake of simplicity put $\sigma_v=\sigma_{i_{v-1}i_v}$ $(1\leqq v\leqq l)$. Assume that $\sigma_l\sigma_1=\cdots=\sigma_{l-k+1}\sigma_k=1$, $\sigma_{l-k}\sigma_{k+1}\neq 1$ $(k\geqq 0)$. Then we have*

$$\deg\{\gamma\}=l-2k\,.$$

(iii) *Let $k=0$. Then the conjugates of γ in Γ which are contained in $S_{mn}^{(l)}$ for some $1\leqq m, n\leqq h$ are*

$$x=\sigma_1\sigma_2\cdots\sigma_l,\ \sigma_2\cdots\sigma_l\sigma_1,\ \cdots,\ \sigma_l\sigma_1\cdots\sigma_{l-1}\,.$$

If $r(r\geqq 1)$ of the above expressions coincides with x (e.g. $\sigma_1=\cdots=\sigma_r=1$ can happen), then x is contained in exactly r different $S_{mn}^{(l)}$'s (l is fixed).

PROOF. (i): Immediate, by homomorphism φ and (4) of §1. (ii), (iii): Immediate, by the fact that S is a set of free generators of Γ and that for any $\gamma\neq 1$ of Γ, $\deg\{\gamma\}$ is the smallest integer l such that γ is conjugate (in Γ) to some element of $\bigcup_{i=1}^{h} S_{ii}^{(l)}$. Q.E.D.

The above lemma shows that if $f(\gamma)$ is any class function on Γ whose value domain is an additive abelian group, then we have, for any positive integer m,

$$\sum_{i=1}^{h}\sum_{\substack{\gamma\in S_{ii}^{(m)};\\ \deg\{\gamma\}=m}} f(\gamma)=\sum_{d\mid m} d\sum_{\deg P=d} f(P^{m/d})\,. \tag{12}$$

Denote the both sides of (12) by $N_{m,f}$ and put

$$a_{m,f}=\sum_{i=1}^{h}\sum_{\gamma\in S_{ii}^{(m)}} f(\gamma)\qquad(m\geqq 1)\,.$$

Then by Lemma 6 (ii), we have

$$a_{m,f}=N_{m,f}+(q-1)\sum_{k=1}^{[m-1/2]} q^{k-1}N_{m-2k,f} \qquad (m\geqq 1) \tag{13}$$

or what is the same,

$$N_{m,f}=a_{m,f}-(q-1)\sum_{k=1}^{[m-1/2]} a_{m-2k,f}\,. \tag{13'}$$

The proof of Theorem 2. In (13′) put $f=\chi$, the character of ρ. Thus $N_{m,\chi}$ coincides with the one defined by (9″), and we have $a_{m,\chi}=\mathrm{tr}.\,A_m^\chi$. Now (1), (2) of § 1 is equivalent with the following equality between the formal power series:

$$\sum_{m=0}^{\infty} G_m x^m=(1-x^2)(1-G_1x+qx^2)^{-1},$$

where $G_m (m\geqq 0)$ are considered as elements of $\mathfrak{T}\subset\mathfrak{R}(G, U)$. Since $G_m\rightarrow A_m^\chi$ gives a representation of $\mathfrak{T}$. we have

$$\sum_{m=0}^{\infty} A_m^\chi x^m=(1-x^2)(1-A_1^\chi x+qx^2)^{-1}\,. \tag{14}$$

Let $a_1, \cdots, a_m$ $(M=\chi(1)h)$ be the eigenvalues of A_1^χ and put $1-a_ix+qx^2=(1-\alpha_ix)(1-\alpha_i'x)$ $(1\leqq i\leqq M)$. Then, by (14), the eigenvalues of A_m^χ $(m\geqq 1)$ are

$$\alpha_i^m+\alpha_i'^m+(q-1)\sum_{k=1}^{[m/2]-1} q^{k-1}(\alpha_i^{m-2k}+\alpha_i'^{m-2k})+\varepsilon_i(m) \;\; (1\leqq i\leqq m)$$

