Изв. Росс. Акад. Наук
Сер. Матем. Том 56 (1992), № 3

Russian Acad. Sci. Izv. Math.
Vol. 40 (1993), No. 3

ABSTRACT PROPERTIES OF S-ARITHMETIC GROUPS AND THE CONGRUENCE PROBLEM

UDC 512.743

V. P. PLATONOV AND A. S. RAPINCHUK

ABSTRACT. Suppose G is a simple and simply connected algebraic group over an algebraic number field K and S is a finite set of valuations of K containing all Archimedean valuations. This paper is a study of the connections between abstract properties of the S-arithmetic subgroup $\Gamma = G_{O(S)}$ and the congruence property, i.e. the finiteness of the corresponding congruence kernel $C = C^S(G)$. In particular, it is shown that if the profinite completion $\Delta = \widehat{\Gamma}$ satisfies condition (PG), (i.e., for any integer $n > 0$ and any prime p there exist c and k such that $|\Delta/\Delta^{np^\alpha}| \leq cp^{k\alpha}$ for all $\alpha > 0$), then C is finite. Examples are given demonstrating the possibility of effectively verifying (PG)′.

§1. Introduction and statement of the main results

Suppose G is a simple and simply connected algebraic group defined over an algebraic number field K and S is a finite subset of the set V^K of all pairwise inequivalent valuations of K containing the set V_∞^K of Archimedean valuations. We denote by $O(S)$ the ring of S-integers of K and by $\Gamma = G_{O(S)}$ the group of S-integral points of G. It is well known (see [7] and [25]) that the solution of the congruence problem for Γ is equivalent to the calculation of the congruence kernel $C = C^S(G)$; if C is finite, we say that Γ *has the congruence property* (CSP). Hypothetical finiteness conditions were stated by Serre [12] in the following form:

$$C \text{ is finite if } \operatorname{rank}_S G = \sum_{v \in S} \operatorname{rank}_{K_v} G \geq 2$$
$$\text{and } G \text{ is } K_v\text{-isotropic for any } v \in S \setminus V_\infty^K.$$

At present Serre's conjecture has been proved for many types of groups [25], but there remains an important class of groups, which includes, for example, the groups of the form $\mathrm{SL}_1(D)$, where D is a finite-dimensional central division algebra over K, for which it is still inaccessible. Even in the minimal case where D is the division ring of quaternions we did not have a single example of an S-arithmetic group with the congruence property. Such examples have appeared only very recently, thanks to the development of an essentially new approach to the congruence problem suggested by the present authors. The underlying idea is to analyze abstract properties of S-arithmetic groups that imply the congruence property. Historically, the first such property was that of finiteness of width (or the bounded generation property (BG)).

Definition. We say that an *abstract group* Γ *has finite width at most* t if there exist elements $\gamma_1, \ldots, \gamma_t \in \Gamma$ such that $\Gamma = \langle\gamma_1\rangle \cdots \langle\gamma_t\rangle$, where $\langle\gamma_i\rangle$ is the cyclic subgroup generated by γ_i.

1991 *Mathematics Subject Classification.* Primary 20G30, 11E57, 20H05.

This abstract definition was motivated to a large extent by [15], in which it was shown that any matrix in $SL_n(O)$, where $n \geq 3$ and O is the ring of integers of the algebraic number field K, is a product of a bounded number of elementary matrices. The paper [15] was mainly oriented towards the solution of a problem in algebraic K-theory (namely, that of the triviality of the SK_1-functor for the so-called nonstandard of rings of algebraic integers), but by virtue of its methods and technical tools (Mennicke symbols, etc.) it had much in common with papers on the congruence problem.

After analyzing the argument in [15] and several other circumstances, the second author conjectured two years ago that for the groups $\Gamma = G_{O(S)}$ the congruence property (CSP) and the bounded generation property (BG) are equivalent. (A discussion of this conjecture can be found in Chapter IV of our book [8].) In view of the classical results of Bass-Milnor-Serre [1], the results of [15] corroborate this conjecture for the groups $G = SL_n$ $(n \geq 3)$. Further support for this conjecture was obtained by Tavgen' [14], who established the bounded generation property for arithmetic and S-arithmetic subgroups of Chevalley groups of rank at least 2 of the ordinary and most of the twisted types (the congruence property for these groups was established by Matsumoto [19] and Deodhar [16]).

We will also give examples of a converse nature: for the groups $SL_2(\mathbf{Z})$ and $SL_2(O)$, where O is the ring of integers of an imaginary quadratic field, the properties (CSP) and (BG) do not hold. In all of these cases, satisfaction or nonsatisfaction of each of the properties (CSP) and (BG) was established separately, but it turned out a posteriori that they were present or absent simultaneously. Of the most interest, however, was the investigation of direct connections between (CSP) and (BG). The first result in this direction, which was obtained in [10], asserts that if the group $\Gamma = G_{O(S)}$ has finite width, then the abelianization $C^{ab} = C/[C, C]$ of the congruence kernel is a finite group.

In this paper it will be shown that finiteness of the width of Γ implies finiteness of the whole congruence kernel, i.e., the property (CSP) (see Corollary 1). We obtain this result (also proved a little later by A. Lubotsky) from more general ones, in which the conditions on Γ are significantly weaker (Theorem 1). On the other hand, F. Grunewald recently found, with the aid of a computer, examples of groups of finite width among the groups of the form $G_{\mathbf{Z}(S)}$, where $G = SL_1(D)$, D is the division ring of quaternions over $\mathbf{Q}$, and $S = \{\infty, p\}$, which are the first examples of quaternion groups with the congruence property.

To state the main results we single out a number of properties of the profinite completion $\widehat{\Gamma}$ of Γ.

Definition. Suppose Δ is a finitely generated profinite group.

1) *The group Δ has finite width at most t as a profinite group* (i.e. has property $(BG)_{pf}$) if there exist elements $\delta_1, \ldots, \delta_t \in \Delta$ such that $\Delta = \overline{\langle \delta_1 \rangle} \cdots \overline{\langle \delta_t \rangle}$, where $\overline{\langle \delta_i \rangle}$ is the closure of the cyclic subgroup generated by δ_i.

2) *The nth Burnside factor Δ_n of Δ* is the factor group Δ/Δ^n with respect to the (closed) subgroup Δ^n generated by the nth powers of all elements of Δ (according to [2], the group Δ_n is finite for any n).

3) *The group Δ satisfies the condition* (PG) *of polynomial growth of the orders of the Burnside factors* if there exist constants c and k such that $|\Delta_n| \leq cn^k$ for all n.

4) *The group Δ satisfies condition* $(PG)'$ if for any natural number n and any prime p there exist c and k such that $|\Delta_{np^\alpha}| \leq cp^{k\alpha}$ for all integers $\alpha > 0$.

It is easy to see that condition (BG) for a discrete finitely generated group Γ

implies condition $(BG)_{pf}$ for its profinite completion $\widehat{\Gamma}$. Moreover, the profinite Burnside factor $\widehat{\Gamma}_n$ is a maximal finite factor group of the discrete Burnside factor Γ_n, which is defined as the factor group Γ/Γ^n with respect to the subgroup generated by the nth powers, so that if Γ_n is finite, then $|\Gamma_n| = |\widehat{\Gamma}_n|$. On the other hand, for any profinite group Δ we have the chain of implications $(BG)_{pf} \Rightarrow (PG) \Rightarrow (PG)'$. It would therefore be interesting to know whether or not any two of these conditions are equivalent in general. (It follows from Theorem 2, stated below, that all of these conditions are equivalent for profinite completions of S-arithmetic subgroups of simple, simply connected groups. Moreover, for a pro-p-group Δ each of these conditions is equivalent to analyticity; see Proposition 5.)

We will also need a standard description of the normal subgroups of G_K:

(1) *If* $T = \{v \in V_f^K = V^K \setminus V_\infty^K | G$ *is* K_v*-anisotropic*$\}$, *then for any non-central normal subgroup* $N \subset G_K$ *there exists an open normal subgroup* $W \subset G_T = \prod_{v \in T} G_{K_v}$ *such that* $N = G_K \cap W$.

(At present, (1) has been proved for most types of simple groups; see Chapter IX of [8].)

Theorem 1. *Assume that a group* G *satisfies condition* (1) *and* $S \cap T = \varnothing$. *If the profinite completion* $\widehat{\Gamma}$ *of the group* $\Gamma = G_{O(S)}$ *satisfies* $(PG)'$, *then the congruence kernel* $C = C^S(G)$ *is finite.*

Corollary 1. *If, under the hypothesis of Theorem* 1, *the group* $\widehat{\Gamma}$ *has finite width as a profinite group (in particular, if* Γ *has finite width as a discrete group), then* C *is finite.*

Note that the converse of Theorem 1 holds without any additional assumptions about G.

Theorem 2. *Suppose* G *is a simple, simply connected* K*-group and* $S \subset V^K$ *is a finite subset containing* V_∞^K. *Then the group* $G_{A_S(S)}$ *of* S*-integral* S*-adeles is a profinite group of finite width. Consequently, if* $\Gamma = G_{O(S)}$ *has the congruence property, then* $\widehat{\Gamma}$ *has finite width as a profinite group.*

Corollary 2. *Under the hypothesis of Theorem* 1, *each of the conditions* $(BG)_{pf}$, (PG), *and* $(PG)'$ *for* $\widehat{\Gamma}$ *is equivalent to condition* (CSP) *for* Γ.

The proof of Theorem 1 presented in §§3–5 utilizes several auxiliary results, which are given in §2. The proof of Theorem 2 is given in §6. Finally, in §7 we give an example demonstrating the possibility of effectively verifying condition $(PG)'$. Namely, it is shown that in the case of the group $\Gamma = SL_n(\mathbf{Z})$ $(n \geq 3)$ the condition $(PG)'$ for $\widehat{\Gamma}$ can easily be verified by purely algebraic means, starting from the presentation of Γ by generators and relations, while the verification of condition (BG) for Γ requires a complicated arithmetic technique (cf. [15]), and a direct verification of $(BG)_{pf}$ and (PG) for $\widehat{\Gamma}$ is not known.

A brief account of the results of this paper was published earlier in [9].

§2. The congruence property and centrality of the congruence kernel. Criteria for centrality

According to the definition, the congruence kernel $C = C^S(G)$ occurs in an exact sequence

(1) $$1 \to C \to \widehat{G} \xrightarrow{\pi} \overline{G} \to 1,$$

where $\widehat{G}$ and $\overline{G}$ are the completions of the group G_K relative to the S-arithmetic and S-congruence topologies and π is the corresponding continuous projection [25]. Putting aside the trivial case $\operatorname{rank}_S G = 0$, when the group $\Gamma = G_{O(S)}$ is finite and therefore $C = \{1\}$, we can easily show by means of the strong approximation theorem (see [5] and [8]) that $\overline{G}$ can be identified with the group $G_{A(S)}$ of S-adeles. We say that the congruence kernel C is *central* if C lies in the center of $\widehat{G}$. It is well known (see [21] and [25]) that centrality implies finiteness. We will apply this result in a somewhat broader context. Suppose $C_1 \subset C$ is a (closed) characteristic subgroup; then C_1 is a normal subgroup of $\widehat{G}$, and hence we can pass from (1) to the sequence

$$1 \to D = C/C_1 \to H = \widehat{G}/C_1 \xrightarrow{\theta} \overline{G} \to 1. \tag{2}$$

We will say that the subgroup D is *central* if D is contained in the center of H.

