Math. Z. 212, 631–636 (1993)

Mathematische Zeitschrift

On infinitely divisible measures on certain finitely generated groups

S.G. Dani* and Riddhi Shah*

Sonderforschungsbereich 170, Mathematisches Institut, Bunsenstrasse 3–5, W-3400 Göttingen, Germany

Received July 12, 1991; in final form July 7, 1992

Let G be a locally compact (Hausdorff) group and let $M^1(G)$ be the topological semigroup of probability measures with convolution product and the weak topology. A $\mu \in M^1(G)$ is said to be infinitely divisible if for each natural number n, μ has an n-th root in $M^1(G)$ and it is said to be embeddable if there exists a continuous semigroup homomorphism ϕ: $\mathbf{R}_+ \to M^1(G)$, from the semigroup $\mathbf{R}_+$ of nonegative real numbers, such that $\phi(1)=\mu$. An embeddable measure is evidently infinitely divisible but the converse is not true in general. Over the last three decades various classes of groups have been identified for which the converse is indeed true; in this case one says that the group has the embedding property. We refer the reader to [H] for an account of results in this regard until mid seventies and [DM 3, Sh] and other literature cited therein, for more recent developments.

While a large class of connected Lie groups is now known to have the embedding property, relatively little is known in this direction for discrete groups. Finite groups and finitely generated nilpotent groups are known to have the embedding property (cf. [H]). Also, McCrudden proved that any polycyclic group has the embedding property (cf. [M 2]). The property can also be deduced for certain discrete subgroups of connected Lie groups from the results on the ambient group. Nevertheless, by and large the problem is open for discrete groups.

In this paper we prove the embedding property for any finitely generated group which can be realised as a subgroup of $GL(n, \mathbf{A})$, where $\mathbf{A}$ is the field of algebraic numbers (see Main Theorem for a somewhat stronger assertion); here the group need not be discrete as a subgroup of $GL(n, \mathbf{C})$, but will be considered equipped with the discrete topology. This implies in particular the embedding property of the classes of discrete groups mentioned above (cf. Remark 1).

By a result of Martin Löf an embeddable measure on a discrete group is a Poisson measure; viz. it is of the form $\exp \nu$, where ν is a (signed) measure of the form $\lambda - \|\lambda\| \omega_K$ for some bounded positive measure λ commuting with

* *Current address:* School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay 400005, India

ω_K, the latter being the normalised Haar measure of some finite subgroup K such that $\lambda(K)=0$ (cf. [H]). In view of this, we can formulate our result in the following stronger form.

Main Theorem. *Let Γ be a finitely generated group equipped with the discrete topology. Let* $\mathbf{A}$ *be the field of algebraic numbers and suppose that there exists an (abstract) homomorphism $\phi: \Gamma \to \mathrm{GL}(n, \mathbf{A})$ such that* $\ker \phi$ *is a finitely generated central subgroup of Γ. Then every infinitely divisible measure on Γ is a Poisson measure.*

We view $\phi(\Gamma)$ as above as a discrete subgroup of a product of matrix groups over certain local fields and deduce the theorem using a sufficient condition for 'shift embeddability' together with some results, from [DM1–DM3] and [Sh], about relative compactness of certain sets of roots, in the case of real and p-adic groups respectively.

1 Preliminaries

Let G be a locally compact group and let $\mu \in M^1(G)$. We denote by $C(\mu)$ the smallest closed subgroup of G containing $\operatorname{supp}\mu$, the support of μ. We denote by $N(\mu, G)$ and $Z(\mu, G)$ the normaliser and centraliser respectively of $C(\mu)$ in G.

For any closed subgroup H of a locally compact group we identify $M^1(H)$ as a subsemigroup of $M^1(G)$ in the cannonical way, extending $\mu \in M^1(H)$ to G by setting $\mu(G-H)=0$. For $\mu \in M^1(H)$ and a subset M of $\mathbf{N}$ let

$$R(M, \mu, H)=\{v^k \mid v \in M^1(H), v^m=\mu \text{ for some } m \in M, m \geqq k\}.$$

In the case when $M=\mathbf{N}$ the above set, namely $R(\mathbf{N}, \mu, H)$, is called the 'root set' of μ on H; μ is said to be *root compact on* H if the root set of μ on H is relatively compact.

