CONGRUENCE PROPERTIES OF ZARISKI-DENSE SUBGROUPS I

C. R. MATTHEWS, L. N. VASERSTEIN, *and* B. WEISFEILER

[Received 9 May 1983]

0. *Introduction*

This paper deals with the following general situation: we are given an algebraic group G defined over a number field K, and a subgroup Γ of the group $G(K)$ of K-rational points of G. Then what should it mean for Γ to be a 'large' subgroup? We might require Γ to be a lattice in G, to be arithmetic, to contain many elements of a specific kind, to have a large closure in some natural topology, et cetera. There are many theorems proving implications between conditions of 'size' of this kind.

We shall consider the case of G a K-simple group, usually Q-simple. The Zariski topology of G, for which the closed sets are those defined by the vanishing of polynomial functions, is very coarse. On the other hand, the various valuations v of K each give rise to a 'strong' topology on $G(K)$; if v is non-archimedean, and K_v is the completion of K with respect to v, then $G(K_v)$ is a non-archimedean Lie group, and if $\mathfrak{O}_v$ is the ring of integers of K_v, the open subgroup $G(\mathfrak{O}_v)$ of $G(K_v)$ of integral points is defined for all but finitely many v. The Zariski closure $\bar{\Gamma}$ of a subgroup Γ of $G(K)$ is a K-algebraic subgroup of G, while the strong closure $\bar{\Gamma}_v$ is a Lie subgroup of $G(K_v)$. For elementary reasons the dimension of $\bar{\Gamma}_v$ is at most the dimension of $\bar{\Gamma}$. Our results are in the opposite direction: we show, under suitable conditions on G, that if $\bar{\Gamma} = G$ then for almost all v we have that $\bar{\Gamma}_v$ contains $G(\mathfrak{O}_v)$. To illustrate this with a specific example, if $M_1, \ldots, M_k$ are matrices in $\mathrm{SL}_2(\mathbf{Q})$ generating a group Γ which is Zariski-dense in SL_2, then for all sufficiently large prime numbers p we have $\bar{\Gamma}_p = \mathrm{SL}_2(\mathbf{Z}_p)$. Further, this result is effective, in the sense that we could, in principle, check the hypothesis for given $M_1, \ldots, M_k$, and derive a bound on p beyond which the conclusion holds. (It is perhaps worth remarking that this special case, which is the simplest application of our results, may be proved with much less effort than the general theorem.)

If we exclude a finite set S of valuations v, the restricted product of the remaining non-archimedean topologies provides the S-adelic or S-congruence topology on $G(K)$. From the local results it follows that for some such S-congruence topology the completion of Γ is open in the completion of $G(K)$. This is an approximation theorem, of the same family as the classical results on strong approximation (see, for example, Kneser [7]), applying to a rather general class of subgroup of $G(K)$; there are however many questions on the structure of the possible approximation sets S which we leave open here.

Our method of proof is by reduction to groups defined over finite fields. We can then apply the powerful tools provided by the theory of finite groups, in particular the recently completed classification of finite simple groups. Our exact needs in terms of the classification and standard properties of finite simple groups are set out in § 2; it seems likely that much of our proof would be subsumed if the general theory of maximal subgroups in groups of Lie type were more advanced, since what is essential

Proc. London Math. Soc. (3), 48 (1984), 514–532.

for us is to show that, generically, there are no subgroups which are both large and unexpected. It should be mentioned that our technique is certainly not limited to the case of groups defined over number fields, and would yield results over finitely generated fields (with certain restrictions on the characteristic).

After reduction, and considering for clarity the case where $K = \mathbf{Q}$, the problem becomes to show that $\Gamma_p = G_p(\mathbf{F}_p)$, where Γ_p is the reduction of Γ and G_p the reduction of G, for all sufficiently large primes p. An analogous situation arises in the classical problem of E. Artin on primitive roots: taking GL_1 for G and the subgroup of $\mathrm{GL}_1(\mathbf{Q})$ generated by a non-zero integer a for Γ, we are led to consider the set $S(a)$ of prime numbers such that a modulo p generates $\mathbf{F}_p^\times$. There is an explicitly defined constant $C(a)$, with $C(a) = 0$ if a is a square and otherwise $C(a)$ strictly between 0 and 1, such that the density of $S(a)$ is conjectured to exist and to take the value $C(a)$; this was proved by Hooley [5] on the assumption of sufficiently many conjectures of Riemann-Hypothesis type.

It seems probable that for any algebraic group G defined over $\mathbf{Q}$ and any finitely generated subgroup Γ of $G(\mathbf{Q})$, the set $S(\Gamma)$ of primes p such that $\Gamma_p = G_p(\mathbf{F}_p)$ should have a density $C(\Gamma)$. Supposing that $G = \tilde{\Gamma}$ is simply-connected and absolutely almost simple, we have this result with $C(\Gamma) = 1$, as the exceptional set of p is finite by our main result. If however the radical of G contains a non-trivial torus, a contribution to $C(\Gamma)$ of the type in the classical Artin problem should arise; and generally if G is not simply-connected, $C(\Gamma)$ will reflect constraints arising from Galois cohomology. One should note that in the case when G is an abelian variety such problems have been considered by Lang and Trotter [8], Serre, and Ram Murty.

Our method may be extended to all simple and many semisimple groups, but not, apparently, to all products of simple groups. It seems not entirely straightforward to find the correct conjectural generalization of our theorem to all semisimple groups, nor to give more than partial extensions of the result.

One area of application of our results is to the idea of A. Lubotzky of congruence closed subgroups of algebraic groups. Discussion of this and of other questions left open above is postponed to later papers.

We close by formulating the main result of §§ 1–6:

THEOREM. *Let G be a connected simply-connected absolutely almost simple algebraic group defined over $\mathbf{Q}$, and Γ a finitely generated subgroup of $G(\mathbf{Q})$ which is Zariski-dense in G. Then for all sufficiently large prime numbers p the reduction Γ_p of Γ is equal to $G_p(\mathbf{F}_p)$.*

1. *Notation*

1.0. Throughout this paper G denotes a linear algebraic group, which is connected and of adjoint type; we assume that G is absolutely simple and defined over the field $\mathbf{Q}$ of rational numbers. We write $\tilde{G}$ for the algebraic simply connected covering group of G.

We denote by $\mathfrak{g}$ the Lie algebra of G and by d the dimension $\dim G$. We write Ad for the adjoint representation of G on $\mathfrak{g}$, and ad for the corresponding representation of $\mathfrak{g}$ on itself. We usually identify G with its image in $\mathrm{GL}(\mathfrak{g})$ under the adjoint representation; the identification of $\mathfrak{g}$ with $\mathrm{ad}(\mathfrak{g})$ is used in §§ 4 and 6. Note that Ad is an absolutely irreducible representation when G is absolutely simple.

1.1. If H is an algebraic group defined over a field L, and K is an extension field of L, we write $H(K)$ for the group of K-rational points of H. We shall use this convention in particular for vector spaces, which we regard as having the underlying structure of an algebraic group.

We fix an algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$; when we choose an algebraic closure $\bar{\mathbf{F}}_p$ of the field $\mathbf{F}_p$ with p elements, we assume this to be obtained in the usual way by reduction from $\bar{\mathbf{Q}}$. We write $\bar{\mathfrak{g}}$ for $\mathfrak{g}(\bar{\mathbf{Q}})$.

1.2. We choose a $\mathbf{Z}$-lattice Λ in $\mathfrak{g}$. If $\mathbf{Q}_p$ is the field of p-adic numbers and $\mathbf{Z}_p$ is the ring of p-adic integers, we identify $\Lambda_p = \Lambda \otimes \mathbf{Z}_p$ with a $\mathbf{Z}_p$-submodule of $\mathfrak{g}(\mathbf{Q}_p)$. We define $G(\mathbf{Z})$ to be the subgroup of $G(\mathbf{Q})$ of elements γ with $\gamma.\Lambda = \Lambda$; similarly we define $G(\mathbf{Z}_p)$ to be the subgroup of $G(\mathbf{Q}_p)$ of elements γ with $\gamma.\Lambda_p = \Lambda_p$. A different choice of Λ changes these groups only for a finite number of primes p.