where $\varepsilon_i(m)=q^{m/2}-q^{m/2-1}(m$ even), $=(q^{m-1/2}-q^{m-3/2})(\alpha_i+\alpha_i')$ (m odd). From this follows directly that the eigenvalues of

$$A_m^\chi-(q-1)\sum_{k=1}^{[m/2]} A_{m-2k}^\chi \qquad (m\geqq 1)$$

are $\alpha_i^m+\alpha_i'^m$ $(1\leqq i\leqq M)$; hence we have:

$$a_{m,\chi}-(q-1)\sum_{k=1}^{[m/2]} a_{m-2k,\chi}=\sum_{i=1}^{M}(\alpha_i^m+\alpha_i'^m). \tag{15}$$

By (13′) and (15), we have

$$N_{m,\chi}=\sum_{i=1}^{h}(\alpha_i^m+\alpha_i'^m)+\begin{cases}(q-1)h\chi(1) \cdots m:\text{even}\\ 0 \qquad\qquad\;\; \cdots m:\text{odd}.\end{cases} \tag{16}$$

Now our theorem follows immediately from (16). Q. E. D.

Remark 1. In the case of $G=PL(2, k)$, k being a locally compact field under a discrete valuation, the above formulae (10) can also be obtained by spectral decomposition of induced representation $\underset{\Gamma\uparrow G}{\mathrm{Ind.}}\,\rho$ and by calculating its trace by making use of Gelfand-Graev's trace formula for unitary representations of $SL(2, k)$. Comparing this with our algebraically obtained formula

(10), we get information on the multiplicity of "special representation" (analogue of the first member of the discrete series in $SL(2, R)$-case) (cf. Gelfand-Graev [1]) of G in $L^2(G/\Gamma)$. Cf. [2], § 2—determinant part correspond to principal series of class one (more or less well-known), and $(1-u^2)^{-g_x}$ correspond to "special representation" part.

REMARK 2. As before, put

$$\det(1-A_1^* u+qu^2)=\prod_{i=1}^{M}(1-\alpha_i u)(1-\alpha_i' u),\ \alpha_i\alpha_i'=q.$$

If ρ is unitary, then A_1^* are hermitian, and hence $a_i=\alpha_i+\alpha_i'$ are real. By a trivial estimation (cf. the proposition below) we have $|a_i|\leqq q+1$ $(1\leqq i\leqq M)$, and $|a_i|<q+1$ except for some obvious cases. But *in general (even if* $\rho=1$), *it is not true that* $|\alpha_i|=|\alpha_i'|=q^{1/2}$ (or equivalently that $|a_i|\leqq 2q^{1/2}$). In the case where $G=PL(2, k)$, k being the same as in the previous remark, it is equivalent to say that *in general* $L^2(G/\Gamma)$ *contains supplementary series.* By Corollary 2 of Theorem 3 (§ 4) it is easy to construct such examples. Some of them are given in [2], § 4.

Although Ramanujan's conjecture for p-part of some modular cusp forms (which belong to some congruence subgroups of the modular group) is equivalent with the statement that, for certain Γ and ρ, $\operatorname{Ind}_{\Gamma\uparrow G}\rho$ does not contain supplementary series, such examples seem to diminish the hope of proving it by group theoretical methods. As for corresponding polynomials (and examples of analogue of Ramanujan's conjectures) for discrete subgroups of $Sp(4, Q_p)$, cf. [4] (though stated in different formulations).