For any $\mu \in M^1(G)$, as above, any root of μ is supported on $N(\mu, G)$; in fact if λ is an n-th root then there exists a $g \in N(\mu, G)$ such that $g^n \in C(\mu)$ and $\operatorname{supp}\lambda \subset gC(\mu)$ (cf. [M1, Lemma 1]). In particular any infinitely divisible measure μ on G is infinitely divisible on $N(\mu, G)$. We next note the following observation, which will be used in the sequel.

Lemma 1.1 *Let G be any locally compact group and $\mu \in M^1(G)$ be infinitely divisible. Let H be a closed normal subgroup of $N(\mu, G)$ containing $C(\mu)$. Suppose there exists a $k \in \mathbf{N}$ such that any element of $N(\mu, G)/H$ which is of finite order is of order at most k. Then μ is infinitely divisible on H.*

Proof. Let η: $N(\mu, G) \to N(\mu, G)/H$ be the natural projection. Let k be as in the hypothesis and $m=k!$. Let $n \in \mathbf{N}$ be arbitrary. Since μ is infinitely divisible there exists a $\lambda \in M^1(G)$ which is an (mn)-th root of μ. Then λ is supported on a coset $aC(\mu)$ where $a \in N(\mu, G)$ and $a^{mn} \in C(\mu)$. Since $C(\mu) \subset H$, $\eta(a)^{mn}=e$, the identity in $N(\mu, G)/H$. By hypothesis this implies that the order of $\eta(a)$ is at most k and hence $\eta(a)^m=e$. Therefore $a^m \in H$. This implies that λ^m, which is an n-th root of μ, is supported on H. Thus for all n there exists an n-th root of μ supported on H, which means that μ is infinitely divisible on H.

Now let K be a locally compact field of characteristic 0. Then K is either $\mathbf{R}$ or $\mathbf{C}$ or a finite extension of the field $\mathbf{Q}_p$ of p-adic numbers, for some prime

p (cf. [We, p. 11, Theorem 5]); we set $c(K)=0$ if $K=\mathbf{R}$ or $\mathbf{C}$ and $c(K)=p$ if K is a finite extension of $\mathbf{Q}_p$. We define a sequence $\{N_i(K)\}$ of subsets of $\mathbf{N}$ (sets of natural numbers) by setting, for all i,

$$N_i(K)=\mathbf{N} \quad \text{if } c(K)=0 \quad \text{and}$$
$$=\{m\in\mathbf{N} \mid p^i \nmid m\}, \quad \text{if } c(K)=p.$$

Let $\tilde{G}$ be an algebraic group defined over K and let G_K be the group of all K-rational points of $\tilde{G}$, equipped with the locally compact topology as a matrix group over K.

The following result is essentially known.

Theorem 1.2 *Let the notation be as above. Let $\mu\in M^1(G_K)$ be such that $Z(\mu, G_K)$ is the center of G_K. Then $R(N_i, \mu, G_K)$ is relatively compact for all i.*

Proof. For $K=\mathbf{R}$ or $\mathbf{C}$ under the above hypothesis μ is in fact root compact. This is implied by Theorem 1.1 of [DM2] together with Proposition 4.4 of [DM1] provided G_K is connected; in general G_K has only finitely many connected components (cf. [BT, Corollaire 14.5]) and the proof still goes through. In the desired general from the result has been noted, together with a somewhat simpler proof, in [DM3].

If K is nonarchimedean, then G_K is a p-adic algebraic group; where $p=c(K)$, and in this case the theorem is only a slight variation of Proposition 3 of [Sh]; the proof is the same beyond the first sentence there.

2 The embedding property

Let Γ be a finitely generated discrete group and let ϕ: $\Gamma\to \mathrm{GL}(n, \mathbf{A})$ be any (abstract) homomorphism, where $n\in\mathbf{N}$ and $\mathbf{A}$ is the field of algebraic numbers. Then $\phi(\Gamma)$ is finitely generated and hence there exists a number field (that is, a finite extension of $\mathbf{Q}$) F such that $\phi(\Gamma)$ is contained in $\mathrm{GL}(n, F)$. Let $\mathscr{A}$ be the set of absolute values on F and for any $v\in\mathscr{A}$ let F_v be the corresponding completion of F. We shall consider F_v and $\mathrm{GL}(n, F_v)$, for any $n\in\mathbf{N}$, to be equipped with the locally compact topology given by the absolute value v. Also for any $v\in\mathscr{A}$ let j_v: $\mathrm{GL}(n, F)\to\mathrm{GL}(n, F_v)$ be the cannonical inclusion homomorphism. Since Γ is finitely generated it follows that $\overline{j_v(\phi(\Gamma))}$, the closure of $j_v(\phi(\Gamma))$ in $\mathrm{GL}(n, F_v)$, is compact for all but finitely many v; if $\{\gamma_1, \ldots, \gamma_k\}$ is a set of generators of $\phi(\Gamma)$ then for all but finitely many $v\in\mathscr{A}$ all the entries of $j_v(\gamma_1), \ldots, j_v(\gamma_k)$ as well as those of $j_v(\gamma_1)^{-1}, \ldots, j_v(\gamma_k)^{-1}$ are of absolute value at most 1 (cf. [We, p. 72, Proposition 2]) and for any v for which this holds $j_v(\phi(\Gamma))$ is contained in a compact subgroup.

