Rigidity Results for Solvable Arithmetic Groups and Applications

Fritz Grunewald
Mathematisches Institut
Heinrich Heine Universität
D-40225 Düsseldorf
e-mail: fritz@math.uni-duesseldorf.de

Vladimir Platonov
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada N2L3G1
e-mail: vplatonov@math.uwaterloo.ca

Table of contents

1. Introduction

The main aim of this paper is to describe solvable arithmetic groups for which natural rigidty properties hold and to apply these rigidity results. We study the automorphism groups of solvable arithmetic groups, prove arithmeticity results for their finite extensions and construct a new class of non-arithmetic polycyclic groups. In fact we work with the more general class of finite extensions of solvable arithmetic groups and obtain rigidity results in this case. This also is a new point of view since all previous rigidity results where related to connected groups.

A $\mathbb{Q}$-*defined linear algebraic group* G is a subgroup $G \leq \mathbf{GL}(n, \mathbb{C})$ ($n \in \mathbb{N}$) which is also an affine algebraic set defined by polynomials with rational coefficients in the natural coordinates of $\mathbf{GL}(n, \mathbb{C})$. If R is a subring of $\mathbb{C}$ we put $G(R) := G \cap \mathbf{GL}(n, R)$. We have $G = G(\mathbb{C})$.

Let G be a $\mathbb{Q}$-defined linear algebraic group. A subgroup $\Gamma \leq G$ is called an *arithmetic subgroup* of G if Γ is commensurable with $G(\mathbb{Z})$. An abstract group Δ is called *arithmetic* if it is isomorphic to an arithmetic subgroup of a $\mathbb{Q}$-defined linear algebraic group. Two subgroups Γ_1, Γ_2 of $\mathbf{GL}(n, \mathbb{C})$ are called *commensurable* if their intersection $\Gamma_1 \cap \Gamma_2$ has finite index both in Γ_1 and Γ_2. These definitions are taken from [P-R]. A more narrow definition is used in [B1], [S]. In these papers the group Γ is called arithmetic if it is isomorphic to a subgroup of $G(\mathbb{Q})$ which is commensurable to $G(\mathbb{Z})$. The relation between the two concepts is explained in [G-P1] and [G-P2].

We consider here the case of finite extensions of solvable linear algebraic groups. The arithmetic subgroups of them are known to be finite extension groups of polycyclic groups. The first question we study is whether an isomorphism between arithmetic subgroups extend to $\mathbb{Q}$-defined rational isomorphisms between the corresponding linear algebraic groups. These questions are traditionally called rigidity problems. Well known results of Margulis [Ma], Mostow [Mo] and Prasad [Pr] establish a positive answer to the rigidity problems for arithmetic subgroups of $\mathbb{Q}$-simple linear algebraic groups of adjoint type under a condition on their real rank. Algebraic groups with radical are analyzed in [G-P2]. The solvable case is studied in [M-P]. The following example shows that in general there will not be any relation between the isomorphisms of arithmetic groups and the rational homomorphisms of the algebraic groups containing them.

Let K be an algebraic number field and $\mathcal{O}$ its ring of integers. We write G_m for the multiplicative group considered as an algebraic group defined over K. Let $\mathbf{R}_{K/\mathbb{Q}}(G_m)$ be the restriction of scalars aplied to G_m. This is a linear algebraic group defined over $\mathbb{Q}$. We have a natural identification $\mathbf{R}_{K/\mathbb{Q}}(G_m)(\mathbb{Z}) = \mathcal{O}^*$ where $\mathcal{O}^*$ stands for the group of units of $\mathcal{O}$. Dirichlet's unit theorem shows that $\mathbf{R}_{K/\mathbb{Q}}(\mathbb{Z})$ contains a subgroup of finite index Γ with $\Gamma \cong \mathbb{Z}^r$ for appropriate $r \in \mathbb{N} \cup \{0\}$. If K is neither $\mathbb{Q}$ nor an imaginary quadratic number field then $r \geq 1$. The group Γ is also isomorphic to an arithmetic subgroup in G_a^r where G_a denotes the additive group. Since $\mathbf{R}_{K/\mathbb{Q}}(G_m)$ is a torus and G_a^r a unipotent group there is no non-trivial rational homomorphism between them.

In this paper we shall show that rigidity results still hold under a natural condition on the solvable-by-finite linear algebraic groups under consideration. Before we can state our results some notation is required. We write $\mathbf{Z}(G)$ for the *center* of a group G, $U(G)$ for the *unipotent radical* and G° for the *connected component of the identity* of a linear algebraic group G. We call a linear algebraic group G *solvable-by-finite* if G° is solvable. The linear algebraic group G acts by conjugation on $U(G)$ and G is called *reduced* if the kernel of this action is contained in $U(G)$ (see Definition 2.4 for more details). If G is reduced then we have $\mathbf{Z}(G) \leq \mathbf{Z}(G^\circ) \leq U(G)$. Our rigidity theorem for solvable-by-finite reduced groups is:

Theorem A: *Let G_1, G_2 be reduced solvable-by-finite linear algebraic groups which are defined over $\mathbb{Q}$. Let $\Gamma_1 \leq G_1(\mathbb{Q})$, $\Gamma_2 \leq G_2(\mathbb{Q})$ be Zariski-dense arithmetic subgroups and $\varphi : \Gamma_1 \to \Gamma_2$ be a group isomorphism. Then there is a rational $\mathbb{Q}$-defined isomorphism $\Phi : G_1 \to G_2$ and a map $u : \Gamma_1 \to \mathbf{Z}(G_2^\circ)(\mathbb{Q})$ such that*

$$\Phi(\gamma) = u(\gamma) \cdot \varphi(\gamma) \tag{1.1}$$

for all $\gamma \in \Gamma_1$. The map u satisfies $u(\gamma_1\gamma_2) = u(\gamma_1)\varphi(\gamma_1)u(\gamma_2)\varphi(\gamma_1)^{-1}$ for all $\gamma_1, \gamma_2 \in \Gamma_1$ and $u(\gamma) = 1$ for all $\gamma \in \Gamma_1 \cap U(G_1)$.

If G_1, G_2 are connected and if the centers of G_1, G_2 are trivial then G_1, G_2 are reduced and Theorem A is contained in [M-P]. If G_1, G_2 are unipotent that is $G_1 = U(G_1)$, $G_2 = U(G_2)$ then Theorem A amounts to a classical result of Malcev, see [Mc]. Theorem A is also a sharper version of a rigidity result for more general linear algebraic groups contained in [G-P2]. The reducedness condition in Theorem A cannot be dropped, this is shown by the examples above.

Before we can explain our further results we have to introduce some notation. A *d-group* is a linear algebraic subgroup which consists of semi-simple elements. Let G be a solvable-by-finite linear algebraic group defined over $\mathbb{Q}$ and $S \leq G$ be a maximal d-subgroup of G which is also defined over $\mathbb{Q}$. We then have a semi-direct product decomposition $G = U(G) \cdot S \cong U(G) \rtimes S$. This is proved in Proposition 2.1. It follows that the quotient $G/U(G)$ is a d-group. Let $\pi_{\mathrm{U}} : G \to G/U(G)$ be the quotient homomorphism. If $\Gamma \leq G(\mathbb{Q})$ is a Zariski-dense arithmetic subgroup then $M(\Gamma) := \pi_{\mathrm{U}}(\Gamma) \cap (G/U(G))^\circ$ is a finitely generated abelian group and $F(\Gamma) := \pi_{\mathrm{U}}(\Gamma)/M(\Gamma)$ is a finite group. The finite group $F(\Gamma)$ acts by conjugation on $M(\Gamma)$. Assume now that G is reduced then the finite group $F(\Gamma)$ also acts by conjugation on the vector space $\mathbf{Z}(G^\circ)(\mathbb{Q}) \leq U(G)$ and stabilizes the subspace $\mathbf{Z}(G)(\mathbb{Q})$. We call Γ *separated* in G if

$$\mathrm{Hom}_{F(\Gamma)}(M(\Gamma), \mathbf{Z}(G^\circ)/\mathbf{Z}(G)(\mathbb{Q})) = \{0\}. \tag{1.2}$$

Here $\mathrm{Hom}_{F(\Gamma)}$ stands for the vector space of $F(\Gamma)$-equivariant homomorphisms. Clearly if G is connected then every arithmetic subgroup is separated. We consider the case of a connected group G as a very important special case in the results which will follow. For more details on the definition of separatedness see Definition 2.8. We prove the following version of Theorem A.

Theorem A': *Let G_1, G_2 be reduced solvable-by-finite linear algebraic groups which are defined over $\mathbb{Q}$. Let $\Gamma_1 \leq G_1(\mathbb{Q})$, $\Gamma_2 \leq G_2(\mathbb{Q})$ be Zariski-dense arithmetic subgroups and $\varphi : \Gamma_1 \to \Gamma_2$ be a group isomorphism. Assume further that Γ_2 is separated in G_2. Then there is a rational $\mathbb{Q}$-defined isomorphism $\Phi : G_1 \to G_2$ and a homomorphism $u : \Gamma_1 \to \mathbf{Z}(G_2)(\mathbb{Q})$ such that $\Phi(\gamma) = u(\gamma) \cdot \varphi(\gamma)$ for all $\gamma \in \Gamma_1$. The homomorphism u satisfies $u(\gamma) = 1$ for all $\gamma \in \Gamma_1 \cap U(G_1)$.*

The concept of separatedness arises naturally as is shown in the following theorem.

Theorem B: *Let G be a reduced solvable-by-finite linear algebraic groups which is defined over $\mathbb{Q}$. Let $\Gamma \leq G(\mathbb{Q})$ be a Zariski-dense arithmetic subgroup. Suppose that for every automorphism φ of Γ there is a rational $\mathbb{Q}$-defined automorphism Φ of G and a homomorphism $u : \Gamma \to \mathbf{Z}(G)(\mathbb{Q})$ which satisfies $u(\gamma) = 1$ for all $\gamma \in \Gamma \cap U(G)$ such that $\Phi(\gamma) = u(\gamma) \cdot \varphi(\gamma)$ for all $\gamma \in \Gamma$. Then Γ is separated in G.*

We go on to prove the following uniform rigidity version of our rigidity result.

Theorem C: *Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup which is seperated in G. Let $\mathfrak{Aut}_{\mathbb{Q}}(G)$ be the group of $\mathbb{Q}$-defined rational automorphisms of G and $\mathrm{Aut}(\Gamma)$ the automorphism group of the abstract group Γ. Then there is a homomorphism*

$$D : \mathrm{Aut}(\Gamma) \to \mathfrak{Aut}_{\mathbb{Q}}(G), \qquad \varphi \mapsto D_\varphi \tag{1.3}$$

and also a map

$$u : \mathrm{Aut}(\Gamma) \to \mathrm{Hom}(\Gamma, \mathbf{Z}(G)(\mathbb{Q})), \qquad \varphi \mapsto u_\varphi \tag{1.4}$$

with $u_\varphi(\gamma) = 1$ for all $\varphi \in \mathrm{Aut}(\Gamma)$ and $\gamma \in \Gamma \cap U(G)$ such that $D_\varphi(\gamma) = u_\varphi(\gamma) \cdot \varphi(\gamma)$ for every $\varphi \in \mathrm{Aut}(\Gamma)$ and $\gamma \in \Gamma$. The homomorphism D and and the map u are uniquely determined by these properties. The map u of (1.4) furthermore satisfies:

$$u_{\varphi \circ \psi}(\gamma) = D_\varphi(u_\psi(\gamma)) \cdot u_\varphi(\psi(\gamma)) \tag{1.5}$$

for all φ, $\psi \in \mathrm{Aut}(\Gamma)$ and $\gamma \in \Gamma$.

Again Theorem C is a sharper version of a uniform rigidity result for more general linear algebraic groups contained in [G-P2].

As our results are mainly for the class of arithmetic subgroups of reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic groups, it is important to note that this class does not differ too much from the class of all arithmetic subgroups of solvable $\mathbb{Q}$-defined linear algebraic groups. In Section 3 we prove for example that each of the latter groups has a subgroup of finite index which embeds as a Zariski-dense arithmetic subgroup into $G(\mathbb{Q})$ where G is a solvable reduced $\mathbb{Q}$-defined linear algebraic group. Theorem 3.4 even contains an abstract characterisation of the arithmetic subgroups of reduced solvable $\mathbb{Q}$-defined linear groups.

Rigidity results like the above have numerous applications. We shall describe three of them. Firstly Theorem B implies:

Theorem D: *Let Γ be a solvable arithmetic group. Then every finite extension of Γ an arithmetic group.*

This result is a corollary of a corresponding result from [G-P2] for more general arithmetic groups Γ. We include a proof in Section 3 since it is much simpler than that of the general case.

As a second application we are able to give a precise description of the automorphism group of certain solvable-by-finite arithmetic groups. This extends results of Malcev on the automorphism group of an arithmetic subgroup of a unipotent $\mathbb{Q}$-defined linear algebraic group. We prove:

Theorem E: *Let $\Gamma \leq G(\mathbb{Q})$ be a Zariski-dense arithmetic subgroup of a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group G which is separated in G. Then* $\mathrm{Aut}(\Gamma)$ *is an arithmetic group. In particular* $\mathrm{Aut}(\Gamma)$ *is an arithmetic group for any Zariski-dense arithmetic subgroup of $G(\mathbb{Q})$ where G is a connected reduced and $\mathbb{Q}$-defined linear algebraic group.*

If Γ is a torsion-free finitely generated nilpotent group then both Γ and $\mathrm{Aut}(\Gamma)$ are arithmetic groups in a very natural way (see [13], chapter 6). Our proof of Theorem E (which is described in Section 4) is similarly canonical. The characterisation of arithmetic subgroups of reduced solvable linear algebraic groups already mentioned yields the following abstract version of Theorem E.

Theorem E': *Let Γ be a solvable arithmetic group with torsion-free Fitting subgroup $\mathcal{F}(\Gamma)$. If $\Gamma/\mathcal{F}(\Gamma)$ is nilpotent then* $\mathrm{Aut}(\Gamma)$ *is an arithmetic group.*

Let G be a reduced solvable linear algebraic group defined over $\mathbb{Q}$ and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup. Let $\mathrm{Aut}_{\mathrm{alg}}(\Gamma)$ be the subgroup of $\mathrm{Aut}(\Gamma)$ consisting of those elements which are the restriction of an element from $\mathfrak{Aut}_{\mathbb{Q}}(G)$. We also can compare $\mathrm{Aut}(\Gamma)$ with $\mathrm{Aut}_{\mathrm{alg}}(\Gamma)$. To do this we call an element $\varphi \in \mathrm{Aut}(\Gamma)$ *$\mathcal{F}$-central* if $\varphi(\gamma)\gamma^{-1} \in \mathbf{Z}(\Gamma)$ for all $\gamma \in \Gamma$ and if φ is the identity when restricted to the Fitting subgroup $\mathcal{F}(\Gamma)$. We define

$$(1.6) \qquad \mathrm{Aut}_0(\Gamma) := \{\, \varphi \in \mathrm{Aut}(\Gamma) \;\;|\;\; \varphi \;\text{ is } \mathcal{F}\text{-central}\,\}.$$

The group $\mathrm{Aut}_0(\Gamma)$ is abelian and normal in $\mathrm{Aut}(\Gamma)$. It can be identified with the group of homomorphisms from $\Gamma/\mathcal{F}(\Gamma)$ to $\mathbf{Z}(\Gamma)$. We have:

Theorem F: *Let G be a reduced solvable linear algebraic group defined over $\mathbb{Q}$ and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup which is separated in G. Then the subgroup $\mathrm{Aut}_0(\Gamma) \cdot \mathrm{Aut}_{\mathrm{alg}}(\Gamma)$ is of finite index in $\mathrm{Aut}(\Gamma)$.*

If G is a $\mathbb{Q}$-defined unipotent linear algebraic group and $\Gamma \leq G(\mathbb{Q})$ is an arithmetic subgroup then $\mathrm{Aut}_{\mathrm{alg}}(\Gamma) = \mathrm{Aut}(\Gamma)$. Theorem F is an extension of this classical result. Theorem F follows directly from Theorem 4.7 where a further decompositon $\mathrm{Aut}_{\mathrm{alg}}(\Gamma)$ is obtained.

As a further application of our techniques we construct new polycyclic groups which are not arithmetic. Notice that, as already mentioned, every arithmetic subgroup Γ of a solvable $\mathbb{Q}$-defined linear algebraic group is a polycyclic group. But not every polycyclic group is arithmetic. The first counterexamples are contained in [P3]. Further examples can be found in [Se], chapter 11. The examples of non-arithmetic polycyclic groups Γ constructed in [P3] and [Se] do not have a subgroup of finite index which is a split extension of a nilpotent group by an abelian group. This in fact immediately implies that Γ is not arithmetic. We propose a new construction of non-arithmetic polycyclic groups in Section 5. Our examples have split extensions of abelian groups by abelian groups as subgroups of arbitrarily high index. This shows that they give new types of groups not commensurable with any previous example. Also it turns out to be much more difficult to prove that they are not arithmetic.

A group Γ is called polycyclic if it has a (finite) decomposition series which has only cyclic factors. If Γ is a polycyclic group then the Hirsch number $h(\Gamma)$ is defined as the number of factors isomorphic to $\mathbb{Z}$ in a decomposition series for Γ. We prove the following surprising theorem.

Theorem G: *Let h be a natural number with $h \geq 4$. Then there are non-arithmetic polycyclic groups of Hirsch number h which are split extensions of $\mathbb{Z}^{h-1}$ by an infinite cyclic group.*

Since it is known that every torsion-free finitely generated nilpotent group is arithmetic and because of Theorem D our examples are in an appropriate sense minimal.

Chapter 11 of [Se] contains an example of a polycyclic group of Hirsch number 5 which is not arithmetic. The author then poses the question whether there are such examples with Hirsch number < 5. We prove:

Theorem H: *The minimal Hirsch number of a non-arithmetic polycyclic group is* 4.

A short exposition of the main results of this paper is contained in [G-P3], [G-P4]. The results and concepts from the theory of linear algebraic groups that we use in this paper can be found in the book [P-R] those on polycyclic groups are contained in [Se].

Acknowledgements: We thank Armand Borel and Dan Segal for advice on the subject. The first version of this paper was prepared while the second named author was visiting the Heinrich-Heine-Universität at Düsseldorf. He was partially supported by grants from the Deutsche Forschungsgemeinschaft and from NSERC. The paper was completed when the second author was visiting the Max-Planck-Institute of Mathematics in Bonn.

2. Rigidity Results

In this section we investigate prove the rigidity results contained in Theorems A, A', C. We also prove Theorem B. We start by establishing some facts about linear algebraic groups which will be needed in the sequel. We write $U(G)$ for the unipotent radical of a linear algebraic group G. The unipotent group $U(G)$ is $\mathbb{Q}$-defined if G has this property. Note that $U(G) = U(G^\circ)$ where G° stands for the connected component of the identity in G. We say that G is a *d-group* if it consists of semi-simple elements only. An algebraic subgroup $H \leq G$ is called a *d-subgroup* if H is a d-group. A *torus* is a connected commutative d-group. Note that a solvable-by-finite d-group is a finite extension of a torus. The following result is contained in section 5 of [B-S]. For connected groups G it is a well known result. We give here a different and simpler proof for the general case which is of independent interest.

Proposition 2.1: *Let G be a solvable-by-finite $\mathbb{Q}$-defined linear algebraic group. Then there is a $\mathbb{Q}$-defined d-subgroup S of G such that*

$$G = U(G) \cdot S \cong U(G) \rtimes S. \tag{2.1}$$

The algebraic group S is a finite extension of a $\mathbb{Q}$-defined torus which is maximal in G°. Also S is a maximal d-subgroup of G. Every maximal $\mathbb{Q}$-defined d-subgroup of G is conjugate to S by an element of $U(G)(\mathbb{Q})$ and every maximal d-subgroup of G is conjugate to S by an element of $U(G)$.

Proof (Existence): We consider now the case of an arbitrary solvable-by-finite group G. We shall first reduce the question of the existence of a decomposition (2.1) to the case when $G^\circ = U(G)$. Let $\pi : G \to G/U(G)$ be the quotient homomorphism. We may choose a $\mathbb{Q}$-defined torus $T \leq G^\circ$ such that $G^\circ = U(G) \cdot T$. Since $G/U(G)$ is a finite extension of $\pi(T)$ it is a d-group. Let $N_G(T)$ be the normalizer of T in G. This is a $\mathbb{Q}$-defined algebraic subgoup of G, it is also solvable by finite. Suppose we have a decomposition $N_G(T) = U(N_G(T)) \cdot \hat{S}$ where $\hat{S}$ is a $\mathbb{Q}$-defined d-group. Since $G/U(G)$ is a d-group we have $\pi(U(N_G(T))) = \{1\}$ and $U(N_G(T)) \leq U(G)$. If $g \in G$ then gTg^{-1} is a maximal torus in G° hence there is a $u \in U(G)$ with $gTg^{-1} = uTu^{-1}$. This shows that $G = U(G) \cdot N_G(T)$ and also $G = U(G) \cdot \hat{S}$. Hence it suffices to establish (2.1) for $N_G(T)$. Note that $G^\circ \cap N_G(T) = U(N_G(T)) \cdot T$. This shows that $N_G(T) = U(N_G(T)) \cdot T$ has finite index in $N_G(T)$ and also that the quotient group $H := N_G(T)/T$ is unipotent by finite. Let $\mathrm{p} : N_G(T) \to H$ be the quotient homomorphism and suppose we know (2.1) for H. This means there is a finite $\mathbb{Q}$-defined algebraic subgroup $\tilde{S} \leq H$ such that $H = U(H) \cdot \tilde{S}$. Consider $\hat{S} := \mathrm{p}^{-1}(\tilde{S})$. Since $\hat{S}$ is a finite extension of T it is a d-group. Since the kernel of p consists of semi-simple elements we get the decomposition $N_G(T) = U(N_G(T)) \cdot \hat{S}$. Hence it is enough to prove (2.1) for an H which is a finite extension of a unipotent group.