We may define $\tilde{G}(\mathbf{Z})$ and $\tilde{G}(\mathbf{Z}_p)$ in the same way using any faithful representation.

1.3. The group G arises as the generic fibre $\mathbf{G} \otimes \mathbf{Q}$ of a group scheme $\mathbf{G}$ defined over $\mathbf{Z}[N^{-1}]$ for some integer N. For any prime number p such that p does not divide N, $\mathbf{G} \otimes \mathbf{F}_p$ is an algebraic group defined over $\mathbf{F}_p$ which we denote by G_p. For such primes p we say that the reduction of G modulo p is defined, and we may identify $G_p(F)$ with $\mathbf{G}(F)$ for any field F containing $\mathbf{F}_p$.

We write $\mathfrak{g}_p$ for the Lie algebra of G_p and $\bar{\mathfrak{g}}_p$ for $\mathfrak{g}_p(\bar{\mathbf{F}}_p)$.

1.4. If S is a set of prime numbers, we say that S contains almost all primes if there are only finitely many primes p not in S.

The set $S(G)$ of primes defined by the following conditions on p contains almost all primes:

(i) we have $p > 2d+1$;

(ii) the reduction G_p is defined, and is an absolutely simple group of the same type as G;

(iii) the reduction Ad_p, which is the adjoint representation of G_p, is absolutely irreducible, and $\mathrm{ad}_p(\mathfrak{g}_p)$ is isomorphic with $\mathfrak{g}_p$.

(For the last part of (iii), equivalent to the semisimplicity of $\mathfrak{g}_p$, consider the Killing form. The rest follows from 3.6.)

1.5. Let Γ be a subgroup of $G(\mathbf{Q})$. We define $S(\Gamma)$ to be set of primes p such that

(i) p is in $S(G)$,

(ii) the group Γ is contained in $G(\mathbf{Z}_p)$,

(iii) the group Γ_p defined by reduction of Γ modulo p acts irreducibly on $\bar{\mathfrak{g}}_p$.

Here of course Condition (iii) makes sense because of (ii).

REMARKS. (a) If Γ is finitely generated then Γ satisfies (ii) for almost all p, since the exceptions must be among the primes dividing the denominators of some entry in matrices representing a finite set of generators, with respect to a basis of Λ.

(b) If Γ is Zariski-dense in G, it follows from 3.6 that Γ satisfies (iii) for almost all p satisfying (i) and (ii).

(c) Combining (a) and (b) we see that for Γ finitely generated and Zariski-dense in G, the set $S(\Gamma)$ contains almost all primes p.

Given a subgroup $\tilde{\Gamma}$ of $\tilde{G}(\mathbf{Q})$ we define $S(\tilde{\Gamma})$ to be the set $S(\Gamma)$ for Γ the image in $G(\mathbf{Q})$ of $\tilde{\Gamma}$.

1.6. We denote the cardinality of a finite set X by $|X|$. The multiplicative group of a field F is written $F^\times$.

If X and Y are groups, we write $X \leqslant Y$ to mean X is a subgroup of Y, $X \lhd Y$ to mean that X is a normal subgroup, and X char Y to mean that X is a characteristic subgroup. We write $\mathrm{Aut}(X)$ for the group of automorphisms of X, and $\mathrm{Inn}(X)$ and $\mathrm{Out}(X)$ for its subgroup of inner automorphisms and quotient group of outer automorphisms, respectively.

2. *Lemmas on finite simple groups*

2.0. In this section we fix a positive integer d. In the rest of the paper d will take the value $\dim G$ of 1.0.

2.1. Let X be a finite group and let d be as in 2.0. We say that X is *large* relative to d if there are a prime number p and an abelian p-subgroup A of X such that

$$|N_X(A)/Z_X(A)| > d!.$$

Here the notations N_X and Z_X mean respectively normalizer and centralizer in X; therefore the quotient $N_X(A)/Z_X(A)$ is naturally identified with the group of automorphisms of A induced by conjugation by elements of X. From this interpretation it follows at once that if X is large and $X \leqslant Y$ then Y is large.

If X is large and satisfies the defining condition for a unique prime p we write $p = p(X)$. If X is not large we say that X is *small*.

2.2. The object of § 2 is to establish the

PROPOSITION. *For fixed d there are only finitely many isomorphism classes of non-abelian finite simple groups which are small relative to d.*

This is a consequence of the classification of finite simple groups (see, for example, Gorenstein [**4**]). It is conceivable, but perhaps not likely, that it could be proved without using the full force of the classification. To be precise about our needs, we require the assertion that when the isomorphism classes of finite simple non-abelian groups are divided as (A) alternating groups, (B) groups of Lie type, (C) others, called sporadic, then (C) contains only finitely many isomorphism classes. Thus we require no more knowledge on sporadic groups than a bound for the order.

2.3. The proof of the Proposition occupies the rest of the section. We assume the classification and need say no more about Class (C).

2.4. Case (A): let X be the alternating group on $\{1,2,\ldots,n\}$ and define r to be the integer part of $\frac{1}{2}n$. Consider the 2-subgroup A of X defined as follows: A consists of the even permutations generated by the transpositions $(1,2),(3,4),\ldots,(2r-1,2r)$. Then A is abelian, of order 2^{r-1}; and A is normalized by the group B of even permutations preserving the set of pairs $\{1,2\},\{3,4\},\ldots,\{2r-1,2r\}$. We have $|N_B(A)/Z_B(A)| = r!$. Therefore if n is greater than $2d$, the group X is large relative to d.

2.5. For Case (B) we divide into two lists of types:

I: A_n, ${}^2A_n$, B_n, C_n, D_n, ${}^2D_n$ for $n \leqslant 8$ and ${}^2B_2$, ${}^3D_4$, E_6, ${}^2E_6$, E_7, E_8, F_4, ${}^2F_4$, G_2, ${}^2G_2$.

II: A_n, ${}^2A_n$, B_n, C_n, D_n, ${}^2D_n$ for $n \geqslant 9$.

The finite simple group $Y(k)$ associated with a type in these lists and a finite field k is a quotient by the centre of the group of points $\tilde{Y}(k)$ of a simply-connected group $\tilde{Y}$ of the type (this description needs modification for types ${}^2B_2$, ${}^2F_4$, ${}^2G_2$—see [2]).

2.6. Case (B)I: we show that if X is a finite simple group associated to a type in list I, and if X is small relative to d, then

$$|k| < 2.d! + 1.$$

Since the list contains only finitely many types, this bounds the order of X.

For this, define p to be the characteristic of k, and take for A a root subgroup X_r of X isomorphic with the additive group of k. If X is a Chevalley group then (see Carter [2, Chapter 6]) the subgroup of X generated by X_r and X_{-r} is isomorphic with $\mathrm{SL}_2(k)$ or $\mathrm{PSL}_2(k)$; and if X_r is represented by matrices

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

the automorphisms

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & c^2 a \\ 0 & 1 \end{pmatrix}$$

for c in $k^\times$ are induced by conjugation from $\langle X_r, X_{-r} \rangle$. This gives rise to a group of automorphisms of A of order at least $\frac{1}{2}|k^\times|$; the required bound follows. For twisted groups there is a similar argument using the known structure [2, Chapter 13] of groups generated by root subgroups.

2.7. Case (B)II: the essential case here is X of type A_n, that is $X = \mathrm{PSL}_{n+1}(k)$. Let A be the subgroup of X represented by matrices written in $(n, 1) \times (n, 1)$ blocks as

$$\begin{pmatrix} I_n & v \\ 0 & 1 \end{pmatrix}.$$

Then A is isomorphic with the additive group of k^n, and so is an abelian p-group where p is the characteristic of k. Let X' be the subgroup of X represented by matrices

$$\begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}$$

for the same partition, with M in $\mathrm{SL}_n(k)$. We have

$$\begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} I_n & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} M^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} I_n & Mv \\ 0 & 1 \end{pmatrix},$$

so that

$$|N_{X'}(A)/Z_{X'}(A)| = |\mathrm{SL}_n(k)|.$$

For the other cases we may use the existence of a subgroup of type A_r. It is known that there is a subgroup of this type for

$$r = n-1 \quad \text{in types } B_n, C_n, D_n,$$

$$r = \tfrac{1}{2}(n-1) \quad \text{in type } {}^2A_n,$$

$$r = n-2 \quad \text{in type } {}^2D_n;$$

this follows, for example, from the theory of relative Dynkin diagrams. Then from the formula

$$q^{\frac{1}{2}m(m-1)}(q^m-1)\dots(q^2-1)$$

for the order of $\mathrm{SL}_m(k)$ where q is the order of k, we have in all cases a lower bound

$$|N_X(A)/Z_X(A)| > c_1 q^{c_2 n}$$

for absolute constants c_1 and c_2. It follows that the small X are finite in number.