Let S be the finite set consisting of all v such that $\overline{j_v(\phi(\Gamma))}$ is noncompact. Let

$$G=\prod_{v\in S}\mathrm{GL}(n, F_v)$$

equipped with the product topology. For each $v\in S$ let π_v: $G\to\mathrm{GL}(n, F_v)$ be the projection homomorphism onto $\mathrm{GL}(n, F_v)$. Let j: $\mathrm{GL}(n, F)\to G$ be the canonical homomorphism such that $\pi_v(j(x))=j_v(x)$ for all $x\in\mathrm{GL}(n, F)$ and $v\in S$ and let ψ: $\Gamma\to G$ be the homomorphism defined by $\psi(\gamma)=j(\phi(\gamma))$ for all $\gamma\in\Gamma$.

We recall that $\mathrm{GL}(n, F)$ is a discrete subgroup of the idele group of $M(n, F)$, the latter being the algebra of $n \times n$ matrices over F (see pp. 71–72 of [We] for reference). Since $\overline{j_v(\phi(\Gamma))}$ is compact for all $v \notin S$, this implies that $\psi(\Gamma)$ is a discrete subgroup of G.

Now let $\mu \in M^1(\Gamma)$ be any infinitely divisible measure. Let $\Gamma^*(\mu)$ be the Zariski closure of $\phi(C(\mu))$ in $\mathrm{GL}(n)$. Since $\phi(\Gamma) \subset \mathrm{GL}(n, F)$, $\Gamma^*(\mu)$ is defined over F (cf. [B, Proposition 1.3]). Let $\Gamma_F^*(\mu)$ be the group of F-rational points of $\Gamma^*(\mu)$ and let Δ be the subgroup of G defined by

$$\Delta = j(\Gamma_F^*(\mu)) \cap \psi(\Gamma).$$

Our first step in proving the theorem is the following:

Proposition 2.1 *μ is infinitely divisible on $\psi^{-1}(\Delta)$.*

Proof. Let $N(\mu)$ and $N^*(\mu)$ be the normalisers of $\phi(C(\mu))$ and $\Gamma_F^*(\mu)$ in $\mathrm{GL}(n, F)$. Since $\Gamma^*(\mu)$ is the smallest algebraic subgroup of $\mathrm{GL}(n)$ containing $\phi(C(\mu))$, it follows that $N(\mu) \subset N^*(\mu)$. Also clearly $\phi(N(\mu, \Gamma)) \subset N(\mu)$. We next note that $N^*(\mu)/\Gamma_F^*(\mu)$ can be realised as a subgroup of an algebraic group defined over F (cf. [B, Theorem 6.8]) and hence as a subgroup of $\mathrm{GL}(m, F)$ for some $m \in \mathbf{N}$. This implies in particular that there is a bound on the orders of finite subgroups of $N^*(\mu)/\Gamma_F^*(\mu)$ (cf. [Se, p. LG 4.35, Theorem 1]). Since $\phi(N(\mu, \Gamma)) \subset N(\mu) \subset N^*(\mu)$, we get further that the orders of finite subgroups of $N(\mu, \Gamma)/\phi^{-1}(\Gamma_F^*(\mu)) \cap N(\mu, \Gamma)$ are bounded. Therefore Lemma 1.1 implies that μ is infinitely divisible on $\phi^{-1}(\Gamma_F^*(\mu))$, which clearly is the same as $\psi^{-1}(\Delta)$.

We realise each F_v, $v \in S$, as a subfield of $\mathbf{C}$ via some embeddings, that will be considered fixed, and correspondingly view $\mathrm{GL}(n, F_v)$ as subgroups of $\mathrm{GL}(n, \mathbf{C})$.

