COMMUNICATIONS IN ALGEBRA, 30(6), 2715–2743 (2002)

ON AUTOMORPHISMS OF ARITHMETIC SUBGROUPS OF UNIPOTENT GROUPS IN POSITIVE CHARACTERISTIC

Lucy Lifschitz[1,*] and Dave Witte[2]

[1]Department of Mathematics, University of Virginia, Charlottesville, VA 22904
E-mail: lifschitz@tufts.edu
[2]Department of Mathematics, Oklahoma State University, Stillwater, OK 74078
E-mail: dwitte@math.okstate.edu

ABSTRACT

Let F be a local field of positive characteristic, and let G be either a Heisenberg group over F, or a certain (nonabelian) two-dimensional unipotent group over F. If Γ is an arithmetic subgroup of G, we provide an explicit description of every automorphism of Γ. From this description, it follows that every automorphism of Γ virtually extends to a virtual automorphism of G.

*Current address: Department of Mathematics, University of Oklahoma, Norman, OK 73019.

 www.dekker.com

1. INTRODUCTION

Roughly speaking, a discrete subgroup Γ of a topological group G is automorphism rigid if every automorphism of Γ extends to a continuous automorphism of G. However, the formal definition below is slightly more complicated, because it allows for passage to finite-index subgroups.

Definition 1.1. It is traditional to say that a group Γ *virtually* has a property if some finite-index subgroup of Γ has the property. It is convenient to extend this terminology to group isomorphisms.

- A *virtual isomorphism* from G_1 to G_2 is an isomorphism $\Lambda : G_1' \to G_2'$, where G_i' is a finite-index, open subgroup of G_i.
- A *virtual automorphism* of G is a virtual isomorphism from G to G.
- A virtual isomorphism Λ from G_1 to G_2 *virtually extends* an isomorphism λ from Γ_1 to Γ_2 if there is a finite-index, open subgroup Γ_1' of Γ_1, such that $\Gamma_1' \subset G_1$, and $\Lambda|_{\Gamma_1'} = \lambda|_{\Gamma_1'}$.

Definition 1.2. A discrete subgroup Γ of a topological group G is *automorphism rigid* in G if every virtual automorphism of Γ virtually extends to a virtual automorphism of G.

A classical example is provided by the work of Malcev.

Definition 1.3 ([6,Rem. 1.11, p. 21]). A discrete subgroup Γ of a topological group G is a (cocompact) *lattice* if G/Γ is compact.

Theorem 1.4 (Malcev[3],[6,Cor. 2.11.1, p. 34]). *If Γ is a lattice in a 1-connected, nilpotent real Lie group G, then Γ is automorphism rigid in G.*

In fact, every virtual automorphism of Γ extends to a unique automorphism of G.

Malcev's Theorem can be restated in the terminology of algebraic groups (cf. [6, after Thm. 2.12, p. 34]). Recall that a matrix group G *is unipotent* if, for every $g \bullet G$, there is some $n \in \mathbb{N}$, such that $(g - \mathrm{Id})^n = 0$. (In other words, 1 is the only eigenvalue of g.)

Corollary 1.5. *Let Γ be an arithmetic subgroup of a unipotent algebraic $\mathbb{Q}$-group $\mathbb{G}$. Then Γ is an automorphism rigid lattice in $\mathbb{G}(\mathbb{R})$.*

In this paper, we discuss the analogue of Malcev's Theorem for unipotent groups over nonarchimedean local fields, instead of $\mathbb{R}$. It is well known that if $\mathbb{G}$ is a unipotent algebraic group over a nonarchimedean local field L of characteristic zero, then the group $\mathbb{G}(L)$ of L-points of $\mathbb{G}$ has no nontrivial discrete subgroups. (For example, $\mathbb{Z}$ is not discrete in the p-adic field $\mathbb{Q}_p$.) Thus the case of characteristic zero is not of interest in this setting; we will consider only local fields of positive characteristic.

For abelian groups, it is easy to prove automorphism rigidity.

Proposition 1.6. *Let Γ_1 and Γ_2 be lattices in a totally disconnected, locally compact, abelian group G. Then every isomorphism $\lambda : \Gamma_1 \to \Gamma_2$ virtually extends to a virtual automorphism $\hat{\lambda}$ of G.*

Proof. Since Γ_1 and Γ_2 are discrete, and G is totally disconnected, there exists a compact, open subgroup K of G, such that $\Gamma_1 \cap K = \Gamma_2 \cap K = e$. Let $\hat{G}_1 = \Gamma_1 K$ and $\hat{G}_2 = \Gamma_2 K$, so $\hat{G}_1$ and $\hat{G}_2$ are finite-index, open subgroups of G, and define $\hat{\lambda} : \hat{G}_1 \to \hat{G}_2$ by $\hat{\lambda}(\gamma c) = \lambda(\gamma)\, c$ for $\gamma \in \Gamma_1$ and $c \in K$. ∎

For nonabelian groups, automorphism rigidity seems to be surprisingly more difficult to prove, but we provide examples of automorphism rigid lattices. Although we do not have a general theory, and we do not have enough evidence to support a specific conjecture, the examples suggest that there may be mild conditions that imply that arithmetic lattices are automorphism rigid.

Notation 1.7.

- Fix a prime p, and a power q of p.
- $\mathbb{F}_q$ denotes the finite field of q elements.
- F denotes the field $\mathbb{F}_q((t))$ of formal power series over $\mathbb{F}_q$.
- F^- denotes $\mathbb{F}_q[t^{-1}]$, the $\mathbb{F}_q$-subalgebra of F generated by t^{-1}.

Note that F is a local field of characteristic p. (Conversely, any local field of characteristic p is isomorphic to $\mathbb{F}_q((t))$, for some q [9, Thm. I.4.8, p. 20].) The subgroup F^- is a lattice in the additive group $(F, +)$.

Definition 1.8. *Let G be a closed subgroup of $\mathrm{GL}(m, F)$, for some $m \in \mathbb{N}$.*

- *Two discrete subgroups Γ_1 and Γ_2 of G are commensurable if $\Gamma_1 \cap \Gamma_2$ is a finite-index subgroup of both Γ_1 and Γ_2 [4, p. 8].*
- *A subgroup Γ of G is arithmetic if it is commensurable with $\mathrm{GL}(m, F^-) \cap G$ (cf. [4, §I.3.1, pp. 60–62]).*

By definition, if Γ_1 and Γ_2 are arithmetic subgroups of G, then Γ_1 is commensurable with Γ_2. Thus, Γ_1 is a lattice in G if and only if Γ_2 is a lattice in G.

Definition 1.9 (cf. [2, Ex. 9.2]). *Fix a power r of p, and let*

$$G_2 = \left\{ \begin{pmatrix} 1 & y^r & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \middle| y, z \in F \right\}.$$

So G_2 is a two-dimensional, unipotent F-group, and has arithmetic lattices. Note that if $r > 1$, then G_2 is nonabelian.

The following theorem describes the virtual automorphisms of any arithmetic lattice in G_2.

Definition 1.10. *For any continuous field automorphism τ of F and any $a \in F\backslash\{0\}$, there is a continuous automorphism $\phi_{\tau,a}$ of G_2, defined by*

$$\phi_{\tau,a} \begin{pmatrix} 1 & y^r & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a^r\tau(y)^r & a^{r+1}\tau(z) \\ 0 & 1 & a\tau(y) \\ 0 & 0 & 1 \end{pmatrix}.$$

Let us say that $\phi_{\tau,a}$ is *standard* if

(1) there exist $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, $\alpha \in \mathbb{F}_q \setminus \{0\}$, and $\beta \in \mathbb{F}_q$, such that

$$\tau\big(f(t^{-1})\big) = \sigma\big(f(\alpha t^{-1} + \beta)\big),$$

for all $f(t^{-1}) \in F^-$, and

(2) there exists some nonzero $b \in F^-$, such that $ab \in F^-$.

Note that if $\phi_{\tau,a}$ is standard, and Γ is an arithmetic lattice in G_2, then $\phi_{\tau,a}(\Gamma)$ is commensurable with Γ.

Theorem 1.11. *Let*

- *Γ be an arithmetic lattice in G_2; and*
- *λ be a virtual automorphism of Γ.*

If $r > 2$, *then there exist*

- *a standard automorphism $\phi_{\tau,a}$* of G_2,
- *a finite-index subgroup Γ' of Γ, and*
- *a homomorphism $\zeta : \Gamma' \to Z(\Gamma)$,*

such that $\lambda(\gamma) = \phi_{\tau,a}(\gamma)\,\zeta(\gamma)$, for all $\gamma \in \Gamma'$.

Corollary 1.12. *If $r \neq 2$, then any arithmetic lattice in G_2 is automorphism rigid.*

Theorem 1.11 and Corollary 1.12 are proved in Sec. 2. The authors do not know whether they remain true in the exceptional case $r = p = 2$.

Definition 1.13. *Let $[\![\cdot,\cdot]\!]: F^{2m} \times F^{2m} \to F$ be a symplectic form, and, for notational convenience, let $Z = F$. The corresponding Heisenberg group is the group $H = (F^{2m} \times Z, \circ)$, where*

$$(v_1, z_1) \circ (v_2, z_2) = \left(v_1 + v_2, z_1 + z_2 + [\![v_1, v_2]\!]\right).$$

We remark that, up to a change of basis, the symplectic form $[\![\cdot,\cdot]\!]$ on F^{2m} is unique, so, up to isomorphism, the Heisenberg group H is uniquely determined by m. Note that Z is the center of H.

Because H is isomorphic to a subgroup of $\mathrm{GL}(m+2, F)$, namely,

$$H \cong \left\{ \begin{pmatrix} 1 & x_1 & x_2 & \cdots & x_m & z \\ & 1 & & & & y_1 \\ & & 1 & 0 & & y_2 \\ & & & \ddots & & \vdots \\ & 0 & & & 1 & y_m \\ & & & & & 1 \end{pmatrix} \middle| \begin{array}{r} x_1, \ldots, x_m \in F, \\ y_1, \ldots, y_m \in F, \\ z \in F \end{array} \right\},$$

we may speak of arithmetic subgroups of H.

We assume that $[\![\cdot,\cdot]\!]$ is defined over F^-, by which we mean that $[\![F^-, F^-]\!] \subset F^-$. Then we may assume that the above isomorphism has been chosen so that a subgroup Γ of H is arithmetic if and only if it is commensurable with $(F^-)^{2m} \times F^-$. Thus, H has arithmetic lattices.