With this the proof is complete.

3. *Elementary lemmas on normal subgroups and representation theory*

3.0. Let H be a group and let N be a normal subgroup of H. Suppose that π is a representation of H on a finite-dimensional vector space V over a field K; we write $\pi|N$ for the restriction of π to N. We need to summarize the relation between the decomposition of π as a direct sum of irreducible representations, and the corresponding decomposition for $\pi|N$, when such decompositions exist.

For an irreducible representation ρ of H, we define the isotypic component V_ρ of V as the sum of all subspaces of V on which H acts by a representation equivalent to ρ.

3.1. We first note that H acts on N by automorphisms, defining $h.n$ as hnh^{-1} for h in H and n in N. Let $\Sigma(N)$ denote the set of equivalence classes of irreducible K-representations of N. Then H acts on $\Sigma(N)$ by

$$(h.\sigma)(n) = \sigma(h^{-1}.n).$$

If ρ is a representation of N on V, we write $T(\rho)$ for the set of σ in $\Sigma(N)$ such that V_σ is non-zero.

3.2. Now suppose that π is irreducible. Then Clifford's theorem (see, for example, [3, p. 70]) states that $\pi|N$ is completely reducible, and that $T(\pi|N)$ consists of a single H-orbit; further

$$V = \bigoplus V_\sigma,$$

where the sum is over σ in $T(\pi|N)$, and H permutes the V_σ transitively.

3.3. Conversely, suppose that N acts completely reducibly on V, so that

$$V = \bigoplus V_\sigma$$

taken over σ in $T(\pi|N)$. Then for h in H, n in N, and v in V we have

$$\pi(n)(\pi(h)v) = \pi(h)(\pi(h^{-1}.n)v),$$

so that $\pi(h)$ maps V_σ to $V_{h.\sigma}$. Therefore H acts as a group of permutations of the set $T(\pi|N)$, and the kernel of this permutation representation is $\pi^{-1}(\prod \mathrm{GL}(V_\sigma))$.

3.4. From 3.3 we have

PROPOSITION. *Let p and q be distinct prime numbers and write L for $\mathrm{GL}_d(\bar{\mathbf{F}}_p)$. Then if A is an abelian q-subgroup of A, we have*

$$|N_L(A)/Z_L(A)| \leqslant d!.$$

Proof. Since $p \neq q$ the representation of A on $\bar{\mathbf{F}}_p^d$ is completely reducible. Therefore as in 3.3 we have

$$\bar{\mathbf{F}}_p^d = \bigoplus V_\chi$$

taken over a set T of one-dimensional characters χ of A. On the other hand, taking H to be $N_L(A)$, we see that the permutation action of H is on T, which is a set with at most d elements. The kernel of this action is $\prod \mathrm{GL}(V_\chi)$, which is equal to $Z_L(A)$. This provides the required estimate.

In the language of 2.1 this gives

COROLLARY. *If X is a subgroup of $\mathrm{GL}_d(\bar{\mathbf{F}}_p)$ which is large with respect to d then $p = p(X)$.*

3.5. In the notation of 1.5 suppose that the subgroup Γ of $G(\mathbf{Q})$ is Zariski-dense in G, and that π is an absolutely irreducible algebraic representation of G on a $\mathbf{Q}$-vector space V.

PROPOSITION. *The restriction $\pi \mid \Gamma$ is absolutely irreducible.*

Proof. If the Proposition is not true, we may choose a basis of $V(\bar{\mathbf{Q}})$ in such a way that $\pi(\Gamma)$ is represented by block matrices

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

for some partitioning, while $\pi(G(\bar{\mathbf{Q}}))$ is not. This contradicts the Zariski-density of Γ.

3.6. In the situation of 3.5, we may define for almost all primes p a reduced representation π_p of G_p on the reduced vector space V_p over $\mathbf{F}_p$. For primes p such that Γ is contained in $G(\mathbf{Z}_p)$ and π_p is defined, we may consider the restriction $\pi_p \mid \Gamma_p$.

PROPOSITION. *There are only finitely many prime numbers p such that π_p and Γ_p are defined and $\pi_p \mid \Gamma_p$ is not absolutely irreducible.*

Proof. From 3.5 we know that the elements $\pi(\gamma)$ for γ in Γ span $\mathrm{End}_{\mathbf{Q}}(V)$ over $\bar{\mathbf{Q}}$. Choosing a basis for V, we have the standard basis for $\mathrm{End}_{\mathbf{Q}}(V) = M_d(\bar{\mathbf{Q}})$ consisting of the elementary matrices E_{ij} for $1 \leqslant i, j \leqslant d = \dim V$. Here E_{ij} has entry 1 in the (i, j) place, and 0 elsewhere. By hypothesis, we may write

$$E_{ij} = \sum \alpha_{ijk} \pi(\gamma_{ijk})$$

for some finite set of α_{ijk} in Γ and γ_{ijk} in $\bar{\mathbf{Q}}$. If the prime number p is such that all the α_{ijk} and $\pi(\gamma_{ijk})$ are p-integral, we may reduce modulo p (more accurately, modulo a prime divisor of p in a suitable number field) to find a relation

$$\bar{E}_{ij} = \sum \bar{\alpha}_{ijk} \pi_p(\bar{\gamma}_{ijk})$$

with $\bar{\alpha}_{ijk}$ in $\bar{\mathbf{F}}_p$. For such a prime p, therefore, the $\pi_p(\bar{\gamma})$ span $\mathrm{End}_{\bar{\mathbf{F}}_p}(V_p)$, and so $\pi_p \mid \Gamma_p$ is absolutely irreducible.

3.7. A characteristic subgroup M of a group H is defined by the property that $\varphi(M) = M$ for all φ in $\mathrm{Aut}(H)$. Then M is normal in H; further if M char M' and

M' char H, we have M char H. We call H characteristically simple if M char H implies that $M = H$ or M is trivial, and H is not trivial.

Recall that a minimal normal subgroup N of H is defined by the properties N non-trivial, $N \lhd H$ but if $N' \lhd H$ and $N' \leqslant N$ then N' is trivial or equal to N. Minimal characteristic subgroups are defined in a similar way. Evidently if H is finite and non-trivial, such minimal subgroups exist.

PROPOSITION. *Let H be a finite characteristically simple group.*

(a) *There is a finite simple group N such that every minimal normal subgroup of H is isomorphic with N, and H is the direct product $N_1 \times \ldots \times N_r$ of certain of its minimal normal subgroups.*

(b) *If H is also not abelian, the N_i are the only minimal normal subgroups of H, so that H acts on the set of the N_i. This gives rise to an exact sequence*

$$1 \to \mathrm{Aut}(N_1) \times \ldots \times \mathrm{Aut}(N_r) \to \mathrm{Aut}(H) \to \Sigma_r \to 1,$$

where Σ_r denotes the symmetric group on r letters. (See, for example, [**9**, *p.* 84 *and p.* 87].)

