Annals of Mathematics, 120 (1984), 271–315

Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups

By Boris Weisfeiler*

To Armand Borel on his sixtieth birthday

1. Introduction

In this paper we show that Zariski density of a subgroup of a semi-simple algebraic group implies very strong restrictions on its finite factor groups. An important part of our results is contained in the following:

(1.1) Theorem. *Let k be an algebraically closed field of characteristic different from 2 and 3, and G an almost simple, connected and simply connected algebraic group defined over k. Let Γ be a finitely generated Zariski dense subgroup of $G(k)$ and A the subring of k generated by the traces* $\operatorname{tr} \operatorname{Ad} \gamma$, $\gamma \in \Gamma$. *Then there exist $b \in A$, a subgroup Γ' of finite index in Γ, and a structure G_{A_b} of a group scheme over A_b on G such that $\Gamma' \subseteq G_{A_b}(A_b)$ and Γ' is dense in $G_{A_b}(\hat{A}_b)$.*

Here A_b denotes the localization of A at $b \in A$ and $\hat{A}_b$ denotes the profinite completion $\varprojlim_{|A_b/I|<\infty}(A_b/I)$. Then $\hat{A}_b$ is a compact topological ring and $G_{A_b}(\hat{A}_b)$ is considered with the topology inherited from $\hat{A}_b$. The precise statements of our main results are given in (8.2) and (9.1.1).

This work grew out of [MVW] where the case $A \subseteq \mathbf{Q}$ was treated. I am grateful to my coauthors in [MVW], C. Matthews and L. Vaserstein.

(1.2) To see what is at issue in the theorem above, let us consider the case when $A = \mathbf{Z}$ and G is a group scheme over $\mathbf{Z}$. Our theorem then implies (see (10.5)) that roughly the same strong approximation result holds for all Zariski dense subgroups of $G(\mathbf{Z})$ independently of whether they are arithmetic or not. This seems to imply that the strong approximation is a general algebraic and not an arithmetic property. (But this is not strange since the Chinese remainder theorem which is, essentially, behind our approximation results, holds in any ring.) The fact that we do not use any arithmetic information enables us to generalize strong approximation to Zariski dense subgroups (instead of arithmetic

*Supported by NSF.

ones) and to base rings of higher dimension (instead of rings of S-integers of global fields).

(1.3) Related to our approach is the fundamental difficulty that we have to work with finite groups, and the structure of algebraic groups is often of no help since the Zariski closures of finite groups are the groups themselves.

To compensate for this handicap we use classification of finite simple groups in our first (in order and in importance) step (see § 3). The classification is used in the form that the number of sporadic groups is finite. Our next step (again in order and in importance) uses the Steinberg representation theory of groups of Lie type in their characteristic (see § 4). Another point where we have difficulty is in Section 7; but there the difficulty is self-imposed: we want to obtain a result for all cases for which we do not know counterexamples. Therefore we have to invoke in Section 7 very detailed information on the structure of Lie algebras of algebraic groups in small characteristics.

(1.4) Let us go back to a Zariski dense subgroup $\Gamma \subset G(\mathbf{Z})$ and take further, $G = \mathrm{SL}_n$. Such a Γ is naturally embedded into every $\mathrm{SL}_n(\mathbf{Z}_p)$ where $\mathbf{Z}_p$ is the ring of p-adic numbers. Since $\mathrm{SL}_n(\mathbf{Z}_p)$ is compact and Γ is infinite, the closure $\Gamma_{(p)}$ of Γ in $\mathrm{SL}_n(\mathbf{Z}_p)$ is not discrete. Then it is a p-adic analytic group and it has a nontrivial Lie algebra L which is a subalgebra of the Lie algebra $\mathrm{Lie}\,\mathrm{SL}_n$ of SL_n. We have $\mathrm{Ad}\,\gamma(L) = L$ by construction for all $\gamma \in \Gamma$. Thus L is invariant under the adjoint action of Γ and, therefore, under the adjoint action of the Zariski closure SL_n of Γ. Therefore $L = (\mathrm{Lie}\,\mathrm{SL}_n)(\mathbf{Q}_p)$. This implies that $\Gamma_{(p)}$ is open in $\mathrm{SL}_n(\mathbf{Z}_p)$. Let $\bar{\Gamma}$ be the closure of Γ in $\mathrm{SL}_n(\hat{\mathbf{Z}})$. Clearly $\bar{\Gamma} \subseteq \prod_p \Gamma_{(p)}$. Let $\mathrm{SL}_n(p, \mathbf{Z}_p)$ be the largest normal pro-p-subgroup of $\mathrm{SL}_n(\mathbf{Z}_p)$. Then $\bar{\Gamma} \subseteq \prod_p \Gamma_{(p)} \mathrm{SL}_n(p, \mathbf{Z}_p)$. For the latter group to be open in $\mathrm{SL}_n(\hat{\mathbf{Z}})$ one needs only (!) that $\Gamma \cdot \mathrm{SL}_n(p, \mathbf{Z}_p)/\mathrm{SL}_n(p, \mathbf{Z}_p)$ is $\mathrm{SL}_n(\mathbf{F}_p)$ for almost all p. This is essentially shown in Sections 3 and 4 (although the pieces are put together only in (8.11)). Once the isomorphism $\Gamma \cdot \mathrm{SL}_n(p, \mathbf{Z}_p)/\mathrm{SL}_n(p, \mathbf{Z}_p) \simeq \mathrm{SL}_n(\mathbf{F}_p)$ is established the rest of strong approximation follows almost formally. The situation is however different in positive characteristics where one must work to establish a similar claim for reductions modulo squares of maximal ideals.

(1.5) Let us now briefly describe the main ideas and steps of the proof. First of all, we make two general remarks: (i) We tried to keep difficult parts of the paper as independent of the rest of the paper as we could, and (ii) As we have already remarked, we strove for a result which would cover all the cases to which

we do not know counterexamples (the counterexamples we do know are described in (12.2)).

In this outline we use the expression "for most ideals" in place of "for all ideals of an appropriate localization."

Let k, G, Γ, and A be as in Theorem (1.1). Using ideas and methods of E. B. Vinberg (see [V]), we establish in Section 8 that G has a structure G_A of a group scheme over A, that for some $c \in A$ the ring A_c is finitely generated and regular, and that $G_{A_c}(A_c) \cap \Gamma$ is of finite index in Γ. We take for Γ' a certain normal subgroup of Γ contained in $G_{A_c}(A_c) \cap \Gamma$. Using standard results about group schemes we can assume that G_{A_c} is smooth, connected and semi-simple. This means, in particular, that the reductions of G_{A_c} modulo the maximal ideals of A_c are semi-simple.

We fix two representations of G: one, denoted $\overline{\mathrm{Ad}}$, on L/C, the Lie algebra of G modulo its center, and another, $\mathrm{Ad}\,\overline{\mathrm{Ad}}$, on the algebra $\mathrm{End}(L/C)$ of the vector-space endomorphisms of L/C. We choose then a very small but still Zariski-dense subgroup Δ of Γ'. Since Δ is Zariski-dense, its reductions modulo most maximal ideals have the same enveloping algebra in the two representations as the reduction of G itself. In particular, the reductions of $\overline{\mathrm{Ad}}\,\Delta$ are absolutely irreducible.

In Section 3 we show that the assumption that the reduction $\overline{\mathrm{Ad}}\,\Delta_M$ of $\overline{\mathrm{Ad}}\,\Delta$ is absolutely irreducible severely restricts the structure of $\overline{\mathrm{Ad}}\,\Gamma_M$. That is, it turns out that $\overline{\mathrm{Ad}}\,\Delta_M$ is the socle of $\overline{\mathrm{Ad}}\,\Gamma_M$ and is isomorphic to a product of finite simple groups of Lie type in the same characteristic as A_c/M. The proof uses classification of finite simple groups. We write down a finite list of finite simple groups, and then show that if a finite simple group H is not on the list but its universal central extension admits a representation of a given dimension ($=$ $\dim(L/C)$ in our case) over a field K, then H is of Lie type and of the same characteristic as K. To compile such a list we include in it all the sporadic groups and then check that it suffices to augment it by only a finite number of the remaining ones.

Once we know that our group is a product $\prod_{1 \le i \le t} N_i$ of simple groups of Lie type, we apply in Section 4 Steinberg's representation theory of such groups and extend the imbeddings of finite groups N_i in $\mathrm{GL}(L/C)$ to representations of the corresponding simply connected algebraic groups H_i. This enables us to use algebraic groups. We establish that if $\mathrm{End}(L/C)$ has the same submodule structure under $\prod N_i$ as under G (both acting via $\mathrm{Ad}\,\overline{\mathrm{Ad}}$), then $t = 1$ and $H_1 \simeq G$. That the submodule structures under $\prod N_i$ and G are the same will follow from (8.9). It is worth pointing out at this point that the crucial argument of Section 4, our proof of (4.8), depends on the type of H_1 and not on that of G.

Therefore, although some types of G are excluded by the assumptions, the proof of (4.8) cannot use these assumptions. The reader could, quite properly, interpret this as an indication of how lopsided the whole situation is.

The combined result of Sections 3 and 4, to wit, that the reduction of Γ' modulo most maximal ideals M of A_c is $G_{A_c}(A_c/M)$, is, actually, the main result of the paper. It is, however, neither deduced nor invoked until (8.11). To extend it to strong approximation requires work, but only work.

Sections 5 and 6 are preparatory for Section 7 and were separated to unload and streamline Section 7. In Section 5 we study group schemes over finite local rings. In Section 6 we obtain a cohomological result suggested by J. Bernstein. In Section 7 we study reductions Γ'_I of Γ' modulo any cofinite ideal I. The essential step is the case when I is the square of a maximal ideal. The difficulty here is that Γ'_{M^2} might be isomorphic to $G_{A_c}(A_c/M)$ but have the same ring of traces as $G_{A_c}(A_c/M^2)$ (if it is skewly embedded into $G_{A_c}(A_c/M^2)$). We reject this possibility (essentially) by showing that if $\Gamma'_{M^2} \simeq G_{A_c}(A_c/M)$ then $A_c/M^2 \to A_c/M$ has a ring section. Then the cohomological result of Section 6 shows (again, essentially) that Γ'_{M^2} is conjugate to the group section $G_{A_c}(A_c/M) \to G_{A_c}(A_c/M^2)$ corresponding to the ring section $A_c/M \to A_c/M^2$. Then, of course, the traces of Γ'_{M^2} are contained in A_c/M in contradiction to the assumptions.

An extension from the case $I = M^2$, M a maximal ideal, to the case of a general ideal is standard and easy.

In Section 8 the stage is set for application of results of Sections 3, 4 and 7 and the corresponding conditions are verified. This gives our main result in its precise form: Theorem (8.2).

In Section 9 several, mostly straightforward, reformulations of (8.2) are derived. In Section 10 we specialize to the case when A is contained in a global field K. In this case the topology of $\hat{A}$ extends to the ring of adeles $\hat{A} \otimes_A K$ making it into a topological ring. This permits us to drop the assumption that Γ is finitely generated. On the other hand in this case we can under suitable reasonable assumptions extend our claim to describe the closure of Γ not only in $G_{A_c}(\hat{A}_c)$ (where G_{A_c} is a smooth semi-simple group scheme over A_c) but also in $G(\hat{A} \otimes_A K)$. In particular, we recover the usual strong approximation theorem over global fields of characteristic zero and extend it to integral Zariski dense subgroups.

In Section 11 we describe an interpretation and generalization given by D. Johnson and J. Millson of the Thurston bending. Given a cocompact arithmetic lattice in $SO(n, 1)$ one can, using Thurston bending, deform it inside $SO_{n+N+1}(\mathbf{C})$ or/and $SL_{n+N+3}(\mathbf{C})$, for every positive integer N, in such a way that the result will be Zariski dense. This gives an example of a non-virtually-free

group which can be imbedded as a Zariski-dense subgroup into infinitely many absolutely almost simple algebraic groups over **C**. Applying to such an embedding our results about Zariski-dense groups, we construct certain quotients of the profinite completion of such a lattice. The considerations of Section 11 are based on results reported by J. Millson at a seminar at Harvard; I am grateful to him for the permission to use them here.

Section 12 contains an observation of D. Kazhdan about the similarity of the present work to Serre's problem on elliptic representations. We also give in Section 12 indications of how our proof and results break down in the excluded cases.

(1.6) After the present work had been submitted, I learned that Madhav V. Nori in "Subgroups of $\mathrm{SL}_n(\mathbf{Z})$ and $\mathrm{SL}_n(\mathbf{F}_p)$", to appear in Invent. Math., obtained independently and simultaneously with us results which substantially generalize the results of [MVW] and, in the case of $\Gamma \subseteq \mathrm{SL}_n(k)$, k a number field, also those of this paper (i.e. they contain our Theorem (10.5)). His generalization permits non-semi-simple groups, and his proof does not use classification of finite simple groups.

NORI'S THEOREM. *Let Γ be a subgroup of $\mathrm{SL}_n(\mathbf{Z}[1/m])$ and let G be its Zariski closure. Then the closure of Γ in $\prod_{p\nmid m}\mathrm{SL}_n(\mathbf{Z}_p)$ contains an open subgroup of $\prod_{p\nmid m}\mathscr{D}(G)(\mathbf{Z}_p)^+$.*

Here $G(\mathbf{Z}_p)^+$ is the subgroup of $G(\mathbf{Z}_p)$ generated by the Sylow pro-p-subgroups of $G(\mathbf{Z}_p)$.

Nori's motivation for finding the quoted theorem came from Serre's work [Se].

(1.7) Help and advice of J. Bernstein and D. Kazhdan were indispensable for completion of this work. I use this opportunity to acknowledge my indebtness and gratitude to them. My thanks also go to A. Lubotzky, C. Matthews, J. Millson, Y. Nisnevich, C. Riehm, D. Sibley, J. Tits, L. Vaserstein, and W. Waterhouse for many helpful suggestions and useful conversations. Finally I am grateful to the Mathematics Department of Harvard University for hospitality which made this work possible.

2. Conventions and notation

(2.1) At certain points in the paper we use terminology of finite group theory, the corresponding general reference is [G1]. However, we recall that "p'" means "prime to p". In particular, a p'-complement in a group exists if a Sylow p-group is normal; then it is a subgroup of order prime to p which together with the Sylow p-subgroup generates our group. A semisimple finite group is one

which has trivial radical, or, the same, has no commutative normal subgroups. The socle of a finite group is the normal subgroup generated by the minimal normal subgroups of that group. We use Sym_n and Alt_n to denote respectively the group of all and even permutations of n letters.

(2.2) For any group abstract or algebraic, and for any Lie algebra we use $C(\cdot)$ to denote its center, $N_\cdot(\cdot)$ (resp. $Z_\cdot(\cdot)$) to denote the normalizer (resp. centralizer) of the object in parentheses, in the object used as a subscript. Next $\mathscr{D}^i(\cdot)$ denotes the i-th derived group or Lie algebra of the object in parentheses. For a group H, again abstract or algebraic, and an integer n, we use $H^{\langle n\rangle}$ to denote the subgroup of H generated by the n-th powers of the elements of H. For a subset S of an algebraic (or abstract) group H we use $\langle S\rangle$ to denote the subgroup of H generated by S.

In some cases we use $(\cdot)/(\text{center})$ to denote $(\cdot)/C(\cdot)$; it should not lead to confusion.

(2.3) If H is an algebraic group then $C(H)$, $N_H(\cdot)$, $Z_H(\cdot)$, $\mathscr{D}^i(H)$, $H^{\langle n\rangle}$, and $\langle\ \cdot\ \rangle$ are all considered in the class of algebraic groups.

(2.4) For an algebraic group we use "simple" or "semi-simple" to mean "connected simple" or "connected semi-simple".

For an algebraic group G and a ring A we use G_A to denote a structure of a group scheme over A on G. Then if B is an A-algebra we get automatically the structure G_B, usually denoted $G_A \otimes_A B$, of a group scheme over B on G. If, however, B is a subring of A then one needs to work to construct a structure of a group scheme over B on G_A.

(2.5) For a group scheme G_A over a ring A, any one of "simple", "semi-simple", or "reductive" is used in the sense of [SGA3]; that is, G_A is assumed to be smooth with connected reductive fibers.

(2.6) For a semi-simple group defined over a field k we use $G^+(k)$ to denote the normal subgroup of $G(k)$ generated by $U(k)$ where U is a maximal unipotent k-subgroup of G contained in a Borel k_s-subgroup of G. For a semi-simple algebraic group G over $\overline{\mathbf{F}}_p$ and an endomorphism σ of $G(\overline{\mathbf{F}}_p)$ we denote by $G_\sigma(\mathbf{F}_q)$ the group of fixed points of G under σ; if $G_\sigma(\mathbf{F}_q) = G_k(k)$ for some structure of an algebraic k-group on G, then we assume $\mathbf{F}_q = k$; if $G_\sigma(\mathbf{F}_q)$ is a finite group of Suzuki or Ree type then $\mathbf{F}_q$ is the smallest field k such that $G_\sigma(\mathbf{F}_q) \subseteq G_k(k)$ for some k-structure G_k on G.

(2.7) All associative rings we consider are assumed to have an identity element. For a ring A and $b \in A$ such that b is not a zero divisor, we use A_b to denote the localization of A at b. However $\mathbf{Q}_p$ and $\mathbf{Z}_p$ denote, as usual, the field

of p-adic numbers and the ring of p-adic integers. We use $\hat{A}$ to denote the profinite completion $\varprojlim_{|A/I|<\infty}(A/I)$ of A; here I runs through the set of cofinite ideals of A.

(2.8) If G is an algebraic group (or group scheme) we use $\mathrm{Lie}\, G$ to denote the Lie algebra of G. The adjoint action of G on $\mathrm{Lie}\, G$ is denoted Ad. For a subset S of $G(k)$, $\mathbf{Z}[\mathrm{tr}\,\mathrm{Ad}\, S]$ denotes the subring of k generated by 1 and the traces of $\mathrm{Ad}\, s$, $s \in S$.

(2.9) For a finitely generated A-module M we use $\mathrm{End}(M)$ (resp. $\mathrm{GL}(M)$) to denote both the algebra (resp. the group) of (invertible) A-endomorphisms of M and the representable functors they define.

(2.10) $\mathrm{Mat}_n(\cdot)$, $\mathrm{GL}_n(\cdot)$, $\mathrm{SL}_n(\cdot)$, SO_n, and Spin_n are used, as usual, to denote the ring of all $(n \times n)$-matrices, the group of invertible $(n \times n)$-matrices, the group of $(n \times n)$-matrices of determinant one, the group of orthogonal $(n \times n)$-matrices of determinant one and the spinor group of a non-singular quadratic n-space. $\mathrm{SO}(n, 1)$ denotes the real special orthogonal group of quadratic form $-x_0^2 + \Sigma_{1 \le i \le n} x_i^2$.

(2.11) $\mathbf{Z}$, $\mathbf{N}$, $\mathbf{N}^+$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}_p$, $\mathbf{Z}_p$, $\mathbf{Z}/n$ all have the usual meaning: integers, natural numbers (0 included), positive natural numbers, rationals, reals, complex numbers, p-adic numbers, p-adic integers, integers modulo n.

(2.12) The symbol ":= " is used as follows: "$A :=\ B$" means that value B is assigned to symbol A; in other words it is a substitute for "define A to be B".

$|A|$ denotes the cardinality of a set A.

3. Algebraicity of certain finite linear groups

Let k be a field of characteristic $l \neq 0$. The result of this section is:

(3.1) THEOREM. *There exist positive integers m and r depending only on d (and not on k) such that if H is a finite subgroup of $\mathrm{GL}_d(k)$, $d \in \mathbf{N}^+$, which satisfies:*

$$(\mathscr{D}^4 H^{\langle m \rangle})^{\langle r \rangle} \text{ is absolutely irreducible,}$$

then $(\mathscr{D}^4 H^{\langle d! \rangle}) \cdot C(H)/C(H)$ is the socle of $H/C(H)$ and is isomorphic to a direct product of finite simple groups of Lie type and of characteristic l.

(3.2) *Amplification.* (i) For m in the theorem one can take $(d!) \cdot b \cdot c$ where c is the least common multiple of the exponents of the automorphism groups of the sporadic simple groups, and b is the least common multiple of the numbers $p^{2d}|\mathrm{Sp}_{2d}(\mathbf{F}_p)|$ when p runs over the primes $\le 2^d$.

(ii) For r one can take the product $e \cdot ((5d)!) \cdot g$ where e is the least common multiple of the orders of non-sporadic finite simple groups having sporadic central extensions (see (3.2.1)) and g is the least common multiple of the orders of finite simple groups of Lie type having absolute rank $\leq d + 2$ over the finite fields $\mathbf{F}_q$ of cardinality $q \leq 2^{d+1} + 1$.

Remark. The estimates for m and r can be significantly lowered for groups H with trivial center: the numbers b and e can be taken then to be 1. Other estimates are also far from the best.

During the proof of the theorem we shall assume (as we may) that k is algebraically closed. Thus "irreducible" = "absolutely irreducible". We consider $V := k^d$ as an H-module. At several points, our proof uses estimates on the size of different groups. These estimates are based on the following:

(3.3) LEMMA. *Let D be a finite commutative subgroup of $\mathrm{GL}_d(k)$ with $l \nmid |D|$. Then*

(i) *D is a product of $\leq d$ cyclic groups;*

(ii) *For any cyclic subgroup $L \simeq \mathbf{Z}/n$ of $N_{\mathrm{GL}_d(k)}(D)/Z_{\mathrm{GL}_d(k)}(D)$, the integer $n \leq 2^d$.*

Proof. Since $l \nmid |D|$, the group D is diagonalizable. Thus $D \subseteq (k^*)^d$. Since any finite subgroup of k^* is cyclic, it follows that a finite subgroup of $(k^*)^d$ is a product of $\leq d$ cyclic subgroups, whence (i).