Definition 1.14. *We say $T \in \mathrm{GL}(2m, F)$ is a symplectic similitude if there exists some nonzero $c_T \in F$, such that, for all $v, w \in V$, we have*

$$[\![T(v), T(w)]\!] = c_T [\![v, w]\!].$$

For every symplectic similitude $T \in \mathrm{GL}(2m, F)$, and every continuous field automorphism τ of F, there is a continuous automorphism $\phi_{T,\tau}$ of H defined by

$$\phi_{T,\tau}(v, z) = (\tau(T(v)), \tau(c_T z)).$$

Let us say that $\phi_{T,\tau}$ is standard if

(1) there exist $\sigma \bullet \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, $\alpha \bullet \mathbb{F}_q \setminus \{0\}$, and $\beta \bullet \mathbb{F}_q$, such that

$$\tau(f(t^{-1})) = \sigma(f(\alpha t^{-1} + \beta))$$

for all $f(t^{-1}) \bullet F$; and

(2) there exists some nonzero $b \bullet F^{-}$, such that $bT \in \mathrm{Mat}(2m, F^{-})$.

Note that if $\phi_{T,\tau}$ is standard, then $\phi_{T,\tau}(\Gamma)$ is commensurable with Γ for any arithmetic lattice Γ of H.

Theorem 1.15. *Let*

- Γ *be an arithmetic lattice in a Heisenberg group H; and*
- λ *be a virtual automorphism of* Γ.

Then there exist

- *a standard automorphism $\phi_{T,\tau}$ of H;*
- *a finite index subgroup* Γ' of Γ; *and*
- *a homomorphism* $\zeta : \Gamma' \to Z(\Gamma)$,

such that $\lambda(\gamma) = \phi_{T,\tau}(\gamma)\zeta(\gamma)$, *for all* $\gamma \in \Gamma'$.

Corollary 1.16. *Any arithmetic lattice in a Heisenberg group H is automorphism rigid.*

Theorem 1.15 and Corollary 1.16 are proved in Sec. 3.

Remark 1.17. Malcev's Theorem 1.4 does not extend to all lattices in solvable Lie groups. (See the work of A. Starkov [7] for a thorough discussion.) On the other hand, the Mostow Rigidity Theorem [5] implies that lattices in most semisimple Lie groups are automorphism rigid.

Superrigidity deals with extending homomorphisms, instead of only isomorphisms. The Margulis Superrigidity Theorem [4, Thm. VII.5.9, p. 230] implies that lattices in most semisimple Lie groups are superrigid. (Lattices in many non-semisimple Lie groups are also superrigid.[10]) The Superrigidity Theorem also applies to arithmetic subgroups of many semisimple groups defined over nonarchimedean local fields, whether they are of characteristic zero or not [4,8].

2. ARITHMETIC SUBGROUPS OF THE TWO-DIMENSIONAL UNIPOTENT GROUP G_2

Recall that r and G_2 are defined in Definition 1.9. (Also recall the definitions of p, q, F, and F^- in Notation 1.7.)

Proof of Theorem 1.11. Let Γ_1 and Γ_2 be finite-index subgroups of Γ, such that λ is an isomorphism from Γ_1 to Γ_2. Then λ induces isomorphisms

$$\lambda^* : \Gamma_1/Z(\Gamma_1) \to \Gamma_2/Z(\Gamma_2) \text{ and } \lambda_* : [\Gamma_1, \Gamma_1] \to [\Gamma_2, \Gamma_2].$$

By identifying each of $G_2/Z(G_2)$ and $Z(G_2)$ with F in the natural way (and noting that $\Gamma_i \cap Z(G_2) = Z(\Gamma_i)$), we may think of $\Gamma_i/Z(\Gamma_i)$ and $[\Gamma_i, \Gamma_i]$ as $\mathbb{F}_p$-subspaces of F. By replacing Γ_1 and Γ_2 with finite-index subgroups, we may assume that these subspaces are contained in F^-. Then, because λ is an isomorphism, we see that the conditions of Notation 2.3 are satisfied, so Theorem 2.4 below implies that there exist

- a standard automorphism $\phi_{\tau,a}$ of G_2, and
- a finite-index subgroup Γ_1' of Γ_1,

such that $\lambda(\gamma) \bullet \phi_{\tau,a}(\gamma)Z(G)$, for all $\gamma \in \Gamma_1'$.

Because $\phi_{\tau,a}(\Gamma_1)$ is an arithmetic lattice, it is commensurable with Γ_2. Thus, replacing Γ_1' with a finite-index subgroup, we may assume that $\phi_{\tau,a}(\Gamma_1') \subset \Gamma_2$. Then we may define $\zeta : \Gamma_1' \to Z(\Gamma_2)$ by $\zeta(\gamma) = \lambda(\gamma)\,\phi_{\tau,a}(\gamma)^{-1}$. □

Lemma 2.1. *Let*

- Γ *be a lattice in a totally disconnected, locally compact group* G,
- A *be a locally compact, abelian group, and*
- $\zeta : \Gamma \to A$ *be a homomorphism.*

Assume

(1) there is a finite-index subgroup Γ' *of* Γ, *such that* $\Gamma' \cap [G, G] \subset [\Gamma, \Gamma]$, *and*
(2) $\Gamma \cap [G, G]$ *is a lattice in* $[G, G]$.

Then there is a finite-index, open subgroup $\hat{G}$ *of* G, *containing* $[G, G]$, *such that* $\zeta|_{\Gamma'}$ *extends to a continuous homomorphism* $\hat{\zeta} : \hat{G} \to A$ *that is trivial on* $[G, G]$.

Proof. Let $\bar{G} = G/[G, G]$, and let $\bar{\Gamma}$ and $\bar{\Gamma}'$ be the images of Γ and Γ', respectively, in $\bar{G}$. Since $\zeta : \Gamma \to A$, and A is abelian, we see that

$[\Gamma, \Gamma] \subset \ker \zeta$, so, by the choice of Γ', we have $\Gamma' \cap [G, G] \subset \ker \zeta$. Hence, ζ induces a well-defined homomorphism $\bar{\zeta} : \bar{\Gamma}' \to A$.

By assumption, $\Gamma \cap [G, G]$ is a lattice in $[G, G]$, so $\bar{\Gamma}$ is closed [6, Thm. 1.13, p. 23], hence discrete. Thus, there is a compact, open subgroup K of $\bar{G}$, such that $\bar{\Gamma}' \cap K = e$. Extend $\bar{\zeta}|_{\bar{\Gamma}'}$ to a homomorphism $\hat{\hat{\zeta}} : \bar{\Gamma}' K \to A$ by defining it to be trivial on K. Then $\hat{\hat{\zeta}}$ induces a homomorphism $\hat{\zeta} : \hat{G} \to A$, where $\hat{G}$ is the pullback of $\bar{\Gamma}' K$ under the canonical homomorphism $G \to \bar{G}$. □

Proof of Corollary 1.12. We may assume $r > 2$. (Otherwise, we must have $r = 1$, which means G_2 is abelian, so Proposition 1.6 applies.) From Theorem 1.11, we may assume there exist

- a standard automorphism $\phi_{\tau,a}$ of G_2, and
- a homomorphism $\zeta : \Gamma_1 \to Z(\Gamma_2)$,

such that $\lambda(\gamma) = \phi_{\tau,a}(\gamma)\zeta(\gamma)$, for all $\gamma \bullet \Gamma_1$. From Lemma 2.1, we may assume that there is a finite-index subgroup G_2' of G_2, such that G_2' contains $[G_2, G_2]$, and ζ extends to a homomorphism $\hat{\zeta} : G_2' \to Z(G_2)$ that is trivial on $[G_2, G_2]$. Let $G_2'' = \phi_{\tau,a}(G_2')$.

Define $\hat{\lambda} : G_2' \to G_2$ by $\hat{\lambda}(g) = \phi_{\tau,a}(g)\hat{\zeta}(g)$, for $g \in G_2'$, so $\hat{\lambda}$ is a continuous homomorphism that extends λ. Because $\hat{\zeta}$ is trivial on $[G_2, G_2]$, we know that $\hat{\lambda}_{[G_2,G_2]} = \phi_{\tau,a}|_{[G_2,G_2]}$. Also, because $\hat{\zeta}(G_2') \subset Z(G_2) = [G_2, G_2]$, we know that $\hat{\lambda}(g) \bullet \phi_{\tau,a}(g)[G_2, G_2]$ for all $g \bullet G_2'$. Thus, $\hat{\lambda}$ induces an automorphism of $[G_2, G_2]$, and an isomorphism $G_2'/[G_2, G_2] \to G_2''/[G_2, G_2]$, so $\hat{\lambda}$ is an isomorphism. □

2.1. Using Linear Algebra to Prove Theorem 1.11

The remainder of this section is devoted to the statement and proof of Theorem 2.4. This result is a reformulation of Theorem 1.11 in terms of linear algebra. The reformulation is not of intrinsic interest, but it clarifies the essential ideas of the proof, and provides more flexibility, by allowing us to focus on the important aspects of the internal structure of Γ that arises from the structure of F^- as a polynomial algebra, without being constrained by the external structure imposed by the group-theoretic embedding of Γ in G_2.

Notation 2.2. Define an $\mathbb{F}_p$-bilinear form $[\![\cdot, \cdot]\!] : F^- \times F^- \to F^-$ by

$$[\![a, b]\!] = a^r b - a b^r.$$

For any $V, W \subset F^-$, $[\![V, W]\!]$ denotes the $\mathbb{F}_p$-subspace of F^- spanned by $\{[\![v, w]\!] \mid v \in V, w \in W\}$.

Notation 2.3. Throughout the remainder of this section, we assume that

- $r > 2$;
- V_1 and V_2 are $\mathbb{F}_p$-subspaces of finite codimension in F^-; and
- $\lambda^* : V_1 \to V_2$ and $\lambda_* : [\![V_1, V_1]\!] \to [\![V_2, V_2]\!]$ are $\mathbb{F}_p$-linear bijections,

such that

$$\lambda_*[\![a, b]\!] = [\![\lambda^*(a), \lambda^*(b)]\!],$$

for all $a, b \in V_1$.