Proposition 1. *If the subgroup D is central, then it is finite. Conversely, if D is finite and G_K has the standard description of normal subgroups, then D is central.*

We will outline the proof of the first part of the proposition, which does not differ much from the proof of the corresponding result for the full congruence kernel (the proof of the second part can be obtained from the more general Proposition 2, since if C is finite, then necessarily $S \cap T = \varnothing$—see [23]). Consider an initial segment of the Hochschild-Serre exact spectral sequence corresponding to (2):

$$H^1(\overline{G}) \xrightarrow{\varphi} H^1(H) \to H^1(D)^{\overline{G}} \xrightarrow{\psi} H^2(\overline{G}),$$

where $H^i(*)$ denotes the ith continuous cohomology group with coefficients in the one-dimensional torus $\mathbf{R}/\mathbf{Z}$. If D is central, then $H^1(D)^{\overline{G}}$ coincides with the group D^* dual to D. On the other hand, $\operatorname{Coker}\varphi$ is the group dual to $\overline{[G_K, G_K]}/\widetilde{[G_K, G_K]}$, where the bar denotes the closure in G_K in the S-congruence topology, and the tilde the closure in the topology induced from H; hence the finiteness of $\operatorname{Coker}\varphi$ follows from the results of Margulis [3].

Also, since (2) splits over the group G_K, it follows that $\operatorname{Im}\psi$ lies in the so-called metaplectic kernel $M(G, S) = \operatorname{Ker}(H^2(G_{A(S)}) \to H^2(G_K))$ (here G_K is regarded as endowed with the discrete topology), which is always finite [21]. Therefore D^* is finite, and hence so is D.

Thus the proof of Theorem 1 is reduced to the proof of

Theorem 1′. *Under the hypothesis of Theorem* 1, *property* (PG)′ *for the group $\Gamma = G_{O(S)}$ implies centrality of the congruence kernel C.*

The centrality of C under property (PG) for Γ was also proved a little later by A. Lubotsky, but our condition (PG)′ is much more effectively verifiable than condition (PG) (see §7).

We will describe the criteria for the centrality of D used in this paper. One of the most convenient criteria involves the concept of a group of type (F), which was introduced in [11]. Recall that a profinite group Δ has type (F) if for any finite group E the set $\operatorname{Hom}(\Delta, E)$ of continuous homomorphisms is finite.

Proposition 2 [24]. *Assume the group G_K admits a standard description of normal subgroups and $S \cap T = \varnothing$. If the subgroup D in* (2) *has type* (F), *then it is central.*

We will obtain this result from a number of auxiliary facts, which are also useful in other situations.

Lemma 1. 1) *Suppose $v \in V^K$ and the group G is K_v-isotropic. Then the group G_{K_v} has no proper subgroups of finite index; hence any homomorphism $\mu: G_{K_v} \to E$ into a profinite group E and any action of G_{K_v} on a finite set are trivial.*

2) *Suppose $S \subset V^K$ is a finite subset such that G is K_v-isotropic for all $v \notin S$. Then any continuous homomorphism $\mu: G_{A(S)} \to E$ into a profinite group E is trivial.*

Proof. This follows easily from the validity of the Kneser-Tits conjecture for G over K_v, i.e. the absence of proper noncentral normal subgroups in G_{K_v} (see [5] and [6]).

Let us put $S_1 = S \cup T$ and denote by $Z = Z_H(D)$ the centralizer of D in H.

Proposition 3 [24]. *If, under the hypothesis of Proposition 2, the image $\theta(Z)$ contains all of the groups G_{K_v}, $v \notin S_1$, then D is central.*

Proof. It is easy to see that the image $\theta(Z)$ is closed; hence it follows from the inclusions $\theta(Z) \supset G_{K_v}$ for all $v \notin S_1$ that $\theta(Z) \supset G_{A(S_1)}$, since the groups G_{K_v} $(v \notin S_1)$ together generate a dense subgroup of $G_{A(S_1)}$. We now use

Lemma 2. *Suppose $P \subset H$ is a closed normal subgroup such that $\theta(P) \supset G_{A(S_1)}$. Then, under the hypothesis of Proposition 2, $D \subset P$.*

Proof. It follows from $\theta(P) \supset G_{A(S_1)}$ that $H = \Phi p$, where $\Phi = \varphi^{-1}(G_T)$. It is easy to see that the group Φ is profinite; hence the factor group H/P is also profinite. Assume $D \not\subset P$, i.e., the image D' of D in H/P is nontrivial. Then there exists an open normal subgroup $U' \subset H/P$ that does not contain D'. Its preimage in H, which we will denote by U, is an open normal subgroup of H of finite index that does not contain D. Then the intersection $N = G_K \cap U$ is a noncentral normal subgroup of G_K, and hence the fact that G_K satisfies condition (1) of §1 implies the existence of an open normal subgroup $W \subset G_T$ such that $N = G_K \cap W$. Since $S \cap T = \varnothing$, we can consider the subgroup $U_1 = \theta^{-1}(W \times G_{A(S_1)})$, and then $G_K \cap U_1 = N = G_K \cap U$. Passing to the closure (in H), we obtain $U = U_1$, which is impossible since U_1 contains D. The lemma is proved.

Applying Lemma 2 to $P = Z$, we obtain $D \subset Z$, i.e. D is abelian; hence the whole group $L = \theta^{-1}(G_{A(S_1)})$ centralizes D. Since the subgroups G_T, $G_{A(S_1)}$, and $G_{A(S)}$ are permutable, it follows that for any $x \in \Phi = \theta^{-1}(G_T)$ and $y \in L$ the element $\varphi_x(y) = yxy^{-1}x^{-1}$ lies in D, and for a fixed x the correspondence $y \mapsto \varphi_x(y)$ defines a continuous homomorphism $\varphi_x: L \to D$. We construct the group $D^{(\Phi)} = \prod_{x \in \Phi} D_x$, $D_x = D$, and consider the continuous homomorphism $\varphi: L \to D^{(\Phi)}$, $\varphi(y) = (\varphi_x(y))_{x \in \Phi}$. Then φ induces a continuous homomorphism $\overline{\varphi}: G_{A(S_1)} = L/D \to D^{(\Phi)}/\varphi(D)$. Since the latter group is profinite, it follows from Lemma 1 that the homomorphism $\overline{\varphi}$ must be trivial. This means that $L = BD$, where B is the centralizer of Φ in L. Therefore $\varphi(B) = \varphi(L) = G_{A(S_1)}$, and hence, by Lemma 2, $D \subset B$, i.e., Φ centralizes D. Therefore, finally, $z \supset \Phi L = H$, and Proposition 3 is proved.

Proof of Proposition 2. This follows from Proposition 3 and the well-known fact that if a profinite group D has type (F), then the group $\mathrm{Aut}(D)$ of its continuous automorphisms is also profinite (this can be proved exactly like the profiniteness of the group of automorphisms of a finitely generated profinite group (Theorem 1.3 of [26])). Indeed, consider the homomorphism $\sigma: H \to \mathrm{Aut}(D)$ obtained from the action of H on D via conjugations. Then σ induces a homomorphism

$$\overline{\sigma}: \overline{G} = H/D \to \mathrm{Out}(D) = \mathrm{Aut}(D)/\mathrm{Int}(D).$$

It follows from what was said above that the latter group is profinite; hence, by

Lemma 1, $\overline{\sigma}(G_{A(S_1)}) = \{1\}$, i.e., $\varphi(Z) \supset G_{A(S_1)}$ in the notation of Proposition 3, an application of which completes the proof.

In order to use Proposition 2 we must have a convenient characterization of profinite groups of type (F). Such a characterization is provided by

Proposition 4. *Suppose a profinite group D is not a group of type* (F). *Then there exist a characteristic subgroup $D_0 \subset D$ of finite index and a finite simple group F such that the set* $\mathrm{Epi}(D_0, F)$ *of continuous epimorphisms is infinite. In addition, if D_1 is the intersection of the kernels of all $\varphi \in \mathrm{Epi}(D_0, F)$, then D_1 is a characteristic subgroup of D and $D_0/D_1 \simeq \prod_{i \in I} F_i$, where $F_i = F$ for all i and the index set I is infinite.*

Proof. By hypothesis, there exists a finite group E such that the set $\mathrm{Hom}(D, E)$ of continuous homomorphisms is infinite. Consider the set $\mathscr{C}$ of all pairs (D', E') consisting of a characteristic subgroup $D' \subset D$ of finite index and a finite group E' such that $\mathrm{Hom}(D', E')$ is infinite. By construction, $\mathscr{C} \neq \varnothing$. Suppose a pair $(D_0, E_0) \in \mathscr{C}$ has the property that the order of E_0 is minimal among the orders of the groups E' for all pairs $(D', E') \in \mathscr{C}$. We will show that the group $F = E_0$ is simple. Suppose $N \subset E_0$ is a nontrivial normal subgroup. Then, in view of our constructions, the set $\Phi = \mathrm{Hom}(D_0, E_0/N)$ is finite, which easily implies that $\widetilde{D} = \bigcap_{\varphi \in \Phi} \mathrm{Ker}\, \varphi$ is a characteristic subgroup of D of finite index. It is easy to see that the restriction mapping

$$\mathrm{Hom}(D_0, E_0 \xrightarrow{\rho} \mathrm{Hom}(\widetilde{D}, E_0)$$

has finite fibers; hence its image Im_ρ is infinite. On the other hand, it follows from our constructions that $\mathrm{Im}_\rho \subset \mathrm{Hom}(\widetilde{D}, N)$; hence $|N| < |E_0|$ implies that $\mathrm{Hom}(\widetilde{D}, N)$ must be finite. Therefore the set Im_ρ must certainly be finite. Contradiction.

Thus the group $F = E_0$ is simple and $\mathrm{Hom}(D_0, F)$ is infinite. Since for any proper subgroup $M \subset F$ the set $\mathrm{Hom}(D_0, M)$ is finite by construction, the set of epimorphisms $\Psi = \mathrm{Epi}(D_0, F)$ is infinite. Let $D_1 = \bigcap_{\psi \in \Psi} \mathrm{Ker}\, \psi$. Then D_1 is a characteristic subgroup of D and the set $\mathrm{Epi}(D_0/D_1, F) = \mathrm{Epi}(D_0, F)$ is infinite; in particular, D_0/D_1 is infinite. On the other hand, in view of Lemma 1.3 of [4], $D_0/D_1 \simeq \prod_{i \in I} F_i$, where $F_i = F$ and I is some index set. This completes the proof of Proposition 4.

Remark. It is easy to see that Proposition 4 admits a converse (which we will not need), so that the condition in the statement of the proposition is actually a characterization of profinite groups not of type (F).

