Rigidity of some characteristic-p nillattices

Dave Witte

Department of Mathematics
Oklahoma State University
Stillwater, OK 74078

(joint work in progress with Lucy Lifschitz)

Outline.

- Rigidity: an example and the definition
- Lattices in unipotent $\mathbb{R}$-groups are rigid
- Totally disconnected local fields $\mathbb{Q}_p$, $\mathbb{F}_p((t))$
- Lattices in t.d. abelian groups are rigid
- Facts about lattices in unipotent $\mathbb{R}$-groups
- A rigid lattice in a 2D unipotent group
- A rigid lattice in a Heisenberg group

• Rigidity: an example and the definition

Eg. $\mathrm{Aut}(\mathbb{Z}^n) = \mathrm{GL}(n, \mathbb{Z})$

$\Rightarrow$ every automorphism of $\mathbb{Z}^n$ extends to $\mathbb{R}^n$

$\Rightarrow$ $\mathbb{Z}^n$ is *rigid* in $\mathbb{R}^n$ (or "automorphism rigid").

Defn. Γ = subgroup of (locally cpct) group G.

Γ is *rigid* if

every automorphism ϕ of Γ virtually extends to a continuous virtual automorphism $\hat{\phi}$ of G.

- $\hat{\phi}$ *virtually extends* ϕ if
  $\exists$ finite-index subgroup Γ' of Γ,
  such that $\hat{\phi}|_{\Gamma'} = \phi|_{\Gamma'}$.
- $\hat{\phi}$ is a *virtual automorphism* of G if
  $\exists$ fin-ind closed subgrps G_1, G_2 of G,
  such that $\hat{\phi}\colon G_1 \cong G_2$.

Defn. Γ is a *lattice* in G if

- Γ is a discrete subgroup of G and
- G/Γ is compact.

Eg. G = simply connected, **abelian** Lie group

$\Rightarrow$ Γ is rigid.

• Lattices in unipotent $\mathbb{R}$-groups are rigid

Eg. $G = U_{4\times 4}(\mathbb{R}) = \begin{pmatrix} 1 & \mathbb{R} & \mathbb{R} & \mathbb{R} \\ 0 & 1 & \mathbb{R} & \mathbb{R} \\ 0 & 0 & 1 & \mathbb{R} \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Defn. Unipotent group = subgroup of $U_{n\times n}(\mathbb{R})$ that is connected and (Zariski) closed.

Eg. $\begin{pmatrix} 1 & 0 & \mathbb{R} & \mathbb{R} \\ 0 & 1 & \mathbb{R} & \mathbb{R} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & \mathbb{R} & \mathbb{R} & \mathbb{R} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$,

$\begin{pmatrix} 1 & s & t & u \\ 0 & 1 & s & t \\ 0 & 0 & 1 & s \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & t & t^2/2 & t^3/6 \\ 0 & 1 & t & t^2/2 \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Zariski: def'd by *polynomial* eqns in mat entries.

Fact. *Any closed, connected subgroup of* $U_{n\times n}(\mathbb{R})$ *is Zariski closed.*

Eg. $\begin{pmatrix} 1 & t & 0 \\ 0 & 1 & 0 \\ 0 & 0 & e^t \end{pmatrix}$ is **not** Zariski closed.

Prop. *G = unipotent $\mathbb{R}$-group $\subset U_{n\times n}(\mathbb{R})$.*
Polynomials defining G have all coeffs in $\mathbb{Q}$
$\Leftrightarrow G \cap U_{n\times n}(\mathbb{Z})$ *= lattice in G.*

Thm (Malcev, 1951). *G = unipotent $\mathbb{R}$-group*
$\Rightarrow \Gamma$ *is rigid.*
In fact, ϕ extends to a unique automorphism of G.

[By induction on $\dim G$: start with $Z(G)$ (abel).]

G = solvable $\mathbb{R}$-group $\not\Rightarrow \Gamma$ is rigid.
A thorough study was made by Starkov.

G = (semi)simple $\mathbb{R}$-group $\Rightarrow \Gamma$ is rigid
"Mostow Rigidity Thm"
except when $G \approx \mathrm{SL}(2,\mathbb{R})$
(if we assume the center of G is trivial).
[Mostow, (Margulis, Prasad)]

Superrigidity deals with extending homomorphisms, instead of only isomorphisms.