Theorem 2.4. *There exist*

- *a subspace V_1' of finite codimension in V_1,*
- *$a \in b^{-1}F^-$, for some $b \in F^-$,*
- *$\alpha, \beta \in \mathbb{F}_q$, with $\alpha \neq 0$, and*
- *$\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$,*

such that

$$\lambda^*\big(f(t^{-1})\big) = a\sigma\big(f(\alpha t^{-1} + \beta)\big),$$

for all $f(t^{-1}) \in V_1'$.

Let us outline the proof of Theorem 2.4, assuming, for simplicity, that $V_1 = V_2 = F^-$. For any power $Q > 1$ of r, we may define an equivalence relation on $F^- \setminus \{0\}$ by $a \equiv_Q b$ iff $a/b \in F^Q$; let $[a]$ denote the equivalence class of a. For each $a \in F^-$, the subspace $[\![a, F^-]\!]$ has infinite codimension in $[\![F^-, F^-]\!]$, but Proposition 2.6 shows that $[\![[a], F^-]\!]$ has finite codimension. Because Corollary 2.10 shows that $\lambda^*([a]) = [\lambda^*(a)]$, this codimension is a useful invariant. Proposition 2.12 shows that it is closely related to the minimum degree of the elements of $[a]$. Using this, Corollary 2.22 shows that there is some $a \in F^-$, a constant k, and some Q, such that $\deg^- \lambda^*(b) = k + \deg^- b$ for all $b \equiv_Q a$. Also, Corollary 2.24 shows that λ^* approximately preserves the degrees of greatest common divisors. Then Proposition 2.25 shows that the restriction of λ^* to the $\mathbb{F}_p$-rational elements of some equivalence class is of the desired form. Finally, we show that λ^* has the desired form on all of F^-.

Notation 2.5.

- We use $\dim W$ to denote the dimension of a vector space W over $\mathbb{F}_p$.

- Let $s = \dim \mathbb{F}_q$, so $q = p^s$.
- For $a = \sum_{i=0}^{n} \alpha_i t^{-i} \in F^-$, with each $\alpha_i \in \mathbb{F}_q$, we let $\deg^- a = n$ if $\alpha_n \neq 0$.

The following proposition is used in almost all of the following results. Because the implication ($\Rightarrow$) of (1) requires the assumption that $r > 2$, it seems that a different approach will be needed for the exceptional case $p = r = 2$.

Proposition 2.6. *(1) Let $a, b \bullet V_i \setminus \{0\}$ and assume $a/b \notin \mathbb{F}_q$. The subspace $[\![a, V_i]\!] + [\![b, V_i]\!]$ has finite codimension in $[\![V_i, V_i]\!]$ if and only if $a/b \in F^r$.*

(2) The subspace $[\![V_i, V_i]\!]$ has finite codimension in F^-.

Proof. Because $[\![a, V_i]\!]$ and $[\![b, V_i]\!]$ have finite codimension in $[\![a, F^-]\!]$ and $[\![b, F^-]\!]$, respectively, we see that $[\![a, V_i]\!] + [\![b, V_i]\!]$ has finite codimension in $[\![a, F^-]\!] + [\![b, F^-]\!]$. Thus, in proving (1), we may assume that $V_i = F^-$.

(1) ($\Leftarrow$) There are some nonzero $u, v \bullet F^-$, such that $au^r = bv^r$. Let $x = a^r u - b^r v$.

We claim that $x \neq 0$. Otherwise, we have

$$a^{r^2-1}(au^r) = (a^r u)^r = (b^r v)^r = b^{r^2-1}(bv^r) = b^{r^2-1}(au^r),$$

so $a^{r^2-1} = b^{r^2-1}$. This implies $a/b \bullet \mathbb{F}_q$, which is a contradiction. This completes the proof of the claim.

For any $y \bullet F^-$, we have

$$\begin{aligned} [\![a, uy]\!] - [\![b, vy]\!] &= (a^r uy - au^r y^r) - (b^r vy - bv^r y^r) \\ &= (a^r uy - b^r vy) - (au^r y^r - bv^r y^r) \\ &= xy - 0, \end{aligned}$$

so $[\![a, F^-]\!] + [\![b, F^-]\!]$ contains xF^-, which is of finite codimension in F^-.

(1) ($\Rightarrow$) We may write b (uniquely) in the form $b = x + y^r a$, with $x, y \in F$, and such that we may write $x = \sum \alpha_i t^{-i}$ with $\alpha_i = 0$ whenever $i \equiv \deg^-(a) (\operatorname{mod} r)$. (Note that we do **not** assume $x, y \bullet F^-$.)

For $u, v \in F^-$, we have

$$\begin{aligned} [\![a, u]\!] - [\![b, v]\!] &= (a^r u - au^r) - (b^r v - bv^r) \\ &= (a^r u - b^r v) - (au^r - (x + y^r a)v^r) \\ &= (a^r u - b^r v) - a(u - yv)^r - xv^r. \end{aligned}$$

Whenever either $\deg^-(u)$ or $\deg^-(v)$ is large, it is obvious that $\deg^-(a^r u - b^r v)$ is much smaller than $\max\{\deg^-(u - yv)^r, \deg^- v^r\}$. Also, we may assume

$x \neq 0$ (otherwise, we have $b/a = y^r \in F^r$, as desired), and, from the definition of x, we know that $\deg^- x \not\equiv \deg^- a \pmod r$, so

$$\deg^-(a(u - yv)^r - xv^r) = \max\{\deg^-(a(u - yv)^r), \deg^-(xv^r)\}.$$

Therefore, we conclude that

$$\deg^-([\![a, u]\!] - [\![b, v]\!]) \in \{\deg^-(a(u - yv)^r), \deg^-(xv^r)\}$$

must be congruent to either $\deg^-(a)$ or $\deg^-(x)$, modulo r. Thus, because of our assumption that $r > 2$, we see that $[\![a, F^-]\!] + [\![b, F^-]\!]$ does not contain elements of all large degrees, so it does not have finite codimension in F^-. Then, from (2), we conclude that it does not have finite codimension in $[\![F^-, F^-]\!]$.

(2) This follows from the above proof of the implication ($\Leftarrow$) of (1). □

Corollary 2.7. *Let $a_1, a_2 \in V_i \setminus \{0\}$. We have $a_1/a_2 \in F^r$ if and only if there is some nonzero $b \in V_1$, such that the subspace $[\![a_j, V_i]\!] + [\![b, V_i]\!]$ has finite codimension in $[\![V_i, V_i]\!]$, for $j = 1, 2$.*

Proof. ($\Rightarrow$) Choose $b \in a_1 F^r \cap V_i \setminus (\mathbb{F}_q a_1 \cup \mathbb{F}_q a_2)$. Then Proposition 2.6(1) implies the desired conclusion.

($\Leftarrow$) From Proposition 2.6(1), we have $a_1/b \in F^r$ and $a_2/b \in F^r$, so $a_1/a_2 \in F^r$. □

Lemma 2.8. *Let $a_1, a_2 \in F^-$, and let $Q > 1$ be a power of r, such that*

$$\lambda^*(a_1(F^-)^Q \cap V_1) = a_2(F^-)^Q \cap V_2.$$

Define

- *subspaces W_1 and W_2 of finite codimension in F^- by $a_i (F^-)^Q \cap V_i = a_i W_i^Q$;*
- *$\mu^* : W_1 \to W_2$ by $\lambda^*(a_1 w^Q) = a_2 \mu^*(w)^Q$; and*
- *$\mu_* : [\![W_1, W_1]\!] \to [\![W_2, W_2]\!]$ by $\lambda_*(a_1^{r+1} w^Q) = a_2^{r+1} \mu_*(w)^Q$.*

Then μ^* and μ_* are $\mathbb{F}_p$-linear bijections, and we have

$$\mu_*[\![a, b]\!] = [\![\mu^*(a), \mu^*(b)]\!],$$

for all $a, b \in W_1$.

Definition 2.9. Let $Q > 1$ be a power of p. An element of F^- is Q-*separable* if it is **not** divisible by a nonconstant Qth power.

Corollary 2.10. *Let $a \in F^-$, and let $Q > 1$ be a power of r, such that a is Q-separable. Then there is some Q-separable $b \in F^-$, such that $\lambda^*\left(a(F^-)^Q \cap V_1\right) = b(F^-)^Q \cap V_2$.*

Proof. Assume, for the moment, that $Q = r$. For $a_1, a_2 \in F^- \setminus \{0\}$, define $a_1 \equiv a_2$ iff $a_1/a_2 \in F^r$. For nonzero $a, b \in V_1$, we see, from Notation 2.3, that $[\![a, V_1]\!] + [\![b, V_1]\!]$ has finite codimension in V_1 if and only if $[\![\lambda^*(a), V_2]\!] + [\![\lambda^*(b), V_2]\!]$ has finite codimension in V_2. Therefore, Corollary 2.7 implies that $a \equiv b$ iff $\lambda^*(a) \equiv \lambda^*(b)$. The equivalence classes are precisely the sets of the form $c(F^-)^r \cap V_i$, for some r-separable $c \in F^-$, so the desired conclusion is immediate.

We may now assume $Q > r$. Let $Q' = Q/r$. There is some Q'-separable $d' \in F^-$, such that $a \in d'(F^-)^{Q'}$. By induction on Q, we know that there is some Q'-separable $b' \in F^-$, such that $\lambda^*\left(d'(F^-)^{Q'} \cap V_1\right) = b'(F^-)^{Q'} \cap V_2$.

From the definition of d', we know there is some $a_1 \in F^-$, such that $a = d'a_1^{Q'}$. Then, because a is Q-separable, we know that a_1 is r-separable.

