Publ. Math. Debrecen
51 / 1-2 (1997), 43–47

Uniqueness of roots in $\ell^1(\Gamma, \mathbb{N}_0)$ over lattices in simply connected nilpotent Lie groups

By DANIEL NEUENSCHWANDER (Lausanne)

Abstract. We show that roots (if they exist) in $\ell^1(\Gamma, \mathbb{N}_0)$ over lattices Γ in certain simply connected nilpotent Lie groups are uniquely determined.

1. Introduction and statement of the result

Let G be a simply connected nilpotent Lie group, which will be identified with its Lie algebra $\mathcal{G} \cong \mathbb{R}^d$. Consider the adjoint reperesentation of the Lie algebra given by $ad(x) : \mathcal{G} \to \mathcal{G}$, $ad(x)(y) := [x, y]$ $(x, y \in \mathcal{G})$. The product on G is then given by the Campbell-Hausdorff formula, (c.f. Serre (1965)), where only the terms up to order, say, $r \in \mathbb{N}_0$ (the step of nilpotency of G) arise:

$$x \cdot y = \sum_{n=1}^{r} z_n, \tag{1}$$

$$z_n = \frac{1}{n} \sum_{p+q=n} (z'_{p,q} + z''_{p,q}), \tag{2}$$

$$z'_{p,q} = \sum_{\substack{p_1+p_2+\ldots+p_m=p \\ q_1+q_2+\ldots+q_{m-1}=q-1 \\ p_i+q_i \geq 1 \\ p_m \geq 1}} \frac{(-1)^{m+1}}{m} \frac{ad(x)^{p_1} ad(y)^{q_1} \ldots ad(x)^{p_m}(y)}{p_1! q_1! \ldots p_m!}, \tag{3}$$

Mathematics Subject Classification: 16U30, 20C07, 22E25, 22E40 (primary), 43A10 (secondary).
Key words and phrases: Simply connected nilpotent Lie groups, lattices in groups, roots in rings, measure algebras.

$$(4)\quad z''_{p,q} = \sum_{\substack{p_1+p_2+\ldots+p_{m-1}=p-1 \\ q_1+q_2+\ldots+q_{m-1}=q \\ p_i+q_i\geq 1}} \frac{(-1)^{m+1}}{m} \frac{ad(x)^{p_1} ad(y)^{q_1} \ldots ad(y)^{q_{m-1}}(x)}{p_1! q_1! \ldots q_{m-1}!}.$$

The first few terms are

$$(5)\qquad x \cdot y = x + y + \frac{1}{2}[x,y] + \frac{1}{12}\{[[x,y],y] + [[y,x],x]\} + \ldots .$$

Clearly, $e = 0$ and $x^{-1} = -x$ ($x \in G$). Consider an adapted vector space decomposition of $G = \mathcal{G}$, i.e.

$$(6)\qquad G \cong \mathcal{G} \cong \mathbb{R}^d \cong \bigoplus_{i=1}^{r} V_i$$

such that

$$\bigoplus_{i=k}^{r} V_i = \mathcal{G}_{k-1},$$

where $\{\mathcal{G}_k\}_{0\leq k\leq r}$ is the *descending central series*:

$$\mathcal{G}_0 := \mathcal{G}, \quad \mathcal{G}_{k+1} := [\mathcal{G}, \mathcal{G}_k]$$

(and thus $\mathcal{G}_r = \{0\}$). In this case, one can take a *Jordan-Hölder basis* for $\mathcal{G} \cong \mathbb{R}^d$, i.e. a basis $E = \bigcup_{i=1}^r E_i$ where $E_i = \{e_{i,1}, e_{i,2}, \ldots, e_{i,d(i)}\}$ is a basis of V_i ($d(i)$ thus being the dimension of V_i). Let $R(r)$ be the least common multiple of the denominators of the coefficients occurring in the Campbell-Hausdorff formula with terms up to order r (so $R(1) = 1$, $R(2) = 2, R(3) = 12, \ldots$). Assume all entries in the matrices describing $[\,.\,,\,.\,]$ are rational. Let D be the least common multiple of all denominators of these constants. Consider the lattice

$$(7)\qquad \Gamma := \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{d(i)} \mathbb{Z} e'_{i,j} \subset \mathcal{G} \cong G$$

(where $e'_{i,j} := (1/(DR(i)))e_{i,j}$), which is evidently a subgroup of G. The most prominent example is the Heisenberg group $\mathbb{H}$ given as $\mathbb{H} = \mathbb{R}^3$ equipped with the multiplication $x \cdot y = x + y + \frac{1}{2}[x,y]$ and $[x,y] = (0, 0, x'y'' - y'x'')$ for $x = (x', x'', x''')$, $y = (y', y'', y''') \in \mathbb{R}^3$ and the subgroup $\Gamma = \mathbb{Z} \times \mathbb{Z} \times \frac{1}{2}\mathbb{Z}$. Write $\{e'_{i,j}\} =: \{e_1, e_2, \ldots, e_d\}$. Consider the set $\ell^1(\Gamma, \mathbb{N}_0)$ of summable $\mathbb{N}_0$-valued functions on Γ with convolution as multiplication. The algebras $\ell^1(\Gamma, \mathbb{Z}_p)$ (where $\mathbb{Z}_p$ denotes the field of integers modulo a prime p) are defined analgously. We show that roots in $\ell^1(\Gamma, \mathbb{N}_0)$ (if they exist) are uniquely determined:

Theorem 1. *Let G be a simply connected nilpotent Lie group such that in the matrices determining $[\,.\,,\,.\,]$ all entries are rational. Let Γ be the lattice (7) and assume $\lambda, \eta \in \ell^1(\Gamma, \mathbb{N}_0), m \in \mathbb{N}$. If $\lambda^m = \eta^m$ then it follows that $\lambda = \eta$.*

The theory of lattices in simply connected nilpotent Lie groups and its history is exhaustively treated in RAGHUNATHAN (1972). See in particular MAL'CEV's (1951) paper.

2. The proof

The proof of Theorem 1 is to a great extent parallel to the proof of the uniqueness property of certain Poisson convolution semigroups of probability measures on simply connected nilpotent Lie groups in NEUENSCHWANDER (1995). Another major ingredient will be the Vandermonde determinant.

Let p be a prime.

Lemma 1. *A $\mathbb{Z}_p$-valued sequence $\mu = \{\mu_0, \mu_1, \dots, \mu_{p-1}\}$ is uniquely determined by its moments in $\mathbb{Z}_p$*

$$M_k = \sum_{j=0}^{p-1} j^k \mu_j \in \mathbb{Z}_p \quad (0 \le k \le p-1).$$

We have that

$$(M_0, M_1, \dots, M_{p-1}) = (\mu_0, \mu_1, \dots, \mu_{p-1}) \cdot A,$$

where $A = (a_{i,j})_{0 \le i,j \le p-1}$ is the matrix (over $\mathbb{Z}_p$) given by

$$a_{i,j} = i^j \quad (i, j \in \mathbb{Z}^p).$$

The submatrix of A which we get by eliminating the first line and the first column is a Vandermonde matrix over $\mathbb{Z}_p$, so

$$\det A = \prod_{1 \le i < j \le p-1} (j - i) \ne 0,$$

hence the assertion.

In the sequel, we will interpret $\mu \in \ell^1(\Gamma, \mathbb{Z}_p)$ as a "$\mathbb{Z}_p$-valued probability measure" on Γ and use the language of probability measures, which seems more elegant in this context. In particular, we will work with "random variables" obeying to a certain "distribution", "independence", and we will write $E(\dots)$ for the "expectation". The carrying over of these notions from the classical situation is straightforward. Put $\Gamma \ni x =: \sum_{i=1}^{d} x_i e_i$. For $\mu \in \ell^1(\Gamma, \mathbb{Z}_p)$, $\beta = (\beta_1, \beta_2, \dots, \beta_d) \in \mathbb{Z}_p^d$, $h = (h_1, h_2, \dots, h_d) \in \mathbb{N}_0^d$, define the "mixed moments"

$$M_h^{(\beta)}(\mu) = \sum_{x \in \Gamma} (\beta_j x_j)^{h_j} \mu_x.$$

Let $H(\mu) = M_0^{(\beta)}(\mu) = \sum_{x \in \Gamma} \mu_x$. Consider on $\mathbb{N}_0^d$ the lexicographic ordering from behind defined by

$$\begin{aligned} &(a_1, a_2, \dots, a_d) < (b_1, b_2, \dots, b_d) \\ \iff &(a_d, a_{d-1}, \dots, a_{d-j+1}) = (b_d, b_{d-1}, \dots, b_{d-j+1}), a_{d-j} < b_{d-j} \\ &\text{for some} \quad j \in \mathbb{N}_0. \end{aligned}$$

Lemma 2. *Assume $m < p$ and $\mu, \nu \in \ell^1(\Gamma, \mathbb{Z}_p)$ satisfying $\mu = \nu^m$. Suppose $H(\mu) \neq 0$. Then the $M_\ell^{(\beta)}(\nu)$ ($\beta \in \mathbb{Z}_p^d, \ell \in \mathbb{N}_0^d$) may be calculated (exactly in case m is odd and up to the sign in case m even) out of the $M_\ell^{(\beta)}(\mu)$ recursively with respect to ℓ.*

Proof. Assume $X_1, X_2, \dots, X_m$ are "i.i.d." Γ-valued random variables with $\mathcal{L}(X_1) = \nu$. Write

$$M_\ell^{(\beta)}(\mu) = E\left(\prod_{j=1}^{d}\left(\beta_j\left(\prod_{i=1}^{m} X_i\right)_j\right)^{\ell_j}\right). \tag{8}$$