Let now H be a $\mathbb{Q}$-defined linear algebraic group with $H^\circ = U(H)$. Suppose we know (2.1) for all H so that $U(H)$ is abelian. We then do induction on the nilpotency class of $U(H)$. Let $\pi : H \to H/\mathbf{Z}(U(H)) =: H_0$ be the quotient homomorphism where $\mathbf{Z}(U(H))$ is the center of $U(H)$. The $\mathbb{Q}$-defined linear algebraic group H_0 again has the property that $H_0^\circ = U(H_0)$ but the nilpotency class of $U(H_0)$ is one less then that of $U(H)$. By induction there is a $\mathbb{Q}$-defined finite subgroup $F_0 \leq H_0$ such that $H_0 = U(H_0) \cdot F_0$. Put $H_1 := \pi^{-1}(F_0)$. The $\mathbb{Q}$-defined linear algebraic group H_1 has the property that $H_1^\circ = U(H_1)$ and $U(H_1)$ is abelian. Hence there is a $\mathbb{Q}$-defined finite subgroup $F_1 \leq H_1$ such that $H_1 = U(H_1) \cdot F_1$. It is straightforward to see that $H = U(H) \cdot F_1$. Hence it is enough to prove (2.1) for an H which is a finite extension of an abelian unipotent group.

Let now H be a $\mathbb{Q}$-defined linear algebraic group with $H^\circ = U(H)$ and where $U(H)$ is abelian. The finite group H/H° acts through conjugation on $U(H)$. Since this action is rational and also $\mathbb{Q}$-defined the centralizer $V(H)$ of H/H° in $U(H)$ is a $\mathbb{Q}$-defined algebraic subgroup of $U(H)$. Suppose we have established (2.1) in the two cases that $V(H) = \{1\}$ and $V(H) = U(H)$. We then consider the $\mathbb{Q}$-defined linear algebraic group $H_1 := H/V(H)$, notice that $V(H)$ is always normal in H. Let $\pi : H \to H_1$ be the quotient homomorphism. We have $V(H_1) = \{1\}$ hence there is a $\mathbb{Q}$-defined finite subgroup $F_1 \leq H_1$ with $H_1 = U(H_1) \cdot F_1$. Put $H_2 := \pi^{-1}(F_1)$. The linear algebraic group H_2 satisfies $H_2^\circ = U(H_2)$ and $V(H_2) = U(H_2)$. Hence there is a $\mathbb{Q}$-defined finite subgroup $F \leq H_2$ with $H_2 = U(H_2) \cdot F$. It is easy to see that also $H = U(H) \cdot F$ holds.

Let now H be a $\mathbb{Q}$-defined linear algebraic group with $H^\circ = U(H)$ and where $U(H)$ is abelian. Let $\overline{\mathbb{Q}}$ be the algebraic closusure of $\mathbb{Q}$ in $\mathbb{C}$. Consider the quotient homomorphism $H(\overline{\mathbb{Q}}) \to H/H^\circ(\overline{\mathbb{Q}}) = H/H^\circ$. Since $H/H^\circ(\overline{\mathbb{Q}})$ is finite and $H^\circ(\overline{\mathbb{Q}})$ is a vector space over $\overline{\mathbb{Q}}$ this homomorphism splits that there is a finite subgroup $F \leq H(\overline{\mathbb{Q}})$

which maps bijectively onto H/H° and which satisfies $H(\overline{\mathbb{Q}}) = U(H)(\overline{\mathbb{Q}}) \cdot F$. We shall show that there is the choice of a $\mathbb{Q}$-defined finite group $F \leq H(\overline{\mathbb{Q}})$ with these properties. Let us first show that two finite subgroups F_1, $F_2 \leq H(\overline{\mathbb{Q}})$ with the properties just indicated are conjugate by an element of $U(H)(\overline{\mathbb{Q}})$. Given $f \in F_1$ there is a unique $u(f) \in U(H)(\overline{\mathbb{Q}})$ such that $u(f)f \in F_2$. The map $u : F_1 \to U(H)(\overline{\mathbb{Q}})$ satisfies $u(f_1 f_2) = u(f_1) f_1 u(f_2) f_1^{-1}$ for all f_1, $f_2 \in F_1$. Hence it is a derivation of the finite group F_1 into the $\overline{\mathbb{Q}}$-vector space $U(H)(\overline{\mathbb{Q}})$ which is made into an F_1-module through conjugation. It is well known that u is inner, that is there is a $v \in U(H)(\overline{\mathbb{Q}})$ such that $u(f) = v^{-1} f v f^{-1}$ for all $f \in F_1$. We conclude that $u(f)f = v^{-1} f v$ for all $f \in F_1$. This implies that $v^{-1} F_1 v = F_2$. We fix now a finite group $F \leq H(\overline{\mathbb{Q}})$ with the properties indicated above. Let $\mathbb{G}$ be the Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$. If σ is an element of $\mathbb{G}$ that $\sigma(F)$ is another finite group with the above properties. Hence there is a $u_\sigma \in U(H)(\overline{\mathbb{Q}})$ with $\sigma(F) = u_\sigma F u_\sigma^{-1}$. If $V(H) = U(H)$ it follows that $\sigma(F) = F$ and F is $\mathbb{Q}$-defined. This already establishes the second of the two cases left open in the previous paragraph. We shall proceed under the further hypothesis that $V(H) = \{1\}$. Then u_σ is uniquely determined by $\sigma \in \mathbb{G}$. The map $u : \mathbb{G} \to U(H)(\overline{\mathbb{Q}})$ satisfies then $u_{\sigma\tau} = u_\sigma \sigma(u_\tau)$ for all σ, $\tau \in \mathbb{G}$. Hence it represents an element of the Galois cohomology set $H^1(\mathbb{Q}, U(H))$. It is well known that $H^1(\mathbb{Q}, U(H))$ consists of the base point only ($U(H)$ is a unipotent group). Hence there is a $v \in U(H)(\overline{\mathbb{Q}})$ such that $u_\sigma = v^{-1}\sigma(v)$ for all $\sigma \in \mathbb{G}$. A simple computation then shows that $S := v^{-1} F v$ satisfies $\sigma(S) = S$ for all $\sigma \in \mathbb{G}$. Hence the finite group S is $\mathbb{Q}$-defined. This establishes the first case left open in the previous paragraph and altogether the existence of a decomposition (2.1) in general.

It is evident that the S just constructed is a maximal $\mathbb{Q}$-defined d-subgroup of G. It is also clear that $S^\circ = G^\circ \cap S$ is a maximal $\mathbb{Q}$-defined torus in G°. It remains to prove the statement about the conjugacy of all $\mathbb{Q}$-defined maximal d-subgroups of G. We postpone this until after the next lemma which is an important step in the proof. □

Lemma 2.2: *Let G be a solvable-by-finite linear algebraic group which is defined over $\mathbb{Q}$. Assume that $F \leq G$ is a $\mathbb{Q}$-defined finite subgroup of G. Then there is a $\mathbb{Q}$-defined maximal torus $T \leq G^\circ$ which is normalized by F.*

Proof: Suppose we have proved the lemma under the assumption that the unipotent radical $U(G)$ is abelian. We now prove the general result by induction on the nilpotency class of $U(G)$. Let $Z := \mathbf{Z}(U(G))$ be the center of the unipotent radical of G. This is a $\mathbb{Q}$-defined normal algebraic subgroup of G. Let $\pi : G \to H := G/Z$ be the quotient homomorphism. Then $\pi(F)$ is a $\mathbb{Q}$-defined finite subgroup of H. By induction there is a $\mathbb{Q}$-defined maximal torus $T_1 \leq H^\circ$ which is normalized by $\pi(F)$. Then $T_1 \cdot \pi(F)$ is a $\mathbb{Q}$-defined d-subgroup of H. Define $H_0 := \pi^{-1}(T_1 \cdot \pi(F))$. The algebraic group H_0 is $\mathbb{Q}$-defined and its unipotent radical $U(H_0)$ is abelian. We in fact have $U(H_0) = Z$. We also have $F \leq H_0$. By assumption we find a $\mathbb{Q}$-defined maximal torus $T_0 \leq H_0$ which is normalized by F. Since $T_0 \cap G^\circ$ has finite index in T_0 and since T_0 is connected we find that $T_0 \leq G^\circ$. It is easy to see that T_0 is a maximal $\mathbb{Q}$-defined torus in G°. In fact the dimension of any maximal torus in G° is equal to the dimension of a maximal in H° and the dimension of T_0 is equal to that of T_1.

We proceed under the hypothesis that $U(G)$ is abelian. We fix a maximal $\mathbb{Q}$-defined torus $T \leq G^\circ$. Let $N_U(T)$ be the normalizer of T in $U(G)$. This is a $\mathbb{Q}$-defined algebraic subgroup of $U(G)$. We shall show that $N_U(T)$ is normal in G. Let $u \in N_U(T)$. By the result in [P1] mentioned already above There is for every $g \in G$ a $u(g) \in U(G)$ such that $gTg^{-1} = u(g)Tu(g)^{-1}$ (see [P1]). We then have

$$\begin{aligned} gug^{-1}Tgu^{-1}g^{-1} &= guu(g^{-1})Tu(g^{-1})^{-1}u^{-1}g^{-1} = gu(g^{-1})uTu^{-1}u(g^{-1})^{-1}g^{-1} \\ &= gg^{-1}Tgg^{-1} = T. \end{aligned} \tag{2.2}$$

It follows that $N_U(T)$ is normal in G. By an argument similar to that in the beginning of this prove (compare G with $G/N_U(T)$) the result (under the assumption that $U(G)$ is abelian) follows from the two particular cases:

Case 1: $U(G) = N_U(T)$. In this case $U(G)$ centralizes T and G° has a unique $\mathbb{Q}$-defined maximal torus T. Of course then F has to normalize T.

Case 2: $N_U(T) = \{1\}$. We write the multiplication in $U(G)$ in this case additively. Note that for every element $f \in F = F(\overline{\mathbb{Q}})$ there is unique $u(f) \in U(G)(\overline{\mathbb{Q}})$ with $fTf^{-1} = u(f)Tu(f)^{-1}$. We make $U(G)(\overline{\mathbb{Q}})$ into an F module through conjugation. The function $u : F \to U(G)(\overline{\mathbb{Q}})$ satisfies $u(f_1 f_2) = u(f_1) + f_1 u(f_2) f_1^{-1}$ for all $f_1, f_2 \in F$. Hence u is a derivation of F into the F-module $U(G)(\overline{\mathbb{Q}})$. Since F is finite it is an inner derivation. Put

$$v := \frac{1}{|F|} \sum_{f \in F} u(f) \tag{2.3}$$

A standard computation shows that $u(f) = -v + fvf^{-1}$ for all $f \in F$. We infer that F normalizes $v^{-1}Tv$. By definition we have $v \in U(G)(\overline{\mathbb{Q}})$. We show now that $v \in U(G)(\mathbb{Q})$. Let $\mathbb{G}$ be the Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$. Since $u(f)$ is uniquely determined by $f \in F$ and since T is defined over $\mathbb{Q}$ we have $\sigma(u(f)) = u(\sigma(f))$ for all $\sigma \in \mathbb{G}$. From the definition (2.3) of v we infer that $\sigma(v) = v$ for all $\sigma \in \mathbb{G}$. It follows that $v^{-1}Tv$ is defined over $\mathbb{Q}$. This finishes the proof. $\square$

Lemma 2.2 is somewhat surprising. The result is not true for linear algebraic groups G which are not solvable-by-finite. There are for example $\mathbb{Q}$-defined finite solvable subgroups of $\mathbf{SL}(n, \mathbb{C})$ which are maximal amongst solvable subgroups. We finish now the proof of Proposition 2.1.

Proof of Proposition 2.1 *(Conjugacy):* We shall proof first that any two maximal $\mathbb{Q}$-defined d-subgroups of a $\mathbb{Q}$-defined solvable-by-finite linear algebraic group G are conjugate by an element of $U(G)(\mathbb{Q})$. Let S be the maximal $\mathbb{Q}$-defined d-subgroup of G constructed in the existence proof above. Let S_1 be another maximal $\mathbb{Q}$-defined d-subgroup of G. The connected component S_1° is a $\mathbb{Q}$-defined torus in G°. As such it is contained in a maximal $\mathbb{Q}$-defined torus which is conjugate by an element of $U(G)(\mathbb{Q})$ to S° (see [P1]). Hence we can from now on assume that $S_1^\circ \leq S^\circ$. We distinguish two cases:

Case 1: The dimension of S is 0. In this case S is a maximal $\mathbb{Q}$-defined finite subgroup of G with $G = U(G) \cdot S$. A simple argument shows that S_1 is also finite. Consider first the case that $U(G)$ is abelian. Make $U(G)(\overline{\mathbb{Q}})$ into an S_1-module through conjugation. Note that for every $f \in S_1$ there is a unique $v(f) \in U(G)(\overline{\mathbb{Q}})$ such that $v(f)f \in S$. The function $v : S_1 \to U(G)(\overline{\mathbb{Q}})$ satisfies $v(f_1 f_2) = v(f_1) f_1 v(f_2) f_1^{-1}$ for all $f_1,\ f_2 \in S_1$. Hence it is a derivation of the finite group S_1 into the S_1-module $U(G)(\overline{\mathbb{Q}})$. We also have $\sigma(v(f)) = v(\sigma(f))$ for every σ in the Galois group $\mathbb{G}$ aand every $f \in S_1$. We find an element $v \in U(G)(\mathbb{Q})$ such that $v(f) = v^{-1} f v f^{-1}$ for all $f \in S_1$, see (2.3). Clearly then $v^{-1} S_1 v \leq S$ and the result follows for abelian unipotent radical $U(G)$. The general case is proved by induction on the nilpotency class of $U(G)$. As done twice before we just compare G to G/Z where Z is the center of $U(G)$. We skip the details but remark that it is relevant here that the map $U(G)(\mathbb{Q}) \to U(G)/Z(\mathbb{Q})$ is surjective.

Case 2: The dimension of S is > 0. We shall first argue that $S_1^\circ = S^\circ$. To do this it suffices to show that the dimensions of S_1° and of S° are the same. Note that we already have arranged that $S_1^\circ \leq S^\circ$. So assume that the dimension of S_1° is strictly smaller than that of S°. Let $N_G(S_1^\circ)$ be the normalizer of S_1° in G. We have $S_1 \leq N_G(S_1^\circ)$ and also $S^\circ \leq N_G(S_1)$ (note that $S_1^\circ \leq S^\circ$ and S° is abelian). Let $H := N_G(S_1^\circ)/S_1^\circ$ and $\pi : N_G(S_1^\circ) \to H$ be the quotient homomorphism. Then $\pi(S_1)$ is a $\mathbb{Q}$-define finite subgroup of H and $\pi(S)$ is a $\mathbb{Q}$-defined torus of positive dimension in H. By Lemma 2.2 there is a $\mathbb{Q}$-defined torus T of positive dimension in H which is normalized by $\pi(S_1)$. Define $S_2 := \pi^{-1}(T) \cdot S_1$. It is easy to show that S_2 is a $\mathbb{Q}$-defined d-subgroup of G which is strictly bigger than S_1. This being a contradiction we can from now on assume that $S_1^\circ = S^\circ$. Let $N := N_G(S^\circ)$ be the normalizer of S° in G. We have $S_1,\ S \leq N$. We may also consider the quotient $N_0 := N/S^\circ$. This is a $\mathbb{Q}$-defined unipotent-by-finite linear algebraic group. We write $\pi : N \to N_0$ for the corresponding quotient homomorphism. Notice that both $\pi(S_1)$ and $\pi(S)$ are $\mathbb{Q}$-defined maximal finite subgroups of N_0. By the first case of this prove there is a $v \in U(N_0)(\mathbb{Q})$ with $v\pi(S_1)v^{-1} = \pi(S)$. Since S° consists of semi-simple elements the map π induces by restriction a $\mathbb{Q}$-defined rational isomorphism $\pi : U(N) \to U(N_0)$. Because $U(N)$ is unipotent the induced map $\pi : U(N)(\mathbb{Q}) \to U(N_0)(\mathbb{Q})$ is also surjective. Hence we find a $u \in U(N)(\mathbb{Q})$ with $\pi(u) = v$. It is easy to prove that $uS_1u^{-1} = S$. It remains to be shown that $u \in U(G)(\mathbb{Q})$. By (2.1) we find $u_1 \in U(G)$ and $s \in S$ such that $u = u_1 \cdot s$. Applying the quotient homomorphism $G \to G/U(G)$ we find that $s = 1$. This finishes the proof of the first part of the conjugacy statement.

To prove the second we go exactly through the same steps as above but with all assumptions about groups or maps being defined over $\mathbb{Q}$ removed. Note that the corresponding Lemma 2.2 can in fact be proved by the method given above. We skip the details. $\square$

Let G be a solvable-by-finite $\mathbb{Q}$-defined linear algebraic group decomposed as $G = U(G) \cdot S$ as in (2.1). It can be proved that there is a maximal $\mathbb{Q}$-defined torus $T \leq S$ and a finite subgroup $F \leq S(\overline{\mathbb{Q}})$ such that $S = T \cdot F$. The finite group F can in general not be chosen as being defined over $\mathbb{Q}$.

In the proofs to come we need following technical result concerning algebraic groups.

Lemma 2.3: *Let G_1, G_2 be two $\mathbb{Q}$-defined d-groups and $\beta : G_1 \to G_2$ a $\mathbb{Q}$-defined rational map which is a group isomorphism. Then β^{-1} is rational and $\mathbb{Q}$-defined.*

Proof: Let us first remark that this lemma is well known (over any field of characteristic 0) if G_1 and G_2 are connected. To treat the more general case we think of G_1, G_2 as closed subsets of some affine space. The map β is then the restriction of a polynomial map to G_1. We define $\overline{\mathbb{Q}}[G_1]$, $\overline{\mathbb{Q}}[G_2]$ to be the rings of regular functions on G_1, G_2 over the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$. We write $\beta^* : \overline{\mathbb{Q}}[G_2] \to \overline{\mathbb{Q}}[G_1]$ for the comorphism induced by β. Clearly β^* is injective. We shall prove that β is also surjective.

Let G_1°, G_2° be the connected components of the identity in G_1 respectively G_2. Then $\beta(G_1^\circ) = G_2^\circ$ because β is regular and a group isomorphism. Let $\mu : G_1^\circ \to G_2^\circ$ be the restriction of β to G_1°. Then β^{-1} is regular and $\mathbb{Q}$-defined. Let $g_1, \ldots, g_n \in G_1$ be a system of representatives for the left cosets of G_1° in G_1. Define $h_i := \beta(g_i)$ for $i = 1, \ldots, n$. Then $h_1, \ldots, h_n$ is a system of representatives for the left cosets of G_2° in G_2. Let i be any element of $\{1, \ldots, n\}$. We get $\overline{\mathbb{Q}}$-defined regular isomorphisms of the cosets $\mu_i : C_1^{[i]} := G_1^\circ g_i \to C_2^{[i]} := G_2^\circ h_i$ by defining $\mu_i(x) := \mu(x g_i^{-1}) h_i$. The (regular) inverse of μ_i is given by $\mu_i^{-1}(x) := \mu^{-1}(x h_i^{-1}) g_i$. Let $\Theta : \overline{\mathbb{Q}}[C_2^{[1]}] \times \ldots \times \overline{\mathbb{Q}}[C_2^{[n]}] \to \overline{\mathbb{Q}}[C_1^{[1]}] \times \ldots \times \overline{\mathbb{Q}}[C_1^{[n]}]$ be the direct product of the comorphisms corresponding to the μ_i. Let k now be 1 or 2 and $\rho_k^{[i]} : \overline{\mathbb{Q}}[G_k] \to \overline{\mathbb{Q}}[C_k^{[i]}]$ be the restriction map. Define ρ_k to be the $\overline{\mathbb{Q}}$-algebra homomorphism from $\overline{\mathbb{Q}}[G_k]$ to $\overline{\mathbb{Q}}[C_k^{[1]}] \times \ldots \times \overline{\mathbb{Q}}[C_k^{[n]}]$ defined by the $\rho_k^{[1]}, \ldots, \rho_k^{[n]}$. We get an obviously commutative diagram of $\overline{\mathbb{Q}}$-algebra homomorphisms:

$$\begin{array}{ccc} \overline{\mathbb{Q}}[G_2] & \xrightarrow{\beta^*} & \overline{\mathbb{Q}}[G_1] \\ \downarrow{\scriptstyle \rho_2} & & \downarrow{\scriptstyle \rho_1} \\ \overline{\mathbb{Q}}[C_2^{[1]}] \times \ldots \times \overline{\mathbb{Q}}[C_2^{[n]}] & \xrightarrow{\Theta} & \overline{\mathbb{Q}}[C_1^{[1]}] \times \ldots \times \overline{\mathbb{Q}}[C_1^{[n]}] \end{array} \quad . \tag{2.4}$$

The map Θ is bijective and ρ_1, ρ_2 are obviously injective. Let $\mathfrak{I}_i$ be the kernel of $\rho_1^{[i]}$. Let $i, j \in \{1, \ldots, n\}$ and $i \neq j$ then the ideal $\mathfrak{a} := \mathfrak{I}_i + \mathfrak{I}_j$ is the kernel of the restriction map from $\overline{\mathbb{Q}}[G_1]$ to $\overline{\mathbb{Q}}[C_1^{[i]} \cap C_1^{[j]}]$. Since $C_1^{[i]} \cap C_1^{[j]} = \emptyset$ Hilbert's Nullstellensatz shows $\mathfrak{a} = \overline{\mathbb{Q}}[G_1]$. The Chinese remainder theorem implies that ρ_1 and also ρ_2 are isomorphisms. The diagram (2.4) shows that β^* is an isomorphism. This means that β^{-1} is regular and $\overline{\mathbb{Q}}$-defined. The Galois criterion shows that the regular map β^{-1} is $\mathbb{Q}$-defined. $\square$

We shall discuss some facts concerning the class of $\mathbb{Q}$-defined solvable-by-finite reduced linear algebraic groups. Let G be such a group. We always write $U(G)$ for its unipotent radical and $\mathfrak{U}(G)$ for the Lie algebra of $U(G)$. Since $U(G)$ is a $\mathbb{Q}$-defined unipotent algebraic group the Lie algebra $\mathfrak{U}(G)$ is also defined over $\mathbb{Q}$. The exponential map $\exp : \mathfrak{U}(G) \to U(G)$ gives us a $\mathbb{Q}$-defined rational identification of $\mathfrak{U}(G)$ with $U(G)$. The automorphism group $\mathrm{Aut}(\mathfrak{U}(G))$ of the Lie algebra $\mathfrak{U}(G)$ is then naturally a $\mathbb{Q}$-defined linear algebraic group. We have a $\mathbb{Q}$-defined rational representation:

$$(2.5)\quad \alpha_G : G \to \mathrm{Aut}(\mathfrak{U}(G)), \quad \alpha_G(g)(x) := \exp^{-1}(g\exp(x)g^{-1}) \quad (g \in G,\, x \in \mathfrak{U}(G)).$$

The kernel of α_G coincides with the centralizer of $U(G)$ in G and contains the center $\mathbf{Z}(U(G))$ of $U(G)$.

