Publ. Math. Debrecen
95/3-4 (2019), 363–376
DOI: 10.5486/PMD.2019.8499

On a characterization theorem on non-discrete totally disconnected locally compact fields

By GENNADIY M. FELDMAN (Kharkiv)
and MARGARYTA V. MYRONYUK (Kharkiv)

Abstract. We prove the following theorem. Let X be a non-discrete totally disconnected locally compact field, R be its ring of integers, P be the nonzero prime ideal of R. Assume that the residue field R/P is a field of characteristic $p > 2$. Let ξ and η be independent identically distributed random variables with values in X and distribution μ, such that μ has a continuous density with respect to a Haar measure on X. This implies that the random variables $S = \xi + \eta$ and $D = (\xi - \eta)^2$ are independent if and only if μ is a shift of the Haar distribution of a compact subgroup of X.

1. Introduction

Let $\xi_1, \xi_2, \ldots, \xi_n$, $n \geq 2$, be independent identically distributed real-valued random variables. It is known that if the sample mean $\bar{\xi} = \frac{1}{n}\sum_{j=1}^{n} \xi_j$ and the sample variance $s^2 = \frac{1}{n}\sum_{j=1}^{n}(\xi_j - \bar{\xi})^2$ are independent, then all ξ_j are Gaussian random variables (see [15], [18], [19], [23], and also [17, §4.2]). For $n = 2$, this theorem can be formulated as follows. If ξ and η are independent identically distributed random variables and their sum $\xi + \eta$ and square of difference $(\xi - \eta)^2$ are also independent, then ξ and η are Gaussian random variables. This characterization theorem can be considered as a generalization of the well-known Kac–Bernstein theorem, where Gaussian distribution on the real line is characterized by independence of the sum and the difference of two independent random variables.

Mathematics Subject Classification: 60B15, 62E10, 43A05.
Key words and phrases: characterization theorem, totally disconnected locally compact field, Haar distribution.

In the last years, much attention has been devoted to the generalization of characterization theorems of mathematical statistics to various algebraic structures, such as locally compact Abelian groups, Lie groups, quantum groups, symmetric spaces (see, e.g., [1]–[14], [16], [20], [21], and also [9] for additional references and related results). However, in all studied characterization problems on groups only linear forms of independent random variables with values in a group were considered. To the best of our knowledge, first a non-linear characterization problem was considered in [14], where, in particular, the following theorem was proved.

Theorem A. *Consider the field of p-adic numbers $\mathbb{Q}_p$, where $p > 2$. Let ξ and η be independent identically distributed random variables with values in $\mathbb{Q}_p$ and distribution μ, such that μ has a continuous density with respect to a Haar measure on $\mathbb{Q}_p$. This implies that the random variables $S = \xi+\eta$ and $D = (\xi-\eta)^2$ are independent if and only if μ is a shift of the Haar distribution of a compact subgroup of $\mathbb{Q}_p$.*

Using the scheme of the proof of Theorem A, we prove in this note that Theorem A holds true for non-discrete totally disconnected locally compact fields. Note that on totally disconnected locally compact Abelian groups, in particular, on totally disconnected locally compact fields, Gaussian measures are degenerated, and shifts of the Haar distributions of compact subgroups play the role of Gaussian measures.

Recall some results about non-discrete totally disconnected locally compact fields (see, e.g., [22]), and introduce the notation that will be used. Let X be a non-discrete totally disconnected locally compact field with an ultra-metric norm $|.|$. Denote by R the ring of integers in X consisting of all elements of X such that $|x| \leq 1$. The ring R is compact and open. Denote by P the prime ideal in R consisting of all elements of R such that $|x| < 1$. The residue field R/P is a field of non-zero characteristic p and consists of q elements, where q is a power of p. The ideal P is principal, i.e., there exists an element $\mathfrak{p} \in P$ such that $P = \mathfrak{p}R$. In so doing, $|\mathfrak{p}| = q^{-1}$ and $X = \bigcup_{n=-\infty}^{\infty} \mathfrak{p}^n R$. The family $\{\mathfrak{p}^n R\}_{n=-\infty}^{\infty}$ forms an open basis at zero of the field X. Denote by e the identity of the field X. There exists an element ε of order $q-1$ in the multiplicative group of the field X. In so doing $|\varepsilon| = 1$, and the elements $0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{q-1} = e$ form the complete set of representatives of the residue classes R/P. Take $B \subset X$. Put $B^{[2]} = \{x \in X : x = t^2,\ t \in B\}$. Consider $A = \{x \in X : |x - e| < 1\}$, i.e., $A = e + P$. Each element $a \in A$ is represented as a convergent series $a = e + a_1\mathfrak{p} + a_2\mathfrak{p}^2 + \ldots$, where either $a_j = 0$ or $a_j = \varepsilon^{k_j}$, $k_j \in \{1, 2, \ldots, q-1\}$.

The set A is a compact subgroup in the multiplicative group of the field X, and when q is odd, satisfies the condition $A^{[2]} = A$. Each element $x \in X$, $x \neq 0$, is uniquely represented in the form $x = \mathfrak{p}^n \varepsilon^k a$, where n is an integer, $k \in \{1, 2, \ldots, q-1\}$, $a \in A$. Denote by $R^\times$ the group of invertible elements of the ring R. It consists of all elements of R such that $|x| = 1$. Then each element $x \in X$, $x \neq 0$ is uniquely represented in the form $x = \mathfrak{p}^n c$, where n is an integer, $c \in R^\times$.