Define W_1, W_2, μ^*, and μ_* as in Lemma 2.8 (with Q', d', and b' in the places of Q, a, and b, respectively). Because a_1 is r-separable, we know, from the case $Q = r$ in the first paragraph of this proof, that there is some r-separable $b_1 \in F^-$, such that $\mu^*(a_1(F^-)^r \cap W_1) = b_1(F^-)^r \cap W_2$. Therefore

$$\begin{aligned}
\lambda^*(a(F^-)^Q \cap V_1) &= \lambda^*[d'(a_1(F^-)^r)^{Q'} \cap V_1] \\
&= \lambda^*[d'(a_1(F^-)^r \cap W_1)^{Q'}] \\
&= d'[\mu^*(a_1(F^-)^r \cap W_1)]^{Q'} \\
&= b'(b_1(F^-)^r \cap W_2)^{Q'} \\
&= b'(b_1(F^-)^r)^{Q'} \cap V_2 \\
&= b'b_1^{Q'}(F^-)^Q \cap V_2,
\end{aligned}$$

as desired. □

Lemma 2.11. *Let $a \in V_i$, let $Q > 1$ be a power of r, and let k be the codimension of V_i in F^-. Then there is some nonzero $b \in F^-$ with $\deg^- b \le r^2(k+1)$, such that $[\![a(F^-)^Q \cap V_i, V_i]\!]$ contains a subspace of codimension $2k$ in the ideal $a^r b^{Q/r} F^-$; that is,*

$$\dim \frac{a^r b^{Q/r} F^-}{[\![a(F^-)^Q \cap V_i, V_i]\!] \cap a^r b^{Q/r} F^-} \leq 2k.$$

Proof. Choose $c \in F^- \setminus \mathbb{F}_q$, such that $ac^Q \in V_i$ and $\deg^- c \leq k+1$; let $b = c^{r^2} - c$. For $y \in F^-$, we have

$$\begin{aligned} a^r b^{Q/r} y &= a^r (c^{rQ} - c^{Q/r}) y \\ &= (a^r c^{rQ} y - ac^Q y^r) - (a^r c^{Q/r} y - ac^Q y^r) \\ &= [\![ac^Q, y]\!] - [\![a, c^{Q/r} y]\!] \\ &\in [\![ac^Q, F^-]\!] + [\![a, F^-]\!], \end{aligned}$$

so $[\![ac^Q, F^-]\!] + [\![a, F^-]\!]$ contains $a^r b^{Q/r} F^-$.

The codimension of $[\![ac^Q, V_i]\!]$ in $[\![ac^Q, F^-]\!]$ is $\leq k$, and the codimension of $[\![a, V_i]\!]$ in $[\![a, F^-]\!]$ is also $\leq k$. Thus, the conclusion of the preceding paragraph implies that $[\![ac^Q, V_i]\!] + [\![a, V_i]\!]$ contains a subspace of codimension $2k$ in $a^r b^{Q/r} F^-$. Because ac^Q and a belong to $a(F^-)^Q \cap V_i$, the desired conclusion follows. ∎

Proposition 2.12. *Let $a \in V_i$, let $Q > 1$ be a power of r, and let k be the codimension of V_i in F^-. Then*

$$\dim \frac{F^-}{[\![a(F^-)^Q \cap V_i, V_i]\!]} = s(r-1)(\deg^- a) + S + X,$$

where

- $S = s \max\{\deg^- c \mid c^r | a,\ c \in F^-\}$, *and*
- $0 \leq X \leq sr(k+1)Q + 3k$.

Proof. Choose b as in Lemma 2.11, and let $I = a^r b^{Q/r} F^-$ and $\bar{F}^- = F^-/I$. It suffices to show

$$\dim \overline{F^-/[\![a(F^-)^Q, F^-]\!]} \geq s(r-1)(\deg^- a) + S \tag{2.13}$$

and

$$\dim \overline{F^-/[\![a, F^-]\!]} \leq S + sr^2(k+1)Q/r + s(r-1) \deg^- a. \tag{2.14}$$

Let $u_1, u_2, \ldots, u_N$ be the irreducible factors of $a^r b^{Q/r}$. Then we may write

$$a = u_1^{m_1} u_2^{m_2} \cdots u_f^{m_N},$$
$$b^{Q/r} = u_1^{\varepsilon_1} u_2^{\varepsilon_2} \cdots u_f^{\varepsilon_N},$$

and

$$a^r b^{Q/r} = u_1^{n_1} u_2^{n_2} \cdots u_f^{n_N},$$

where $n_j = rm_j + \varepsilon_j$.

From the Chinese Remainder Theorem, we know that the natural ring homomorphism from $\bar{F}^-$ to

$$\bigoplus_{j=1}^{N} \frac{F^-}{u_j^{n_j} F^-}$$

is an isomorphism. Thus, we may work in each factor $F^-/u_j^{n_j}F^-$, and add up the resulting codimensions.

Define $\phi_j : F^- \to F^-/(u_j^{rm_j}F^-)$ by $\phi_j(x) = ax^r$. Then, letting $m_j' = m_j - \lfloor m_j/r \rfloor$, we have

$$\ker \phi_j = \{x \bullet F^- \mid u_j^{m_j'} | x\},$$

so

$$\dim \frac{F^-}{u_j^{rm_j}F^- + a(F^-)^r} = \dim \frac{\ker \phi_j}{u_j^{rm_j}F^-}$$
$$= s \dim_{\mathbb{F}_q} \frac{\ker \phi_j}{u_j^{rm_j}F^-}$$
$$= s(rm_j - m_j')\deg^- u_j$$
$$= s(r-1)\deg^- u_j^{m_j} + s\lfloor m_j/r \rfloor \deg^- u_j.$$

We have $a^r \bullet u_j^{rm_j}F^-$, so

$$\begin{aligned} [\![a(F^-)^Q, F^-]\!] &\subset a^r(F^-)^{Qr}F^- + a(F^-)^Q(F^-)^r \\ &\subset u_j^{rm_j}F^- + a(F^-)^r \end{aligned} \tag{2.15}$$

and

$$[\![a, F^-]\!] + u_j^{rm_j}F^- = u_j^{rm_j}F^- + a(F^-)^r. \tag{2.16}$$

From (2.15), we have

$$\begin{aligned}\dim \frac{F^-}{[\![a(F^-)^Q, F^-]\!] + u_j^{n_j}F^-} &\geq \dim \frac{F^-}{[\![a(F^-)^Q, F^-]\!] + u_j^{rm_j}F^-}\\ &\geq \dim \frac{F^-}{u_j^{rm_j}F^- + a(F^-)^r}\\ &= s(r-1)\deg^- u_j^{m_j} + s\lfloor m_j/r\rfloor \deg^- u_j,\end{aligned}$$

so

$$\begin{aligned}\dim \overline{F^-/[\![a(F^-)^Q, F^-]\!]} &\geq \sum_{j=1}^{N} (s(r-1)\deg^- u_j^{m_j} + s\lfloor m_j/r\rfloor \deg^- u_j)\\ &= s(r-1)\deg^- a + S.\end{aligned}$$

This establishes (2.13).

Because $\dim(u_j^{pm_j}F^-/u_j^{n_j}F^-) = s\varepsilon_j \deg^- u_j$, and from (2.16), we have

$$\begin{aligned}\dim \frac{F^-}{[\![a, F^-]\!] + u_j^{n_j}F^-} &\leq \dim \frac{F^-}{[\![a, F^-]\!] + u_j^{rm_j}F^-} + s\varepsilon_j \deg^- u_j\\ &= \dim \frac{F^-}{u_j^{rm_j}F^- + a(F^-)^r} + s\varepsilon_j \deg^- u_j\\ &= s(r-1)\deg^- u_j^{m_j} + s\lfloor m_j/r\rfloor \deg^- u_j + s\varepsilon_j \deg^- u_j,\end{aligned}$$

so

$$\begin{aligned}\dim \overline{F^-/[\![a, F^-]\!]} &\leq \sum_{j=1}^{N} (s(r-1)\deg^- u_j^{m_j} + s\lfloor m_j/r\rfloor \deg^- u_j\\ &\qquad + s\varepsilon_j \deg^- u_j)\\ &= s(r-1)\deg^- a + S + s\deg^- b^{Q/r}\\ &\leq s(r-1)\deg^- a + S + sr^2(k+1)Q/r.\end{aligned}$$

This establishes (2.14). □

Lemma 2.17. *For any $a \in F^-$ and any $n \geq 0$, we have*

$$[\![a, F^-]\!] + [\![1, F^-]\!] \subset [\![a^{r^n}, F^-]\!] + [\![1, F^-]\!].$$

Proof. For any $v \in F^-$, we have

$$\begin{aligned}
[\![v, a]\!] &= v^r a - va^r \\
&= v^r a - (v^{r^2} a^r - v^{r^2} a^r) - (v^r a^{r^2} - v^r a^{r^2}) - va^r \\
&= [\![v^r a, 1]\!] + [\![v^r, a^r]\!] + [\![va^r, 1]\!] \\
&\in [\![1, F^-]\!] + [\![a^r, F^-]\!].
\end{aligned}$$

Then the proof is completed by induction on n. □

Proposition 2.18. *There is some $N \in \mathbb{N}$ (depending only on the codimensions of V_1 and V_2, not on the choice of V_1, V_2, λ^*, or λ_*), such that* $\deg^- \lambda^*(1) \le N$.

Proof. Let k be the codimension of V_1. Choose a power $Q > 1$ of r so large that $\lambda^*(1)$ is Q-separable. Then Corollary 2.10 implies $\lambda^*((F^-)^Q \cap V_1) = \lambda^*(1)(F^-)^Q \cap V_2$.

Choose $c \in F^- \setminus \mathbb{F}_q$, such that $c^Q \in V_1$ and $\deg^- c \le r + 1$. We have

$$\begin{aligned}
[\![(F^-)^Q \cap V_1, V_1]\!] &\supset [\![1, V_1]\!] + [\![c^Q, V_1]\!] \\
&\approx [\![1, F^-]\!] + [\![c^Q, F^-]\!] \\
&\supset [\![1, F^-]\!] + [\![c^r, F^-]\!] \quad \text{(see 2.17)} \\
&\supset (c^{r^2} - c)F^- \quad \text{(proof of (2.11))}.
\end{aligned}$$

So $[\![(F^-)^Q \cap V_1, V_1]\!]$ has small codimension in $[\![V_1, V_1]\!]$. Therefore $[\![\lambda^*(1)(F^-)^Q \cap V_2, V_2]\!] = \lambda_*[\![(F^-)^Q \cap V_1, V_1]\!]$ must have small codimension in $[\![V_2, V_2]\!]$, so $\deg^- \lambda^*(1)$ must be small, as desired. ■

Corollary 2.19. *There is some $N \in \mathbb{N}$ (depending only on the codimensions of V_1 and V_2, not on the choice of V_1, V_2, λ^*, or λ_*), such that, for every power $Q > 1$ of r and every Q-separable element a of V_1, we have* $\deg^- \lambda^*(a) - \deg^- a' \le QN$, *where a' is the Q-separable element of $\lambda^*(a)F^Q$.*

Proof. Apply Proposition 2.18 to the map μ^* of Lemma 2.8. □

Proposition 2.20. *There is a power $Q > 1$ of r, and some $d > 0$, such that, for every $v \in V_i$ with* $\deg^- v > d$, *there are Q-separable elements $v_1, \ldots, v_m$ of V_i, such that $v = v_1 + \cdots + v_m$ and* $\deg^- v_j \le \deg^- v$, *for $j = 1, \ldots, m$.*

Proof. Let k be the codimension of V_i in F^-, and choose $Q > k+4$ so large that, for every $m \geq Q$, the subspace V_i contains elements of degree m whose leading coefficients span $\mathbb{F}_q$. For any element of V_1 of degree m, we show that there is a Q-separable element of V_i of degree m with the same leading coefficient.