Definition 2.4: *Let G be a solvable-by-finite $\mathbb{Q}$-defined algebraic group. We call G reduced if* $\ker(\alpha_G) \le U(G)$.

We shall often need the following elementary results about reduced groups.

Lemma 2.5: *Let G, G_1 be solvable-by-finite $\mathbb{Q}$-defined linear algebraic groups. Let S be a maximal $\mathbb{Q}$-defined d-subgroup of G. If H is a subgroup of G we define $\mathbf{Z}_U(H)$ to be its subgroup consisting of those elements which centralize $U(G)$. We have:*

(i) *G is reduced if and only if* $\ker(\alpha_G) = \mathbf{Z}(U(G))$.

(ii) *If G is reduced then we have* $\mathbf{Z}(G) \le \mathbf{Z}(U(G))$.

(iii) *G is reduced if and only if* $\mathbf{Z}_U(S) = \{1\}$.

(iv) *$\mathbf{Z}_U(S)$ is a $\mathbb{Q}$-defined normal subgroup of G and the quotient $G/\mathbf{Z}_U(S)$ is a reduced solvable $\mathbb{Q}$-defined linear algebraic group.*

(v) *If $G_1 \le G$ is a $\mathbb{Q}$-defined subgroup of finite index in G and if G is reduced then G_1 is reduced.*

(vi) *If $G_1 \le G$ is a $\mathbb{Q}$-defined subgroup of finite index in G and if G_1 is reduced then $\mathbf{Z}_U(S)$ is a finite $\mathbb{Q}$-defined normal subgroup of G.*

Proof: (i) and (ii) are evident.

(iii): Assume that $\mathbf{Z}_U(S) = \{1\}$. We have $G = U(G) \cdot S$ as stated in (2.1). Let $u \cdot s \in \ker(\alpha_G)$ with $u \in U(G)$ and $s \in S$. We have $\alpha_G(u) = \alpha_G(s)^{-1}$. Since the left-hand side of this equation is unipotent and the right-hand side is semi-simple both sides are equal to 1. By our assumption we have $s = 1$. This proves one direction of our statement. The other direction is evident.

(iv): The group $\mathbf{Z}_U(S)$ is evidently $\mathbb{Q}$-defined, we prove that it is normal in G. Let $g \in G$ be decomposed as $g = us$ with $u \in U(G)$ and $s \in S$. Then $g^{-1}tg = s^{-1}ts$ for all $t \in \mathbf{Z}_U(S)$ which then shows that $\mathbf{Z}_U(S)$ is normal in G. We write $\hat{G}$ for the quotient group $\hat{G} = G/\mathbf{Z}_U(S)$. Let $\hat{S}$ be the image of S in $\hat{G}$. It is a maximal $\mathbb{Q}$-defined d-subgroup of $\hat{G}$. Let $t \in S$ represent an element of $\mathbf{Z}_U(\hat{S})$. This means that $tut^{-1}u^{-1} \in \mathbf{Z}_U(S)$ for all $u \in U(G)$. The element $tut^{-1}u^{-1}$ is also in $U(G)$ and hence it is equal to 1. This implies that $t \in \mathbf{Z}_U(S)$. The result (iv) is then implied by (iii).

(v): Since $U(G)$ is connected we find $U(G_1) = U(G)$ and the result follows.

(vi): We again have $U(G_1) = U(G)$. Let n be the index be the index of G_1 in G and $m := n!$. Then $g^m \in G_1$ for all $g \in G$. There is a maximal $\mathbb{Q}$-defined d-subgroup S_1 of G_1 which is contained in S. The decompositions (2.1) for G_1 and G show that $s^m \in S_1$ for all $s \in S$. This implies using (iii) that $s^m = 1$ for all $s \in \mathbf{Z}_U(S)$. Since every linear group of finite exponent is finite we can infer that $\mathbf{Z}_U(S)$ is finite. Everything else follows from (iv). $\square$

In addition to the notation already introduced some more is required in the following. Let G be a solvable-by-finite $\mathbb{Q}$-defined linear algebraic group which is also assumed to be reduced. We define

$$\text{(2.6)} \quad \mathfrak{ZU}(G) := \exp^{-1}(\mathbf{Z}(U(G))),\ \mathfrak{Z}(G^\circ) := \exp^{-1}(\mathbf{Z}(G^\circ)),\ \mathfrak{Z}(G) := \exp^{-1}(\mathbf{Z}(G)).$$

The subspaces $\mathfrak{ZU}(G)$, $\mathfrak{Z}(G^\circ)$ and $\mathfrak{Z}(G)$ of the Lie algebra $\mathfrak{U}(G)$ are defined over $\mathbb{Q}$ and invariant under the action (2.5) of G. The $\mathbb{Q}$-subspace $\mathfrak{ZU}(G)(\mathbb{Q})$ underlying $\mathfrak{ZU}(G)$ is defined to be $\mathfrak{ZU}(G)(\mathbb{Q}) := \exp^{-1}(\mathbf{Z}(U(G))(\mathbb{Q}))$. We define analogously $\mathfrak{Z}(G^\circ)(\mathbb{Q}) = \exp^{-1}(\mathbf{Z}(G^\circ)(\mathbb{Q}))$ and $\mathfrak{Z}(G)(\mathbb{Q}) = \exp^{-1}(\mathbf{Z}(G)(\mathbb{Q}))$. All of the spaces $\mathfrak{ZU}(G)(\mathbb{Q})$, $\mathfrak{Z}(G^\circ)(\mathbb{Q})$, $\mathfrak{Z}(G)(\mathbb{Q})$ are invariant under $G(\mathbb{Q})$. The group $U(G)$ acts trivially on $\mathfrak{ZU}(G)$. Since $G/U(G)$ is reductive we get a decompositions

$$\text{(2.7)} \qquad \mathfrak{ZU}(G) = \mathfrak{Y}_G \oplus \mathfrak{Z}(G^\circ), \qquad \mathfrak{Z}(G^\circ) = \mathfrak{Y}_G^\circ \oplus \mathfrak{Z}(G)$$

where $\mathfrak{Y}_G$ and $\mathfrak{Y}_G^\circ$ are $\mathbb{Q}$-defined G-invariant subspace. We again write $\mathfrak{Y}_G(\mathbb{Q})$, $\mathfrak{Y}_G^\circ(\mathbb{Q})$ for the underlying ($G(\mathbb{Q})$-invariant) $\mathbb{Q}$-vector spaces. Note that the centralizer of G in $\mathfrak{Y}_G \oplus \mathfrak{Y}_G^\circ$ (that is the space of all elements of $\mathfrak{Y}_G \oplus \mathfrak{Y}_G^\circ$ which are fixed by all $g \in G$) is trivial. The same result holds for the centralizer of G° in $\mathfrak{Y}_G$. Note that the exponential map followed by the quotient homomorphism induces $G/U(G)$-module isomorphisms

$$\text{(2.8)} \qquad \exp : \mathfrak{Y}_G(\mathbb{Q}) \to \mathbf{Z}(U(G))/\mathbf{Z}(G^\circ)(\mathbb{Q}), \qquad \exp : \mathfrak{Y}_G^\circ(\mathbb{Q}) \to \mathbf{Z}(G^\circ)/\mathbf{Z}(G)(\mathbb{Q})$$

where the action of $G/U(G)(\mathbb{Q})$ on the right-hand groups is by conjugation.

We come now to the discussion of arithmetic subgroups of solvable-by-finite linear algebraic groups. We shall often use the following facts from the theory of arithmetic groups. Suppose that G is a $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G$ an arithmetic subgroup. If H is a $\mathbb{Q}$-defined subgroup then $H \cap \Gamma$ is arithmetic in H. If H is also normal in G, then Γ projects to an arithmetic subgroup of G/H. We shall also use that if Γ is a Zariski-dense subgroup of G then $\Gamma \cap G^\circ$ is Zariski-dense in G°. See [B2] and [P-R] for these results.

Let G be a solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G$ be an arithmetic subgroup. It is known that Γ is a polycyclic group, in fact every solvable subgroup of $\mathbf{GL}(n, \mathbb{Z})$ is polycyclic (see [Se], Chapter 2). We define

$$U(G, \Gamma) := \Gamma \cap U(G). \tag{2.9}$$

The finitely generated and torsion-free group $U(G, \Gamma)$ is an arithmetic subgroup of $U(G)$. It is always contained in $U(G)(\mathbb{Q})$ because $U(G)$ is uniquely divisible. Also $U(G, \Gamma)$ is always Zariski-dense in $U(G)$. It is further known that the $\mathbb{Q}$-span of $\exp^{-1}(U(G, \Gamma))$ is equal to $\mathfrak{U}(G)(\mathbb{Q})$. See [Se], chapter 6 for these properties of $U(G, \Gamma)$. Let $S \leq G$ be a maximal $\mathbb{Q}$-defined d-subgroup. Then $\Gamma \cap S$ is an arithmetic subgroup of S and $U(G, \Gamma) \cdot (\Gamma \cap S)$ has finite index in Γ.

If Γ is a linear group we write $\mathcal{F}(\Gamma)$ for its Fitting subgroup, that is its biggest normal nilpotent subgroup. The following lemma is important in the proofs of Theorems A, A' and B. Its proof uses an argument from [P2]. We write $\langle M \rangle$ for the subgroup generated by a substset $M \subseteq G$ of a group G.

Lemma 2.6: *Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G$ an arithmetic subgroup. Then $\mathcal{F}(\Gamma) = U(G, \Gamma)$.*

Proof: Clearly $U(G, \Gamma)$ is contained in $\mathcal{F}(\Gamma)$. Let γ be an element from $\mathcal{F}(\Gamma)$, put $A := U(G, \Gamma) \cdot \langle \gamma \rangle$ and let $\overline{A}$ be the Zariski-closure of A. Then $\overline{A}$ is a nilpotent linear algebraic group. Let $\gamma = \gamma_u \cdot \gamma_s$ be the Jordan decomposition of γ, that is γ_u is unipotent, γ_s is semi-simple and the two commute. We also have γ_u, $\gamma_s \in \overline{A}$. From $U(G, \Gamma) \leq A$ we infere that $U(G) \leq \overline{A}$. Hence the group $U(G) \cdot \langle \gamma_s \rangle$ is nilpotent. This implies that $\mathfrak{U}(G) \rtimes \langle \alpha_G(\gamma_s) \rangle$ is nilpotent. Since $\alpha_G(\gamma_s)$ is a semi-simple transformation of $\mathfrak{U}(G)$ this can only happen if $\alpha_G(\gamma_s) = 1$. We infer that $\gamma_s = 1$ because G is reduced. Hence γ is unipotent. Let now $G = U(G) \cdot S$ be decomposed as in (2.1). Let $\gamma = \gamma_1 \cdot \gamma_2$ with $\gamma_1 \in U(G)$ and $\gamma_2 \in S$. Since γ and γ_1 are unipotent we have $\gamma_2 = 1$ and the result follows. □

Let G be a solvable-by-finite linear algebraic group defined over $\mathbb{Q}$ and $S \leq G$ be a maximal d-subgroup of G which is also defined over $\mathbb{Q}$. We then have $G = U(G) \cdot S$

as in (2.1). Then $G/U(G)$ is a $\mathbb{Q}$-defined d-group (in fact isomorphic to S). The connected component $(G/U(G))^\circ$ is a $\mathbb{Q}$-defined maximal torus in $G/U(G)$. We write $\pi_{\mathrm{U}} : G \to G/U(G)$ for the quotient homomorphism. Let $\Gamma \le G$ be a Zariski-dense arithmetic subgroup. Then $\pi_{\mathrm{U}}(\Gamma)$ is a finitely generated abelian-by-finite group which is Zariski-dense in $G/U(G)$. Its abelian subgroup $\pi_{\mathrm{U}}(\Gamma) \cap (G/U(G))^\circ$ is Zariski-dense in $(G/U(G))^\circ$. We define

$$(2.10) \qquad M(\Gamma) := \pi_{\mathrm{U}}(\Gamma) \cap (G/U(G))^\circ, \qquad F(\Gamma) := \pi_{\mathrm{U}}(\Gamma)/M(\Gamma).$$

It is easy to see that $M(\Gamma)$ is a finitely generated abelian group and $F(\Gamma)$ is a finite group. We obtain an exact sequence

$$(2.11) \qquad \{1\} \to M(\Gamma) \to \pi_{\mathrm{U}}(\Gamma) \to F(\Gamma) \to \{1\}.$$

We also think of $M(\Gamma)$ as a $F(\Gamma)$-module the action being induced by conjugation by representatives taken from $\pi_{\mathrm{U}}(\Gamma)$. Suppose now further that G is reduced. The action (by conjugation) of Γ on $U(G,\Gamma)$ leads to an action of $\pi_{\mathrm{U}}(\Gamma)$ on the spaces $\mathfrak{Y}_G(\mathbb{Q})$, $\mathfrak{Y}_G^\circ(\mathbb{Q})$ introduced in (2.6), (2.7), (2.8). The action of $M(\Gamma)$ on $\mathfrak{Y}_G^\circ(\mathbb{Q})$ is trivial.

If A is a group and B, C are A-modules we write $\mathrm{Hom}_A(B,C)$ for the group of A-equivariant homomorphisms. For $i \in \mathbb{N}$ we denote the i-th cohomology group of A with coefficients in B by $H^i(A,B)$ (see [W] for the definition). By definition $H^0(A,B)$ is the subgroup of those elements in B which are left fixed by all elements of A. The first cohomology group $H^1(A,B)$ is the group of derivations modulo its sugroup of inner derivations. We need the following computation of cohomology groups.

Lemma 2.7: *Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma \le G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup. Then the following hold.*

(i) $H^0(M(\Gamma), \mathfrak{Y}_G(\mathbb{Q})) = \{0\}$.

(ii) $H^1(\pi_{\mathrm{U}}(\Gamma), \mathfrak{Y}_G(\mathbb{Q})) = \{0\}$.

(iii) $H^1(\pi_{\mathrm{U}}(\Gamma), \mathfrak{Y}_G^\circ(\mathbb{Q})) \cong \mathrm{Hom}_{F(\Gamma)}(M(\Gamma), \mathfrak{Y}_G^\circ(\mathbb{Q}))$, *where the isomorphism is given by restricting derivations from $\pi_{\mathrm{U}}(\Gamma)$ to $M(\Gamma)$.*

(iv) *If $\pi_{\mathrm{U}}(\Gamma)$ is nilpotent then* $H^1(\pi_{\mathrm{U}}(\Gamma), \mathfrak{Y}_G^\circ(\mathbb{Q})) = \{0\}$.

Proof: (i): Let $v \in H^0(M(\Gamma), \mathfrak{Y}_G(\mathbb{Q}))$ then v is an element in $\mathfrak{Y}_G(\mathbb{Q}))$ which is left fixed by all elements of $M(\Gamma)$. Consider $u = \exp(v) \in \mathbf{Z}(U(G))$. Then u is centralized by $M(\Gamma)$. Since $M(\Gamma)$ is Zariki-dense in $(G/U(G))^\circ$ it is even centralized by $(G/U(G))^\circ$. Since $\pi_{\mathrm{U}}(G^\circ) = (G/U(G))^\circ$ the element u is centralized by G°. Since $\mathbf{Z}(U(G)) \le G^\circ$ we have $u \in \mathbf{Z}(G^\circ)$ and $v = 0$.

(ii): From (i) we can infer that $H^1(M(\Gamma), \mathfrak{Y}_G(\mathbb{Q})) = \{0\}$. This result can be found in [Se], chapter 3, theorem 2^{**}. Since $\mathfrak{Y}_G(\mathbb{Q})$ is a $\mathbb{Q}$-vector space the restriction homomorphism $H^1(\pi_{\mathrm{U}}(\Gamma), \mathfrak{Y}_G(\mathbb{Q})) \to H^1(M(\Gamma), \mathfrak{Y}_G(\mathbb{Q}))$ is injective.

(iii): Since $M(\Gamma)$ acts trivially on $\mathfrak{Y}^\circ_G(\mathbb{Q}))$ the exact sequence (2.11) leads to the 5-term exact sequence of cohomology

$$
\begin{aligned}
\{0\} \to H^1(F(\Gamma), \mathfrak{Y}^\circ_G(\mathbb{Q})) &\to H^1(\pi_{\mathrm{U}}(\Gamma), \mathfrak{Y}^\circ_G(\mathbb{Q})) \\
&\to \mathrm{Hom}_{F(\Gamma)}(M(\Gamma),\, \mathfrak{Y}^\circ_G(\mathbb{Q})) \to H^2(F(\Gamma), \mathfrak{Y}^\circ_G(\mathbb{Q})).
\end{aligned} \tag{2.12}
$$

We have $H^1(F(\Gamma), \mathfrak{Y}^\circ_G(\mathbb{Q})) = \{0\}$ and $H^2(F(\Gamma), \mathfrak{Y}^\circ_G(\mathbb{Q})) = \{0\}$ because $F(\Gamma)$ is a finite group. We remark that the isomorphism between $H^1(\pi_{\mathrm{U}}(\Gamma), \mathfrak{Y}^\circ_G(\mathbb{Q}))$ and $\mathrm{Hom}_{F(\Gamma)}(M(\Gamma),\, \mathfrak{Y}^\circ_G(\mathbb{Q}))$ which then follows from (2.12) is given by the restriction of derivations from $\pi_{\mathrm{U}}(\Gamma)$ to $M(\Gamma)$.

(iv): If $\pi_{\mathrm{U}}(\Gamma)$ is nilpotent then $F(\Gamma)$ acts unipotently on $M(\Gamma)$ (that is we have a composition series of $F(\Gamma)$-submodules in $M(\Gamma)$ such that $F(\Gamma)$ acts trivially on its factors) and trivially on $\mathbb{Q} \otimes_{\mathbb{Z}} M(\Gamma)$. Let $\varphi \in \mathrm{Hom}_{F(\Gamma)}(M(\Gamma),\, \mathfrak{Y}^\circ_G(\mathbb{Q}))$ and $\mathrm{Im}(\varphi) \leq \mathfrak{Y}^\circ_G(\mathbb{Q})$ its image. It follows from our definitions that $\exp(\mathrm{Im}(\varphi))$ is contained in $\mathbf{Z}(G)$ hence $\mathrm{Im}(\varphi) = \{0\}$. □

The following definition is motivated by Lemma 2.7. It is relevant in the formulation of Theorem A'.

Definition 2.8: *Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G$ a Zariski-dense arithmetic subgroup. We call Γ separated in G if*

$$
\mathrm{Hom}_{F(\Gamma)}(M(\Gamma),\, \mathbf{Z}(G^\circ)/\mathbf{Z}(G)(\mathbb{Q})) = \{0\}. \tag{2.13}
$$

Clearly if G is connected then every arithmetic subgroup is separated. Note that $H^1(\pi_{\mathrm{U}}(\Gamma), \mathfrak{Y}^\circ_G(\mathbb{Q})) = \{0\}$ if Γ is separated in G. It follows from Lemma 2.7 (iv) that Γ is separated in G if $\Gamma/U(G,\Gamma)$ is nilpotent.

We are now ready to give the

Proof of Theorems A, A': By Lemma 2.6 φ induces an isomorphism $\varphi : U(G_1, \Gamma_1) \to U(G_2, \Gamma_2)$. By results of Malcev (see [Mc]) we find a $\mathbb{Q}$-defined rational isomorphism $\Phi_u : U(G_1) \to U(G_2)$ such that $\Phi_u(\gamma) = \varphi(\gamma)$ for all $\gamma \in U(G_1, \Gamma_1)$. This rational isomorphism induces a $\mathbb{Q}$-defined Lie algebra isomorphism $\tilde{\Phi}_u : \mathfrak{U}(G_1) \to \mathfrak{U}(G_2)$ by $\tilde{\Phi}_u := \exp^{-1} \circ \Phi_u \circ \exp$. The isomorphism $\tilde{\Phi}_u$ gives us a $\mathbb{Q}$-defined rational isomorphism $\Psi_u : \mathrm{Aut}(\mathfrak{U}(G_1)) \to \mathrm{Aut}(\mathfrak{U}(G_2))$ of the automorphism groups of the corresponding Lie algebras defined by $\Psi_u(\Theta) := \tilde{\Phi}_u \circ \Theta \circ \tilde{\Phi}_u^{-1}$ where $\Theta \in \mathrm{Aut}(\mathfrak{U}[G_1])$.

In the following k is always supposed to be 1 or 2. Let $\alpha_k = \alpha_{G_k} : G_k \to \mathrm{Aut}(\mathfrak{U}(G_k))$ be the homomorphism defined in (2.5). The map α_k is a $\mathbb{Q}$-defined rational homomorphism of G_k into the automorphism group $\mathrm{Aut}(\mathfrak{U}(G_k))$. We have $\ker(\alpha_k) = \mathbf{Z}(U(G_k))$. Notice also that $\Psi_u(\alpha_1(u)) = \alpha_2(\Phi_u(u))$ holds for all $u \in U(G_1)$.

By a straightforward computation using our definitions we find for $\gamma \in \Gamma_1$:

$$\Psi_u(\alpha_1(\gamma)) = \alpha_2(\varphi(\gamma)). \tag{2.14}$$

The groups $\alpha_k(\Gamma_k)$ are Zariski-dense arithmetic subgroups in $\alpha_k(G_k)$. We infer from (2.14) that $\Psi_u(\alpha_1(G_1)) = \alpha_2(G_2)$. Hence Ψ_u gives us a $\mathbb{Q}$-defined rational isomorphism between $\alpha_1(G_1)$ and $\alpha_2(G_2)$.