Let $V = \oplus V_i$ be the decomposition of V into weight subspaces for D. The group $N_{\mathrm{GL}_d(k)}(D)/Z_{\mathrm{GL}_d(k)}(D)$ is isomorphic to a group of permutations of the V_i. Thus it is a subgroup of Sym_d whence our claim.

Now we can start our proof of the theorem.

(3.4) LEMMA. *Let R be a normal subgroup of H. If $H^{\langle d! \rangle}$ is irreducible then V is isomorphic as an R-module to a multiple of a simple R-module.*

Proof. By Clifford's theorem [G1, Theorem 3.1.1], V is a direct sum of isotypic components, $V = \oplus_{1 \leq i \leq n} V_i$, with each V_i a multiple of a non-trivial simple R-module and V_i and V_j having no isomorphic R-modules in common if $i \neq j$ (i.e., $\mathrm{Hom}_R(V_i, V_j) = 0$ if $i \neq j$). The action of H on V permutes the V_i, $1 \leq i \leq n$, and therefore defines a homomorphism $f\colon H \to \mathrm{Sym}_n$. Since $\dim V = d$ and $\dim V_i \geq 1$ we have $n \leq d$. Therefore $f(H^{\langle d! \rangle}) = \{1\} \subset \mathrm{Sym}_n$, i.e., $H^{\langle d! \rangle}$ preserves each V_i, $1 \leq i \leq n$. Since $H^{\langle d! \rangle}$ is irreducible we must have $n = 1$, as claimed.

(3.5) COROLLARY. *If $H^{\langle d! \rangle}$ is irreducible then every commutative normal subgroup of H is central and cyclic.*

Proof. Let $C \lhd H$ be commutative. Then any simple C-module is one-dimensional, and therefore, by (3.4), $C \subset k \cdot \mathrm{Id}_V$. Thus C is central and, as a subgroup of the multiplicative group k^* of the field k, it is cyclic as well.

Remark. If h has no center then (3.5) implies that H has no radical either. This permits one, under the assumption $C(H) = \{1\}$, to bypass Proposition (3.6) below and get a better expression for m.

(3.6) PROPOSITION. *If $H^{\langle b \cdot d! \rangle}$ is irreducible then the radical of H is equal to the center $C(H)$ of H. In particular, $H/C(H)$ is semi-simple.*

Proof. Assume that H has non-central radical. Let C be the center of H, and let $\bar{S}$ be the radical of Socle (H/C). We have $\bar{S} \neq \{1\}$ since the radical is non-central. By the definition of the socle, $\bar{S}$ is a product of elementary commutative subgroups, $\bar{S} \simeq \prod(\mathbf{Z}/q)^{t_q}$, where the q are different primes and $t_q \in \mathbf{N}$. Let S be the preimage of $\bar{S}$ in H. Since $[S, S] \subseteq C$, the group S is nilpotent. Let $S = \prod S_q$ be its decomposition into the product of its Sylow subgroups (see [G1, Theorem 2.3.5]). Since the only irreducible representation of an l-group in characteristic l is the trivial one (see [G1, Theorem 3.1.2]), it follows from (3.3) that $S_l = \{1\}$. Suppose that $S_q \neq \{1\}$. Write $C_q = C \cap S_q$. Since S_q/C_q is elementary abelian by construction and since C_q is cyclic by (3.5), we have in view of [G1, Lemma 5.6.1(v)] that $[S_q, S_q] \subset \tilde{C}_q$ where $\tilde{C}_q$ is the (only) subgroup of C_q of order q. (Indeed, in notation of this lemma, we have $P_1 := S_q$, $P_2 \subset C_q$, $P_3 = \{1\}$. Since $x^q \in C_q$ for $x \in S_q$, $[x, y]^q \equiv [x^q, y] \equiv 1 \bmod P_3$ by [G1, Lemma 5.6.1(v)]. Since $P_3 = \{1\}$ this gives $[x, y]^q = 1$ for $x, y \in S_q$ as claimed.) Then by [G1, Lemma 5.6.1(i)–(v)] the commutator map $(x, y) \mapsto [x, y]$ factors through to give a skew-symmetric (with zero diagonal if $q = 2$) bilinear form F_q on $\bar{S}_q = S_q/C_q$ with values in $\tilde{C}_q \simeq \mathbf{F}_q$. Let S_q' be the preimage in S_q of the kernel $\{s \in \bar{S}_q | F_q(\bar{S}_q, s) = 0\}$ of F_q. Since S, S_q, C_q, and $\tilde{C}_q$ are all characteristic subgroups of h, it follows that S_q' is one as well. In particular, S_q' is a commutative normal subgroup of H. By (3.5) $S_q' = C_q$, and therefore F_q is a non-degenerate form. In particular, t_q is even, $t_q = 2s_q$. Let $\bar{M}$ be a maximal totally isotropic (i.e., $F_q(\bar{M}, \bar{M}) = \{0\}$) subspace of $\bar{S}_q$. Then the preimage M of $\bar{M}$ in S_q is commutative. Since $\bar{M} = M/C_q$ is a product of s_q cyclic groups $\mathbf{Z}/q$ and since an image in $\bar{M}$ of a cyclic subgroup of M is cyclic, we get that M is a product of at least s_q cyclic subgroups. Therefore, by (3.3(i)), $s_q \leq d$. Since F_q is non-degenerate we have $Z_{S_q}(M) = M$. Therefore $N_{S_q}(M)/Z_{S_q}(M) \supset \mathbf{Z}/q$, whence by (3.3(ii)), $q \leq 2^d$.

Since S_q is a characteristic subgroup of h and since C_q is central in H, the action of H by conjugation defines a homomorphism φ_q from H into the group A_q of the automorphisms of S_q trivial on C_q. This latter group contains $\bar{S}_q$ as a

normal subgroup, and we have that $A_q/\bar{S}_q$ is a subgroup of $\mathrm{Sp}_{2s_q}(\mathbf{F}_q)$. As $s_q \leq d$ and $q \leq 2^d$ we see from the definition of b that $\varphi_q(H^{\langle b\rangle}) = \{1\}$ for all q. Thus $H^{\langle b\rangle} \subseteq Z_H(S)$. Since $H^{\langle b\rangle}$ is irreducible and $S \subseteq Z_{\mathrm{GL}_d(k)}(H^{\langle b\rangle})$, it follows that S is commutative in contradiction to the assumptions.

Remark. One can obtain much better estimates if one uses the representation theory of extra-special (= Heisenberg) groups. One gets then that $\prod_q q^{s_q} \leq d$ (see [G1, Theorem 5.5.5]).

We assume from now till the end of this section that $\bar{H} := H/C$ is semi-simple. The conditions which guarantee this will always be included in the statements.

Let $\bar{N}$ be the socle (the product of minimal normal subgroups) of $\bar{H}$. Since $\bar{H}$ is semi-simple $\bar{N}$ is uniquely a (finite) direct product $\bar{N} = \prod_{1\leq i\leq t}\bar{N}_i$ of simple non-commutative groups. The action by conjugation of H on the preimage N of $\bar{N}$ induces a homomorphism φ: $H \to \mathrm{Aut}\,\bar{N}$ with $\mathrm{Ker}\,\varphi = C$.

(3.7) LEMMA. *If $H^{\langle b\cdot d!\rangle}$ is irreducible then $\varphi(H^{\langle d!\rangle}) \subseteq \prod_{1\leq i\leq t}\mathrm{Aut}\,\bar{N}_i$.*

Proof. Let N and the N_i, $i = 1,\ldots,t$, be the commutator groups of the preimages in H of $\bar{N}$ and the $\bar{N}_i$ respectively. By (3.4) the N-module V is a multiple of a simple N-module, say W. Then, being an irreducible representation of the central product N of the groups N_i, W decomposes (see [G1, Theorems 3.7.1, 3.7.2 and subsequent remarks]) into a tensor product $W = \otimes_{1\leq i\leq t}W_i$ of simple N_i-modules W_i. Since the groups N_i are not commutative and since their representations on the W_i are faithful (since they are on V), we have $\dim W_i \geq 2$. Therefore $2^t \leq \dim W \leq \dim V = d$. Thus $t \leq \log_2 d \leq d$. Since the decomposition of a finite group into a direct product of noncommutative simple ones is unique (if it exists) (see [Su 1, Corollary to Theorem 2.4.8]), the action of H by conjugation on the set of the $\bar{N}_i$, $i \leq 1 \leq t$, gives rise to a homomorphism π: $H \to \mathrm{Sym}_t$. Since $t \leq d$, we have $\pi(H^{\langle d!\rangle}) \subseteq (\mathrm{Sym}_t)^{\langle d!\rangle} = \{1\}$ whence our claim.

(3.8) COROLLARY. *If $\mathscr{D}^4H^{\langle b\cdot c\cdot d!\rangle}$ is irreducible then $\mathscr{D}^4\bar{H}^{\langle d!\rangle}$ is a direct product of non-sporadic finite simple groups.*

Proof. Let φ and the $\bar{N}_i$ be as in (3.7). Then $\varphi(\mathscr{D}^4\bar{H}^{\langle c\cdot d!\rangle}) = \mathscr{D}^4\varphi(\bar{H})^{\langle c\cdot d!\rangle} \subseteq \prod\mathscr{D}^4((\mathrm{Aut}\,\bar{N}_i)^{\langle c\rangle})$ (by (3.7)). Now $(\mathrm{Aut}\,\bar{N}_i)^{\langle c\rangle} = \{1\}$ if $\bar{N}_i$ is sporadic (by the choice of c). Next $\mathscr{D}(\mathrm{Aut}(\mathrm{Alt}_n)) = \mathrm{Alt}_n$ for $n \geq 3$ (since by [Su 1, (2.19)] we have $[\mathrm{Aut}\,\mathrm{Alt}_n\colon \mathrm{Alt}_n] \leq 4$ and since groups of order ≤ 4 are commutative). Further, for a simple group $X(\mathbf{F}_q)$ of Lie type, the group $\mathrm{Out}\,X(\mathbf{F}_q) := \mathrm{Aut}\,X(\mathbf{F}_q)/\mathrm{Int}\,X(\mathbf{F}_q)$ is (see [S1, Theorems 30 and 36]) an extension of the group $\mathrm{Gal}(\mathbf{F}_q)$ of "field automorphisms", which is commutative in the case of

finite fields, by the group of algebraic automorphisms which in turn is an extension of the group of "graph automorphisms", which can be $\{1\}$, or $\mathbf{Z}/2$, or (only for type D_4)Sym_3, by the group of "diagonal automorphisms" which is always commutative. Thus $\mathscr{D}^4\overline{H}^{\langle b\cdot c\cdot d!\rangle}$ is a product of non-sporadic finite simple groups, $\mathscr{D}^4\overline{H}^{\langle b\cdot c\cdot d!\rangle} = \prod_{i\in I}\overline{N}_i$ where $I \supset \{1,\dots,t\}$. If $j \notin I$, $1 \le j \le t$, then N_j centralizes $\prod_{i\in I}N_i$ and, therefore, $\mathscr{D}^4H^{\langle b\cdot c\cdot d!\rangle}$ is not irreducible. This contradicts our assumptions whence all the $\overline{N}_i$ are non-sporadic. Now our claim follows from (3.7) and the remark that $\mathscr{D}^4(\mathrm{Aut}\,\overline{N}_i) \simeq \overline{N}_i$ for non-sporadic simple groups.

(3.9) To complete the proof of Theorem (3.1) we pick an elementary abelian p-subgroup D in a simple group Q under consideration. We try to embed a central extension $\tilde{Q}$ of Q in $\mathrm{GL}_d(k)$. If $p \neq l$ and the central extension splits over D, then the inclusions of D in $\mathrm{GL}_d(k)$ and of $N_Q(D)/Z_G(D)$ in $N_{\mathrm{GL}_d(k)}(D)/Z_{\mathrm{GL}_d(k)}(D)$ permit us to use the estimates (3.3). This leads to a conclusion that, for a finite number of exceptions which do not depend on l, only groups of Lie type and of characteristic l can appear as groups $\overline{N}_i$. The finite number mentioned above is then eliminated by raising everything to an appropriate power r.

(3.9.1) As a first precaution we kill off the Alt_n for $n = 6, 7$ and the groups of Lie type which can have non-algebraic central extensions (see [Gr1], [S2, Theorem 1.1 and the next to last paragraph of the introduction], and [D]). They are finite in number. Therefore we can take the least common multiple of their orders and denote it by e.

(3.9.2) Assume $\overline{N}_i$ is isomorphic to Alt_h for some $h \ge 5$, $h \neq 6, 7$. If $l \neq 3$ (resp. $l \neq 5$) take $D = \langle (1,2,3),(4,5,6),\dots\rangle \subset \mathrm{Alt}_h$ (resp. $D = \langle (1,2,3,4,5), (6,7,8,9,10),\dots\rangle \subset \mathrm{Alt}_h$). We have $D \simeq (\mathbf{Z}/3)^{[h/3]}$ (resp. $D \simeq (\mathbf{Z}/5)^{[h/5]}$). Since the Schur multiplier of Alt_h is 2 for $h \ge 5$, $h \neq 6, 7$, the preimage of D in N_i splits over D so that we can consider D as a subgroup of H. Therefore by (3.3(i)) we have in both cases $h \le 5d + 4$.

(3.9.3) If $\overline{N}_i$ is isomorphic to a finite simple group of Lie type, we can assume (since we have taken care of exceptions in (3.9.1)) that N_i is a central quotient of $X(\mathbf{F}_q)$ where X is either a simply connected absolutely almost simple algebraic group defined over $\mathbf{F}_q$ or a Suzuki or Ree group of types ${}^2B_2$, ${}^2G_2$, ${}^2F_4$.

Let $q = p^s$ and let U be a Sylow p-subgroup of N_i (i.e., points of a maximal unipotent subgroup of X defined over $\mathbf{F}_q$ in the case of algebraic group X). Let D be the center of U and assume that $p \neq l$. Then D is diagonalizable. The action of the Borel subgroup $N_{N_i}(U)$ on D factors through a one-dimensional split torus and defines, therefore, a homomorphism $\mathbf{F}_q^* \to N_{N_i}(D)/Z_{N_i}(D)$ whose

kernel is of order at most two. Therefore by (3.3(ii)), $q - 1/2 \leq 2^d$, or $q \leq 2^{d+1} + 1$.

(3.9.4) It remains to bound off the ranks of the prospective candidates for an N_i. Note first that $\mathrm{SL}_n(\mathbf{F}_q)$ contains a vector group L which is the unipotent radical of the stabilizer of a point in the natural representation. We have $L \simeq (\mathbf{Z}/p)^{(n-1)s}$. By (3.3(i)), we have (under the assumption $p \neq l$) that $(n-1)s \leq d$. Note next that any group of Lie type and of absolute rank $u \geq 4$ contains a subgroup A_n with $n \geq [(u-2)/2]$. Thus by the preceding remarks $(u-2)/2 \leq n+1 \leq d+2$.

(3.9.5) We can now conclude the proof of Theorem (3.1). By (3.8), $\mathscr{D}^4\overline{H}^{\langle d! \rangle}$ is a direct product of non-sporadic finite simple groups. In view of (3.9.1), (3.9.2), (3.9.3), and (3.9.4), $(\mathscr{D}^4\overline{H}^{\langle d! \rangle})^{\langle e \cdot (5d)! \cdot g \rangle}$ must consist of only groups of Lie type and of characteristic l. Since $(\mathscr{D}^4 H^{\langle d! \rangle})^{\langle m \rangle}$, $m = e \cdot (5d)! \cdot g$, is irreducible by assumption, we must have by the same argument as in the conclusion of our proof of (3.8) that $\mathscr{D}^4 H^{\langle d! \rangle}$ is a product of simple groups of Lie type and of characteristic l.

4. Algebraicity of certain homomorphisms between finite groups of Lie type

Let p be a fixed prime, k a field of characteristic p, G an absolutely almost simple simply connected algebraic group defined over k, $m_i \in \mathbf{N}^+$ for $1 \leq i \leq t$, $q_i := p^{m_i}$, the H_i absolutely almost simple simply connected algebraic groups defined over $\mathbf{F}_{q_i}$, $H_{i,\sigma_i}(\mathbf{F}_{q_i})$ universal (see [S1]) groups of Lie type (where σ_i is the twisting automorphism of $H_i(\overline{\mathbf{F}}_p)$), f: $\prod_{1 \leq i \leq t} H_{i,\sigma_i}(\mathbf{F}_{q_i}) \to G(k)$ a group homomorphism with central kernel.

If $p = 2$ and $n \in \mathbf{N}$, there exists $e = e(n) \in \mathbf{N}$ such that if $m \geq e$ and D is a 2′-complement in the normalizer of a Sylow 2-subgroup of $H(\mathbf{F}_q)$ (with $q = 2^m$), a universal group of Lie type, where H is an absolutely almost simple simply connected algebraic group over $\overline{\mathbf{F}}_q$ of rank $\leq n$, then $T := Z_H(D)$ is a maximal torus of H and D distinguishes the roots of T in Lie H. Indeed since the number of possible groups H of rank $\leq n$ and of possible types of σ is finite, we can assume that H and the type of σ are fixed. Then existence of e follows from the fact that the union in T of groups D over infinitely many m is dense in T. See also (5.5) below.

(4.1) THEOREM. *Let g: $G \to \mathrm{GL}_d$ be a rational absolutely irreducible k-representation of G. Assume*

(i) *g cannot be represented as a non-trivial tensor product of irreducible representations of G;*

(ii) $g \circ f(\prod_{1 \le i \le t} H_{i,\sigma_i}(\mathbf{F}_{q_i}))$ *is absolutely irreducible.*

(iii) *Every* $(\mathrm{Ad} \circ g \circ f)$ $(\prod_{1 \le i \le t} H_{i,\sigma_i}(\mathbf{F}_{q_i}))$*-submodule of* Mat_d *over* $\bar{k}$ *is* $(\mathrm{Ad} \circ g)(G)$*-invariant*).

(iv) *If* $p = 3$ *then* G *is not of type* G_2 *and if* $p = 2$ *then* $m_i \ge e(1 + \mathrm{rank}\, G)$, $1 \le i \le t$, *and* G *is not of type* $B_n (n \ge 1)$, $C_n (n \ge 1)$, *or* F_4.

Then $t = 1$, G *is defined over* $\mathbf{F}_{q_1}$, *and there exist a rational* $\mathbf{F}_q$*-isomorphism* $\tilde{f}\colon H_1 \to G$ *and an integer* n *such that* $(\tilde{f} \circ \mathrm{Fr}^n)(a) = f(a)$ *for* $a \in H_{1,\sigma_1}(\mathbf{F}_{q_1})$.

Here Ad denotes the action of GL_d on Mat_d by conjugation: $(\mathrm{Ad}\, a)(x) = a \times a^{-1}$ for $a \in \mathrm{GL}_d$, $x \in \mathrm{Mat}_d$; and Fr denotes the Frobenius endomorphism.

(4.2) We assume (as we may) in the proof of the theorem that k is algebraically closed. Since $g \circ f\colon \prod H_{i,\sigma_i}(\mathbf{F}_{q_i}) \to \mathrm{GL}_d$ is irreducible, it can be decomposed (see [G1, Theorems 3.7.1 and 3.7.2]) into a tensor product $g \circ f = \otimes_{1 \le i \le t} h_i$ where the $h_i\colon H_{i,\sigma_i}(\mathbf{F}_{q_i}) \to \mathrm{GL}_{d_i}$, $i = 1, \ldots, t$, are irreducible representations of the $H_{i,\sigma_i}(\mathbf{F}_{q_i})$, and $d = \prod_{1 \le i \le t} d_i$. By [S1, Theorem 43] the h_i are restrictions of rational representations $\tilde{h}_i\colon H_i \to \mathrm{GL}_{d_i}$. Set $\tilde{h} = \otimes_{1 \le i \le t} \tilde{h}_i$.

(4.3) Lemma. $t = 1$.

Proof. Assume $t \ge 2$. Then $[\tilde{h}_1(H_1), \tilde{h}_2(H_2)] = \{1\}$. In particular, $(\mathrm{Ad} \circ h_1)(H_1)$ acts trivially on $L_2 := \mathrm{Lie}\, \tilde{h}_2(H_2) \subset \mathrm{Mat}_d$. Since L_2 is $\prod_{1 \le i \le t} H_i$-invariant, it follows from assumption (4.1) (iii) that L_2 is $(\mathrm{Ad} \circ g)$ (G)-invariant. The group $K := \{a \in G \mid \mathrm{Ad} \circ g(a)(l) = l \text{ for all } l \in L_2\}$ is a normal subgroup of G. Since G is almost simple and since $f(H_{1,\sigma_1}(\mathbf{F}_{q_1})) \subset K$, it follows that $K = G$. Thus G acts trivially on L_2. Hence $\tilde{h}_2(H_{2,\sigma_2}(\mathbf{F}_{q_2}))$ acts trivially on $L_2 = \mathrm{Lie}\, \tilde{h}_2(H_2)$. This is impossible. Therefore $t = 1$.