3.8. Let H be a finite group such that every minimal normal subgroup of H is non-abelian. Each minimal normal subgroup is characteristically simple, so the intersections of pairs of minimal normal subgroups are trivial; further, a product $N_1 \ldots N_j$ of minimal normal subgroups contains no minimal normal subgroups other than $N_1, \ldots, N_j$. Therefore if we define $\mathrm{soc}(H)$ to be the subgroup generated by the minimal normal subgroups, we have that $\mathrm{soc}(H)$ is the direct product of the minimal normal subgroups N_i. It is also the product of the minimal characteristic subgroups of H. For if M is a minimal characteristic subgroup, it contains a minimal normal subgroup N. The subgroup of M generated by the $\varphi(N)$ for φ in $\mathrm{Aut}(H)$ must coincide with M; therefore M is a product of certain of the minimal normal subgroups of H. Separating the minimal normal subgroups of H into orbits under $\mathrm{Aut}(H)$, we arrive at a decomposition

$$\mathrm{soc}(H) = \prod M_j$$

with the minimal characteristic subgroups M_j each the product of the N_i in a single orbit.

4. *Lemmas on unipotent elements and representation theory*

4.0. We shall recall some well-known properties of the logarithm and exponential maps in characteristic zero, and shall later show that these extend, under certain restrictions, to characteristic p.

Let K be a field of characteristic zero; we write $\mathrm{Unip}_n(K)$ for the set of $n \times n$ matrices M over K satisfying $(M-I)^n = 0$, and $\mathrm{Nilp}_n(K)$ for the set of $n \times n$ matrices over K satisfying $M^n = 0$. Then the maps

$$\log\colon M \to -\sum_1^{n-1} (I-M)^k/k$$

and

$$\exp\colon M \to \sum_1^{n-1} M^k/k!$$

give mutually inverse bijections

$$\log: \mathrm{Unip}_n(K) \to \mathrm{Nilp}_n(K)$$

and

$$\exp: \mathrm{Nilp}_n(K) \to \mathrm{Unip}_n(K).$$

Further log and exp are isomorphisms for the underlying structures of algebraic varieties.

4.1. If U is a unipotent K-subgroup of GL_n then $\log U(K)$ is a nilpotent subalgebra of the Lie algebra $\mathfrak{gl}_n(K)$. Conversely, if $\mathfrak{n}$ is a nilpotent subalgebra of $\mathfrak{gl}_n(K)$ then $\exp(\mathfrak{n})$ is $U(K)$ for a unipotent K-subgroup U of GL_n.

We have the following identities:

(i) if M is in $\mathrm{GL}_n(K)$ then

$$\log(MAM^{-1}) = M.\log A.M^{-1}$$

for A in $\mathrm{Unip}_n(K)$, and

$$\exp(MAM^{-1}) = M.\exp A.M^{-1}$$

for A in $\mathrm{Nilp}_n(K)$;

(ii) if A and B in $\mathrm{Unip}_n(K)$ have $AB = BA$ then AB is in $\mathrm{Unip}_n(K)$ and

$$\log(AB) = \log A + \log B$$

and

$$\log A.\log B = \log B.\log A;$$

(iii) for A in $\mathrm{Unip}_r(K)$ and B in $\mathrm{Unip}_s(K)$, the tensor products $A \otimes I_s$, $I_r \otimes B$, and $A \otimes B$ lie in $\mathrm{Unip}_{rs}(K)$ and we have

$$\log(A \otimes B) = \log(A \otimes I_s) + \log(I_r \otimes B).$$

4.2. Suppose that p is a prime number with p greater than n. Then the properties of 4.0 and 4.1 hold also for the field $\bar{\mathbf{F}}_p$; this follows by reduction if we take for K a field having a valuation with residue field $\bar{\mathbf{F}}_p$. Here for 4.1 (iii) we assume that rs is at most n.

4.3. Suppose that K is a finite extension of $\mathbf{Q}_p$, and that G is an algebraic K-subgroup of GL_d, such that G is semisimple and of dimension d. We may then identify the Lie algebra $\mathfrak{g}$ of G with the subalgebra $\mathrm{ad}(\mathfrak{g})$ of $\mathfrak{gl}_d$. Then for a unipotent element u of $G(K)$ the logarithm $\log(u)$ is a nilpotent element of $\mathfrak{g}(K)$; and for a nilpotent element n of $\mathfrak{g}(K)$ we have $\exp(n)$ a unipotent element of $G(K)$.

4.4. We wish to extend the property of 4.3 to groups H defined over a finite field F. If F is the residue field of K, and H is obtained by reduction from G, this follows from 4.3 provided p is greater than d, where p is the characteristic of F. For the H which will concern us such a lifting G exists, at least if we pass to an extension of F. However, the following direct argument is sufficient: if H is a semisimple group over F, it is known that the unipotent elements of H and the nilpotent elements of $\mathfrak{h}$ both are irreducible varieties, having the same dimension. If p is greater than $2d+1$ and n is a nilpotent element of $\mathfrak{h}(F)$, we have [**6**] that $\exp(n)$ is in $H(F)$. It follows by elementary algebraic geometry that under this condition on p the restrictions of exp and log give mutually

inverse isomorphisms between the variety of nilpotent elements of $\mathfrak{h}$ and the variety of unipotent elements of H.

4.5. We write $\mathbf{G}_a$ for the additive group (with underlying variety the affine line). Suppose we have a unipotent 1-parameter subgroup of GL_n, that is, a morphism

$$\varphi\colon \mathbf{G}_a \to \mathrm{GL}_n$$

with image contained in Unip_n, defined over a field. Then the differential $d\varphi$ is a K-linear map from the Lie algebra of $\mathbf{G}_a$, which we identify with $\mathbf{G}_a$ itself, to $\mathfrak{gl}_n$. We say that φ is *good* if the image of $d\varphi$ is non-zero and spanned by $\log \varphi(1)$.

For K of characteristic zero every non-trivial unipotent 1-parameter subgroup is good, but this is no longer true in positive characteristic.

4.6. We shall apply results on the representation theory of finite groups of Lie type, due in essentials to Steinberg (see [**12**] and references therein, and also [**1**]). For an almost simple group H defined over a finite field F, these results put in correspondence the representations of the abstract group $H(F)$ with representations which are constructed from algebraic representations of H, and the compositions of these with automorphisms arising from the automorphisms of F (see 4.8 below). We have to deal with twisted groups H, not just the case of split (Chevalley) groups; but by passing to a suitable finite extension F' of F we may assume that H is split, while the (almost) algebraic nature of the abstract representations of $H(F)$ means that all such representations extend to representations of $H(F')$. For our purposes, therefore, we shall be able to assume that H is split.

Let H be an absolutely almost simple group and π a non-trivial infinitesimally irreducible rational representation of H, defined over a finite field F of characteristic p.

LEMMA. *If p is greater than the degree of π, the 1-parameter group $\pi \circ x_\alpha$ is good for every root subgroup x_α of H.*

Proof. From [**1**, 5.13] we may write

$$\pi(x_\alpha(t)) = \sum_0^N t^i X_{\alpha,i}$$

for certain matrices $X_{\alpha,i}$; and

$$X_{\alpha,j} = (j!)^{-1}(d(\pi \circ x_\alpha)(1))^j$$

for $j = 0, 1, \ldots, p-1$. Now the results of [**1**, 6.4] apply to π (this follows from [**1**, 6.3 and 7.2]); therefore the $X_{\alpha,j}$ vanish if j is at least p. Thus

$$\pi(x_\alpha(t)) = \exp(td(\pi \circ x_\alpha)(1)),$$

and inverting we have

$$\log((\pi \circ x_\alpha)(1)) = d(\pi \circ x_\alpha)(1).$$

Therefore $\pi \circ x_\alpha$ is good.

Since H always has root subgroups defined over F, we may also assume that $\pi \circ x_\alpha$ is defined over F.

4.7. To exploit the tensor product theorem of Steinberg, we need a technical result which depends essentially on the linear independence of the automorphisms of a field.