Finally put $G'=\bigcup_{i=0}^{\infty} G_{2l}$. By (G, l, I, II), G' forms a normal subgroup of G with index two in G. Put $\Gamma'=G'\cap\Gamma$ and define sgn by $\operatorname{sgn}\gamma=1$ for $\gamma\in\Gamma'$, $=-1$ for $\gamma\notin\Gamma'$, Then we have:

PROPOSITION. *If* ρ *is unitary, then* $|a_i|\leqq q+1$ $(1\leqq i\leqq M)$. *If moreover* ρ *is irreducible and not* 1 *or* sgn, *then* $|a_i|<q+1$. *When* $\rho=1$ (resp. sgn), A_1^* *has* $q+1$ (resp. $-(q+1)$) *as an eigenvalue with multiplicity one* (*when* $\Gamma=\Gamma'$, *both* $\pm(q+1)$ *are simple eigenvalues*).

PROOF. First let us recall that $S_{\rho(p)j}\neq\phi$ for any $j=2, \cdots, h$. So, for any two given indices i, j $(1\leqq i\neq j\leqq h)$ we can find a sequence $i=i_1, i_2, \cdots, i_r=j$ of indices among $\{1, 2, \cdots, h\}$ such that $S_{i_\nu i_{\nu+1}}\neq\phi$ for $\nu=1, 2, \cdots, r-1$.

Let $\mathfrak{M}$ be the (unitary) representation space of ρ. Let $x={}^t(x_1, x_2, \cdots, x_h)$; $x_i\in\mathfrak{M}$ $(1\leqq i\leqq h)$ be an eigenvector of A_1^*. Thus $A_1^*x=\lambda x$ with some real λ. We can assume that $\|x_{i_0}\|=\operatorname{Max}_{1\leqq i\leqq h}\|x_i\|=1$ for some i_0, where $\|\ \|$ denotes the metric of $\mathfrak{M}$. Thus we have $\sum_{j=1}^{h}\sum_{\gamma\in S_{i_0 j}}\rho(\gamma)x_j=\lambda x_{i_0}$. Since $\sum_{j-1}^{h}|S_{i_0 j}|=q+1$, by taking $\|\ \|$ of both sides we obtain $|\lambda|\leqq q+1$. If $\lambda=q+1$ we have $A_1^*x=(q^l+q^{l-1})x$

for $l=1, 2, \cdots$, and $\| x_1 \| = \cdots = \| x_h \|$. Then it follows directly that for any $\gamma \in S_{ij}^{(l)}$ we have $\rho(\gamma)x_j = x_i$. Since any element γ of Γ is contained in $S_{11}^{(l)}$ for some l, we have $\rho(\gamma)x_1 = x_1$ for all $\gamma \in \Gamma$, and so if ρ is irreducible ρ must be 1, and hence $x_1 = x_2 = \cdots = x_h$. If $\lambda = -(q+1)$ we obtain $A_l^* x = (-1)^l (q^l + q^{l-1})x$, for $l=1, 2, \cdots$, and $\rho(\gamma)x_1 = \operatorname{sgn}(\gamma)x_1$ for any $\gamma \in \Gamma$. Hence, by irreducibility we have $\rho(\gamma) = \operatorname{sgn}(\gamma)$, and the equation $\rho(\gamma)x_i = -x_j$ for all $\gamma \in S_{ij}$ determines $x_1, \cdots, x_n$ up to a scalar multiple. Q. E. D.

§ 4. The construction of Γ.

Our purpose in this section is to construct (all) Γ satisfying (ΓI). For the sake of simplicity we assume here that:

ASSUMPTION IN § 4: G_1 consists of a single U-double-coset, or, what is the same, (G, l) are those constructed in example 3 (§ 1 and § 5, Supplement 1). E. g. $G = PL(2, k)$ satisfies this.