Let α be the leading coefficient of some element of V_1 of degree m. Then V_i contains exactly r^{m-k} elements of degree m with leading coefficient α.

On the other hand, if a is an element of F^- that is of degree m and is not Q-separable, then a must be of the form $a = x^Q y$, where x is an element of F^- of some degree j, and y is an element of F^- of degree $m - Qj$. Thus, the number of such elements a of degree m is no more than

$$\sum_{j=1}^{\infty} q^{j+1} q^{m-Qj+1} = q^{m+2} \sum_{j=1}^{\infty} q^{j(1-Q)} = \frac{q^{m+2}}{q^{Q-1}-1} \leq \frac{q^{m+2}}{q^{Q-2}} < Q^{m-Q+4} < \frac{Q^m}{r^k}.$$

Therefore, not every element of V_i of degree m whose leading coefficient is α can be such an element a, so V_i has a Q-separable element of degree m with leading term α, as desired. □

Corollary 2.21. *For each $b \in F^-$, there exists $N \in \mathbb{N}$, such that, for every $a \in b(F^-)^r \cap V_1$, we have $|\deg^- \lambda^*(a) - \deg^- a| \leq N$.*

Proof. By symmetry, it suffices to show $\deg^- \lambda^*(a) \leq \deg^- a + N$. We may assume b is r-separable. By combining Proposition 2.20 with Lemma 2.8, we may choose a power $Q > 1$ of r, such that each element of $b(F^-)^r$ is a sum of Q-separable elements of $b(F^-)^r$ of smaller degree. Thus, we may assume a is Q-separable (and our bound N may depend on Q).

Define S as in the statement of Proposition 2.12, and let k_i be the codimension of V_i. Because $a \in b(F^-)^r$ and b is r-separable, we have $S = s(\deg^- a - \deg^- b)/r$, so Proposition 2.12 implies

$$\left|\dim \frac{F^-}{[\![a(F^-)^Q \cap V_1, V_1]\!]} - s(r-1+1/r)\deg^- a\right| \leq s\frac{\deg^- b}{r} + (sr(k_1+1)Q + 3k_1)$$

is bounded. Similarly, letting a' be the Q-separable element of $\lambda^*(a)F^Q$, and b' be the r-separable element of $\lambda^*(b)F^r$, we know that

$$\left|\dim \frac{F^-}{[\![a'(F^-)^Q \cap V_2, V_2]\!]} - s(r-1+1/r)\deg^- a'\right|$$
$$\leq s\frac{\deg^- b'}{r} + (sr(k_2+1)Q + 3k_2)$$

is bounded. Then, because

$$\dim \frac{[\![V_1, V_1]\!]}{[\![a(F^-)^Q \cap V_1, V_1]\!]} = \dim \frac{[\![V_2, V_2]\!]}{[\![a'(F^-)^Q \cap V_2, V_2]\!]},$$

we see that $|\deg^- a' - \deg^- a|$ is bounded. Corollary 2.19 asserts that $|\deg^- \lambda^*(a) - \deg^- a'|$ is also bounded. □

Corollary 2.22. *For each $b \in F^-$, there is a power Q of r, such that, for every $a_1, a_2 \in b(F^-)^Q \cap V_1$, we have $\deg^- \lambda^*(a_1) - \deg^- \lambda^*(a_2) = \deg^- a_1 - \deg^- a_2$.*

Proof. Choose N as in Corollary 2.21. Now choose $Q > 2N$. Because

$$\deg^- \lambda^*(a_1) \equiv \deg^- \lambda^*(a_2) \pmod{Q}$$

and

$$\deg^- a_1 \equiv \deg^- a_2 \pmod{Q},$$

we have

$$\deg^- \lambda^*(a_1) - \deg^- a_1 \equiv \deg^- \lambda^*(a_2) - \deg^- a_2 \pmod{Q},$$

so, from the choice of N and Q, we conclude that

$$\deg^- \lambda^*(a_1) - \deg^- a_1 = \deg^- \lambda^*(a_2) - \deg^- a_2.$$ ■

Proposition 2.23. *There is a constant $C > 0$, such that, for all $a_1, a_2 \in V_i$, and every power Q of r, we have*

$$s\deg^- \gcd(a_1, a_2) - C \leq \dim \frac{[\![V_i, V_i]\!]}{[\![a_1(F^-)^Q \cap V_i, V_i]\!] + [\![a_2(F^-)^Q \cap V_i, V_i]\!]}$$
$$\leq C\deg^- \gcd(a_1, a_2) + C.$$

Proof. Because
$$[\![a_1(F^-)^Q \cap V_i, V_i]\!] + [\![a_2(F^-)^Q \cap V_i, V_i]\!] \subset \gcd(a_1, a_2)F^-,$$
the left-hand inequality is obvious.

Let $c = \gcd(a_1, a_2)$ and let k be the codimension of V_i. Then Lemma 2.11 implies that there exist nonzero $b_1, b_2 \in F^-$ with $\deg^- b_j \leq r^2(k+1)$, such that $[\![a_j(F^-)^Q \cap V_i, V_i]\!]$ contains a subspace of codimension $2k$ in $a_j^r b_j^{Q/r} F^-$, for $j = 1, 2$. Then, letting $b = b_1 b_2$, we have $\deg^- b \leq 2r^2(k+1)$, and $[\![a_1(F^-)^Q \cap V_i, V_i]\!] + [\![a_2(F^-)^Q \cap V_i, V_i]\!]$ contains a subspace of codimension $4k$ in the ideal $I = c^r b^{Q/r} F^-$. Thus, it suffices to show that the codimension of $[\![a_1, F^-]\!] + [\![a_2, F^-]\!] + I$ in F^- is bounded above by $s(r+2)\deg^- c + s\deg^- b$.

Let $u_1, \ldots, u_N$ be the irreducible factors of $c^r b^{Q/r}$, so we may write

$$c = u_1^{m_1} \cdots u_N^{m_N},$$
$$b = u_1^{\varepsilon_1} \cdots u_N^{\varepsilon_N},$$

and

$$c^r b^{Q/r} = u_1^{n_1} \cdots u_N^{n_N},$$

where $n_j = rm_j + \varepsilon_j Q/r$. From the Chinese Remainder Theorem, we have $F^-/I \cong \oplus_{j=1}^N F^-/u^{n_j}F^-$, so we may calculate the codimension in each factor, and then add them.

Fix j. By interchanging a_1 and a_2 if necessary, we may assume that $u_j^{m_j+1} \nmid a_1$. It suffices to show that

$$\dim \frac{F^-}{[\![a_1, F^-]\!] + u^{n_j}F^-} \leq s((r+2)m_j + \varepsilon_j)\deg^- u_j;$$

thus (because $m_j + \varepsilon_j \geq 1$), we need only show that $u_j^{(r+1)m_j+1} F^- \subset [\![a_1, F^-]\!] + u_j^{n_j} F^-$. To show this, let M be minimal, such that $u_j^{M+1} F^- \subset [\![a, F^-]\!] + u_j^{n_j} F^-$. (Obviously, we have $M < n_j$; we wish to show $M \leq (r+1)m_j$.) Suppose $M > (r+1)m_j$. (This will lead to a contradiction.) We have $m_j + r(M - rm_j) > M$, so

$$\begin{aligned}
u_j^M F^- &= u_j^{rm_i} u_j^{M-rm_j} F^- \\
&\subset a_1^r u_j^{M-rm_j} F^- + u^{n_j} F^- \\
&\subset [\![a_1, u_j^{M-rm_j} F^-]\!] + a_1 u_j^{r(M-rm_j)} F^- + u^{n_j} F^- \\
&\subset [\![a_1, F^-]\!] + u_j^{m_j + r(M-rm_j)} F^- + u^{n_j} F^- \\
&\subset [\![a_1, F^-]\!] + u_j^{M+1} F^- + u^{n_j} F^- \\
&= [\![a_1, F^-]\!] + u^{n_j} F^-.
\end{aligned}$$

This contradicts the minimality of M. □

Corollary 2.24. *There is a constant $C > 0$, such that, for all $a, b \in V_1$, we have*

$$\frac{\deg^- \gcd(a,b)}{C} - C \leq \deg^- \gcd(\lambda^*(a), \lambda^*(b)) \leq C \deg^- \gcd(a,b) + C.$$

Proposition 2.25. *There exist $b \in V_1$, $b' \in V_2$, $\alpha, \beta \in \mathbb{F}_q$, and some Q that is a power of both r and q, such that, for all $b\, f(t^{-Q}) \in b(\mathbb{F}_p[t^{-1}])^Q \cap V_1$, we have $\lambda^*(b\, f(t^{-Q})) = b'\, f(\alpha t^{-Q} + \beta)$.*

Proof. Corollary 2.22 shows that, by replacing V_1 with some $(F^-)^Q \cap V_1$ (using Lemma 2.8), we may assume $\deg^- \lambda^*(a) = \deg^- a$, for every $a \in V_1$.

The terms $-C$ and $+C$ in Corollary 2.24 are significant only when $\deg^- \gcd(a,b)$ is small. On the other hand, $\deg^- \gcd(a,b)$ can never be small (and nonzero) if $a, b \in (F^-)^Q$ for some large Q. Thus, by replacing V_1 with some $(F^-)^Q \cap V_1$ (using Lemma 2.8), we may assume

$$\frac{1}{C} \deg^- \gcd(a,b) \leq \deg^- \gcd(\lambda^*(a), \lambda^*(b)) \leq C \deg^- \gcd(a,b),$$

for every $a, b \in V_1$. In particular, $\gcd(a,b) = 1$ if and only if $\gcd(\lambda^*(a), \lambda^*(b)) = 1$.