§3. Proof of Theorem 1′. Preliminary constructions

To begin the proof of Theorem 1′, assume that under its hypothesis the congruence kernel $C = C^S(G)$ is not central. Then, by Proposition 2, C is not a group of type (F), and so by Proposition 4 there exist characteristic subgroups $C_1 \subset C_0 \subset C$ such that C_0 has finite index in C and $C_0/C_1 \simeq \prod_{i \in I} F_i$, where $F_i = F$ is a finite simple group for all i and the index set I is infinite. It is clear that C_0 and C_1 are normal subgroups of $\widehat{G}$, which enables us to obtain from the congruence sequences (1) of

§2 the exact sequences

$$1 \to D_1 = C/C_1 \to H_1 = \widehat{G}/C_1 \xrightarrow{\theta} \overline{G} \to 1\,, \tag{1}$$

$$1 \to D = C_0/C_1 \to H_1 \xrightarrow{\psi} H_0 = \widehat{G}/C_0 \to 1\,, \tag{2}$$

$$1 \to D_0 = C/C_0 \to H_0 \xrightarrow{\varphi} \overline{G} \to 1\,. \tag{3}$$

We denote by Z the centralizer $Z_{H_1}(D)$, and by Z_1 the centralizer $Z_{H_1}(D_1)$. We claim that for some $v \in V^K \setminus (T \cup S)$ we have

$$\theta(Z) \not\supset G_{K_v}\,. \tag{4}$$

Indeed, assume $\theta(Z) \supset G_{K_v}$ for all $v \in V^K \setminus (T \cup S)$. We will show that we then have $\theta(Z_1) \supset G_{K_v}$ for all $v \in V^k \setminus (T \cup S)$. Then, by Proposition 3, the extension (1) must be central, and so D_1 is finite (see Proposition 1). Contradiction.

Suppose $U \subset D_1$ is any open normal subgroup contained in D. Then, obviously, we can consider the action of Z on $X = D_1/U$ via conjugations and the corresponding homomorphism $\alpha\colon Z \to \operatorname{Aut} X$, which induces a homomorphism $\kappa\ \theta(Z) \to \operatorname{Out} X$. It follows from Lemma 1 that $\kappa(G_{K_v}) = \{e\}$, i.e., for $Z_U = \operatorname{Ker}\alpha$ we have $\theta(Z_U) \supset G_{K_v}$. Now assume there exists an element $g \in G_{K_v} \setminus \theta(Z_1)$. Let $Y = \theta^{-1}(g) \cap Z$ and let $c_1, \ldots, c_n$ be representatives of the distinct cosets in D_1/D. Consider the mapping $\beta\colon Y \to D_1^n$, $y \mapsto ([y, c_1], \ldots, [y, c_n])$, where $[y, c] = ycy^{-1}c^{-1}$. By construction, the image $\beta(Y)$ is a compact subset that does not contain $(e, \ldots, e)$. This implies the existence of an open normal subgroup $U \subset D_1$ contained in D such that $(U \times \cdots \times U) \cap \beta(Y) = \varnothing$. Then clearly $Y \cap Z_U = \varnothing$, and hence $g \notin \theta(Z_U)$. Contradiction. Thus $\theta(Z_1) \supset G_{K_v}$, as required.

We now fix a valuation $v \in V^K \setminus (T \cup S)$ satisfying (4).

Lemma 3. *The groups $B_v = \varphi^{-1}(G_{K_v})$ and $B_v' = \varphi^{-1}(G_{A(S \cup \{v\})})$ commute elementwise.*

Proof. Suppose $g \in G_{K_v}$, $g' \in G_{A(S \cup \{v\})}$ and $b \in \varphi^{-1}(g)$, $b' \in \varphi^{-1}(g')$. Then it is easy to verify that the formula

$$\rho(g, g') = [b, b']$$

gives a well-defined bimultiplicative pairing $\rho\colon G_{K_v} \times G_{A(S \cup \{v\})} \to D_0$. Since the group G_{K_v} is equal to its commutant, ρ must be trivial, which implies the assertion of the lemma.

Next, let $\mu_v\colon \widetilde{G}_{K_v} \to G_{K_v}$ be a universal central topological extension (see §10 of [22]). Then there exists a unique continuous homomorphism $\delta_v\colon \widetilde{G}_{K_v} \to H_0$ such that the diagram

$$\begin{array}{ccc} H_0 & \xrightarrow{\varphi} & \overline{G} \\ {\scriptstyle \delta_v}\uparrow & & \cup \\ \widetilde{G}_{K_v} & \xrightarrow{\mu_v} & G_{K_v} \end{array}$$

is commutative. It turns out that for the group $H_v = \delta_v(\widetilde{G}_{K_v})$ there is an analogue of assertion 1) of Lemma 1.

Lemma 4. *The group H_v has no proper subgroups of finite index; hence any action of H_v on a finite set is trivial.*

Indeed, it suffices to prove the first assertion of the lemma for $\widetilde{G}_{K_v}$. But if $N \subset \widetilde{G}_{K_v}$ is a subgroup of finite index, then, since μ_v is surjective, $\mu_v(N)$ is a subgroup of

finite index in G_{K_v}, and hence $\mu_v(N) = G_{K_v}$ by assertion 1) of Lemma 1. Therefore $\widetilde{G}_{K_v} = N \operatorname{Ker} \mu_v$; hence $[N, N] = [\widetilde{G}_{K_v}, \widetilde{G}_{K_v}]$ in view of the centrality of μ_v, and $N = \widetilde{G}_{K_v}$ inasmuch as $\widetilde{G}_{k_v}$ is equal to its commutant.

It follows from Lemma 4 that H_v is equal to the commutant of the group B_v in Lemma 3.

The rest of the argument will be carried out by the following scheme. We will first use the sequences (2) and (3) to construct certain new exact sequences with special properties, and then show, using condition (PG)′ for $\widehat{\Gamma}$, that in fact there can be no such sequences. In §4 we will examine the case where $F = \mathbf{F}_p$ is a cyclic group of prime order p, and in §5 the case of a simple nonabelian group F. To carry out this plan we will need some properties of profinite groups.

Proposition 5. (i) *If a (discrete) group* Γ *satisfies condition* (BG), *then its profinite completion* $\widehat{\Gamma}$ *satisfies condition* $(\mathrm{BG})_{\mathrm{pf}}$.

(ii) *If a profinite group* Δ *has finite width (resp., satisfies condition* (PG) *or* (PG)′), *then any factor group or any group commensurable*[1] *with it in some larger topological group also has finite width (resp., satisfies condition* (PG) *or* (PG)′).

(iii) *For any profinite group* Δ *we have the implications* $(\mathrm{BG})_{\mathrm{pf}} \Rightarrow (\mathrm{PG}) \Rightarrow (\mathrm{PG})'$.

(iv) *For a pro-p-group* Δ, *each of the conditions* $(\mathrm{BG})_{\mathrm{pf}}$, (PG), *and* (PG)′ *is equivalent to the analyticity of* Δ.

Proof. (i) Suppose $\Gamma = \langle\gamma_1\rangle \cdots \langle\gamma_t\rangle$. Let δ_i denote the image of γ_i in $\widehat{\Gamma}$. Since the closure $\overline{\langle\delta_i\rangle}$ of $\langle\delta_i\rangle$ in $\widehat{\Gamma}$ is compact, the product $\overline{\langle\delta_1\rangle} \cdots \overline{\langle\delta_t\rangle}$ is a closed subset of $\widehat{\Gamma}$ containing the dense subset $\langle\delta_1\rangle \cdots \langle\delta_t\rangle$, the image of Γ in $\widehat{\Gamma}$. Therefore $\widehat{\Gamma} = \overline{\langle\delta_1\rangle} \cdots \overline{\langle\delta_t\rangle}$, as required.

(ii) The assertion pertaining to factor groups is obvious, so we will consider the case of commensurable groups. It suffices to show that the properties $(\mathrm{BG})_{\mathrm{pf}}$, (PG), and (PG)′ for a group Δ and an arbitrary open subgroup $\Sigma \subset \Delta$ are equivalent; clearly we may assume Σ is a normal subgroup of Δ.

Since Δ is the union of a finite number of cosets with respect to Σ, finiteness of the width of Σ obviously implies finiteness of the width of Δ. We will establish the reverse implication. Suppose $\Delta = \overline{\langle\delta_1\rangle} \cdots \overline{\langle\delta_t\rangle}$ for certain $\delta_1, \ldots, \delta_t \in \Delta$. It suffices to show the existence of $\sigma_1, \ldots, \sigma_t \in \Sigma$ such that the product $\overline{\langle\sigma_1\rangle} \cdots \overline{\langle\sigma_t\rangle}$ contains a subset open in Σ. Let $U_i = \overline{\langle\delta_i\rangle}$ and $W_i = U_i \cap \Sigma$, and consider, for each i, a decomposition $U_i = \bigcup_{j=1}^{n_i} z_{ij} W_i$. Then

$$\Delta = \bigcup_{j_1=1}^{n_1} \cdots \bigcup_{j_t=1}^{n_t} (z_{1j_1} W_1) \cdots (z_{tj_t} W_t).$$

It follows from Baire's lemma on categories that there exists a set of indices $(j_1, \ldots, j_t)$, $1 \le j_i \le n_i$, such that the set $W(j_1, \ldots, j_t) = (z_{1j_1} W_1) \cdots (z_{tj_t} W_t)$ contains a subset open in Δ. Then the set

$$W(j_1, \ldots, j_t)(z_{1j_1} \cdots z_{tj_t})^{-1} = (z_{1j_1} W_1 z_{1j_1}^{-1})((z_{1j_1}, z_{2j_2}) W_2 (Z_{1j_1} z_{2j_2})^{-1}) \times \cdots \times ((z_{1j_1} \cdots z_{tj_t}) W_t (z_{1j_1} \cdots z_{tj_t})^{-1})$$

also contains a subset open in Δ. Therefore if $W_i = \overline{\langle\delta_i^{m_i}\rangle}$, then the elements

$$\sigma_i = (z_{1j_1} \cdots z_{ij_i}) \delta_i^{m_i} (z_{1j_1} \cdots z_{ij_i})^{-1}, \qquad i = 1, \ldots, t,$$

are as desired.

(1) Recall that two subgroups of a group are called *commensurable* if their intersection has finite index in each of them.

We now show that (PG) holds for Δ if and only if it holds for Σ. Let $m = [\Delta : \Sigma]$. If Δ satisfies (PG), then, by definition, there exist constants c and k such that

$$|\Delta_n| \leq cn^k \quad \text{for all } n.$$

But $\Delta^m \subset \Sigma$, so for any n we have $\Sigma^n \supset (\Delta^m)^n \supset \Delta^{mn}$, and hence

$$|\Sigma_n| \leq |\Delta_{mn}| \leq (cm^k)n^k,$$

i.e., Σ also satisfies (PG). Conversely, if

$$|\Sigma_n| \leq cn^k \quad \text{for all } n,$$

then, since $\Sigma^n \subset \Delta^n$, we have

$$|\Delta_n| \leq m|\Sigma_n| \leq (cm)n^k,$$

hence Δ satisfies (PG). The argument for (PG)′ is completely analogous.

(iii) The implication (PG) $\Rightarrow$ (PG)′ is obvious, so we will show that (BG) $\Rightarrow$ (PG). If $\Delta = \overline{\langle \delta_1 \rangle} \cdots \overline{\langle \delta_t \rangle}$, then representatives of all cosets in Δ/Δ^n can be found among the elements of the form $\delta_1^{\alpha_1} \cdots \delta_t^{\alpha_t}$, $1 \leq \alpha_i \leq n$, for all $i = 1, \ldots, t$. Hence $|\Delta_n| \leq n^t$.