Now for each $v \in S$ let $\Gamma_v^*(\mu)$ denote the group of F_v-rational points of $\Gamma^*(\mu)$ and let

$$G^*(\mu) = \prod_{v \in S} \Gamma_v^*(\mu) \subset G.$$

Clearly, $j(\Gamma_F^*(\mu))$ is a (not necessarily discrete) subgroup of $G^*(\mu)$. In particular $G^*(\mu)$ contains Δ, which is a discrete subgroup containing $C(\psi(\mu))$. Since, by Proposition 2.1, μ is infinitely divisible on $\psi^{-1}(\Delta)$ it follows that $\psi(\mu)$ is infinitely divisible on Δ and hence on $G^*(\mu)$.

Now for each $v \in S$ let $\{N_i(F_v)\}$ be the sequence of subsets of $\mathbf{N}$ as in § 1, associated to the locally compact field F_v. For each $i \in \mathbf{N}$ put

$$N_i = \bigcap_{v \in S} N_i(F_v).$$

We observe the following.

Proposition 2.2 *For all $i \in \mathbf{N}$, $R(N_i, \psi(\mu), G^*(\mu))$ is a relatively compact subset of $M^1(G^*(\mu))$.*

Proof. It is enough to prove that for each $v \in S$ and $i \in \mathbf{N}$, $\pi_v(R(N_i, \psi(\mu), G^*(\mu)))$ is a relatively compact subset of $M^1(\Gamma_v^*(\mu))$. Observe that

$$\pi_v(R(N_i, \psi(\mu), G^*(\mu))) \subset R(N_i, \pi_v(\psi(\mu)), \Gamma_v^*(\mu)) \subset R(N_i(F_v), \pi_v(\psi(\mu)), \Gamma_v^*(\mu))$$

for all $v \in S$ and $i \in \mathbf{N}$. The proposition would therefore follow from Theorem 1.2 if we show that, for all $v \in S$, $Z(\pi_v(\psi(\mu)), \Gamma_v^*(\mu))$ is the center of $\Gamma_v^*(\mu)$. Let $v \in S$ be given. Observe that $\pi_v(C(\psi(\mu))) = j_v(\phi(C(\mu)))$. Since $\phi(C(\mu))$ is Zariski-dense in $\Gamma^*(\mu)$, the centraliser of $j_v(\phi(C(\mu)))$ in $\Gamma^*(\mu)$ is contained in the center of $\Gamma^*(\mu)$. Since $Z(\pi_v(\psi(\mu)), \Gamma_v^*(\mu))$ is the centraliser in $\Gamma_v^*(\mu)$ of the the subgroup $C(\pi_v(\psi(\mu)))$ and since the latter contains $\pi_v(C(\psi(\mu)))$, the preceding assertion implies that the centraliser is contained in the center of $\Gamma^*(\mu)$ and hence in the center of $\Gamma_v^*(\mu)$. This proves the proposition.

Proof of the Main Theorem. Since $\psi(\Gamma)$ is a closed subgroup of G, Proposition 2.2 implies in particular that $R(N_i, \psi(\mu), \psi(\Gamma))$ is relatively compact for all i. Since $\ker \psi = \ker \phi$ is a finitely generated central subgroup of Γ, it is strongly root compact (cf. [H, Theorem 3.1.17 or 3.1.12]). By Lemma 2 of [Sh] these two conclusions imply that $R(N_i, \mu, \Gamma)$ is relatively compact in $M^1(\Gamma)$ for all i. An argument as in the proof of Theorem 3 of [Sh], using in particular the criterion for shift embeddability, now shows that there exists a continuous homomorphism $f: \mathbf{R}_+ \to M^1(\Gamma)$ and a homomorphism $\alpha: \mathbf{Q} \to \Gamma$ such that $\mu = \alpha(1) f(1)$.