Let k be the codimension of V_1 in F^-. Choose some

$$N > 4(C(C+k)p^{C+k+1} + k + 1).$$

Choose a power Q of r, such that $Q > Nk$. There is some nonzero $b \in \mathbb{F}_p[t^{-1}]$, with $\deg^- b \leq Nk$, such that

$$b(\mathbb{F}_p + t^{-Q}\mathbb{F}_p + t^{-2Q}\mathbb{F}_p + \cdots + t^{-NQ}\mathbb{F}_p) \subset V_1.$$

Because $\deg^- b < Q$, we know that b is Q-separable, so, by applying Lemma 2.8 to $b(F^-)^Q \cap V_1$, we may assume

$$\mathbb{F}_p + t^{-1}\mathbb{F}_p + t^{-2}\mathbb{F}_p + \cdots + t^{-N}\mathbb{F}_p \subset V_1.$$

By composing λ^* with a map of the form $f(t^{-1}) \mapsto \gamma f(\alpha t^{-1} + \beta)$, for some $\alpha, \beta, \gamma \in \mathbb{F}_q$ (with $\alpha\gamma \neq 0$), we may assume $\lambda^*(1) = 1$ and $\lambda^*(t^{-1}) = t^{-1}$, so $\lambda^*|_{\mathbb{F}_p + \mathbb{F}_p t^{-1}} = \mathrm{Id}$.

Let $V_1^{\mathbb{F}_p} = V_1 \cap \mathbb{F}_p[t^{-1}]$. It suffices to show $\lambda^*(a) = a$ for every $a \bullet V_1^{\mathbb{F}_p}$. Suppose $\lambda^*|_{V_1^{\mathbb{F}_p}} \neq \mathrm{Id}$, and let

$$m = \min\{\deg^- a | \lambda^*(a) \neq a, a \in V_1^{\mathbb{F}_p}\} \geq 2.$$

Let $\Delta = \lambda^*(a) - a$, for any monic $a \in V_1^{\mathbb{F}_p}$ with $\deg^- a = m$. (Note that the definition of m implies that Δ is independent of the choice of a.)

Case 1. Assume $m \leq N$. Let u be any irreducible element of $\mathbb{F}_p[t^{-1}]$ with $\deg^- u \leq m - 1$.

We claim that $V_1^{\mathbb{F}_p}$ contains a (monic) element a, such that $\deg^- a = m$ and $u|a$. To see this, let $b \in V_1^{\mathbb{F}_p}$ with $\deg^- b = m$. There is some $a \bullet F^-$, such that $u|a$ and $\deg^-(a - b) < \deg^- u < \deg^- b$. Because $\deg^- b \leq N$, this implies $a - b \bullet V_1^{\mathbb{F}_p}$, so $a \in V_1^{\mathbb{F}_p}$.

Because $u|a$ (and $\lambda^*(u) = u$), we know $\gcd(u, \lambda^*(a)) \neq 1$. Because u is irreducible, we conclude that $u|\lambda^*(a)$. We also have $u|a$, so this implies $u|(\lambda^*(a) - a) = \Delta$.

Thus, we see that Δ is divisible by every irreducible polynomial over $\mathbb{F}_p$ of degree $\leq m - 1$, so Δ is divisible by $t^{-p^{m-1}} - t^{-1}$. Therefore $\deg^- \Delta \geq p^{m-1}$. However, we also know $\deg^- \Delta \leq \deg^- a = m$ (and all nonzero polynomials in $\mathbb{F}_2[t^{-1}]$ are monic, so $\deg^- \Delta < m$ if $p = 2$). This is a contradiction.

Case 2. Assume $m > N$. Choose some monic $a \bullet V_1^{\mathbb{F}_p}$, with $\deg^- a = m$. By subtracting a polynomial of degree $\leq k$, we may assume $t^{-(k+1)}|a$; let $u = a/t^{-(k+1)}$. There is some nonzero $x \in \mathbb{F}_p[t^{-1}]$ with $\deg^- x \leq k$, such that $ux \in V_1^{\mathbb{F}_p}$. (Note that $\deg^- ux \leq k + \deg^- u < m$.)

Let

$$\mathcal{C} = \{c \in \mathbb{F}_p[t^{-1}] \setminus \{0\} | \deg^- c < C\},$$

and

$$b = \prod_{\deg^- c \leq C+k} c,$$

so $\deg^- b < (C + k)p^{C+k+1}$. Now, for each $c \bullet \mathcal{C}$, let

$$u_c = (u + c)x \quad \text{and} \quad u_c' = \frac{u_c}{\gcd(u_c, b)}.$$

For $c \in \mathcal{C}$, we have $\{cx, ct^{-(k+1)}\} \subset V_1^{\mathbb{F}_p}$, so $u_c \in V_1^{\mathbb{F}_p}$ and $a + ct^{-(r+1)} \in V_1^{\mathbb{F}_p}$. Also, because $a = ut^{-(k+1)}$, we have $(u+c)|(a+ct^{-(k+1)})$. Then, since $\lambda^*(u+c) = u+c$, we have $\deg^- \gcd(\lambda^*(a+ct^{-(k+1)}), u+c) \geq (\deg^- (u+c))/ C$, so

$$\begin{aligned}\deg^-\gcd(\Delta, u_c') &\geq \deg^-\gcd(\Delta, u_c) - \deg^- b \\ &= \deg^-\gcd(\lambda^*(a+ct^{-(k+1)}) \\ &\quad - (a+ct^{-(k+1)}), u_c) - \deg^- b \\ &\geq \frac{\deg^-(u+c)}{C} - \deg^- b \\ &\geq \frac{m-k-1}{C} - (C+k)p^{C+k+1} \\ &\geq \frac{m}{4C}.\end{aligned}$$

Also, for $c_1, c_2 \in \mathcal{C}$, we have

$$\deg^-\gcd(u_{c_1}, u_{c_2}) \leq \deg^-(u_{c_1} - u_{c_2}) = \deg^-((c_1 - c_2)x) \leq C + k,$$

so we see that $\gcd(u'_{c_1}, u'_{c_2}) = 1$ whenever $c_1 \neq c_2$. Thus, we conclude that

$$\deg^-\Delta \geq p^C \frac{m}{4C} > m.$$

This is a contradiction. □

Proof of Theorem 2.4. Choose b, b', α, β, Q as in Proposition 2.25. By replacing λ^* with $x \mapsto (b')^{-1}\lambda^*(bx)$ and replacing λ_* with $x \mapsto (b')^{-(r+1)}$ $\lambda^*(b^{r+1}x)$, we may assume $b = b' = 1$. Then, by composing λ^* and λ_* with $t^{-1} \mapsto \alpha^{-1}(t^{-1} - \beta)$, we may assume $\alpha = 1$ and $\beta = 0$. Thus,

$$\lambda^*(a) = a \text{ for all } a \bullet \mathbb{F}_p[t^{-Q}] \cap V_1. \tag{2.26}$$

We wish to show that there is some $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, such that, for every $a \bullet V_1$, we have $\lambda^*(a) = \sigma(a)$.

Step 1. For each $a \in V_1$, there is some $\sigma \bullet \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, such that $\lambda^*(a) = \sigma(a)$. Fix $a \in V_1$. Choose C as in Corollary 2.24, let k be the codimension of V_1, and choose $b \in \mathbb{F}_p[t^{-Q}] \cap V_1$, such that

$$\frac{\deg^- b}{C} - C > Q(s(\deg^- a + \deg^- \lambda^*(a)) + k).$$

Let

$$c = \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} (b - \sigma(a)) \qquad \in \mathbb{F}_p[t^{-1}],$$

and choose some nonzero $x \in \mathbb{F}_p[t^{-1}]$, such that $(cx)^Q \in V_1$ and $\deg^- x \leq k$.

We have

$$\begin{aligned} Q(\deg^- \gcd(b-\lambda^*(a),c)+k) &\geq \deg^- \gcd(b-\lambda^*(a),(cx)^Q) \\ &= \deg^- \gcd(\lambda^*(b-a),\lambda^*((cx)^Q)) \quad \text{(see 2.26)} \\ &\geq \frac{\deg^- \gcd(b-a,(cx)^Q)}{C} - C \quad \text{(choice of } C\text{)} \\ &= \frac{(\deg^- b)}{C} - C \qquad ((b-a)|c) \\ &> Q(s(\deg^- a + \deg^- \lambda^*(a)) + k) \text{(choice of } b\text{)}. \end{aligned}$$

Thus, from the definition of c, we conclude that there is some $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, such that

$$\begin{aligned} \deg^- \gcd(b - \lambda^*(a), b - \sigma(a)) &> \deg^- a + \deg^- \lambda^*(a) \\ &= \deg^- \sigma(a) + \deg^- \lambda^*(a) \\ &\geq \deg^- (\sigma(a) - \lambda^*(a)) \\ &= \deg^- ((b - \lambda^*(a)) - (b - \sigma(a))). \end{aligned}$$

Therefore $(b - \lambda^*(a)) - (b - \sigma(a)) = 0$, so $\lambda^*(a) = \sigma(a)$.

Step 2. There is some $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, *such that* $\lambda^*(a) = \sigma(a)$ *for every* $a \in V_1$. For $v \in F^-$, let $\bar{v}$ denote the leading coefficient of v. Choose $b \in V_1$, such that $\bar{b}$ generates $\mathbb{F}_q$, that is, $\mathbb{F}_q = \mathbb{F}_p[\bar{b}]$. From Step 1, we know there is some $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, such that $\lambda^*(b) = \sigma(b)$. We show $\lambda^*(a) = \sigma(a)$ for every $a \in V_1$.