The additive group of the field X is a locally compact Abelian group. We also denote this group by X. Denote by (x, y), $x, y \in X$, elements of the group X^2. Denote by T the mapping $T : X^2 \mapsto X^2$ defined by the formula $T(x, y) = (x + y, (x - y)^2)$. The element $x \in X$ is said to be compact if the smallest closed subgroup of X containing x is compact. Denote by m_X a Haar measure on X. Choose a Haar measure m_X such that $m_X(R) = 1$. Then $m_X(\mathfrak{p}^n R) = q^{-n}$. We shall also assume that $m_{X^2} = m_X \times m_X$. Denote by $I(X)$ the set of all shifts of the Haar distributions m_K of compact subgroups K of the group X. Denote by E_x the degenerate distribution concentrated at a point $x \in X$. If ξ and η are random variables with values in X, then we denote by μ_ξ the distribution of the random variable ξ, and by $\mu_{(\xi,\eta)}$ the distribution of the random vector (ξ, η).

2. The main theorem

The main result of the work is the proof of the following statement.

Theorem 1. *Let X be a non-discrete totally disconnected locally compact field such that the residue field R/P is a field of characteristic $p > 2$. Let ξ and η be independent identically distributed random variables with values in X and distribution μ, such that μ has a continuous density with respect to a Haar measure m_X. The random variables $S = \xi + \eta$ and $D = (\xi - \eta)^2$ are independent if and only if $\mu \in I(X)$.*

To prove Theorem 1, we need some lemmas.

Lemma 1. *Let X be a non-discrete totally disconnected locally compact field such that the residue field R/P is a field of characteristic $p > 2$. Then on the set $X^{[2]}$, there exists a continuous function $\mathfrak{s}(x)$ satisfying the equation*

$$\mathfrak{s}^2(x) = x, \quad x \in X^{[2]}. \tag{1}$$

PROOF. Let $x \in X$, $x \neq 0$. Then x is uniquely represented in the form $x = \mathfrak{p}^n \varepsilon^k a$, where n is an integer, $k \in \{1, 2, \dots, q-1\}$, $a \in A$, and the elements $0, \varepsilon, \varepsilon^2, \dots, \varepsilon^{q-1} = e$ form the complete set of representatives of the residue classes of R/P. We have $x^2 = \mathfrak{p}^{2n} \varepsilon^{2k} a^2$. The representation

$$X = \{0\} \cup \bigcup_{n=-\infty}^{\infty} \mathfrak{p}^n R^\times$$

implies that

$$X^{[2]} = \{0\} \cup \bigcup_{n=-\infty}^{\infty} \mathfrak{p}^{2n} (R^\times)^{[2]}. \tag{2}$$

Put $A_k = \varepsilon^k + P = \varepsilon^k A$, $k = 1, \dots, q-1$. Note that $A_{q-1} = A$ and $R^\times = \bigcup_{k=1}^{q-1} A_k$. Since q is odd, we have $A^{[2]} = A$. It follows from this that $A_k^{[2]} = A_{2k}$ if $k = 1, \dots, \frac{q-1}{2}$, and $A_k^{[2]} = A_{2k-q+1}$ if $k = \frac{q+1}{2}, \dots, q-1$. First define the function $\mathfrak{s}(x)$ on the set $(R^\times)^{[2]} = \bigcup_{k=1}^{\frac{q-1}{2}} A_{2k}$. Let $x \in A_{2k}$. Then the equation $x = t^2$ has two roots $t_1 \in A_k$ and $-t_1 \in A_{k+\frac{q-1}{2}}$, and they belong to different residue classes. The residue class A_k is a compact set, the function $g(x) = x^2$ is continuous on A_k and it is a one-to-one mapping of the set A_k on A_{2k}. This implies that the inverse to $g(x)$ mapping $\mathfrak{s}_k : A_{2k} \mapsto A_k$ is also continuous, and hence is a homeomorphism between A_{2k} and A_k. Put $\mathfrak{s}(x) = \mathfrak{s}_k(x)$, if $x \in A_{2k}$, $k = 1, 2, \dots, \frac{q-1}{2}$. Since A_{2k} is an open set in X, the function $\mathfrak{s}(x)$ is continuous and satisfies equation (1) on $(R^\times)^{[2]}$. Taking into account (2), put

$$\mathfrak{s}(x) = \begin{cases} \mathfrak{p}^n \mathfrak{s}(c), & \text{if } \ x = \mathfrak{p}^{2n} c, \ c \in (R^\times)^{[2]}, \\ 0, & \text{if } \ x = 0. \end{cases}$$

It is obvious that $\mathfrak{s}(x)$ is the required function. □

Lemma 2. *Let X be a non-discrete totally disconnected locally compact field such that the residue field R/P is a field of characteristic $p > 2$. Let $(x_0, y_0) \in X^2$, and assume that $|x_0 - y_0| = q^{-l}$. Then for $k \geq l+1$, the following equality*

$$T\{(x_0, y_0) + (\mathfrak{p}^k R)^2\} = (x_0 + y_0, (x_0 - y_0)^2) + (\mathfrak{p}^k R) \times (\mathfrak{p}^{k+l} R) \tag{3}$$

holds.