(iv) In view of (iii), it suffices to show that analyticity of Δ implies $(\mathrm{BG})_{\mathrm{pf}}$, and (PG)′ implies analyticity of Δ. Suppose Δ is an analytic p-adic group of dimension r and $\Delta_1, \ldots, \Delta_r$ are one-parametric subgroups of Δ corresponding to some basis of the Lie algebra Δ. Then the product $\Delta_1 \cdots \Delta_r$ contains a subset open in Δ. Since $\Delta_i \simeq \mathbf{Z}_p$ for any i, this obviously implies property $(\mathrm{BG})_{\mathrm{pf}}$ for Δ. To deduce analyticity from (PG)′ we use the following criterion for analyticity (see [18], p. 590): a finitely generated pro-p-group Δ is analytic if and only if

$$\varlimsup_{m \to \infty} m^{-1} \log_p [\Delta : \Delta^{p^m}] < \infty. \tag{5}$$

But of course if $|\Delta_{p^\alpha}| \leq cp^{k\alpha}$ in accordance with (PG)′, then the limit in (5) does not exceed k. This completes the proof of Proposition 5.

We will also need some facts about the finiteness of continuous cohomology groups that follow from the results of Raghunathan [23].

Proposition 6. *Suppose p is a prime.*

1) *For any $v \in V_f^K$ and any compact open subgroup $U \subset G_{K_v}$ the continuous cohomology group $H^2(U, \mathbf{F}_p)$ with coefficients in the cyclic group $\mathbf{F}_p$ of prime order with the discrete topology is finite.*

2) *For any finite subset $S \subset V^K$ containing V_∞^K and for any compact open subgroup $W \subset G_{A(S)}$ the group $H^2(W, \mathbf{F}_p)$ is finite.*

Proof. In view of the results of Raghunathan [23], the continuous cohomology groups $H^i(U)$ and $H^i(W)$ $(i = 1, 2)$ with coefficients in $\mathbf{R}/\mathbf{Z}$ are finite. To deduce finiteness of the groups in question we consider the exact sequence

$$0 \to \mathbf{F}_P \to \mathbf{R}/\mathbf{Z} \xrightarrow{[p]} \mathbf{R}/\mathbf{Z} \to 0,$$

where $[p]$ denotes multiplication by p, and segments of the corresponding cohomology sequences

$$H^1(U) \to H^2(U, \mathbf{F}_p) \to H^2(U), \tag{6}$$

$$H^1(W) \to H^2(W, \mathbf{F}_p) \to H^2(W). \tag{7}$$

The desired conclusion obviously follows from the exactness of (6) and (7).

§4. The case $F = \mathbf{F}_p$

We will first show how to obtain from the sequence (2) of the previous section an exact sequence of topological groups

$$1 \to E \to P \xrightarrow{\tau} H_v \to 1 \tag{1}$$

with the following properties:

(i) E is the product of an infinite number of copies of $\mathbf{F}_p$.

(ii) For any compact open subgroup $W \subset H_v$ the group $\tau^{-1}(W)$ is a finitely generated profinite group satisfying (PG)′.

Since the group D in (2) of §2 is commutative, the action of H_1 on D via conjugations induces an action of H_0. We see from condition (4) of §2 that the restriction of this action to H_v is nontrivial; hence the induced action of H_v on the group of characters $D^* = \mathrm{Hom}(D, \mathbf{F}_p)$ is also nontrivial.

Suppose $\chi_0 \in D^*$ is not a fixed point for H_v. Let Φ denote the $\mathbf{F}_p$-subspace of D^* generated by all shifts $h\chi_0$, $h \in H_v$; it follows from Lemma 4 that $\dim_{\mathbf{F}_p} \Phi$ is infinite. Since the group D^* is discrete, any compact subgroup of H_0 acts on D^* locally finitely; hence there exists a compact open subgroup $U \subset B_v'$ that does not meet D_0 and acts trivially on χ_0. Then, by Lemma 3, U acts trivially on the whole space Φ. Let D' denote the intersection of the kernels of all characters $\chi \in \Phi$. The group D' is invariant under the action of U and H_v, and U acts on the factor group $E_1 = D/D'$ trivially. Consider the exact sequence

$$1 \to E_1 \to R \xrightarrow{\tau_1} M \to 1,$$

where $M = U \times H_v \subset H_0$ (the product is direct since U does not meet D_0) and $R = \psi^{-1}(M)/D'$. We will obtain a sequence (1) with properties (i) and (ii) by putting

$$E = E_1/(E_1 \cap [\tau_1^{-1}(U), \tau_1^{-1}(U)]), \qquad P = \tau_1^{-1}([U, U] \times H_v)/[\tau_1^{-1}(U), \tau_1^{-1}(U)]$$

and taking as τ the corresponding quotient morphism for the morphism τ_1. Indeed, it follows from our constructions that for any compact open subgroup $W \subset H_v$ the preimage $\tau^{-1}(W)$ is a factor group of the preimage $\pi^{-1}(\varphi([U, U] \times W))$, where π is the projection in the congruence sequence (1) in §2. Therefore condition (PG)′ for $\widehat{\Gamma}$ and Proposition 5 imply condition (PG)′ for $\tau^{-1}(W)$. Thus it remains to show that E is infinite. Consider the exact sequence

$$1 \to E_1 \to \tau_1^{-1}(U) \to U \to 1 \tag{2}$$

and the corresponding spectral continuous cohomology sequence (recall that by construction the extension (2) is central)

$$\cdots \to H^1(\tau_1^{-1}(U), \mathbf{F}_p) \xrightarrow{\alpha} H^1(E_1, \mathbf{F}_p) \to H^2(U, \mathbf{F}_p). \tag{3}$$

In view of our constructions, the group U is isomorphically projected via φ onto a compact open subgroup of $G_{A(S \cup \{v\})}$; hence, by Proposition 6, $H^2(U, \mathbf{F}_p)$ is finite. Then it follows from (3) that $\mathrm{Im}\,\alpha$ has finite index in $H^1(E_1, \mathbf{F}_p) = E_1^*$. But any element $\chi \in \mathrm{Im}\,\alpha$, regarded as a character of E_1, is trivial on $E_1 \cap [\tau_1^{-1}(U), \tau_1^{-1}(U)]$; hence this intersection is finite and so the group $E = E_1/(E_1 \cap [\tau_1^{-1}(U), \tau_1^{-1}(U)])$ is infinite. Thus the existence of a sequence (1) with properties (i) and (ii) has been established. We will now show that in fact there can exist no such sequence.

We denote by q the prime corresponding to v and consider separately the cases $p = q$ and $p \neq q$. In the first case, the preimage $\tau^{-1}(W)$ of any compact open

subgroup $W \subset H_v$ is almost a pro-p-group, and so, by Proposition 5, a Sylow p-subgroup $B \subset \tau^{-1}(W)$ must satisfy (PG)', i.e. be analytic. It follows easily that E is finite. Contradiction.

In the rest of this section we will assume $q \neq p$. We choose an element $s \in G_{K_v}$ such that the closure of the cyclic subgroup it generates is noncompact (an element with this property can be chosen in any nontrivial K_v-decomposable subtorus of G) and, letting β be the restriction of φ to H_v, we fix an element $t \in \beta^{-1}(s)$. Let $L \subset H_v$ be a compact open subgroup such that the set $LtLt^{-1}$ meets $\operatorname{Ker}\beta$ only in the identity element (in particular, $L \cap \operatorname{Ker}\beta = \{e\}$).

We denote by $G_{O_v}(\mathfrak{p}_v^l)$ the congruence subgroup of G_{O_v} of level $\mathfrak{p}_v^l$, where $\mathfrak{p}_v \subset O_v$ is a maximal ideal. It is easy to see that for all sufficiently large l the following assertions hold:

(a) $\beta(L) \supset G_{O_v}(\mathfrak{p}_v^l)$.

(b) $G_{O_v}(\mathfrak{p}_v^l)^{q^\alpha} = G_{O_v}(\mathfrak{p}_v^{l+f\alpha})$ for any $\alpha \geq 0$, where $f = v(q)$.

We fix, for a time, some l satisfying (a) and (b), and we put $\Delta = L \cap \beta^{-1}(G_{O_v}(\mathfrak{p}_v^l))$ and $\Delta(m) = L \cap \beta^{-1}(G_{O_v}(\mathfrak{p}_v^m))$ for $m \geq l$.

Consider the natural action of H_v on E in the sequence (1) induced by the action of P on E via conjugations.

Lemma 5. 1) *The action of Δ on E is completely reducible, i.e. $E = \prod_{j \in J} E_j$, where the E_j are finite irreducible Δ-modules.*

2) *If $\Sigma \subset \Delta$ is a normal open subgroup and $E_j^\Sigma \neq (0)$, then Σ acts trivially on E_j. (Here E_j^Σ is the subgroup of elements fixed under Σ.)*

3) $\dim_{\mathbf{F}_p} E^\Sigma < \infty$, *or, equivalently,* $E_j^\Sigma = 0$ *for almost all* j.

Proof. By construction, Δ is a pro-p-group; hence assertion 1) follows from the condition $q \neq p$ and Maschke's lemma. To prove 2) it suffices to observe that E_j^Σ is a Δ-submodule of E_j; hence $E_j^\Sigma = (0)$ inasmuch as $E_j^\Sigma = E_j$. To prove 3), consider the exact sequence

$$1 \to E \to \tau^{-1}(\Sigma) \to \Sigma \to 1$$

and the corresponding spectral sequence

$$H^1(\tau^{-1}(\Sigma), \mathbf{F}_p) \to H^1(E, \mathbf{F}_p)^\Sigma \to H^2(\Sigma, \mathbf{F}_p). \tag{4}$$

By construction, Σ is projected via β onto a compact open subgroup of G_{K_v}; hence, by Proposition 6, $H^2(\Sigma, \mathbf{F}_p)$ is finite. On the other hand, since $\tau^{-1}(\Sigma)$ is finitely generated, it follows that $H^1(\tau^{-1}(\Sigma), \mathbf{F}_p)$ is finite, and therefore, since (4) is exact, $H^1(E, \mathbf{F}_p)^\Sigma$ is finite. But $H^1(E, \mathbf{F}_p)$ is the character group E^* and $E^* = \bigoplus_{j \in J} E_j^*$; hence $(E^*)^\Sigma = \bigoplus_{j \in J} (E_j^*)^\Sigma$. Since $(E^*)^\Sigma$ is finite, it follows that $(E_j^*)^\Sigma = 0$ for almost all j. For such j the equality $E_j^\Sigma = E_j$ is impossible; hence we see from 2) that $E_j^\Sigma = 0$. Lemma 5 is completely proved.

It follows from Lemma 5 that the group E^{H_v} is finite. Since E is infinite and the groups $\Delta(m)$ form a fundamental system of neighborhoods of the identity element in Δ, by increasing the initially chosen l we can satisfy, along with (a) and (b), the condition

(c) $E^\Delta \neq E^{H_v}$.

So we will assume all three conditions (a)–(c) are satisfied. We put $r = 2\max(|v(s_{ij})|, |v(s'_{ij})|)$, where $s = (s_{ij})$ and $s^{-1} = (s'_{ij})$, and for $d \geq 0$ we denote the subgroup $\Delta(l + dr)$ by W_d.