(4.4) Since $t = 1$, we may (and shall) drop subscripts of $H, q, H_\sigma(\mathbf{F}_q), h, f, \tilde{h}$, etc. Set $\tilde{H} := \tilde{h}(H)$, $\tilde{L} := \mathrm{Lie}\, \tilde{H}$, $N := N_{\mathrm{GL}_d}(\tilde{L})$, and $Z := Z_{\mathrm{GL}_d}(\tilde{L})$. Clearly, Z is normal in N, and we have a natural monomorphism of algebraic groups $N/Z \to \mathrm{Aut}\, \tilde{L}$. Since $\tilde{h}$ extends $g \circ f\colon H_\sigma(\mathbf{F}_q) \to \mathrm{GL}_d$, it follows from (4.1) (iii) that $\tilde{L}$ is $g(G)$-invariant, i.e. $g(G) \subset N$. Let π denote the composition $N \to N/Z \to \mathrm{Aut}\, \tilde{L}$. Let $M := \pi(N) \subset \mathrm{Aut}\, \tilde{L}$, $\bar{h} := \pi \circ \tilde{h}$, $\bar{g} := \pi \circ g$, $\bar{H} := \bar{h}(H)$, and $\bar{G} := \bar{g}(G)$.

(4.5) Lemma. $\bar{G}$ *and* $\bar{H}$ *are absolutely simple* (*adjoint*) *subgroups of* M *such that*

(i) $\bar{G}^+(k) \cap \bar{H} \supset \bar{H}^+_\sigma(\mathbf{F}_q)$;

(ii) *Any* $\mathrm{Ad}\, \bar{H}^+_\sigma(\mathbf{F}_q)$*-invariant subspace of* $\mathrm{Lie}\, M$ *is* $\mathrm{Ad}\, \bar{G}$*-invariant*;

(iii) *If* $p = 2$, $q = 2^m$, *then* $m \ge e(1 + \mathrm{rank}\, G)$.

Proof. Since $\bar{H}^+_\sigma(\mathbf{F}_q) = H_\sigma(\mathbf{F}_q)/(\text{center})$, (i) follows from the assumption that $f(H_\sigma(\mathbf{F}_q)) \subseteq G$ and from the fact that the image of $G(k)$ in $\bar{G}$ is contained

in $\overline{G}^+(k)$ (see [BT3, Corollary 6.5]). To prove (ii), take an $\mathrm{Ad}\,\overline{H}^+_\sigma(\mathbf{F}_q)$-invariant subspace P of $\mathrm{Lie}\,M$ and pull it back to an $\mathrm{Ad}\,H_\sigma(\mathbf{F}_q)$-invariant subspace $\tilde{P}$ of $\mathrm{Lie}\,N \subset \mathrm{Mat}_d$. Then it is $\mathrm{Ad}\,G$-invariant by (4.1) (iii), whence (ii); (iii) is a repetition of (4.1) (iv).

(4.6) LEMMA. *Let $\overline{H}$ be an absolutely simple algebraic group as above.*

(i) *The irreducible $\mathrm{Ad}\,\overline{H}$-subquotients of $\mathrm{Lie}\,\overline{H}$ are also $\mathrm{Ad}\,\overline{H}^+_\sigma(\mathbf{F}_q)$-irreducible.*

(ii) *$\mathrm{Lie}\,\overline{H}$ is irreducible under $\mathrm{Ad}\,\overline{H}$ unless $\overline{H}$ is of type $A_{np-1}(n \geq 1)$, or $p = 3$ and $\overline{H}$ is of type G_2 or E_6, or $p = 2$ and $\overline{H}$ is of type $B_n(n \geq 1)$, $C_n(n \geq 1)$, $D_n(n \geq 1, n \neq 2)$, E_7, or F_4.*

(iii) *If $\overline{H}$ is of type A_{np-1} ($A_1 = B_1 = C_1$), or $p = 3$ and $\overline{H}$ is of type E_6, or $p = 2$ and $\overline{H}$ is of type D_n ($n \geq 3$) or E_7 then the derived algebra of $\mathrm{Lie}\,\overline{H}$ is the only $\mathrm{Ad}\,\overline{H}$-composition factor of $\mathrm{Lie}\,\overline{H}$ which is a non-trivial $\mathrm{Ad}\,\overline{H}$-module.*

(iv) *If $p = 3$ (resp. 2) and $\overline{H}$ is of type G_2 (resp. F_4), then $\mathrm{Lie}\,\overline{H}$ has exactly two non-zero $\mathrm{Ad}\,\overline{H}$-composition quotients; both of them are Lie algebras of type A_2 (resp. D_4).*

(v) *If $p = 2$ and $\overline{H}$ is of type C_n ($n \geq 2$) or B_n ($n \geq 2$), then $\mathrm{Lie}\,\overline{H}$ has exactly two non-trivial composition factors and one one-dimensional one; the non-trivial factors come from subgroups of type $A_1 + \cdots + A_1$ (n times) and D_n which are normalized by a maximal torus.*

Proof. Statements (ii)–(iv) are essentially well-known (and are contained in the table on pp. 124, 125 of [H]). Now (i) is a corollary of [S1, Theorem 43]; in bad cases listed in (4.6) (iv) and (v), one must also point out that a twist by Frobenius or by a non-central isogeny of an irreducible $\mathrm{Ad}\,\overline{H}$- or $\mathrm{Ad}\,\overline{H}^+_\sigma(\mathbf{F}_q)$-module is again irreducible.

(4.7) LEMMA. *Let $\tilde{H}$ be an absolutely almost simple algebraic group, $\tilde{L} = \mathrm{Lie}\,\tilde{H}$, and $\overline{H}$ the adjoint group of $\tilde{H}$.*

(i) *$\mathscr{D}(\mathrm{Aut}\,\tilde{L})^0 = \mathrm{Ad}\,\overline{H}$ unless $p = 2$ and $\tilde{H}$ is of type G_2, or is isomorphic to an orthogonal group SO_n, $n \geq 3$, $n \neq 4$, or is isomorphic to Sp_{2n}, $n \geq 1$.*

(ii) *If $p = 2$ and $\tilde{H}$ is of type G_2 (resp. isomorphic to SO_{2n} ($n \geq 3$)), then $\mathscr{D}(\mathrm{Aut}\,\tilde{L})^0$ is of type C_3 (resp. C_n).*

(iii) *If $p = 2$ and $\tilde{H}$ is isomorphic to Sp_{2n} ($n \geq 1$) or SO_{2n+1} ($n \geq 1$), then $\mathscr{D}(\mathrm{Aut}\,L)^0 = \mathbf{G}_a^{2n} \rtimes (\mathrm{Ad}\,\overline{H})$ and $\mathrm{Ad}\,\overline{H}$ acts irreducibly on (the $2n$-dimensional vector space) $\mathbf{G}_a^{2n}$.*

Proof. These statements are a summary of (a part) of the table on p. 98 of [H].

(4.8) PROPOSITION. *Assume that* (4.5) (i), (ii), *and* (iii) *hold.*

(i) *If conditions of* (4.7) (ii) *do not hold then* $M = \overline{G} = \overline{H}$.

(ii) *In any case* $\overline{G} \supseteq \overline{H}$; *if* $\overline{G} \neq \overline{H}$ *then* G *is of type* C_n *for some* $n \geq 3$ *and* $M = \overline{G}$.

Proof. The proof is rather involved because of many possibilities for $\operatorname{Aut} \tilde{L}$ and $\operatorname{Lie} \overline{H}$.

(4.8.1) *Case:* (4.6) (ii) or (iii) and (4.7) (i) hold.

Since $\mathscr{D}(\operatorname{Aut} \tilde{L}) = \operatorname{Ad} \overline{H}$ (by (4.7) (i)) and $\overline{G}$ is simple we have $\overline{G} \subseteq \overline{H}$. Then $\operatorname{Lie} \overline{G}$ is an $\operatorname{Ad} \overline{H}^+_\sigma(\mathbf{F}_q)$-invariant subspace of $\operatorname{Lie} \overline{H}$. Now $\operatorname{Lie} \overline{H}$ has exactly one $\operatorname{Ad} H$-subquotient which is a nontrivial $\operatorname{Ad} \overline{H}$-module and by [H, table on pp. 124, 125] this submodule is the derived algebra of $\operatorname{Lie} \overline{H}$. Since $\overline{G}$ is simple it must contribute non-trivially to the non-trivial submodule of $\operatorname{Lie} \overline{H}$. Thus $\operatorname{Lie} \overline{G}$ contains the derived algebra $\mathscr{D}(\operatorname{Lie} \overline{H})$ of $\operatorname{Lie} \overline{H}$. An (attentive) glance at the tables on pp. 124, 125 of [H] or at classification tables shows that $\operatorname{Lie} \overline{G} \supset \mathscr{D}(\operatorname{Lie} \overline{H})$ and $\overline{G} \subseteq \overline{H}$ imply that $\overline{G} = \overline{H}$, except in the case when $p = 2$ and H is of type $A_3 = D_3$. In this latter case the commutator of $\operatorname{Lie} \overline{H}$ is the Lie algebra of a subgroup of type G_2 of $\overline{H}$ (see [S3], [H], or [W1, Appendix]). Then $\overline{G} \neq \overline{H}$ and the simplicity of G imply that G is of type G_2. Let D be a 2-complement in the normalizer of a Sylow 2-subgroup of $\overline{H}^+_\sigma(\mathbf{F}_q)$. Then by (4.5) (iii), D is contained in a unique maximal $\mathbf{F}_q$-torus T of $\overline{H}$ and in a unique maximal $\mathbf{F}_q$-torus T_1 of $\overline{G}$. We have $T_1 \subseteq T$ and $T/T_1 \simeq \mathbf{G}_{m,\mathbf{F}_q}$ or $(R_{\mathbf{F}_{q^2}/\mathbf{F}_q}(\mathbf{G}_{m,\mathbf{F}_{q^2}}))/\mathbf{G}_{m,\mathbf{F}_q}$. In both cases $T(\mathbf{F}_q)/T_1(\mathbf{F}_q) \neq \{1\}$ (by (4.5) (iii)). Since $T(\mathbf{F}_q) = D$ (since $p = 2$), the above is a contradiction to the assumption $T(\mathbf{F}_q) \subseteq \overline{G}$ (which is implied by (4.5) (i)).

(4.8.2) *Case:* (4.6) (iv) and (4.7) (i) hold (i.e., $p = 3$ (resp. 2) and H is of type G_2 (resp. F_4)).

If $\operatorname{Lie} \overline{H} = \operatorname{Lie} \overline{G}$ then $\overline{H} = \overline{G}$. If $\operatorname{Lie} \overline{H} \neq \operatorname{Lie} \overline{G}$ then since $\operatorname{Lie} \overline{H}$ has exactly two non-zero $\operatorname{Ad} \overline{H}$-subquotients both of which are of type A_2 (resp. D_4) it follows from (4.6) that $\overline{G}$ is of type A_2 (resp. D_4). Since $p = 3$ (resp. 2) we have $\operatorname{PSL}_3(k) \simeq \operatorname{SL}_3(k)$ (resp. $\operatorname{PSpin}_8(k) \simeq \operatorname{Spin}_8(k)$). Since $\overline{H}^+_\sigma(\mathbf{F}_q) \subset \overline{G}^+(k)$ by (4.5) (i), the assumption that $\overline{G}$ is of type A_2 (resp. D_4) implies that $H_\sigma(\mathbf{F}_q)$ has a (faithful) representation of dimension 3 (resp. 8) which is not the case by [S1, Theorem 43] since H does not have such a representation.

(4.8.3) *Case:* (4.6) (v) and (4.7) (i) hold (i.e. $p = 2$ and $\tilde{H}$ is isomorphic to PSp_{2n} ($n \geq 3$) or to $\operatorname{Spin}_{2n+1}$ ($n \geq 3$)). Since by (4.5) (i) $\operatorname{Ad} \overline{G}$ is $\operatorname{Ad} \overline{H}^+_\sigma(\mathbf{F}_q)$-invariant, it follows from (4.6) (i) and (v) that $\operatorname{Lie} \overline{G}$ projects either on both or on exactly one non-trivial $\operatorname{Ad} \overline{H}$-subquotient of $\operatorname{Lie} \overline{H}$. In the latter case, D, a 2′-complement in the normalizer of a 2-subgroup of $\overline{H}^+_\sigma(\mathbf{F}_q)$, has fewer roots in $\overline{G}$ than in $\overline{H}^+_\sigma(\mathbf{F}_q)$ which is impossible in view of (4.5) (iii).

(4.8.4) *Case:* (4.6) (v) and (4.7) (iii) hold (i.e. $p = 2$ and $\tilde{H}$ is isomorphic to Sp_{2n} ($n \geq 1$) or SO_{2n+1} ($n \geq 1$)). Let $\tilde{U}$ be the unipotent radical of N and V the set of fixed points of $\tilde{U}$ on k^d. Since $\tilde{U}$ is unipotent we have $V \neq 0$. Since $\tilde{H}$ normalizes $\tilde{U}$ it follows that $\tilde{H}V \subseteq V$. Since $\tilde{H}$ is absolutely irreducible we have $V = k^d$ whence $\tilde{U} = \{1\}$. Thus N and, therefore, M are reductive. By (4.7) (iii) we have then that $\mathscr{D}M = \mathrm{Ad}\,\overline{H}$, whence again $\overline{G} \subseteq \overline{H}$. Now the argument is concluded exactly as in (4.8.3).

(4.8.5) *Case:* (4.7) (ii) holds. Let $A = \mathrm{Lie}\,M$ and $I = \mathscr{D}(\mathrm{Lie}\,\overline{H})$. By (4.6) (i) and (v), I is irreducible under $\overline{H}$, $\overline{H}_\sigma(\mathbf{F}_q)$, and, therefore, under $\overline{G}$ as well. If $\mathrm{Lie}\,\overline{G} \cap I = 0$, then $\overline{G}$ must be of type $A_1 + A_1 + \cdots + A_1$ (r times) where $r = 3$ or n if $\overline{H}$ is of type G_2 or D_n. Since $\overline{G}$ is absolutely simple this possibility does not occur and, therefore, $\mathrm{Lie}\,\overline{G} \supset I$. If $\mathrm{Lie}\,\overline{G} \not\subset \mathrm{Lie}\,\overline{H}$ then $\mathrm{Lie}\,\overline{G} \supset I$ implies that either $\mathrm{Lie}\,\overline{G} = A$ (and then $\overline{G} = M$, whence $\overline{H} \subseteq \overline{G}$ as desired) or $\overline{H}$ is of type G_2 and $\overline{G}$ is of type A_3. In this latter case, let D be a $2'$-complement in the normalizer of a Sylow 2-subgroup of $\overline{H}^+_\sigma(\mathbf{F}_q)$. Then D is contained in a unique maximal $\mathbf{F}_q$-subtorus T of $\overline{H}$ and $D = T(\mathbf{F}_q)$. Since the root subspaces of T on $\mathrm{Lie}\,\overline{H}$ are then one-dimensional, $T_1 = Z_{\overline{G}}(D)$ is the maximal torus of $\overline{G}$. The root subgroups of D on $\overline{H}^+_\sigma(\mathbf{F}_q)$ are contained in the root subgroups of T_1 on $\overline{G}$ and since $T \subseteq T_1$ the conjugates of elements of these root subgroups by T are again contained in appropriate root subgroups of T_1 on $\overline{G}$. Thus the root subgroups of T in $\overline{H}$ are exactly the root subgroups of T_1 in $\overline{G}$ whence $\overline{G} = \overline{H}$ (and the case under consideration: $\overline{G}$ of type A_3, $\overline{H}$ of type G_2, is thus impossible).

We are left with the case $\mathrm{Lie}\,\overline{H} \supseteq \mathrm{Lie}\,\overline{G} \supseteq I$. Let D and T be as in the above proof. An inspection of the table on pp. 124, 125 of [H] shows that $T = T_1$ unless $\overline{G}$ is of type G_2 and $\overline{H}$ of type A_3. This latter case can be excluded as in (4.8.1) (or by the present proof after slight notational modifications). So we can assume $T = T_1$. Now the proof we used above (using consideration of root subgroups) works here as well and yields $\overline{G} = \overline{H}$.

(4.9) *Proof of* (4.1) *concluded.* The group N is reductive (it was proved in (4.8.4)). Since $g(G) \subseteq N$ (by (4.1) (iii)), it follows that $g(G) \subseteq \mathscr{D}N$. Write $\mathscr{D}N = \prod_{1 \leq i \leq s} N_i$ where the product is almost direct and the N_i are absolutely almost simple. $\mathscr{D}N$ acts irreducibly on k^d since H (or G) does. Let φ: $\mathscr{D}N \to \mathrm{GL}_d$ be the natural imbedding. We can write $\varphi = \otimes_{1 \leq i \leq s} \varphi_i$ where φ_i is an irreducible representation of N_i, $1 \leq i \leq s$. Let π_i be the projection of N on N_i, $1 \leq i \leq s$. Then $g(a) = \otimes_{1 \leq i \leq s} \varphi_i \circ \pi_i(a)$. By (4.1) (i), it follows that $\varphi_i \circ \pi_i = 1$ for all but one i. Since G is irreducible we have $\pi_i(G) \neq \{1\}$ for $1 \leq i \leq s$. Thus $\varphi_i = 1$ for all but one i whence $\mathscr{D}N$ is absolutely almost simple. Now the projection $\mathscr{D}N \to M$ has only scalars in the kernel. Therefore $\overline{G} \supseteq \overline{H}$

implies that $g(G) \supseteq \tilde{h}(H)$. If $\overline{G} = \overline{H}$ then simple connectedness of H implies existence of $\bar{f}$: $H \to G$ such that $g \circ \bar{f} = \tilde{h}$. If $\overline{G} \supseteq \overline{H}$, $G \neq \overline{H}$, then by (4.8) $\overline{G}$ is of type C_n. Therefore G is of type C_n or B_n, the case excluded by (4.1) (iv). Thus we obtain a rational surjective homomorphism $\bar{f}$: $H \to G$ with $\bar{f}(a) = (g \circ \bar{f})(a) = \tilde{h}(a) = h(a)$ for $a \in H_\sigma(\mathbf{F}_q)$. By (4.1) (iv), $\bar{f} = \tilde{f} \circ \mathrm{Fr}^n$ where $\tilde{f}$ is a central isogeny and, since G is simply connected, $\tilde{f}$ is an isomorphism. Thus $\tilde{f}$ gives G the structure of an $\mathbf{F}_q$-group for which $\tilde{f}$ is an $\mathbf{F}_q$-isomorphism. (Another way to see $\mathbf{F}_q$-structure on G is to observe that $\overline{G} = (\mathrm{Aut}\,\tilde{L})^0$, whence $\mathbf{F}_q$-structure on $\tilde{L}$ yields $\mathbf{F}_q$-structure on $\overline{G}$ and then to use [BT2, (2.24) (ii)]).

5. Remarks on semi-simple group schemes over finite local rings

Let A be a finite local ring with identity R its radical, $k = A/R$, $k \simeq \mathbf{F}_q$, $q = p^m$, p a prime.

Let G be a connected and simply connected absolutely almost simple group scheme over A (see [SGA3, § XIX.2]). Recall (see [B3, (16.6)]) that G_k is quasi-split. Every Galois extension k' of k lifts to a unique Galois extension A' of A (by [Mc, § XV]) and we have that $\mathrm{Gal}(A'/A)$ is canonically isomorphic to $G(k'/k)$. Since G_k is quasi-split, it is determined (see [SGA3, XXIV.3.11]) by a homomorphism r: $\mathrm{Gal}(k'/k) \to \mathrm{Aut}\,\mathrm{Dyn}\,G$ where k' is a splitting field of G and $\mathrm{Dyn}\,G$ is the Dynkin diagram of G. Lift k' to A' as above and define a quasi-split form G'_A of G_A using the same homomorphism r: $\mathrm{Gal}(A'/A)(\simeq \mathrm{Gal}(k'/k)) \to \mathrm{Aut}\,\mathrm{Dyn}\,G$. Now [SGA3, XXIV.1.12 or XXIV.1.21] implies that G'_A and G_A are isomorphic (since they have the same reductions). Thus we have:

(5.1) Lemma. *G is quasi-split over A.*

Denote by f_i, $i \geq 1$, the reduction mod R^i maps f_i: $A \to A/R^i$, f_i: $G_A \to G_{A/R^i}$, and f_i: $G(A) \to G(A/R^i)$. We write f for f_1. Set $G(R^i) := \mathrm{Ker}(f_i\colon G(A) \to G(A/R^i))$.

(5.2) Lemma. (i) *The $G(k)$-module $G(R^i)/G(R^{i+1})$ is isomorphic for $i > 0$ to $L(k) \otimes R^i/R^{i+1}$ where $G(k)$ acts trivially on the second factor and acts on the first factor via* Ad.

(ii) *The map $(x, y) \to [x, y]$ maps $G(R^i) \times G(R^j)$ into $G(R^{i+j})$ and the induced map of $G(R^i/R^{i+1}) \times G(R^j/R^{j+1})$ into $G(R^{i+j}/R^{i+j+1})$ is given by $[(l_1 \otimes r_1), (l_2 \otimes r_2)] = [l_1, l_2] \otimes r_1 r_2$ where $l_1, l_2 \in L(k)$, $r_1 \in R^i/R^{i+1}$, $r_2 \in R^j/R^{j+1}$ and we identify $G(R^s/R^{s+1})$ with $L(k) \otimes R^s/R^{s+1}$;*

(iii) *If $[L(k), L(k)] = L(k)$ then $[G(R), G(R)] = G(R^2)$.*

Proof. This is well-known (for general smooth group schemes as well). We can assume that $R^{i+1} = 0$. Then L is a free A-module with, therefore, $L(R^i) \simeq$

$L(k) \otimes R^i$. The "exponential map" $l \mapsto l + 1$ identifies $L(R^i)$ with $G(R^i)$. The claim (i) follows since everything we did commutes with the action of $G(k)$.