PROOF. Since $|x_0 - y_0|_p = q^{-l}$, we have $x_0 - y_0 = \mathfrak{p}^l c$, where $c \in R^\times$. Note that on the one hand, the equality

$$\begin{aligned} T\{(x_0, y_0)+(\mathfrak{p}^k R)^2\} &= T\{(x_0 + \mathfrak{p}^k x, y_0 + \mathfrak{p}^k y) : x, y \in R\} \\ &= \{(x_0+y_0+\mathfrak{p}^k(x+y), (x_0-y_0)^2+2\mathfrak{p}^k(x_0-y_0)(x-y) \\ &\quad + \mathfrak{p}^{2k}(x-y)^2) : x, y \in R\} \\ &= \{(x_0+y_0+\mathfrak{p}^k s, (x_0-y_0)^2+2\mathfrak{p}^{k+l}ct+\mathfrak{p}^{2k}t^2) : s, t \in R\} \quad (4) \end{aligned}$$

holds true for any k. On the other hand, the equality

$$\{2ct + \mathfrak{p}^{k-l}t^2 : t \in R\} = R \tag{5}$$

holds true for $k \geq l + 1$. Indeed, note that $(e + \mathfrak{p}^m R)^{[2]} = e + \mathfrak{p}^m R$ is fulfilled for any $m \geq 1$. This implies that $(c + \mathfrak{p}^m R)^{[2]} = c^2 + \mathfrak{p}^m R$ for all $c \in R^\times$, i.e., $\{c^2 + 2c\mathfrak{p}^m t + \mathfrak{p}^{2m}t^2 : t \in R\} = c^2 + \mathfrak{p}^m R$, and hence, $\{2ct + \mathfrak{p}^m t^2 : t \in R\} = R$. For $k \geq l + 1$, this equality implies (5). Taking into account (5), we get that (3) follows from (4). □

Lemma 3. *Let X be a non-discrete totally disconnected locally compact field such that the residue field R/P is a field of characteristic $p > 2$. Let a function $\mathfrak{s}$ be as constructed in the proof of Lemma 1. Consider the mappings S_j from $X \times X^{[2]}$ to X^2 of the form*

$$S_1(u, v) = \left(\frac{u + \mathfrak{s}(v)}{2}, \frac{u - \mathfrak{s}(v)}{2}\right), \qquad S_2(u, v) = \left(\frac{u - \mathfrak{s}(v)}{2}, \frac{u + \mathfrak{s}(v)}{2}\right).$$

Let $(u_0, v_0) \in X \times X^{[2]}$, and assume that $|\mathfrak{s}(v_0)| = q^{-l}$. Put $E_k = (u_0, v_0) + (\mathfrak{p}^k R) \times (\mathfrak{p}^{k+l} R)$. Then for $k \geq l + 1$, the following statements are valid:

(i) $E_k \subset X \times X^{[2]}$,

(ii) $S_1(E_k) \cap S_2(E_k) = \emptyset$,

(iii) $\int\limits_{S_j(E_k)} \Phi_j(x, y) dm_{X^2}(x, y) = \int\limits_{E_k} \Phi_j(S_j(u, v))|\mathfrak{s}(v)|^{-1} dm_{X^2}(u, v)$, $j = 1, 2$,

for any continuous function $\Phi_j(x, y)$ on $S_j(E_k)$.

PROOF. (i) Note that $|v_0| = q^{-2l}$. It follows from the proof of Lemma 1 that if $w_0 \in X^{[2]}$ and $|w_0| = q^{-2l}$, then $w_0 + w \in X^{[2]}$ for $w \in \mathfrak{p}^{2l+1}R$. Since $k \geq l+1$, from what has been said it follows that (i) is fulfilled.

(ii) Assume that $S_1(E_k) \cap S_2(E_k) \neq \emptyset$. Then as easily seen, there exist elements $v_1, v_2 \in R$ such that

$$\mathfrak{s}(v_0 + \mathfrak{p}^{k+l}v_1) = -\mathfrak{s}(v_0 + \mathfrak{p}^{k+l}v_2). \tag{6}$$

Since $v_0 \in X^{[2]}$ and $|v_0| = q^{-2l}$, we have $v_0 = \mathfrak{p}^{2l}c$, where $c \in (R^\times)^{[2]}$ and $v_0 + \mathfrak{p}^{k+l}v_i = \mathfrak{p}^{2l}(c + \mathfrak{p}^{k-l}v_i) \in \mathfrak{p}^{2l}(c + \mathfrak{p}^{k-l}R)$, $i = 1, 2$. It follows from the definition of the function $\mathfrak{s}$ that $\{\mathfrak{s}(x) : x \in (c+\mathfrak{p}R)\} \bigcap \{-\mathfrak{s}(x) : x \in (c+\mathfrak{p}R)\} = \emptyset$. Since $k \geq l + 1$, this implies that $\{\mathfrak{s}(x) : x \in \mathfrak{p}^{2l}(c + \mathfrak{p}^{k-l}R)\} \bigcap \{-\mathfrak{s}(x) : x \in \mathfrak{p}^{2l}(c + \mathfrak{p}^{k-l}R)\} = \emptyset$, contrary to (6). Hence, (ii) is proved.