Proposition 7. *There exist numbers* a, b, *and* e $(a > 0)$ *such that*

$$\dim_{\mathbf{F}_p} E^{W_d} \geq ad^2 + bd + e$$

for all sufficiently large d.

Proof. We will first show that for any $d \geq 0$ we have

$$tW_d t^{-1} \supset W_{d+1}. \tag{5}$$

Indeed, it follows from our constructions that

$$s^{-1} G_{O_v}(\mathfrak{p}_v^{l+(d+1)r}) s \subset G_{O_v}(\mathfrak{p}_v^{l+dr}),$$

and hence $t^{-1}W_{d+1}t \subset \beta^{-1}(\beta(W_d))$. But if $w \in W_{d+1}$ and $\beta(t^{-1}wt) = \beta(\overline{w})$, then $\overline{w}^{-1}t^{-1}wt \in (Lt^{-1}Lt) \cap \operatorname{Ker}\beta$, and hence $\overline{w} = t^{-1}wt \in W_d$ because of the choice of the subgroup L. Thus (5) is proved.

We now turn to the decomposition $E = \prod_{j \in J} E_j$ in Lemma 5 and for $d \geq 0$ we put $J_d = \{j | E_j \subset E^{W_d}\}$, so that the module $F_d = \prod_{j \in J_d} E_j$ is equal to E^{W_d} and, in particular, is finite. We have the chain of inclusions $J_0 \subset J_1 \subset \cdots \subset J_d \subset \cdots$.

We claim that all inclusions in this chain are strict. We will first show that for any d the submodule F_d is not t-invariant. If it were, F_d would be invariant under the subgroup $R \subset H_v$ generated by Δ and t. We now use a result of Prasad [20], according to which G_{K_v} has no proper noncompact open subgroups. It would then follow that $\beta(R) = G_{K_v}$, and therefore, since $\operatorname{Ker}\beta$ is finite, R would have finite index in H_v; hence $R = H_v$ by Lemma 4. Thus the finite module F_d would be invariant under the action of H_v; hence, repeatedly applying Lemma 4, we see that this action would be trivial. But then $E^{\Delta} \subset F_d \subset E^{H_v}$. Contradiction.

Thus $t(F_d) \neq F_d$. This means there exists an index $j \in J \setminus J_d$ such that $t(F_d)$ has a nonzero projection on E_j. Since W_d acts trivially on F_d, it follows that $tW_d t^{-1}$ acts trivially on $t(F_d)$, so we see from (5) that $E_j^{W_{d+1}} \neq 0$ and therefore, in view of assertion 2) of Lemma 5, W_{d+1} acts trivially on E_j, i.e. $j \in J_{d+1} \setminus J_d$, and everything is proved.

For each $k = 1, 2, \ldots$ we choose an index $j_k \in J_k \setminus J_{k-1}$ and construct the spaces

$$E(d) = \prod_{k=1}^{d} E_{j_k}.$$

It is clear that $E(d) \subset E^{W_d}$; hence it suffices to establish the existence of a, b, and e $(a > 0)$ such that

$$\dim_{\mathbf{F}_p} E(d) \geq ad^2 + bd + e.$$

We will need two lemmas.

Lemma 6. *Suppose* Δ *is a pro-q-group and* p *is a prime different from* q. *Then there exists a constant* $\beta > 0$ *such that, for any continuous representation* $\rho: \Delta \to \mathrm{GL}_m(\mathbf{F}_p)$,

$$m \geq \beta \log_q |\rho(\Delta)|.$$

Proof. For an integer $n > 0$ we will denote by $\operatorname{ord}_q n$ the exponent of the power to which q occurs in the factorization of n. Then

$$\log_q |\rho(\Delta)| = \operatorname{ord}_q |\rho(\Delta)| \leq \operatorname{ord}_q |\mathrm{GL}_m(\mathbf{F}_p)|,$$

and everything comes down to obtaining an estimate of the form

$$\operatorname{ord}_q |\mathrm{GL}_m(\mathbf{F}_p)| \leq bm.$$

Recall that the order of $\mathrm{GL}_m(\mathbf{F}_p)$ is given by

$$|\mathrm{GL}_m(\mathbf{F}_p)| = p^{m(m-1)/2} n(m), \quad \text{where } n(m) = (p^m - 1)\dots(p-1).$$

Clearly $\mathrm{ord}_q |\mathrm{GL}_m(\mathbf{F}_p)| = \mathrm{ord}_q n(m)$. To estimate the latter we use the following elementary fact:

(6) *If* $a > 1$ *and* $\mathrm{ord}_q(a-1) > 0$ *if* $q \neq 2$, $\mathrm{ord}_q(a-1) > 1$ *if* $q = 2$, *then for any integer* $k \geq 1$ *we have* $\mathrm{ord}_q(a^k - 1) = \mathrm{ord}_q(a-1) + \mathrm{ord}_q k$.

We first consider the case $q \neq 2$. Let l be the smallest positive integer such that $p^l \equiv 1 \pmod q$ and $\mathrm{ord}_q(p^l - 1) = t$. Obviously $p^i - 1 \not\equiv 0 \pmod q$ if $i \not\equiv 0 \pmod l$. On the other hand, if $i = kl$, then it follows from (6) that $\mathrm{ord}_q(p^i - 1) = t + \mathrm{ord}_q k$. Therefore

$$\mathrm{ord}_q n(m) = \sum_{\substack{k \geq 1 \\ kl \leq m}} (t + \mathrm{ord}_q k) = \left[\frac{m}{t}\right] t + \mathrm{ord}_q\left(\left[\frac{m}{l}\right]!\right)$$

$$\leq mt + \mathrm{ord}_q(m!) \leq \frac{tq}{q-1} m$$

(square brackets denote the integral part), and we can put $b = tq/(q-1)$. Here we have used the fact that

$$\mathrm{ord}_q(m!) = \left[\frac{m}{q}\right] + \left[\frac{m}{q^2}\right] + \dots \leq m\left(\frac{1}{q} + \frac{1}{q^2} + \dots\right) = m\frac{1}{q-1}.$$

The case $q = 2$ differs only slightly from the one just considered. Let $t_1 = \mathrm{ord}_q(p-1)$ and $t_2 = \mathrm{ord}_q(p^2-1)$ (clearly $t_2 \geq 3$). If i is odd, then $\mathrm{ord}_q(p^i-1) = t_1$; if $i = 2k$, then it follows from (6) that $\mathrm{ord}_q(p^i - 1) = t_2 + \mathrm{ord}_q k$. Therefore

$$\mathrm{ord}_q n(m) = \sum_{\substack{k \leq m \\ k-}} t_1 + \sum_{\substack{k \geq 1 \\ 2k \leq m}} (t_2 + \mathrm{ord}_q k) \leq \left(\left[\frac{m}{2}\right] + 1\right) t_1 + \left[\frac{m}{2}\right] t_2 + \mathrm{ord}_q\left(\left[\frac{m}{2}\right]!\right)$$

$$\leq mt_1 + mt_2 + m = (t_1 + t_2 + 1)m,$$

and we can put $b = t_1 + t_2 + 1$. The lemma is proved.

Lemma 7. *For suitable integers* c, c_1 *and* c_2 $(c_2 > 0)$

1) $[\Delta : W_i] = q^{c_1 + ic_2}$ *for all sufficiently large* i *(say* $i \geq i_0$*); and*

2) *for any normal subgroup* $N \subset \Delta$ *containing* W_i *but not* W_{i-1} *we have* $[N : W_i] \leq c$.

Proof. We use the theory of analytic pro-p-groups (see [17] and [18]).

Let $m_k = \dim_{\mathbf{F}_p} E_{j_k}$ and $n_k = |\sigma_{j_k}(\Delta)|$, where σ_{j_k} is a homomorphism of Δ into $\mathrm{Aut}(E_{j_k}) \simeq \mathrm{GL}_{m_k}(\mathbf{F}_p)$, and fix $d \geq 1$. By Lemma 6,

(7) $$\dim_{\mathbf{F}_p} E(d) = m_1 + \dots + m_d \geq \beta(\log_q n_1 + \dots + \log_q n_d).$$

But it follows from Lemma 7 and our constructions that for $k \geq i_0$

$$n_k \geq (1/c) q^{c_1 + kc_2},$$

and hence

$$\log_q n_k \geq c_1 + kc_2 - \varepsilon,$$

where $\varepsilon = \log_q c$. Then we see from (7) that for $d > i_0$

$$\dim_{\mathbf{F}_p} E(d) \geq \beta(\log_q n_1 + \dots + \log_q n_{i_0 - 1} + (c_1 + i_0 c_2 - \varepsilon) + \dots + (c_1 + dc_2 - \varepsilon))$$

$$= \frac{\beta c_2}{2} d^2 + \frac{\beta(2(c_1 - \varepsilon) + c_2)}{2} d$$

$$+ \beta\left(\log_q n_1 + \dots + \log_q n_{i_0 - 1} + \frac{c_2}{2}(i_0 - i_0^2) + (c_1 - \varepsilon)(-i_0 + 1)\right).$$

The proposition is proved.

It is now easy to show that a sequence (1) cannot exist. Let us put $\Phi = \tau^{-1}(\Delta)$ and estimate from below the order of the Burnside factor $\Phi_{pq^\alpha} = \Phi/\Phi^{pq^\alpha}$. We have

$$|\Phi_{pq^\alpha}| \geq |\Phi/\Phi(\alpha)^p| \geq |\Phi(\alpha)/\Phi(\alpha)^p|, \tag{8}$$

where $\Phi(\alpha) = \Phi^{q^\alpha}$; also, $\Phi(\alpha) = \tau^{-1}(\Delta(l + f\alpha))$. We claim that for some subgroup $\Omega \subset \Phi(\alpha)$ we have a direct product decomposition

$$\Phi(\alpha) = E^{\Phi(\alpha)} \times \Omega. \tag{9}$$

Indeed, it follows from Maschke's theorem and the condition $p \neq q$ that E is a semisimple $\Phi(\alpha)$-module; hence for some $\Phi(\alpha)$-submodule $E' \subset E$ we have $E = E^{\Phi(\alpha)} \times E'$. In addition, $E^{\Phi(\alpha)}$ centralizes (any) Sylow pro-q-subgroup $\Psi \subset \Phi(\alpha)$; hence we can take as Ω the semidirect product $\Psi \leftthreetimes E'$. Let $d = [\alpha f/r]$. Then obviously $\Phi(\alpha) \subset \tau^{-1}(W_d)$, and so from (8), (9), and Proposition 7 we obtain

$$|\Phi_{pq^\alpha}| \geq |E^{\Phi(\alpha)}| \geq |E^{W_d}| \geq p^{ad^2+bd+e} \tag{10}$$

for sufficiently large α. On the other hand, by hypothesis, $|\Phi_{pq^\alpha}| \leq cq^{k\alpha}$ for all α and suitable constants c and k. Since $d \geq \alpha f/r - 1$, we obtain a contradiction to (10) by taking α sufficiently large.

§5. The case where F is a nonabelian simple group

The argument for this case is analogous to that of the preceding section and differs from it only in certain technical details. Again we first construct an exact sequence

$$1 \to E \to P \xrightarrow{\tau} H_v \to 1 \tag{1}$$

with the following properties:

(i) E is the product of an infinite number of copies of F.