To prove (ii), notice that for a split G it follows from Chevalley commutation relations. For quasi-split G we extend our ring and then use descent, noting that everything we claim and do is compatible with the action of the Galois group. Now (iii) is an evident corollary of (ii).

Let T be a maximal A-torus of G contained in a Borel A-subgroup of G.

(5.3) LEMMA. *T is the unique maximal A-torus of G such that $f(T) = T_k$.*

Proof. This follows from [SGA3, XI.1.11 and XXII.5.6.13].

(5.4) LEMMA. $T(A) \simeq T(k) \times T(R)$.

Proof. $T(A)$ is a finite commutative group; its image under f is a p'-group $T(k)$ and its kernel is a p-group $T(R)$. Thus (6.4) follows from the structure theorem of commutative groups.

Denote the p'-component of $T(A)$ by $T(p')$; by (5.4) $T(p') \simeq T(k)$. We say that $T(p')$ distinguishes the roots of T on G if for two roots r_1, r_2 of T on G, $r_1|T(p') \equiv r_2|T(p')$ implies that $r_1 = r_2$.

(5.5) LEMMA. *There exists $\tilde{e} = \tilde{e}(G) \in \mathbf{N}$ (which does not depend on k) such that if $|k| > \tilde{e}$ then $T(p')$ distinguishes the roots of T on G.*

Proof. For any pair of roots there are only finitely many fields $l \subseteq \bar{k}$ which do not distinguish the given pair (because an infinite number would be dense in T and then T would not distinguish these roots, which is absurd). As there are only finitely many pairs of roots our claim follows.

Assume now that $R^m \neq 0$, $R^{m+1} = 0$, and let K be a subgroup of $G(R^m) \simeq L(k) \otimes R^m$ invariant under $\mathrm{Ad}\, G(A)$. Since $\mathrm{Ad}\, G(R)$ acts trivially on $G(R^m)$, K is just a $G(k)$-invariant subgroup of $L(k) \otimes R^m$. Write $K = \sum L_i(k) \otimes D_i$ where the L_i are $G(k)$-invariant subspaces of L (in particular, ideals of L) and the D_i are subspaces of R^m. By inspection of the tables at the end of [H] we establish that:

(5.6) L possesses a largest $G(k)$-invariant subspace $\tilde{L}$ which is not L itself. That is:

(i) $\tilde{L} = \{0\}$ if L is not of type A_{np-1}, $n \geq 1$; G_2 or E_6 if $p = 3$; B_n, C_n, D_n, E_7, or F_4 if $p = 2$;

(ii) $\tilde{L}$ is the center of L if L is of type A_{np-1}, $n \geq 1$; E_6 with $p = 3$; D_n, $n \neq 2$, or E_7 if $p = 2$;

(iii) $\tilde{L}$ is of type A_2 (resp. D_4, resp. D_n) if L is of type G_2 and $p = 3$ (resp. F_4 and $p = 2$, resp. C_n and $p = 2$);

(iv) $\tilde{L}$ is of type $A_1 + \cdots + A_1$ (n times) if L is of type B_n and $p = 2$.

(5.7) LEMMA. *There exists a long absolute root b with respect to T such that the corresponding root subgroup $U := U_b$ of G is defined over A and* $\mathrm{Lie}\, U \not\subset \tilde{L}$.

Proof. This is trivial if G is split. If G is not split (but then it is quasi-split) then G is of type A_n, D_n, or E_6. In these cases the condition $\mathrm{Lie}\, U \not\subset \tilde{L}$ is empty since in these cases $\tilde{L} \subseteq \mathrm{Lie}\, T$ (see tables at the end of [H]). Now by inspection of possible actions of the automorphism groups of Dynkin diagrams one observes that any such action fixes a simple root (which then verifies (5.7)) unless L is of type A_{2n}. In this latter case let $a_1, \ldots, a_{2n}$ be simple roots; then $b := a_1 + \cdots + a_{2n}$ satisfies (5.7).

6. Cohomological remarks

Let k be a finite field, G an absolutely almost simple simply connected algebraic group over k, and L its Lie algebra. We are interested in $H^1(G(k), L(k))$.

(6.1) LEMMA. *Let C be the center of L. If $|k| > 9$ then the natural map*

$$H^1(G(k), L(k)) \to H^1(G(k), L(k)/C(k))$$

is an isomorphism.

Proof. Consider the exact cohomology sequence

$$H^1(G(k), C(k)) \to H^1(G(k), L(k)) \to H^1(G(k), L(k)/C(k)) \to H^2(G(k), C(k))$$

associated to the exact sequence

$$0 \to C(k) \to L(k) \to L(k)/C(k) \to 0$$

of $G(k)$-modules. The group $H^1(G(k), C(k)) \simeq \mathrm{Hom}(G(k), C(k))$ is trivial since $G(k)$ is equal (if $|k| > 3$) to its own commutator group (by [S1, Theorems 5, 34, and Corollary to Lemma 64]). Similarly, the group $H^2(G(k), C(k))$ of central extensions of $G(k)$ by $C(k)$ is trivial since (if $|k| > 9$) $G(k)$ has no central extensions (by [S2]).

Now let $\bar{L}$ be the adjoint Lie algebra of L and $\mathrm{ad}: L \to \bar{L}$ the adjoint map. Since $\mathrm{Ker}\, \mathrm{ad} = C$ we have an exact sequence

$$0 \to L(k)/C(k) \xrightarrow{\mathrm{ad}} \bar{L}(k) \to \bar{L}(k)/\mathrm{ad}\, L(k) \to 0.$$

The group $S = \bar{L}(k)/\mathrm{ad}\, L(k)$ is commutative and isomorphic to $C(k)^* = \mathrm{Hom}_k(C(k), k)$ (see [H, pp. 124, 125]); $G(k)$ acts trivially on S. Associated to the

above exact sequence we have a long cohomology exact sequence

$$H^0(G(k), \bar{L}(k)) \to H^0(G(k), S) \xrightarrow{\delta} H^1(G(k), L(k)/C(k)) \to H^1(G(k), \bar{L}(k)).$$

We have $H^0(G(k), \bar{L}(k)) = \bar{L}(k)^{G(k)} = \{0\}$ and $H^0(G(k), S) = S^{G(k)} = S$. Thus we obtain an injective map δ: $S \to H^1(G(k), L(k)/C(k))$.

(6.2) PROPOSITION (J. Bernstein). *Suppose* $|k| > 9$ *and that the only* $G(k)$*-invariant ideals of* L *are central. Then* δ *is an isomorphism.*

Proof. Since δ is injective it remains to prove that it is surjective. Now [CPS1, CPS2] imply, under our conditions on G and k, that $\dim_k H^1(G(k), L(k)) \leq \dim C$ (so that our claim follows from (6.1)). That is, if G is split then, as was pointed out to me by Brian Parshall, statements (2.8), (2.7), and (3.3) of [CPS1] combine to give the result. Indeed, in our case $V = L$ so that $L^B = L^G$, $\dim L_0 =$ (rank of G), and also ψ can be taken to be the simple roots. Now [CPS1, (2.7a)] says in view of [CPS1, (3.3)] that $\dim Z^1(U_\alpha, L)^T \leq 1$, whence [CPS1, (2.8)] gives that $\dim_k H^1(G(k), L(k)) \leq \dim L^G$ as required. For G of twisted type the desired inequality is explicitly contained in the table in [CPS2].

Remarks. (i) J. Bernstein has shown me how to use $\bar{L}$ and the action of $\bar{G}$ (see (6.4) below) to construct non-trivial elements in $H^1(G(k), L(k))$, and B. Parshall told me how to derive the inequality $\dim_k H^1(G(k), L(k)) \leq \dim C$ from results of [CPS1] in the case $\dim C \geq 1$.

(ii) We also have δ: $\bar{L}/\mathrm{ad}\, L \to H^1(G, L)$ which is injective; λ is also surjective by [SGA3, XXIV.1.12] (see (6.4) below). Thus δ is an isomorphism in this case as well.

(6.3) COROLLARY. $H^1(G(k), L(k)) \simeq C(k)^*$.

Proof. Combine (6.1) and (6.2).

We now assume that A is a finite local ring, R is its radical, $R^2 = 0$, and $A/R \simeq k$. Let G be an absolutely almost simple simply connected group scheme over A, $H = R_{A/k}G$. Let C be the center of L and $\tilde{C}$ the connected reduced center of H. Then $\tilde{C}(k) \subseteq R_{A/k}G(R) \simeq L(k) \otimes R$ and $\tilde{C}(k) = C(k) \otimes R$ if we identify $R_{A/k}G(R)$ with $L(k) \otimes R$. Let $M = H/\tilde{C}$. In view of previous remarks $M(k)$ has the largest normal p-subgroup P which is isomorphic to $(L(k)/C(k)) \otimes R = \mathrm{ad}\, L(k) \otimes R$. Let h denote the projection $M(k) \to G(k) = M(k)/P$.

The P-conjugacy classes of sections s: $G(k) \to M(k)$ of h: $M(k) \to G(k)$ are (by [CPS1, § 2]) in one-to-one correspondence with the elements of

$$H^1(G(k), P) = H^1(G(k), \mathrm{ad}\, L(k) \otimes R) = H^1(G(k), \mathrm{ad}\, L(k)) \otimes R.$$

Let $\overline{G}$ be the adjoint group of G. Then $\overline{G}$ acts on G by automorphisms. Therefore $\overline{G}(A)$ acts by automorphisms on $G(A)$ and on $M(k)$. Clearly, the automorphisms from $\overline{G}(R)(\simeq \overline{L}(k) \otimes R)$ when acting on $M(k)$ map a section of h to a section. Now (6.2) can be reformulated as

(6.4) PROPOSITION. *$\overline{G}(R)$ acts transitively on the sections of h.*

Proof. Fix one section s_0: $G(k) \to M(k)$ of h, and take it for $0 \in H^1(G(k), P)$. Then for $\bar{p} \in \overline{G}(R)$ and $(0 \rtimes g) \in s_0(G(k))$, we have $\bar{p}(0 \rtimes g) = ((\mathrm{Ad}\, g)(\bar{p}) - \bar{p}) \rtimes g = \bar{l}(g) \rtimes g$. Then $\bar{l}$: $G(k) \to P$ is the cocycle determining the section $\bar{p}(s_0)$; this cocycle is cohomologous to 0 if and only if $\bar{p} \in \mathrm{ad}\, L(k) \otimes R$. Thus on the cohomology level, the class of $\bar{l}$ is represented by $(\mathrm{Ad}\, g)(\bar{p}) - \bar{p}$. This class is exactly the image under δ of $\bar{p}(\mathrm{mod}\, \mathrm{ad}\, L(k) \otimes R) \in S \otimes R = H^0(G(k), S \otimes R)$ where S is as in (6.2). Thus (6.4) does, indeed, follow from (6.2).

7. Approximation on the finite level

Let A be a finite ring (with 1) and R its radical. Then A (see [M, (VI.2)]) is a direct sum of local rings, $A = \oplus_{1 \le i \le t} A_i$, and $R_i := A_i \cap R$ is the radical (= the maximal ideal) of A_i. Write $k_i := A_i/R_i$, $k_i \simeq \mathbf{F}_{q_i}$ where $q_i = p_i^{m_i}$ with primes p_i, $1 \le i \le t$. Set $R^0 := A$. We say that A is of class m if $R^m \neq 0$, $R^{m+1} = 0$.

Let G be a connected and simply connected absolutely almost simple group scheme over A of constant type (see [SGA3, § XXII.2]). The groups G_{A_i} are quasi-split by (5.1) and therefore G itself is quasi-split. We use notation $T, T(p')$ of Section 5.

As in Section 5 we denote by f_i the projections

$$A \to A/R^i,\ G(A) \to G(A/R^i),\ G_A \to G_{A/R^i},\ L(A) \to L(A/R^i) \text{ etc.}$$

and set $G(R^i) = \mathrm{Ker}\,\{f_i\colon G(A) \to G(A/R^i)\}$. Set $f := f_1$.

Let $L := \mathrm{Lie}\, G$ be the Lie algebra of G. It is a free A-module. The action of G on L is denoted, as usual, by Ad. We denote by C_i the center of L_{k_i}.

Let Γ be a subgroup of $G(A)$.

(7.1) *Assumptions.* (i) $q_i \ge \max(10, \tilde{e}(G))$, $1 \le i \le t$, where $\tilde{e}(G)$ is the same as in (5.5);

(ii) The only proper ideals of the Lie algebra $L(k_i) \simeq L(\mathbf{F}_{q_i})$, $1 \le i \le t$, are central;

(iii) The image of Γ in $G(k_i)$ under the reduction modulo $R \oplus \oplus_{j \neq i} A_j$ is the whole $G(k_i)$;

(iv) $\mathbf{Z}[\mathrm{tr}\,\mathrm{Ad}\, f_2(\Gamma)] = A/R^2$.

In (iv) trace is taken in a free A/R^2-module $L(A/R^2)$.

Remark. Condition (7.1) (ii) excludes types G_2 if $p_i = 3$ for some i, and B_n ($n \geq 1$), C_n ($n \geq 1$), and F_4 if $p_i = 2$ for some i. On the other hand, it and (7.1) (i) enable us to use (6.4).

(7.2) THEOREM. *If* (7.1) (i)–(iv) *hold, then* $\Gamma = G(A)$.

The proof will be given in several steps.

(7.3) *Step 1.* The theorem holds if $R = 0$.

Proof. In this case Γ is a subgroup of $\prod_{1 \leq i \leq t} G(\mathbf{F}_{q_i})$ where the $G(\mathbf{F}_{q_i})$ are universal groups of Chevalley or Steinberg type. Since $q_i \geq 5$, $1 \leq i \leq t$, these groups are perfect and simple modulo their centers [by [S1, Theorems 5, 34, and Corollary to Lemma 64]). Since Γ projects onto each $G(\mathbf{F}_{q_i})$ by (5.1) (iii), it follows that Γ modulo the center is a direct product of simple groups. Since $[G(\mathbf{F}_{q_i}), G(\mathbf{F}_{q_i})] = G(\mathbf{F}_{q_i})$ and since Γ is a subgroup of $\prod_{1 \leq i \leq t} G(\mathbf{F}_{q_i})$, it follows that Γ is isomorphic to a direct product, $\Gamma = \prod_{1 \leq j \leq r} \Gamma_j$, $r \leq t$, of finite simple groups each of which is isomorphic to some $G(\mathbf{F}_{q_i})$, $1 \leq i \leq t$. Let pr_i, $1 \leq i \leq t$, be the projection of $G(A)$ onto $G(A_i)$. For each j, $1 \leq j \leq r$, let $I(j) := \{i | pr_i \Gamma_j = G(A_i)\}$. By (7.1) (iii), we have $\bigcup_{1 \leq j \leq r} I(j) = [1, t]$, and, since $[\Gamma_k, \Gamma_j] = \{1\}$ for $k \neq j$, we also have $I(j) \cap I(k) = \varnothing$ if $k \neq j$.

Suppose that $|I(j)| > 1$ for some j. Then Γ_j projects onto each $G(A_i)$, $i \in I(j)$, and the kernel of each such projection is trivial. Thus we have isomorphisms h_i: $\Gamma_j \to G(A_i)$ for all $i \in I(j)$. Fix some $s \in I(j)$ and set $\tilde{h}_i := h_i \circ h_s^{-1}$ for $i \in I(j)$. Then $\tilde{h}_i$: $G(A_s) \to G(A_i)$ is an isomorphism, $i \in I(j)$. By [S1, Theorems 30 and 36] all A_i, $i \in I(j)$, are isomorphic and each $\tilde{h}_i$, $i \in I(j)$, is a composition of an algebraic A_i-isomorphism u_i: $G_{A_s} \to G_{A_i}$ (recall that (7.1) (iii) keeps us away from bad characteristics) and of a field isomorphism σ_i: $A_s \to A_i$.

We have $\operatorname{tr}\operatorname{Ad} g = \operatorname{tr}\operatorname{Ad} u_i(g)$ and $\sigma_i(\operatorname{tr}\operatorname{Ad} g) = \operatorname{tr}\operatorname{Ad} \sigma_i(g)$ for $g \in G(A_i)$. Thus the subring $\mathbf{Z}[\operatorname{tr}\operatorname{Ad}\Gamma]$ is contained in $\oplus_{1 \leq j \leq r} B_j$ where B_j is the subring of $\oplus_{i \in I(j)} A_i$ generated by $\{\oplus_{i \in I(j)} \sigma_i(a), a \in A_s\}$. This latter ring is isomorphic to A_s. Since by (7.1) (iv), we must have $B_j = \oplus_{i \in I(j)} A_i$, it follows that $I(j) = \{s\}$ in contradiction to our assumption that $|I(j)| > 1$.

(7.4) *Step 2.* If $t = 1$ and $R^2 = 0$ then (7.2) holds.

Proof. Assume the contrary. Let $K := A/R$ and $p := p_1 (= \operatorname{char} k)$. By (7.1) (iii), $f(\Gamma) = G(k)$. Let $\tilde{\Gamma}$ be the preimage of $T(k)$ under f. The kernel P of f: $G(A) \to G(k)$ is a p-group and therefore, so is the kernel $\tilde{P}$ of f: $\Gamma \to G(k)$. Since $T(k)$ is a p'-group, we have by [G1, Theorem 6.4.1(i)] that $\tilde{\Gamma}$ is a

semi-direct product of a p'-group $\tilde{P}'$ and of $\tilde{P}$. By (5.4) $\tilde{P}'$ is conjugated by an element of P to $T(p')$ ($= p'$-component of $T(A)$). Therefore, replacing Γ, if needed, by its conjugate in $G(A)$ we can assume that

$$T(p') \subset \Gamma. \tag{7.4.1}$$

Let K be the kernel of f: $\Gamma \to G(k)$, $K \subseteq G(R) \simeq L(k) \otimes R$. Since $f(\Gamma) = G(k)$ we get that K is $G(k)$-invariant. We identify $G(R)$ with $L(k) \otimes R$. Then by (5.6) there exists $D \subset R$ such that $K \subseteq \tilde{L}(k) \otimes R + L(k) \otimes D$ where $D \neq R$ since $\Gamma \neq G(A)$. Take $D_1 \subseteq R$, $D_1 \supseteq D$, $\dim_k R/D_1 = 1$. Replacing A by A/D_1 and Γ by its image in $G(A/D_1)$ (which does not affect conditions (7.1) (i)–(iv)), we can assume that $D_1 = 0$; i.e. we can assume

$$\dim_k R = 1, \qquad K \subseteq \tilde{L}(k). \tag{7.4.2}$$

Let b and U_b be as in (5.7). Since $U_b(k) = f(U_b(A))$ is contained in a root subgroup of $T(k) = f(T(p'))$, since $U_b(k) \subseteq f(\Gamma)$, and since $T(p')$ distinguishes the roots of T by (5.5), it follows that

$$f(\Gamma \cap U_b(A)) = U_b(k). \tag{7.4.3}$$

In particular, $\Gamma \cap U_b(A)$ is nontrivial. Since $U_b(A) \simeq \mathbf{G}_{a,A}(A) \simeq A$ for our choice of b, we can consider $\Gamma \cap U_b(A)$ as a subgroup V of A. By (7.4.2) and by our choice of b we have that $V \cap R = \{0\}$ and f: $(\Gamma \cap U_b(A)) \to U_b(k)$ is an isomorphism. Thus $A = V + R$, a direct product of two elementary abelian groups. In particular, $pA = 0$ and, by [Mc, (XXII.1)], $A \supseteq k$ (as rings) and $A = k[\varepsilon]$ for any $\varepsilon \in R$ (since $\dim_k R = 1$). Thus we have proved

$$A = k[\varepsilon], \qquad \varepsilon^2 = 0. \tag{7.4.4}$$

Now we can complete the proof of (7.4). By (7.4.2) the image $\bar{\Gamma}$ of Γ in $H := G(A)/\tilde{L}(k)$ (where $\tilde{L}(k) \subset L(k) = G(R)$) is a section of $H \to G(k)$. By (7.4.5) $A = k[\varepsilon]$ and therefore there is a section s_0: $G(k) \to G(A)$, $g \to 0 \rtimes g \in L(k) \rtimes G(k)$. This gives rise to a section $\bar{s}_0$: $G(k) \to H$.

Now (for the first time) use (7.1) (ii). It implies that $\tilde{L}(k) \subset C(k)$, the center of $L(k)$. Then (6.4) tells us that by applying an automorphism from $\bar{G}(A)$, $\bar{G}$ the adjoint group of G, we can assume that $\bar{\Gamma} = \bar{s}_0(G(k))$ (the assumptions (7.1) are not affected by such change). Therefore $\Gamma \subseteq s_0(G(k)) \cdot C(k)$. Therefore $\operatorname{tr} \operatorname{Ad} \Gamma \subseteq \operatorname{tr} \operatorname{Ad} s_0(G(k)) \subseteq k$ (the latter by our choice of s_0). This contradicts (7.1) (iv).

(7.5) *Step* 3. If $R^2 = 0$ then (7.2) holds.