(iii) We will prove that equality (iii) holds true for S_1. For S_2 the reasoning is similar. Put $(x_0, y_0) = S_1(u_0, v_0) = \left(\frac{u_0+\mathfrak{s}(v_0)}{2}, \frac{u_0-\mathfrak{s}(v_0)}{2}\right)$, and verify that

$$S_1(E_k) = (x_0, y_0) + (\mathfrak{p}^k R)^2. \tag{7}$$

Let $u \in \mathfrak{p}^k R$, $v \in \mathfrak{p}^{k+l}R$. We have

$$S_1(u_0 + u, v_0 + v) = \left(\frac{u_0 + u + \mathfrak{s}(v_0 + v)}{2}, \frac{u_0 + u - \mathfrak{s}(v_0 + v)}{2}\right).$$

Since the residue field R/P is a field of characteristic $p > 2$, we have $|2x| = |x|$ for all $x \in X$. Hence,

$$\left|\frac{u_0 + u + \mathfrak{s}(v_0 + v)}{2} - \frac{u_0 + \mathfrak{s}(v_0)}{2}\right| \leq \max\{|u|, |\mathfrak{s}(v_0 + v) - \mathfrak{s}(v_0)|\}. \tag{8}$$

It follows from $u \in \mathfrak{p}^k R$ that

$$|u| \leq q^{-k}. \tag{9}$$

Since $\mathfrak{s}^2(x) = x$, we have

$$|\mathfrak{s}(v_0 + v) - \mathfrak{s}(v_0)| = \frac{|v|}{|\mathfrak{s}(v_0 + v) + \mathfrak{s}(v_0)|}. \tag{10}$$

Note that $v_0 + v = \mathfrak{p}^{2l}c + \mathfrak{p}^{k+l}t$ for some $t \in R$. This implies that $\mathfrak{s}(v_0 + v) = \mathfrak{p}^l\mathfrak{s}(c+\mathfrak{p}^{k-l}t)$. Moreover, $\mathfrak{s}(v_0) = \mathfrak{p}^l\mathfrak{s}(c)$. Since the points $\mathfrak{s}(c+\mathfrak{p}^{k-l}t)$ and $\mathfrak{s}(c)$ are at the same residue class of the ideal P in R, we have $|\mathfrak{s}(c+\mathfrak{p}^{k-l}t)+\mathfrak{s}(c)| = 1$, and hence, $|\mathfrak{s}(v_0 + v) + \mathfrak{s}(v_0)| = q^{-l}$. Taking into account that $|v| \leq q^{-k-l}$, it follows from (10) that

$$|\mathfrak{s}(v_0 + v) - \mathfrak{s}(v_0)| \leq q^{-k}. \tag{11}$$

Taking into account (9) and (11), we find from (8) that inequality

$$\left|\frac{u_0+u+\mathfrak{s}(v_0+v)}{2}-\frac{u_0+\mathfrak{s}(v_0)}{2}\right|\le q^{-k} \tag{12}$$

holds true. We note that if $T(a,b)=T(a',b')$, then either $(a,b)=(a',b')$ or $(a,b)=(b',a')$. Since $|x_0-y_0|=|\mathfrak{s}(v_0)|=q^{-l}$, and $k\ge l+1$, the restriction of the mapping T to the set $(x_0,y_0)+(\mathfrak{p}^kR)^2$ is injective. Taking this into account, (7) follows from Lemma 2 and (12). Moreover, it follows from what has been said that the mappings T and S_1 are inverse homeomorphisms of the sets $(x_0,y_0)+(\mathfrak{p}^kR)^2$ and E_k.

Let $m\ge 1$. Represent the group $(\mathfrak{p}^kR)^2$ as a union of cosets of the subgroup $(\mathfrak{p}^{k+m}R)^2$. We have

$$(\mathfrak{p}^kR)^2=\bigcup_{i=1}^{q^{2m}}B_i.$$

Then by Lemma 2,

$$S_1(E_k)=\bigcup_{i=1}^{q^{2m}}\{(x_0,y_0)+B_i\}. \tag{13}$$

We note that $m_{X^2}\{(x_0,y_0)+B_i\}=m_{X^2}(B_i)=q^{-2k-2m}$. Let $(x_i,y_i)\in(x_0,y_0)+B_i$. Then $T(x_i,y_i)=(u_i,v_i)\in T\{(x_0,y_0)+B_i\}\subset E_k$. By the condition of the lemma, $|\mathfrak{s}(v)|=q^{-l}$ for $(u,v)\in E_k$. Thus $|\mathfrak{s}(v_i)|=q^{-l}$. It follows from $k\ge l+1$ that $(x_0,y_0)+B_i=(\widetilde{x}_0,\widetilde{y}_0)+(\mathfrak{p}^{k+m}R)^2$, where $|\widetilde{x}_0-\widetilde{y}_0|=q^{-l}$. Then Lemma 2 implies that $T\{(x_0,y_0)+B_i\}=T\{(\widetilde{x}_0,\widetilde{y}_0)+(\mathfrak{p}^{k+m}R)^2\}=(\widetilde{x}_0+\widetilde{y}_0,(\widetilde{x}_0-\widetilde{y}_0)^2)+(\mathfrak{p}^{k+m}R)\times(\mathfrak{p}^{k+m+l}R)$. We obtain from here that $m_{X^2}\{T\{(x_0,y_0)+B_i\}\}=q^{-(2k+2m+l)}$. It follows from what has been said that the equality