- Semisimple: Margulis, (Bass-Milnor-Serre, Raghunathan, Corlette)
- Solvable: Witte, (Saito, Gorbacevic)

• Totally disconnected local fields $\mathbb{Q}_p$, $\mathbb{F}_p((t))$

Fix a prime p.

$$\mathbb{Q}_p = \left\{ \sum_{i=n}^{\infty} a_i p^i \;\middle|\; \begin{array}{c} a_i \in \{0, 1, 2, \ldots, p-1\} \\ n \in \mathbb{Z} \end{array} \right\}.$$

This is a field (usual power series ops, plus carries).

$(\mathbb{Q}_p, d_p)$ is a metric space (complete, t.d., loc cpct)
and the field operations are continuous.

Eg. $1, p, p^2, p^3, \ldots \to 0$
and $1, p^{-1}, p^{-2}, p^{-3}, \ldots \to \infty$.

Defn. For $a = \sum_{i=n}^{\infty} a_i p^i \in \mathbb{Q}_p$,

- define $|a|_p = p^{-n}$ if $a_n \neq 0$; and
- $d_p(a, b) = |a - b|_p$.

Eg. unipotent $\mathbb{Q}_p$-group

$$U_{4\times 4}(\mathbb{Q}_p) = \begin{pmatrix} 1 & \mathbb{Q}_p & \mathbb{Q}_p & \mathbb{Q}_p \\ 0 & 1 & \mathbb{Q}_p & \mathbb{Q}_p \\ 0 & 0 & 1 & \mathbb{Q}_p \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Fact. *G = unipotent $\mathbb{Q}_p$-group $\Rightarrow \nexists\ \Gamma$ (lattice).*

Proof. In fact, the only discrete subgroup is e.

Let Γ be a discrete subgrp of $(\mathbb{Q}_p, +) \cong U_{2\times 2}(\mathbb{Q}_p)$.

For $\gamma \in \Gamma$, we have $\gamma, p\gamma, p^2\gamma, \ldots \to 0$.

Γ discrete $\Rightarrow p^n\gamma = 0$ for some n.

$\mathbb{Q}_p$ is a field $\Rightarrow \gamma = 0$.

So $\Gamma = \{0\}$. ∎

Fix a prime p. Let $\mathbf{F} = \mathbb{F}_p((T))$

$$= \left\{ \sum_{i=n}^{\infty} a_i T^i \;\middle|\; \begin{array}{c} a_i \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \\ n \in \mathbb{Z} \end{array} \right\}.$$

This is a field (under usual power series operations — there are no carries).

$\mathbf{F}$ has characteristic p.

$(\mathbf{F}, d)$ is a metric space (complete, t.d., loc cpct) and the field operations are continuous.

Eg. $1, T, T^2, T^3, \ldots \to 0$ and $1, T^{-1}, T^{-2}, T^{-3}, \ldots \to \infty$.

Defn. For $a = \sum_{i=n}^{\infty} a_i T^i \in \mathbf{F}$,

- define $|a| = p^{-n}$ if $a_n \neq 0$; and
- $d(a,b) = |a - b|$.

Eg. unipotent $\mathbf{F}$-group

$$U_{4\times 4}(\mathbf{F}) = \begin{pmatrix} 1 & \mathbf{F} & \mathbf{F} & \mathbf{F} \\ 0 & 1 & \mathbf{F} & \mathbf{F} \\ 0 & 0 & 1 & \mathbf{F} \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Eg. Unipotent $\mathbf{F}$-groups can have lattices.

- $\mathbf{F}^+ = \left\{ \sum_{i=1}^{\infty} a_i T^i \right\}$ and
- $\mathbf{F}^- = \left\{ \sum_{i=-n}^{0} a_i T^i \right\}$.

Then $\mathbf{F}^-$ is discrete ($d(a,b) = p^{\geq 0} \geq 1$).

We have $\mathbf{F} = \mathbf{F}^+ + \mathbf{F}^-$ and $\mathbf{F}^+$ is compact,
so $\mathbf{F}/\mathbf{F}^-$ is compact.

Eg. $U_{n\times n}(\mathbf{F}^-)$ is a lattice in $U_{n\times n}(\mathbf{F})$.
(“S-arithmetic”)

Rem. A discrete subgroup Γ of $\mathbf{F}$ is a lattice
$\Leftrightarrow$ for all large n, $\exists \gamma \in \Gamma$, s.t. $|x|_p = p^n$.