Proof. We have $R = \oplus_{1 \le i \le t} R_i$ so that $G(R) = \prod_{1 \le i \le t} G(R_i)$. For $m \in G(R)$, write $m = \prod_{1 \le i \le t} m_i$ with $m_i \in G(R_i)$. By (7.4) given s, $1 \le s \le t$, there exists $m \in \Gamma \cap G(R)$ such that $m_s \notin C_s(k_s)$. Let Γ_s be the preimage in Γ

of $G(k_s)$ under the projection $\Gamma \to G(k_s)$. Then $\Gamma_s \subseteq G(A_s + R)$, whence $gm_ig^{-1} = m_i$, for $g \in \Gamma_s$ and $i \neq s$. Therefore $gmg^{-1}m^{-1} \in G(R_s)$. Since $m_s \notin C_s(k_s)$ and since $G(k_s)$, and, therefore, Γ_s act irreducibly over k_s on $M_s := L(k_s)/C_s(k_s)$ (by [S1, Theorem 43]) it follows that the images in M_s of the $gmg^{-1}m^{-1}$, $g \in \Gamma_s$, generate M_s. Since $L(k_s)$ does not have proper invariant $G(k_s)$-submodules for the possible exception of $C_s(k_s)$, it follows that $\Gamma_s \supset G(R_s)$. Thus $\Gamma \supset \prod_{1 \leq i \leq t} G(R_i)$. This together with (7.3) implies that $\Gamma = G(A)$ as claimed.

(7.6) *Step 4.* Theorem (7.2) holds.

Proof. Let $\Gamma' = \Gamma \cap G(R)$. By (7.5), $\Gamma' \cdot G(R^2) = G(R)$ and by (5.2), $[G(R), G(R)] = G(R^2)$. Thus by [G1, Theorem 5.1.1] $\Gamma' = G(R)$ whence by (7.1) (iii) $\Gamma = G(A)$ as claimed.

8. Global approximation

Let k be an algebraically closed field of characteristic p, G an almost simple simply connected algebraic group defined over k, L its Lie algebra, C the center of L, c the order of the schematic center of G. Let Γ be a subgroup of $G(k)$ and let $A = \mathbf{Z}[\operatorname{tr} \operatorname{Ad} \Gamma]$ be the subring of k generated by the $\operatorname{tr} \operatorname{Ad} \gamma$, $\gamma \in \Gamma$. Set $\tilde{\Gamma} := \mathscr{D}\Gamma \cdot \Gamma^{\langle c \rangle}$, $\Gamma' := \mathscr{D}\tilde{\Gamma} \cdot \tilde{\Gamma}^{\langle c \rangle}$, and $A' := \mathbf{Z}[\operatorname{tr} \operatorname{Ad} \Gamma']$.

(8.1) *Assumptions.* If $p = 3$, assume that G is not of type G_2 and if $p = 2$ it is not of type B_n ($n \geq 1$), C_n ($n \geq 1$), or F_4 (see (12.2) below for comments about these excluded cases).

(8.2) THEOREM. *Suppose that Γ is finitely generated and that it is Zariski-dense in G. Then there exists $b \in A'$ such that*

(i) *A_b is finitely generated;*

(ii) *$A_b = A'_b$;*

(iii) *G has a structure G_{A_b} of a semi-simple group scheme over A_b such that $\Gamma' \subseteq G_{A_b}(A_b)$;*

(iv) *Γ' is dense in $G_{A_b}(\hat{A}_b)$.*

(8.3) LEMMA. (i) *$\tilde{\Gamma}$ and Γ' are normal in Γ;*

(ii) *$\Gamma/\tilde{\Gamma}$ is a finite commutative group of period c, Γ/Γ' is a finite solvable group of period c^2;*

(iii) *$\tilde{\Gamma}$ and Γ', are finitely generated;*

(iv) *Any homomorphism of Γ into a commutative group of period c factors through $\tilde{\Gamma}$.*

Proof. (i), (ii), and (iv) are evident; (iii) follows from the finiteness of $\Gamma/\tilde{\Gamma}$ and Γ/Γ' and finite generation of Γ (by [MKS, Corollary 2.7.1]).

Let $\overline{G}$ be the adjoint group of G.

The action of $\overline{G}$ on L preserves C and therefore there exists a homomorphism h: $\overline{G} \to \mathrm{GL}(L/C)$.

(8.4) LEMMA. $\operatorname{Ker} dh = 0$.

Proof. In view of (8.1) and [S3] (or [H]) $\mathscr{D}(\operatorname{Lie}\overline{G}) \simeq L/C$ and since L/C is non-commutative $\operatorname{Ker} dh$ does not contain $\mathscr{D}(\operatorname{Lie}\overline{G})$. On the other hand L/C is irreducible under $\overline{G}$ by (4.6) (i), (ii) whence $\operatorname{Ker} dh \cap \mathscr{D}(\operatorname{Lie}\overline{G}) = 0$. But $\mathscr{D}(\operatorname{Lie}\overline{G})$ is the unique minimal ideal of $\operatorname{Lie}\overline{G}$ (by tables on pp. 124, 125 of [H]) whence $\operatorname{Ker} dh$ (which is an ideal) must be zero.

(8.5) COROLLARY. *h: $\overline{G} \to h(\overline{G})$ is an isomorphism.*

Proof. Since $\overline{G}$ is simple $\operatorname{Ker} h$ can only be infinitesimal. This latter possibility is rejected by (8.4).

Now we need several comments on fields and rings of definition of Γ; in these comments we follow E. B. Vinberg [V, §§ 1, 2].

Let K be the field of quotients of A.

(8.6) PROPOSITION. (i) *K is finitely generated;*

(ii) *G has the structure G_K of an algebraic K-group such that $\Gamma' \subseteq G_K(K)$;*

(iii) *The field of quotients of A' is K.*

Proof. Let $\gamma_1, \ldots, \gamma_s$ be generators of Γ. Choose a basis of L and consider the field $\tilde{K}$ generated by the matrix entries $a_{ij}(\gamma_m)$ of the matrices $\operatorname{Ad}\gamma_m$. Then $\tilde{K}$ has $s \cdot (\dim L)^2$ generators. Since $K \subseteq \tilde{K}$, it follows that K is also finitely generated (by [Ba1, Lemma 3.7]).

Denote by $\overline{\mathrm{Ad}}$ the representation of $\overline{G}$ on L/C. Note that $\operatorname{tr}\overline{\mathrm{Ad}}\,h = \operatorname{tr}\mathrm{Ad}\,h$ for all $h \in \overline{G}$. Let D be the K-subalgebra of $\mathrm{End}_k(L/C)$ generated by $\overline{\mathrm{Ad}}\,\Gamma$. Since $\overline{\mathrm{Ad}}$ is absolutely irreducible for $\overline{\mathrm{Ad}}\,\overline{G}$ and since $\overline{\mathrm{Ad}}\,\Gamma$ is Zariski-dense in $\overline{\mathrm{Ad}}\,\overline{G}$, it follows that L/C is absolutely irreducible for $\overline{\mathrm{Ad}}\,\Gamma$ as well. Thus D is central and simple over K. In a K-basis of D the operators $R \circ \overline{\mathrm{Ad}}\,\gamma$ of right multiplication by $\overline{\mathrm{Ad}}\,\gamma$, $\gamma \in \Gamma$, are given then by matrices with coefficients in K. Therefore the Zariski-closure $R \circ \overline{\mathrm{Ad}}\,\overline{G}$ of $R \circ \overline{\mathrm{Ad}}(\Gamma)$ is defined over K. By (8.5) this gives us a K-structure on $\overline{G}$; we denote it by $\overline{G}_K$. We have $\mathrm{Ad}\,\Gamma \subseteq \overline{G}_K(K)$ by construction.

By [BT2, (2.24) (ii)], G has then a unique structure G_K of a K-group for which the projection Ad: $G \to \overline{G}$ is a K-map. By [BT3, (3.17)] we know that $\mathrm{Ad}(G_K(K))$ is normal in $\overline{G}_K(K)$ and the quotient is an abelian group of exponent c. Thus $\mathscr{D}(\overline{G}_K(K))\overline{G}_K(K)^{\langle c\rangle} \subseteq \mathrm{Ad}(G_K(K))$. In particular, by (8.3) (iv), $\mathrm{Ad}\,\tilde{\Gamma} \subseteq \mathrm{Ad}(G_K(K))$, i.e. for every $\gamma_1, \gamma_2 \in \tilde{\Gamma}$ there exist $h_1, h_2 \in G_K(K)$ such that $\gamma_i h_i^{-1} \in C(G)$ for $i = 1, 2$. Write $x_i := \gamma_i h_i^{-1}$, $i = 1, 2$, with $x_i \in C(G)$. Then

$\gamma_i^c = h_i^c \cdot x_i^c = h_i^c$, $i = 1, 2$, i.e. $\gamma_i^c \in G_K(K)$. Also $[\gamma_1, \gamma_2] = [h_1 x_1, h_2 x_2] = [h_1, h_2]$, whence $[\gamma_1, \gamma_2] \in G_K(K)$. Thus $\Gamma' = \mathscr{D}\tilde{\Gamma} \cdot \tilde{\Gamma}^{\langle c \rangle} \subseteq G_K(K)$ as claimed.

Now denote by K' the field generated by A'. Then $K' \subseteq K$. As in the previous case $\overline{G}$ has a structure of a K'-group which is described by a K'-subspace V of L/C. Since $\overline{\mathrm{Ad}}\,\Gamma'$ acts absolutely irreducibly on L/C this subspace V is determined up to multiplication by a scalar. But then PV, the projectivization of V, is determined uniquely. Denote by P the map $\overline{\mathrm{Ad}}\,\overline{G} \to \mathrm{PGL}(L/C)$. For $h \in N_{\mathrm{PGL}(L/C)}(P \circ \overline{\mathrm{Ad}}\,\Gamma)$, we have $h(PV) = PV$ in view of uniqueness. If $h \in \overline{G}(K)$ then the above says that $P \circ \overline{\mathrm{Ad}}\,h \in P\,\overline{\mathrm{Ad}}\,\overline{G}(k) \cap \mathrm{PGL}(PV)$, i.e. $P \circ \overline{\mathrm{Ad}}\,h \in P \circ \overline{\mathrm{Ad}}\,\overline{G}_{K'}(K')$. Since P and $\overline{\mathrm{Ad}}$ are K'-isomorphisms we have that $h \in \overline{G}_{K'}(K')$. Since $\Gamma' \triangleleft \Gamma$, this implies that $\mathrm{Ad}\,\gamma \in \overline{G}_{K'}(K')$ for $\gamma \in \Gamma$. But then $\mathbf{Z}[\mathrm{tr}\,\mathrm{Ad}\,\Gamma] \subseteq K'$, whence $K = K'$ as claimed.

(8.7) PROPOSITION. *There exists $\bar{b} \in A'$ such that*

(i) *$A_{\bar{b}}$ is finitely generated and regular;*

(ii) *$A_{\bar{b}} = A'_{\bar{b}}$;*

(iii) *G has a structure $G_{A_{\bar{b}}}$ of a semi-simple groupscheme over $A_{\bar{b}}$ such that*

(a) *$G_{A_{\bar{b}}}(A_{\bar{b}}) \supseteq \Gamma'$;*

(b) *$(\mathrm{Lie}\,G_{A_{\bar{b}}})(A_{\bar{b}})$ and $(\mathrm{Lie}\,G_{A_{\bar{b}}})(A_{\bar{b}})/(\text{center})$ are free $A_{\bar{b}}$-modules.*

Proof. Pick elements $\gamma_1, \ldots, \gamma_s$ from Γ' such that the field generated by the $\mathrm{tr}\,\mathrm{Ad}\,\gamma_i$, $1 \le i \le s$, is K (possible in view of (8.6) (i) and (iii)). Let $\tilde{A}'$ be the ring generated by the $\mathrm{tr}\,\mathrm{Ad}\,\gamma_i$, $1 \le i \le s$. Augment $\gamma_1, \ldots, \gamma_s$ to a generating set $\gamma_1, \ldots, \gamma_m$, $m \ge s$, for Γ (recall: Γ is finitely generated). Take a K-basis of $\mathrm{Lie}\,G_K(K)$ and let $\tilde{A}$ be the subring of K generated by the matrix entries of the $\mathrm{Ad}\,\gamma_i$, $1 \le i \le m$, in this basis. We have then that $\mathrm{Ad}\,\Gamma \subseteq \mathrm{GL}_d(\tilde{A})$.

Since $\tilde{A} \supseteq A \supseteq A' \supseteq \tilde{A}'$, since $\tilde{A}$ and $\tilde{A}'$ are finitely generated, and since $\tilde{A}$ and $\tilde{A}'$ have the same fields of quotients there exists $b' \in \tilde{A}'$ such that $\tilde{A}_{b'} = \tilde{A}'_{b'}$ (for example, take for b' the product of denominators in expressions of the generators of $\tilde{A}$ through elements of $\tilde{A}'$). In particular, $\tilde{A}_{b'} = A_{b'} = A'_{b'} = \tilde{A}'_{b'}$ are finitely generated (although A and A' may be infinitely generated). Since $A_{b'}$ is finitely generated and integral, there is $b'' \in A_{b'}$ such that $A_{b'b''}$ is regular.

Now pick a set $f_1, \ldots, f_m$ of K-algebra generators of $k[G]$ and a set $\gamma_1, \ldots, \gamma_r$ of generators of Γ' (possible by (8.3) (iii)). Let b_{ij}, $1 \le i \le m$, $1 \le j \le r$, be the denominator of $f_i(\gamma_j) \in K$ in its expression as a fraction of elements of $A_{b'b''}$. Next consider comultiplication μ: $K[G] \to K(G) \otimes K[G]$ and coinversion ι: $K[G] \to K[G]$ and pick $b_i, b_i' \in A_{b'b''}$ such that $b_i \mu(f_i) \in A_{b'b''}[f_1, \ldots, f_m] \otimes A_{b'b''}[f_1, \ldots, f_m]$ and $b_i' \iota(f_i) \in A_{b'b''}[f_1, \ldots, f_m]$ for $1 \le i \le m$. Set $\tilde{b} := b'b'' \prod_{1 \le i \le m} \prod_{1 \le j \le r} b_{ij} b_i b_i'$. Then $A_{\tilde{b}}[f_1, f_2, \ldots, f_m]$ is a Hopf algebra over $A_{\tilde{b}}$ and, therefore, defines a structure of a group scheme $G_{A_{\tilde{b}}}$ over $A_{\tilde{b}}$ on G_K. Since $f_i(\gamma_j) \in A_{\tilde{b}}$ it follows that $\Gamma' \subseteq G_{A_{\tilde{b}}}(A_{\tilde{b}})$.

The set of points $x \in \operatorname{Spec} A_{\bar{b}}$ such that G_x is smooth, connected and semi-simple contains an open subset U of $\operatorname{Spec} A_{\bar{b}}$. (That is, by [SGA3, Corollary VI_B.2.3, Proposition VI_B.3.5] there exists an open $V \subset \operatorname{Spec} A_{\bar{b}}$ and an open subscheme H_V of G_V such that H_V is smooth with connected fibers. Therefore $G_V - H_V$ is closed, whence its image S under the structure map into V is constructible. Since the generic fiber G_K is smooth and connected it follows that the generic point of V is not in S. Therefore, since S is constructible, $V - S$ contains an open set W of V; that is, G_W is smooth with connected fibers. Then [SGA3, XIX.2.5] shows that an open U with desired properties does exist.) Let $b_1, \ldots, b_t$ be generators of the ideal defining the complement to U. Then $G_{A_{\bar{b}b_1 \cdots b_r}}$ is semi-simple over $A_{\bar{b}b_1 \cdots b_r}$.

Since $G_{\bar{b}b_1 \cdots b_r}$ is smooth, its Lie algebra is a projective $A_{\bar{b}b_1 \cdots b_r}$-module. After an additional localization at appropriate $b_{r+1} \in A$, it will become free.

In the case of $(\operatorname{Lie} G_{A_b})(A_b)/(\text{center})$ we first localize to kill torsion and then proceed as above. Denote the combined element by which we localized by b_{r+2} (so that $b_{r+2} = 1$ if $C = 0$). Then (8.6) holds with $\bar{b} = \tilde{b}b_1 \cdots b_r b_{r+1} b_{r+2}$.

Let B be a subring of k, $B \supseteq A_{\bar{b}}$. For any ideal I of B, we have a map $f_{B,I}\colon G_B \to G_{B/I}$, the reduction modulo I. It induces a map on points $f^0_{B,I}\colon G_B(B) \to G_B(B/I) = G_{B/I}(B/I)$.

Let m and r be numbers constructed in (3.1) for $d := \dim(L/C)$. Further, let r' be the least common multiple of $|\mathrm{GL}_d(\mathbf{F}_{2^m})|$ for $m \le e(d)$ where $e(d)$ is from Section 4. Consider $\Delta := (\mathscr{D}^4\Gamma^{\langle mc^2\rangle})^{\langle rr'\rangle}$. Since $\Gamma' \supseteq \Gamma^{\langle c^2\rangle}$, we have that

$$(*) \qquad \Delta \subseteq (\mathscr{D}^4\Gamma'^{\langle m\rangle})^{\langle rr'\rangle}.$$

We still have that Δ is Zariski dense in G (because the Zariski closure of Δ is $(\mathscr{D}^4 G^{\langle mc^2\rangle})^{\langle rr'\rangle} = G$).

Let $\bar{L}$ denote the free $A_{\bar{b}}$-module structure on L/C. For a ring B, a B-module M and a subgroup Π of $(\operatorname{End}_B M)^*$ we denote by $B \cdot \Pi$ the B-envelope of Π in $\operatorname{End}_B M$.

To give meaning to the next statement we remark that the adjoint representation of a B-group scheme is always a B-morphism (see [SGA3, § II.4]). Therefore so is $\overline{\mathrm{Ad}}$.

(8.8) Lemma. *There exists $\hat{b} \in A_{\bar{b}}$ such that for any maximal ideal M of $A_{\bar{b}\hat{b}}$ the reduction $H := f^0_{A_{\bar{b}\hat{b}},M}(\Gamma')$ satisfies the assumptions of* (3.1).

Proof. Since $\bar{L}$ is free, so is $\operatorname{End}_{A_{\bar{b}}}(\bar{L})$; let $e_1, \ldots, e_{d^2}$ be its basis. Since Δ is Zariski dense in G and is absolutely irreducible on $\bar{L}$, it follows that $K\,\overline{\mathrm{Ad}}\,\Delta = \operatorname{End}_K(\bar{L})$ so that one can write $e_i = \sum a_{i\delta}\delta$ (finite sum) with $1 \le i \le d^2$ and $a_{i\delta} \in K$. Let $\hat{b}$ be the product of denominators of the $a_{i\delta}$. Then $A_{\bar{b}\hat{b}} \cdot \overline{\mathrm{Ad}}\,\Delta = \operatorname{End}_{A_{\bar{b}\hat{b}}}(\bar{L})$. Set $B := A_{\bar{b}\hat{b}}$.

Now we have

$$(\mathscr{D}^4 H^{\langle m\rangle})^{\langle r\rangle} = f^0_{B,M}\big((\mathscr{D}^4\Gamma'^{\langle m\rangle})^{\langle r\rangle}\big) \supseteq f^0_{B,M}(\Delta).$$

By the previous paragraph we know that $B \cdot \Delta = \mathrm{End}_B(\bar{L})$, whence

$$(B/M) \cdot f^0_{B,M}(\Delta) = f^0_{B,M}(B \cdot \Delta) = \mathrm{End}_{B/M}(\bar{L} \otimes_B (B/M)).$$

Thus $f^0_{B,M}(\Delta)$ is absolutely irreducible, whence so is $(\mathscr{D}^4 H^{\langle m\rangle})^{\langle r\rangle}$ as claimed.

(8.9) LEMMA. *There exists* $\tilde{b} \in B := A_{\bar{b}\bar{b}}$ *such that for every maximal ideal* M *of* $\tilde{B} := A_{\bar{b}\bar{b}\tilde{b}}$ *every* $\mathrm{Ad}\,\overline{\mathrm{Ad}} f^0_{\tilde{B},M}(\Delta)$*-submodule of* $(\mathrm{End}\,\mathrm{End}\,\bar{L}) \otimes (\tilde{B}/M)$ *is also an* $\mathrm{Ad}\,\overline{\mathrm{Ad}}\, G_{\tilde{B}/M}$*submodule.*

This means that over a sufficiently large residue field the sub-module lattices of $\mathrm{End}(\bar{L}) \otimes \tilde{B}/M$ under the finite group $\mathrm{Ad}\,\overline{\mathrm{Ad}} f^0_{\tilde{B},M}(\Delta')$ and under the algebraic group $\mathrm{Ad}\,\overline{\mathrm{Ad}}\, G_{\tilde{B}/M}$ are the same.

Proof (J. Bernstein). Set $F := \mathrm{Ad}\,\overline{\mathrm{Ad}}$, $E := \mathrm{End}\,\mathrm{End}\,\bar{L}$. Thus $F\colon G \to E$. By localization at some $a \in B$ we can assume (see [SGA3, Proposition VI_B.2.2]) that F is a smooth embedding of smooth schemes. Let J be the B_a-ideal defining $F(G)$ as a B_a-subscheme of E. Now consider the envelope $K \cdot (F(\Delta))(\subset E \otimes K)$ and let $\{\gamma_i\}_{1 \le i \le s}$, $\gamma_i \in F(\Delta)$, be its basis. Let further $l_1, \ldots, l_m$, $m = d^2 - s$, be a K-basis of linear forms on $E \otimes K$ which vanish on $K \cdot (F(\Delta))$. Since Δ is Zariski dense in G, it follows that $k \cdot (F(\Delta)) = k \cdot F(G)$, i.e. that the l_i vanish on $F(G)$ as well.

Thus $l_i \in J \otimes K$, $1 \le i \le m$ (by Hilbert Nullstellensatz and smoothness of $F(G) \subset E$). We can assume by multiplying the l_i by appropriate $a_i \in B$ that $l_i \in \check{E}$ (the dual of E) and that $l_i \in J$ for $1 \le i \le t$.