$$\begin{aligned}\sum_{i=1}^{q^{2m}}&\Phi_1(x_i,y_i)m_{X^2}\{(x_0,y_0)+B_i\}\\&=\sum_{i=1}^{q^{2m}}\Phi_1(S_1(u_i,v_i))m_{X^2}\{T\{(x_0,y_0)+B_i\}\}|\mathfrak{s}(v_i)|^{-1}\end{aligned} \tag{14}$$

is valid. Moreover, (13) implies that the sum in the left-hand side of equality (14) tends to the integral of the left-hand side of equality (iii) as $m\to\infty$. Since $TS_1(E_k)=E_k$, it follows from (13) that

$$E_k=\bigcup_{i=1}^{p^{2m}}T\{(x_0,y_0)+B_i\}.$$

Thus the sum in the right-hand side of equality (14) tends to the integral of the right-hand side of equality (iii) as $m \to \infty$. Passing to the limit in equality (14) as $m \to \infty$, we get (iii). □

Lemma 4. *Let X be a non-discrete totally disconnected locally compact field such that the residue field R/P is a field of characteristic $p > 2$. Let ξ and η be independent identically distributed random variables with values in X and distribution μ, such that μ has a continuous density ρ with respect to m_X and $\rho(0) > 0$. This implies that the random variables $S = \xi + \eta$ and $D = (\xi - \eta)^2$ are independent if and only if the density ρ satisfies the equation*

$$\rho^2(u)\rho(v)\rho(-v) = \rho^2(0)\rho(u+v)\rho(u-v), \quad u, v \in X. \tag{15}$$

Proof. First, we shall prove that the distribution $\mu_{(S,D)}$ has a density ϱ with respect to m_{X^2} and get a representation for ϱ. Inasmuch as $\mu_{(S,D)} = T(\mu_{(\xi,\eta)})$ and the distribution $\mu_{(\xi,\eta)}$ is absolutely continuous with respect to m_{X^2}, so is $\mu_{(\xi,\eta)}\{(t,t) : t \in X\} = 0$. Therefore, the distribution $\mu_{(S,D)}$ is concentrated at the set $X \times (X^{[2]} \backslash \{0\})$. Fix a function $\mathfrak{s}$ constructed in the proof of Lemma 1. Let the mappings S_j and the sets E_k be the same as in Lemma 3. Let $(u_0, v_0) \in X \times (X^{[2]} \backslash \{0\})$. Represent the element $\mathfrak{s}(v_0)$ in the form $\mathfrak{s}(v_0) = \mathfrak{p}^l c$, where $c \in R^\times$. By Lemma 3, (i) and (ii) hold for $k \geq l+1$. We have

$$\mu_{(S,D)}\{E_k\} = T(\mu_{(\xi,\eta)})\{E_k\} = \mu_{(\xi,\eta)}\{T^{-1}(E_k)\} = \int\limits_{T^{-1}(E_k)} \rho(x)\rho(y)dm_{X^2}(x,y)$$

$$= \int\limits_{S_1(E_k)} \rho(x)\rho(y)dm_{X^2}(x,y) + \int\limits_{S_2(E_k)} \rho(x)\rho(y)dm_{X^2}(x,y). \tag{16}$$

Using equality (iii) of Lemma 3, transform the integrals in the right-hand side of equality (16). We obtain

$$\int\limits_{S_1(E_k)} \rho(x)\rho(y)dm_{X^2}(x,y) = \int\limits_{E_k} \rho\left(\frac{u+\mathfrak{s}(v)}{2}\right)\rho\left(\frac{u-\mathfrak{s}(v)}{2}\right)|\mathfrak{s}(v)|^{-1}dm_{X^2}(u,v),$$

$$\int\limits_{S_2(E_k)} \rho(x)\rho(y)dm_{X^2}(x,y) = \int\limits_{E_k} \rho\left(\frac{u-\mathfrak{s}(v)}{2}\right)\rho\left(\frac{u+\mathfrak{s}(v)}{2}\right)|\mathfrak{s}(v)|^{-1}dm_{X^2}(u,v).$$

Then (16) implies that

$$\mu_{(S,D)}\{E_k\} = 2\int\limits_{E_k} \rho\left(\frac{u+\mathfrak{s}(v)}{2}\right)\rho\left(\frac{u-\mathfrak{s}(v)}{2}\right)|\mathfrak{s}(v)|^{-1}dm_{X^2}(u,v).$$

This equality means that the distribution $\mu_{(S,D)}$ has a density $\varrho(u,v)$ with respect to m_{X^2}, and this density is of the form

$$\varrho(u,v)=\begin{cases}2\rho\left(\frac{u+\mathfrak{s}(v)}{2}\right)\rho\left(\frac{u-\mathfrak{s}(v)}{2}\right)|\mathfrak{s}(v)|^{-1}, & \text{if } u\in X,\ v\in X^{[2]}\backslash\{0\},\\ 0, & \text{if } u\in X,\ v\notin (X^{[2]}\backslash\{0\}).\end{cases} \tag{17}$$

Note that when we got representation (17) for the density of the distribution $\mu_{(S,D)}$, we did not use the independence of the random variables S and D.