• Lattices in t.d. abelian groups are rigid

Prop. *G = totally disconn, abelian $\Rightarrow \Gamma$ is rigid.*

Proof. Γ discrete $\Rightarrow \exists$ nbhd $\mathcal{O}$ of e, s.t. $\Gamma \cap \mathcal{O} = e$.
G t.d. $\Rightarrow \exists$ cpct, open subgrp K of G,
s.t. $K \subset \mathcal{O}$.

Let $G' = K \times \Gamma \subset G$.

Define $\hat{\phi}\colon G' \to G'$ by
$$\hat{\phi}(k, \gamma) = \bigl(k, \phi(\gamma)\bigr).$$

Then $\hat{\phi}$ extends ϕ
and is a virtual automorphism of G.

- G/Γ cpct, $\Gamma \subset G' \Rightarrow G/G'$ cpct.
- $K \subset G' \Rightarrow G'$ open $\Rightarrow G/G'$ discrete.

So G/G' is finite. (I.e., G' has finite index in G.)

• Facts about lattices in unipotent $\mathbb{R}$-groups

Assume $G =$ unipotent $\mathbb{R}$-group.

Prop. *$Z(\Gamma)$ is a lattice in $Z(G)$.*

Same is true over $\mathbf{F}$ instead of $\mathbb{R}$
(if Γ is Zariski dense).

Prop. *$\hat{\phi}: G_1 \to G_2$ is a homomorphism,*
$\Rightarrow \hat{\phi}$ is a polynomial and
$\hat{\phi}(G_1)$ is (almost) Zariski closed in G_2.

Not true over $\mathbf{F}$.

Eg. $\{\,\text{poly autos of } \mathbf{F}\,\} = \{\, x \mapsto \alpha x \mid \alpha \in \mathbf{F}^{\times}\,\}$,
so $\mathbf{F}$ has only one poly auto that fixes 1.
But unctbly many autos of $\mathbf{F}^{-} \cong (\mathbb{F}_p)^{\infty}$ fix 1.

Eg. Define $\hat{\phi}: \mathbf{F} \to \mathbf{F}$ by $\hat{\phi}(x) = x^p$.
Then $\hat{\phi}(\mathbf{F}) = \sum_{i=n}^{\infty} a_i T^{pi}$ (all exp's mult of p)
is Zariski dense in $\mathbf{F}$, but is not open.

Prop. *$[\Gamma, \Gamma]$ is a lattice in $[G, G]$.*

Question. *Is this true over $\mathbf{F}$?*

• A rigid lattice in a 2D unipotent group

Let

- $\langle s,t\rangle = \begin{pmatrix} 1 & s^p & t \\ 0 & 1 & s \\ 0 & 0 & 1 \end{pmatrix}$
- $G = \{\, \langle s,t\rangle \mid s,t \in \mathbf{F} \,\}$, and
- $\Gamma = \{\, \langle s,t\rangle \mid s,t \in \mathbf{F}^- \,\}$.

So Γ is a lattice in G.

Thm (Lifschitz-Witte). Γ *is rigid in* G.

(We expect to show finite-index subgroups of Γ are also rigid, but the proof is not quite complete.)

We have

- $\langle s_1,t_1\rangle\langle s_2,t_2\rangle = \langle s_1+s_2, t_1+t_2+s_1^p s_2\rangle$; and
- $[\langle s_1,\cdot\rangle, \langle s_2,\cdot\rangle] = \langle 0, [\![s_1,s_2]\!]\rangle$,
  where $[\![x,y]\!] = x^p y - x y^p$.

Defn. Define $\phi^*, \phi_* \colon \mathbf{F}^- \to \mathbf{F}^-$ by

$$\phi(\langle s,t\rangle) = \big\langle \phi^*(s), \phi_*(t) + \varepsilon(s) \big\rangle.$$

Then $[\![\phi^*(s_1), \phi^*(s_2)]\!] = \phi_*([\![s_1,s_2]\!])$.

Note that $\mathbf{F}^- = \mathbb{F}_p[T^{-1}]$ is a polynomial ring.