Now localize at $a' \in B_a$ to ensure that the reductions $l_{i,M}$ modulo any maximal ideal M of $B_{aa'}$ of the l_i are linearly independent and that the same holds for the reductions $\bar{\gamma}_{i,M}$ of the γ_i. Then since $l_i \in J$, $1 \le i \le t$, we have that $\bar{l}_{i,M} \in J \otimes (B_{aa'}/M)$, whence $F(G)_{B_{aa'}/M} \subseteq \bigcap_{1 \le i \le t} \mathrm{Ker}\, l_{i,M}$. On the other hand since the $\bar{\gamma}_{i,M}$ are still independent we have

$$(B_{aa'}/M) \cdot F(\Delta) = \bigcap_{1 \le i \le t} \mathrm{Ker}\, \bar{l}_{i,M}.$$

Now

$$(B_{aa'}/M)F(\Delta) \subseteq F(G)_{B_{aa'}/M} \subseteq \bigcap \mathrm{Ker}\, \bar{l}_{i,M}$$

implies that

$$(B_{aa'}/M) \cdot F(\Delta) = (B_{aa'}/M) \cdot F(G)_{B_{aa'}/M}$$

as claimed (set $\tilde{b} := aa'$).

(8.10) LEMMA. *The G-module* L/C *cannot be represented as a non-trivial tensor product of irreducible G-modules.*

Proof. Let $\lambda_1, \dots, \lambda_m$ be the fundamental weights of G and let $\lambda = \sum_{1 \le i \le m} a_i \lambda_i$ be the highest weight of $\overline{\mathrm{Ad}}$. We have (in an appropriate numeration of the λ_i) that $\lambda = \lambda_1 + \lambda_n$ for type A_n, $\lambda = \lambda_2$ for type B_n, $\lambda = 2\lambda_1$ for type C_n, $\lambda = \lambda_2$ for type D_n, $\lambda = \lambda_2$ for type E_6, $\lambda = \lambda_1$ for type E_7, $\lambda = \lambda_8$ for type E_8, $\lambda = \lambda_1$ for type F_4, and $\lambda = \lambda_2$ for type G_2.

If $\overline{\mathrm{Ad}}$ is a tensor product of, say, two representations with highest weights μ_1, μ_2, then $\mu_1 + \mu_2$ is the highest weight of $\overline{\mathrm{Ad}}$. From the expressions for λ we see that this is only possible for type A_n with $\mu_1 = \lambda_1$, $\mu_2 = \lambda_n$ or $\mu_1 = \lambda_n$ $\mu_2 = \lambda_n$ and for type C_n with $\mu_1 = \mu_2 = \lambda_1$. But in these cases the tensor product in question is reducible.

(8.11) *Proof of* (8.2) *concluded.* It remains only to find b so that (8.2) (iv) will be satisfied. Let $B := A_{\bar{b}\bar{b}\bar{b}}$. Since B is finitely generated, the set S of maximal ideals M of B such that $|B/M| < \max(10, \tilde{e}(G))$ with $\tilde{e}(G)$ from (5.5) is finite. Pick an element s_M in each $M \in S$ and set $a = \prod_{M \in S} s_M$. Then $|B_a/I| \ge \max(10, \tilde{e}(G))$ for any ideal I of B_a.

Let M be a maximal ideal of B_a and let $p := \mathrm{char}\, B_a/M$. Set $\Gamma'_M := f^0_{B_a, M}(\overline{\mathrm{Ad}}\,\Gamma')$. By (8.8) and since $\bar{L}$ is a free B_a-module, we have $B_a \overline{\mathrm{Ad}}\,\Delta \simeq \mathrm{Mat}_d B_a$. Therefore $(B_a/M) \cdot f^0_{B_a, M}(\overline{\mathrm{Ad}}\,\Delta) \simeq \mathrm{Mat}_d(B_a/M)$ whence $f^0_{B_a, M}(\overline{\mathrm{Ad}}\,\Delta)$ is absolutely irreducible. Since $f^0_{B_a, M}(\overline{\mathrm{Ad}}\,\Delta) \subseteq (\mathscr{D}^4 \Gamma'^{\langle m \rangle}_M)^{\langle r \rangle}$, it follows that Γ'_M satisfies the assumption of (3.1). Let N be the socle of $\Gamma'_M / C(\Gamma'_M)$.

By (3.1), there exist simply connected absolutely almost simple algebraic groups H_i, $1 \le i \le t$, each defined over a finite field $\mathbf{F}_{q_i}$, $q_i = p^{m_i}$, and a homomorphism $f: \prod_{1 \le i \le t} H_i(\mathbf{F}_{q_i}) \to G_{B_a}(B_a/M)$ with central kernel (the case of Suzuki and Ree groups is excluded by (8.1)) such that $(\overline{\mathrm{Ad}} \circ f)(\prod_{1 \le i \le t} H_i(\mathbf{F}_{q_i})) = \overline{\mathrm{Ad}}\,N$. We want to check that the conditions of (4.1) are satisfied with $g := \overline{\mathrm{Ad}}$.

Indeed, (4.1) (i) holds by (8.10), (4.1) (ii) holds by (8.8), and (4.1) (iii) holds by (8.9). The restrictions on the type of G in (4.1) (iv) are contained in (8.1). It remains to check that $m_i \ge e(1 + \mathrm{rank}\, G)$, $1 \le i \le t$, is satisfied. We have by (3.1) that

$$N \supseteq f^0_{B_a, M}\Big(\big(\mathscr{D}^4 \Gamma'^{\langle m \rangle}_M\big)^{\langle r \rangle}\Big)^{\langle r' \rangle} / (\text{center}) \supseteq f^0_{B_a, M}(\Delta)/(\text{center}).$$

Now if $m_j < e(d)$ for some j, then by definition of r' we have $(H_j(\mathbf{F}_{q_j}))^{\langle r' \rangle} \subseteq C(H_j)$, whence $f^0_{B_a, M}(\Delta)$ will not be absolutely irreducible (the same argument as in (3.8)). Thus the conditions of (4.1) are satisfied and, therefore, the conclusions of (4.1) hold: $t = 1$, G is defined over $\mathbf{F}_{q_1}$, and there exist an $\mathbf{F}_{q_1}$-isomorphism $\tilde{f}$: $H_1 \to G_{B_a/M}$ and $n \in \mathbf{N}$ such that $f \circ \mathrm{Fr}^n$ extends f. Thus $N = G(\mathbf{F}_q)/(\text{center})$ for some $q = p^m$. Since the central extension $G(\mathbf{F}_q)$ of N is a perfect group, we have that $\Gamma'_M = G(\mathbf{F}_q)$. By (8.6) (ii) we have $A'/(A' \cap M) = B_a/M$, whence $\mathbf{F}_q \simeq B_a/M$.

Now let I be an ideal of B_a such that B_a/I is finite. We shall check that the conditions of (7.1) hold with $A := B_a/I$. First, (7.1) (i) holds by our choice of a in the beginning of (8.11) and (7.1) (ii) follows from our assumption (8.1). Then (7.1) (iii) holds by the conclusions of the preceding paragraph and (7.1) (iv) holds since $\mathbf{Z}[\operatorname{tr}\operatorname{Ad} f^0_{B_a,I}(\Gamma')] = B_a/I$ in view of the Chinese remainder theorem and (8.6) (ii).

Thus $\varprojlim f^0_{B_a,I}(\Gamma') = \varprojlim G_{B_a}(B_a/I) = G_{B_a}(\hat{B}_a)$ where the inverse limits are taken over cofinite ideals of B_a. Thus (8.2) holds with $b = \bar{b}\tilde{b}\hat{b}ba$.

9. Some reformulations

(9.1) Our first result is an extension of (8.2) to semi-simple (simply connected) groups which are not necessarily absolutely almost simple. To formulate the result it is convenient to view the group $G \times G$ as the group G over the algebra $k \oplus k$.

Thus let $G_1, \dots, G_m$ be simply connected Chevalley group schemes over $\mathbf{Z}$ and let $k_1, \dots, k_m$ be algebraically closed fields. We can consider $G := \prod_{1 \le i \le m} G_i$ as a group scheme over $k := \oplus_{1 \le i \le m} k_i$; in general, it is not of constant type.

Let $c = c(G)$ denote the order of the schematic center of G so that $c(G) = \prod_{1 \le i \le m} c(G_i)$. Also if S is a group, write S^+_c for the group $(S^{\langle c^2 \rangle}\mathscr{D}S)^{\langle c^2 \rangle}\mathscr{D}(S^{\langle c^2 \rangle} \cdot \mathscr{D}S)$.

(9.1.1) THEOREM. *Let Γ be a subgroup of $G(k)$. Assume*

(a) *Γ is finitely generated.*

(b) *Projection of Γ on each G_i is Zariski-dense there.*

(c) *If G_i is of type G_2 (resp. B_n, C_n or F_4) then* $\operatorname{char} k_i \neq 3$ (*resp.* $\operatorname{char} k_i \neq 2$).

Then there exist $b \in A := \mathbf{Z}[\operatorname{tr}\operatorname{Ad}\Gamma]$, $b \in k^*$, and a structure G_{A_b} on G of a semi-simple group scheme over A_b such that

(i) *A_b is finitely generated;*

(ii) *$\Gamma^+_{c(G)} \subseteq G_{A_b}(A_b)$;*

(iii) *$\Gamma^+_{c(G)}$ is dense in $G_{A_b}(\hat{A}_b)$.*

Remark. This theorem can be proved in exactly the same way as (8.2). We will however, outline an approach which is somewhat simpler.

Let e_i be the identity of k_i and pr_i be the projection of k on k_i and of G on G_i.

(9.1.2) LEMMA. *There exists $b' \in A \cap k^*$ such that $A_{b'} = \oplus_{1 \le \alpha \le t} B_\alpha$ where the B_α are integral domains.*

Proof. Suppose that e is a minimal idempotent of A and that Ae has a zero divisor a. Let $S = \{i \mid 1 \le i \le m,\ ak_i = 0\}$. Then $\tilde{a} := a + \sum_{i \in S} e_i \in k^*$ and

$a/\tilde{a} \in A_{\tilde{a}}$ is an idempotent of A_e different from e. Repeating this process at most m times we find a b' satisfying the conclusions of (9.1.1).

Let K_i, $1 \leq i \leq t$, be the quotient field of B_i, let $\tilde{e}_i$ be its identity, and let $S_i := \{ j | 1 \leq j \leq m,\ \tilde{e}_i e_j \neq 0 \}$.

(9.1.3) Lemma. *For every* i, $1 \leq i \leq t$, *and any* j, $s \in S_i$:

(i) $\operatorname{char} k_j = \operatorname{char} k_s$;

(ii) G_j *is of the same type as* G_s.

Remark. A version of (9.1.3) (ii) was originally obtained jointly with C. Matthews as a part of intended joint work. I am grateful to him for his permission to use it here.

Proof. We have $\tilde{e}_i = \sum_{j \in S_i} e_j$. If $\operatorname{char} k_j = p_j$, $p_j \neq 0$, and $\operatorname{char} k_s = p_s$ and $p_j \neq p_s$ then $p_j \tilde{e}_i \neq 0$ whence it follows that $\tilde{e}_i$ is not a primitive idempotent of B_i in contradiction to assumptions.

Suppose now that for j, $s \in S_i$, the type of G_j differs from that of G_s. Consider $\Gamma_j := pr_j \Gamma \subseteq G_j$ and $\Gamma_s := pr_s \Gamma \subseteq G_s$. By (8.2) applied to both $\Gamma_j \subseteq G_j$ and $\Gamma_s \subseteq G_s$, there is a $b \in B_i$ such that for every maximal ideal M of $(B_i)_b$, reduction of $(\Gamma_i)_c^+ \bmod M$ is a universal finite group of the same type as G_i and similarly for G_s. Assuming that $|(B_i)_b/M| \geq 10$ (which can be achieved by additional localizations), we see that Γ projects on $\Delta_1 \times \Delta_2$ where Δ_1 and Δ_2 are universal groups of Lie type which are not isomorphic. Thus reduction of $\Gamma \bmod M$ contains a direct product of groups, whence the ring $((B_i)_b/M)[\operatorname{tr} \operatorname{Ad} \Gamma]$ is not a field, in contradiction to either the maximality of M or the integrity of B_i.

(9.1.4) *Proof of* (9.1.1). Replacing k_i by $\overline{K}_j$, we are now in the situation where we can apply (8.2) to each factor $(G_i, pr_i \Gamma)$. After having done that, we note that we have the conditions of (7.1) with the only difference that G now is not of constant type. But the proof of (7.2) goes through anyway in this slightly more general case.

(9.2) Let A be a finitely generated integral domain and G an absolutely almost simple simply connected semi-simple group scheme over A. Let Γ be a subgroup of $G(A)$ such that the field of quotients $A \cdot A^{-1}$ of A coincides with that of $\mathbf{Z}[\operatorname{tr} \operatorname{Ad} \Gamma]$. For $s \in \operatorname{Spec} A$, let $k(s)$ be the residue field of s and Γ_s be the image of Γ in $G(k(s))$.

(9.2.1) Theorem. *Assume that* G *is not of type* G_2 *if* $\operatorname{char}(A \cdot A^{-1}) = 3$ *and not of type* B_n, C_n, F_4 *if* $\operatorname{char}(A \cdot A^{-1}) = 2$. *If* $\{ s \in \operatorname{Spec} A | \dim s = 0$ *and* $\Gamma_s \neq G(k(s)) \}$ *is Zariski-dense in* $\operatorname{Spec} A$ *then* Γ *is not Zariski-dense in* G.

Proof. If Γ is finitely generated and Zariski-dense then, by (8.2), there exists an open $U \subseteq \operatorname{Spec} A$ such that $\Gamma_s = G(k(s))$ for all closed points $s \in U(A)$.

Hence our claim holds for a finitely generated Γ. Reduction to this case is done as in the proof of (8.6).

(9.3) Now let Γ be a finitely generated subgroup of $GL_n(k)$ where k is an algebraically closed field of characteristic $\neq 2$ or 3.

(9.3.1) THEOREM. *There exist a subgroup Γ' of finite index in Γ, a finitely generated ring A, a simply connected semisimple group scheme G over A, and a homomorphism f: $\Gamma' \to G(A)/C(G(A))$ such that*

(i) $\operatorname{Ker} f$ *is solvable;*

(ii) $\operatorname{Im} f$ *is dense in $G(\hat{A})/C(G(\hat{A}))$.*

Proof. Let H be the Zariski closure of Γ in GL_n. Take $\Delta := \Gamma \cap H^0$; Δ is finitely generated because Γ is and $|\Gamma/\Delta| = |H/H^0| < \infty$. Let R be the radical of H^0. Then $\bar{G} := H^0/R$ is semi-simple and adjoint. Let f: $H^0 \to \bar{G}$ be the projection. Since $\operatorname{Ker} f \subseteq R$, it is solvable. Let $\bar{\Gamma} := f(\Delta)$; it is Zariski-dense in $\bar{G}$.

Let G be the universal cover of $\bar{G}$ and π: $G \to \bar{G}$ the corresponding map. Let $\bar{\gamma}_1, \ldots, \bar{\gamma}_t$ be generators of $\bar{\Gamma}$ (it is finitely generated since Δ is). Let $\tilde{\gamma}_i \in \pi^{-1}(\bar{\gamma}_i)$, $1 \leq i \leq t$. Set $\tilde{\Gamma} := \langle \tilde{\gamma}_1, \ldots, \tilde{\gamma}_t \rangle$. Since $\bar{\Gamma}$ is Zariski dense, so is $\tilde{\Gamma}$. By (9.1.1) there exist a finitely generated ring A (denoted A_b in (9.1.1)) and a structure G_A of a semi-simple group scheme G_A on G such that $\tilde{\Gamma} \cap G_A(A)$ is dense in $G_A(\hat{A})$ and $\tilde{\Gamma}' := \tilde{\Gamma} \cap G_A(A)$ is of finite index in $\tilde{\Gamma}$. Setting $\Gamma' := f^{-1}(\pi(\tilde{\Gamma}'))$, we obtain our claim.

(9.3.2) *Amplification.* If $\operatorname{char} k = 0$ then there exists a function ε: $\mathbf{N}^+ \to \mathbf{N}^+$ such that for every Γ as in (9.3.1) there exist (in addition to A, G, Γ', f having properties (i) and (ii) of (9.3.1)) normal subgroups Γ_1 and Γ_2 of Γ with $\Gamma \supseteq \Gamma_1 \supseteq \Gamma' \supseteq \Gamma_2$ and

(iii) $|\Gamma/\Gamma_1| \leq \varepsilon(n)$,

(iv) $\mathscr{D}^3(\Gamma_1/\Gamma_2) = \{1\}$.

Proof. We use notation of the proof of (9.3.1). By [Ba 2] we know that H/H^0 contains an abelian normal subgroup M of index $\leq \varepsilon(n)$ with appropriate ε. We have by construction that $\Gamma/(\Gamma \cap H^0) \simeq H/H^0$. Let Γ_1 be the preimage of M in Γ. It is a normal subgroup of Γ of index $\leq \varepsilon(n)$. So it is finitely generated since Γ is. Let m be the exponent of M. Then $N := (\Gamma_1)_m^+$ is a characteristic normal subgroup of Γ_1, whence it is normal in Γ. Γ_1/N is a commutative group of exponent m; since it is finitely generated it is finite. Therefore N is finitely generated. By construction $N \subseteq H^0$ and since $\Gamma \cap H^0$ is Zariski-dense and $(\Gamma \cap H^0)/N < \infty$, it follows that N is also Zariski-dense.

Let G, $\bar{G}$, f, and π be the same as in the proof of (9.3.1). Let $n_1, \ldots, n_t$ be a set of generators of N, let $\tilde{n}_i \in \pi^{-1}(n_i)$, $1 \leq i \leq t$, and let $\tilde{N} = \langle \tilde{n}_1, \ldots, \tilde{n}_t \rangle$.

Then by (9.1.1), the characteristic normal subgroup $\tilde{N}_2 := N^+_{c(G)}$ is contained in $G(A)$ and dense in $G(\hat{A}_b)$. The group $\Gamma_2 = \pi(\tilde{N}_2)$ clearly has the desired property.

Remark. Actually one can take $\pi(N^{\langle c\rangle} \cdot \mathscr{D}N)$ for Γ_2 because we factor the center out anyway.

(9.4) Let G be an algebraic semi-simple simply connected $\mathbf{R}$-group such that $H := G(\mathbf{R})$ has no compact factors. Let K be a maximal compact subgroup of H and $X := H/K$. Let Γ be an irreducible torsion-free lattice subgroup of H and $Y := \Gamma \backslash X$ so that Y is a locally symmetric space of finite volume. Write $G = G_1 \times G_2 \times \cdots \times G_m$, a product of $\mathbf{R}$-groups. Suppose the G_i, $1 \le i \le n$, are absolutely almost simple, and $G_i = R_{\mathbf{C}/\mathbf{R}} G_i'$, $n+1 \le i \le m$, where the $\mathbf{C}$-groups G_i' are absolutely almost simple.

(9.4.1) THEOREM. *If $m = 1$ assume that $G \neq \mathrm{SL}_{2,\mathbf{R}}$. There exist a number field k with the ring of integers A, $a, b \in A$, an absolutely almost simple simply connected group scheme $\mathscr{G}_{A_b}$ over A_b with G being an $\mathbf{R}$-factor of*

$$\left(R_{k/\mathbf{Q}}\left(\mathscr{G}_{A_b} \otimes k\right)\right) \otimes \mathbf{R}$$

and a finite cover $Y' \to Y$ with solvable group such that for any ideal I of A_b there is a cover $Y'' \to Y'$ with the group $\mathscr{G}_{A_b}(A_b/I)$.

Proof. If $rk_{\mathbf{R}} G = 1$ then by [GR, Theorem 0.11], we have that $\mathbf{Q}[\mathrm{tr\,ad}\,\Gamma]$ is a number field and by [R, Corollary 13.20], Γ is finitely generated. The same (and more!) holds in the case $rk_{\mathbf{R}} G > 1$ by a result of D. Kazhdan (finite generation) and G. Margulis (arithmeticity) (see [M]). By A. Borel's density theorem (see [B1] and [B2]) Γ is Zariski-dense and, therefore, (9.1.1) is applicable. It, together with the inclusion $A \subseteq \mathbf{Q}[\mathrm{tr\,Ad}\,\Gamma]$, implies our claim (take $Y' := \Gamma' \backslash X$, and, for $\Gamma'' := \mathrm{Ker}\{\mathscr{G}_{A_b}(A) \to \mathscr{G}_{A_b}(A_b/I)\}$ take $Y'' := \Gamma'' \backslash X$).

(9.4.2) *Remarks.* (i) The above proof needed only finite generation of Γ, Zariski-density of Γ in G, and local rigidity of Γ. Therefore the claim also holds for finitely generated, Zariski-dense, torsion-free Γ such that $H^1(\Gamma, \mathrm{Ad}) = 0$ (see [R, Theorem 6.7]).

(ii) (9.4.1) follows directly from Margulis' super rigidity (see [M]) if $rk_{\mathbf{R}} G > 1$. Indeed, Γ is then arithmetic and our claim reduces to the usual strong approximation theorem.

10. The one dimensional case

Let k be a global field (i.e. either a number field or a field of functions on a curve over $\mathbf{F}_q$ for some q). Assume (8.1). Let o be the ring of integers of k and V the set of all inequivalent valuations of k. Let V_a be the set of archimedean valuations of k. For $v \in V - V_a$, let k_v denote the completion of k at v, o_v the

ring of integers in k_v, and p_v the residual characteristic of o_v. We use $\prod^{\text{res}}_{v \in S} k_v$ to denote the restricted product of the k_v over $v \in S \subseteq V$. For a subset T of V we set $k_T := \prod^{\text{res}}_{v \in T} k_v$ and $o_T := \prod_{v \in T} o_v$.