Let us first treat the simplest case where $h = |\Gamma \backslash G/U| = 1$, i. e. $G = U\Gamma$. In this case Γ is generated by $G_1 \cap \Gamma$ which can be expressed as $G_1 \cap \Gamma = T \cup T^{-1}$, $T \cap T^{-1} = \phi$, $G_1 = \sum_{\gamma \in T} U\gamma + \sum_{\gamma \in T} U\gamma^{-1}$ (disjoint). So $q+1$ must be even (and in this case it can be seen directly by Lemma 1 and corollary of Lemma 5 that Γ is a free group over T). Conversely, suppose that $q+1$ is even. Let σ be any substitution on the set of indices $\{0, 1, 2, \cdots, q\}$ such that $\sigma^2 = 1$ and that $\sigma(i) \neq i$ for all i $(0 \leqq i \leqq q)$. Let $G_1 = \sum_{i=0}^{q} U\pi_i$ and choose any element z_i from $U\pi_i \cap \pi_{\sigma(i)}^{-1} U$ $(0 \leqq i \leqq q, \neq \phi$ by our assumption) in such a way that $z_{\sigma(i)} = z_i^{-1}$ for all i. Then, if we put $\{z_0, \cdots, z_q\} = T \cup T^{-1}$, $T \cap T^{-1} = \phi$, from Lemma 1 and corollary of Lemma 5, it follows that T generates a (free) subgroup Γ of G satisfying ($\Gamma I, II$) with $h=1$.

Now we shall briefly discuss the general case. Let $\pi_0, \pi_1, \cdots, \pi_q$ be again a set of representatives of $U \backslash G_1$ and let Π_l, Π and its lexicographic orderings be defined as before. For each $i = 0, 1, 2, \cdots, q$, put $U\pi_i^{-1} = U\pi_{\varphi(i)}$, with $0 \leqq \varphi(i) \leqq q$.

For any $1 \leqq h \leqq \infty$, assume that we are given some $h \times h$ matrix $A = ((a_{ij}))$ satisfying the following properties (A1-3).

(A1) a_{ij} $(1 \leqq i, j \leqq h)$ are non-negative rational integers, and a_{ii} $(1 \leqq i \leqq h)$ are even.

(A2) $a_{ij} = a_{ji}$ $(1 \leqq i, j \leqq h)$ and $\sum_{i=1}^{h} a_{ij} = q+1$ for each $j (1 \leqq j \leqq h)$. (Hence for each i (resp. j) there exists only a finite number of j (resp. i) such that $a_{ij} \neq 0$).

(A3) For each $i > 1$ let $j = \rho(i)$ be the minimum suffix j such that $a_{ij} \neq 0$. Then $\rho(i) < i$ and $\rho(2) \leqq \rho(3) \leqq \cdots$.

These properties are possessed by the matrix $A = ((|x_i^{-1} G_1 x_j \cap \Gamma|))$ where

Γ is a subgroup of G satisfying (ΓI) and where $\mathfrak{R}=\{1=x_1<x_2<\cdots\}\subset\Pi$ is the set of "smallest" representatives of $U\backslash G/\Gamma$ (i. e. $x_i=\mathrm{Min}\,(Ux_i\Gamma\cap\Pi)$) (cf. § 2). Our problem here is, conversely, for given A satisfying (A1-3), to construct (all) Γ satisfying (ΓI) such that $A=((|x_i^{-1}G_1x_j\cap\Gamma|))$.

Put $Q=\{0,1,2,\cdots,q\}$. For any (i,j) $1\leqq i,j\leqq h$, we choose a subset P_{ij} of Q satisfying the following conditions.

(P1) $|P_{ij}|=a_{ij}$ $(1\leqq i,j\leqq h)$.

(P2) For each $j(1\leqq j\leqq h)$, $Q=\sum_{i=1}^{h}P_{ij}$ (disjoint).

(P3) For each $i>1$, let μ_i be the minimum element of $P_{i\rho(i)}$.
Then $\varphi(\mu_i)\in P_{\rho(i)i}$; and for each given $j\geqq 1$ and $i,i'>1$ such that $\rho(i)=\rho(i')=j$, we assume $\mu_i>\mu_{i'}$ if and only if $i>i'$.

