Proc. Indian Acad. Sci. (Math. Sci.) Vol. 117, No. 4, November 2007, pp. 443–455.
© Printed in India

Explicit representation of roots on p-adic solenoids and non-uniqueness of embeddability into rational one-parameter subgroups

PETER BECKER-KERN

Fachbereich Mathematik, Universität Dortmund, 44221 Dortmund, Germany
E-mail: pbk@math.uni-dortmund.de

MS received 9 October 2006

Abstract. This note generalizes known results concerning the existence of roots and embedding one-parameter subgroups on p-adic solenoids. An explicit representation of the roots leads to the construction of two distinct rational embedding one-parameter subgroups. The results contribute to enlighten the group structure of solenoids and to point out difficulties arising in the context of the embedding problem in probability theory. As a consequence, the uniqueness of embedding of infinitely divisible probability measures on p-adic solenoids is solved under a certain natural condition.

Keywords. Solenoid; root multiplicity; infinite divisibility; one-parameter subgroup; embedding problem; convolution semigroup; uniqueness of embedding.

1. Introduction

Given a prime number p let S_p denote the p-adic solenoid, i.e. the subgroup of the infinite-dimensional torus representable as

$$S_p = \{y = (y_0, y_1, y_2, \dots) \in \mathbb{T}^{\mathbb{N}} \colon y_j = y_{j+1}^p \text{ for all } j \in \mathbb{Z}_+\},$$

where $\mathbb{T} = \{\mathrm{e}^{it} \colon t \in [0, 2\pi)\}$ is the usual torus group. Due to the Tychonov theorem S_p is a compact Abelian topological group. Solenoids are one of the prototypes of compact groups that are connected but not arc-wise connected. For elementary facts about p-adic solenoids we refer to the monographs [12], [13] and [16]. For each $n \in \mathbb{Z}_+$ the shift-operator $K_n \colon S_p \to S_p$ defined as $K_n(y_0, y_1, y_2, \dots) = (y_n, y_{n+1}, y_{n+2}, \dots)$ is a continuous automorphism of S_p, serving as a p^n-th root, since $K_n(y)^{p^n} = y$ for all $y \in S_p$. Further, let $\theta \colon \mathbb{R} \to S_p$ be given by $\theta(x) = (\mathrm{e}^{ix}, \mathrm{e}^{ix/p}, \mathrm{e}^{ix/p^2}, \dots)$, which defines a continuous homomorphism. Its image $\theta(\mathbb{R}) = S_p^{\mathrm{arc}}$ is the arc-component, a dense, arc-wise connected subgroup of S_p. This fact is responsible for the notion of a solenoidal group (see Definition (9.2) of [12]). The arc-component is the union of all images of possible continuous one-parameter subgroups. Namely, for $y = \theta(x) \in S_p^{\mathrm{arc}}$ we have the continuous one-parameter subgroup $\big(\phi_\alpha(y) = \theta(\alpha x)\big)_{\alpha \in \mathbb{R}}$, i.e. $\phi_\alpha \cdot \phi_\beta = \phi_{\alpha+\beta}$ for all $\alpha, \beta \in \mathbb{R}$ and $\alpha \mapsto \phi_\alpha$ is continuous. Hence $\theta(x/n) = \phi_{1/n}(y)$ serves as an n-th root on the dense subgroup S_p^{arc} and any $y = \phi_1(y) \in S_p^{\mathrm{arc}}$ is embeddable into a continuous one-parameter subgroup. But even for $y \in S_p \setminus S_p^{\mathrm{arc}}$ it is well-known that roots of arbitrary order exist. Since S_p is connected and compact, Mycielski [20] first states (without proof) that the existence

of roots is an easy consequence of a general approximation of compact groups by Lie groups. The explicit arguments were provided in a more general (probabilistic) context by Carnal [7] and are given below. General proofs for the fact that on compact (Abelian) groups connectedness is equivalent to divisibility e.g., can be found in Theorem (24.25) of [12], Corollary 1 to Theorem 31 of [19], or for the non-Abelian case in Theorem 9.35 of [16].

This research was originally motivated by probabilistic questions. The existence of roots and embedding one-parameter subgroups have probabilistic counterparts in the question of infinite divisibility of a probability measure and the embedding problem. The remaining part of this Introduction is about the probabilistic impact to the group theoretic questions. In the last decade solenoids have drawn attention as relevant examples on various fields of probability theory (see [1–4]).

A probability measure μ on a locally compact group G is said to be *infinitely divisible* if for every $n \in \mathbb{N}$ there exists a probability measure μ_n on G such that its n-fold convolution power ${\mu_n}^{*n}$ coincides with μ. The existence of roots of arbitrary order of an element $x \in G$ is thus equivalent to the infinite divisibility of the Dirac measure δ_x. Further, μ is called *weakly infinitely divisible* if for every $n \in \mathbb{N}$ there exists a probability measure μ_n on G and an element $x_n \in G$ such that $\mu = {\mu_n}^{*n} * \delta_{x_n}$. These notions play an important role for limit theorems in probability theory (see for e.g. [22] and [13]). Clearly, for Abelian groups, both definitions coincide in case Dirac measures are infinitely divisible. Now the existence of n-th roots on $G = S_p$ can, for example, be derived from necessary and sufficient conditions for infinite divisibility, as follows. As a compact group, S_p is a Lie projective group (for the definition see for e.g., p. 12 of [13]) for the definition. Namely, let $H_n = \{y \in S_p \colon y_j = 1 \text{ for all } j = 0, \ldots, n-1\}$.Then $(H_n)_{n\in\mathbb{N}}$ builds a descending family of compact normal subgroups of S_p with $\bigcap_{n\in\mathbb{N}} H_n = \{e = (1, 1, \ldots)\}$ and factors