We now choose a maximal $\mathbb{Q}$-defined d-subgroup S_1 in G_1. Then $\hat{S}_2 := \Psi_u(\alpha_1(S_1))$ is a maximal $\mathbb{Q}$-defined d-subgroup of $\alpha_2(G_2)$. Consider now the $\mathbb{Q}$-defined algebraic subgroup $H := \alpha_2^{-1}(\hat{S}_2)$ of G_2 and let S_2 be a maximal $\mathbb{Q}$-defined subgroup in H. Clearly S_2 is also a maximal $\mathbb{Q}$-defined d-subgroup in G_2 and α_2 induces a $\mathbb{Q}$-defined rational homomorphism $\beta := \alpha_2|_{S_2} : S_2 \to \hat{S}_2$ which is also a group isomorphism. The latter is implied by the fact that the kernel of α_2 is unipotent. Hence β^{-1} is rational and $\mathbb{Q}$-defined by Lemma 2.3.

We shall now define a map Φ_0 which after some slight modification will serve as our Φ. Given an element $g \in G_1$ we may uniquely decompose it as $g = t_g \cdot u_g$ with $t_g \in S_1$ and $u_g \in U(G_1)$. We put

$$\Phi_0(g) := \beta^{-1} \circ \Psi_u \circ \alpha_1(t_g) \cdot \Phi_u(u_g). \tag{2.15}$$

Some straightforward considerations show that $\Phi_0 : G_1 \to G_2$ is a $\mathbb{Q}$-defined rational isomorphism. It is for example necessary to show

$$\Phi_u(t \cdot u \cdot t^{-1}) = \beta^{-1}(\Psi_u(\alpha_1(t))) \cdot \Phi_u(u) \cdot (\beta^{-1}(\Psi_u(\alpha_1(t))))^{-1} \tag{2.16}$$

for $t \in S_1$ and $u \in U(G_1)$. This can easily be done on the level of the Lie algebras $\mathfrak{U}(G_1)$, $\mathfrak{U}(G_2)$. From what was said above it follows that

$$\alpha_2(\Phi_0(g)) = \Psi_u(\alpha_1(g)) \qquad \text{for all } g \in G_1. \tag{2.17}$$

For $\gamma \in \Gamma_1$ we get from (2.14), (2.17) that $\alpha_2(\Phi_0(\gamma)\varphi(\gamma)^{-1}) = 1$, hence

$$v(\gamma) := \Phi_0(\gamma) \cdot \varphi(\gamma)^{-1} \in \mathbf{Z}(U(G_2))(\mathbb{Q}). \tag{2.18}$$

Note that if $\gamma \in U(G_1, \Gamma_1)$ then $v(\gamma) = 1$. We have now constructed a $\mathbb{Q}$-defined rational isomorphism $\Phi_0 : G_1 \to G_2$ and a map $v : \Gamma_1 \to \mathbf{Z}(U(G_2))(\mathbb{Q})$ so that the analogue of (1.1) is satisfied. Our construction depends basically on the choice of the d-subgroup S_2 in H. We shall now show that by possibly altering this choice we can make the new v have its values in $\mathbf{Z}(G_2^\circ)(\mathbb{Q})$.

Consider the $\mathbb{Q}$-vector spaces $\mathfrak{Z}\mathfrak{U}(G_2)(\mathbb{Q})$, $\mathfrak{Z}(G_2^\circ)(\mathbb{Q})$ and $\mathfrak{Y}_{G_2}(\mathbb{Q})$ defined in (2.6), (2.7). We shall use now the notation introduced just before Lemma 2.7. Make $\mathfrak{Z}\mathfrak{U}(G_2)(\mathbb{Q})$ into a Γ_1-module by defining $\gamma \cdot x := \exp^{-1}(\varphi(\gamma)\exp(x)\varphi(\gamma)^{-1})$ for $\gamma \in \Gamma_1$ and

$x \in \mathfrak{ZU}(G_2)(\mathbb{Q})$. In fact $U(G_1, \Gamma_1)$ acts trivially and we may consider $\mathfrak{ZU}(G_2)(\mathbb{Q})$ as a $\pi_{\mathrm{U}}(\Gamma_1)$ module. Both $\mathfrak{Z}(G_2^\circ)(\mathbb{Q})$ and $\mathfrak{Y}_{G_2}(\mathbb{Q})$ are submodules. Define $\tilde{v} : \Gamma_1 \to \mathfrak{ZU}(G_2)(\mathbb{Q})$ by $\tilde{v}(\gamma) := \exp^{-1}(v(\gamma))$ $(\gamma \in \Gamma_1)$. An obvious computation shows that the map $\tilde{v}$ is a derivation of Γ_1 into $\mathfrak{ZU}(G_2)(\mathbb{Q})$. That is $\tilde{v}(\gamma_1\gamma_2) = \tilde{v}(\gamma_1) + \gamma_1 \cdot \tilde{v}(\gamma_2)$ holds for γ_1, $\gamma_2 \in \Gamma_1$. Hence the component of $\tilde{v}$ in $\mathfrak{Y}_{G_2}(\mathbb{Q}))$ represents an element of $H^1(\pi_{\mathrm{U}}(\Gamma_1), \mathfrak{Y}_{G_2}(\mathbb{Q}))$. By Lemma 2.6 φ induces an isomorphism between $\pi_{\mathrm{U}}(\Gamma_1)$ and $\pi_{\mathrm{U}}(\Gamma_1)$. We infer from Lemma 2.7 (ii) that $H^1(\pi_{\mathrm{U}}(\Gamma_1), \mathfrak{Y}_{G_2}(\mathbb{Q})) = \{0\}$.

We have proved now that we may alter the derivation $\tilde{v}$ by an inner derivation so that the result has values in $\mathfrak{Z}(G_2^\circ)(\mathbb{Q})$. This means that there is a $x \in \mathbf{Z}(U(G_2))(\mathbb{Q})$ so that

$$v(\gamma) \cdot x\,\varphi(\gamma)\,x^{-1}\,\varphi(\gamma)^{-1} \in \mathbf{Z}(G_2^\circ)(\mathbb{Q}) \qquad \text{for all } \gamma \in \Gamma_1. \tag{2.19}$$

Define $\Phi(g) = x\,\Phi_0(g)\,x^{-1}$ for all $g \in G_1$ and

$$u(\gamma) := \Phi(\gamma)\,\varphi(\gamma)^{-1} = x\,\Phi_0(\gamma)\,x^{-1}\varphi(\gamma)^{-1} = v(\gamma) \cdot x\,\varphi(\gamma)\,x^{-1}\,\varphi(\gamma)^{-1}. \tag{2.20}$$

Theorem A is implied by (2.19), (2.20). Theorem A' is proved by the same argument but using $\mathfrak{Y}^\circ_{G_2}(\mathbb{Q})$ instead of $\mathfrak{Y}_{G_2}(\mathbb{Q})$. The relevant vanishing result for the cohomology follows from Lemma 2.7 (iii). □

The choices made for the construction of the homomorphism Φ in Theorem A' imply certain compatibility properties. These are formulated in Theorem C and Proposition 2.10. In the proofs to come we shall several times use an argument which we formulate in the following simple lemma.

Lemma 2.9: *Let G be a reduced solvable $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup. Let Φ, Ψ be two $\mathbb{Q}$-defined rational automorphisms of G. Assume that there is a homomorphism $w : \Gamma \to \mathbf{Z}(G)$ which is trivial on $\mathcal{F}(\Gamma)$ such that $\Phi(\gamma) = w(\gamma) \cdot \Psi(\gamma)$ for all $\gamma \in \Gamma$. Then $\Phi = \Psi$ and $w \equiv 1$.*

Proof: Define $\Theta(g) := \Phi(g) \cdot \Psi(g)^{-1}$ for $g \in G$. This is a $\mathbb{Q}$-defined rational map from G to G. We have $\Theta(\Gamma) \subseteq \mathbf{Z}(G)$. We conclude $\Theta(G) \subseteq \mathbf{Z}(G)$ because Γ is Zariski-dense in G. The computation

$$\begin{aligned} \Theta(g_1g_2) &= \Phi(g_1g_2)\,\Psi(g_1g_2)^{-1} \\ &= \Phi(g_1)\ \Phi(g_2) \cdot \Psi(g_2)^{-1}\ \Phi(g_1)^{-1}\ \Phi(g_1) \cdot \Psi(g_1)^{-1} = \Theta(g_1)\,\Theta(g_2). \end{aligned} \tag{2.21}$$

then shows that then Θ is a homomorphism from G to G. If $\gamma \in \Gamma \cap U(G) = U(G, \Gamma)$ then $\Theta(\gamma) = 1$ by Lemma 2.6 and our assumption. Since $U(G, \Gamma)$ is Zariski-dense in $U(G)$ we infer that Θ is trivial on $U(G)$. Let G be decomposed as in (2.1). The restriction of Θ to S is a $\mathbb{Q}$-defined rational homomorphism of the d-group S into the unipotent group $\mathbf{Z}(G)$ and hence has to be trivial. We conclude that Θ is trivial on G. This proves the lemma. $\square$

Proof of Theorem B: We shall use here the notation introduced just before Lemma 2.7. Suppose that Γ is not separated in G. Then by Lemma 2.7 (iii) there is a derivation $\tilde{w} : \pi_{\mathrm{U}}(\Gamma) \to \mathfrak{Y}_G(\mathbb{Q})$ which is not an inner derivation. Multiplying w by a suitable integer we may assume that $\tilde{w}(\gamma) \in \exp^{-1}(\mathbf{Z}(U(G,\Gamma)) \cap G^\circ)$ for all $\gamma \in \pi_{\mathrm{U}}(\Gamma)$. The restriction $\tilde{w}_0$ of $\tilde{w}$ to $M(\Gamma)$ is a homomorphism $\tilde{w}_0 : M(\Gamma) \to \mathfrak{Z}(G^\circ)$. Moreover the image of $\tilde{w}_0$ is not contained in $\mathfrak{Z}(G)$. This follows because the isomorphism described in Lemma 2.7 (iii) is given by restriction from $\pi_{\mathrm{U}}(\Gamma)$ to $M(\Gamma)$ (see the proof of Lemma 2.7 (iii)).

Define $w(\gamma) := \exp(\tilde{w}(\pi_{\mathrm{U}}(\gamma)))$ for $\gamma \in \Gamma$ and $w_0(\gamma) := \exp(\tilde{w}_0(\pi_{\mathrm{U}}(\gamma)))$ for $\gamma \in \Gamma \cap G^\circ$. Notice w_0 is the restriction of w to $\Gamma \cap G^\circ$ and that the image of w_0 is not contained in $\mathbf{Z}(G)$. Define further $\varphi(\gamma) := w(\gamma) \cdot \gamma$ for $\gamma \in \Gamma$. By our assumptions we have $\varphi(\gamma) \in \Gamma$ for all $\gamma \in \Gamma$. It is straightforward to see that φ is an automorphism of Γ.

Suppose now that there are Φ and u as described in the statement of the theorem. In particular we have $\Phi(\gamma) = u(\gamma) w_0(\gamma)\gamma$ for all $\gamma \in \Gamma \cap G^\circ$. Since G° is reduced by Lemma 2.5 (v) and since $\Gamma \cap G^\circ$ is Zariski-dense in G° we are in the position to apply Lemma 2.9 and obtain that $w_0(\gamma) = u(\gamma)^{-1}$ for all $\gamma \in \Gamma \cap G^\circ$. This contradicts the fact that the image of w_0 is not contained in $\mathbf{Z}(G)$ and the Theorem is proved. $\square$

Proof of Theorem C: Let $\varphi_1, \varphi_2 \in \mathrm{Aut}(\Gamma)$ and put $\varphi_3 := \varphi_1 \circ \varphi_2$. Let $\Phi_1, \Phi_2, \Phi_3 : G \to G$ be the algebraic isomorphisms corresponding to $\varphi_1, \varphi_2, \varphi_3$ constructed in Theorem A'. Let $u_1, u_2, u_3 : \Gamma \to \mathbf{Z}(G)(\mathbb{Q})$ be the corresponding homomorphisms. We shall show that $\Phi_3 = \Phi_1 \circ \Phi_2$.

For $\gamma \in \Gamma$ we have from (1.1):

$$(2.22)\quad \Phi_1 \circ \Phi_2(\gamma) = \Phi_1(u_2(\gamma)) \cdot u_2(\varphi_2(\gamma)) \cdot \varphi_1 \circ \varphi_2(\gamma), \qquad \Phi_3(\gamma) = u_3(\gamma) \cdot \varphi_1 \circ \varphi_2(\gamma).$$

The formulas (2.22) and Theorem A' show that Φ_3 and $\Phi_1 \circ \Phi_2$ satisfy the hypotheses of Lemma 2.9. We conclude that $\Phi_3 = \Phi_1 \circ \Phi_2$.

This shows the existence of the homomorphism D. The properties which relate D and u are simple consequences of Theorem A'. The uniqueness of D, u follows from Lemma 2.9 by a straightforward argument. $\square$

Before we proceed we need some terminology. Let Δ be a group and M an abelian group. A Δ-bimodule structure on M is an action $(\delta, m) \mapsto \delta \cdot m$ together with an action from the right $(m, \delta) \mapsto m \cdot \delta$ ($\delta \in \Delta$, $m \in M$) of Δ on M such that $(\delta \cdot m) \cdot \rho = \delta \cdot (m \cdot \rho)$ for all $\delta, \rho \in \Delta$ and $m \in M$. A bimodule derivation of Δ into the bimodule M is a map $\lambda : \Delta \to M$ such that

$$(2.23)\qquad \lambda(\delta_1\delta_2) = \lambda(\delta_1) \cdot \delta_2 + \delta_1 \cdot \lambda(\delta_2) \qquad \text{for all } \delta_1, \delta_2 \in \Delta.$$

A bimodule derivation λ is called inner if there is an $m \in M$ so that $\lambda(\delta) = \delta \cdot m - m \cdot \delta$. The first cohomology group $H^1_{\mathrm{bi}}(\Delta, M)$ of the group Δ in its bimodule M is defined to be the group of bimodule derivations modulo its subgroup of inner derivations.

In the following we formulate some further properties of the homomorphism D and the map u from Theorem C.

Proposition 2.10: *Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup which is separated in G. Let $D : \mathrm{Aut}(\Gamma) \to \mathrm{Aut}_{\mathbb{Q}}(G)$ and $u : \mathrm{Aut}(\Gamma) \to \mathrm{Hom}(\Gamma, \mathbf{Z}(G)(\mathbb{Q}))$ be defined as in Theorem C. Then the following hold:*

(i) *If φ is an inner automorphism of Γ, then D_φ is the corresponding inner automorphism of G and $u_\varphi \equiv 1$.*

(ii) *Take on $\mathrm{Hom}(\Gamma, \mathbf{Z}(G)(\mathbb{Q}))$ the $\mathrm{Aut}(\Gamma)$-bimodule structure given by $\varphi_1 \cdot v \cdot \varphi_2 := D_{\varphi_1} \circ v \circ \varphi_2$. Then the map $\varphi \to u_\varphi$ is a bi-module derivation of $\mathrm{Aut}(\Gamma)$ into $\mathrm{Hom}(\Gamma, \mathbf{Z}(G)(\mathbb{Q}))$.*

Proof: (i): Let $\delta \in \Gamma$ such that $\varphi(\gamma) = \delta\gamma\delta^{-1}$ for all $\gamma \in \Gamma$. Define a map $\Theta : G \to G$ by $\Theta(g) := D_\varphi(g)\gamma g^{-1}\gamma^{-1}$. By the same arguments as in the proof of Theorem C we find that Θ is a $\mathbb{Q}$-defined rational homomorphism from G into $\mathbf{Z}(G)$ which is trivial on $U(G)$. This implies that $\Theta \equiv 1$.

(ii) follows by a straightforward computation. □

3. Embedding Results

This section contains various embedding results. The first is a restricted but also more specific version of Theorem D.

Proposition 3.1: *Let G be a reduced connected solvable $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup. Let $\Delta \geq \Gamma$ be a finite extension group of Γ such that Γ is normal in Δ. Then there is a $\mathbb{Q}$-defined linear algebraic group H which contains a $\mathbb{Q}$-defined algebraic subgroup of finite index rationally isomorphic over $\mathbb{Q}$ to G and an arithmetic subgroup $\Delta_0 \leq H(\mathbb{Q})$ which is isomorphic to Δ. If Δ/Γ is solvable then H also has this property.*

In the proof of Proposition 3.1 two technical ingredients are required. The first is the following simple fact about bimodule cohomology. For the definitions see the end of Section 2.

Lemma 3.2: *Let A be a finite group and V a finite dimensional $\mathbb{Q}$-vector space with an A-bimodule structure. Then $H^1_{\mathrm{bi}}(A, V) = 0$.*

Proof: Define an action from the left of A on V by $a * v := a \cdot v \cdot a^{-1}$ ($a \in A$, $v \in V$). Given a bimodule derivation $f : A \to V$ define $\tilde{f} : A \to V$ by $\tilde{f}(a) := f(a) \cdot a^{-1}$ ($a \in A$). Then $\tilde{f}$ is a derivation in the ordinary sense of A into the left A-module defined above. It is easy to see that f is inner (in the bimodule sense) if and only if $\tilde{f}$ is inner (in the ordinary sense). Our result then follows from the analogous result in the standard cohomology theory of finite groups, see [W]. □

The second ingredient in the proof of Proposition 3.1 is an induction procedure which we describe now. This will also be of importance in the arguments to come.

Let $G \leq GL(n, \mathbb{C})$ be a linear algebraic group and $\Gamma \leq G$ a subgroup. Let $\Gamma \leq \Delta$ be a finite extension group so that Γ is normal in Δ. Write $H = \overline{\Gamma}$ for the Zariski-closure of Γ. Let $\Delta = \Gamma r_1 \cup \ldots \cup \Gamma r_m$ be the decomposition of Δ into left cosets. Assume that there are rational isomorphisms $f_1, \ldots, f_m : G \to G$ so that

$$(3.1) \qquad f_i(\gamma) = r_i \gamma r_i^{-1} \qquad (i = 1, \ldots, m)$$

for all $\gamma \in \Gamma$. We then have $f_i(H) = H$ for $i = 1, \ldots, m$. Let $\psi : \Delta \to \mathbf{GL}(mn, \mathbb{C})$ be the homomorphism inducing the injection of Γ into $\mathbf{GL}(n, \mathbb{C})$ with respect to the chosen coset decomposition. The map ψ has the property

$$(3.2) \qquad \psi(\gamma) = \begin{pmatrix} r_1 \gamma r_1^{-1} & 0 & \ldots & 0 \\ 0 & r_2 \gamma r_2^{-1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & r_m \gamma r_m^{-1} \end{pmatrix} \qquad \text{for all } \gamma \in \Gamma.$$

If $r_i r_j = \gamma_{jk} r_k$ with $\gamma_{jk} \in \Gamma$ then the matrix $\psi(r_i)$ has γ_{jk} in the (j, k)-position. The entries of $\psi(r_i)$ not specified by this are equal to 0. By our assumptions we may now extend the injective homomorphism $\psi : \Gamma \to \mathbf{GL}(mn, \mathbb{C})$ to a injective rational homomorphism $\Psi : H \to \mathbf{GL}(nm, \mathbb{C})$ by the definition

$$(3.3) \qquad \Psi(h) = \begin{pmatrix} f_1(h) & 0 & \ldots & 0 \\ 0 & f_2(h) & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & f_m(h) \end{pmatrix} \qquad (h \in H).$$

We define now

$$(3.4) \qquad \mathbf{I}(G, \Gamma, \Delta) := \Psi(H) \cdot \psi(\Delta).$$

It is clear that $\psi(\Delta)$ normalizes $\Psi(H)$, hence $\mathbf{I}(G, \Gamma, \Delta)$ is a subgroup of $\mathbf{GL}(mn, \mathbb{C})$. It is furthermore easy to see that $\Psi(H)$ has index m in $\mathbf{I}(G, \Gamma, \Delta)$. Hence $\mathbf{I}(G, \Gamma, \Delta)$ is an algebraic subgroup of $\mathbf{GL}(mn, \mathbb{C})$. We have now:

Lemma 3.3: *Let $G \leq GL(n, \mathbb{C})$ be a linear algebraic group defined over $\mathbb{Q}$ and $\Gamma \leq G(\mathbb{Z})$ be a subgroup of finite index. Define H to be the Zariski-closure of Γ. Let $\Gamma \leq \Delta$ be a finite extension group so that Γ is normal in Δ. Let $\Delta = \Gamma r_1 \cup \ldots \cup \Gamma r_m$ be the decomposition of Δ into left cosets. Assume that there are rational isomorphisms $f_1, \ldots, f_m$ satisfying* (3.1) *which are $\mathbb{Q}$-defined when restricted to H. Then $\mathbf{I}(G, \Gamma, \Delta)$ is a $\mathbb{Q}$-defined linear algebraic group and $\Psi(H)$ is a $\mathbb{Q}$-defined algebraic subgroup of $\mathbf{I}(G, \Gamma, \Delta)$ which rationally isomorphic over $\mathbb{Q}$ to H. The subgroup $\psi(\Delta)$ of $\mathbf{I}(G, \Gamma, \Delta)$ is contained in $\mathbf{I}(G, \Gamma, \Delta)(\mathbb{Q})$ and is arithmetic. If G and Δ/Γ are solvable then so is $\mathbf{I}(G, \Gamma, \Delta)$.*

The proof uses only elementary considerations, see [G-P1] and [G-P2] for more comments.

Proof of Proposition 3.1: We have to start with some preliminary considerations. Define

$$(3.5) \qquad \mathcal{V} := \{\, w : \Gamma \to \mathbf{Z}(G)(\mathbb{Q}) \ \ | \ \ w \text{ is a homomorphism trivial on } \ U(G, \Gamma) \,\}.$$

We shall sometimes think of $\mathcal{V}$ as a $\mathbb{Q}$-vector space and write the composition additively. For $w \in \mathcal{V}$ define

$$(3.6) \qquad \Lambda_w : \Gamma \to G, \qquad \Lambda_w(\gamma) := w(\gamma) \cdot \gamma \quad (\gamma \in \Gamma).$$

It is easy to see that Λ_w is an injective group homomorphism. The image $\Gamma_w := \Lambda_w(\Gamma)$ is commensurable with Γ and hence is an arithmetic subgroup of $G(\mathbb{Q})$, see [G-P2] Lemma 3.8. Let $\Delta_w > \Gamma_w$ be an extension group of Γ_w so that there is an isomorphism $\Lambda_w : \Delta \to \Delta_w$ which restricts to the original Λ_w on Γ. The existence of Δ_w can be seen by constructing its multiplication table.