Since $\rho(i)<i$, and since we can start choosing P_{ij} from smaller j's, it is clear that it is possible to choose such $\{P_{ij};1\leqq i,j\leqq h\}$. Now for each i,j $(1\leqq i,j\leqq h)$, we choose a bijection σ_{ij} of P_{ij} on P_{ji} such that $\sigma_{ij}\sigma_{ji}=1$, $\sigma_{i\rho(i)}(\mu_i)=\varphi(\mu_i)$ for $i>1$, and $\sigma_{ii}(\nu)\neq\nu$ for each $\nu\in P_{ii}$. (This is possible since $|P_{ii}|=a_{ii}$ is even.) For each i,j and $\nu\in P_{ij}$ choose *any* element $x_{ij}^{(\nu)}$ out of $U\pi_\nu\cap\pi_{\sigma_{ij}\nu}^{-1}U(\neq\phi$ by our assumption on $(G,l))$ in such a way that $x_{ji}^{(\sigma_{ij}(\nu))}=x_{ij}^{(\nu)-1}$ holds for each i,j,ν and that $x_{i\rho(i)}^{(\mu_i)}=\pi_{\mu_i}$ (hence $x_{\rho(i)i}^{\varphi(\mu_i)}=\pi_{\mu_i}^{-1}$) for each $i>1$. Define $x_1,x_2,\cdots$ inductively by $x_1=1$, $x_i=\pi_{\mu_i}x_{\rho(i)}$ for each $i>1$. (Thus $x_i\in\Pi$ for all $i=1,2,\cdots$, and by (P3), $1=x_1<x_2<\cdots$) Put $\boldsymbol{P}_{ij}=\{x_{ij}^{(\nu)}|\nu\in P_{ij}\}\subset G_1$, $S_{ij}=x_i^{-1}\boldsymbol{P}_{ij}x_j$ $(1\leqq i,j\leqq h)$. Thus $S_{i\rho(i)}\ni 1$ for $i>1$. Then we have:

THEOREM 3. *The notations being as above, the subgroup Γ of G generated by all S_{ij} $(1\leqq i,j\leqq h)$ satisfies (ΓI). Moreover $\mathfrak{R}=\{1=x_1<x_2<\cdots\}$ constitutes a complete set of representatives of $U\backslash G/\Gamma$ with $x_i=\mathrm{Min}\,(Ux_i\Gamma\cap\Pi)$ $(i=1,2,\cdots)$; and $x_i^{-1}G_1x_j\cap\Gamma=S_{ij}$ (hence $G_1\cap x_i\Gamma x_j^{-1}=\boldsymbol{P}_{ij}$, and $A=((|x_i^{-1}G_1x_j\cap\Gamma|))$ holds for each i,j $(1\leqq i,j\leqq h)$).*

Conversely every subgroup Γ of G satisfying (ΓI) is constructed in this manner.

SKETCH OF PROOF. Converse part is essentially proved in § 2.

Now, by our construction, the family of subsets $\boldsymbol{P}_{ij}(1\leqq i,j\leqq h)$ of G_1 has the following properties (i)-(v).

(i) $x\in\boldsymbol{P}_{ij}$ $y\in\boldsymbol{P}_{kj}$ $x\neq y\rightarrow Ux\neq Uy$.
$x\in\boldsymbol{P}_{ij}$ $y\in\boldsymbol{P}_{ik}$ $x\neq y\rightarrow xU\neq yU$.

(ii) $\boldsymbol{P}_{ij}^{-1}=\boldsymbol{P}_{ji}$ $x\in\boldsymbol{P}_{ii}\rightarrow Ux\neq Ux^{-1}$.

(iii) $\sum_{i=1}^{h}|\boldsymbol{P}_{ij}|=q+1$ $\forall j=1,2,\cdots,h$.

(iv) $x\in\boldsymbol{P}_{ij}\rightarrow ux^{-1}x_i\geqq x_j$, $u'xx_j\geqq x_i$ where $u,u'\in U$ are so chosen that $ux^{-1}x_i$, $u'xx_j\in\Pi$. Equalities hold if and only if $j=\rho(i)$, $x=\pi_{\mu_i}$, $u=u'=1$ or $i=\rho(j)$ $x=\pi_{\mu_j}^{-1}$, $u=u'=1$.