Recall that k_v is a locally compact field with o_v open in k_v and k_T is a topological ring with o_T open in it.

Let G be an absolutely almost simple algebraic k-group. For any k-group H, $H(k_v)$ is a locally compact topological group with $H(o_v)$ open in $H(k_v)$. If k is a number field then $H(k_v)$ is an analytic group over $\mathbf{Q}_{p_v}$ and so is every closed subgroup of $H(k_v)$. The analytic $\mathbf{Q}_{p_v}$-groups have Lie algebras which are Lie algebras over $\mathbf{Q}_{p_v}$. We use U (with any modifiers) to denote an open neighborhood of the identity in the topological group in question.

(10.1) THEOREM. *Let G be an absolutely almost simple simply connected algebraic group over k. Suppose that* $\operatorname{char} k \neq 3$ *if G is of type G_2 and* $\operatorname{char} k \neq 2$ *if G is of type $B_n (n \geq 1)$, $C_n (n \geq 1)$, or F_4. Let Γ be a Zariski dense subgroup of G such that $\Gamma \subseteq G(k)$ and the subfield of k generated by* $\operatorname{tr} \operatorname{Ad} \Gamma$ *is k itself. Then there exists a finite set S, $S \supseteq V_a$, such that the closure of Γ in $G(\prod^{\text{res}}_{v \notin s} k_v)$ is open.*

Proof. Let $\gamma_1, \ldots, \gamma_n$ be elements of Γ chosen so that $\tilde{\Gamma} := \langle \gamma_1, \ldots, \gamma_n \rangle$ is Zariski-dense in G (possible since $\dim G < \infty$) and the field generated by $\operatorname{tr} \operatorname{Ad} \tilde{\Gamma}$ is k (possible since k is finitely generated). Then by (8.2), there exists $b \in o$ such that $\operatorname{tr} \operatorname{Ad} \Gamma \subseteq o_b$ (= localization of o at b) and such that $\tilde{\Gamma}$ is dense in $G_{o_b}(\hat{o}_b)$. Let S be the finite subset of V consisting of the archimedean valuations and of such v that $b \notin o_v$. Then the above says that $\tilde{\Gamma}$ is dense in $G_{k_{V-S}}(o_{V-S})$; since this latter group is open in $G_{k_{V-S}}(k_{V-S})$, we get our claim.

Now we want to obtain the strongest approximation theorem possible for our methods. To this end, we use the following observation from the proof of Lemma 2.1 in [P].

(10.2) LEMMA. *Let K be a locally compact ring, H an algebraic group scheme over K, and Γ a subgroup of (the locally compact group) $H(K)$. Then there exists an open neighborhood U of the identity of $H(K)$ such that for any U', $U' \subseteq U$, the Zariski closure of $\Gamma \cap U'$ is normalized by the Zariski closure of Γ.*

We recall our convention that U with any modifiers always denotes an open neighborhood of the identity in the group in question.

Proof. Let $H_{\tilde{U}}$ be the Zariski closure of $\Gamma \cap \tilde{U}$. Since $H_{\tilde{U}} \supseteq H_{\tilde{U}'}$ when $\tilde{U} \supseteq \tilde{U}'$ and by the Noetherian property of the algebraic varieties, it follows that there exists a U such that the Zariski closures of $\Gamma \cap U$ and $\Gamma \cap U'$ coincide for all $U' \subseteq U$. For any $\gamma \in \Gamma$ there exists then a U_γ so small that $\gamma U_\gamma \gamma^{-1} \subseteq U$.

Thus $\gamma(U_\gamma \cap \Gamma)\gamma^{-1} \subseteq U \cap \Gamma$, and since the Zariski closures of $U \cap \Gamma$ and $U_\gamma \cap \Gamma$ coincide, it follows that γ normalizes this Zariski closure.

(10.3) LEMMA. *Let k be a global field, G an absolutely almost simple algebraic group defined over k, Γ a Zariski-dense (in G) subgroup of $G(k)$ such that the field generated by* $\operatorname{tr}\operatorname{Ad}\Gamma$ *is k. Let $S \subseteq V$, $S \supseteq V_a$. Then either Γ is discrete in $G(k_{V-S})$ or there exists a $U \subseteq G(k_{V-S})$ such that for any $U' \subseteq U$, $\Gamma \cap U'$ is Zariski-dense in G and the field generated by* $\operatorname{tr}\operatorname{Ad}(\Gamma \cap U')$ *is k.*

Proof. Take U as in (10.2) for $K = k_{V-S}$ and $H = G$. Assume (as we may) that U is a subgroup. Since the Zariski closure of $U \cap \Gamma$ is normalized by G (which is the Zariski closure of Γ) and since G is absolutely almost simple it follows that if Γ is not discrete in $G(k_{V-S})$ then $U \cap \Gamma$ is Zariski-dense in G. Let k' be the field generated by $\operatorname{tr}\operatorname{Ad}(\Gamma \cap U')$ for a $U' \subseteq U$; k' is not finite since otherwise $\Gamma \cap U'$ would be finite (by [Ba1, Corollary 1.3(a)]) and this would contradict the Zariski-density of $\Gamma \cap U'$. (Note that we used the fact that $\Gamma \cap U'$ is a group.)

Therefore $[k: k'] < \infty$. As in the proof of (8.6) (ii), it follows that G has a structure $G_{k'}$ of a k'-group such that $\operatorname{Ad}(\Gamma \cap U') \subseteq \operatorname{Ad} G(k')$. Let us replace G by $\operatorname{Ad} G$ (which does not affect either assumptions or conclusions). Let $G' := R_{k/k'}G$. (Note that G' is not semi-simple if k/k' is not separable.) Since G is defined over k' we have the natural k'-homomorphism s: $G \to G'$ (induced by $k' \to R_{k/k'}k$). Let s^0: $G(k') \to G'(k')$ and $R^0_{k/k'}$: $G(k) \to G'(k')$ be the homomorphisms of groups of points induced by s and $R_{k/k'}$. For a sufficiently small $\tilde{U}$, open in $G'(k')$, we have that the Zariski closure of $\tilde{U} \cap R^0_{k/k'}\Gamma$ is normalized by $R^0_{k/k'}\Gamma$ (by (10.2)) and contained in $s(G)$ by construction. Thus $R^0_{k/k'}\Gamma \subseteq N_{G'}(s(G))$.

The unipotent radical $R_u G'$ of G' is isomorphic over $\bar{k}'$ to a direct sum of a number of copies of $\operatorname{Lie} G$ on each of which $s(G)$ acts via the adjoint representation, and $G'/R_u G'$ is isomorphic to a direct product of a number of copies of G in which $s(G)$ is embedded diagonally. Then by simplicity of G one easily establishes that $N_{G'/R_u G'}(s(G)) = s(G)$ and that $N_{R_u G'}(s(G)) = \{1\}$ whence $N_{G'}(s(G)) = s(G)$; that is, $R^0_{k/k'}\Gamma \subseteq s(G)$. Since $R^0_{k'/k}\Gamma \subseteq G'(k')$, it follows that $R^0_{k/k'}\Gamma \subseteq G'(k') \cap s(G) = s(G)(k')$. Thus, since s was a k'-map, we have $\Gamma \subseteq G(k')$, whence $\operatorname{tr}\operatorname{Ad}\Gamma \subseteq k'$, whence $k' = k$ as claimed.

(10.4) COROLLARY. *Let k, G, and Γ be as* (10.3). *There exists a finite $S \subseteq V$, $S \supseteq V_a$, such that $\tilde{\Gamma} := \Gamma \cap G(o_{V-S})$ has the following properties:*

(i) *$\tilde{\Gamma}$ is Zariski-dense in G;*

(ii) *$\tilde{\Gamma}$ is discrete in $G(k_w)$ for any finite $w \in S$;*

(iii) *The fields generated by* $\operatorname{tr}\operatorname{Ad}\Gamma$ *and* $\operatorname{tr}\operatorname{Ad}\tilde{\Gamma}$ *are the same.*

Proof. For any $T \subseteq V$, set $\tilde{\Gamma}_T := \Gamma \cap \prod_{v \in T} G(o_v)$. By (10.3) there exists a finite S' having properties (i) and (iii). Since for $w \in S'$ the projection of $G(k_w) \times G(o_{V-S'}) \to G(k_w)$ has compact kernel, it follows that if Γ is discrete in $G(k_w) \times G(o_{V-S'})$, it is also discrete in $G(k_w)$. Therefore if (ii) does not hold with $w \in S'$, then Γ is not discrete in $G(k_w) \times G(o_{V-S'})$. Applying (10.3) with $S := S' - \{w\}$, we get that $\Gamma \cap G(o_{V-S})$ still has properties (i) and (iii). Since S' is finite it follows that after a finite number of steps it will become impossible to carry on the above procedure. At this point (ii) will hold as well.

(10.5) THEOREM. *Let k be a number field, G an absolutely almost simple simply connected algebraic group defined over k, Γ a Zariski-dense (in G) subgroup of $G(k)$, such that the field generated by* $\operatorname{tr} \operatorname{Ad} \Gamma$ *is k. Then there exists a finite S, $V_a \subseteq S \subseteq V$, such that:*

(i) *The closure of Γ is open in $G(k_{V-S})$ and*

(ii) *$\Gamma \cap G(o_{V-S})$ is discrete and Zariski-dense in $G(k_w)$ for each $w \in S - V_a$.*

Remark. Our work on (10.5) was started jointly with C. Matthews and the ideas of our proof were developed at that time. I am grateful to C. Matthews for his permission to use them here.

Proof. Take S as in (10.4) and $\tilde{\Gamma} := \Gamma \cap G(o_{V-S})$. Then $\tilde{\Gamma}$ is Zariski-dense in G by (10.4) (i) and, therefore, by (10.1) the closure of $\tilde{\Gamma}$ in $G(o_{V-(T \cup S)})$ is equal to $G(o_{V-(T \cup S)})$ for some finite $T \subseteq V - S$. Extend T so that in addition to the above properties (i) it will contain all $v \in V - S$ such that $p_v = p_w$ for some $w \in T$, and (ii) G is quasi-split over k_v and split by an unramified extension of k_v if $v \in V - S - T$. Since $\tilde{\Gamma}$ is Zariski-dense it is infinite and since $G(o_T)$ is compact, $\tilde{\Gamma}$ is not discrete in $G(o_T)$. Since the field generated by $\operatorname{tr} \operatorname{Ad} \tilde{\Gamma}$ is k which is dense in k_T it follows that the projection of $\tilde{\Gamma}$ on every direct factor $G(o_w)$, $w \in T$, of $G(o_T)$ is not discrete. Let H_T be the closure of $\tilde{\Gamma}$ in $G(o_T)$. It is a $\mathbf{Q}_T$ $(= \prod_{w \in T} \mathbf{Q}_{p_w})$-analytic group. Let L be the Lie algebra of H_T considered as an analytic group; L is a Lie algebra over $\mathbf{Q}_T$. Consider it as a subalgebra of $(\operatorname{Lie} G)(k_T)$. The $\mathbf{Q}_T$-subalgebra of $\operatorname{End}_{k_T}((\operatorname{Lie} G)(k_T))$ generated by $\operatorname{Ad} \tilde{\Gamma}$ contains (by (10.4) (iii)) k_T. Thus L is actually a k_T-subalgebra of $(\operatorname{Lie} G)(k_T)$ which has nontrivial projection on every $(\operatorname{Lie} G)(k_w)$, $w \in T$. Since it is invariant under $\operatorname{Ad} \tilde{\Gamma}$ and since $\tilde{\Gamma}$ is Zariski-dense in G, it follows that L is $\operatorname{Ad} G$-invariant and by simplicity of $(\operatorname{Lie} G)(k_w)$ it follows that $pr_w L = (\operatorname{Lie} G)(k_w)$. Therefore, since L is a k_T-algebra, we have $L = (\operatorname{Lie} G)(k_T)$.

Since $(\operatorname{Lie} G)(k_T) = \operatorname{Lie} H_T$ it follows that the analytic $\mathbf{Q}_T$-groups $G(k_T)$ and H_T share a common neighborhood of identity; i.e. H_T is open in $G(k_T)$. Let H be the closure of $\tilde{\Gamma}$ in $G(o_{V-S})$. We know that $pr_T H$ is open in $G(k_T)$ and

$pr_{V-(T\cup S)}H = G(o_{V-(T\cup S)})$. Write pr_1 for pr_T, pr_2 for $pr_{V-(S\cup T)}$, and H_i for $pr_i H$, $i = 1, 2$. We consider H as a subgroup of $H_1 \times H_2$. Take $h \in H_1$ and let $\tilde{h} \in pr_1^{-1}h \subset h \times H_2$. Then set $\bar{h} := pr_2\tilde{h}$. Then we can consider $\bar{h}$ as an element of $H_2/H \cap H_2$. This defines an homomorphism φ: $H_1 \to H_2/H \cap H_2$. Since $\{p_v, v \in T\} \cap \{p_v, v \in V - (S \cup T)\} = \varnothing$ and since every $G(o_v)$ is virtually a pro-p_v-subgroup it follows that φ is trivial on a subgroup $\tilde{H}_1$ of finite index in H_1. Let $\tilde{H}$ be the preimage of $\tilde{H}_1$ in H. Then $\varphi(\tilde{H}_1) = \{1\}$, whence $\tilde{H} \cap H_2 = pr_2\tilde{H}$. This establishes our claim.

(10.6) COROLLARY. *With the assumptions of* (10.5), *if* $\Gamma \subseteq G(o_{V-\tilde{S}})$ *for some finite* $\tilde{S} \subseteq V$, $\tilde{S} \supseteq V_a$, *then the closure of* Γ *in* $G(o_{V-\tilde{S}})$ *is open.*

Proof. Since Γ is Zariski-dense it cannot be discrete in the compact group $G(o_{V-\tilde{S}})$. Since $\Gamma = \Gamma \cap G(o_{V-\tilde{S}})$, it follows that S as constructed in the proof of (10.5) contains $\tilde{S}$, whence our claim.

(10.7) COROLLARY. *With the assumptions of* (10.5), *assume that* Γ *contains a unipotent element. Then the closure of* Γ *in* $G(k_{V-V_a})$ *is open.*

Proof. The subgroup generated by a unipotent element is never discrete in $G(k_{V-V_a})$. Therefore $\Gamma \cap G(o_{V-V_a})$ is not discrete, whence our claim in view of (10.5).

11. On the profinite completion of some arithmetic cocompact lattices in SO(n, 1)

Let $k := \mathbf{Q}(\sqrt{p})$ where p is a rational prime, let A be the ring of integers of k, and $f := -\sqrt{p}\,x_0^2 + \sum_{1\le i\le n} x_i^2$ a quadratic form over k. Denote by $G :=$ SO(f,) the special orthogonal group of f; it is a group scheme over A. By [R, Theorem 6.15] the group $G(A)$ is finitely generated. The constructions of this section are based on Millson's report on [JM] at a seminar at Harvard; I am grateful for his permission to use them here.

(11.1) THEOREM. *With* N *an integer* ≥ 1, *there exist subgroups* Γ_N *and* Γ'_N *of finite index in* $G(A)$ *such that* $\hat{\Gamma}_N$ *has* $\mathrm{Spin}(f_N, \hat{R}_F)/(\mathit{center})$ *and* $\hat{\Gamma}'_N$ *has* $\mathrm{SL}_{n+N+3}(\hat{R}'_{F'})$ *as quotients. Here*

$$R = A\left[t_1, t_1^{-1}, \ldots, t_{[(N+1)/2]}, t_{[(N+1)/2]}^{-1}\right] \text{ and } F \in R;$$

$$R' = A\left[t_1, \ldots, t_{2[(N+1)/2]-1}, \left(t_1 t_2 \cdots t_{2[(N+1)/2]-1}\right)^{-1}\right] \text{ and } F' \in R';$$

$$f_N = -\sqrt{p}\,x_0^2 + \sum_{1\le i\le N+n} x_i^2.$$

This shows the extent to which the congruence subgroup property fails to hold for $G(A)$; that it does not hold is known from [Mi].

In our proof of (11.1) we shall construct Zariski-dense embeddings of a congruence subgroup Γ of $G(A)$ into $\mathrm{SO}_{n+N+1}(\mathbf{C})$ and into $\mathrm{SL}_{n+N+3}(\mathbf{C})$ thus proving:

(11.2) THEOREM. *A cocompact lattice in* $\mathrm{SO}(n,1)$ *has faithful homomorphisms, with Zariski-dense image into infinitely many nonisomorphic almost simple algebraic* **C***-groups.*

Remark. "Infinitely many" in the statement above can be most probably replaced by "almost all up to isomorphism".

Theorem (11.2) exhibits again how properties of the irreducible lattices in rank ≥ 2 Lie groups fail miserably in rank 1. In this case Margulis' super-rigidity (a homomorphism with Zariski-dense but not relatively compact image into a simple Lie group extends to a homomorphism of Lie groups, see [M]) does not hold. (Cf. [W2, (5.6), (7.2)] for a discussion of other differences between rank 1 and rank ≥ 2 cases.)

We fix an embedding of k into $\mathbf{C}$. Let $\mathbf{R}$ be the subfield of real numbers in $\mathbf{C}$. Let $V := \mathbf{R}^{n+1}$ with basis $e_0, \ldots, e_n$ and assume that f has the given form in this basis. Consider $V' := \sum_{i \leq n-1} \mathbf{R}e_i$ and let G' be the special orthogonal group of $f' := -\sqrt{p}\, x_0^2 + \sum_{i \leq n-1} x_i^2$. Then $G(\mathbf{R}) \simeq \mathrm{SO}(n,1)$, $G'(\mathbf{R}) \simeq \mathrm{SO}(n-1,1)$. Let $K = G(\mathbf{R}) \cap \mathrm{GL}(\sum_{1 \leq i \leq n} \mathbf{R}e_i)$; it is a maximal compact subgroup of $G(\mathbf{R})$ and $K' = G'(\mathbf{R}) \cap K$ is a maximal compact subgroup of $G'(\mathbf{R})$. Let $H := G(\mathbf{R})/K$ and $H' := G'(\mathbf{R})/K'$; these are hyperbolic symmetric spaces and H' (which we consider embedded in H) is a totally geodesic subspace of H. J. Millson introduced (in [Mi]) geometric methods for studying $G(A) \backslash H$. Namely, he has shown that for an appropriate torsion-free congruence subgroup Γ of $G(A)$, the $(n-1)$-dimensional submanifold $M := (\Gamma \cap G'(\mathbf{R})) \backslash H'$ does not separate $X := \Gamma \backslash H$. Therefore $[M]$ is a non-trivial cohomology class in $H^{n-1}(X, \mathbf{R})$. Since X is compact, by Poincaré duality there exists a loop s which represents the dual class, $[s] \in H^1(X, \mathbf{R})$.

Recall that H and H' are simply connected and therefore $\pi_1(X) \simeq \Gamma$ and $\pi_1(M) \simeq \Gamma'$. Now Millson's results on $[M]$ and $[s]$ permit one to give a presentation for Γ. Let $Y := X - M$, let U_M and U_s be small tubular neighborhoods of M and S, and let $Z := U_M \cup U_s$. Then Z, Y, and $Y \cap Z$ are connected and open in X and $X = Y \cup Z$. Take a base point on s. Then by the van Kampen theorem [O, Corollary to Theorem II], $\pi_1(X) \simeq \pi_1(Y) *_{\pi_1(Y \cap Z)} \pi_1(Z)$ (free product with an amalgamated subgroup). Let us identify two copies of M in $Y \cap Z$ via retraction of U_M to M. Now note that $Z \cap Y$ retracts to $M \vee M$ (one-point joint of M with M). Therefore $\pi_1(Y \cap Z) \simeq \pi_1(M) * \pi_1(M)$. Similarly

Z retracts to $M \vee s$ whence $\pi_1(Z) \simeq \pi_1(M) * \langle s \rangle$. Now we have to describe the maps α and β induced by the natural embeddings of $\pi_1(Y \cap Z)$ into $\pi_1(Y)$ and $\pi_1(Z)$. Because of our identification of copies of M in $Y \cap Z$ we have that α: $\pi_1(Y \cap Z) \to \pi_1(Z)$ is given by $\alpha(c_1 * c_2) = c_1 c_2^{-1} * s^0 \in \pi_1(Z)$ for $c_1, c_2 \in \pi_1(M)$. Now the map β: $\pi_1(Y \cap Z) \to \pi_1(Y)$ is given by two homomorphisms φ_i: $\pi_1(M) \to \pi_1(Y)$, $i = 1, 2$, so that $\beta(c_1 * c_2) = \varphi_1(c_1)\varphi_2(c_2^{-1})$. For the composite map $\pi_1(Y \cap Z) \to \pi_1(Y) \to \pi_1(X)$ which we denote ω, we can assume that $(\omega \circ \varphi_1)(c) = c$. Then $(\omega \circ \varphi_2)(c) = scs^{-1}$. Thus the van Kampen theorem gives us

(11.3) LEMMA. *Γ has a presentation*

$$\Gamma = \langle \omega(\pi_1(Y)), s | scs^{-1} = \omega(\varphi_2(c)) \text{ for } c \in \Gamma' \rangle$$

where φ_2: $\Gamma' \to \omega(\pi_1(Y)) \subseteq \Gamma$ is a homomorphism.

Set $\Delta := \omega(\pi_1(Y)) \subseteq \Gamma$ and let n: $\Gamma \to G(\mathbf{R})$ denote the natural embedding.