(ii) For any compact open subgroup $W \subset H_v$ the preimage $\tau^{-1}(W)$ is a finitely generated profinite group satisfying $(PG)'$.

To do this we again turn to sequence (2) in §3. Since the group D has the form $D = \prod_{i \in I} F_i$, where $F_i = F$ for all $i \in I$, and F is a nonabelian simple group, it follows that the group of automorphisms $\operatorname{Aut} D$ is a semidirect product:

$$\operatorname{Aut} D = S_I \leftthreetimes \prod_{i \in I} \operatorname{Aut} F_i,$$

where S_I is the symmetric group of the set I. The action of H_1 on D via conjugations defines a homomorphism $\eta: H_1 \to \operatorname{Aut} D$, which, in turn, induces homomorphisms

$$\overline{\eta}: H_0 = H_1/D \to \operatorname{Out} D = \operatorname{Aut} D/\operatorname{Int} D = S_I \leftthreetimes \prod_{i \in I} \operatorname{Out} F_i,$$

$$\mu: H_0 \to S_I.$$

We will show that in our situation $\mu(H_v) \neq \{e\}$. If this were not so, then $\overline{\eta}(H_v) \subset \prod_{i \in I} \operatorname{Out} F_i$, and then it would follow from Lemma 4 that $\overline{\eta}(H_v) = \{e\}$. Therefore $\eta(\psi^{-1}(H_v)) = \operatorname{Int} D$; hence $\psi^{-1}(H_v) \subset DZ$, where $Z = Z_{H_1}(D)$, and $\psi(Z) \supset H_v$, which would contradict condition (4) of §3.

Consider a point $i_0 \in I$ that is not a fixed point for $\mu(H_v)$, and let I_0 denote the orbit $\mu(H_v)i_0$; it follows from Lemma 4 that I_0 is infinite. For any subset $I' \subset I$ we denote $\prod_{i \in I'} F_i$ by $F_{I'}$. We will show that the image $\psi(Z_{H_1}(F_{I_0}))$ contains some

compact open subgroup $U \subset B_v'$ having trivial intersection with D_0. There exists a compact open subgroup $U_0 \subset B_v'$, not meeting D_0, such that $\mu(U_0)i_0 = i_0$. Then, by Lemma 3, $\mu(U_0)i = i$ for any $i \in I_0$. Therefore $\psi^{-1}(U_0)$ normalizes F_{I_0}, and the image of the natural homomorphism $U_0 \to \mathrm{Out}(F_{I_0})$ lies in $\prod_{i\in I_0} \mathrm{Out}\, F_i$. Since U_0 is finitely generated, there are only a finite number of continuous homomorphisms $U_0 \to \mathrm{Out}\, F$; let U denote the intersection of the kernels of all such homomorphisms. Then U is an open subgroup of U_0 and the above homomorphism $U_0 \to \mathrm{Out}(F_{I_0})$ has trivial restriction to U; hence we obtain the desired inclusion $\psi(Z_{H_1}(F_{I_0})) \supset U$.

Consider the subgroup $U \times H_v \subset H_0$ (the product is direct since U does not meet D_0) and its preimage $M = \psi^{-1}(U \times H_v)$. Obviously M normalizes each of the groups $\psi^{-1}(U)$ and $Z_{H_1}(F_{I_0})$, and therefore normalizes their intersection $B = \psi^{-1}(U) \cap Z_{H_1}(F_{I_0})$. In view of our constructions, $\psi(B) = U$ and $B \cap D = F_{I\setminus I_0}$; hence it follows easily that as the desired sequence (1) we can take

$$1 \to E = D/(D \cap B) \to P = M/B \xrightarrow{\tau} H_v \to 1,$$

where τ is obtained as a quotient of ψ (note that $E = F_{I_0}$).

We will now show that a sequence (1) with properties (i) and (ii) cannot exist. Consider the following morphisms arising from the action of P on E via conjugations:

$$\eta_0 \colon P \to \mathrm{Aut}\, E = S_{I_0} \leftthreetimes \prod_{i\in I_0} \mathrm{Aut}\, F_i, \qquad \bar{\eta}_0 \colon H_v \to \mathrm{Out}\, E = S_{I_0} \leftthreetimes \prod_{i\in I_0} \mathrm{Out}\, F_i,$$

$$\mu_0 \colon H_v \to S_{I_0}.$$

For any subgroup $W \subset H_v$ we denote by I_0^W the set of elements $i \in I_0$ that are fixed under $\mu_0(W)$.

Lemma 8. *For any open subgroup $W \subset H_v$ the set I_0^W is finite.*

Proof. We may assume with no loss of generality that W is compact; then, in view of (ii), the group $V = \tau^{-1}(W)$ is finitely generated. Let $J = I_0^W$. Then the group F_J is normalized by V, and we can consider the homomorphism

$$\eta' \colon V \to \mathrm{Aut}(F_J) = S_J \leftthreetimes \prod_{i\in J} o\, \mathrm{Aut}\, F_i;$$

it follows from our constructions that $\eta'(V) \subset \prod_{i\in J} \mathrm{Aut}\, F_i$. Being finitely generated, V has only a finite number of homomorphisms into $\mathrm{Aut}\, F$; let V_0 denote the intersection of the kernels of all these homomorphisms. Then V_0 is an open subgroup of V of finite index. On the other hand, by construction, $\eta'(V_0) = \{e\}$, i.e., $V_0 \subset Z_V(F_J)$. But since F is a nonabelian simple group, we have $Z_V(F_J) \cap F_J = \{e\}$; hence $F_J \cap V_0 = \{e\}$. Therefore $|F_J| \le [V : V_0] < \infty$, and everything is proved.

As in §4, we choose an element $s \in G_{K_v}$ that topologically generates a noncompact subgroup, an element $t \in \beta^{-1}(s)$, and a compact open subgroup $L \subset H_v$ such that $Lt^{-1}Lt \cap \mathrm{Ker}\, \beta = \{e\}$. Let $\Delta(m) = L \cap \beta^{-1}(G_{O_v}(\mathfrak{p}_v^m))$. Arguing as above and using Lemma 8 instead of Lemma 5, we can easily show that for sufficiently large l conditions (a) and (b) of §4 are satisfied, as well as the condition

(c′) $I_0^{\Delta(l)} \neq I_0^{H_v}$.

We fix an l for which all three conditions (a), (b), and (c′) are satisfied, and put $\Delta = \Delta(l)$. We also keep the notation introduced in §4: $r = 2 \max_{i,j}(|v(s_{ij})|, |v(s'_{ij})|)$, where $s = (s_{ij})$ and $s^{-1} = (s'_{ij})$, and $W_d = \Delta(l + dr)$ $(d \ge 0)$. Then we have the following analogue of Proposition 7.

Proposition 8. *There exist numbers* a, b, *and* e $(a > 0)$ *such that*

$$|I_0^{W_d}| \geq ad^2 + bd + e$$

for all sufficiently large d.

Proof. Let $\{I_j\}_{j\in J}$ be the set of all orbits of the action of the group Δ on I_0, so that $E = \prod_{j\in J} E_j$, where $E_j = \prod_{i\in I_j} F_i$. As in the proof of Proposition 7, we consider the sets $J_d = \{j \in J | I_j \subset I_0^{W_d}\}$, which are connected by the inclusions $J_0 \subset J_1 \subset \cdots \subset J_d \subset \cdots$; we will show that all of these inclusions are strict. By Lemma 8, for any d the set $A_d = \bigcup_{j\in J_d} I_j$ is finite; hence by repeating verbatim the argument in the proof of Proposition 7 we see that A_d is not t-invariant.

Suppose $i \in \mu_0(t)(A_d)\backslash A_d$ and I_k is the orbit of Δ containing i. In the proof of Proposition 7 we showed that $tW_d t^{-1} \supset W_{d+1}$, from which it follows that the index i is fixed under W_{d+1}. Since W_{d+1} is normal in Δ, we see that any element of I_k is fixed under W_{d+1}, i.e. $k \in J_{d+1}\backslash J_d$, as required.

For each $k = 1, 2, \ldots$ we choose an index $j_k \in J_k\backslash J_{k-1}$ and consider the set $R_d = \bigcup_{k=1}^{d} I_{j_k}$. Clearly $R_d \subset I_0^{W_d}$; hence it suffices to establish the existence of a, b, and e $(a > 0)$ such that

$$|R_d| \geq ad^2 + bd + e$$

for all sufficiently large d.

Lemma 9. *Suppose* Δ *is a pro-q-group. There exists a constant* $\gamma > 0$ *such that for any continuous homomorphism* $\rho: \Delta \to S_m$ *into the symmetric group of degree* m *we have*

$$m \geq \gamma \log_q |\rho(\Delta)|.$$

Proof. This follows from the fact that

$$\operatorname{ord}_q |S_m| = \operatorname{ord}_q(m!) = \left[\frac{m}{q}\right] + \left[\frac{m}{q^2}\right] + \cdots \leq \frac{m}{q-1}.$$

We now put $m_k = |I_{j_k}|$ and $n_k = |\mu_{j_k}(\Delta)|$, where $\mu_{j_k}: \Delta \to S_{I_{j_k}}$ is a homomorphism into the symmetric group of the set I_{j_k}, and we fix $d \geq 1$. By Lemma 9,

$$|R_d| = m_1 + \cdots + m_d \geq \gamma(\log_q n_1 + \cdots + \log_q n_d).$$

The proof of Proposition 8 can now be completed exactly like the proof of Proposition 7.

It is now easy to show that there can exist no sequence (7) with properties (i) and (ii). Let $\Phi = \tau^{-1}(\Delta)$; we will obtain a lower bound for the order of the Burnside factor $\Phi_{nq^{\alpha+\delta}}$, where $n = |F|$ and q^δ is the highest power of q dividing the order of the group $\operatorname{Out} F$ of outer automorphisms. As in the commutative case,

$$|\Phi_{nq^{\alpha+\delta}}| \geq |\Phi/\Phi(\alpha+\delta)^n| \geq |\Phi(\alpha+\delta)/\Phi(\alpha+\delta)^n|, \tag{2}$$

where $\Phi(\alpha+\delta) = \Phi^{q^{\alpha+\delta}}$. Let us put $d = [\alpha f/r]$ and show that

$$\Phi(\alpha+\delta) = F_{I_0^{W_d}} \times Z_{\Phi(\alpha+\delta)}(F_{I_0^{W_d}}). \tag{3}$$

In view of our constructions, $\Phi(\alpha+\delta) \supset E$ and $\Phi(\alpha) \subset \tau^{-1}(W_d)$. Therefore each of the groups F_i $(i \in I_0^{W_d})$ is invariant under $\Phi(\alpha)$. In other words, the image of $\Phi(\alpha)$ in $\operatorname{Out} F_{I_0^{W_d}} = S_{I_0^{W_d}} \wr \prod_{i\in I_0^{W_d}} \operatorname{Out} F_i$ lies in the second factor; hence $\Phi(\alpha+\delta) \subset \Phi(\alpha)^{q^\delta}$

has trivial image in $\operatorname{Out} F_{I_0^{w_d}}$. This means that $\Phi(\alpha+\delta) = F_{I_0^{w_d}} \cdot Z_{\Phi(\alpha+\delta)}(F_{I_0^{w_d}})$, which necessarily implies (3) since the center of F is trivial. Then, using (2), (3), and Proposition 8, we obtain

$$|\Phi_{nq^{\alpha+\delta}}| \geq |F_{I_0^{w_d}}| \geq n^{ad^2+bd+\varepsilon} \tag{4}$$

for sufficiently large α. But, by hypothesis, $|\Phi_{nq^{\alpha+\delta}}| \leq cq^{k(\alpha+\delta)}$ for all α and suitable constants c and k. Since $d \geq \alpha f/r - 1$, we obtain a contradiction to (4) by taking α sufficiently large.