Necessity. By the condition of the lemma, the random variables S and D are independent. Therefore, there exist integrable with respect to m_X functions r_j on X, such that the equality

$$r_1(u)r_2(v)=2\rho\left(\frac{u+\mathfrak{s}(v)}{2}\right)\rho\left(\frac{u-\mathfrak{s}(v)}{2}\right)|\mathfrak{s}(v)|^{-1} \tag{18}$$

holds true almost everywhere with respect to m_{X^2} on $X\times(X^{[2]}\backslash\{0\})$. Since the function in the right-hand side of equality (18) is continuous, we can assume without loss of generality that the functions r_j are also continuous, and equality (18) holds true everywhere on $X\times(X^{[2]}\backslash\{0\})$. Since $\rho(0)>0$, it is easily seen that $r_1(0)>0$. Put $v=t^2$, $t\neq 0$. It follows from (18) that

$$r_2(t^2)=2r_1^{-1}(0)\rho\left(\frac{\mathfrak{s}(t^2)}{2}\right)\rho\left(-\frac{\mathfrak{s}(t^2)}{2}\right)|\mathfrak{s}(t^2)|^{-1},\quad t\in X,\ t\neq 0. \tag{19}$$

Note that (18) and (19) imply the equality

$$\begin{aligned}&r_1(u)\rho\left(\frac{\mathfrak{s}(t^2)}{2}\right)\rho\left(-\frac{\mathfrak{s}(t^2)}{2}\right)\\ &\quad=r_1(0)\rho\left(\frac{u+\mathfrak{s}(t^2)}{2}\right)\rho\left(\frac{u-\mathfrak{s}(t^2)}{2}\right),\quad (u,t)\in X^2,\ t\neq 0.\end{aligned} \tag{20}$$

It follows from the continuity of ρ and r_1 that equality (20) holds true for all $u,t\in X$. Put in (20) $t=0$. We deduce from the resulting equality that

$$r_1(u)=\frac{r_1(0)}{\rho^2(0)}\rho^2\left(\frac{u}{2}\right),\quad u\in X. \tag{21}$$

Substituting (21) into (20), we find that

$$\begin{aligned}&\rho^2\left(\frac{u}{2}\right)\rho\left(\frac{\mathfrak{s}(t^2)}{2}\right)\rho\left(-\frac{\mathfrak{s}(t^2)}{2}\right)\\ &\quad=\rho^2(0)\rho\left(\frac{u+\mathfrak{s}(t^2)}{2}\right)\rho\left(\frac{u-\mathfrak{s}(t^2)}{2}\right),\quad u,t\in X.\end{aligned} \tag{22}$$

Note that either $\mathfrak{s}(t^2) = t$ or $\mathfrak{s}(t^2) = -t$. This implies that the equalities

$$\rho\left(\frac{\mathfrak{s}(t^2)}{2}\right)\rho\left(-\frac{\mathfrak{s}(t^2)}{2}\right) = \rho\left(\frac{t}{2}\right)\rho\left(-\frac{t}{2}\right), \quad t \in X, \tag{23}$$

and

$$\rho\left(\frac{u+\mathfrak{s}(t^2)}{2}\right)\rho\left(\frac{u-\mathfrak{s}(t^2)}{2}\right) = \rho\left(\frac{u+t}{2}\right)\rho\left(\frac{u-t}{2}\right), \quad u,t \in X, \tag{24}$$

are fulfilled for an arbitrary function ρ. Substituting (23) and (24) into (22), we get that the density ρ satisfies equation (15). The necessity is proved.

Sufficiency. It follows from (17) and (24) that we have the following representation for the density ϱ of the distribution $\mu_{(S,D)}$:

$$\varrho(u,v) = \begin{cases} 2\rho\left(\frac{u+t}{2}\right)\rho\left(\frac{u-t}{2}\right)|\mathfrak{s}(t^2)|^{-1}, & \text{if} \quad u \in X,\ v = t^2,\ t \neq 0, \\ 0, & \text{if} \quad u \in X,\ v \notin (X^{[2]} \setminus \{0\}). \end{cases} \tag{25}$$

If a density ρ satisfies equation (15), it is easily seen that the density $\varrho(u,v)$ is represented as a product of a function of u and a function of v. This implies the independence of S and D. □

Lemma 5. *Let X be a non-discrete totally disconnected locally compact field such that the residue field R/P is a field of characteristic $p > 2$. Let ξ and η be independent identically distributed random variables with values in X and distribution μ, such that μ has a continuous density ρ with respect to m_X and $\rho(0) > 0$. If the random variables $S = \xi + \eta$ and $D = (\xi - \eta)^2$ are independent, then the set $K = \{x \in X : \rho(x) > 0\}$ is a subgroup of X.*

Proof. By Lemma 4, the function $\rho(x)$ satisfies equation (15). Assume that $\rho(x) > 0$ at a point $x \in X$. Put in (15) $u = v = \frac{x}{2}$. We get

$$\rho^3\left(\frac{x}{2}\right)\rho\left(-\frac{x}{2}\right) = \rho^3(0)\rho(x). \tag{26}$$

Since $\rho(0) > 0$ and $\rho(x) > 0$, it follows from (26) that

$$\rho\left(\frac{x}{2}\right)\rho\left(-\frac{x}{2}\right) > 0. \tag{27}$$

Put in (15) $u = v = -\frac{x}{2}$. We obtain

$$\rho^3\left(-\frac{x}{2}\right)\rho\left(\frac{x}{2}\right) = \rho^3(0)\rho(-x). \tag{28}$$

Taking into account (27), it follows from (28) that $\rho(-x) > 0$. So we proved that if $\rho(x) > 0$, then $\rho(-x) > 0$. Taking this into account, (15) implies that the set $K = \{x \in X : \rho(x) > 0\}$ is a subgroup in X. □

Now we can prove the main theorem.