$$\begin{aligned} G_n &= S_p/H_n \\ &\cong \{y = (y_0, \ldots, y_{n-1}) \in \mathbb{T}^n \colon y_j = y_{j+1}^p \text{ for all } j = 0, \ldots, n-2\} \cong \mathbb{T} \end{aligned}$$

such that the projective limit of the Lie groups $(G_n)_{n\in\mathbb{N}}$ coincides with S_p. Since obviously the Dirac measures on $G_n \cong \mathbb{T}$ are infinitely divisible, it follows from Hilfssatz 1.2 of [7] that all Dirac measures on S_p are infinitely divisible. Hence the well-known existence of roots of arbitrary order for every $y \in S_p$ follows. This is also a consequence of Satz 1.1 in [9] but both proofs rely on compactness arguments and hence are general existence results without being constructive. The same is true for the above-mentioned general group theoretic proofs, which show the equivalence of connectedness and divisibility for compact (Abelian) groups. Among other things the infinite divisibility of Dirac measures on S_p shows that the characterization of weakly infinitely divisible probability measures on S_p in [1] is in fact a characterization of all infinitely divisible probability measures. Beyond their existence, we will prove an explicit representation of the roots on S_p in §2, which also gives their multiplicity. The proof relies on solving a number theoretic problem, for which the author is not aware of an existing solution in the mathematical literature.

An infinitely divisible probability measure μ on G is said to be *rationally embeddable* if there exists a one-parameter (convolution) semigroup $(\mu_q)_{q\in\mathbb{Q}_+}$ of probability measures on G with $\mu = \mu_1$. Further, μ is called *continuously embeddable* if there exists a continuous one-parameter semigroup $(\mu_t)_{t\geq 0}$ of probability measures on G with $\mu = \mu_1$. Clearly, for Dirac measures $\mu = \delta_x$ with $x \in G$, rational, respectively continuous embeddability is

equivalent to the existence of a rational one-parameter subgroup $(\phi_q)_{q\in\mathbb{Q}}$, respectively a continuous one-parameter subgroup $(\phi_\alpha)_{\alpha\in\mathbb{R}}$ in G such that $\phi_1 = x$. The locally compact group G is said to have the *embedding property* if every infinitely divisible probability measure is continuously embeddable. The *embedding problem*, originated by Parthasarathy [21] (for compact groups, see also [23]), is known as the problem of characterizing the locally compact groups admitting the embedding property. We refer to Chapter III of [13] and the survey articles of Heyer [14, 15] and McCrudden [17, 18] for an overview of the (recent) developments and open problems concerning the embedding problem. In fact, the p-adic solenoid $G = S_p$ is known as an example of a locally compact group not having the embedding property, since any Dirac measure $\mu = \delta_y$ with $y \in S_p \setminus S_p^{\mathrm{arc}}$ is not continuously embeddable. In this sense, as an example of Dixmier [8], the p-adic solenoid is what is called *indecent* (in Definition 3.5 of [18]) to the embedding property. But every Dirac measure is rationally embeddable by Satz 11 of Böge [6], since the p-adic solenoid as a compact group is strongly root compact (see Definition 3.1 of [18]) by Theorem 3.10 together with Example 3.11 of [18]. Root compactness is decisive for rational embeddability. In general, for Abelian groups it is only possible to show a weaker *submonogeneous embedding* as in Hazod and Schmetterer [10]; see also [13]. Whereas the submonogeneous embedding is constructive, again Böge's result in [6] only shows the existence of a rational one-parameter embedding subgroup for any $y \in S_p$. The explicit representation of roots in §2 enables us to show in §3 that for any $y \in S_p$ the rational embedding is not unique, whereas for $y \in S_p^{\mathrm{arc}}$ the above continuous embedding is. As a further consequence, we show that an infinitely divisible probability measure μ on S_p with $\mu(S_p^{\mathrm{arc}}) = 1$ is uniquely embeddable into a continuous convolution semigroup. For problems concerning the uniqueness of embedding we refer to the comments in Chapter 2.6 of [11]. The non-unique rational embedding of Dirac measures on S_p has simple consequences to the embedding problem. It is known by Theorem 6.1 of [23] that a translate of an arbitrary infinitely divisible probability measure μ on S_p is embeddable into a continuous convolution semigroup $(\nu_t)_{t\geq 0}$, i.e. $\mu = \nu_1 * \delta_x$ for some $x \in S_p$. Hence our result in §3 shows the non-uniqueness of rational embedding one-parameter semigroups for any infinitely divisible probability measure on S_p. In particular, for Gaussian measures $\gamma * \omega_C * \delta_x$ in the sense of Parthasarathy [22], where γ is a symmetric Gaussian and ω_C is the Haar probability measure on some compact subgroup $C \subseteq S_p$, in case $x \in S_p \setminus S_p^{\mathrm{arc}}$ we do not have continuous embeddability, and in any case we have non-unique rational Gaussian embedding semigroups. These play an important role in [1–4].

2. Construction of roots

The following explicit construction of roots is based on the simple fact that any $y = (y_0, y_1, y_2, \dots) \in S_p$ can be represented as

$$y_d = \exp\left[i \left(t + 2\pi \sum_{\ell=1}^{d} k_\ell p^{\ell-1} \right) \Big/ p^d \right] \tag{2.1}$$

for all $d \in \mathbb{Z}_+$ and some unique $t \in [0, 2\pi)$ and $k_\ell \in \{0, \dots, p-1\}$, $\ell \in \mathbb{N}$. For each $n \in \mathbb{N}$, let $\Delta_n(y) = \{z \in S_p : z^n = y\}$ denote the set of n-th roots of $y \in S_p$.