The proof of Theorem 1 is complete.

§6. Proof of Theorem 2

We begin with two simple results.

Lemma 10. 1) *Suppose Δ is a profinite group and N is a closed normal subgroup. Assume the groups N and Δ/N have finite width. Then the group Δ also has finite width.*

2) *Suppose $\Delta_1, \ldots, \Delta_r$ are profinite groups of finite width. Then their direct product $\Delta_1 \times \cdots \times \Delta_r$ also has finite width.*

Indeed, suppose $N = \overline{\langle \eta_1 \rangle} \cdots \overline{\langle \eta_s \rangle}$ and $\Delta/N = \overline{\langle \theta_1 \rangle} \cdots \overline{\langle \theta_t \rangle}$, where $\theta_i = \delta_i N$, $\delta_i \in \Delta$. Then it is easy to see that $\Delta = \overline{\langle \delta_1 \rangle} \cdots \overline{\langle \delta_t \rangle \langle \eta_1 \rangle} \cdots \overline{\langle \eta_s \rangle}$. Assertion 2) is obvious.

Suppose p is a prime. We will say that $\delta \in \Delta$ is a *p-element* if the group $\overline{\langle \delta \rangle}$ is isomorphic to a cyclic group of order p^m $(m \geq 0)$ or to $\mathbf{Z}_p$.

Lemma 11. *Suppose Π is a (finite or infinite) set of primes and $\{\Delta(p)\}_{p \in \Pi}$ is a family of profinite groups indexed by the elements of Π. Assume that for each $p \in \Pi$ there exist p-elements $\delta_1(p), \ldots, \delta_t(p) \in \Delta(p)$ such that $\Delta(p) = \overline{\langle \delta_1(p) \rangle} \cdots \overline{\langle \delta_t(p) \rangle}$. Then the group $\Delta = \prod_{p \in \Pi} \Delta(p)$ has finite width at most t.*

Proof. Let $\delta_i = (\delta_i(p))_{p \in \Pi} \in \Delta$, $i = 1, \ldots, t$. It follows from the Chinese remainder theorem that $\overline{\langle \delta_i \rangle} = \prod_{p \in \Pi} \overline{\langle \delta_i(p) \rangle}$. Therefore

$$\overline{\langle \delta_1 \rangle} \cdots \overline{\langle \delta_t \rangle} = \prod_{p \in \Pi} (\overline{\langle \delta_1(p) \rangle} \cdots \overline{\langle \delta_t(p) \rangle}) = \Delta.$$

For each $v \in V_f^K$ the congruence subgroup $G_{O_v}(\mathfrak{p}_v) \subset G_{O_v}$ is an analytic pro-p-group relative to the prime p corresponding to the valuation v; hence it has finite width (see Proposition 5). Then the whole group G_{O_v} also has finite width. Using assertion 2) of Lemma 10, we see that in the proof of Theorem 2 we can replace S by any finite set of valuations. Thus, in view of known results on reduction of algebraic groups and varieties (see [8], Chapter III, §3), we may assume that for $v \notin S$ the following conditions are satisfied:

1) The prime p corresponding to v is odd and the corresponding extension $K_v/\mathbf{Q}_p$ is unramified.

2) The logarithmic and exponential mappings induce mutually inverse bijections between $G_{O_v}(\mathfrak{p}_v)$ and $\mathfrak{p}_v \mathfrak{g}_{O_v}$, where $\mathfrak{g}$ is the Lie algebra of G. (It is assumed that we have fixed a matrix realization $G \subset \mathrm{GL}_n$.)

3) There exists a smooth reduction $G^{(v)}$ that is a simple, connected, simply connected group of the same type as G.

Consider in the group $\Delta = G_{A_S(S)}$ the normal subgroup $N = \prod_{v \notin S} \Delta_v$, where $\Delta_v = G_{O_v}(\mathfrak{p}_v)$. In view of assertion 1) of Lemma 10, it suffices to show the groups

N, Δ/N have finite width. Let $\prod$ denote the set of primes corresponding to the valuations $v \notin S$. Then $N = \prod_{p \in \Pi} N_p$, where $N_p = \prod_{\substack{v \in S \\ v|p}} \Delta_v$. Since over each p there lie at most $[K : Q]$ valuations v, to apply Lemma 11 to the subgroups N_p it suffices to establish the existence of a constant t such that $\Delta_v = \langle \delta_1 \rangle \cdots \langle \delta_t \rangle$ for suitable elements $\delta_1, \ldots, \delta_t \in \Delta_v$ (note that Δ_v is a pro-p-group, so that these elements are necessarily p-elements). We will show that as t we can take $t = [K : Q] \dim G$. Indeed, it follows from our constructions that

$$\Delta_v^p = G_{O_v}(p\mathfrak{p}_v) = G_{O_v}(\mathfrak{p}_v^2);$$

on the other hand,

$$[\Delta_v, \Delta_v] \subset G_{O_v}(\mathfrak{p}_v^2).$$

Thus $\Delta_v^p \supset [\Delta_v, \Delta_v]$, i.e., the group Δ_v is powerful in the terminology of [17]. Moreover, the group Δ_v/Δ_v^p is isomorphic to $\mathfrak{g}_{O_v}/\mathfrak{p}_v \mathfrak{g}_{O_v}$, i.e., is a vector space over $\mathbf{F}_p$ of dimension $d = [K_v : \mathbf{Q}_p] \dim G \leq t$. By Proposition 3.7 of [17], there exists a representation of the form $\Delta_v = \overline{\langle \delta_1 \rangle} \cdots \overline{\langle \delta_d \rangle}$ for suitable $\delta_1, \ldots, \delta_d \in \Delta_v$, as required.

It remains to show that the factor group Δ/N is also a group of finite width. We have

$$\Delta/N \simeq \prod_{v \notin S} G_{k_v}^{(v)},$$

where k_v is the residue field of K_v. Arguing as above, we see that it suffices to establish the existence of an l such that

$$G_{k_v}^{(v)} = \langle \gamma_1 \rangle \cdots \langle \gamma_l \rangle \tag{1}$$

for suitable p-elements $\gamma_1, \ldots, \gamma_t \in G_{k_v}^{(v)}$, where $v|p$. We will use the fact that $G_{k_v}^{(v)}$ is a Chevalley group over k_v of normal or twisted type. It follows from a Bruhat decomposition in such groups (see [13]) that any element in $G_{k_v}^{(v)}$ is a product of a bounded number of unipotent root elements, and an upper bound for this number depends only on the number of roots in the corresponding root system, i.e., does not depend on v. Since any unipotent element is a p-element, we obtain the existence of a decomposition of the form (1). Theorem 2 is proved.

§7. Example: condition (PG)′ for $\mathrm{SL}_m(\mathbf{Z})$, $m \geq 3$

In this section we will show that condition (PG)′ for the profinite completion $\widehat{\Gamma}$ of the group $\Gamma = \mathrm{SL}_m(\mathbf{Z})$ $(m \geq 3)$ can be verified directly rather easily, starting from a presentation of Γ by generators and relations. It is well known that Γ is generated by the elementary matrices $\{e_{ij} | i, j = 1, \ldots, m; i \neq j\}$, which satisfy the commutation relations

$$[e_{ij}^{\alpha}, e_{kl}^{\beta}] = \begin{cases} 1, & \text{if } i \neq l,\ j \neq k, \\ e_{il}^{\alpha\beta}, & \text{if } i \neq l,\ j = k \end{cases} \tag{1}$$

(where $\alpha, \beta \in \mathbf{Z}$ and $[x, y] = xyx^{-1}y^{-1}$). As we have already mentioned, the profinite Burnside factor $\widehat{\Gamma}_n$ is a maximal finite factor group of the discrete Burnside factor Γ_n. It is known (see, for example, [3]), however, that any noncentral normal subgroup of Γ has finite index, so that for any n the group Γ_n is finite and $|\widehat{\Gamma}_n| = |\Gamma_n|$. We denote by H_n the subgroup of Γ generated by $\{e_{ij}^n | i, j = 1, \ldots, m; i \neq j\}$, and by E_n the smallest normal subgroup of Γ containing H_n. It is easy to see that $E_n \subset \Gamma^n$, so it suffices to estimate $|\Gamma/E_n|$. We will need

Lemma 12. *$E_{n^2} \subset H_n$ for any n.*

Proof. (cf. [27]). We denote by $\Gamma^{(ij)}$ the subgroup of Γ generated by e_{ij} and e_{ji}, and by $E_d^{(ij)}$ the normal subgroup of $\Gamma^{(ij)}$ generated by e_{ij}^d and e_{ji}^d (d a positive integer). Using induction on the length of an expression of an element $x \in \Gamma^{(ij)}$ in terms of the generators e_{ij} and e_{ji}, we can easily obtain from (1) the commutator relations

$$[x, e_{kl}^{d\alpha}] = \begin{cases} 1, & \text{if } \{i, j\} \cap \{k, l\} = \varnothing, \\ e_{ki}^{d\beta} e_{kj}^{d\gamma}, & \text{if } l = i, k \neq j, \end{cases} \tag{2}$$

for any integer α and suitable integers β and γ. We will now show that for any d the group E_d is generated by the groups $E_d^{(ij)}$. It suffices to show that the subgroup $E' \subset E_d$ generated by these groups is a normal subgroup of Γ. In view of the commutator identities

$$\begin{aligned} [x_1 x_2, y] &= x_1 [x_2, y] x_1^{-1} [x_1, y], \\ [x, y_1 y_2] &= [x, y_1] y_1 [x, y_2] y_1^{-1} \end{aligned} \tag{3}$$

it suffices to show that $z = [x e_{ij}^d x^{-1}, e_{kl}] \in E'$ for any indices $i \neq j$, $k \neq l$ and any $x \in \Gamma^{(ij)}$. If $(k, l) = (i, j)$ or $(k, l) = (j, i)$, this is obvious. If $\{i, j\} \cap \{k, l\} = \varnothing$, then, by (2), $z = 1$. There remains essentially only one case: $l = i$, $k \neq j$ (the other cases are handled analogously). In view of (2),

$$z = x[e_{ij}^d, x^{-1} e_{kl} x] x^{-1} = x[e_{ij}^d, e_{ki}^{\alpha} e_{kj}^{\beta}] x^{-1} = [x, e_{kj}^{-d\alpha}] e_{kj}^{-d\alpha} = e_{ki}^{d\gamma} e_{kj}^{d\delta} e_{kj}^{-d\alpha} \in E'.$$

It is now easy to prove the lemma. It suffices to show that $E_{n^2}^{(ij)} \subset H_n$ for any indices $i \neq j$, i.e. that $x e_{ij}^{n^2} x^{-1} \in H_n$ for any $x \in \Gamma^{(ij)}$. Choose an index $k \in \{1, \ldots, m\}$ different from i and j. Using (1) and (2), we obtain

$$\begin{aligned} x e_{ij}^{n^2} x^{-1} &= x[e_{ik}^n, e_{kj}^n] x^{-1} = [[x, e_{ik}^n] e_{ik}^n, [x, e_{kj}^n] e_{kj}^n] \\ &= [e_{ik}^{n\alpha} e_{jk}^{n\beta}, e_{ki}^{n\gamma} e_{kj}^{n\delta}] \in H_n. \end{aligned}$$

The lemma is proved.