Proof of Theorem 1. *Necessity.* It is obvious that replacing, if it is necessary, the random variables ξ and η by new independent random variables $\xi + x$ and $\eta + x$, we can assume from the beginning that $\rho(0) > 0$. It follows from Lemma 4 that the function ρ satisfies equation (15). By Lemma 5, the set $K = \{x \in X : \rho(x) > 0\}$ is a subgroup in X. Obviously, this subgroup is open. Hence, it is closed. Let $x \in K$. Denote by G the minimal closed subgroup generated by x. There are two possibilities: either X is a field of characteristic zero or X is a field of non-zero characteristic p.

Assume that X is a field of characteristic zero. It is well-known that then X is a finite extension of the field of the p-adic numbers $\mathbb{Q}_p$, and hence the additive group of the field X is topologically isomorphic to the group $\mathbb{Q}_p^m$ for some m. This implies that X consists of compact elements. Thus G is a compact subgroup. Consider the restriction of equation (15) to G. Put $\varphi(x) = \log \rho(x)$, $x \in G$. It follows from (15) that

$$2\varphi(u) + \varphi(v) + \varphi(-v) = 2\varphi(0) + \varphi(u+v) + \varphi(u-v), \quad u, v \in G.$$

Integrate both sides of this equality by the measure $dm_G(v)$. We get that $\varphi(u) = \varphi(0)$ for all $u \in G$, and hence $\rho(x) = \rho(0)$ for all $x \in K$. It follows from this that K is a compact group and $\mu = m_K$.

If X is a field of non-zero characteristic p, then the subgroup G is topologically isomorphic to the group of residue classes modulo p and we reason similarly. The necessity is proved.

Sufficiency. Let K be a nonzero compact subgroup of X. Assume that X is a field of characteristic zero. Then the additive group of the field X is topologically isomorphic to the group $\mathbb{Q}_p^m$ for some m. Since K is a compact subgroup, K is topologically isomorphic to some subgroup of the group $\mathbb{Z}_p^m$, where $\mathbb{Z}_p$ is the ring of p-adic integers. It is not difficult to verify that in this case the subgroup K possesses the property:

(i) if $x \in K$, then $\frac{x}{2} \in K$.

If X is a field of non-zero characteristic p, then obviously, (i) holds true.

Let ξ and η be independent identically distributed random variables with values in X and distribution $\mu = m_K * E_x$. It follows from (i) that then $\xi + \eta$ and $\xi - \eta$ are independent ([9, §7])). Hence, the random variables S and D are also independent. □

Remark 1. Let X be an arbitrary non-discrete totally disconnected locally compact field. Comparing Theorems A and 1, we note that, generally speaking,

it is not true that if a characterization theorem holds for a field $\mathbb{Q}_p$, then it holds for X. Below we give an example of a characterization theorem which holds true when $X = \mathbb{Q}_p$, where $p > 2$, but fails, generally speaking, for an arbitrary X.

Denote by $\mathrm{Aut}(X)$ the set of all topological automorphisms of the additive group of the field X, by I the identity automorphism of X, and by $S(X)$ the subset of $\mathrm{Aut}(X)$ consisting of those $\alpha \in \mathrm{Aut}(X)$ which have the following property: there exists a nonzero compact subgroup K of X such that $\alpha(K) = (I+\alpha)(K) = K$. The following statement follows from the main theorem proved in [12].

Theorem B. *Let $X = \mathbb{Q}_p$, where $p > 2$. Let α be a topological automorphism of the additive group of the field X. Let ξ_1 and ξ_2 be independent random variables with values in X and distributions μ_1 and μ_2. The symmetry of the conditional distribution of the linear form $L_2 = \xi_1 + \alpha\xi_2$ given $L_1 = \xi_1 + \xi_2$ implies that $\mu_1, \mu_2 \in I(X)$ if and only if $\alpha \in S(X)$.*

We will verify that, generally speaking, Theorem B fails if X is an arbitrary non-discrete totally disconnected locally compact field such that the residue field R/P is a field of characteristic $p > 2$. Assume that X is a field of characteristic zero. Then the additive group of the field X is topologically isomorphic to the group $\mathbb{Q}_p^m$ for some m. In order not to complicate the notation, we assume that $X = \mathbb{Q}_p^m$. Let $m > 1$. Any topological automorphism α of the additive group of the field X is defined by an reversible $(m \times m)$-matrix with elements of $\mathbb{Q}_p$. Assume that a diagonal matrix $\alpha_0 = \mathrm{diag}\{e, \dots, e, -e\}$ corresponds to a topological automorphism α_0. It follows from $p > 2$ that $I \in S(\mathbb{Q}_p)$, and hence, obviously, $\alpha_0 \in S(X)$.