(v) For any $i>1$, $\boldsymbol{P}_{i\rho(i)}\ni\pi_{\mu_i}$.

(All except (iv) are direct consequences of our construction. As for (iv), since $\boldsymbol{P}_{ij}=\boldsymbol{P}_{ji}^{-1}$ we need only check $u'xx_j \geqq x_i$. First, assume that $l(x_j) \geqq l(x_i)$. Since $x_j=\pi_{\mu_j}x_{\rho(j)}$, we have $l(u'xx_j)=1+l(x_j)>l(x_i)$; hence $u'xx_j>x_i$ unless $x\pi_{\mu_j} \in U$. But $\boldsymbol{P}_{\rho(j)j} \ni \pi_{\mu_j}^{-1}$ by (v); hence if $Ux=U\pi_{\mu_j}^{-1}$, (i) shows that $i=\rho(j)$, $x=\pi_{\mu_j}^{-1}$ must be the case. In this case $u=1$, $xx_j=x_i$. Secondly assume that $l(x_j)<l(x_i)$, Since we assume that $\boldsymbol{P}_{ij} \neq \phi$ we have $j \geqq \rho(i)$ and hence $x_j \geqq x_{\rho(i)}$, If $j>\rho(i)$ then by our definition of ordering we have $u'xx_j>\pi_{\mu_i}x_{\rho(i)}=x_i$. If $j=\rho(i)$, by our choice of μ_i (minimum element of $P_{i\rho(i)}$) we have $u'xx_j \geqq x_i$, the equality being valid if and only if $x=\pi_{\mu_i}$ (and hence $u'=1$); hence (iv) is verified.)

By using (i)-(v) we can prove the theorem without any difficulties. Let Γ be the subgroup of G generated by all S_{ij} $(1 \leqq i, j \leqq h)$. First, we can verify that if $x \in \Pi$ is not contained in $\mathfrak{R}$ then $\bigcup_{i,j}(UxS_{ij}) \cap \Pi \subset Ux\Gamma \cap \Pi$ contains an element which is smaller than x. (In fact put $x=\pi_{i_l} \cdots \pi_{i_1}$ $y_m=\pi_{i_{m-1}} \cdots \pi_{i_1}$ $(0 \leqq m \leqq l, y_0=1)$ and let $m=m_0$ be the maximum suffix for which $y_m \in \mathfrak{R}$. Put $y_{m_0}=x_k$. Let j be the suffix for which $P_{jk} \ni i_{m_0}$. Then $x_j<y_{m_0+1}=\pi_{i_{m_0}}x_k$ by (iv), and hence if we put $\gamma=x_k^{-1}\pi_{i_{m_0}}^{-1}x_j \in S_{kj}$, we have $x\gamma<x$.) Since, by the property of our ordering, $Ux\Gamma \cap \Pi$ must have the minimum element, we have $G=\bigcup_{i=1}^{h} Ux_i\Gamma$.