Theorem 2.1. *For any $n \in \mathbb{N}$, any $y \in S_p$ has root multiplicity $|\Delta_n(y)| = l$, where $l \in \mathbb{N}$ is such that $n = lp^k$ with $k \in \mathbb{Z}_+$ and* $\gcd(l, p) = 1$.

For the proof assume $z = (z_0, z_1, z_2, \dots) \in \Delta_n(y)$. Using (2.1) we get for all $d \in \mathbb{Z}_+$,

$$z_d = \exp\left[i \left(t + 2\pi \sum_{\ell=1}^{d} k_\ell p^{\ell-1} \right) \Big/ (np^d) + 2\pi i \, \frac{m_d}{n} \right] \tag{2.2}$$

for some $m_d \in \{0, \dots, n-1\}$. Since $z \in S_p$, we further have $z_{d+1}^p = z_d$ and hence for all $d \in \mathbb{Z}_+$ we get

$$z_{d+1} = \exp\left[i \left(t + 2\pi \sum_{\ell=1}^{d} k_\ell p^{\ell-1} \right) \Big/ (np^{d+1}) + 2\pi i \, \frac{m_d}{np} + 2\pi i \, \frac{q_{d+1}}{p} \right] \tag{2.3}$$

for some $q_{d+1} \in \{0, \dots, p-1\}$. Comparing z_{d+1} in (2.2) and (2.3) yields

$$\frac{m_d}{np} + \frac{q_{d+1}}{p} = \frac{k_{d+1}}{np} + \frac{m_{d+1}}{n} + r_d$$

for some $r_d \in \mathbb{Z}$. We have $np \cdot r_d = m_d + nq_{d+1} - k_{d+1} - pm_{d+1} \le n - 1 + n(p-1) < np$ and $np \cdot r_d \ge -(p-1) - p(n-1) > -np$. Thus $r_d = 0$ for all $d \in \mathbb{Z}_+$ and we arrive at

$$k_{d+1} = m_d - pm_{d+1} + nq_{d+1} \quad \text{for all } d \in \mathbb{Z}_+. \tag{2.4}$$

Now it is sufficient to prove that for any $n \in \mathbb{N}$, given $y \in S_p$ with the corresponding sequence $(k_d)_{d\in\mathbb{N}} \in \{0, \dots, p-1\}^{\mathbb{N}}$, we can choose exactly $|\Delta_n(y)|$ different sequences $(m_d)_{d\in\mathbb{Z}_+} \in \{0, \dots, n-1\}^{\mathbb{N}}$ and the accompanying sequences $(q_d)_{d\in\mathbb{N}} \in \{0, \dots, p-1\}^{\mathbb{N}}$ such that (2.4) holds. For different representations of n this number theoretic problem will be subsequently solved by the following lemmas which also show how to choose $(m_d)_{d\in\mathbb{Z}_+}$ explicitly given $(k_d)_{d\in\mathbb{N}}$. Hence by (2.2) we have an explicit though inconvenient representation of the roots belonging to $\Delta_n(y)$. However, it enables us to construct at least two distinct rational embedding one-parameter subgroups in the next section, showing non-uniqueness of rational embeddability. We start with n being a positive integer power of p for which it might already be obvious that we have uniqueness of n-th roots due to the structure of the p-adic solenoid.

Lemma 2.2. *If $n = p^k$ for some $k \in \mathbb{N}$, given any sequence $(k_d)_{d\in\mathbb{N}} \in \{0, \dots, p-1\}^{\mathbb{N}}$, there exist unique sequences $(m_d)_{d\in\mathbb{Z}_+} \in \{0, \dots, n-1\}^{\mathbb{N}}$ and $(q_d)_{d\in\mathbb{N}} \in \{0, \dots, p-1\}^{\mathbb{N}}$ such that* (2.4) *holds.*

Proof. The assertion follows by induction. For $k = 1$, simply observe that due to $-pm_{d+1} + nq_{d+1}$ being an integer multiple of p and both m_d and k_{d+1} belonging to $\{0, \dots, p-1\}$, by (2.4) we must have $m_d = k_{d+1}$ and $q_{d+1} = m_{d+1}$ for all $d \in \mathbb{Z}_+$. Now assume that the assertion is true for all $m \le k \in \mathbb{N}$. Equivalent to a solution of (2.4), let $z_{(k)}$, $z \in S_p$ be the unique solutions of ${z_{(k)}}^{p^k} = y$ and $z^p = z_{(k)}$, respectively. Clearly, we have $z^{p^{k+1}} = y$. Assume $\tilde{z} \in S_p$ such that $\tilde{z}^{p^{k+1}} = y$. Then both $z^p = z_{(k)}$ and $\tilde{z}^p$ belong to $\Delta_{p^k}(y)$ so that by assumption we have $z^p = \tilde{z}^p$ and thus $z = \tilde{z}$ due to the uniqueness of roots of order p^m with $m \le k$. □

Note that for the unique p^n-th root we already know about the simple explicit representation $z = K_n(y) \in \Delta_{p^n}(y)$ using the shift operator.