Define $\varphi_\delta : \Gamma \to \Gamma$ for $\delta \in \Delta$ by $\varphi_\delta(\gamma) := \delta\, \gamma\, \delta^{-1}$. Let $D_{\varphi_\delta} : G \to G$ be the corresponding $\mathbb{Q}$-defined rational isomorphism constructed in Theorem C. Note that Γ is separated in G since G is connected. We now define a Δ-bimodule structure on $\mathcal{V}$ by

$$(3.7) \qquad \delta \cdot w \cdot \mu := D_{\varphi_\delta} \circ w \circ \varphi_\mu \qquad (\delta,\, \mu \in \Delta,\ w \in \mathcal{V}).$$

From the definition (3.7) and Proposition 2.10 (i) it is obvious that $\gamma \cdot w = w$ and $w \cdot \gamma = w$ for all $\gamma \in \Gamma$ and $w \in \mathcal{V}$. Hence $\mathcal{V}$ is a bi-module for the finite group $A := \Delta/\Gamma$. The map $\delta \mapsto u_{\varphi_\delta}$ is a derivation of Δ into $\mathcal{V}$. Since this derivation is trivial on Γ by Proposition 2.10 (i) we may use Lemma 3.2 and obtain that it is inner. This means that there is a $w \in \mathcal{V}$ such that

$$(3.8) \qquad u_{\varphi_\delta}(\gamma) = w(\varphi_\delta(\gamma)) - D_{\varphi_\delta}(w(\gamma)) \qquad \text{for all } \delta \in \Delta,\, \gamma \in \Gamma.$$

Consider now $\mu \in \Delta_w$ and $\rho \in \Gamma_w$. Find $\delta \in \Delta$ and $\gamma \in \Gamma$ such that $\Lambda_w(\delta) = \mu$ and $\Lambda_w(\gamma) = \rho = w(\gamma) \cdot \gamma$. Do the following two obvious computations:

$$\begin{aligned} \mu\,\rho\,\mu^{-1} &= \Lambda_w(\delta\,\gamma\,\delta^{-1}) = w(\delta\,\gamma\,\delta^{-1}) \cdot \delta\,\gamma\,\delta^{-1} = w(\varphi_\delta(\gamma)) \cdot \varphi_\delta(\gamma), \\ D_{\varphi_\delta}(\rho) &= D_{\varphi_\delta}(w(\gamma) \cdot \gamma) = D_{\varphi_\delta}(w(\gamma)) \cdot D_{\varphi_\delta}(\gamma) = u_{\varphi_\delta}(\gamma) \cdot D_{\varphi_\delta}(w(\gamma)) \cdot \varphi_\delta(\gamma). \end{aligned} \tag{3.9}$$

From (3.8) and (3.9) we conclude that $\mu\,\rho\,\mu^{-1} = D_{\varphi_\delta}(\rho)$. The proposition is then proved by applying Lemma 3.3. □

The next result characterizes arithmetic subgroups of reduced solvable linear algebraic groups.

Theorem 3.4: *Let Γ be an arithmetic subgroup in a solvable $\mathbb{Q}$-defined linear algebraic group G. Then Γ is isomorphic to a Zariski-dense arithmetic subgroup contained in $H(\mathbb{Q})$ for a reduced solvable $\mathbb{Q}$-defined linear algebraic group H if and only if the Fitting subgroup of Γ is torsion-free.*

The following is an immediate corollary of Theorem 3.4.

Corollary 3.5: *Let Γ be an arithmetic subgroup of a solvable-by-finite $\mathbb{Q}$-defined linear algebraic group. Then there is a subgroup Γ_0 of finite index in Γ and a reduced solvable $\mathbb{Q}$-defined linear algebraic group H so that Γ_0 is isomorphic to an arithmetic Zariski-dense subgroup of $H(\mathbb{Q})$.*

Proof of Theorem 3.4: The only if part of our proposition follows from Lemma 2.6 because a unipotent linear algebraic group is torsion-free.

We proceed by proving the if statement. Let $\tilde{\Gamma} \leq G(\mathbb{Z}) \cap \Gamma$ be a subgroup of finite index which is normal in Γ. Let $\gamma \in \Gamma$ be given. We have $\gamma\tilde{\Gamma}\gamma^{-1} = \tilde{\Gamma}$. This implies that there is a $\mathbb{Q}$-defined rational isomorphism $f : G \to G$ with $f(h) = \gamma h \gamma^{-1}$ for all $h \in G$ (see [G-P2] Lemma 2.2). We now use Lemma 3.3 to replace G by one of its solvable finite extensions so that Γ is a subgroup of $G(\mathbb{Q})$.

Let G be decomposed as in (2.1) and let $T \leq S$ be a $\mathbb{Q}$-defined torus which is of finite index in S. Then $\Gamma \cap (U(G) \cdot T)$ is of finite index in Γ. Then there is a torsion-free subgroup $\Gamma_0 \leq \Gamma \cap (U(G) \cdot T)$ which is normal and of finite index in Γ. Let $G_0 := \overline{\Gamma}_0$ be the Zariski-closure of Γ_0 in G. Then G_0 is a solvable $\mathbb{Q}$-defined linear algebraic group and if $G_0 = U(G_0) \cdot S_0$ is its decomposition (2.1) then S_0 is a commutative $\mathbb{Q}$-defined d-group. We shall now prove that Γ_0 is isomorphic to a Zariski-dense arithmetic subgroup of a reduced solvable $\mathbb{Q}$-defined linear algebraic group.

Let S_1 be the kernel of α_{G_0} in S_0. Then S_1 can also be described as the centralizer of $U(G_0)$ in S_0. Choose a $\mathbb{Q}$-defined d-subgroup $S_2 \leq S_0$ such that $S = S_1 \cdot S_2$ and such that $S_1 \cap S_2$ is finite. The possibility to choose such a S_2 follows from the well known (contravariant) equivalence between the category of $\mathbb{Q}$-defined commutative d-groups and the category of continuous finitely generated $\mathbb{Z}$-modules for the absolute Galois group of $\mathbb{Q}$. See Section 5 for more details on this equivalence of categories. The $\mathbb{Q}$-defined finite group $S_1 \cap S_2$ is normal in G_0 and hence $\Gamma_0 \cap S_1 \cap S_2 = \{1\}$ since Γ_0 is torsion-free. Define

$$(3.10)\quad \hat{G}_0 := G_0/(S_1 \cap S_2),\ \hat{S}_0 := S/(S_1 \cap S_2),\ \hat{S}_1 := S_1/(S_1 \cap S_2),\ \hat{S}_2 := S_2/(S_1 \cap S_2).$$

Then $\hat{G}_0$ is a solvable $\mathbb{Q}$-defined linear algebraic group which decomposes as $\hat{G}_0 = U(\hat{G}_0) \cdot \hat{S}_0$. Let $\hat{\Gamma}_0$ be the image of Γ_0 in $\hat{G}_0$. Note that $\hat{\Gamma}_0$ a Zariski-dense arithmetic subgroup of $\hat{G}_0(\mathbb{Q})$ isomorphic to Γ_0.

Let $s \in S_0$ represent an element of $\hat{S}_0$ which centralizes $U(\hat{G}_0)$. Then $sus^{-1}u^{-1} \in S_1 \cap S_2$ for all $u \in U(G_0)$. This implies $sus^{-1}u^{-1} = 1$ for all $u \in U(G_0)$ and hence $s \in S_1$. We infer that $\hat{S}_1$ is the centralizer of $U(\hat{G}_0)$ in $\hat{S}$. We also have $\hat{S} = \hat{S}_1 \cdot \hat{S}_2$ and $\hat{S}_1 \cap S_2 = \{1\}$. This shows that $U(\hat{G}_0) \cdot \hat{S}_2$ is a reduced solvable $\mathbb{Q}$-defined linear algebraic group.

Consider now the residue map $\pi : \hat{G}_0 \to \hat{G}_0/(U(\hat{G}_0) \cdot \hat{S}_2) \cong \hat{S}_1$. The image $\pi(\hat{\Gamma}_0)$ of $\hat{\Gamma}_0$ is an arithmetic subgroup of $\hat{G}_0/(U(\hat{G}_0) \cdot \hat{S}_2)(\mathbb{Q})$ and hence a finitely generated abelian group. Let $\pi(\hat{\Gamma}_0)_{\mathrm{tor}}$ be its torsion subgroup and $C := \overline{\pi(\hat{\Gamma}_0)_{\mathrm{tor}}}$ its Zariski-closure in S_1. The group C is finite and $\mathbb{Q}$-defined and is contained in the center of $\hat{G}_0$. We define

$$(3.11)\qquad \tilde{G}_0 := \hat{G}_0/C, \quad \tilde{S} := \hat{S}/C, \quad \tilde{S}_1 := \hat{S}_1/C, \quad \tilde{S}_2 := \hat{S}_2 \cdot C/C \cong \hat{S}_2.$$

The solvable $\mathbb{Q}$-defined linear algebraic group $\tilde{G}_0$ decomposes as $\tilde{G}_0 = U(\tilde{G}_0) \cdot \tilde{S}$ and $\tilde{S} = \tilde{S}_1 \cdot \tilde{S}_2$ with $\tilde{S}_1 \cap \tilde{S}_2 = \{1\}$. The $\mathbb{Q}$-defined torus $\tilde{S}_1$ is contained in the center of $\tilde{G}_0$ and its complement $U(\tilde{G}_0) \cdot \tilde{S}_2$ is a reduced solvable $\mathbb{Q}$-defined linear algebraic group because it is isomorphic to $U(\hat{G}_0) \cdot \hat{S}_2$ by a $\mathbb{Q}$-defined rational isomorphism. Let $\tilde{\Gamma}_0$ be the image of $\hat{\Gamma}_0$ in $\tilde{G}_0$. This group is isomorphic to Γ_0 because $\hat{\Gamma}_0 \cap C = \{1\}$. Consider now the residue maps

$$(3.12)\qquad \pi_1 : \tilde{G}_0 \to \tilde{G}_0/\tilde{S}_1 \cong U(\tilde{G}_0) \cdot \tilde{S}_2, \qquad \pi_2 : \tilde{G}_0 \to \tilde{G}_0/(U(\tilde{G}_0) \cdot \tilde{S}_2) \cong \tilde{S}_1.$$

The groups $\pi_1(\tilde{\Gamma}_0)$, $\pi_2(\tilde{\Gamma}_0)$ are Zariski-dense arithmetic subgroups of the $\mathbb{Q}$-defined linear algebraic groups $\tilde{G}_0/\tilde{S}_1 \cong U(\tilde{G}_0) \cdot \tilde{S}_2$, $\tilde{G}_0/(U(\tilde{G}_0) \cdot \tilde{S}_2) \cong \tilde{S}_1$. Since $\tilde{\Gamma}_0$ is an arithmetic subgroup of the two latter groups it gets mapped injectively by the direct product of the residue maps $\pi_1 \times \pi_2$ to a subgroup of finite index in $\pi_1(\tilde{\Gamma}_0) \times \pi_2(\tilde{\Gamma}_0)$. It is easy to see that $\pi_2(\tilde{\Gamma}_0)$ is now finitely generated abelian and torsion-free. Choose an $r \in \mathbb{N} \cup \{0\}$ and an isomorphism $\pi_2(\tilde{\Gamma}_0) \cong \mathbb{Z}^r$. Put $U_1 := G_a^r$ and

$$(3.13)\qquad H_0 := (U(\tilde{G}_0) \cdot \tilde{S}_2) \times U_1.$$

From what was said above we infer that H_0 is a reduced solvable $\mathbb{Q}$-defined linear algebraic group. Embed now $\mathbb{Z}^r$ as a Zariski-dense arithmetic subgroup into $U_1(\mathbb{Q})$. This shows that $\pi_1(\tilde{\Gamma}_0) \times \pi_2(\tilde{\Gamma}_0)$ is isomorphic to a Zariski-dense arithmetic subgroup of $H_0(\mathbb{Q})$. Hence Γ_0 is isomorphic to an arithmetic subgroup Γ_1 contained in $H_0(\mathbb{Q})$. The Zariski-closure $\overline{\Gamma_1}$ of Γ_1 in H_0 is of of finite index in H_0. By Lemma 2.5 this implies that $\overline{\Gamma_1}$ is reduced. We replace H_0 by $\overline{\Gamma_1}$ and have thus shown that Γ_0 is isomorphic to the Zariski-dense arithmetic subgroup Γ_1 contained in the $\mathbb{Q}$-points of the reduced solvable linear algebraic group H_0.

Let Δ be an extension group of Γ_1 such that Δ is isomorphic to the Γ we startet with and such that Γ_1 is normal and of finite index in Δ. We use now Lemma 3.3 to construct a solvable $\mathbb{Q}$-defined linear algebraic group H such that Δ is isomorphic to a Zariski-dense subgroup of $H(\mathbb{Q})$. We may further assume that H_0 is a $\mathbb{Q}$-defined subgroup of finite index in H. Let S be a maximal $\mathbb{Q}$-defined d-subgroup of H. From Lemma 2.5 we infer that $\mathbf{Z}_U(S)$ is a finite $\mathbb{Q}$-defined normal subgroup of H. The intersection $\Delta \cap \mathbf{Z}_U(S)$ is then a finite normal subgroup of Δ. If it is non-trivial it contains a non-trivial abelian characteristic subgroup. This subgroup is contained in the Fitting subgroup of Δ. Our assumption implies that $\Delta \cap \mathbf{Z}_U(S) = \{1\}$. We replace H by its quotient $H/\mathbf{Z}_U(S)$ and have proved the result using Lemma 2.5. $\square$

Finally for this Section we give the proof of Theorem D.

Proof of Theorem D: Let Δ be a finite extension of the solvable arithmetic group Γ. It is easily shown that there is a subgroup $\Gamma_0 \leq \Gamma$ which is normal and of finite index in Δ and which has torsion-free Fitting subgroup. We now apply Theorem 3.4 (to Γ_0) and find a reduced $\mathbb{Q}$-defined linear algebraic group H and a Zariski-dense arithmetic subgroup $\Gamma_1 \leq H(\mathbb{Q})$ which is isomorphic to Γ_0. Let Δ_1 the finite extension group of Γ_1 corresponding to the finite extension Δ of Γ_0. Put $\Gamma_2 := \Gamma_1 \cap H^\circ$ and let Γ_3 be a subgroup of finite index in Γ_2 which is normal in Δ_1. Theorem D follows by using Proposition 3.1 for the extension Δ_1 of $\Gamma_3 \leq H^\circ(\mathbb{Q})$. $\square$

4. Automorphism Groups

This section describes the automorphism group of certain arithmetic polycyclic groups. The main results are contained in Theorems 4.7 and 4.9. We first prove a structure theorem for the group of rational automorphisms of a reduced solvable-by-finite linear algebraic group. The group of rational automorphisms $\mathfrak{Aut}(G)$ of a $\mathbb{Q}$-defined linear algebraic group G is in general a locally algebraic group of type ALA (see [B-S], chapter 5) that is an extension of a $\mathbb{Q}$-defined linear algebraic group by an arithmetic group. In case G is solvable-by-finite and reduced we can be much more specific. Before we can describe our result some preliminary considerations in which we identify $\mathfrak{Aut}(G)$

with a $\mathbb{Q}$-defined linear algebraic group are required. Our approach is similar to that of [B-S].

Let G be a reduced $\mathbb{Q}$-defined solvable-by-finite linear algebraic group which is decomposed as in (2.1). Given $\Phi \in \mathfrak{Aut}(G)$ we have $\Phi(U(G)) = U(G)$ and let $\rho_U(\Phi) : U(G) \to U(G)$ be the restriction of Φ to $U(G)$. We also obtain an isomorphism $\Phi_S : U(G)\backslash G \to U(G)\backslash G$ induced by Φ. Both $\rho_U(\Phi)$ and Φ_S are rational maps. We define

$$\begin{aligned} \mathfrak{Aut}^1(G) &:= \{\, \Phi \in \mathfrak{Aut}(G) \;\; | \;\; \Phi_S = \mathrm{id}_{U(G)\backslash G} \,\}, \\ \mathfrak{A}_S(G) &:= \{\, \Phi \in \mathfrak{Aut}(G) \;\; | \;\; \Phi(S) = S \,\}, \\ \mathfrak{A}_S^1(G) &:= \{\, \Phi \in \mathfrak{A}_S(G) \;\; | \;\; \Phi|_S = \mathrm{id}_S \,\}. \end{aligned} \tag{4.1}$$

Consider the restriction homomorphism $\rho_U : \mathfrak{Aut}(G) \to \mathfrak{Aut}(U(G))$. The automorphism group $\mathfrak{Aut}(U(G))$ is a $\mathbb{Q}$-defined linear algebraic group since it can be identified via the exponential map with the automorphism group of the Lie algebra $\mathfrak{U}(G)$. Let $\Phi \in \mathfrak{A}_S$ be in the kernel of ρ_U. Then Φ satisfies $\Phi(sus^{-1}) = sus^{-1} = \Phi(s)u\Phi(s)^{-1}$ for all $s \in S$ and $u \in U(G)$. Hence ρ_U is injective on $\mathfrak{A}_S(G)$ because G is reduced. We shall show now that $\rho_U(\mathfrak{A}_S(G))$ is a $\mathbb{Q}$-defined algebraic subgroup of $\mathfrak{Aut}(U(G))$. Let $\rho_S : \mathfrak{A}_S(G) \to \mathfrak{Aut}(S)$ be the restriction homomorphism and let $\sigma \in \mathfrak{Aut}(S)$ be given. Then $\rho_U(\rho_S^{-1}(\sigma))$ consists of those $\Psi \in \mathfrak{Aut}(U(G))$ which satisfy $\Psi(sus^{-1}) = \sigma(s)\Psi(u)\sigma(s)^{-1}$ for all $s \in S$ and $u \in U(G)$. This shows that $\rho_U(\rho_S^{-1}(\sigma))$ is a $\mathbb{Q}$-defined Zariski-closed subset of $\mathfrak{Aut}(U(G))$.

We shall now show that $\rho_S(\mathfrak{A}_S(G))$ is finite. Let $\hat{S} := \alpha_G(S)$ be the image of S in $\mathrm{Aut}(\mathfrak{U}(G))$ and $\beta : S \to \hat{S}$ the restriction of α_G to S. By Lemma 2.3 β is a $\mathbb{Q}$-defined rational isomorphism because G is reduced. An element $\sigma \in \mathfrak{Aut}(S)$ gives now rise to the automorphism $\hat{\sigma} := \beta^{-1} \circ \sigma \circ \beta \in \mathfrak{Aut}(\hat{S})$. To an element $\Psi \in \mathfrak{Aut}(U(G))$ corresponds via the exponential map to an automorphism $\hat{\Psi} \in \mathrm{Aut}(\mathfrak{U}(G))$. An element $\sigma \in \mathfrak{Aut}(S)$ is in the image $\rho_S(\mathfrak{A}_S)$ if there is a $\Psi \in \mathfrak{Aut}(U(G))$ such that $\Psi(sus^{-1}) = \sigma(s)\Psi(u)\sigma(s)^{-1}$ for all $s \in S$ and $u \in U(G)$. This implies that $\hat{\Psi}$ is in the normalizer of $\hat{S}$ in $\mathrm{Aut}(\mathfrak{U}(G))$ and that $\hat{\sigma}(x) = \hat{\Psi}x\hat{\Psi}^{-1}$ for all $x \in \hat{S}$. Since the normalizer of $\hat{S}$ in $\mathrm{Aut}(\mathfrak{U}(G))$ induces (by conjugation) only a finite group of automorphisms of $\hat{S}$ we have proved that $\rho_S(\mathfrak{A}_S(G))$ is finite. Since

$$\rho_U(\mathfrak{A}_S(G)) = \bigcup_{\sigma \in \mathfrak{Aut}(S)} \rho_U(\rho_S^{-1}(\sigma)) \tag{4.2}$$

we have shown that $\rho_U(\mathfrak{A}_S)$ is a $\mathbb{Q}$-defined algebraic subgroup of $\mathfrak{Aut}(U(G))$. We further infer from the above that $\mathfrak{A}_S^1(G)$ has finite index in $\mathfrak{A}_S(G)$ and that $\rho_U(\mathfrak{A}_S^1(G))$ is a $\mathbb{Q}$-defined subgroup of finite index in $\rho_U(\mathfrak{A}_S(G))$.

By results of Malcev [Mc] the split extension $U(G) \rtimes \mathfrak{Aut}(U(G))$ is a $\mathbb{Q}$-defined algebraic group. We conclude that $U(G) \rtimes \rho_U(\mathfrak{A}_S(G))$ also has this property. Consider now the homomorphism

$$(4.3) \qquad \Theta : U(G) \rtimes \rho_U(\mathfrak{A}_S(G)) \to \mathfrak{Aut}(G), \qquad \Theta : (u, \rho_U(\Phi)) \mapsto \mathrm{In}_u \circ \Phi$$

where In_u is the inner automorphism corresponding to $u \in U(G)$, that is $\mathrm{In}_u(g) = ugu^{-1}$ for all $g \in G$. The homomorphism Θ is surjective because (Proposition 2.1) all maximal d-subgroups of G are conjugate by elements of $U(G)$. The kernel $\ker(\Theta)$ of Θ is easily seen to be a $\mathbb{Q}$-defined algebraic subgroup of $U(G) \rtimes \rho_U(\mathfrak{A}_S(G))$. We have now identified $\mathfrak{Aut}(G)$ with the $\mathbb{C}$-points of a $\mathbb{Q}$-defined algebraic group. Note that Θ gives by restriction rise to a surjective homomorphism

$$(4.4) \qquad \Theta : U(G) \rtimes \rho_U(\mathfrak{A}^1_S(G)) \to \mathfrak{Aut}^1(G), \qquad \Theta : (u, \rho_U(\Phi)) \mapsto \mathrm{In}_u \circ \Phi$$

This shows that $\mathfrak{Aut}^1(G)$ is of finite index in $\mathfrak{Aut}(G)$.