Lem. $\dim_{\mathbb{F}_p} \dfrac{[\![\mathbf{F}^-, \mathbf{F}^-]\!]}{[\![a, \mathbf{F}^-]\!] + [\![b, \mathbf{F}^-]\!]} < \infty$
$\Leftrightarrow b \in a\mathbf{F}^p \setminus \mathbb{F}_p.$

Proof. ($\Leftarrow$) $\exists\ u, v \in \mathbf{F}^-$, such that $au^p = bv^p$.
For $r \in \mathbf{F}^-$, we have

$$\begin{aligned}
&[\![a, ur]\!] - [\![b, vr]\!] \\
&\qquad = (a^p ur - au^p r^p) - (b^p vr - bv^p r^p) \\
&\qquad = (a^p ur - b^p vr) - (au^p r^p - bv^p r^p) \\
&\qquad = (a^p u - b^p v)r - 0.
\end{aligned}$$

So $[\![a, \mathbf{F}^-]\!] + [\![b, \mathbf{F}^-]\!] \ni$ el't of any large degree. ■

For future reference:

Cor (of proof). $(T^{-p^2} - T^{-1})\mathbf{F}^- \subset [\![(\mathbf{F}^-)^p, \mathbf{F}^-]\!]$.

Proof. $a = T^{-p}$, $b = 1$, $u = 1$, $v = T^{-1}$
$\Rightarrow a^p u - b^p v = T^{-p^2} - T^{-1}$. ■

Defn. $a \in \mathbf{F}^-$ is *separable* if a is not divisible by any nonconstant pth power.

Cor. *$a \in \mathbf{F}^-$ separable $\Rightarrow \exists$ separable $b \in \mathbf{F}^-$, such that $\phi^*\big(a(\mathbf{F}^-)^p\big) = b(\mathbf{F}^-)^p$.*

Proof. For $a, b \in \mathbf{F}^- \setminus \{0\}$, define $a \equiv b \Leftrightarrow b \in a\mathbf{F}^p$.

Lemma: $a \equiv b \Leftrightarrow \phi^*(a) \equiv \phi^*(b)$.

Each equiv class is $c(\mathbf{F}^-)^p$, for sep'ble $c \in \mathbf{F}^-$. ∎

Prop. *$a \in \mathbf{F}^-$ separable $\Rightarrow$*

$$\dim_{\mathbb{F}_p} \frac{[\![\mathbf{F}^-, \mathbf{F}^-]\!]}{[\![a(\mathbf{F}^-)^p, \mathbf{F}^-]\!]} = (p-1)(\deg^- a) + Q,$$

where $Q = \#$ irreducible quadratic factors of a.

Cor. $[\![a(\mathbf{F}^-)^p, \mathbf{F}^-]\!] = [\![\mathbf{F}^-, \mathbf{F}^-]\!] \Leftrightarrow a \in \mathbb{F}_p \setminus 0$.

Cor. $\phi^*\big((\mathbf{F}^-)^p\big) = (\mathbf{F}^-)^p$.

In fact, $\phi^*\big((\mathbf{F}^-)^{p^n}\big) = (\mathbf{F}^-)^{p^n}$ for each n.

Cor. $\phi^*(\mathbb{F}_p) = \mathbb{F}_p$.

Proof. $\mathbb{F}_p = \bigcap_{n=0}^{\infty} (\mathbf{F}^-)^{p^n}$. ∎

Cor. $\phi^*(\text{separable}) = \text{separable}.$

Proof. Restrict attention to

$$\phi^*|_{a(\mathbf{F}^-)^p} \colon a(\mathbf{F}^-)^p \to b(\mathbf{F}^-)^p. \quad \blacksquare$$

Cor. $\deg^- \phi^*(a) = \deg^- a$ *for all* $a \in \mathbf{F}^-$.