By (i), (ii), (v) and corollary of Lemma 5 in §2 it is easy to see that S_{ij} $(1 \leqq j<i \leqq h\ j \neq \rho(i))$, $S_{i\rho(i)}$ $(2 \leqq i \leqq h)$, T_i $(1 \leqq i \leqq h)$; where $S_{ii}=T_i \cup T_i^{-1}$, $T_i \cap T_i^{-1}=\phi$, are mutually disjoint and their union S is a set of free generators of Γ, i.e. Γ is a free group over S. In particular Γ is torsion-free. To verify $\Gamma \cap x^{-1}Ux=\{1\}$ for all $x \in G$, it is enough to see $\Gamma \cap x_i^{-1}Ux_i=\{1\}$ for $i=1; 2, \cdots$, which can be verified in the same manner. The disjointness of $Ux_i\Gamma(1 \leqq i \leqq h)$ is as follows. Let us suppose that $x_i=ux_j\gamma_1 \cdots \gamma_t$ for some $i \neq j$, where $u \in U$ and $\gamma_\nu \in S_{i_\nu j_\nu}$ for some i_ν, j_ν, and let $\gamma_1 \cdots \gamma_t$ be the reduced expression. Put $\gamma_t=x_{i_t}^{-1}\pi x_{j_t}$. Then in the factorization of x_i, πx_{j_t} must appear on the right side, i.e. $x_i=z \cdot (\pi x_{j_t})$ (free product) with some $z \in G$. Then $\pi x_{j_t}=u'x_k$ with some $u' \in U$ and k, which is impossible by (i) and (v). Now if we put $S'_{ij}=x_i^{-1}\Gamma x_j \cap G_1 \supset S_{ij}$, $\sum_{i=1}^{h}|S'_{ij}|=q+1=\sum_{i=1}^{h}|S_{ij}|$ must hold; hence $S'_{ij}=S_{ij}$. Q.E.D.

COROLLARY 1. *Assume that G satisfies the assumption of §4 and let Γ be a subgroup of G satisfying $(\Gamma I, II)$. Then there exists a subgroup $U'=U'(\Gamma)$ of U with finite index in U such that if $S=\{z_1, \cdots, z_t\}$ is a set of free generators of Γ and if $u_1, \cdots, u_t \in U'$, then $S'=\{u_1z_1, \cdots, u_tz_t\}$ also generates a free group Γ' over S' which satisfies $(\Gamma I, II)$ with $|U\backslash G/\Gamma'|=|U\backslash G/\Gamma|$.*

COROLLARY 2. *Let G be as above, let h be a positive integer and let A be an $h \times h$ matrix whose entries are non-negative integers. Then A can be ex-*

pressed as $A=((|\Gamma\cap x_i^{-1}G_1x_j|))$ *by some subgroup* Γ *of* G *satisfying* $(\Gamma I, II)$ *and by some set of representatives* $x_1, \cdots, x_h$ *of* $U\backslash G/\Gamma$ *if and only if there exists a substitution matrix* T *such that* $T^{-1}AT$ *satisfies* (A1-3).

§ 5. Supplements.

1. *On example 3 of* § 1. (Construction of (G, l) satisfying (G, l, I, II) such that G_1 consists of only one U-double-coset.)

Let U be a group with a proper subgroup H_1 such that $(U:H_1)<\infty$ and let H be another group which has a subgroup H_2 with $(H:H_2)=2$. Assume that there exists an isomorphism θ of H_1 onto H_2. Let G be the free product of U, H with amalgamated subgroups $H_i(i=1, 2)$, i. e. the free product of U, H modulo all relations which arise by identification of elements of H_1 and H_2 by θ. If $1=M_1.\cdots, M_n$ $(n=(U:H_j))$ are the set of representatives of $H_1\backslash U$ and if σ is any element of H not contained in H_2, then every element of G can be expressed *uniquely* (cf. e. g. A. G. Kurosh [5]) in the form

$$x=hM_i\sigma M_j\sigma\cdots$$

or

$$=h\sigma M_i\sigma M_j\cdots$$

where $h\in H_1$ (identified by θ with H_2), $i, j, \cdots\neq 1$. Let $l(x)$ be the number of σ's in the above expression. Then (G, l) satisfies (G, l, I, II) with $U=G_0$, $q+1=(U:H_1)$ and G_1 consists of a single U-double-coset. Conversely every such (G, l) can be defined in this way. In fact if $x\in G_1$ by our assumption we have $xU\cap Ux^{-1}\neq\phi$. Let σ be any element of $xU\cap Ux^{-1}$, and so $\sigma^{-1}\in U\sigma\cap\sigma U$. Put $H_2=\sigma^{-1}U\sigma\cap U$. Then it is easy to see (e. g. by Lemma 1) that G is the free product of U and $H_2\sigma$ with an amalgamated subgroup H_2.