By the same arguments as above we find that Θ also induces a group isomorphism

$$(4.5) \qquad \Theta : (U(G) \rtimes \rho_U(\mathfrak{A}_S(G))/\ker(\Theta))(\mathbb{Q}) \to \mathfrak{Aut}_{\mathbb{Q}}(G).$$

We have to introduce some notation concerning automorphisms of abstract groups. Let Γ be a group. We call an element $\varphi \in \mathrm{Aut}(\Gamma)$ *$\mathcal{F}$-central* if $\varphi(\gamma)\gamma^{-1} \in \mathbf{Z}(\Gamma)$ for all $\gamma \in \Gamma$ and if φ is the identity when restricted to the Fitting subgroup $\mathcal{F}(\Gamma)$. We define

$$(4.6) \qquad \mathrm{Aut}_0(\Gamma) := \{ \varphi \in \mathrm{Aut}(\Gamma) \quad | \quad \varphi \ \text{ is } \mathcal{F}\text{-central} \}.$$

As already mentioned $\mathrm{Aut}_0(\Gamma)$ is abelian and normal in $\mathrm{Aut}(\Gamma)$. We can now formulate the first main result of this section.

Proposition 4.1: *Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup which is separated in G. Then the following hold.*

(i) $\mathfrak{Aut}(G)$ *is a $\mathbb{Q}$-defined linear algebraic group.*

(ii) *Let $D : \mathrm{Aut}(\Gamma) \to \mathfrak{Aut}(G)$ be the homomorphism defined in Theorem C. Then the image of D is an arithmetic subgroup of $\mathfrak{Aut}(G)$ and the kernel of D is $\mathrm{Aut}_0(\Gamma)$.*

While (i) is already established by what was said in the begining of this section we need some further considerations concerning arithmetic subgroups of reduced solvable-by-finite algebraic groups before we can prove (ii).

Definition 4.2: *Let G be a solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $S \leq G$ a maximal $\mathbb{Q}$-defined d-subgroup. An arithmetic subgroup $\Gamma \leq G(\mathbb{Q})$ is called S-split if $\Gamma = U(G, \Gamma) \cdot (\Gamma \cap S)$. Two arithmetic subgroups $\Gamma_2 \leq \Gamma_1$ are called S-related if $\mathrm{pr}_S(\Gamma_2) = \mathrm{pr}_S(\Gamma_1)$ where $\mathrm{pr}_S : G \to G/U(G) \cong S$ is the projection homomorphism.*

Suppose we are in the situation of the definition and $\Gamma \leq G$ is a Zariski-dense and S-split arithmetic subgroup. Then $\Gamma \cap S$ is Zariski-dense in S beause $\Gamma \cap S = \mathrm{pr}_S(\Gamma)$. The proof of (ii) in Proposition 4.1 will first be carried through for S-split arithmetic groups. The following lemma will then allow us the reduction to this case.

Lemma 4.3: *Let G be a solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $S \leq G$ a maximal $\mathbb{Q}$-defined d-subgroup. Let further $\Gamma \leq G(\mathbb{Q})$ be an arithmetic subgroup. Then there is an S-split arithmetic subgroup $\tilde{\Gamma} < G(\mathbb{Q})$ which contains Γ such that Γ and $\tilde{\Gamma}$ are S-related.*

If $\Gamma_2 \leq \Gamma_1$ are two groups we define

$$\mathrm{Aut}(\Gamma_1)_{\Gamma_2} := \{\, \varphi \in \mathrm{Aut}(\Gamma_1) \quad | \quad \varphi(\Gamma_2) = \Gamma_2 \,\} \tag{4.7}$$

to be the stabilizer of Γ_2 in $\mathrm{Aut}(\Gamma_1)$ and $\rho_{\Gamma_1/\Gamma_2} : \mathrm{Aut}(\Gamma_1)_{\Gamma_2} \to \mathrm{Aut}(\Gamma_2)$ to be the homomorphism given by reduction. The following lemma is needed in the proof of Lemma 4.3 and also in a later argument.

Lemma 4.4: *Let U be a unipotent $\mathbb{Q}$-defined linear algebraic group and $\mathfrak{U}$ its Lie algebra. Let $\hat{\Psi} \in \mathrm{Aut}(\mathfrak{U})$ be the element which is associated to $\Psi \in \mathfrak{Aut}(U)$ via the exponential map and*

$$\hat{\Delta} := \{\, \hat{\Psi} \quad \Big| \quad \Psi \in \Delta \,\} \leq \mathrm{Aut}(\mathfrak{U}) \tag{4.8}$$

the subgroup corresponding to a subgroup $\Delta \leq \mathfrak{Aut}(U)$. Let $\Lambda \leq U(\mathbb{Q})$ be an arithmetic subgroup. We have:

(i) *Let $x_1, \ldots, x_n$ be finitely many elements of $U(G)(\mathbb{Q})$ then $\langle\, \Lambda, x_1, \ldots, x_n \,\rangle$ contains Λ as a subgroup of finite index.*

(ii) *Let $\Delta \leq \mathfrak{Aut}(U)$ be a subgroup so that $\hat{\Delta} \leq \mathrm{Aut}(\mathfrak{U})$ is an arithmetic subgroup contained in the group of $\mathbb{Q}$-points of a $\mathbb{Q}$-defined algebraic subgroup of $\mathrm{Aut}(\mathfrak{U})$. Then there is a subgroup $\tilde{\Lambda} \leq U(\mathbb{Q})$ which contains Λ as a subgroup of finite index and which is left invariant by Δ.*

(iii) *Let $\Lambda_2 \leq \Lambda_1 \leq U(\mathbb{Q})$ be two arithmetic subgroups. Then $\rho_{\Lambda_1/\Lambda_2}(\mathrm{Aut}(\Lambda_1)_{\Lambda_2})$ has finite index in $\mathrm{Aut}(\Lambda_2)$.*

(iv) *Let $H \leq \mathfrak{Aut}(U)$ be such that $\hat{H}$ is a $\mathbb{Q}$-defined algebraic subgroup of $\mathrm{Aut}(\mathfrak{U})$. Put*

$$\Delta_\Lambda := \{\, \Phi \in H \quad | \quad \Phi(\Lambda) = \Lambda \,\}. \tag{4.9}$$

Then $\hat{\Delta}_\Lambda$ is an arithmetic subgroup of $\hat{H}$.

Lemma 4.4 is a straightforward exercise using the theory of arithmetic subgroups of unipotent algebraic groups, see [Se], Chapter 6. we skip the details.

Proof of Lemma 4.3*:* Let

$$\mathrm{pr}_U : G \to U(G), \qquad \mathrm{pr}_S : G \to S \tag{4.10}$$

be the projection maps associated to the decomposition (2.1) of G. Then $\mathrm{pr}_S(\Gamma)$ is an arithmetic subgroup of S and $U(G,\Gamma)\cdot(\Gamma\cap S)$ has finite index in Γ. Let $\gamma_1,\dots,\gamma_n$ be coset representatives for $U(G,\Gamma)\cdot(\Gamma\cap S)$ in Γ and $x_1 := \mathrm{pr}_U(\gamma_1),\dots,x_n := \mathrm{pr}_U(\gamma_n)$. By a combination of Lemma 4.4 (i), (ii) we find a subgroup $\tilde{\Lambda} \le U(\mathbb{Q})$ which contains $U(G,\Gamma)$ as a subgroup of finite index and also the $x_1,\dots,x_n$ and which is normalized by $\mathrm{pr}_S(\Gamma)$. Then $\tilde{\Gamma} := \tilde{\Lambda}\cdot\mathrm{pr}_S(\Gamma)$ satisfies the requirements of the lemma. □

Lemma 4.5: *Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma_2 \le \Gamma_1 \le G(\mathbb{Q})$ two S-related arithmetic subgroups. Then ρ_{Γ_1/Γ_2} is injective and its image has finite index in* $\mathrm{Aut}(\Gamma_2)$*.*

Proof: We first prove that ρ_{Γ_1/Γ_2} is injective. Suppose that $\varphi \in \mathrm{Aut}(\Gamma_1)_{\Gamma_2}$ is the identitity when restricted to Γ_2. Let $\gamma \in U(G,\Gamma_1)$ and choose $n \in \mathbb{N}$ so that $\gamma^n \in U(G,\Gamma_2)$. Then $\varphi(\gamma^n) = \varphi(\gamma)^n = \gamma^n$. Since $U(G)$ is uniquely divisible we get $\varphi(\gamma) = \gamma$. This shows that the restriction of φ to $U(G,\Gamma_1)$ is the identity. Let now $\gamma = us \in \Gamma_1$ with $u \in U(G)(\mathbb{Q})$ and $s \in S$. Since Γ_2 and Γ_1 are S-related there is a $v \in U(G)(\mathbb{Q})$ such that $vs \in \Gamma_2$. Note that $uv^{-1} \in U(G,\Gamma_1)$. We then have

$$\varphi(us) = \varphi(uv^{-1}\cdot vs) = \varphi(uv^{-1})\cdot\varphi(vs) = us. \tag{4.11}$$

This shows that ρ_{Γ_1/Γ_2} is injective.

Next we prove that $\rho_{\Gamma_1/\Gamma_2}(\mathrm{Aut}(\Gamma_1)_{\Gamma_2})$ has finite index in $\mathrm{Aut}(\Gamma_2)$. By Lemma 2.6 we have a reduction homomorphism $\rho_U : \mathrm{Aut}(\Gamma_1) \to \mathrm{Aut}(U(G,\Gamma_1))$ which maps $\mathrm{Aut}(\Gamma_1)_{\Gamma_2}$ into $\mathrm{Aut}(U(G,\Gamma_1))_{U(G,\Gamma_2)}$. Put

$$B := \{\, \varphi \in \mathrm{Aut}(\Gamma_2) \ \mid\ \rho_U(\varphi) \in \rho_{U(G,\Gamma_2)}(\mathrm{Aut}(U(G,\Gamma_1)_{U(G,\Gamma_2)}))\,\}. \tag{4.12}$$

By Lemma 4.4 (iii) $\rho_{U(G,\Gamma_1)/U(G,\Gamma_2)}(\mathrm{Aut}(U(G,\Gamma_1))_{U(G,\Gamma_2)})$ has finite index in the group $\mathrm{Aut}(U(G,\Gamma_2))$ and hence B has finite index in $\mathrm{Aut}(\Gamma_2)$. We prove that $B = \rho_{\Gamma_1/\Gamma_2}(\mathrm{Aut}(\Gamma_1)_{\Gamma_2})$. It is evident that $B \ge \rho_{\Gamma_1/\Gamma_2}(\mathrm{Aut}(\Gamma_1)_{\Gamma_2})$, so let $\varphi \in B$. Take $\psi \in \mathrm{Aut}(U(G,\Gamma_1))_{U(G,\Gamma_2)}$ such that $\rho_{U(G,\Gamma_1)/U(G,\Gamma_2)}(\psi) = \rho_U(\varphi)$. As above let $\gamma = us \in \Gamma_1$ with $u \in U(G)(\mathbb{Q})$ and $s \in S(\mathbb{Q})$. Since Γ_2 and Γ_1 are S-related there is a $v \in U(G)(\mathbb{Q})$ such that $vs \in \Gamma_2$. Define a map $\varphi_1 : \Gamma_1 \to \Gamma_1$ by putting

$$\varphi_1(\gamma) = \varphi_1(us) = \varphi_1(uv^{-1}\cdot vs) := \psi(uv^{-1})\cdot\varphi(vs). \tag{4.13}$$

We shall show that φ_1 is in $\mathrm{Aut}(\Gamma_1)_{\Gamma_2}$ and satisfies $\rho_{\Gamma_1/\Gamma_2}(\varphi_1) = \varphi$.

Notice first of all that the value of φ_1 does not depend on the choice of v. This follows by a straightforward computation. Next we show that φ_1 is a homomorphism. Let

γ_1, γ_2 be two elements of Γ_1 and $\gamma_1 = u_1 s_1$, $\gamma_2 = u_2 s_2$ where u_1, $u_2 \in U(G)(\mathbb{Q})$ and s_1, $s_2 \in S$. Choose v_1, $v_2 \in U(G)(\mathbb{Q})$ such that $v_1 s_1$, $v_2 s_2 \in \Gamma_2$. Then $\gamma_1\gamma_2 = u_1 s_1 u_2 s_1^{-1} \cdot s_1 s_2$ and $v_1 s_1 v_2 s_1^{-1} \cdot s_1 s_2 \in \Gamma_2$. By definition we find

$$\varphi_1(\gamma_1\gamma_2) = \psi(u_1 s_1 u_2 s_1^{-1} \cdot (v_1 s_1 v_2 s_1^{-1})^{-1}) \cdot \varphi(v_1 s_1 v_2 s_1^{-1} \cdot s_1 s_2). \tag{4.14}$$

On the other hand we have $\varphi_1(\gamma_1)\varphi_1(\gamma_2) = \psi(u_1 v_1^{-1})\varphi(v_1 s_1) \cdot \psi(u_2 v_2^{-1})\varphi(v_2 s_2)$. A small computation shows that $\varphi_1(\gamma_1)\varphi_1(\gamma_2) = \varphi_1(\gamma_1\gamma_2)$ is implied by

$$\varphi(v_1 s_1)\, \psi(u_2 v_2^{-1})\, \varphi(v_1 s_1)^{-1} = \psi(v_1 s_1\, u_2 v_2^{-1}\, (v_1 s_1)^{-1}). \tag{4.15}$$

Let x be the left-hand side and y be the right-hand side of (4.15). Choose a $\ell \in \mathbb{N}$ such that $(u_2 v_2^{-1})^\ell \in U(G, \Gamma_2)$. We infer from (4.15) that $x^\ell = y^\ell$. Since $U(G)(\mathbb{Q})$ is uniquely divisible we have $x = y$ and φ_1 is a homomorphism. Next we show that φ_1 is injective. Let $\gamma = us \in \Gamma_1$ and $vs \in \Gamma_2$ (u, $v \in U(G)(\mathbb{Q})$, $s \in S$) with $\varphi_1(\gamma) = 1$. We then have $1 = \varphi_1(\gamma) = \psi(uv^{-1})\varphi(vs)$. It follows that $\varphi(vs) \in U(G, \Gamma_2)$ which implies $vs \in U(G, \Gamma_2)$ and also $s = 1$. We infer that $\gamma \in U(G, \Gamma_1)$ and $\varphi_1(\gamma) = \psi(\gamma)$. This implies $\gamma = 1$ and hence the injectivity of φ_1. follows. Next we show that φ_1 is surjective. Let $\gamma = us \in \Gamma_1$ and $vs \in \Gamma_2$ (u, $v \in U(G)(\mathbb{Q})$, $s \in S$). Define then $\gamma' := \psi^{-1}(uv^{-1})\varphi^{-1}(vs)$. We show that $\varphi_1(\gamma') = \gamma$. Let $v' \in U(G)(\mathbb{Q})$ and $s' \in S$ be chosen such that $\varphi^{-1}(vs) = v's'$. Define $u' := \psi^{-1}(uv^{-1})v' \in U(G)(\mathbb{Q})$, then $\gamma' = u's'$ and $\varphi_1(\gamma') = \psi(u'v'^{-1})\varphi(v's') = \gamma$ follows. From our definition of φ_1 it is evident that φ_1 is in $\mathrm{Aut}(\Gamma_1)_{\Gamma_2}$ and that $\rho_{\Gamma_1/\Gamma_2}(\varphi_1) = \varphi$ is satisfied. $\square$

Lemma 4.5 is rather surprising since it is hopelessly false in the general situation of two arithmetic groups $\Gamma_2 \leq \Gamma_1$.

Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group which is decomposed as in (2.1) and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup. We define the following subgroup of $\mathfrak{A}^1_S(G)$:

$$\mathfrak{A}^1_S(G, \Gamma) := \{\, \Phi \in \mathfrak{A}^1_S(G) \;\;\big|\;\; \Phi(U(G, \Gamma)) = U(G, \Gamma) \,\}. \tag{4.16}$$

We infer from Lemma 2.6 that $\mathcal{F}(\Gamma) = U(G, \Gamma)$. Given a $\varphi \in \mathrm{Aut}(\Gamma)$ we then have $\varphi(U(G, \Gamma)) = U(G, \Gamma)$. Hence φ induces an isomorphism $\varphi_S : U(G, \Gamma)\backslash\Gamma \to U(G, \Gamma)\backslash\Gamma$. We define the following subgroups of $\mathrm{Aut}(\Gamma)$:

$$\begin{aligned} \mathrm{Aut}^1(\Gamma) :&= \{\, \varphi \in \mathrm{Aut}(\Gamma) \;\;|\;\; \varphi_S = \mathrm{id}_{U(G,\Gamma)\backslash\Gamma} \,\}, \\ \mathrm{In}_U(\Gamma) :&= \{\, \mathrm{In}_u \in \mathrm{Aut}(\Gamma) \;\;|\;\; u \in U(G, \Gamma) \,\} \\ \mathrm{A}^1_S(G, \Gamma) :&= \{\, \Phi|_\Gamma \;\;|\;\; \Phi \in \mathfrak{A}^1_S(G, \Gamma) \,\} \leq \mathrm{Aut}^1(\Gamma) \end{aligned} \tag{4.17}$$

The following is a simple consequence of our definitions.

Lemma 4.6: *Let G be a $\mathbb{Q}$-defined reduced solvable-by-finite linear algebraic group and $\Gamma \leq G$ a Zariski-dense arithmetic subgroup which is separated in G, then the following hold:*

(i) *Let $D : \mathrm{Aut}(\Gamma) \to \mathfrak{Aut}(G)$ be the homomorphism of Theorem C. Then* $\mathrm{Aut}^1(\Gamma)$ *is the preimage of $\mathfrak{Aut}^1(G)$ under D.*

(ii) $\mathrm{Aut}^1(\Gamma)$ *is of finite index in* $\mathrm{Aut}(\Gamma)$.

(iii) $\mathfrak{A}^1_S(G,\Gamma)$ *is an arithmetic subgroup of* $\mathfrak{A}^1_S(G)$.

(iv) $\mathfrak{A}^1_S(G,\Gamma)$ *is by restriction isomorphic to* $\mathrm{A}^1_S(G,\Gamma)$.

Proof: (i): A $\varphi \in \mathrm{Aut}(\Gamma)$ is in $\mathrm{Aut}^1(\Gamma)$ if and only if $\varphi(\gamma)\cdot\gamma^{-1} \in U(G,\Gamma)$ for all $\gamma \in \Gamma$. Correspondingly a $\Phi \in \mathfrak{Aut}(G)$ is in $\mathfrak{Aut}^1(G)$ if and only if $\Phi(g)\cdot g^{-1} \in U(G)$ for all $g \in G$. The statement then follows from the properties of D formulated in Theorem C.

(ii): follows from (i) and the fact that $\mathfrak{Aut}^1(G)$ has finite index in $\mathfrak{Aut}(G)$.

(iii): follows from Lemma 4.4 (iv).

(iv): holds since Γ is Zariski-dense in G. □

If G is a solvable-by-finite linear algebraic group decomposed as in (2.1) it follows from Proposition 2.1 that

$$\mathfrak{Aut}(G) = \mathrm{In}_U(G)\cdot\mathfrak{A}_S(G). \tag{4.18}$$

The following theorem contains a corresponding result but for arithmetic groups.

Theorem 4.7: *Let G be a $\mathbb{Q}$-defined solvable-by-finite and reduced linear algebraic group and $\Gamma \leq G$ an arithmetic subgroup which is separated in G, then the subgroup* $A(\Gamma) := \mathrm{Aut}_0(\Gamma)\cdot\mathrm{In}_U(\Gamma)\cdot\mathrm{A}^1_S(G,\Gamma)$ *is of finite index in* $\mathrm{Aut}(\Gamma)$.

Before we can prove Theorem 4.7 we have to establish the following finiteness result.

Proposition 4.8: *Let $G = U \rtimes S$ be a $\mathbb{Q}$-defined linear algebraic group where U is unipotent and S is a finite extension of a torus. Let $\Gamma \leq G(\mathbb{Q})$ be an arithmetic subgroup which can be decomposed as $\Gamma = \Gamma_U \rtimes \Gamma_S$ where $\Gamma_U \leq U(\mathbb{Q})$ and $\Gamma_S \leq S(\mathbb{Q})$ are arithmetic subgroups and where Γ_S is Zariski-dense in S. Assume further that Γ is separated in G. Then the set*

$$\mathcal{C}(G,\Gamma) := \{\, \Delta \leq \Gamma \;\;\big|\;\; \Delta = u\Gamma_S u^{-1} \text{ for some } u \in U(\mathbb{Q}) \,\} \tag{4.19}$$

falls into finitely many Γ_U-conjugacy classes.

Proof: We first consider the case when U is abelian. Let $U_1 \leq U$ be the centralizer of S in U. Since S acts by semi-simple transformations on U there is a $\mathbb{Q}$-defined,

S-invariant subspace $U_2 \leq U$ complementary to U_1 in U. We also fix a finite system $\gamma_1, \ldots, \gamma_n$ of Γ_S.

A derivation of Γ_S in U_2 is a map $c : \Gamma_S \to U_2$ satisfying $c(\gamma_1\gamma_2) = c(\gamma_1)\gamma_1 c(\gamma_2)\gamma_1^{-1}$. A derivation c is called inner if there is a $v \in U_2$ with $c(\gamma) = v\gamma v^{-1}\gamma^{-1}$ for all $\gamma \in \Gamma_S$. A derivation is determined by its values on the generators $\gamma_1, \ldots, \gamma_n$ of Γ_S. We call an n-tuple $(u_1, \ldots, u_n) \in U_2^n$ admissible if the is a derivation $c : \Gamma_S \to U_2$ with $c(\gamma_1) = u_1, \ldots, c(\gamma_n) = u_n$. Taking a $\mathbb{Q}$-basis of $U(\mathbb{Q})$ it is easy to see that $(u_1, \ldots, u_n) \in U_2^n$ is admissible if and only if certain polynomial equations with rational coefficients between the coordinates of the $(u_1, \ldots, u_n)$ are satisfied. Hence

$$\mathcal{B} := \{ (u_1, \ldots, u_n) \in U_2^n \quad | \quad (u_1, \ldots, u_n) \text{ is admissible} \} \tag{4.20}$$

is a $\mathbb{Q}$-defined Zariski-closed subset of U_2^n. Consider the map

$$I : U_2 \to \mathcal{B}, \qquad I(v) := (v\gamma_1 v^{-1}\gamma_1^{-1}, \ldots, v\gamma_1 v^{-1}\gamma_1^{-1}) \qquad (v \in U_2). \tag{4.21}$$

It is easy to see that I is a $\mathbb{Q}$-defined, injective rational map (note that Γ_S is Zariski-dense in S).