Let us now fix an integer $n > 0$ and a prime p and estimate $|\Gamma / E_{np^\alpha}|$. Assuming $\alpha \geq 8$, we have

$$|\Gamma / E_{np^\alpha}| = c |E_{np^8} / E_{np^\alpha}|,$$

where $c = |\Gamma / E_{np^8}|$. Consider the profinite group $\Delta = \varprojlim_{\alpha > 8} E_{np^8} / E_{np^\alpha}$.

Lemma 13. *For any $\alpha \geq 8$ the factor group $E_{np^\alpha} / E_{np^{\alpha+2}}$ is an abelian p-group.*

Proof. The group E_{np^α} is generated by the elements of the form $g e_{ij}^{np^\alpha} g^{-1}$ for all $i \neq j$ and all $g \in \Gamma$. Since

$$(g e_{ij}^{np^\alpha} g^{-1})^{p^2} = g e_{ij}^{np^{\alpha+2}} g^{-1} \in E_{np^{\alpha+2}},$$

it suffices to show that $E_{np^\alpha} / E_{np^{\alpha+2}}$ is abelian. In view of (3) and the fact that $E_{np^\alpha} \subset H_{p^4}$ for $\alpha \geq 8$ (by Lemma 12), it suffices to show that $z = [e_{ij}^{np^\alpha}, e_{kl}^{p^4}] \in E_{np^{\alpha+2}}$ for any indices $i \neq j$ and $k \neq l$. Suppose first that $l \neq i$. In view of (1), $z = 1$ if $j \neq k$, and $z = e_{il}^{np^{\alpha+4}} \in E_{np^{\alpha+2}}$ if $j = k$. Now suppose $l = i$. If $j \neq k$, we again have

$$z = [e_{kl}^{p^4}, e_{ij}^{np^\alpha}]^{-1} = e_{kj}^{-np^{\alpha+4}} \in E_{np^{\alpha+2}}.$$

It remains to consider the case when $k = j$ and $l = i$. Choosing an index $t \in \{1, \ldots, m\}$ different from i and j, we have

$$z = [e_{ij}^{np^\alpha}, [e_{jt}^{p^2}, e_{ti}^{p^2}]] = [e_{it}^{np^{\alpha+2}} e_{jt}^{p^2}, e_{tj}^{-np^{\alpha+2}} e_{ti}^{p^2}] e_{ji}^{-p^4}.$$

It is clear that the latter element lies in the same coset of the subgroup $E_{np^{\alpha+2}}$ as the element $[e_{jt}^{p^2}, e_{ti}^{p^2}] e_{ji}^{-p^4} = 1$, i.e., $z \in E_{np^{\alpha+2}}$. The lemma is proved.

It follows from Lemma 13 that any factor E_{np^8}/E_{np^α} is a p-group; hence Δ is a pro-p-group. Moreover, since $E_{np^\alpha}/E_{np^{\alpha+1}}$ is abelian, we have $E_{np^{\alpha+1}} = (E_{np^\alpha})^p$; hence it follows easily by induction that

$$(E_{np^\alpha})^{p^\beta} = E_{np^{\alpha+\beta}}$$

for all $\alpha \geq 8$ and all $\beta \geq 0$. In particular,

$$E_{np^{10}} = (E_{np^8})^{p^2} \supset [E_{np^3}, E_{pn^3}],$$

and hence $\Delta^{p^2} \supset [\Delta, \Delta]$. Using one of Lazard's analyticity criteria [18] (or the results on powerful p-groups [17]), we see that the group Δ is analytic and therefore satisfies each of the conditions $(\mathrm{BG})_{\mathrm{pf}}$, (PG), and $(\mathrm{PG})'$. It follows from what was said above that

$$\Delta/\Delta^{p^\alpha} \simeq E_{np^8}/E_{np^{\alpha+8}},$$

hence $|E_{np^8}/E_{np^\alpha}|$ grows polynomially relative to p^α. But then the same is true of the order $|\Gamma/E_{np^\alpha}|$, as required.

By generalizing this argument we can obtain the following sufficient condition for the validity of the congruence property for the group $\Gamma = G_{O(S)}$.

Theorem 3. *Suppose, under the hypothesis of Theorem* 1, *that the group* $\Gamma = G_{O(S)}$ *has a system* $\{N_n\}_{n \geq 1}$ *of normal subgroups of finite index such that*

1) $N_n^m \supset N_{mn}$ *for all integers* $m, n \geq 1$, *and*

2) *for any integer* $n \geq 1$ *and any prime* p *such that* $(n, p) = 1$ *the factor group* $N_{np^\alpha}/N_{np^{\alpha+2}}$ *is an abelian group of exponent* p^2 *for all sufficiently large* α.

Then Γ *has the congruence property.*

Note that in fact condition 2) can be weakened to the following condition:

2′) *For any integer* $n \geq 1$ *and any odd prime* p *such that* $(n, p) = 1$ *the factor group* $N_{np^\alpha}/N_{np^{\alpha+1}}$ *is an abelian group of exponent* p *and, in addition, for any odd* n *the factor group* $N_{2^\alpha n}/N_{2^{\alpha+2}n}$ *is an abelian group of exponent* 4 *for sufficiently large* α.

We will also indicate a fairly universal method for constructing such a system of normal subgroups $\{N_n\}_{n \geq 1}$. Suppose $\gamma_1, \ldots, \gamma_d$ is any system of elements of Γ that includes an element of infinite order. Let N_n denote the normal subgroup of Γ generated by the elements $\gamma_1^n, \ldots, \gamma_d^n$. If $\mathrm{rank}_S G \geq 2$, then each N_n has finite index in Γ (see [3]). Moreover, condition 1) is necessarily satisfied for such a system, and condition 2) reduces to proving the factor group $N_{np^\alpha}/N_{np^{\alpha+2}}$ is abelian, which, in turn, is equivalent to the inclusions

$$[\gamma_i^{np^\alpha}, g\gamma_j^{np^\alpha} g^{-1}] \in N_{np^{\alpha+2}}$$

for all $i, j = 1, \ldots, d$ and all $g \in \Gamma$ for sufficiently large α.

BIBLIOGRAPHY

1. H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Inst. Hautes Études Sci. Publ. Math., no. 33 (1967), 59–137.
2. E. I. Zel'manov, *Solution of the restricted Burnside problem for groups of odd exponent*, Izv. Akad. Nauk SSSR Ser. Mat. **54** (1990), 42–59; English transl. in Math. USSR Izv. **36** (1991).
3. G. A. Margulis, *Finiteness of factor groups of discrete groups*, Funktsional. Anal. i Prilozhen. **13** (1979), no. 3, 28–39; English transl. in Functional Anal. Appl. **13** (1979).
4. O. V. Mel'nikov, *Normal subgroups of free profinite groups*, Izv. Akad. Nauk SSSR Ser. Mat. **42** (1978), 3–25; English transl. in Math. USSR Izv. **12** (1978).
5. V. P. Platonov, *The strong approximation problem and the Kneser-Tits conjecture for algebraic groups*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 1211–1219; English transl. in Math. USSR Izv. **3** (1969).
6. ——, *Arithmetical and structural problems in linear algebraic groups*, Proc. Internat. Congr. Math. (Vancouver, 1974), vol. 1, Canad. Math. Congr., Montréal, 1975, pp. 471–476; English transl. in Amer. Math. Soc. Transl. (2) **109** (1977).
7. ——, *Arithmetic theory of algebraic groups*, Uspekhi Mat. Nauk **37** (1982), no. 3 (225), 3–54; English transl. in Russian Math. Surveys **37** (1982).
8. V. P. Platonov and A. S. Rapinchuk, *Algebraic groups and number theory*, "Nauka", Moscow, 1991. (Russian)
9. ——, *Abstract characterizations of arithmetic groups with the congruence property*, Dokl. Akad. Nauk SSSR **319** (1991), 1322–1327; English transl. in Soviet Math. Dokl. **44** (1992).
10. A. S. Rapinchuk, *The congruence problem for arithmetic groups of finite width*, Dokl. Akad. Nauk SSSR **314** (1990), 1327–1331; English transl. in Soviet Math. Dokl. **42** (1991).
11. Jean-Pierre Serre, *Cohomologie galoisienne*, 2nd ed., Lecture Notes in Math., vol. 5, Springer-Verlag, Berlin, 1964.
12. ——, *Le problème des groupes de congruence pour* SL_2, Ann. of Math. (2) **92** (1970), 489–527.
13. Robert Steinberg, *Lectures on Chevalley groups*, Yale Univ., New Haven, CT, 1967.
14. O. I. Tavgen', *Bounded generation of Chevalley groups over rings of algebraic S-integers*, Izv. Akad. Nauk SSSR Ser. Mat. **54** (1990), 97–122; English transl. in Math. USSR Izv. **36** (1991).
15. D. Carter and G. Keller, *Bounded elementary generation of* $SL_n(O)$, Amer. J. Math. **105** (1983), 673–687.
16. V. Deodhar, *On central extensions of rational points of algebraic groups*, Amer. J. Math. **100** (1978), 303–386.
17. J. D. Dixon et al., *Analytic pro-p-groups*, Cambridge Univ. Press, Cambridge, 1991.
18. M. Lazard, *Groupes analytiques p-adiques*, Inst. Hautes Études Sci. Publ. Math., no. 26 (1965), 389–603.
19. Hideya Matsumoto, *Sur les sous-groupes arithmétiques des groupes semi-simples déployées*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 1–62.
20. Gopal Prasad, *Elementary proof of a theorem of Bruhat-Tits-Rousseau and of a theorem of Tits*, Bull. Soc. Math. France **110** (1982), 197–202.
21. G. Prasad and M. S. Raghunathan, *On the congruence subgroup problem: Determination of the metaplectic kernel*, Invent. Math. **71** (1983), 21–42.
22. ——, *Topological central extensions of semi-simple groups over local fields*, Ann. of Math. (2) **119** (1984), 143–268.
23. M. S. Raghunathan, *On the congruence subgroup problem*, Inst. Hautes Études Sci. Publ. Math., no. 46 (1976), 107–161.
24. A. S. Rapinchuk, *Combinatorial theory of arithmetic groups*, preprint no. 20 (420), Inst. Math. Acad. Sci. BSSR, Minsk, 1990. (English)
25. ——, *The congruence subgroup problem for algebraic groups*, Topics in Algebra, Part 2 (Warsaw, 1988), Banach Center Publ., vol. 26, PWN, Warsaw, 1990, pp. 399–410.(English)

26. J. H. Smith, *On products of profinite groups*, Illinois J. Math. **13** (1969), 680–688.
27. Jacques Tits, *Systèmes générateurs de groupes de congruence*, C. R. Acad. Sci. Paris Sér. A **283** (1976), 693–695.

Received 13/DEC/91

Translated by G. A. KANDALL