Given $a \in V_1$, choose some $c \in V_1$, such that $\bar{c}$ generates $\mathbb{F}_q$, and such that $\deg^- c > \max\{\deg^- a, \deg^- b\}$. From Step 1, there exist $\sigma', \sigma'' \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, such that $\lambda^*(c) = \sigma'(c)$ and $\lambda^*(a+c) = \sigma''(a+c)$. Because $\deg^- c > \deg^- a$, we have $\bar{c} = \overline{a+c}$ and $\overline{\lambda^*(a+c)} = \overline{\lambda^*(c)}$. Thus, we have

$$\begin{aligned} \sigma''(\bar{c}) &= \sigma''(\overline{a+c}) = \overline{\sigma''(a+c)} = \overline{\lambda^*(a+c)} = \overline{\lambda^*(a) + \lambda^*(c)} = \overline{\lambda^*(c)} \\ &= \sigma'(\bar{c}). \end{aligned}$$

Because $\bar{c}$ generates $\mathbb{F}_q$, we conclude that $\sigma'' = \sigma'$. Therefore

$$\lambda^*(a) = \lambda^*(a+c) - \lambda^*(c) = \sigma''(a+c) - \sigma'(c) = \sigma'(a+c) - \sigma'(c)$$
$$= \sigma'(a).$$

Similarly, we have $\lambda^*(b) = \sigma'(b)$. Because we also have $\lambda^*(b) = \sigma(b)$, and $\bar{b}$ generates $\mathbb{F}_q$, we conclude that $\sigma' = \sigma$.

Therefore $\lambda^*(a) = \sigma'(a) = \sigma(a)$, as desired. □

3. ARITHMETIC SUBGROUPS OF HEISENBERG GROUPS

Proof of Theorem 1.15. Let Γ_1, Γ_2 be finite-index subgroups of Γ, such that $\lambda : \Gamma_1 \to \Gamma_2$ is an isomorphism. Let $\bar{\Gamma}_i$, $i = 1, 2$ be the image of Γ_i in F^{2m} under the projection $H \to F^{2m}$ with kernel Z. By passing to a finite-index subgroup, we can assume that $\bar{\Gamma}_i \subset (F^-)^{2m}$. Since $Z(\Gamma_i) = \Gamma_i \cap Z$, we can identify $\bar{\Gamma}_i$ with $\Gamma_i/Z(\Gamma_i)$, so λ induces an isomorphism $\bar{\lambda} : \bar{\Gamma}_1 \to \bar{\Gamma}_2$.

Step 1. We can assume $\bar{\lambda}(av) = a\bar{\lambda}(v)$ for all $a \in F^-$ and $v \in \bar{\Gamma}_1$, such that $av \in \bar{\Gamma}_1$. For each nonzero $v \in \bar{\Gamma}_1$, let $A_v = \{a \bullet F^- \mid av \in \bar{\Gamma}_1\}$. Note that A_v is a finite-index subgroup of F^-. For $g, h \bullet \Gamma_i$, we have $F\bar{g} = F\bar{h}$ if and only if $C_{\Gamma_i}(g) = C_{\Gamma_i}(h)$, so $\bar{\lambda}(A_v v) = F\bar{\lambda}(v) \cap \bar{\Gamma}_2$. Thus, we can define a function $\tau_v : A_v \to F$ by $\tau_v(a)\bar{\lambda}(v) = \bar{\lambda}(av)$. Let $w \in \bar{\Gamma}_1$ be such that $[\![v, w]\!] \neq 0$, and let $a \bullet A_v \cap A_w$. Then

$$\begin{aligned}
\tau_v(a)[\![\bar{\lambda}(v), \bar{\lambda}(w)]\!] &= [\![\bar{\lambda}(av), \bar{\lambda}(w)]\!] \\
&= \lambda([\![av, w]\!]) \\
&= \lambda([\![v, aw]\!]) \\
&= [\![\bar{\lambda}(v), \bar{\lambda}(aw)]\!] \\
&= \tau_w(a)[\![\bar{\lambda}(v), \bar{\lambda}(w)]\!].
\end{aligned}$$

Thus

$$\tau_v = \tau_w \text{ on } A_v \cap A_w \text{ whenever } [\![v, w]\!] \neq 0. \tag{3.1}$$

For any nonzero $v, w \bullet \bar{\Gamma}_1$ and any $a \in A_v \cap A_w$, since $\bar{\Gamma}_1 \cap a^{-1}\bar{\Gamma}_1$ is of finite index in $\bar{\Gamma}_1$, we can find $u \in \bar{\Gamma}_1$ so that $a \in A_u$, $[\![u, v]\!] \neq 0$, and $[\![u, w]\!] \neq 0$. Then it follows from Eq. (3.1) that $\tau_v(a) = \tau_u(a) = \tau_w(a)$. Since $a \in A_v \cap A_w$ was arbitrary, we conclude that

$$\tau_v = \tau_w \text{ on } A_v \cap A_w, \text{ for all nonzero } v, w \in \bar{\Gamma}_1. \tag{3.2}$$

For an arbitrary $a \in F^-$ we can always find $w \in \bar{\Gamma}_1$ so that $a \in A_w$, thus we can define a function $\tau : F^- \to F$, by $\tau(a) = \tau_w(a)$. Eq. (3.2) implies that τ is well defined. Note that $\tau(1) = 1$. Since

$$\begin{aligned}\tau(a)\tau(b)[\![\bar{\lambda}(u), \bar{\lambda}(v)]\!] &= [\![\bar{\lambda}(au), \bar{\lambda}(bv)]\!] \\ &= \lambda([\![au, bv]\!]) \\ &= \lambda([\![abu, v]\!]) \\ &= [\![\bar{\lambda}(abu), \bar{\lambda}(v)]\!] \\ &= \tau(ab)[\![\bar{\lambda}(u), \bar{\lambda}(v)]\!],\end{aligned}$$

we have $\tau(a)\tau(b) = \tau(ab)$. Since τ is also an additive homomorphism, and $\bar{\lambda}$ is an isomorphism, we conclude that τ is a ring automorphism of F^-. Therefore $\tau(f(t^{-1})) = \sigma(f(\alpha t^{-1} + \beta))$ for $f(t^{-1}) \in F^-$, where $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, $\alpha \in \mathbb{F}_q \setminus \{0\}$, and $\beta \in \mathbb{F}_q$. Hence, by composing with the standard automorphism $T_{\mathrm{Id},\tau^{-1}}$, we obtain the claim.

Step 2. We may assume that $\lambda|_{Z(\Gamma_1)}$ is the identity map. Let $v_1, w_1, v_2, w_2 \in \bar{\Gamma}$ with $[\![v_i, w_i]\!] \neq 0$. There is a finite-index subgroup A of F^-, such that $av_i \in \bar{\Gamma}$, for every $a \in A$ and $i = 1, 2$. Then, for all $a \in A$, Step 1 implies that

$$\frac{\lambda(a[\![v_i, w_i]\!])}{a[\![v_i, w_i]\!]} = \frac{\lambda([\![v_i, w_i]\!])}{[\![v_i, w_i]\!]}.$$

Thus, choosing $a_1, a_2 \in A$, such that $a_1[\![v_1, w_1]\!] = a_2[\![v_2, w_2]\!]$, we have

$$\frac{\lambda([\![v_1, w_1]\!])}{[\![v_1, w_1]\!]} = \frac{\lambda(a_1[\![v_1, w_1]\!])}{a_1[\![v_1, w_1]\!]} = \frac{\lambda(a_2[\![v_2, w_2]\!])}{a_2[\![v_2, w_2]\!]} = \frac{\lambda([\![v_2, w_2]\!])}{[\![v_2, w_2]\!]}.$$

We conclude that $\lambda(z)/z = C$ is constant, for $z \in [\![\bar{\Gamma}_1, \bar{\Gamma}_1]\!] \setminus \{0\}$.

By composing with a standard automorphism $\phi_{T,\mathrm{Id}}$, such that $c_T = 1/C$, we may assume that $C = 1$, so $\lambda|_{[\Gamma_1,\Gamma_1]} = \mathrm{Id}$. Then, by replacing Γ_1 with a finite-index subgroup Γ_1', such that $\Gamma_1' \cap Z \subset [\Gamma_1, \Gamma_1]$, we may assume $\lambda|_{Z(\Gamma_1)} = \mathrm{Id}$.

Step 3. $\bar{\lambda} : \bar{\Gamma}_1 \to \bar{\Gamma}_1$ can be extended to a symplectic similitude $\bar{\Lambda} : F^{2m} \to F^{2m}$, with $c_{\bar{\Lambda}} = 1$. By Step 1, $\bar{\lambda}(av) = a\bar{\lambda}(v)$ for all $a \in F^-$ and $v \in \bar{\Gamma}_1$ such that $av \in \bar{\Gamma}_1$. Because $\bar{\Gamma}_1$ is commensurable with $(F^-)^{2m}$, this implies that $\bar{\lambda}$ extends (uniquely) to an F-linear map $\bar{\Lambda} : F^{2m} \to F^{2m}$. For any $v, w \in \bar{\Gamma}_1$, we have

$$\llbracket \bar{\Lambda}(v), \bar{\Lambda}(w) \rrbracket = \llbracket \bar{\lambda}(v), \bar{\lambda}(w) \rrbracket = \lambda(\llbracket v, w \rrbracket) = \llbracket v, w \rrbracket,$$

by Step 2. Because $\bar{\Gamma}_1$ spans F^{2m}, this implies that $\bar{\Lambda}$ is a symplectic similitude, with $c_{\bar{\Lambda}} = 1$.

Step 4. Completion of the proof. Define $\hat{\Lambda} : H \to H$ by $\hat{\Lambda}(v, z) = (\bar{\Lambda}(v), z)$. From Step 3, we see that $\hat{\Lambda}$ is an automorphism. Denote by $\zeta : \Gamma_1 \to Z(H)$ the map defined by $\zeta(\gamma) = \hat{\Lambda}(\gamma)^{-1}\lambda(\gamma)$. Then ζ is a homomorphism and $\lambda(\gamma) = \zeta(\gamma)\hat{\Lambda}(\gamma)$, for $\gamma \in \Gamma_1$. □

Proof of Corollary 1.16. From Theorem 1.15, we may assume that the following exist

- a standard automorphism $\phi_{T,\tau}$ of H; and
- a homomorphism $\zeta : \Gamma_1 \to Z(H)$,

such that $\lambda(\gamma) = \phi_{T,\tau}(\gamma)\zeta(\gamma)$ for all $\gamma \bullet \Gamma_1$. By Lemma 2.1, there exists a finite-index open subgroup $\hat{H}$ of H, containing $[H, H]$, such that ζ extends to $\hat{\zeta} : \hat{H} \to Z(H)$. Let $H' = \phi_{T,\tau}(\hat{H})$.