Lemma 2.3. *Let* $n = lp$ *with* $l \in \mathbb{N}\setminus\{1\}$ *and* $\gcd(l, p) = 1$. *Then for any sequence* $(k_d)_{d\in\mathbb{N}} \in \{0, \dots, p-1\}^{\mathbb{N}}$ *there exist exactly* l *sequences* $(m_d)_{d\in\mathbb{Z}_+} \in \{0, \dots, n-1\}^{\mathbb{N}}$ *and for each of these a unique sequence* $(q_d)_{d\in\mathbb{N}} \in \{0, \dots, p-1\}^{\mathbb{N}}$ *such that* (2.4) *holds.*

Proof. The solutions of (2.4) for a fixed $d \in \mathbb{Z}_+$ can be taken from table 1. According to this, given k_1 the choices of m_0 are determined by $k_1 = m_0 (\mathrm{mod}\, p)$ for which we have

Table 1. Solutions of (2.4) for $n = lp$.

k_{d+1}	=	m_d	− p	m_{d+1}	+ n	q_{d+1}
0		0		0		0
⋮		⋮		⋮		⋮
$p-1$		$p-1$		0		0
0		p		1		0
⋮		⋮		⋮		⋮
$p-1$		$2p-1$		1		0
			⋮			
0		$(l-1)p$		$l-1$		0
⋮		⋮		⋮		⋮
$p-1$		$lp-1=n-1$		$l-1$		0
0		0		l		1
⋮		⋮		⋮		⋮
$p-1$		$p-1$		l		1
			⋮			
0		$(l-1)p$		$2l-1$		1
⋮		⋮		⋮		⋮
$p-1$		$lp-1=n-1$		$2l-1$		1
			⋮			
			⋮			
0		0		$(p-1)l$		$p-1$
⋮		⋮		⋮		⋮
$p-1$		$p-1$		$(p-1)l$		$p-1$
			⋮			
0		$(l-1)p$		$pl-1=n-1$		$p-1$
⋮		⋮		⋮		⋮
$p-1$		$lp-1=n-1$		$pl-1=n-1$		$p-1$

exactly l possibilities. Fixing one of these, say $m_0 = k_1 + r_0 p$ for some $r_0 \in \{0, \ldots, l-1\}$, this uniquely determines m_1 by $m_1 (\mathrm{mod}\, l) = r_0$ and $m_1 (\mathrm{mod}\, p) = k_2$, since $m_1 \in \{0, \ldots, n-1 = lp-1\}$ and $\gcd(l, p) = 1$. This further uniquely determines q_1 by (2.4). Inductively, m_{d+1} and q_{d+1} are uniquely determined by k_{d+2} and m_d, respectively by (2.4). □

Lemma 2.4. *Let $n = lp^k$ with $k \in \mathbb{N}$, $l \in \mathbb{N} \setminus \{1\}$ and* $\gcd(l, p) = 1$. *Then the assertion of Lemma* 2.3 *holds true.*

Proof. Again, this follows by induction. For $k = 1$ the result follows from Lemma 2.3. Assume that the assertion is true for some $k \in \mathbb{N}$. Equivalent to a solution of (2.4), let $\{z_{(1)}, \ldots, z_{(l)}\} = \Delta_{lp^k}(y)$ and let $\widetilde{z_{(i)}}$ be the unique solution by Lemma 2.2 of $\widetilde{z_{(i)}}^p = z_{(i)}$ for $i = 1, \ldots, l$. Clearly, we have $\widetilde{z_{(i)}} \neq \widetilde{z_{(j)}}$ for $i \neq j$ and $\widetilde{z_{(i)}}^{lp^{k+1}} = y$ for any $i = 1, \ldots, l$. Assume $\tilde{z} \in S_p$ such that $\tilde{z}^{lp^{k+1}} = y$. Then $\tilde{z}^p$ belongs to $\Delta_{lp^k}(y)$ and hence there exists $i_0 \in \{1, \ldots, l\}$ such that $\tilde{z}^p = z_{(i_0)}$. It follows that $\tilde{z} = \widetilde{z_{(i_0)}}$ is due to the uniqueness in Lemma 2.2. □

Up to now we have solved Theorem 2.1 for all positive integer multiples n of p. It remains to consider the case when n and p are relatively prime.

Lemma 2.5. *Let $n \in \mathbb{N}$ with $n < p$. Given any sequence $(k_d)_{d\in\mathbb{N}} \in \{0, \ldots, p-1\}^{\mathbb{N}}$ there exist exactly n sequences $(m_d)_{d\in\mathbb{Z}_+} \in \{0, \ldots, n-1\}^{\mathbb{N}}$ and for each of these a unique sequence $(q_d)_{d\in\mathbb{N}} \in \{0, \ldots, p-1\}^{\mathbb{N}}$ such that* (2.4) *holds.*

Proof. The solutions of (2.4) for a fixed $d \in \mathbb{Z}_+$ can be taken from table 2. Since $\gcd(n, p) = 1$, the first two columns show that any combination of $k_{d+1} \in \{0, \ldots, p-1\}$ and $m_d \in \{0, \ldots, n-1\}$ is possible. Hence given k_1 there are exactly n possible choices for m_0. Fixing one of these, say $m_0 = (r_0 p (\mathrm{mod}\, n) + k_1) (\mathrm{mod}\, n)$ for some $r_0 \in \{0, \ldots, n-1\}$, this uniquely determines $m_1 = r_0$. Further, q_1 is uniquely determined by (2.4). Inductively, m_{d+1} and q_{d+1} are uniquely determined by k_{d+1} and m_d, respectively by (2.4). □

Lemma 2.6. *Let $n \in \mathbb{N}$ with $n > p$ and* $\gcd(n, p) = 1$. *Then the assertion of Lemma* 2.5 *remains valid.*

Proof. Write $n = mp + r$ with $m \in \mathbb{N}$ and $r \in \{1, \ldots, p-1\}$. Then the solutions of (2.4) for a fixed $d \in \mathbb{Z}_+$ can be taken from table 3. Since $\gcd(n, p) = 1$, the first two columns show that any combination of $k_{d+1} \in \{0, \ldots, p-1\}$ and $m_d \in \{0, \ldots, n-1\}$ is possible. Hence given k_1 there are exactly n possible choices for m_0. Fixing one of these, this uniquely determines all other coefficients similar to the proof of Lemma 2.5. □

Theorem 2.1 is now completely proven by Lemmas 2.2–2.6. For every $n \in \mathbb{N}$ and $y \in S_p$, the explicit construction of roots shows that once we have chosen one out of $|\Delta_n(y)|$ possible m_0's, the sequence $(m_d)_{d\in\mathbb{Z}_+}$ and thus $z \in \Delta_n(y)$ is uniquely determined. Hence we immediately get the following.