LEMMA. *Let F be a field with p^l elements. Suppose that for $i = 0,\dots,l-1$ we have a good 1-parameter subgroup φ_i of $\mathrm{GL}_{d(i)}$, defined over F, where $d(0)d(1)\dots d(l-1) = n$ is less than p. Define the '1-parameter subgroup' φ of GL_n by*

$$\varphi = \varphi_0 \otimes (\varphi_1 \circ \mathrm{Fr}) \otimes \dots \otimes (\varphi_{l-1} \circ \mathrm{Fr}^{l-1}),$$

where Fr *is the Frobenius automorphism of F, so that φ gives a map from $\mathbf{G}_a(F)$ to $\mathrm{GL}_n(F)$. Then the elements $\log \varphi(t)$ of $\mathfrak{gl}_n(F)$, for t in F, span the same subspace as the elements*

$$L_i = I \otimes I \otimes \dots \otimes \log \varphi_i(t) \otimes \dots \otimes I.$$

Proof. Firstly, using 4.1 (ii) and (iii), we have

$$\log \varphi(t) = \sum_0^{l-1} \log(I \otimes \dots \otimes I \otimes \varphi_i(t^{p^i}) \otimes I \otimes \dots \otimes I).$$

Then since φ_i is good we have F-linearity:

$$\log \varphi_i(t^{p^i}) = t^{p^i} \log \varphi_i(1).$$

This shows that the $\log \varphi(t)$ lie in the subspace spanned by the L_i; the converse follows from the linear independence of the Fr^i.

4.8. For H as in 4.6, and π an irreducible F-representation of H, the tensor product theorem of Steinberg [**12**, **1**] states that there are infinitesimally irreducible rational representations $\pi_0,\dots,\pi_{l-1}$ of H, defined over F, such that π is equivalent to

$$\pi_0 \otimes (\pi_1 \circ \mathrm{Fr}) \otimes \dots \otimes (\pi_{l-1} \circ \mathrm{Fr}^{l-1});$$

here Fr as before is the Frobenius automorphism, acting on $H(F)$. We give a criterion for all but one of the π_i to be trivial, so that the representation π is in fact algebraic (after twisting with a power of Fr), and infinitesimally irreducible.

Let V be the vector space on which H acts via π. Assume that $H(F)$ acts irreducibly on the subspace of $\mathrm{End}(V)$ spanned by the elements $\log \pi(u)$ for u a unipotent element of $H(F)$. Choose for each non-trivial representation π_i a good root subgroup $\varphi_i = \pi_i \circ x_\alpha$ defined over F, as in 4.6. The elements L_i of 4.7 lie in the subspaces

$$W_i = I \otimes \dots \otimes I \otimes d\pi_i(h) \otimes \dots \otimes I$$

of V, where h is the Lie algebra of H. Each W_i is an invariant subspace of $\mathrm{End}(V)$ for the action of $H(F)$, and is irreducible since the adjoint representation of $H(F)$ is irreducible. Then the assumption implies that all the W_i coincide. Since any two of the W_i would have trivial intersection, this shows that there is just one non-trivial π_i, as required.

5. *Proof of the main result, begun*

5.0. We use the notation of § 1. The subgroup Γ of $G(\mathbf{Q})$ is from now on assumed to be Zariski-dense in G. We denote by $\Gamma^{\langle s \rangle}$ the subgroup of Γ generated by the elements γ^s for γ in Γ, and $s = 1, 2, \dots$. It follows from the density of Γ that $\Gamma^{\langle s \rangle}$ is also

Zariski-dense in G: in fact, the sth-power map on G is polynomial, with dense image. Further, $S(\Gamma^{\langle s\rangle})$ is contained in $S(\Gamma)$.

5.1. We first kill possible permutation actions of Γ_p arising in the adjoint representation.

LEMMA. *Suppose that p is in $S(\Gamma^{\langle d!\rangle})$ and $N \lhd \Gamma_p$. Then $\bar{\mathfrak{g}}_p$ is an isotypic N-module, so that, in the notation of* § 3, *we have $\bar{\mathfrak{g}}_p = \bar{\mathfrak{g}}_{p,\sigma}$ for some σ in $\Sigma(N)$.*

Proof. By assumption (1.5(iii)) the action of Γ_p on $\bar{\mathfrak{g}}_p$ is irreducible. From 3.2 we may write

$$\bar{\mathfrak{g}}_p = \bigoplus_T \bar{\mathfrak{g}}_{p,\sigma}$$

as N-module, where Γ_p permutes T transitively. We have $|T|$ at most d, so that the group of permutations of T has exponent dividing $d!$. Now $\Gamma_p^{\langle d!\rangle}$ normalizes N and acts irreducibly; therefore it must also permute T transitively. This implies that T has one element only.

5.2. As a corollary of 5.1 we have

PROPOSITION. *For p in $S(\Gamma^{\langle d!\rangle})$ the group* $\mathrm{soc}(\Gamma_p)$ *of* 3.8 *is a product of non-abelian simple groups.*

Proof. From 3.7 and 3.8 it is enough to show that Γ_p has no non-trivial normal abelian subgroup A. For such a subgroup A it would follow from 5.1 that A acted on $\bar{\mathfrak{g}}_p$ by a non-trivial scalar character. But this would contradict the fact that the image of an adjoint representation contains no non-trivial scalars.

5.3. Suppose that p is in $S(\Gamma^{\langle d!\rangle})$. Then from 3.8 and 5.2 we may write

$$\mathrm{soc}(\Gamma_p) = N_1 \times \ldots \times N_m$$

with the N_i non-abelian simple groups.

LEMMA. *The integer m is bounded by a function of d; more precisely we have $m \leqslant \log_2 d$.*

Proof. From the Clifford theory of 3.2 we know that the faithful representation of $\mathrm{soc}(\Gamma_p)$ on $\bar{\mathfrak{g}}_p$ is completely reducible; from 5.1 it is isotypic. Suppose that V is an irreducible subspace of $\bar{\mathfrak{g}}_p$; we may write V, up to equivalence, as $V_1 \otimes \ldots \otimes V_m$, where N_i acts faithfully on V_i. Since V_i must have dimension at least 2, the bound follows.

5.4. Define d_1 to be $[\log_2 d]!$. Let r be an integer divisible by $d!\,d_1$.

LEMMA. *If p is in $S(\Gamma^{\langle r\rangle})$, we have that $\Gamma_p^{\langle r\rangle}$ normalizes N_i, for $i = 1, \ldots, m$.*

Proof. From 3.8, if we write $\mathrm{soc}(\Gamma_p)$ as a product $\prod M_j$ of minimal characteristic subgroups, the conjugation action of Γ_p gives rise to a homomorphism

$$\Gamma_p \to \prod \mathrm{Aut}(M_j).$$

Applying 5.3 and the definition of d_1, we see that this homomorphism maps $\Gamma_p^{\langle r\rangle}$ to the subgroup fixing the set of N_i. Hence $\Gamma_p^{\langle r\rangle}$ normalizes N_i.

5.5. For any value of r we have that $\mathrm{soc}(\Gamma_p^{\langle r\rangle})$ is characteristic in Γ_p. A minimal characteristic subgroup of $\Gamma_p^{\langle r\rangle}$ is therefore minimal characteristic in Γ_p; so from 3.8 and 5.2 we have that $\mathrm{soc}(\Gamma_p^{\langle r\rangle})$ is the product of precisely those N_i which are subgroups of $\Gamma_p^{\langle r\rangle}$, provided $d!$ divides r.

5.6. Define d_2 to be the least common multiple of the orders $|\mathrm{Aut}(X)|$, where X is a non-abelian finite simple group which is either sporadic or small relative to d. From 2.2 this definition is legitimate.

Suppose the integer r is divisible by $d!d_1d_2$.

LEMMA. *If p is in $S(\Gamma^{\langle r\rangle})$ and the simple group N_i lies in $\Gamma_p^{\langle r\rangle}$, then N_i is a simple group of Lie type associated with a finite field of characteristic p.*

Proof. Conjugation gives a homomorphism

$$\psi\colon \Gamma_p^{\langle d!d_1\rangle} \to \mathrm{Aut}(\mathrm{soc}(\Gamma_p^{\langle r\rangle})).$$

Under our assumption on p the N_i are non-abelian simple groups; if therefore N_i is a subgroup of $\mathrm{soc}(\Gamma_p^{\langle r\rangle})$, the intersection of N_i with the kernel of ψ is trivial. Then from 5.5 it follows that ψ is injective. Further, from 5.4 the image of ψ lies in $\prod \mathrm{Aut}(N_i)$. Then by definition of d_2 we have

$$\psi(\Gamma_p^{\langle r\rangle}) \leqslant \prod_I \mathrm{Aut}(N_i),$$

where I is the set of indices i such that N_i is large with respect to d and not a sporadic group. By the Corollary in 3.4 we have $p(N_i) = p$; since $p \neq 2$ (say by 1.4(i)) we have that N_i is not an alternating group. Thus N_i must be as described.