For any $v \in S$ such that F_v is a finite extension of Q_p, p a prime, Lemma 4 of [Sh] shows that $\operatorname{Im} \pi_v \circ \psi \circ \alpha$ is contained in a closed subgroup of $\Gamma_v^*(\mu)$ topologically isomorphic to $\mathbf{Q}_p^{n_p}$ for some $n_p \in \mathbf{N}$. In real (or complex) algebraic groups any abelian subgroup has a subgroup of finite index contained in a closed subgroup isomorphic to $\mathbf{T}^a \times \mathbf{R}^b$ for some $a, b \geqq 0$. Combining these observations and noting that $\mathbf{Q}$ has no proper subgroup of finite index we deduce that $\psi(\alpha(\mathbf{Q}))$ is contained in a closed subgroup of G topologically isomorphic to $\mathbf{T}^a \times \mathbf{R}^b \times \mathbf{Q}_{p_1}^{n_1} \times \ldots \times \mathbf{Q}_{p_l}^{n_l}$ for some primes $p_1, \ldots, p_l$ and $a, b, n_1, \ldots, n_l \geqq 0$. We note that the latter group has no nontrivial divisible discrete subgroups; this follows from the fact if x is any element of the group and p is a prime such that $p \neq p_i$ for any i then the set $\{y \mid y^m = x \text{ for some } m = p^k, k \in \mathbf{N}\}$ is relatively compact. Since $\psi(\alpha(\mathbf{Q}))$ is contained in $\psi(\Gamma)$, it is discrete; further it is also divisible and hence we are led to the conclusion that $\psi \circ \alpha$ is a trivial homomorphism. Therefore $\alpha(\mathbf{Q})$ is contained in $\ker \psi = \ker \phi$. Since by hypothesis $\ker \phi$ is a finitely generated abelian group, this further implies that α is trivial. Thus we get that $\mu = f(1)$ where $f: \mathbf{R}_+ \to M^1(\Gamma)$ is a continuous homomorphism. In other words, μ is embeddable. This proves the theorem.

Remarks. 1. The theorem implies in particular the embeddability of infinitely divisible probability measures on finite groups, finitely generated nilpotent groups and more generally the polycyclic groups, which was known earlier (cf. [H] and [M2]); these groups can be realised as subgroups of $\mathrm{GL}(n, \mathbf{A})$; (see [W, §2.1 and Theorem 2.5]). There are also other abstract conditions on groups which ensure embeddability of a group as a subgroup of $\mathrm{GL}(n, \mathbf{A})$. We refer the reader to a discussion on pp. 25–26 of [W] in this regard.

2. Arguing as in the above proof and using the fact that for each prime p and $n \in \mathbf{N}$, there is a bound on the order of finite subgroups of $\mathrm{GL}(n, \mathbf{Q}_p)$, one can also prove the following: If Γ is any discrete subgroup of $\prod_{i=1}^{l} \mathrm{GL}(n, \mathbf{Q}_{p_i})$ for some l, $n \in \mathbf{N}$ and primes $p_1, \ldots, p_l$ then every infinitely divisible measure on Γ is a Poisson measure.

Acknowledgement. The authors would like to thank the Sonderforschungsbereich 170, "Geometrie und Analysis", Göttingen, and Professor Denker in particular, for hospitality while this work was done.

References

[B] Borel, A.: Linear Algebraic Groups. New York: Benjamin 1969

[BT] Borel, A., Tits, J.: Groupes reductifs. Publ. Math., Inst. Hautes Étud. Sci. **27**, 55–150 (1965)

[DM1] Dani, S.G., McCrudden, M.: Factors, roots and embeddability of measures on Lie groups. Math. Z. **199**, 369–385 (1988)

[DM2] Dani, S.G., McCrudden, M.: On the factor sets of measures and local tightness of convolution semigroups over Lie groups. J. Theor. Probab. **1**, 357–370 (1988)

[DM3] Dani, S.G., McCrudden, M.: Embeddability of infinitely divisible distributions on linear Lie groups. Invent. Math. **110**, 237–261 (1992)

[H] Heyer, H.: Probability Measures on Locally Compact Groups. Berlin Heidelberg New York: Springer 1977

[M1] McCrudden, M.: Infinitely divisible probabilities on SL(2, **C**) are continuously embedded. Math. Proc. Camb. Philos. Soc. **92**, 101–107 (1982)

[M2] McCrudden, M.: Infinitely divisible probabilities on polycyclic group are Poisson (unpublished Manuscript)

[Se] Serre, J.-P.: Lie Algebras and Lie Groups. New York: Benjamin 1964

[Sh] Riddhi Shah: Infinitely divisible measures on p-adic groups. J. Theor. Probab. **4**, 391–405 (1991)

[W] Wehrfritz, B.A.F.: Infinite Linear Groups. Berlin Heidelberg New York: Springer 1972

[We] Weil, A.: Basic Number Theory, 2nd ed. Berlin Heidelberg New York: Springer 1973