COROLLARY 2.7

Let $x, z \in \Delta_n(y)$. Then $x = z$ if and only if $x_0 = z_0$.

Remark 2.8. It has been communicated to the author by Guntram Hainke, University of Bielefeld, that the roots constructed in this section are in fact the roots on the isomorphic

Table 2. Solutions of (2.4) for $n < p$.

k_{d+1}	=	m_d	−	p	m_{d+1}	+	n	q_{d+1}
0		0			0			0
⋮		⋮			⋮			⋮
$n-1$		$n-1$			⋮			0
n		0			⋮			1
⋮		⋮			⋮			⋮
			⋮					
$p-1$		⋮			0			$\lfloor p/n \rfloor$
0		$p \pmod n$			1			⋮
⋮		⋮			⋮			⋮
			⋮					
$p-1$		⋮			1			⋮
0		$2p \pmod n$			2			⋮
⋮		⋮			⋮			⋮
			⋮					
			⋮					
$p-1$		⋮			$n-2$			⋮
0		$(n-1)p \pmod n$			$n-1$			⋮
⋮		⋮			⋮			⋮
			⋮					
$p-n-1$		$n-1$			⋮			$p-2$
$p-n$		0			⋮			$p-1$
⋮		⋮			⋮			⋮
$p-1$		$n-1$			$n-1$			$p-1$

group $[0, 2\pi) \times \Omega_p \cong S_p$ given by Theorem (10.15) in [12]. Here $\Omega_p = (\{0, \dots, p-1\}^{\mathbb{N}}, +)$ denotes the p-adic integers with the addition $k + l$ of $k = (k_1, k_2, \dots)$ and $l = (l_1, l_2, \dots)$ defined as in Definition (10.2) of [12] by

$$(k+l)_d = \begin{cases} k_1 + l_1 \pmod p, & \text{if } d = 1, \\ k_d + l_d + \left\lfloor \frac{k_{d-1}+l_{d-1}}{p} \right\rfloor \pmod p, & \text{if } d \geq 2. \end{cases}$$

Table 3. Solutions of (2.4) for relatively prime $n > p$.

k_{d+1}	=	m_d	$-$	p	m_{d+1}	+	n	q_{d+1}
0		0			0			0
⋮		⋮			⋮			⋮
$p-1$		$p-1$			0			0
0		p			1			0
⋮		⋮			⋮			⋮
$p-1$		$2p-1$			1			0
			⋮					
0		mp			m			0
⋮		⋮			⋮			⋮
$r-1$		$mp+r-1=n-1$			m	$=\lfloor n/p \rfloor$		0
$r=n \pmod p$		0			m			1
⋮		⋮			⋮			⋮
$p-1$		$p-r-1$			m			1
0		$p-r$			$m+1$			1
⋮		⋮			⋮			⋮
			⋮					
⋮		$n-1$			⋮			1
$2n \pmod p$		0			⋮			2
⋮		⋮			⋮			⋮
			⋮					
			⋮					
⋮		$n-1$			⋮			$p-2$
$(p-1)n \pmod p$		0			⋮			$p-1$
⋮		⋮			⋮			⋮
			⋮					
$p-1$		$n-1$			$n-1$			$p-1$

The addition on the Abelian group $[0, 2\pi) \times \Omega_p$ is given by

$$(t, k) + (s, l) = (t + s \,(\mathrm{mod}\, 2\pi), k + l + \lfloor t + s \rfloor u),$$

where $u = (1, 0, 0, \dots) \in \Omega_p$ is fixed. Using the representation (2.1), the isomorphism $\varphi\colon S_p \to [0, 2\pi) \times \Omega_p$ is then simply given by $\varphi(y) = \varphi(y_0, y_1, \dots) = (t, k_1, k_2, \dots)$.

Now for $z \in \Delta_n(y)$ we need $n \cdot \varphi(z) = (t, k_1, k_2, \dots)$ and hence $(\varphi(z))_0 = \frac{t+m_0}{n}$ for some $m_0 \in \{0, \dots, n-1\}$. For the first component in Ω_p this implies $k_1 = n \cdot (\varphi(z))_1 + m_0 \pmod p$. If $n = p$ then $k_1 = m_0$ and the coefficients $(\varphi(z))_d$ are inductively unique defined by the group addition. If $\gcd(n, p) = 1$, then for fixed $m_0 \in \{0, \dots, n-1\}$ again the coefficients $(\varphi(z))_d$ are inductively unique defined by the group addition. In fact the uniqueness relation can easily be rewritten as equation (2.4). A combination of these arguments provides another simple proof of Theorem 2.1 and Corollary 2.7 which build the basis for §3. Since explicit representation was our primary concern, a more detailed proof is given by Lemmas 2.2–2.6, especially by including tables 1–3.

3. Embeddability into one-parameter subgroups

According to Corollary 2.7 and the representation (2.2), for any $n \in \mathbb{N}$ with $\gcd(n, p) = 1$ we might fix a specific $m_0 = m_0^{(n)} \in \{0, \dots, n-1\}$ for all $y \in S_p$ to get a well-defined n-th root $y^{1/n} \in \Delta_n(y)$. We refer to the sequence $(m_0^{(n)})_{n \in \mathbb{N} \setminus p\mathbb{N}}$ as a *root procedure*.