Define $\hat{\Lambda} : \hat{H} \to H$ by $\hat{\Lambda}(h) = \phi_{T,\tau}(h)\hat{\zeta}(h)$, so that $\hat{\Lambda}$ is a continuous homomorphism virtually extending λ. Because $\hat{\zeta}$ is trivial on $[H, H]$, we have $\hat{\Lambda}|_{[H,H]} = \phi_{T,\tau}|_{[H,H]}$, so $\hat{\Lambda}|_{[H,H]}$ is an automorphism. Because $\hat{\zeta}(\hat{H}) \subset Z(H) = [H, H]$, we see that $\hat{\Lambda}$ induces an isomorphism $\hat{H}/[H, H] \to H'/[H, H]$. So $\hat{\Lambda} : \hat{H} \to H'$ is an isomorphism. □

Definition 3.3. *Let*

$$H_p = \left\{ \begin{pmatrix} 1 & x_1^p & x_2^p & \cdots & x_m^p & z \\ & 1 & & & & y_1^p \\ & & 1 & 0 & & y_2^p \\ & & & \ddots & & \vdots \\ & 0 & & & 1 & y_m^p \\ & & & & & 1 \end{pmatrix} \middle| \begin{array}{r} x_1, \ldots, x_m \in F, \\ y_1, \ldots, y_m \in F, \\ z \in F \end{array} \right\}.$$

Remark 3.4. H_p could also be described as the F-points of the group obtained from H by applying the isogeny of factoring by the Lie algebra of $Z(H)$ [1, Prop. V.17.4, p. 215].

Corollary 3.5. *Any arithmetic lattice in H_p is automorphism rigid.*

Proof. Let $\lambda_p : \Gamma_1 \to \Gamma_2$ be an isomorphism, where Γ_1 and Γ_2 are arithmetic lattices in H_p. Define

$$H'_p = \left\{ \begin{pmatrix} 1 & x_1^p & x_2^p & \cdots & x_m^p & z \\ & 1 & & & & y_1^p \\ & & 1 & 0 & & y_2^p \\ & & & \ddots & & \vdots \\ & 0 & & & 1 & y_m^p \\ & & & & & 1 \end{pmatrix} \middle| \begin{array}{r} x_1, \dots, x_m \in F, \\ y_1, \dots, y_m \in F, \\ z \in F \end{array} \right\}$$

and

$$A = \left\{ \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & z \\ & 1 & & & & 0 \\ & & 1 & 0 & & 0 \\ & & & \ddots & & \vdots \\ & 0 & & & 1 & 0 \\ & & & & & 1 \end{pmatrix} \middle| \begin{array}{l} z = \sum_{\substack{0 \le i \le n \\ i \not\equiv 0 \pmod p}} \alpha_i t^{-i}, \\ n \in \mathbb{N}, \\ \alpha_i \in \mathbb{F}_q \end{array} \right\}$$

Then $H_p = H'_p \times A$. By passing to a finite-index subgroup we may assume that $\Gamma_1 = \Gamma'_1 \times \Gamma_{1,A}$, where $\Gamma'_1 = \Gamma_1 \cap H'_p$ and $\Gamma_{1,A} = \Gamma_1 \cap A$. Let $\Omega = \lambda_p(\Gamma_{1,A}) \subset Z(\Gamma_2)$ and $\Gamma'_2 = \lambda_p(\Gamma'_1)$. Then, by passing to a finite-index subgroup, we may assume $\Omega \cap H'_p = e$ and $\Gamma'_2 \cap A = e$.

Step 1. Let $\pi_A : Z(H_p) \to A$ denote the projection with kernel H'_p. Then $\pi_A \circ \lambda_p : \Gamma_{1,A} \to \pi_A(\Omega)$ virtually extends to a virtual automorphism Ψ of A. It is easy to see that $\pi_A(Z(\Gamma_2))$ is closed in A and hence is a lattice. Because $Z(\Gamma'_1) \times \Gamma_{1,A}$ has finite index in $Z(\Gamma_1)$, we know $\lambda_p(Z(\Gamma'_1)) \times \lambda_p(\Gamma_{1,A})$ has finite index in $Z(\Gamma_2)$. Then, since $[\Gamma'_1, \Gamma'_1]$ has finite index in $Z(\Gamma'_1)$ and

$$\lambda_p([\Gamma'_1, \Gamma'_1]) \subset [\Gamma'_2, \Gamma'_2] \subset H'_p = \ker \pi_A$$

we conclude that $\pi_A(\Omega) = \pi_A(\lambda_p(\Gamma_{1,A}))$ has finite index in $\pi_A(Z(\Gamma_2))$. Hence $\pi_A(\Omega)$ is a lattice in A. By Proposition 1.6 $\pi_A \circ \lambda_p : \Gamma_{1,A} \to \pi_A(\Omega)$ virtually extends to a virtual automorphism Ψ of A.

Step 2. Let $\pi' : H_p \to H'_p$ be the projection with kernel A, and let $\mu_p = \pi' \circ \lambda_p|_{\Gamma'_1} : \Gamma'_1 \to \pi'(\Gamma'_2)$. Then μ_p virtual extends to a virtual automorphism of H'_p.

We claim that $\pi'(\Gamma'_2)$ is an arithmetic lattice in H'_p. Because $\Gamma_1 = \Gamma'_1 \times \Gamma_{1,A}$ and $\Gamma_{1,A} \subset Z(\Gamma_1)$, we have

$$\Gamma_2 = \Gamma'_2 \times \Omega \subset \Gamma'_2 Z(H_p).$$

Then, because $\Gamma'_2 \subset \Gamma_2$, we conclude that $\Gamma'_2 Z(H_p) = \Gamma'_2 Z(H_p)$ is a lattice in $H_p/Z(H_p) \cong H'_p/Z(H'_p)$. So the image of $\pi'(\Gamma'_2)$ in $H'_p/Z(H'_p)$ is a lattice. Also,

$$\pi'(\Gamma_2') \cap Z(H_p') \supset [\Gamma_2', \Gamma_2'] = [\Gamma_2, \Gamma_2],$$

so $\pi'(\Gamma_2') \cap Z(H_p')$ is a lattice in $[H_p, H_p] = Z(H_p')$. Thus, we conclude that $\pi'(\Gamma_2')$ is a lattice in H_p'. Because $\pi'(\Gamma_2')$ is contained in the arithmetic lattice $\pi'(\Gamma_2)$, this implies that $\pi'(\Gamma_2')$ is arithmetic.

From the preceding paragraph, we know that μ_p is an isomorphism of arithmetic lattices in H_p'. Let $\mathrm{F}_{\bar{\mathrm{r}}} : H \to H_p'$ denote the group isomorphism induced by the Frobenius automorphism $x \to x^p$ of the ground field F. Then there exist arithmetic lattices $\hat{\Gamma}_1, \hat{\Gamma}_2$ in H, such that $\mathrm{F}_{\bar{\mathrm{r}}}(\hat{\Gamma}_1) = \Gamma_1'$ and $\mathrm{F}_{\bar{\mathrm{r}}}(\hat{\Gamma}_2) = \pi'(\Gamma_2')$, and an isomorphism $\lambda = \mathrm{Fr}^{-1} \circ \mu_p \circ \mathrm{Fr} : \hat{\Gamma}_1 \to \hat{\Gamma}_2$. By Corollary 1.16, we can virtually extend λ to a virtual automorphism Λ of H. Then $\Lambda_p' = \mathrm{Fr} \circ \Lambda \circ \mathrm{Fr}^{-1}$ is a virtual automorphism of H_p' virtually extending μ_p.

Let $\tilde{\Lambda}_p = \Lambda_p' \times \Psi$, so $\tilde{\Lambda}_p$ is a virtual automorphism of H_p. We can define a map ζ on some finite index subgroup of Γ_1 by $\zeta(\gamma) = \lambda_p(\gamma)\tilde{\Lambda}_p(\gamma)^{-1}$. By Lemma 2.1, ζ virtually extends to $\hat{\zeta} : H_p \to Z(H_p)$. Then $\Lambda_p = \tilde{\Lambda}_p\zeta$ is a virtual endomorphism of H_p. Since $\ker(\zeta) \supset [H_p, H_p]$ we conclude (much as in the proof of Corollary 1.12) that Λ_p is a virtual automorphism. It is easy to see that it virtually extends λ_p. □

ACKNOWLEDGMENTS

The authors would like to thank the University of Bielefeld (Germany), the Isaac Newton Institute for Mathematical Sciences (Cambridge, U.K.), the University of Virginia, and Oklahoma State University for their hospitality. Most of this research was carried out during productive visits to these institutions. The authors would also like to thank Gopal Prasad for pointing out an error in a previous version of the manuscript. Financial support was provided by the German-Israeli Foundation for Research and Development and the National Science Foundation (DMS-9801136).

REFERENCES

1. Borel, A. *Linear Algebraic Groups*, 2nd Ed.; Springer-Verlag: New York, 1991.
2. Borel, A.; Springer, T.A. Rationality Properties of Linear Algebraic Groups II. Tôhoku Math. J. **1968**, *20* (2), 443–497.

3. Malcev, A.I. On a Class of Homogeneous Spaces. Amer. Math. Soc. Transl. **1951**, *1951* (39), 1–33; translated from Izv. Akad. Nauk SSSR Ser. Mat. **1949**, *13*, 9–32.
4. Margulis, G.A. *Discrete Subgroups of Semisimple Lie Groups*; Springer-Verlag: New York, 1991.
5. Mostow, G.D. *Strong Rigidity of Locally Symmetric Spaces*; Princeton University Press: Princeton, NJ, 1973.
6. Raghunathan, M.S. *Discrete Subgroups of Lie Groups*; Springer-Verlag: New York, 1972.
7. Starkov, A.N. Rigidity Problem for Lattices in Solvable Lie Groups. Proc. Indian Acad. Sci. Math. Sci. **1994**, *104*, 495–514.
8. Venkataramana, T.N. On Superrigidity and Arithmeticity of Lattices in Semisimple Groups over Local Fields of Arbitrary Characteristic. Invent. Math. **1988**, *92*, 255–306.
9. Weil, A. *Basic Number Theory*; Springer-Verlag: New York, 1967.
10. Witte, D. Superrigidity of Lattices in Solvable Lie Groups. Invent. Math. **1995**, *122*, 147–193.

Received December 2000
Revised May 2001