5.7. To summarize the proof at this stage: we have shown that the subgroup $\Gamma_p^{\langle r\rangle}$ of Γ_p has, for p in $S(\Gamma^{\langle r\rangle})$ and r sufficiently divisible, all its minimal normal subgroups of Lie type for the correct characteristic p. The remainder of the proof forces one such N_i to be the whole group $\mathrm{Ad}(\tilde{G}_p(\mathbf{F}_p))$ which we wish Γ_p to be.

6. *Proof of the main result, completed*

6.0. We assume the notation of § 5. We have shown there that if $d!d_1d_2$ divides r then $\mathrm{soc}(\Gamma_p^{\langle r\rangle})$ is a product $\prod N_i$ with each N_i a simple group of Lie type for the characteristic p. As in the proof in 5.6, the homomorphism

$$\psi\colon \Gamma_p^{\langle r\rangle} \to \prod \mathrm{Aut}(N_i),$$

arising from conjugation, is injective.

6.1. LEMMA. *There is a bound d_3, depending only on G, for the order $|\mathrm{Out}(N_i)|$ where N_i is as in* 6.0.

Proof. If N is a simple group of Lie type over a finite field F, we may write $N = \mathrm{Ad}(H(F))$ for H a simply-connected group defined over F. The structure of

Out(N) is known (see, for example, Steinberg [**12**]). In fact there is a composition series

$$1 = O_4 \lhd O_3 \lhd O_2 \lhd O_1 = \mathrm{Out}(N),$$

where O_1/O_2 is isomorphic with $\mathrm{Gal}(F/\mathbf{F}_p)$, the group O_2/O_3 arises from Dynkin-diagram automorphisms and has order at most 6, and O_3/O_4 is isomorphic with $(\mathrm{Ad}\,H)(F)/\mathrm{Ad}(H(F))$.

To bound $|O_1/O_2| = \log_p|F|$, note that N has order at least

$$|\mathrm{PSL}_2(F)| = \tfrac{1}{2}|F|(|F|^2-1),$$

while, on the other hand, $|N|$ is crudely bounded by $|M_d(\mathbf{F}_p)| = p^{d^2}$. This gives a bound

$$\text{constant}.d^2$$

for $\log_p|F|$.

To bound $|O_3/O_4|$ we use the exact sequence of Galois cohomology arising from the exact sequence

$$1 \to Z \to X \to \mathrm{Ad}\,X \to 1,$$

where Z is the centre of X; this gives us

$$X(F) \to (\mathrm{Ad}\,X)(F) \to H^1(F,Z) \to 1$$

on applying the triviality of $H^1(F,X)$ (see, for example, [**10**]). We see that O_3/O_4 is isomorphic with $H^1(F,Z)$. The possibilities for the $\mathrm{Gal}(\bar{F}/F)$-module Z are known. For H of type A_{n-1} or ${}^2A_{n-1}$ we have Z isomorphic with the Galois module μ_n of nth roots of 1. Since the orders of $\mathrm{PSL}_n(F)$ and $\mathrm{PU}_n(F)$ tend to infinity with n, there is a bound for n here. For H of other types, we have that Z has order at most 4. For any F the group $\mathrm{Gal}(\bar{F}/F)$ is isomorphic with the profinite completion $\hat{\mathbf{Z}}$ of the infinite cyclic group. We conclude that only finitely many isomorphism classes of modules may occur, so that the order of the cohomology group $H^1(F,Z)$ is bounded.

Finally, therefore, there is a bound d_3 for the order of $\mathrm{Out}(N_i)$, depending only on G.

6.2. We have $\mathrm{Inn}(N_i)$ isomorphic with N_i. Therefore from 6.1 if r is divisible by $d!d_1d_2d_3$ and p is in $S(\Gamma^{\langle r\rangle})$, we have

$$\psi(\Gamma_p^{\langle r\rangle}) \leqslant \prod \mathrm{Inn}(N_i),$$

and so $\Gamma_p^{\langle r\rangle}$ is the product of its minimal normal subgroups $N_1,\ldots,N_s$, say.

6.3. We show first that $s = 1$, so that $\Gamma_p^{\langle r\rangle} = N_1 = N$, say. Suppose that we have N_i isomorphic with $H_i^+(F_i)$, where we write $H^+(F)$ for $\mathrm{Ad}(H(F))$ and the H_i are simply connected, absolutely almost simple groups and F_i is a finite subfield of $\bar{\mathbf{F}}_p$.

LEMMA. *Under the hypothesis of* 6.2 *on* r *we have* $s = 1$.

Proof. We suppose that s is greater than 1 and derive a contradiction. The product $N_1 \times \ldots \times N_s$ acts irreducibly on $\bar{\mathfrak{g}}_p$, since p is in $S(\Gamma^{\langle r\rangle})$. We may write this representation as $\pi_1 \otimes \ldots \otimes \pi_s$, up to equivalence. Let u be an element of $N_1 = H_1^+(F_1)$ which is unipotent and not the identity. Then from 4.2, $\log \pi_1(u)$ is a

non-zero nilpotent endomorphism; if we identify $\log \pi_1(u) \otimes I \otimes \ldots \otimes I$, which from 4.4 lies in $\mathrm{ad}(\mathfrak{g}_p)$, with an element of $\mathfrak{g}_p$, it is fixed under $N_2 \times \ldots \times N_s$. Then, by irreducibility, $\pi_2, \ldots, \pi_s$ are trivial representations: but the original representation is faithful. This gives a contradiction.

6.4. Write $N = H^+(F)$ as in 6.3, so that N acts irreducibly on $\bar{\mathfrak{g}}_p$. Then 4.8 applies: the representation of N is the restriction to N of an infinitesimally irreducible rational representation π of H. Consider $d\pi(\mathfrak{h})$, where $\mathfrak{h}$ is the Lie algebra of H. This is an invariant non-zero subspace of $\mathrm{ad}(\mathfrak{g}_p)$; since N acts irreducibly on $\mathrm{ad}(\mathfrak{g}_p)$, we must have $d\pi(\mathfrak{h}) = \mathrm{ad}(\mathfrak{g}_p)$. Since $d\pi$ induces an isomorphism of Lie algebras, the algebraic group H must be the simply-connected cover $\tilde{G}_p$; we therefore have $F = \mathbf{F}_p$, and N isomorphic with $\tilde{G}_p^+(\mathbf{F}_p)$. So we have

THEOREM. *For all primes p in $S(\Gamma^{\langle r \rangle})$ where $d!d_1d_2d_3$ divides r, we have $\Gamma_p = \tilde{G}_p^+(\mathbf{F}_p)$.*

6.5. For almost all p the simply-connected cover $\tilde{G}_p$ may be obtained by reduction from the simply-connected cover $\tilde{G}$ of G.

LEMMA. *Suppose that p is at least 5 and that X is a subgroup of $\tilde{G}_p(\mathbf{F}_p)$ with image $\tilde{G}_p^+(\mathbf{F}_p)$ in $G_p(\mathbf{F}_p)$. Then $X = \tilde{G}_p(\mathbf{F}_p)$.*

Proof. The kernel of the adjoint representation is central, so that $\tilde{G}_p(F_p)$ is XA for a central subgroup A. Therefore the commutator subgroup of $\tilde{G}_p(F_p)$ is contained in X; but if p is at least 5 the commutator subgroup is the whole group [**12**], and our assertion follows.

6.6. Combining 6.4 and 6.5 we find the version of the Theorem stated in the Introduction, if we take into account the remarks in 1.5 and 5.0.

7. *Application to p-adic closures*

7.0. In this section, as before, G is an absolutely simple adjoint group over $\mathbf{Q}$, and $\tilde{G}$ its simply-connected covering group. As in 6.3 we denote by $G_p^+(\mathbf{F}_p)$ the image of $\tilde{G}_p(\mathbf{F}_p)$ in $G_p(\mathbf{F}_p)$.