Lemma 3.1. *Choosing the root procedure* $m_0^{(n)} = 0$ *for all* $n \in \mathbb{N}$ *with* $\gcd(n, p) = 1$ *or* $m_0^{(n)} = n - 1$ *for all* $n \in \mathbb{N}$ *with* $\gcd(n, p) = 1$, *all procedures of taking roots of order being relatively prime to p are commuting. By prime number decomposition, equivalently for arbitrary primes* $q \neq p$ *and* $r \neq p$ *we have*

$$(y^{1/q})^{1/r} = (y^{1/r})^{1/q} = y^{1/(rq)} \quad \text{for all } y \in S_p. \tag{3.1}$$

Proof. To ensure (3.1), by Corollary 2.7 we only have to compare the first components, since every side of the equation belongs to $\Delta_{rq}(y)$. Namely, these first components can be easily derived as

$$(y^{1/(rq)})_0 = \exp\left[\frac{it}{rq} + 2\pi i\,\frac{m_0^{(rq)}}{rq}\right],$$

$$((y^{1/q})^{1/r})_0 = \exp\left[\frac{it}{rq} + 2\pi i\,\frac{m_0^{(q)}}{rq} + 2\pi i\,\frac{m_0^{(r)}}{r}\right],$$

$$((y^{1/r})^{1/q})_0 = \exp\left[\frac{it}{rq} + 2\pi i\,\frac{m_0^{(r)}}{rq} + 2\pi i\,\frac{m_0^{(q)}}{q}\right].$$

Thus for arbitrary primes $q \neq p$ and $r \neq p$ we have

$$m_0^{(rq)} = m_0^{(q)} + q \cdot m_0^{(r)} = m_0^{(r)} + r \cdot m_0^{(q)} \in \{0, \dots rq - 1\},$$

which is fulfilled by any of the two given root procedures. □

Remark 3.2. Note that Lemma 3.1 does not extend to the case $q = p$ or $r = p$. To see this, observe that by (3.1) for the unique p^k-th roots $y^{1/p^k} = K_k(y)$ and any $n > p$ with $\gcd(n, p) = 1$ we get $(K_k(y))^{1/n} = K_k(y^{1/n})$ for all $k \in \mathbb{N}$. Since both sides of the equation belong to $\Delta_{np^k}(y)$, by Corollary 2.7 their first components have to coincide. Namely these are

$$((K_k(y))^{1/n})_0 = \exp\left[i\left(t + 2\pi \sum_{\ell=1}^{k} k_\ell\right) \Big/ (np^k) + \frac{m_0^{(n)}}{n}\right],$$

$$(K_k(y^{1/n}))_0 = \exp\left[i \left(t + 2\pi \sum_{\ell=1}^{k} k_\ell \right) \Big/ (np^k) + \frac{m_k^{(n)}}{n} \right].$$

Hence we must have $m_0^{(n)} = m_k^{(n)} \in \{0, \dots, n-1\}$ for all $k \in \mathbb{N}$. In the case of our first root procedure with $m_0^{(n)} = 0$, by Lemma 2.6 (see the first row in table 3) this implies $k_\ell = 0$ for all $\ell \in \mathbb{N}$ such that by (2.1) we conclude that $y = \theta(t) \in S_p^{\mathrm{arc}}$. In the case of our second root procedure with $m_0^{(n)} = n-1$, again by Lemma 2.6 (see the last row in table 3) this implies $k_\ell = p-1$ for all $\ell \in \mathbb{N}$ such that by (2.1) we easily calculate that $y = \theta(t - 2\pi) \in S_p^{\mathrm{arc}}$. Hence, in general, for $y \in S_p \setminus S_p^{\mathrm{arc}}$ it is not possible to have commuting procedures of taking roots of arbitrary order.

Moreover, this shows that the root procedures cannot serve to define the n-th root $y \mapsto y^{1/n}$ as a homomorphism on S_p in general, since in this case we must have

$$y^{1/n} = ((y^{1/p})^p)^{1/n} = ((y^{1/p})^{1/n})^p,$$

which gives commuting roots $(y^{1/n})^{1/p} = (y^{1/p})^{1/n}$ by applying the automorphic p-th root on both sides. Note that for any choice of roots it is simply impossible to define $y \mapsto \psi_n(y) \in \Delta_n(y)$ as a homomorphism on S_p for $n \neq p^k$, since in this case by Proposition 1.3 of [24] necessarily the additive subgroup $\mathbb{Q}_n$ of $\mathbb{Q}$ generated by $\{n^{-k} : k \in \mathbb{N}\}$, called the n-ary rationals, has to be a subgroup of $\mathbb{Q}_p$.

As an easy consequence of (3.1) we obtain $(y^{1/(rq)})^q = y^{1/r}$ for all primes $q \neq p$ and $r \neq p$ and every $y \in S_p$. Note that in general we do not have $(y^q)^{1/q} = y$, hence our preferable order will be to take roots first and then the powers. For arbitrary $n \in \mathbb{N}$, we write $n = lp^k$ with $k \in \mathbb{Z}_+$ and $\gcd(l, p) = 1$ and define for any $y \in S_p$,

$$y^{1/n} = (y^{1/l})^{1/p^k} = K_k(y^{1/l}). \tag{3.2}$$

Note that by Lemma 3.1 we can use the primary decomposition of $l \in \mathbb{N} \setminus p\mathbb{N}$ to calculate $y^{1/l}$ above, successively by taking the appropriate prime roots in an arbitrary order.