By the adaptedness, we get, by multiplying out the product in (8),

$$\left(\beta_j\left(\prod_{i=1}^{m} X_i\right)_j\right)^{\ell_j} = \sum_{i=1}^{m} (\beta_j (X_i)_j)^{\ell_j} + P_j, \tag{9}$$

P_j being a polynomial in $(X_1)_1, (X_2)_1, \dots, (X_m)_1, (X_1)_2, (X_2)_2, \dots, (X_m)_2, \dots\dots, (X_1)_j, (X_2)_j, \dots, (X_m)_j$, where in every monomial the exponents of $(X_1)_j, (X_2)_j, \dots, (X_m)_j$ are strictly smaller than ℓ_j. Now, by multiplying out the product $\prod_{j=1}^{d} (\dots)^{\ell_j}$ in (8), we get by (9)

$$\prod_{j=1}^{d} (\dots)^{\ell_j} = \sum_{i=1}^{d} \prod_{j=1}^{d} (\beta_j (X_i)_j)^{\ell_j} + P,$$

where P is a polynomial in $(X_1)_1, (X_2)_1, \dots, (X_m)_1, (X_1)_2, (X_2)_2, \dots, (X_m)_2, \dots\dots, (X_1)_d, (X_2)_d, \dots, (X_m)_d$ such that for every monomial

$\gamma \prod_{i=1}^m \prod_{j=1}^d (\beta_j(X_i)_j)^{r_j}$ we have $(r_1, r_2, \dots r_d), (s_1, s_2, \dots, s_d) < \ell$. Now the assertion follows from the independence of the X_i, the fact that $E(\prod_{j=1}^d (\beta_j(X_i)_j)^{\ell_j})$ is equal for every i, and the relation $H(\mu) = H(\nu)^m$. □

Now we may prove our theorem:

Proof of Theorem 1. W.l.o.g. we may assume that $K(\mu) = \sum_{x\in\Gamma} \mu_x > 0$. Let $p > \max\{m, 2, K(\mu)\}$ be a prime and consider the quotient group

$$\Gamma_p := \bigoplus_{i=1}^{d} \mathbb{Z}_p e_i \tag{10}$$

of Γ. Denote by $\pi_p : \Gamma \to \Gamma_p$ and $\tau_p : \mathbb{Z} \to \mathbb{Z}_p$ the canonical projections and let, for $\mu \in \ell^1(\Gamma, \mathbb{Z})$, $\mu^{(p)} \in \ell^1(\Gamma, \mathbb{Z}_p)$ be defined by $\mu_x^{(p)} := \sum \tau_p(\mu(\pi_p^{-1}(x)))$ $(x \in \Gamma)$. Then $(\lambda^{(p)})^m = (\eta^{(p)})^m$. By Lemmas 1 and 2 it follows that $\lambda^{(p)} = \eta^{(p)}$.

2. Now for $\mu = \{\mu_{1,-\frac{p-1}{2}}, \mu_{1,-\frac{p-1}{2}+1}, \dots, \mu_{1,\frac{p-1}{2}}, \mu_{2,-\frac{p-1}{2}}, \mu_{2,-\frac{p-1}{2}+1}, \dots, \mu_{2,\frac{p-1}{2}}, \dots \mu_{d,-\frac{p-1}{2}}, \mu_{d,-\frac{p-1}{2}+1}, \dots, \mu_{d,\frac{p-1}{2}}\} \in \ell^1(\Gamma_p, \mathbb{Z}_p)$ let $q_p(\mu)$ be the "same" (formally) $\mathbb{Z}$-valued sequence over the index set $\bigoplus_{i=1}^d \{-\frac{p-1}{2}, -\frac{p-1}{2}+1, \dots, \frac{p-1}{2}\} e_i \subset \Gamma$. Clearly, we have $q_p(\mu^{(p)})_x \to \mu_x$ $(p \to \infty)$ for every $x \in \Gamma$, hence by 1. it follows also that $\lambda = \eta$.

Acknowledgement. The author would like to thank the anonymous referee for his important remarks.

References

[1] A. I. Mal'cev, On a class of homogeneous spaces, *Amer. Math. Soc. Transl.* **39** (1951).
[2] D. Neuenschwander, On the uniqueness problem for continuous convolution semigroups of probability measures on simply connected nilpotent Lie groups, (1997), (*preprint*).
[3] M. S. Raghunathan, Discrete subgroups of Lie groups, *Springer*, *Berlin*, 1972.
[4] J.-P. Serre, Lie algebras and Lie groups, *Benjamin*, *New York*, 1965.

UNIVERSITÉ DE LAUSANNE
ECOLE DES HAUTES ETUDES COMMERCIALES
INSTITUT DE SCIENCES ACTUARIELLES
CH–1015 LAUSANNE
SWITZERLAND
PHONE +41 32 323 60 75.

(Received March 4, 1996; revised October 29, 1996)