Given an element $v \in U(\mathbb{Q})$ we write v_2 for its component in U_2. We shall be able to use the map I because of the following evident implications.

$$v\Gamma_S v^{-1} \leq \Gamma \iff v_2\Gamma_S v_2^{-1} \leq \Gamma \iff I(v_2) \in \Gamma_U^n \tag{4.22}$$

There is furthermore a $\mathbb{Q}$-defined rational action of U_2 on $\mathcal{B}$ given by

$$v \cdot (u_1, \ldots, u_n) := (u_1 v\gamma_1 v^{-1}\gamma_1^{-1}, \ldots, u_n v\gamma_n v^{-1}\gamma_n^{-1}) \tag{4.23}$$

for $v \in U_2$ and $(u_1, \ldots, u_n) \in \mathcal{B}$.

Adapting the proof of Lemma 2.7 appropriately we have $H^1(\Gamma_S, U_2) = \{0\}$. This means that every derivation of Γ_S in U_2 is inner. This in turn implies that the map I is also bijective and that the action of U_2 on $\mathcal{B}$ is transitive. We also infer that $\mathcal{B}$ is connected and smooth. Hence I is a $\mathbb{Q}$-defined rational isomorphism.

Let now $\mathbb{A}$ be the ring of adeles of $\mathbb{Q}$ and $\mathbb{A}_f$ be the subring of finite adeles, that $\mathbb{A}_f$ is $\mathbb{A}$ with the component consistng of the real numbers left off. Let $\mathbb{A}_f^\infty$ be the ring of finite integral adeles which is a compact and open subring of $\mathbb{A}_f$. See [P-R], Chapter 5 for more details. It is for example easy to see that there is an open compact subgroup $V \leq U_2(\mathbb{A}_f^\infty)$ such that $V \cap U_2(\mathbb{Q}) = \Gamma_U$.

By [P-R] Proposition 5.2 we infer that $I : U_2 \to \mathcal{B}(\mathbb{A}_f)$ is a homeomorphism. Hence $I^{-1}(V^n \cap \mathcal{B}(\mathbb{A}_f))$ is compact and falls into finitely many orbits under translation by elements of V. Since we have $V \cap U_2(\mathbb{Q}) = \Gamma_U$ the set $I^{-1}(V^n \cap \mathcal{B}(\mathbb{Q})) = I^{-1}(\Gamma_U^n \cap \mathcal{B})$ falls into finitely many orbits under translation by elements of Γ_U. This proves the result in case U is abelian.

In the general case we use an induction on the dimension of U. First of all we define $\bar{U} := \mathbf{Z}(U)\backslash U$ and $\bar{G} := \mathbf{Z}(U)\backslash G \cong \bar{U} \rtimes S$, We write $\pi : G \to \bar{G}$ for the projection map. We shall call two subgrups Δ_1, Δ_2 congruent ($\Delta_1 \equiv \Delta_2$) if and only if $\pi(\Delta_1) = \pi(\Delta_2)$. Then $\pi(\Gamma) = \pi(\Gamma_U) \rtimes \pi(\Gamma_S)$ satisfies the hypotheses of the proposition. By induction this implies that there are finitely many $w_1, \ldots, w_k \in U(\mathbb{Q})$ so that $w_i \Gamma_S w_i^{-1} \leq \Gamma$ for $i = 1, \ldots, k$ and so that every subgroup $u\Gamma_S u^{-1} \leq \Gamma$ ($u \in U(\mathbb{Q})$) can be conjugated by an element of Γ_U to satisfy $u\Gamma_S u^{-1} \equiv w_i \Gamma_S w_i^{-1}$ for some $i \in \{1, \ldots, k\}$. Put

$$\mathcal{M}_i := \left\{ \Delta \leq \Gamma \;\middle|\; \begin{array}{l} \Delta = u\Gamma_S u^{-1} \text{ for some } u \in U(\mathbb{Q}), \\ \Delta \equiv w_i \Gamma_S w_i^{-1} \end{array} \right\} \tag{4.24}$$

for $i = 1, \ldots, k$. It suffices to show that each of the $\mathcal{M}_i$ intersects only finitely many Γ_U-conjugacy classes.

Before we do this we have to add some facts about centralizers. If $\Sigma \leq S$ is a subgroup put

$$\begin{aligned} \mathbf{Z}(U, \Sigma) : &= \{\, u \in U(\mathbb{Q}) \;\;|\;\; \sigma u \sigma^{-1} = u \text{ for all } \sigma \in \Sigma \,\}, \\ \bar{\mathbf{Z}}(U, \Sigma) : &= \{\, u \in U(\mathbb{Q}) \;\;|\;\; \pi(\sigma u \sigma^{-1}) = \pi(u) \text{ for all } \sigma \in \Sigma \,\}. \end{aligned} \tag{4.25}$$

Since Γ_S is Zariski-dense in S we have $\mathbf{Z}(U, \Gamma_S) = \mathbf{Z}(U, S)$ and $\bar{\mathbf{Z}}(U, \Gamma_S) = \bar{\mathbf{Z}}(U, S)$. We shall prove now that

$$\bar{\mathbf{Z}}(U, S) = \mathbf{Z}(U)(\mathbb{Q}) \cdot \mathbf{Z}(U, S). \tag{4.26}$$

This can be done by transfering the question to the Lie algebra $\mathfrak{U}$ of U. In fact, similar to (2.5) we use the exponential map to establish an action of S on $\mathfrak{U}$. Then there is an S-invariant complement to the center of $\mathfrak{U}$. Decomposing $\exp^{-1}(u)$ ($u \in \bar{\mathbf{Z}}(U, S)$) accordingly and applying exp again we find the decomposition of u in (4.26). The details are straightforward, we skip them.

Finally we show that each of the $\mathcal{M}_i$ in (4.24) intersects only finitely many Γ_U-conjugacy classes. We replace Γ_S by $w_i \Gamma_S w_i^{-1}$ and S by $w_i S w_i^{-1}$. Notice that $\Gamma = \Gamma_U \cdot w_i \Gamma_S w_i^{-1}$. If $u \in \mathcal{M}_i$ then $u w_i^{-1} \in \bar{\mathbf{Z}}(U, w_i S w_i^{-1})$ and according to (4.26) (applied to $w_i S w_i^{-1}$) there is a $z_u \in \mathbf{Z}(U)(\mathbb{Q})$ so that

$$z_u \cdot w_i \Gamma_S w_i^{-1} \cdot z_u^{-1} = u w_i^{-1} \cdot w_i \Gamma_S w_i^{-1} \cdot w_i u^{-1}. \tag{4.27}$$

To finish we apply the first part of the proof to the groups $\Gamma_U \cap \mathbf{Z}(U) \leq \mathbf{Z}(U)$, $w_i \Gamma_S w_i^{-1} \leq w_i S w_i^{-1}$ which are contained in $\mathbf{Z}(U) \rtimes w_i S w_i^{-1}$. $\square$

The proof just given is reminiscent of the proof of Theorem 5.10 from [P-R].

Proof of Theorem 4.7: Clearly $A(\Gamma) \leq \mathrm{Aut}^1(\Gamma)$ and by Lemma 4.6 (ii) we need only to prove that $A(\Gamma)$ is of finite index in $\mathrm{Aut}^1(\Gamma)$. We shall do this first for S-split groups Γ and afterwards consider the general case.

Let Γ be S-split. Let $\pi : G(\mathbb{Q}) \to \mathbf{Z}(G)(\mathbb{Q})\backslash G(\mathbb{Q})$ be the projection map and call two subgroups Δ_1, $\Delta_2 \leq G(\mathbb{Q})$ congruent ($\Delta_1 \sim \Delta_2$) if $\pi(\Delta_1) = \pi(\Delta_2)$. Consider the set

$$(4.28) \qquad \mathcal{C}_Z := \left\{ \Delta \leq \Gamma \;\middle|\; \begin{array}{l} \Delta \cap \mathbf{Z}(G)(\mathbb{Q}) = \{1\}, \\ \Delta \sim v(\Gamma \cap S)v^{-1} \text{ for some } v \in U(G)(\mathbb{Q}) \end{array} \right\} / \sim .$$

The subgroup $\Gamma \cap S$ represents a class in $\mathcal{C}_Z$ Using Theorem C it is straightforward to see that $\mathrm{Aut}^1(\Gamma)$ acts on $\mathcal{C}_Z$ where a $\varphi \in \mathrm{Aut}^1(\Gamma)$ sends a class of $\mathcal{C}_Z$ represented by $\Delta \leq \Gamma$ to the class represented by $\varphi(\Delta)$. The group $U(G,\Gamma)$ acts on $\mathcal{C}_Z$ by conjugation. The map

$$(4.29) \qquad \mathcal{C}_Z \to \mathcal{C}(\mathbf{Z}(G)\backslash G, \mathbf{Z}(\Gamma)\backslash\Gamma), \qquad \Delta \mapsto \pi(\Delta)$$

is well-defined, $U(G,\Gamma)$-equivariant and injective. Proposition 4.8 then implies that $U(G,\Gamma)\backslash\mathcal{C}_Z$ is finite. Let B be the stabilizer of the class of $\Gamma \cap S$ in this set. Then B has finite index in $\mathrm{Aut}^1(\Gamma)$.

Assume that $\varphi \in B$. Then there is a $w \in U(G,\Gamma)$ such that $\pi(\varphi(\Gamma \cap S)) = \pi(w(\Gamma \cap S)w^{-1})$. Put $\varphi_1 := \mathrm{In}_w^{-1} \circ \varphi$. Then $\pi(\varphi_1(\Gamma \cap S)) = \pi(\Gamma \cap S)$. Since $\varphi_1 \in \mathrm{Aut}^1(\Gamma)$ we find that for every $s \in \Gamma \cap S$ there is a $z(s) \in \mathbf{Z}(\Gamma)$ such that $\varphi(s) = z(s) \cdot s$. It is easy to see that

$$(4.30) \qquad \psi(\gamma) := u\, z(s)\, s \qquad (\gamma = u \cdot s \in \Gamma,\ u \in U(G,\Gamma),\ s \in \Gamma \cap S)$$

defines an element of $\mathrm{Aut}_0(\Gamma)$. Put $\varphi_2 := \psi^{-1} \cdot \varphi_1$.

We then have $\varphi_2(s) = s$ for all $s \in \Gamma \cap S$. By an argument similar to that of Lemma 2.9 we infer that D_{φ_2} satisfies $D_{\varphi_2}(s) = s$ for all $s \in S$. This implies that φ_2 is the restriction of D_{φ_2} to Γ and hence is in $\mathrm{A}_S^1(\Gamma)$. All of this shows that $B \leq A(\Gamma)$ and the result follows for S-split groups Γ.

Let now Γ be a general Zariski-dense arithmetic subgroup of G which is separated in G. Using Lemma 4.3 we choose an arithmetic group $\tilde{\Gamma} \geq \Gamma$ which is S-related to Γ. It is easy to see that $\tilde{\Gamma}$ is also Zariski-dense and separated in G. Using Lemma 4.5 it is straightforward to deduce that $\mathrm{A}(\Gamma)$ is of finite index in $\mathrm{Aut}(\Gamma)$ from the fact that the index of $\mathrm{A}(\tilde{\Gamma})$ in $\mathrm{Aut}(\tilde{\Gamma})$ is finite. □

Proof of Proposition 4.1: We have established (i) already in the remarks preceeding our proposition. Let us prove next that $\ker(D) = \mathrm{Aut}_0(\Gamma)$. From the statement of Theorem C we conclude that $\ker(D) \leq \mathrm{Aut}_0(\Gamma)$. Assume that φ is an element of $\mathrm{Aut}_0(\Gamma)$. Then there is a homomorphism $v : \Gamma \to \mathbf{Z}(\Gamma)$ which is trivial on $\mathcal{F}(\Gamma)$ such that $\varphi(\gamma) = v(\gamma) \cdot \gamma$ for all $\gamma \in \Gamma$. It is then evident that D_φ and id_G satisfy the hypotheses of Lemma 2.9. We conclude that $D_\varphi = \mathrm{id}_G$.

It remains to prove that $D(\mathrm{Aut}(\Gamma))$ is an arithmetic subgroup of $\mathfrak{Aut}(G)$. We first do this in case Γ is S-split. Similar to the reduction map $\rho_U : \mathfrak{Aut}(G) \to \mathfrak{Aut}(U(G))$

introduced above there is the reduction map $\rho_U : \mathrm{Aut}(\Gamma) \to \mathrm{Aut}(U(G,\Gamma))$. It is injective when restricted to $\mathrm{A}^1_S(G,\Gamma)$. Hence we may as in (4.3) define a map

$$\Theta : U(G,\Gamma) \rtimes \rho_U(\mathrm{A}^1_S(G,\Gamma)) \to \mathrm{Aut}(\Gamma), \qquad \Theta : (u, \rho_U(\varphi)) \mapsto \mathrm{In}_u \circ \varphi. \tag{4.31}$$

We furthermore have a natural homomorphism

$$\mu : \mathrm{Aut}(U(G,\Gamma)) \to \mathfrak{Aut}(U(G)). \tag{4.32}$$

The map μ is injective since $\mu(\varphi)$ is an extension of $\varphi \in \mathrm{Aut}(U(G,\Gamma))$ to a rational automorphism of $U(G)$. It is straightforward to check that we obtain a commutative diagram

$$\begin{array}{ccc} U(G,\Gamma) \rtimes \rho_U(\mathrm{A}^1_S(G,\Gamma)) & \xrightarrow{\Theta} & \mathrm{Aut}(\Gamma) \\ \big\downarrow{\scriptstyle \mathrm{id}\times\mu} & & \big\downarrow{\scriptstyle D} \\ U(G) \rtimes \rho_U(\mathfrak{A}^1_S(G,\Gamma)) & \xrightarrow{\Theta} & \mathfrak{Aut}(G) \end{array} . \tag{4.33}$$

By Lemma 4.6 the image of the left-upper corner gets mapped to an arithmetic subgroup of the left-lower corner. Since the lower Θ is a $\mathbb{Q}$-defined rational map the image of the left-upper corner is an arithmetic subgroup of $\mathfrak{Aut}(G)$. By Theorem 4.7 $D(\mathrm{Aut}(\Gamma))$ contains this arithmetic group as a subgroup of finite index and hence is arithmetic.

This finishes the proof of Proposition 4.1 in case of an S-split arithmetic group. To prove the general case let $\Gamma_1 \geq \Gamma$ be a group which contains Γ of finite index and which is S-split and S-related to Γ. The existence of Γ_1 is garantied by Lemma 4.3. We obtain a commutative diagram:

$$\begin{array}{ccc} \mathrm{Aut}(\Gamma_1)_\Gamma & \xrightarrow{D} & \mathfrak{Aut}(G) \\ \big\downarrow & & \big\downarrow{\scriptstyle \mathrm{Id}_G} \\ \mathrm{Aut}(\Gamma) & \xrightarrow{D} & \mathfrak{Aut}(G) \end{array} . \tag{4.34}$$

where the homomorphism down-left is given by restriction. Lemma 4.5 establishes then the general result. □

Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup which is separated in G. We shall construct now a $\mathbb{Q}$-defined linear algebraic group $\mathfrak{Aut}(\Gamma)$ which will contain $\mathrm{Aut}^1(\Gamma)$ as an arithmetic subgroup. Let $(\Gamma/\mathcal{F}(\Gamma))^{\mathrm{ab}}$ be the abilianised quotient of $\Gamma/\mathcal{F}(\Gamma)$ and $r := \dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} (\Gamma/\mathcal{F}(\Gamma))^{\mathrm{ab}}$. Let $\mathfrak{Aut}(G)$ act diagonally on $\mathbf{Z}(G)^r$ and define

$$\mathfrak{Aut}(\Gamma) := \mathbf{Z}(G)^r \rtimes \mathfrak{Aut}(G) \tag{4.35}$$

where $\mathfrak{Aut}(G)$ acts diagonally on $\mathbf{Z}(G)^r$. We fix elements $s_1, \ldots, s_r \in \Gamma$ such that their images in $\mathbb{Q} \otimes_{\mathbb{Z}} (\Gamma/\mathcal{F}(\Gamma))^{\mathrm{ab}}$ are a $\mathbb{Q}$-basis. We define

$$\Sigma : \mathrm{Aut}^1(\Gamma) \to \mathfrak{Aut}(\Gamma), \qquad \Sigma : \varphi \mapsto (u_\varphi(s_1), \ldots, u_\varphi(s_r); D_\varphi) \tag{4.36}$$

where u_φ and D_φ are as in Theorem C. For φ, $\psi \in \mathrm{Aut}(\Gamma)$ we find from Theorem C

$$u_{\varphi \circ \psi}(\gamma) = D_\varphi(u_\psi(\gamma)) \cdot u_\varphi(\psi(\gamma)). \tag{4.37}$$

If ψ is contained in $\mathrm{Aut}^1(\Gamma)$ then $\psi(\gamma) \cdot \gamma^{-1} \in U(G, \Gamma)$ for all $\gamma \in \Gamma$. This implies that Σ is a homomorphism.

Theorem 4.9: *Let G be a reduced solvable-by-finite $\mathbb{Q}$-defined linear algebraic group and $\Gamma \leq G(\mathbb{Q})$ a Zariski-dense arithmetic subgroup which is separated in G. Then the following hold.*

(i) *$\mathfrak{Aut}(\Gamma)$ is a $\mathbb{Q}$-defined linear algebraic group.*

(ii) *The map Σ defined in* (4.36) *is injective and $\Sigma(\mathrm{Aut}^1(\Gamma))$ is an arithmetic subgroup of $\mathfrak{Aut}(\Gamma)$.*

Proof: (i): is obvious.

(ii): The injectivity of Σ follows from Proposition 4.1 (ii). By Proposition 4.1 (ii) and Lemma 4.6 (ii) $D(\mathrm{Aut}^1(\Gamma))$ is a arithmetic subgroup of $\mathfrak{Aut}(G)$. Since $\Sigma(\mathrm{Aut}_0(\Gamma))$ evidently is an arithmetic subgroup of $\mathbf{Z}(G)^r$ the result follows. □

Proof of Theorem E: Theorem 4.9 together with Lemma 4.6 shows that $\mathrm{Aut}(\Gamma)$ contains an arithmetic subgroup of finite index. This does not apriori imply that $\mathrm{Aut}(\Gamma)$ is arithmetic (see [G-P1], [G-P2]). Let $\tau \in \mathrm{Aut}(\Gamma)$. We shall construct a $\mathbb{Q}$-defined rational homomorphism $M_\tau : \mathfrak{Aut}(\Gamma) \to \mathfrak{Aut}(\Gamma)$ such that $\Sigma(\tau\varphi\tau^{-1}) = M_\tau(\Sigma(\varphi))$ for all $\varphi \in \mathrm{Aut}^1(\Gamma)$. Lemma 3.3 then shows that $\mathrm{Aut}(\Gamma)$ is arithmetic. We deduce from (4.37) the formula

$$\begin{aligned} u_{\tau\varphi\tau^{-1}}(\gamma) &= D_\tau(D_\varphi(u_{\tau^{-1}}(\gamma))) \cdot D_\tau(u_\varphi(\tau^{-1}(\gamma))) \cdot u_\tau(\varphi\tau^{-1}(\gamma)) \\ &= D_\tau(D_\varphi(u_{\tau^{-1}}(\gamma))) \cdot D_\tau(u_\varphi(\tau^{-1}(\gamma))) \cdot u_\tau(\tau^{-1}(\gamma)) \end{aligned} \tag{4.38}$$

For all $\varphi \in \mathrm{Aut}^1(\Gamma)$. We define

$$\mathfrak{w}(\tau) := (u_{\tau^{-1}}(s_1), \ldots, u_{\tau^{-1}}(s_r)), \quad \hat{\mathfrak{w}}(\tau) := (u_\tau(\tau^{-1}(s_1)), \ldots, u_\tau(\tau^{-1}(s_r))). \tag{4.39}$$

These are two elements of $\mathbf{Z}(G)^r(\mathbb{Q})$. The automorphism τ^{-1} of Γ induces a $\mathbb{Q}$-linear automorphism of the $\mathbb{Q}$ vector space $\mathbb{Q} \otimes_{\mathbb{Z}} (\Gamma/\mathcal{F}(\Gamma))^{\mathrm{ab}}$ which we also denote by τ^{-1}. Hence there are rational numbers a_{ij} for $1 \leq i, j \leq r$ such that

$$\tau^{-1}(\hat{s}_i) = \sum_{j=1}^{r} a_{ji}\, \hat{s}_j \qquad (i = 1, \ldots, r) \tag{4.40}$$

where $\hat{s}_i$ stands for the image of s_i in $\mathbb{Q} \otimes_{\mathbb{Z}} (\Gamma/\mathcal{F}(\Gamma))^{\mathrm{ab}}$. Define now a $\mathbb{Q}$-linear automorphism $\ell_\tau : \mathbf{Z}(G)^r \to \mathbf{Z}(G)^r$ by

$$\ell_\tau(u_1, \dots, u_r) := \left(\sum_{j=1}^{r} a_{j1}\, u_j, \dots, \sum_{j=1}^{r} a_{jr}\, u_j \right). \tag{4.41}$$

Here we have identified $\mathbf{Z}(G)^r$ with a $\mathbb{C}$-vector space. The automorphism $\ell_\tau : \mathbf{Z}(G)^r \to \mathbf{Z}(G)^r$ satisfies

$$\ell_\tau((u_\varphi(s_1), \dots, u_\varphi(s_r))) = (u_\varphi(\tau^{-1}(s_1)), \dots, u_\varphi(\tau^{-1}(s_r))) \tag{4.42}$$

for all $\varphi \in \mathrm{Aut}^1(\Gamma)$. Define

$$M_\tau((\mathfrak{u}; g)) := (D_\tau \circ g(\mathfrak{w}(\tau)) \cdot D_\tau(\ell_\tau(\mathfrak{u})) \cdot \hat{\mathfrak{w}}(\tau); D_\tau g D_\tau^{-1}) \tag{4.43}$$

for $\mathfrak{u} \in \mathbf{Z}(G)^r$ and $g \in \mathfrak{Aut}(G)$. The map $M_\tau : \mathfrak{Aut}(\Gamma) \to \mathfrak{Aut}(\Gamma)$ satisfies $\Sigma(\tau\varphi\tau^{-1}) = M_\tau(\Sigma(\varphi))$ for all $\varphi \in \mathrm{Aut}^1(\Gamma)$ by (4.38). It is obviously rational and defined over $\mathbb{Q}$ in the coordinates we have already chosen in $\mathbf{Z}(G)^r$ and $\mathfrak{Aut}(G)$. Noticing $D_\tau(\mathfrak{w}(\tau)) \cdot \hat{\mathfrak{w}}(\tau) = 1$ it is straightforward to show that M_τ is also a group homomorphism. □

Proof of Theorem E': This result follows by first using Theorem 3.4 then Lemma 2.7 (iv) and finally Theorem E. □

5. Non-arithmetic Polycyclic Groups

In this section we prove Theorem E. We start off with an arithmetic construction of some polycyclic groups which will supply the non-arithmetic examples needed for the proof of Theorem G.