7.1. LEMMA. *Let X be a subgroup of $G_p^+(\mathbf{Z}/p^n\mathbf{Z})$, for $n \geqslant 1$, such that the image of X in $G_p(\mathbf{F}_p)$ is $G_p^+(\mathbf{F}_p)$. Then X is the full group $G_p^+(\mathbf{Z}/p^n\mathbf{Z})$, provided p exceeds a bound $f(G)$.*

Proof. We assume that the prime p is sufficiently large for G to have good reduction at p, and is quasi-split over $\mathbf{Q}_p$. Assume also that $p \geqslant 5$. We drop the subscript p in the proof.

By the assumption that G is quasi-split it has a subgroup isomorphic over $\mathbf{Q}_p$ to SL_2 or PSL_2. For these groups the proposition is true (see, for example, Serre [**11**, IV.3.4] for SL_2, from which the case of PSL_2 follows).

Now take the case where $n = 2$ for general G. We identify the kernel of the reduction homomorphism from $G(\mathbf{Z}/p^2\mathbf{Z})$ to $G(\mathbf{Z}/p\mathbf{Z})$ with the abelian group B underlying $\mathfrak{g}(\mathbf{F}_p)$. We have an exact sequence

$$1 \to B \to G(\mathbf{Z}/p^2\mathbf{Z}) \to G(\mathbf{Z}/p\mathbf{Z}) \to 1$$

with the action of $G(\mathbf{Z}/p\mathbf{Z})$ on B being the adjoint action, and hence irreducible. Let X be a subgroup of $G(\mathbf{Z}/p^2\mathbf{Z})$ mapping onto $G(\mathbf{Z}/p\mathbf{Z})$; then $X \cap B$ is invariant under $G(\mathbf{Z}/p\mathbf{Z})$, and hence is trivial or the whole group. In the latter case we have $X = G(\mathbf{Z}/p^2\mathbf{Z})$; if the intersection is trivial and H is the subgroup of G of type A_1 mentioned above, we have $X \cap H(\mathbf{Z}/p^2\mathbf{Z})$ a proper subgroup mapping onto $H(\mathbf{Z}/p\mathbf{Z})$, a contradiction to the result quoted.

Now assuming that $n \geqslant 2$, note that the kernel B_n of reduction from $G(\mathbf{Z}/p^n\mathbf{Z})$ to $G(\mathbf{Z}/p\mathbf{Z})$ is a p-group, containing the kernel C_n of reduction from $G(\mathbf{Z}/p^n\mathbf{Z})$ to $G(\mathbf{Z}/p^2\mathbf{Z})$. We establish below that C_n is in fact the Frattini subgroup of B_n. Then given X as in the Proposition, let Y be its image in $G(\mathbf{Z}/p^2\mathbf{Z})$; from the case where $n = 2$ treated above, we have that Y is the full group. Therefore $X \cap B_n$ maps onto B_n/C_n; by the elementary properties of the Frattini subgroup we have $X \cap B_n = B_n$. This implies that $X = G(\mathbf{Z}/p^n\mathbf{Z})$, as required.

To complete the proof we show that C_n is the Frattini subgroup of B_n. Since the quotient B_n/C_n is a subgroup of B, which is elementary abelian, we certainly have that C_n contains the Frattini subgroup; in fact $B_n/C_n = B$ by Hensel's Lemma, and hence has rank $d = \dim G$. To complete the proof we show that B_n is generated by d elements.

In fact we show that the subgroup G_1 of $G(\mathbf{Z}_p)$ of elements congruent to I modulo p is topologically generated by d elements; this implies what we want for its quotients B_n. We write $\mathfrak{g}(\mathbf{Z}_p)$ for the stabilizer in $\mathfrak{g}(\mathbf{Q}_p)$ of the lattice Λ of 1.2, and $\mathfrak{g}_r$ for $p^r\mathfrak{g}(\mathbf{Z}_p)$. We show that if $x_1, \ldots, x_d$ are a $\mathbf{Z}_p$-basis of $\mathfrak{g}_1$ then the $\exp(x_i)$ are topological generators for G_1; here the exponential and logarithm maps are given by the usual series, which converge and give homeomorphisms of G_1 and $\mathfrak{g}_1$. Let K be the closed subgroup of G_1 generated by the $\exp(x_i)$; then $\log(K)$ is closed since K is compact. The Campbell–Hausdorff formula $\log(\exp(x)\exp(y)) = x + y + \frac{1}{2}[x, y] + \ldots$ here gives a convergent series for x, y in $\mathfrak{g}_1$. Given x in $\mathfrak{g}_1$ we can construct inductively $0 = x^{(0)}$, $x^{(1)}, \ldots$ with $x^{(j)} \equiv x$ modulo $\mathfrak{g}_{j+1}$ by writing

$$x - x^{(j-1)} \equiv p^j \sum n_{ij} x_i \quad \text{modulo } \mathfrak{g}_{j+1},$$

with n_{ij} positive integers, and taking

$$x^{(j)} = \log(\exp(x^{(j-1)})\exp(x_1)^{a(1)} \ldots \exp(x_d)^{a(d)})$$

with $a(i) = n_{ij}p^j$. This shows that x is in $\log(K)$, whence $\log(K) = \mathfrak{g}_1$ and $K = G_1$, as required. This completes the proof.

7.2. Now consider the exact sequence

$$1 \to Z \to \tilde{G} \to G \to 1$$

where Z is the centre of $\tilde{G}$. This gives rise to the sequences

$$1 \to Z(\mathbf{Q}_p) \to \tilde{G}(\mathbf{Q}_p) \to G(\mathbf{Q}_p)$$

and

$$1 \to Z_p(\mathbf{F}_p) \to \tilde{G}_p(\mathbf{F}_p) \to G_p(\mathbf{F}_p).$$

For a given G, the groups $Z(\mathbf{Q}_p)$ and $Z(\mathbf{F}_p)$ are isomorphic if p is large enough, for then we can assume that Z is smooth and Hensel's lemma applies. For such p we then have

a diagram

$$\begin{array}{ccc} \tilde{G}(\mathbf{Z}/p^n\mathbf{Z}) & \longrightarrow & G(\mathbf{Z}/p^n\mathbf{Z}) \\ \downarrow & & \downarrow \\ \tilde{G}(\mathbf{Z}/p\mathbf{Z}) & \longrightarrow & G(\mathbf{Z}/p\mathbf{Z}) \end{array}$$

with the kernels of the vertical arrows isomorphic.

7.3. From 7.1, 7.2, and 6.6 we have

PROPOSITION. *Any subgroup X of $\tilde{G}(\mathbf{Z}/p^n\mathbf{Z})$ with image $G^+(\mathbf{F}_p)$ in $G(\mathbf{F}_p)$ is equal to $\tilde{G}(\mathbf{Z}/p^n\mathbf{Z})$, provided p is at least $f(G)$.*

Applying this to the situation of 6.5 we have

THEOREM. *If $\tilde{\Gamma}$ is Zariski-dense in $\tilde{G}$ then for almost all p in $S(\tilde{\Gamma})$ the p-adic closure of $\tilde{\Gamma}$ in $\tilde{G}(\mathbf{Q}_p)$ is $\tilde{G}(\mathbf{Z}_p)$.*

Proof. Recalling that for almost all p we have

$$\tilde{G}(\mathbf{Z}_p) = \varprojlim \tilde{G}(\mathbf{Z}/p^n\mathbf{Z}),$$

we see that this follows from 6.5 and the Proposition above.

7.4. Suppose that $\tilde{\Gamma}$ is Zariski-dense in $\tilde{G}$. Then $\tilde{\Gamma}$ contains elements of infinite order (a short proof of this well-known fact comes from the theorem of C. Jordan that a finite subgroup of $\mathrm{GL}_m(\mathbf{C})$ has an abelian normal subgroup of index dividing $b(m)$, for some function b; so that if this is not so, $\tilde{\Gamma}^{\langle b(m)\rangle}$ would be commutative, which is absurd since G is not).