(11.4) LEMMA. *$n(\Delta)$ is Zariski-dense in G.*

Proof. We saw that ω: $\Gamma' * 1 \xrightarrow{\sim} \Gamma' \subseteq \Gamma$ (where $\pi_1(Y)$ is identified with $\Gamma' * \Gamma'$). Since Γ' is Zariski-dense in G' (by [B1] or [B2]) it follows that the Zariski closure of $n(\Delta)$ contains G'. Since $sG's^{-1} \neq G'$ because $s\Gamma's^{-1} = \omega(1 * \Gamma') \subset \Delta$, and since G' is a maximal connected subgroup of G, it follows that our claim is true.

Now embed V into an inner product space $\mathbf{R}^{n+N+1}$ by adding new orthonormal vectors $e_{n+1}, \ldots, e_{n+N}$ and assuming that they are orthogonal to V. Define $r_0 = 0$, $r_1 = 1$, $r_{i+1} = r_{i-1} + r_i^2 + 1$. Define for $t \leq (N+1)/2$,

$$\tilde{e}_{2t-1} = e_n - \sum_{i=0}^{2t-2} r_i e_{n+i} + e_{n+2t-1},$$

$$\tilde{e}_{2t} = e_n - \sum_{i=0}^{2t-1} r_i e_{n+i} + e_{n+2t},$$

where we assume that $e_{n+N+1} = 0$. Set $P_t = \mathbf{R}\tilde{e}_{2t-1} + \mathbf{R}\tilde{e}_{2t}$ for $1 \leq t \leq (N+1)/2$.

(11.5) LEMMA. (i) *The P_i are mutually orthogonal;*
(ii) *The P_i are orthogonal to V';*
(iii) *Each P_i has a non-trivial projection on $\mathbf{R}e_n$.*

Set $d := [(N+1)/2]$. Let σ_i be an orthogonal transformation in the plane P_i, $i = 1, \ldots, d$. The Thurston bending (see [JM]) of Γ in SO_{n+N+1} is the group

$$\Gamma(\sigma_1, \ldots, \sigma_d) := \langle n(\Delta), n(s)\sigma_1 \cdots \sigma_d \rangle \subseteq \mathrm{SO}_{n+N+1}.$$

(11.6) LEMMA. *The map* $c \mapsto n(\omega(c))$ *for* $c \in \pi_1(Y)$, $s \mapsto n(s)\sigma_1 \cdots \sigma_d$, *defines a homomorphism of* Γ *onto* $\Gamma(\sigma_1, \ldots, \sigma_d)$.

Proof. It is sufficient to verify that the above map preserves the defining relations of Γ from (11.3). But since the σ_i commute with Γ' (by (11.5) (ii)) we have

$$n(s)\sigma_1 \cdots \sigma_d \cdot n(c) \cdot \sigma_d^{-1} \cdots \sigma_1^{-1} n(s^{-1}) = n(s)n(c)n(s^{-1})$$
$$= n(scs^{-1}) = n(\varphi_2(c))$$

and the relation holds since $\varphi_2(c) \subset \Delta$ and Δ is not bent.

Pick d independent transcendental numbers $t_1, \ldots, t_d \in \mathbf{C}$ and define $\tilde{\sigma}_i \in \mathrm{GL}(P_i)$ by $\tilde{\sigma}_i := \begin{pmatrix} t_i & 0 \\ 0 & t_i^{-1} \end{pmatrix}$ in the basis $\{\tilde{e}_{2i-1} + \tilde{e}_{2i}, \tilde{e}_{2i-1} - \tilde{e}_{2i}\}$ of P_i. Then $\tilde{\sigma}_i \in \mathrm{SO}_{n+N+1}$.

(11.7) LEMMA. $\tilde{\Gamma} := \Gamma(\tilde{\sigma}_1, \ldots, \tilde{\sigma}_d)$ *is Zariski-dense in* SO_{n+N+1}.

Proof. Note first that by the definition of the Thurston bending, $n(\Delta)$ remains unbent and, therefore (by (11.4)) the Zariski closure of $\tilde{\Gamma}$ contains $G \simeq \mathrm{SO}_{n+1}$. Since $n(s) \in \mathrm{SO}_{n+1}$, it follows that the Zariski closure of $\tilde{\Gamma}$ contains $\tilde{\sigma}_1 \cdots \tilde{\sigma}_d$. Since there are no algebraic relations (sufficient: no relations which are monomials) between eigenvalues of the different $\tilde{\sigma}_i$, $1 \le i \le d$, it follows that the Zariski closure of $\langle \tilde{\sigma}_1 \cdots \tilde{\sigma}_d \rangle$ contains the product of orthogonal groups $\mathrm{SO}(P_i)$ of the P_i. And then it is routine to verify (by (11.5) (i) and (iii)) that the $\mathrm{SO}(P_i)$ together with G generate SO_{n+N+1}.

Let now $\bar{t}_1, \ldots, \bar{t}_{2d-1}$ be independent transcendental numbers, $\bar{t}_{2d} := (\bar{t}_1 \cdots \bar{t}_{2d-1})^{-1}$, and define $\bar{\sigma}_i$, in the basis $\tilde{e}_{2i-1}, \tilde{e}_{2i}$ of P_i by $\bar{\sigma}_i = \begin{pmatrix} \bar{t}_{2i-1} & 0 \\ 0 & \bar{t}_{2i} \end{pmatrix}$. Define Thurston bending in SL_{n+N+1} in exactly the same way as before, permitting, however, arbitrary $\sigma_i \in \mathrm{GL}(P_i)$.

(11.8) LEMMA. $\bar{\Gamma} := \Gamma(\bar{\sigma}_1, \ldots, \bar{\sigma}_d)$ *is Zariski-dense in* SL_{n+N+1} *if* $N \ge 3$.

Proof. As in the proof of (11.7), we have at once that G and the group of all diagonal, in the basis $\{\tilde{e}_i\}$, transformations of $\sum_{1 \le i \le N} \mathbf{C}\tilde{e}_i$ is contained in the Zariski closure of $\bar{\Gamma}$. By use of the maximality of SO_{n+1} in SL_{n+1}, it is not difficult then to derive our claim.

(11.9) *Proof of* (11.1) *and* (11.2). Let us consider only the case of SO_{n+N+1}. By construction $\tilde{\Gamma}$ is Zariski-dense in SO_{n+N+1}. Specialization $t_i \to 0$, $i = 1, \ldots, d$, gives us a homomorphism of $\tilde{\Gamma}$ onto Γ; by (11.6) it is an isomorphism. Since the orthogonal groups $\mathrm{SO}(P_i)$ lie in the Zariski closure of $\tilde{\Gamma}$ it follows that the $\tilde{\sigma}_i$ must be all written over the field of definition K of $\tilde{\Gamma}$. Thus $K \supset k(t_1, \ldots, t_d)$. On the other hand $\tilde{\Gamma} \subseteq \mathrm{SO}(f_N, A[t_1, t_1^{-1}, \ldots, t_d, t_d^{-1}])$. Therefore

$K = k(t_1, \ldots, t_d)$. Now let $\Gamma'_N := \tilde{\Gamma} \cap$ (image in SO_{N+n+1} of $\mathrm{Spin}_{N+n+1}(K)$). Since $\tilde{\Gamma}$ is finitely generated, it follows that $|\tilde{\Gamma}/\Gamma'_N| < \infty$ (see e.g. (8.4) (ii) and (8.6) (iii) (a)). On the other hand, the argument in the proof of (8.6) (ii) and the above information give us that there is a localization of $\mathbf{Z}[\mathrm{tr}\,\mathrm{Ad}\,\tilde{\Gamma}]$ which coincides with a localization of $A[t_1, t_1^{-1}, \ldots, t_d, t_d^{-1}]$. Now a reference to (8.2) concludes the proof.

12. Miscellania

(12.1) The similarity to Serre's problem on l-adic representations was observed and explained to me by D. Kazhdan. Recall (see [Se]) that the problem in question is to describe the action of the Galois group $\mathrm{Gal}(\bar{k}/k)$ on the l-adic cohomology of an algebraic variety X defined over a number field k. An analogue of this problem in the case when k is a function field and X an elliptic curve was solved by J. Igusa [I]. In the functional case over $\mathbf{C}$, the Galois (= monodromy) group action on l-adic cohomology comes from its action on the integral cohomology and our results from (8.2), or (9.1), or (9.3), or (10.5), or (10.6) give at once information about the l-adic closure of such an action. In particular, they say that if the Zariski closure G of the monodromy group is semi-simple then the closure of the image of the monodromy group in the l-adic cohomologies is open in the groups of $\mathbf{Q}_l$-rational points of the Zariski completion. And, even more, as in [Se], they say that for almost all l these l-adic closures must contain the subgroup $G^+(\mathbf{Z}_l)$ of $G(\mathbf{Z}_l)$ generated by the unipotents of $G(\mathbf{Z}_l)$.

(12.2) *Situation in the excluded cases.*

(12.2.1) In the cases when $\mathrm{char}\,k = 3$ and G is of type G_2 or $\mathrm{char}\,k = 2$ and G is of type B_2 or F_4, it is possible that our Zariski-dense subgroup Γ is contained in an infinite version of a group of Suzuki or Ree (see [T2]). In this case the closure of Γ in $G(\hat{A}_b)$ will not be $G(\hat{A}_b)$. This, probably, can be detected on the level of reductions modulo maximal ideals—such reductions will be, probably, finite groups of Suzuki and Ree. Besides, this case can have, as well, other deviations described below.

(12.2.2) Let now $p = 3$ if G is of type G_2, and $p = 2$ if G is of type B_n ($n \geq 2$), C_n ($n \geq 2$), or F_4. Consider a split group G defined over $\mathbf{F}_p$ and let T be a maximal split $\mathbf{F}_p$-torus in G, and R the system of roots of G with respect to T. Write $R = R_l \cup R_s$ for the partition of R into the sets of long and short roots. Let further x_r: $\mathbf{G}_{a,\mathbf{F}_p} \to G$ be a Chevalley system of $\mathbf{F}_p$-parametrizations of the root subgroups of G with respect to T.

Now let $k \supseteq \mathbf{F}_p$ be any field of characteristic p (preferably imperfect). For two additive subgroups A and B of k we define, following [VW, § 6], the

subgroup

$$G^E(A, B) := \langle x_r(B), r \in R_l; x_{r'}(A), r' \in R_s \rangle \text{ of } G(k).$$

For a subgroup Γ of $G(k)$ and $r \in R$, write $C_r(\Gamma) := \{c \in k | x_r(c) \in \Gamma\}$. It was shown in [VW, § 6] that $C_r(G^E(A, B)) = A$ for $r \in R_s$ and $C_r(G^E(A, B)) = B$ for $r \in R_l$ if A and B satisfy the following necessary and sufficient conditions (see [VW, Theorem 1.1]):

(i) $AB \subset A$;

(ii) $BA^p \subset B$;

(iii) $A^p \subset B \subset A$;

(iv) $BB \subset B$ *if* R_l *is connected*;

(v) $AA \subset A$ *if* R_s *is connected*.

(12.2.3) We are interested in finitely generated groups. Therefore we take finite subsets A_0 and B_0 of k and consider $\Gamma := G^E(A_0, B_0)$. Then $A := C_r(\Gamma)$, $r \in R_s$, and $B := C_r(\Gamma), r \in R_l$, satisfy (i)–(v) (actually, A and B are, of course, the smallest subsets of k which satisfy (i)–(v) and contain respectively A_0 and B_0). Although (i)–(iii) do not necessarily imply that either one of A and B is closed under multiplication (e.g. $p = 2$, $K = \mathbf{F}_2$, $k = K(t)$, $A := \sum_{i \neq 0,1,2,4,7,8} Kt^i$, $B := \sum_{i \geq 6, i \neq 7,8,11,13,17,23} Kt^i$), it seems that (since we are going to localize anyway) that we can assume that A and B are rings (without identity). Then only (iii) remains and we are, essentially, reduced to the case considered by J. Tits in [T1, Section 10.3.2]. But then the closure of $G^E(A, B)$ in $G^E(\hat{A})$ will be, clearly, $G^E(\hat{A}, \hat{B})$. Thus it is impossible to prove (8.2) in the cases rejected there. But it is reasonable to expect that if the groups of the type considered here, as well as the groups of Suzuki and Ree are taken into account then a version of (8.2) should hold.

(12.2.4) The point where the above phenomenon (of $A \supset B \supset A^p$) is detected by our proof is when we consider reduction modulo the square of a maximal ideal M. For the groups of (12.2.3) the groups $G(M/M^2)$ (in notation of § 7) will be equal sometimes to $\tilde{L}(k)$ where $\tilde{L}(k)$ is as described in (5.6). However it seems to be the only place where the feature under discussion influences the proof. Finally, to recover A we should, as before, take $\mathbf{Z}[\operatorname{tr} \operatorname{Ad} \Gamma]$. To recover B we should take $\mathbf{Z}[\operatorname{tr} \operatorname{Ad} \circ \iota(\Gamma)]$ where ι is an inseparable isogeny with $d\iota \neq 0$ (see [BT3, (3.8)]).

(12.2.5) Finally, in addition to the above complications there may exist non-trivial (or even anisotropic) forms of groups in (12.2.1) and (12.2.3), (see, however, [BT3, (3.9)–(3.14)]).

(12.3) *Comments on other possible versions of strong approximation.*

What we did in this work was to take $\hat{A}$ for the definition of the adele ring of A. However geometric considerations invariably lead to other definitions related to families ("flags") of embedded subvarieties (see [Pa]). Such an approach would require a completely different (from profinite) topology on A, and the corresponding results would be very interesting.

(12.4) *Relevant recent work.*

Two very recent papers: R. Griess, Quotients of infinite reflection groups, Math. Ann. **263** (1983), 267–278, and J. Cohen, Homomorphisms of cocompact Fuchsian groups on $\mathrm{PSL}_2(\mathbf{Z}_p[x]/(f(x)))$, Trans. A. M. S. **281** (1984), 571–585, intersect (on very particular cases) with results of the present work. The former paper gives also very precise information on reductions mod p for *all* p.

Another work (of which we knew while writing this paper) is: R. S. Kulkarni, Surface-symmetries, holomorphic maps, and tessellations, to appear, which studies (among other things) "frequency" of simple quotients of the Fuchsian groups. As with the Artin problem (see [Ma]), very interesting information is obtained modulo certain generalized Riemann hypotheses.

Finally, we analyzed the proof of Section 3 more closely and it yielded the following statement: There exists a function f: $\mathbf{N} \to \mathbf{N}$ such that for every field k of characteristic exponent p, every finite subgroup H of $\mathrm{GL}_n(k)$ contains a normal subgroup H_1 such that $|H/H_1| \leq f(n)$ and H_1 contains normal subgroups $H_2 \supseteq H_3$ such that H_3 is a p-group, H_2/H_3 is a commutative p'-group and H_1/H_2 is a product of simple groups of Lie type and of characteristic p. Moreover $f(n) \leq (n+2)!$ for all sufficiently large n.

PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA.

REFERENCES

[Ba1] H. BASS, Groups of integral representation type, Pacific J. Math. **86** (1980), 15–51.

[Ba2] _____, Theorems of Jordan and Burnside for algebraic groups, J. Alg. **82** (1983), 245–254.

[B1] A. BOREL, Density properties of certain subgroups of semi-simple groups without compact components, Ann. of Math. **72** (1960), 179–188.

[B2] _____, Density and maximality of arithmetic groups, J. reine angw. Math. **224** (1966), 78–89.

[B3] _____, *Linear Algebraic Groups*, Benjamin, New York, 1969.

[BT1] A. BOREL and J. TITS, Groupes réductifs, Publ. Math. IHES, **27** (1965), 659–755.

[BT2] _____, Complémentes à l'article "Groupes réductifs", Publ. Math. IHES **41** (1972), 253–276.

[BT3] _____, Homomorphisms "abstraits" de groupes algébriques simples, Ann. of Math. **97** (1973), 499–571.

[CPS1] E. CLINE, B. PARSHALL, and L. SCOTT, Cohomology of finite groups of Lie type I, Publ. Math. IHES **45** (1975), 169–191.

[CPS2] _____, Cohomology of finite groups of Lie type, II, J. Alg. **45** (1977), 182–198.

[CPSK] E. CLINE, B. PARSHALL, L. SCOTT, and W. VAN DER KALLEN, Rational and generic cohomology, Invent. Math. **39** (1977), 143–163.

[D] V. V. DEODHAR, On central extensions of rational points of algebraic groups, Amer. J. Math. **100** (1978), 303–386.

[G1] D. GORENSTEIN, *Finite Groups*, 2nd ed., Chelsea Publ. Co., New York, 1980.

[G2] _____, *Finite Simple Groups*, Plenum Press, New York and London, 1982.

[Gr1] R. L. GRIESS, JR., Schur multipliers of the known finite simple groups, II, pp. 279–282, in *The Santa Cruz Conference on Finite Groups*, Proc. Symp. Pure Math., vol. 37, AMS, Providence, R.I. 1980.

[GR] H. GARLAND and M. S. RAGHUNATHAN, Fundamental domains for lattices in (R-) rank 1 semisimple Lie groups, Ann. of Math. **92** (1970), 279–326.

[H] G. M. D. HOGEWEIJ, Ideals and automorphisms of almost classical Lie algebras, Thesis, Utrecht University, the Netherlands, 1978.

[I] J. IGUSA, Fibre systems of Jacobian varieties, II and III, Amer. J. Math. **78** (1956), 745–770, and **81** (1959), 453–476.

[JM] D. JOHNSON and J. MILLSON, in preparation.

[K1] M. KNESER, Strong approximation, in *Algebraic Groups and Discontinuous Subgroups*, Proc. Symp. Pure Math., vol. 9, A. M. S., Providence, 1966, pp. 187–196.

[K2] _____, Schwache Approximation in algebraishen Gruppen, Colloque sur la théorie des groupes algebriques CBRM, Brussels, 1962, pp. 41–52.

[MKS] W. MAGNUS, A. KARRASS, D. SOLITAR, *Combinatorial Group Theory*, Intersci. Pub., New York, 1966.

[M] G. MARGULIS, Arithmeticity of the irreducible lattices in semi-simple groups of rank greater than 1, appendix to Russian translation of [R], Mir, Moscow, 1977 (an English translation, Inventiones Math.) **76** (1984), 93–120.

[Ma] C. R. MATTHEWS, Counting points modulo p for some finitely generated subgroups of algebraic groups, Bull. London Math. Soc. **14** (1982), 149–154.

[MVW] C. R. MATTHEWS, L. N. VASERSTEIN, and B. WEISFEILER, Congruence properties of Zariski-dense subgroups, Proc. London Math. Soc. **48** (1984), 514–532.

[Mc] B. MCDONALD, *Finite Rings with Identity*, M. Dekker, New York, 1974.

[Mi] J. J. MILLSON, On the first Betti number of a constant negatively curved manifold, Ann. of Math. **104** (1976), 235–247.

[Mo] G. D. MOSTOW, *Strong Rigidity of Locally Symmetric Spaces*, Ann. Math. Studies, no. 78, Princeton Univ. Press, Princeton, 1973.

[O] P. OLUM, Non-abelian cohomology and van Kampen's theorem, Ann. of Math. **68** (1958), 658–668.

[Pa] A. N. PARSHIN, On the arithmetic of two-dimensional schemes. I. Distributions and residues, Math. USSR: Izvestija, **10** (1976), 695–729 and
A. N. Parshin, Chern classes, adeles and L-functions, J. reine angew. Math. **341** (1983), 174–192.

[P] G. PRASAD, Strong approximation for semi-simple groups over function fields, Ann. of Math. **105** (1977), 553–572.

[R] M. S. RAGHUNATHAN, *Discrete Subgroups of Lie Groups*, Springer-Verlag, New York, 1972.

[Se] J-P. SERRE, *Abelian l-Adic Representations and Elliptic Curves*, Benjamin, New York, 1968,

Propriétés galoisiennes des pointes d'ordre fini des courbes elliptiques, Inv. Math. **15** (1972), 259–331.

[S1] R. STEINBERG, Lectures on Chevalley groups, Yale University Lecture Notes, 1968.

[S2] _____, Generators, relations and coverings of algebraic groups, II, J. Alg. **71** (1981), 527–543.

[S3] _____, Automorphisms of classical Lie algebras, Pacific J. Math. **11** (1960), 1119–1129.

[Su1] M. SUZUKI, *Group Theory* I, Springer-Verlag, New York, 1982.

[T1] J. TITS, *Buildings of Spherical Type and Finite* BN-*Pairs*, Lecture Notes in Math., no. 386, Springer, New York, 1974.

[T2] _____, Les groupes simples de Suzuki et de Ree, Sém Bourbaki, exp. **210** (1960), 16;
_____, Ovoides et groupes de Suzuki, Archiv Math. **13** (1962), 187–198;
_____, Moufang octagons and Ree groups of type ${}^2F_4$, Amer. J. Math. **105** (1983), 539–594.

[VW] L. N. VASERSTEIN and B. WEISFEILER, On full subgroups of Chevalley groups, preprint.

[V] E. B. VINBERG, Rings of definition of dense subgroups of semi-simple linear groups, Mathematics USSR: Izvestija **5** (1971), 45–55.

[W1] B. WEISFEILER, Monomorphisms between subgroups of groups of type G_2, J. Alg. **68** (1981), 306–334.

[W2] _____, A survey of abstract homomorphisms between big subgroups of algebraic groups, in *Topics in Algebraic Groups*, Notre Dame Math. Lectures series, no. 12, Notre Dame, 1983.

(Received May 5, 1983)