Let K be a number field and $\mathcal{O}_K$ its ring of integers. Assume that K has r_1 real and $2r_2$ complex embeddings. Hence K is of degree $n = r_1 + 2r_2$ over $\mathbb{Q}$. We write $\mathcal{O}_K^*$ for the group of units of $\mathcal{O}_K$. By Dirichlet's unit theorem we have an isomorphism $\mathcal{O}_K^* \cong C \times \mathbb{Z}^{r_K}$ where C is a finite cyclic group and $r_K = r_1 + r_2 - 1$. We write $\mathcal{O}_K^+$ for the additive group of $\mathcal{O}_K$. The group $\mathcal{O}_K^*$ acts by multiplication on $\mathcal{O}_K^+$. Let $\mathcal{O}_K^+ \rtimes \mathcal{O}_K^*$ be the corresponding split extension. Let now G_a, G_m be the additive and multiplicative group considered as linear algebraic groups over K. Then G_m acts by multiplication on G_a and we again write $G_a \rtimes G_m$ for the corresponding split extension. Let $G_K := \mathbf{R}_{K/\mathbb{Q}}(G_a \rtimes G_m) = \mathbf{R}_{K/\mathbb{Q}}(G_a) \rtimes \mathbf{R}_{K/\mathbb{Q}}(G_m)$ be the base field restriction of this group to $\mathbb{Q}$. Then G_K is a reduced solvable linear algebraic group defined over $\mathbb{Q}$ and have natural identifications

$$G_K(\mathbb{Q}) = K^+ \rtimes K^*, \qquad G_K(\mathbb{Z}) = \mathcal{O}_K^+ \rtimes \mathcal{O}_K^*. \tag{5.1}$$

Let $A \leq \mathcal{O}_K^*$ be a subgroup. Put

$$\Gamma_K(A) := \mathcal{O}_K^+ \rtimes A \ \leq \ \mathcal{O}_K^+ \rtimes \mathcal{O}_K^*. \tag{5.2}$$

The group $\Gamma_K(A)$ is polycyclic and its Fitting subgroup $\mathcal{F}(\Gamma_K(A))$ is equal to the additive group of $\mathcal{O}_K$ which is naturally embedded in $\Gamma_K(A)$. Hence we have $\mathcal{F}(\Gamma_K(A)) \cong \mathbb{Z}^n$. The following lemma characterizes the subgroups $A \leq \mathcal{O}_K^*$ for which $\Gamma_K(A)$ is an arithmetic group.

Proposition 5.1: *Let K be an algebraic number field of degree n over $\mathbb{Q}$ and Then the group $\Gamma_K(A)$ is arithmetic if and only if there is a $\mathbb{Q}$-defined algebraic subgroup $S \leq \mathbf{R}_{K/\mathbb{Q}}(G_m)$ such that A is contained as a Zariski-dense arithmetic subgroup in S.*

Proof: Let $S \leq \mathbf{R}_{K/\mathbb{Q}}(G_m)$ be a $\mathbb{Q}$-defined algebraic subgroup. If $A \leq S$ is commensurable with $S(\mathbb{Z})$ then $\Gamma_K(A)$ is obviously an arithmetic subgroup of the $\mathbb{Q}$-defined linear algebraic group $\mathbf{R}_{K/\mathbb{Q}}(G_a) \rtimes S$.

Suppose now that the group $\Gamma_K(A)$ constructed above is arithmetic. We then find by application of Theorem 3.4 a reduced solvable $\mathbb{Q}$-defined linear algebraic group H so that there is an isomorphism $\psi : \Gamma_K(A) \to \Gamma$ where Γ is a Zariski-dense arithmetic subgroup of $H(\mathbb{Q})$. We consider $\mathcal{O}_K^+$ and A to be identified with the corresponding subgroups of $\Gamma_K(A)$. By Lemma 2.6 the Fitting subgroup of Γ is $\Gamma \cap U(H)$. We infer that $\psi(\mathcal{O}_K^+) = \Gamma \cap U(H)$. Assume from now on that $A \neq \{1\}$. It is then easy to see that A is a maximal commutative subgroup of $\Gamma_K(A)$. Let S_0 be the Zariski-closure of $\psi(A)$ in H. This is a $\mathbb{Q}$-defined commutative algebraic subgroup of H. It follows that $\Gamma \cap S_1$ is an arithmetic subgroup of S_0. Since $\psi(A)$ is maximal commutative in Γ we have $\Gamma \cap S_0 = \psi(A)$. This implies that $\psi(A)$ is a Zariski-dense arithmetic subgroup of $S_0(\mathbb{Q})$.

From Lemma 2.6 and the remarks above we find that the Lie algebra $\mathfrak{U}(H)(\mathbb{Q})$ is abelian of dimension n over $\mathbb{Q}$ and $\exp^{-1}(\Gamma \cap U(H)) = \exp^{-1}(\psi(\mathcal{O}_K^+))$ is an abelian subgroup of $\mathfrak{U}(H)(\mathbb{Q})$ which contains a $\mathbb{Q}$-basis of this space. Choose a $\mathbb{Q}$-basis $\mathcal{B}$ inside $\mathcal{O}_K^+$ of the $\mathbb{Q}$-vector space K. This provides us with a rational $\mathbb{Q}$-defined injective representation $\Lambda : \mathbf{R}_{K/\mathbb{Q}}(G_m) \to \mathbf{GL}(n, \mathbb{C})$. For $k \in K^*$ its image $\Lambda(k)$ is the matrix corresponding to the multiplication by k. Note that Λ even gives a rational $\mathbb{Q}$-defined isomorphism between $\mathbf{R}_{K/\mathbb{Q}}(G_m)$ and the Zariski-closure of $\Lambda(K^*) \leq \mathbf{GL}(n, \mathbb{C})$. The homomorphism $\exp^{-1} \circ \psi : \mathcal{O}_K^+ \to \mathfrak{U}(H)(\mathbb{Q})$ can be extended to a $\mathbb{Q}$-linear isomorphism $\Theta : K \to \mathfrak{U}(H)(\mathbb{Q})$. Taking the basis $\Theta(\mathcal{B})$ for $\mathfrak{U}(H)(\mathbb{Q})$ we obtain the rational $\mathbb{Q}$-defined representation $\alpha_H : H \to \mathbf{GL}(n, \mathbb{C})$ (see (2.5)). The representations Λ, α_H evidently satisfy

$$\Theta^{-1} \circ \alpha_H(\psi(a)) \circ \Theta = \Lambda(a) \tag{5.3}$$

for all $a \in A$. Put $S := \Theta^{-1}\alpha_H(S_0)\Theta$. The subgroup $S < \mathbf{GL}(n, \mathbb{C})$ is defined over $\mathbb{Q}$. The image of $\psi(A)$ in S is Zariski-dense and by a result of Borel [B2] also arithmetic in S. Using (5.3) we see that $\Lambda(A)$ is a Zariski-dense arithmetic subgroup S. This proves the proposition. $\square$

Before we proceed we report on some facts from the theory of commutative d-groups. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and $\mathbb{G}$ its Galois group. For a $\mathbb{Q}$-defined commutative d-group S let $X(S)$ be the group of ($\overline{\mathbb{Q}}$-defined) characters of S. If $\varphi : S_1 \to S_2$ is a $\mathbb{Q}$-defined rational homomorphism between two commotative $\mathbb{Q}$-defined d-groups S_1, S_2 we write $X(\varphi) : X(S_2) \to X(S_1)$ for the corresponding homomorphism between the character modules. All of this gives a contravariant functorial equivalence between the category of $\mathbb{Q}$-defined d-groups and the category of continuos $\mathbb{G}$-modules which are finitely generated as $\mathbb{Z}$-modules. We write $S_1 \sim S_2$ if S_1, S_2 are isogenous. Then $S_1 \sim S_2$ if and only if $\mathbb{Q}\otimes_{\mathbb{Z}} X(S_1)$ and $\mathbb{Q}\otimes_{\mathbb{Z}} X(S_2)$ are isomorphic as $\mathbb{G}$-modules. For a commutative d-group S let $\dim(S)$ its dimension as an algebraic group. We have $\dim(S) = \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} X(S)$. Let $L \subseteq \mathbb{C}$ be a subfield then S is called L-split if every element of $X(S)$ is defined over L. It is easy to see that there is a minimal splitting field L_S for S. That is a subfield $L_S \subseteq \overline{\mathbb{Q}}$ such that S is L_S-split and such that $L_S \subseteq L$ for every other field $L \subseteq \mathbb{C}$ which has the property that S is L-split.

Let K be a number field. We have the following equality of $\mathbb{G}$-modules

$$X(\mathbf{R}_{K/\mathbb{Q}}(G_m)) = \mathbb{Z}[\mathbb{G}/\mathbb{U}(K)] \tag{5.4}$$

where $\mathbb{U}(K) \leq \mathbb{G}$ is the open subgroup of finite index in $\mathbb{G}$ with fixed-field K and $\mathbb{Z}[\mathbb{G}/\mathbb{U}(K)]$ is the corresponding permutation module. The d-group $\mathbf{R}_{K/\mathbb{Q}}(G_m)$ is split over the Galois-closure $\hat{K}$ of K in $\overline{\mathbb{Q}}$. The norm map $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ defines a $\mathbb{Q}$-defined character of $\mathbf{R}_{K/\mathbb{Q}}(G_m)$. We define $\mathbf{R}^1_{K/\mathbb{Q}}(G_m)$ to be its kernel. The character module of $\mathbf{R}^1_{K/\mathbb{Q}}(G_m)$ is isomorphic to $\mathbb{Z}[\mathbb{G}/\mathbb{U}(K)]/\mathbb{Z}$. We have $\mathbf{R}^1_{K/\mathbb{Q}}(G_m)(\mathbb{Z}) = \mathcal{O}^1_K$ where $\mathcal{O}^1_K$ stands for the group of units of norm 1 in $\mathcal{O}_K$.

In the following we show that Proposition 5.1 can really be used to construct non-arithmetic polycyclic groups.

Proposition 5.2: *Let K be a totally real number field with $[K : \mathbb{Q}] = n \geq 3$. Then the following hold:*

(i) *There are up to commensurability only finitely many infinite cyclic subgroups $A \leq \mathcal{O}^*_K$ such that $\Gamma_K(A)$ is arithmetic.*

(i) *If K is a Galois extension of $\mathbb{Q}$ and if $[K : \mathbb{Q}]$ is odd then the group $\Gamma_K(A)$ is non-arithmetic for every infinite cyclic subgroup $A \leq \mathcal{O}^*_K$.*

Proof: To prove the proposition it is sufficient to discuss infinite cyclic subgroups $A \leq \mathcal{O}^1_K$ which have the property that $\Gamma_K(A)$ is arithmetic. Put $T := \mathbf{R}^1_{K/\mathbb{Q}}(G_m)$ and let $S \leq T$ be a $\mathbb{Q}$-defined algebraic subgroup so that A is arithmetic and Zariski-dense in S. The d-group T is $\mathbb{R}$-split since K is totally real. In fact we have an $\mathbb{R}$-defined rational isomorphism $T(\mathbb{R}) \cong (\mathbb{R}^*)^{n-1}$. Moreover $T(\mathbb{Z})$ is discrete in $T(\mathbb{R})$ and (by Dirichlet's unit theorem) $T(\mathbb{R})/T(\mathbb{Z})$ is compact. This implies that S is $\mathbb{R}$-split and $\dim(S)$=1. Let L_S be the splitting field of S. Since $\mathbb{Q} \otimes_{\mathbb{Z}} X(S)$ is one dimensional we have $[L_S : \mathbb{Q}] \leq 2$. Since $S(\mathbb{Z})$ is infinite S cannot be $\mathbb{Q}$-split. Hence $[L_S : \mathbb{Q}] = 2$. Let $\hat{K}$ be the Galois-closure of K. Since S is K-split we find $L_S \leq K$. This proves (ii) of our proposition. To prove (i) define $S_1 := \mathbf{R}_{L_S/\mathbb{Q}}(G_m) \leq T$. Since every irreducible one dimensional representation of $\mathbb{G}$ occurs in $\mathbb{Q} \otimes_{\mathbb{Z}} X(T)$ at most once we have $S = S_1$ and A is commensurable with $S_1(\mathbb{Z})$. Finally we note that $\hat{K}$ has only finitely many quadratic subfields. □

Proposition 5.1 allows for the construction of many more non-arithmetic groups $\Gamma_K(A)$ than those appearing in Proposition 5.2. For general (not totally real) number fields K the situation is not so simple. This is shown by the following proposition.

Proposition 5.3: *Let K be a Galois extension of degree 6 over $\mathbb{Q}$ with Galois group isomorphic to the symmetric group $\mathbf{S}_3$. Let K_0 be its unique quadratic subfield. Assume that K_0 is imaginary quadratic. Then $\Gamma_K(A)$ is an arithmetic group for every subgroup $A \leq \mathcal{O}_K^*$.*

Proof: Since K is totally imaginary the group $\mathcal{O}_K^*$ has a subgroup of finite index which is isomorphic to $\mathbb{Z}^2$. From the well known decomposition of the group ring $\mathbb{Q}[\mathbf{S}_3]$ into irreducible ideals we find that $\mathbf{R}_{K/\mathbb{Q}}(G_m) \sim T_0 \times T_1 \times T_2$ where T_0 is isogenous to $\mathbf{R}_{K_0/\mathbb{Q}}(G_m)$ and where T_1 and T_2 are $\mathbb{Q}$-defined tori which are isomorphic over $\mathbb{Q}$ (see the remarks around 5.4). This implies that both $T_1(\mathbb{Z})$ and $T_2(\mathbb{Z})$ contain an infinite cyclic subgroup of finite index. Of course $T_0(\mathbb{Z})$ is finite. Since $T_1 \times T_2$ contains the one dimensional $\mathbb{Q}$-defined tori $\{\, (t_1^a, t_2^b) \;\mid\; t_1 \in T_1,\, t_2 \in T_2 \,\}$ for $a, b \in \mathbb{N}$ the result follows from Proposition 5.1. □

Proof of Theorem G: Let $h \in \mathbb{N}$ with $h \geq 4$ be given. By Dirichlet's theorem on primes in arithmetic progressions there is a prime number p such that $(p-1)/2$ is divisible by $h-1$. It is then easy to see that the $(h-1)$-th cyclotomic extension of $\mathbb{Q}$ contains a subfield which is totally real and of degree $h-1$ over $\mathbb{Q}$. We then apply Proposition 5.2. □

It is known (see [Me]) that there are totally real number fields K of degree $n \geq 3$ over $\mathbb{Q}$ such that the Galois group of the Galois-closure of K is isomorphic to the alternating group $\mathbf{A}_n$. Theorem G can also be deduced (along the same lines as above) from the following proposition.

Proposition 5.4: *Let K be a totally real number field of degree $n \geq 3$ over $\mathbb{Q}$. Assume that the Galois group of the Galois-closure of K is isomorphic to the alternating group*

$\mathbf{A}_n$. *Then* $\Gamma_K(A)$ *is a non-arithmetic group for every infinite cyclic subgroup* $A \leq \mathcal{O}_K^*$.

Proof: Assume that $A \leq \mathcal{O}_K^*$ is an infinite cyclic subgroup such that $\Gamma_K(A)$ is an arithmetic group. By Proposition 5.1 we find a $\mathbb{Q}$-defined torus $S \leq \mathbf{R}_{K/\mathbb{Q}}(G_m)$ such that A is commensurable with $S(\mathbb{Z})$. Similarly to the proof of Proposition 5.2 it can be argued that S is one dimensional and that the splitting field L_S of S is of degree 2 over $\mathbb{Q}$. Also L_S is contained in the Galois-closure of K. This is a contradiction. □

Proof of Theorem H: Let Γ be a polycyclic group of Hirsch-length ≤ 3. We have to prove that Γ is arithmetic. It is well known that Γ contains a torsion-free subgroup of finite index Γ_0 so that $\Gamma_0/\mathcal{F}(\Gamma_0)$ is also torsion-free. Using Theorem C we need only to show that Γ_0 is arithmetic. We make a case distinction on the structure of the Fitting subgroup.

Case 1: $h(\mathcal{F}(\Gamma_0)) = 3$. In this case Γ_0 is nilpotent. Every finitely generated nilpotent group is arithmetic by a result of Malcev [Mc].

Case 2: $h(\mathcal{F}(\Gamma_0)) = 2$. In this case $\mathcal{F}(\Gamma_0)$ is abelian, in fact $\mathcal{F}(\Gamma_0) \cong \mathbb{Z}^2$. By our choice of Γ_0 we have $\Gamma_0/\mathcal{F}(\Gamma_0) \cong \mathbb{Z}$. Pick a $\sigma \in \Gamma_0$ so that its image generates the quotient $\Gamma_0/\mathcal{F}(\Gamma_0)$. Put $T := \langle\sigma\rangle$. Then we have an isomorphism $\Gamma_0 = \mathcal{F}(\Gamma_0) \cdot T \cong \mathcal{F}(\Gamma_0) \rtimes T$. Conjugation by σ on $\mathcal{F}(\Gamma_0)$ gives us a matrix $A \in \mathbf{GL}(2, \mathbb{Z})$. Put $T_1 := \angle A\rangle$. Let the elements of T_1 act linearly on $\mathbb{Z}^2$ and let $\Gamma_1 := \mathbb{Z}^2 \rtimes T_1$ be the corresponding split extension. The groups Γ_0 and Γ_1 are isomorphic. Let K be the $\mathbb{Q}$-algebra generated by A in the 2×2 matrix ring. By Dirichlet's unit theorem K is a real-quadratic extension field of $\mathbb{Q}$. Let the multiplicative group G_m act on the additive group G_a by multiplication and let $G_a \rtimes G_m$ be the corresponding split extension. It is easy to see that Γ_1 is isomorphic to an arithmetic subgroup of the restriction of scalars $\mathbf{R}_{K/\mathbb{Q}}(G_a \rtimes G_m)$ of $G_a \rtimes G_m$.

The cases $h(\mathcal{F}(\Gamma_0)) = 0$, 1 are easily seen to be impossible. □

References

[B1] Borel, A.: *Arithmetic properties of linear algebraic groups.* Proc. I.C.M. Stockholm (1962), 10-22

[B2] Borel, A.: *Density and maximality of arithmetic subgroups.* J. Reine Angew. Math. **224**, (1966), 78–89

[B-S] Borel, A., Serre, J.-P.: *Théorème de finitude en cohomologie galoisienne.* Comment. Math. Helv. **39**, (1964), 111-164

[G-P1] Grunewald, F., Platonov, V.: *On finite extensions of arithmetic groups.* C. R. Acad. Sci. Paris **325**, 1153–1158, (1997) [G-P2] Grunewald, F., Platonov, V.: *Rigidity Results for Groups with Radical, Cohomology of Finite Groups and Arithmeticity Problems.* To appear

[G-P3] Grunewald, F., Platonov, V.: *Non-arithmetic polycyclic groups.* C. R. Acad. Sci. Paris, (1998) (to appear)

[G-P4] Grunewald, F., Platonov, V.: *Rigidity and Automorphism Groups of Solvable Arithmetic Groups.* C. R. Acad. Sci. Paris, (1998) (to appear)

[Mc] Malcev, A.I.: *On a class of homogeneous spaces.* Am. Math. Soc. Transl. **9**, (1962), 409–438

[Ma] Margulis, G.: *Discrete subgroups of semisimple Lie groups.* Springer Verlag (1991)

[Me] Mestre, J.-F.: *Extension régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{\mathbf{A}}_n$.* J. Algebra **131**, No. 2, 483–495, (1990)

[Mo] Mostow, G.: *Strong rigidity of locally symmetric spaces.* Ann. Math. Studies **78**, Princeton (1973)

[P1] Platonov, V.: *The Theory of algebraic linear groups and periodic groups.* Am. Math. Soc. Transl. **69**, (1968), 61-110

[P2] Platonov, V.: *Splittable linear groups.* Soviet Math. Dokl. **4**, (1963), 1002–1005

[P3] Platonov, V.: *On the congruence problem for solvable integral groups.* Dokl. Akad. Nauk BSSR **15**, (1971), 869–872

[P-M] Platonov, V., Milovanov, M.V.: *Determination of Algebraic Groups by Arithmetic Subgroups.* Soviet Math. Dokl. **14**, (1973), 331–335

[P-R] Platonov, V., Rapinchuk, A.: *Algebraic Groups and Number Theory.* Academic Press (1994)

[Pr] Prasad, G.: *Strong rigidity of $\mathbb{Q}$-rank 1 lattices.* Inv. math. **21**, (1973), 255–286

[Se] Segal, D. *Polycyclic groups.* Cambridge University Press (1983)

[S1] Serre, J.-P.: *Arithmetic groups.* London Math. Soc. Lecture Notes **36**, (1979), 105-135

[W] Weiss, E.: *Cohomology of Groups.* Academic Press (1969)