2. "$\mathfrak{p}$*-unit groups*" *of totally definite quaternion algebras.*

Let D be a totally definite quaternion algebra over a totally real algebraic number field F. Let $\mathfrak{p}$ be a finite prime of F which does not divide the discriminant of D. Let $\mathfrak{g}$ be the maximal order of F and let $\mathfrak{o}$ be a $\mathfrak{g}$-order of D such that $\mathfrak{o}\underset{\mathfrak{g}}{\otimes}\mathfrak{g}_{\mathfrak{p}}$ is maximal. Put

$\tilde{\Gamma}=\{a\in D\,|\,a\in\mathfrak{p}^{\lambda}\mathfrak{o}$ for some $\lambda\in\boldsymbol{Z}$ and $(Na)=\mathfrak{p}^{\mu}$ for some $\mu\in\boldsymbol{Z}\}$

$\Gamma=\tilde{\Gamma}/\tilde{\Gamma}\cap F^{\times}$.

Then, by the isomorphism

$D\underset{F}{\otimes}F_{\mathfrak{p}}\cong M(2, F_{\mathfrak{p}})$, where $F_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-adic completion of F, Γ can be regarded as a discrete subgroup of $G=PL(2, F_{\mathfrak{p}})$ with compact quotient space (finiteness of group index between unit groups of $\mathfrak{o}$ and that of F, and finiteness of class number of $\mathfrak{o}$). Thus if Γ is torsion-free (of course if we take a suitable suborder $\mathfrak{o}'$ of $\mathfrak{o}$, Γ' defined from $\mathfrak{o}'$ will be so), then it is free group with $\frac{1}{2}(q-1)h+1$ generators, where $q=N\mathfrak{p}$, and $h=|U\backslash G/\Gamma|$, $U=PL(2,\mathfrak{g}_{\mathfrak{p}})$. Now, h is the number of such left $\mathfrak{o}$-ideal classes (we only consider such ideals whose left orders are $\mathfrak{o}$) that are represented by some ideals which coincide with $\mathfrak{o}$ except at $\mathfrak{p}$; and by Eichler-Kneser's (generalized) approximation theorem on quaternion algebra, if $\mathfrak{o}$ is maximal it is equal to the quotient of the class number of D by the class number of F with respect to the ideal group generated by $\mathfrak{p}$ and all ideals of the form (a), a: totally positive.

University of Tokyo, and
The Institute for Advanced Study

References

[1] Gelfand-Graev, Representations of a group of matrices of the second order with elements from a locally compact field, Uspehi Mat. Nauk, **18** (1963). English translation: Russian Math. Surveys, **18** (1963), 29-100.

[2] Y. Ihara, Discrete subgroups of $PL(2, k_{\mathfrak{p}})$, Proceedings of Symposia in Pure Mathematics Series (to appear).

[3] Y. Ihara, Algebraic curves mod. p and arithmetic groups, Ibid, (to appear).

[4] Y. Ihara, On certain arithmetical Dirichlet series, J. Math. Soc. Japan, **16** (1964) 214-225.

[5] A.G. Kurosh, The theory of groups (Vol. 2), Chelsea, New York, 1956.

[6] I. Mautner, Spherical functions over $\mathfrak{p}$-adic fields II, Amer. J. Math., **86** (1964), 171-200.

[7] I. Satake, Theory of spherical functions on reductive algebraic groups over $\mathfrak{p}$-adic fields, Inst. Hautes Études Sci. Publ. Math., **18** (1963), 1-69.

[8] I. Satake, Spherical functions and Ramanujan's conjectures, Proceedings of Symposia in Pure Mathematics Series (to appear).

[9] T. Tamagawa, Discrete subgroups of $\mathfrak{p}$-adic algebraic groups (to appear).