Proof. Suffices to prove for a separable
(with no quadratic factors).
Proposition: $\deg^- \phi^*(a) \le \deg^- a$.
By induction on $\deg^- a$, must have equality. $\blacksquare$

Lem. $[\![a(\mathbf{F}^-)^p, \mathbf{F}^-]\!] + [\![b(\mathbf{F}^-)^p, \mathbf{F}^-]\!] = [\![\mathbf{F}^-, \mathbf{F}^-]\!]$
$\Leftrightarrow \gcd(a, b) = 1.$

Proof. Generalization of first corollary. $\blacksquare$

Cor. $\gcd(a, b) = 1 \Leftrightarrow \gcd\big(\phi^*(a), \phi^*(b)\big) = 1.$

We may assume $\phi^*(a) = a$ whenever $\deg^- a \le 1$.
(Compose with $\lambda\big(a(T)\big) = \alpha a(\beta T + \gamma)\big)\big)$.
Show, by induction on $\deg^- a$, that $\phi^* = \mathrm{Id}$. $\blacksquare$

Prop. *$a \in \mathbf{F}^-$ separable $\Rightarrow$*

$$\dim_{\mathbb{F}_p} \frac{[\![\mathbf{F}^-, \mathbf{F}^-]\!]}{[\![a(\mathbf{F}^-)^p, \mathbf{F}^-]\!]} = (p-1)(\deg^- a) + Q,$$

where Q = # irreducible quadratic factors of a.

Proof. For simplicity, assume $a = 1$.

We wish to show $[\![(\mathbf{F}^-)^p, \mathbf{F}^-]\!] = [\![\mathbf{F}^-, \mathbf{F}^-]\!]$.

Recall that $(T^{-p^2} - T^{-1})\mathbf{F}^- \subset [\![(\mathbf{F}^-)^p, \mathbf{F}^-]\!]$, so we may work in the quotient ring

$$\overline{R} = \mathbf{F}^-/(T^{-p^2} - T^{-1})\mathbf{F}^-.$$

Chinese Remainder Theorem:

$$\overline{R} \cong \bigoplus_{f | T^{-p^2} - T^{-1}} \frac{\mathbf{F}^-}{f\mathbf{F}^-}$$

$$\cong (\mathbb{F}_p)^p \oplus (\mathbb{F}_{p^2})^{p(p-1)/2}$$

since $T^{-p^2} - T^{-1} = \prod\{\text{irred polys of deg} \leq 2\}$.

We have

- $[\![\mathbb{F}_p, \mathbb{F}_p]\!] = 0 = [\![1, \mathbb{F}_p]\!]$ and
- $[\![\mathbb{F}_{p^2}, \mathbb{F}_{p^2}]\!] = \mathbb{F}_p = [\![1, \mathbb{F}_{p^2}]\!]$,

so

$$[\![\overline{R}, \overline{R}]\!] = [\![1, \overline{R}]\!] = [\![\overline{R}^p, \overline{R}]\!]. \blacksquare$$

• A rigid lattice in a Heisenberg group

Thm (Lifschitz-Witte). $G = U_{3\times 3}(\mathbf{F})$
$\Rightarrow U_{3\times 3}(\mathbf{F}^-)$ *is rigid in* G*.*

Question. *Is* Γ *essentially the only lattice in* G*?*

I.e., given a lattice Γ' of G,
is there always a virtual automorphism ψ of G,
such that $\psi(\Gamma)$ is virtually Γ'?

Problem. *Suppose* V *is a lattice in* $\mathbf{F}$*,*
such that xV *is virtually* V*, for each* $x \in V$*.*
Is V *virtually a subring of* $\mathbf{F}$*?*

References

• V. V. Gorbacevič: Generalized Ljapunov Theorem on Mal'cev manifolds, *Math. USSR-Sb.* 23 (1974) 155–168.

• A. I. Malcev, On a class of homogeneous spaces, *Amer. Math. Soc. Transl.* No. 39 (1951) = 9 (1962) 276–307.

• G. A. Margulis, *Discrete Subgroups of Semisimple Lie Groups*, Springer-Verlag, New York, 1991.

• G. D. Mostow: *Strong Rigidity of Locally Symmetric Spaces*, Princeton University Press, Princeton, 1973.

• M. S. Raghunathan, *Discrete Subgroups of Lie Groups,* Springer-Verlag (New York) 1972.

• M. Saito, Sur certains groupes de Lie résolubles II, *Sci. Papers Coll. Gen. Ed. Tokyo* 7 (1957) 157–168.

• A. N. Starkov, Rigidity problem for lattices in solvable Lie groups, *Proc. Indian Acad. Sci. (Math. Sci.)* 4 (1994) 495–514.

• D. Witte, Superrigidity of lattices in solvable Lie groups, *Inventiones Math.* 122 (1995) 147-193.