It is not difficult to verify that if L_1 and L_2 are random variables with values in an arbitrary locally compact Abelian group, then the conditional distribution of the random variable L_2 given L_1 is symmetric if and only if the random vectors (L_1, L_2) and $(L_1, -L_2)$ are identically distributed. This implies that if η_1 and η_2 are independent identically distributed random variables with values in X, then the conditional distribution of the linear form $L_2 = \eta_1 - \eta_2$ given $L_1 = \eta_1 + \eta_2$ is symmetric. Let ξ_1 and ξ_2 be independent identically distributed random variables with values in X and distribution μ supported in the subgroup $G = \{0\}^{m-1} \times \mathbb{Q}_p$. Since the restriction of α_0 to G coincides with $-I$, it follows from what has been said above that the conditional distribution of the linear form $L_2 = \xi_1 + \alpha_0\xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric. Since μ is an arbitrary distribution, Theorem B fails for the field X.

References

[1] G. M. Feldman, Characterization of the Gaussian distribution on groups via the independence of linear statistics, *Siberian Math. J.* **31** (1990), 336–345.

[2] G. M. Feldman, On the Skitovich–Darmois theorem on abelian groups, *Theory Probab. Appl.* **37** (1993), 621–631.

[3] G. M. Feldman, On the Skitovich–Darmois theorem for compact groups, *Theory Probab. Appl.* **41** (1997), 768–773.

[4] G. M. Feldman, The Skitovich–Darmois theorem for discrete periodic abelian groups, *Theory Probab. Appl.* **42** (1998), 611–617.

[5] G. M. Feldman, A characterization of the Gaussian distribution on abelian groups, *Probab. Theory Related Fields* **126** (2003), 91–102.

[6] G. M. Feldman, On the Heyde theorem for finite abelian groups, *J. Theoret. Probab.* **17** (2004), 929–941.

[7] G. M. Feldman, On a characterization theorem for locally compact abelian groups, *Probab. Theory Related Fields* **133** (2005), 345–357.

[8] G. M. Feldman, On the Heyde theorem for discrete abelian groups, *Studia Math.* **177** (2006), 67–79.

[9] G. M. Feldman, Functional Equations and Characterization Problems on Locally Compact Abelian Groups, EMS Tracts in Mathematics, Vol. **5**, *European Mathematical Society (EMS)*, *Zurich*, 2008.

[10] G. M. Feldman, The Heyde theorem for locally compact abelian groups, *J. Funct. Anal.* **258** (2010), 3977–3987.

[11] G. M. Feldman, On a characterization of convolutions of Gaussian and Haar distributions, *Math. Nachr.* **286** (2013), 340–348.

[12] G. M. Feldman, On a characterization theorem for the group of p-adic numbers, *Publ. Math. Debrecen* **87** (2015), 147–166.

[13] G. M. Feldman and P. Graczyk, The Skitovich–Darmois theorem for locally compact abelian groups, *J. Aust. Math. Soc.* **88** (2010), 339–352.

[14] G. M. Feldman and M. V. Myronyuk, On a characterization of idempotent distributions on discrete fields and on the field of p-adic numbers, *J. Theoret. Probab.* **30** (2017), 608–623.

[15] R. C. Geary, The distribution of "Student's" ratio for non-normal samples, *Suppl. J. Roy. Statist. Soc.* **3** (1936), 178–184.

[16] P. Graczyk and J.-J. Loeb, A Bernstein property of measures on groups and symmetric spaces, *Probab. Math. Statist.* **20** (2000), 141–149.

[17] A. M. Kagan, Yu. V. Linnik and C. R. Rao, Characterization Problems in Mathematical Statistics, *John Wiley & Sons*, *New York – London – Sydney*, 1973.

[18] T. Kawata and H. Sakamoto, On the characterisation of the normal population by the independence of the sample mean and the sample variance, *J. Math. Soc. Japan* **1** (1949), 111–115.

[19] E. Lukacs, A characterization of the normal distribution, *Ann. Math. Statistics* **13** (1942), 91–93.

[20] M. Myronyuk, Heyde's characterization theorem for discrete abelian groups, *J. Aust. Math. Soc.* **88** (2010), 93–102.

[21] D. Neuenschwander and R. Schott, The Bernstein and Skitovič–Darmois characterization theorems for Gaussian distributions on groups, symmetric spaces, and quantum groups, *Exposition. Math.* **15** (1997), 289–314.

[22] A. Weil, Basic Number Theory, *Springer-Verlag*, *New York*, 1967.

[23] A. A. Zinger, On independent samples from normal populations, *Uspehi Matem. Nauk (N.S.)* **6** (1951), 172–175 (in *Russian*).

GENNADIY M. FELDMAN
B. VERKIN INSTITUTE FOR
LOW TEMPERATURE PHYSICS
AND ENGINEERING OF
THE NATIONAL ACADEMY OF
SCIENCES OF UKRAINE
47, NAUKY AVE
KHARKIV, 61103
UKRAINE

E-mail: feldman@ilt.kharkov.ua

MARGARYTA V. MYRONYUK
B. VERKIN INSTITUTE FOR
LOW TEMPERATURE PHYSICS
AND ENGINEERING OF
THE NATIONAL ACADEMY OF
SCIENCES OF UKRAINE
47, NAUKY AVE
KHARKIV, 61103
UKRAINE

E-mail: myronyuk@ilt.kharkov.ua

(Received November 14, 2018; revised May 28, 2019)