Lemma 3.3. *Choosing the root procedure* $m_0^{(n)} = 0$ *for all* $n \in \mathbb{N}$ *with* $\gcd(n, p) = 1$ *or* $m_0^{(n)} = n-1$ *for all* $n \in \mathbb{N}$ *with* $\gcd(n, p) = 1$, *for any* $y \in S_p$ *the well-defined roots* $y^{1/n} \in \Delta_n(y)$, $n \in \mathbb{N}$ *in* (3.2) *fulfill*

$$(y^{1/(mn)})^m = y^{1/n} \quad \textit{for all } m, n \in \mathbb{N}. \tag{3.3}$$

Proof. Let $n = lp^k$ and $m = sp^r$ with $k, r \in \mathbb{Z}_+$ and $\gcd(l, p) = 1 = \gcd(s, p)$. Since the shift operators are automorphisms on S_p fulfilling $K_r \circ K_k = K_{r+k}$ we get

$$\begin{aligned}(y^{1/(mn)})^m &= (K_{r+k}(y^{1/(ls)}))^{sp^r} = ((K_r \circ K_k(y^{1/(ls)}))^{p^r})^s \\ &= (K_k(y^{1/(ls)}))^s = K_k((y^{1/(ls)})^s) = K_k(y^{1/l}) = y^{1/n},\end{aligned}$$

where the first but last equality holds since (3.3) is already fulfilled in case m, n are relatively prime to p by Lemma 3.1. □

Now we are ready to state our main result concerning non-uniqueness of rational embedding. Let $q = m/n \in \mathbb{Q}$ for some $m \in \mathbb{Z}$ and $n \in \mathbb{N}$ and define for any $y \in S_p$,

$$y^q = y^{m/n} = (y^{1/n})^m \quad \text{with } y^{1/n} \text{ as in (3.2).} \tag{3.4}$$

Clearly, the above definition uses $y^0 = e = (1, 1, \dots) \in S_p$ and $y^{-m} = (y^m)^{-1} = (y^{-1})^m$ for any $y \in S_p$ and $m \in \mathbb{N}$.

Theorem 3.4. *Choosing the root procedure* $m_0^{(n)} = 0$ *for all* $n \in \mathbb{N}$ *with* $\gcd(n, p) = 1$ *or* $m_0^{(n)} = n - 1$ *for all* $n \in \mathbb{N}$ *with* $\gcd(n, p) = 1$, *for any* $y \in S_p$ *the well-defined elements* $\phi_q(y) = y^q$, $q \in \mathbb{Q}$ *in* (3.4) *build a rational one-parameter subgroup, i.e.*

$$\phi_q(y) \cdot \phi_r(y) = \phi_{q+r}(y) \quad \text{for all } q, r \in \mathbb{Q},$$

embedding the roots $\phi_{1/n}(y) \in \Delta_n(y)$ *for all* $n \in \mathbb{N}$. *Further, if* $q = 1/n$ *with* $\gcd(n, p) = 1$ *and* $r \in \mathbb{Q}$ *then for any* $y \in S_p$ *we have* $\phi_r(\phi_q(y)) = \phi_{rq}(y)$.

Proof. By Lemma 3.3 the definition in (3.4) does not depend on the representation of $q \in \mathbb{Q}$ and hence $\phi_q(y)$ is well-defined for $y \in S_p$. For $q = m/n$ and $r = k/l$ with $m, k \in \mathbb{Z}$ and $n, l \in \mathbb{N}$ by Lemma 3.3 we get

$$\begin{aligned}\phi_q(y) \cdot \phi_r(y) &= (y^{1/n})^m (y^{1/l})^k \\ &= (y^{1/(nl)})^{ml} (y^{1/(nl)})^{kn} = (y^{1/(nl)})^{ml+kn} = \phi_{q+r}(y).\end{aligned}$$

Further, the last assertion follows directly from Lemma 3.1 together with (3.4). □

Remark 3.5. For $y \in S_p \setminus S_p^{\mathrm{arc}}$ we cannot expect more than rational embeddability of the roots, simply because the unique p^n-th roots $\phi_{1/p^n}(y) = K_n(y)$ in general, do not converge as $n \to \infty$. Moreover, for $y = \theta(x) \in S_p^{\mathrm{arc}}$ it is quite obvious that our first root procedure with $m_0^{(n)} = 0$ for all $n \in \mathbb{N}$ with $\gcd(n, p) = 1$ extends to the continuous one-parameter subgroup $(\phi_\alpha(y) = \theta(\alpha x))_{\alpha \in \mathbb{R}}$. But since the p-ary rationals $\mathbb{Q}_p = \{k/p^n : k \in \mathbb{Z},\ n \in \mathbb{N}\}$ are dense in $\mathbb{R}$ and the p^n-th roots are unique, by (3.4) we have uniqueness of the continuous one-parameter subgroup, showing that our second root procedure with $m_0^{(n)} = n - 1$ for all $n \in \mathbb{N}$ with $\gcd(n, p) = 1$ cannot be extended to a continuous one-parameter subgroup even on S_p^{arc}.

In fact, as conjectured by Riddhi Shah of Tata Institute of Fundamental Research, the uniqueness of embedding for Dirac measures on S_p^{arc} remains true for more general infinitely divisible probability measures as follows.