LEMMA. *There is a finitely generated subgroup Γ_0 of $\tilde{\Gamma}$ with Γ_0 Zariski-dense in $\tilde{G}$.*

Proof. Choose a finitely generated subgroup Γ_1 of $\tilde{\Gamma}$ with $\dim(\bar{\Gamma}_1)$ maximal; by the remarks above, $\dim(\bar{\Gamma}_1)$ is at least 1. If $\mathfrak{g}_1$ is the Lie algebra of $\bar{\Gamma}_1$, it is an invariant subspace for the action of $\tilde{\Gamma}$, by its maximality; since, from 3.5, $\tilde{\Gamma}$ acts irreducibly on $\mathfrak{g}$, we must have $\mathfrak{g}_1 = \mathfrak{g}$. Therefore we may take $\Gamma_0 = \Gamma_1$.

7.5. If $\tilde{\Gamma}$ of 7.3 is finitely generated, the exceptional set of p not in $S(\tilde{\Gamma})$ is finite. Therefore from 7.3 and 7.4 we have

THEOREM. *If $\tilde{\Gamma}$ is Zariski-dense in $\tilde{G}$, the p-adic closure of $\tilde{\Gamma}$ contains $\tilde{G}(\mathbf{Z}_p)$ for almost all p.*

8. *Application to adelic closures and approximation sets*

8.0. We define a *prime divisor* v of $\mathbf{Q}$ to be a prime number p or the symbol ∞; we then write $\mathbf{Q}_v$ to be the completion $\mathbf{Q}_p$ for a prime p or $\mathbf{Q}_\infty = \mathbf{R}$. For $\tilde{G}$ as in § 1 we define the adele group $\tilde{G}(\mathbf{A}_S)$, for any set S of prime divisors, to be the restricted product $\prod \tilde{G}(\mathbf{Q}_v)$, taken over v not in S, formed with respect to the compact

subgroups $\tilde{G}(\mathbf{Z}_p)$ which are defined by 1.2 for almost all p. Then $\tilde{G}(\mathbf{A}_S)$ becomes a topological group.

Any given element γ of $\tilde{G}(\mathbf{Q})$ lies in $\tilde{G}(\mathbf{Z}_p)$ for almost all p; therefore there is an embedding of $\tilde{G}(\mathbf{Q})$ in $\tilde{G}(\mathbf{A}_S)$, provided the set S is not the set of all prime divisors.

Given a subgroup $\tilde{\Gamma}$ of $\tilde{G}(\mathbf{Q})$ we say that S is an *approximation set* for $\tilde{\Gamma}$ if the closure of $\tilde{\Gamma}$ in $\tilde{G}(\mathbf{A}_S)$ is open. Classical results characterize the approximation sets for $\tilde{G}(\mathbf{Q})$ as being those S which contain some v such that $\tilde{G}(\mathbf{Q}_v)$ is not compact.

8.1. We prove

THEOREM. *If the subgroup $\tilde{\Gamma}$ of $\tilde{G}(\mathbf{Q})$ is Zariski-dense, there is a finite approximation set S for $\tilde{\Gamma}$.*

The proof occupies the rest of this section. As a first remark, note that by the Lemma in 7.4 we may assume that $\tilde{\Gamma}$ is finitely generated. Further we may assume that S contains ∞, so that $\tilde{G}(\mathbf{A}_S)$ is a restricted product of p-adic groups.

8.2. In the situation of 8.1, the finitely generated group $\tilde{\Gamma}$ is from 7.5 dense in $\tilde{G}(\mathbf{Z}_p)$ for almost all p. We define S to be the set of prime numbers such that p is at most 5, or G_p or $\tilde{\Gamma}_p$ is not defined, or $\tilde{\Gamma}$ is not dense in $\tilde{G}(\mathbf{Z}_p)$, together with ∞. Then S is finite; we show that $\tilde{\Gamma}$ is dense in the open subgroup $\prod\tilde{G}(\mathbf{Z}_p)$ of $\tilde{G}(\mathbf{A}_S)$, where the product is taken over primes p not in S. This proves the theorem.

8.3. LEMMA. *There is a topological isomorphism of the product $\prod\tilde{G}(\mathbf{Z}_p)$ of* 8.2 *and the inverse limit of the system of all finite products*

$$\tilde{G}(n) = \prod\tilde{G}(\mathbf{Z}/p^{r(p)}\mathbf{Z}),$$

indexed by integers $n = \prod p^{r(p)}$ prime to the elements of S.

Proof. Combine the definitions of the product and inverse topologies with the topological isomorphism of $\tilde{G}(\mathbf{Z}_p)$ and $\varprojlim \tilde{G}(\mathbf{Z}/p^r\mathbf{Z})$.

8.4. LEMMA. *For p not in S define $Y(p^r)$ to be $\tilde{G}_p(\mathbf{Z}/p^r\mathbf{Z})$. Let Y be the product $Y(p_1^{r(1)}) \times \ldots \times Y(p_k^{r(k)})$ and X a subgroup of Y having projection $Y(p_i^{r(i)})$ on the i-th factor for $i = 1, \ldots, k$, where the p_i are distinct primes in S. Then $X = Y$.*

Proof. The $Y^+(p) = G_p^+(\mathbf{F}_p)$ are simple groups, which are not isomorphic for distinct primes p. We show first that the composition factors of X, counted with multiplicity, include at least those of the $Y^+(p_i^{r(i)})$.

The kernel of the reduction map from $Y^+(p^n)$ to $Y^+(p)$ is a p-group; for in a matrix representation if we have

$$\gamma \equiv I \quad \text{modulo } p$$

then $\gamma = I + pu$, whence $\gamma^{p^n} = 1$. Therefore the kernel has exponent a power of p.

Therefore if the p_i are distinct, the image of X in $Y^+ = \prod Y^+(p_i^{r(i)})$ is Y^+, as we see by counting composition factors.

Now let X_i be the inverse image in X of $Y^+(p_i^{r(i)})$. Any element of X_i may be written as zx where z is central in Y and x lies in $Y(p_i^{r(i)})$. The commutator $[z_1x_1, z_2x_2]$ of two

such elements is $[x_1, x_2]$ which lies in $Y(p_i^{r(i)})$. Therefore from 6.6 we have $X_i = Y(p_i^{r(i)})$, which shows that $X = Y$.

8.5. The Theorem of 8.1 follows from 8.2, 8.3, and 8.4.

References

1. A. BOREL et al., *Seminar on algebraic groups and related finite groups*, Lecture Notes in Mathematics 131 (Springer, Berlin, 1970).
2. R. W. CARTER, *Simple groups of Lie type* (Wiley–Interscience, London, 1972).
3. D. GORENSTEIN, *Finite groups* (Chelsea, New York, 1980).
4. D. GORENSTEIN, *Finite simple groups* (Plenum Press, New York, 1982).
5. C. HOOLEY, 'On Artin's conjecture', *J. Reine Angew. Math.*, 225 (1967), 209–220.
6. V. KAC and B. WEISFEILER, 'Exponentials in Lie algebras of characteristic p', *Math. USSR-Izv.*, 5 (1971), 777–803.
7. M. KNESER, 'Starke Approximation in algebraischen Gruppen I', *J. Reine Angew. Math.*, 218 (1965), 190–203.
8. S. LANG and H. TROTTER, 'Primitive points on elliptic curves', *Bull. Amer. Math. Soc.*, 83 (1977), 289–292.
9. D. J. S. ROBINSON, *A course in the theory of groups* (Springer, New York, 1980).
10. J.-P. SERRE, *Cohomologie Galoisienne*, Lecture Notes in Mathematics 5 (Springer, Berlin, 1965).
11. J.-P. SERRE, *Abelian l-adic representations and elliptic curves* (W. A. Benjamin, New York, 1968).
12. R. STEINBERG, *Lectures on Chevalley groups*, Yale lecture notes, 1968.

C. R. Matthews
Department of Pure Mathematics and Mathematical Statistics
16 *Mill Lane*
Cambridge

L. N. Vaserstein and B. Weisfeiler
Department of Mathematics
Pennsylvania State University
University Park
PA 16802, *U.S.A.*