COROLLARY 3.6

Any infinitely divisible probability measure μ *on* S_p *with* $\mu(S_p^{\mathrm{arc}}) = 1$ *is uniquely embeddable into a continuous convolution semigroup.*

Proof. Let $n \in \mathbb{N}$ be fixed and ν be a probability measure on S_p such that $\nu^{p^n} = \mu$. Since $\mu(S_p^{\mathrm{arc}}) = 1$, we have $\nu(yS_p^{\mathrm{arc}}) = 1$ for some $y \in S_p$ and hence $y^{p^n} \in S_p^{\mathrm{arc}}$ follows. Due to the uniqueness of p^n-th roots we have $y \in S_p^{\mathrm{arc}}$ and thus $\nu(S_p^{\mathrm{arc}}) = 1$. This shows that the p^n-th roots of the infinitely divisible measure μ all assign measure 1 to S_p^{arc}. Now the assertion follows due to the fact that θ defines an isomorphism between $\mathbb{R}$ and S_p^{arc}, and uniqueness of embedding for probability measures on $\mathbb{R}$ is well-known. □

Note that Corollary 3.6 is in general not true without the condition $\mu(S_p^{\mathrm{arc}}) = 1$. On the one hand, by Remark 3.5 we know that Dirac measures $\mu = \delta_x$ with $x \in S_p \setminus S_p^{\mathrm{arc}}$ are only (non-uniquely) rationally and not continuously embeddable. On the other hand, using the compact subgroups H_n with $S_p/H_n \cong \mathbb{T}$ appearing in the Introduction, by a result of Böge [5] one can construct different Poisson semigroups $(\mu_t)_{t \geq 0}$, $(\nu_t)_{t \geq 0}$ with $\mu_1 = \nu_1$ (see also the Proposition on p. 417 of [11]).

Acknowledgements

The author is grateful to Professors Wilfried Hazod, Gyula Pap and Riddhi Shah for their valuable remarks and comments. He further wishes to express his sincere thanks to Gyula Pap for great hospitality and support during the author's visit to the Faculty of Informatics, University of Debrecen. This research has partly been carried out while the author was staying at the University of Debrecen, Hungary, with the kind support of Deutsche Forschungsgemeinschaft.

References

[1] Barczy M and Pap G, Weakly infinitely divisible measures on some locally compact Abelian groups, Preprint (University of Debrecen) (2004) arXiv: 0707.2186VI
[2] Barczy M, Bendikov A and Pap G, Limit theorems on locally compact Abelian groups, Preprint (University of Debrecen) (2004) to appear in *Mathematische Nachrichten*, arXiv: math / 0702078VI
[3] Bendikov A and Ritter G, Gaussian measures on solenoids, Unpublished manuscript (1997)
[4] Bendikov A and Saloff-Coste L, Brownian motions on compact groups of infinite dimension, in: Heat kernels and analysis on manifolds, graphs, and metric spaces (eds) P Auscher *et al*, Lecture notes from a quarter program on heat kernels, random walks, and analysis on manifolds and graphs, Paris, April 2002, *Contemp. Math.* (2003) (Providence: AMS) vol. 338, pp. 41–63
[5] Böge W, Über die Charakterisierung sukzessiv unendlich teilbarer Wahrscheinlichkeitsverteilungen, *J. Reine Angew. Math.* **201** (1959) 150–156
[6] Böge W, Zur Charakterisierung sukzessiv unendlich teilbarer Wahrscheinlichkeitsverteilungen auf lokalkompakten Gruppen, *Z. Wahrsch. Verw. Geb.* **2** (1964) 380–394
[7] Carnal H, Unendlich oft teilbare Wahrscheinlichkeitsverteilungen auf kompakten Gruppen, *Math. Annalen* **153** (1964) 351–383
[8] Dixmier J, Quelques propriétés des groupes abélien localement compacts, *Bull. Sci. Math. Ser. II* **81** (1957) 113–121
[9] Hazod W, Einige Sätze über unendlich teilbare Wahrscheinlichkeitsmaße auf lokalkompakten Gruppen, *Arch. Math.* **26** (1975) 297–312
[10] Hazod W and Schmetterer L, Über einige mit der Wahrscheinlichkeitstheorie zusammenhängende Probleme der Gruppentheorie, *J. Reine Angew. Math.* **263** (1973) 144–152
[11] Hazod W and Siebert E, Stable probability measures on Euclidean spaces and on locally compact groups, Structural properties and limit theorems (2001) (Dordrecht: Kluwer)
[12] Hewitt E and Ross K A, Abstract harmonic analysis I (1963) (Berlin: Springer)
[13] Heyer H, Probability measures on locally compact groups (1977) (Berlin: Springer)
[14] Heyer H, Recent contributions to the embedding problem for probability measures on a locally compact group, *J. Multivariate Anal.* **19** (1986) 119–131
[15] Heyer H, Das Einbettungsproblem der Wahrscheinlichkeitstheorie, *Österr. Z. Stat. Inf.* **19** (1989) 191–213
[16] Hofmann K H and Morris S A, The structure of compact groups (1998) (Berlin: De Gruyter)
[17] McCrudden M, An introduction to the embedding problem for probabilities on locally compact groups, in: Positivity in Lie theory: Open problems (eds) Hilgert J *et al* (1998) (Berlin: De Gruyter) pp. 147–164
[18] McCrudden M, The embedding problem for probabilities on locally compact groups, in: Probability measures on groups: Recent directions and trends (eds) Dani S G and Graczyk P (2006) (New Delhi: Narosa Publ. House)

[19] Morris S A, Pontryagin duality and the structure of locally compact Abelian groups (1977) (Cambridge: Cambridge University Press)
[20] Mycielski J, Some properties of connected compact groups, *Coll. Math.* **5** (1958) 162–166
[21] Parthasarathy K R, On the imbedding of an infinitely divisible distribution in a one-parameter convolution semigroup, *Teor. Veroyatn. Primen.* **12** (1967) 426–432 and *Theory Probab. Appl.* **12** (1967) 373–380
[22] Parthasarathy K R, Probability measures on metric spaces (1967) (New York: Academic Press)
[23] Parthasarathy K R, On the imbedding of an infinitely divisible distribution in a one parameter convolution semigroup, *Sankhya* **A35** (1973) 123–132
[24] Wilson A M, On endomorphisms of a solenoid, *Proc. Am. Math. Soc.* **55** (1976) 69–74