On a characterization theorem for the group of p-adic numbers

By GENNADIY FELDMAN (Kharkov)

Abstract. It is well known Heyde's characterization of the Gaussian distribution on the real line: Let $\xi_1, \xi_2, \ldots, \xi_n$, $n \geq 2$, be independent random variables, let α_j, β_j be nonzero constants such that $\beta_i \alpha_i^{-1} + \beta_j \alpha_j^{-1} \neq 0$ for all $i \neq j$. If the conditional distribution of the linear form $L_2 = \beta_1 \xi_1 + \beta_2 \xi_2 + \cdots + \beta_n \xi_n$ given $L_1 = \alpha_1 \xi_1 + \alpha_2 \xi_2 + \cdots + \alpha_n \xi_n$ is symmetric, then all random variables ξ_j are Gaussian. We prove an analogue of this theorem for two independent random variables in the case when they take values in the group of p-adic numbers Ω_p, and coefficients of linear forms are topological automorphisms of Ω_p.

1. Introduction

It is well known Heyde's characterization of the Gaussian distribution on the real line by the symmetry of the conditional distribution of one linear form given another ([8], see also [9, §13.4.1]):

Theorem A. *Let $\xi_1, \xi_2, \ldots, \xi_n$, $n \geq 2$, be independent random variables, let α_j, β_j be nonzero constants such that $\beta_i \alpha_i^{-1} + \beta_j \alpha_j^{-1} \neq 0$ for all $i \neq j$. If the conditional distribution of the linear form $L_2 = \beta_1 \xi_1 + \beta_2 \xi_2 + \cdots + \beta_n \xi_n$ given $L_1 = \alpha_1 \xi_1 + \alpha_2 \xi_2 + \cdots + \alpha_n \xi_n$ is symmetric, then all random variables ξ_j are Gaussian.*

Let X be a second countable locally compact Abelian group, $\mathrm{Aut}(X)$ be the group of topological automorphisms of X, ξ_j, $j = 1, 2, \ldots, n$, $n \geq 2$, be independent random variables with values in X and distributions μ_j. Consider

the linear forms $L_1 = \alpha_1 \xi_1 + \alpha_2 \xi_2 + \cdots + \alpha_n \xi_n$ and $L_2 = \beta_1 \xi_1 + \beta_2 \xi_2 + \cdots + \beta_n \xi_n$, where $\alpha_j, \beta_j \in \text{Aut}(X)$. We formulate the general problem.

Problem 1. *Let X be a given group. Describe distributions μ_j assuming that the conditional distribution of L_2 given L_1 is symmetric. In particular, for which groups X the symmetry of the conditional distribution of L_2 given L_1 implies that all μ_j are either Gaussian distributions or belong to a class of distributions which we can consider as a natural analogue of the class of Gaussian distributions.*

This problem for different classes of locally compact Abelian groups was studied in series articles (see [1]–[3], [5], [6], [10]–[12]). In this article we continue these investigations. We study Problem 1 for two independent random variables with values in the group of p-adic numbers.

We will use some results of the duality theory for locally compact Abelian groups (see e.g. [7]). Before we formulate the main theorem remind some definitions and agree on notation. For an arbitrary locally compact Abelian group X let $Y = X^*$ be its character group, and (x, y) be the value of a character $y \in Y$ at an element $x \in X$. If K is a closed subgroup of X, we denote by $A(Y, K) = \{y \in Y : (x, y) = 1 \text{ for all } x \in K\}$ its annihilator. If $\delta : X \mapsto X$ is a continuous endomorphism, then the adjoint endomorphism $\widetilde{\delta} : Y \mapsto Y$ is defined by the formula $(x, \widetilde{\delta}y) = (\delta x, y)$ for all $x \in X$, $y \in Y$. We note that $\delta \in \text{Aut}(X)$ if and only if $\widetilde{\delta} \in \text{Aut}(Y)$. Denote by I the identity automorphism of a group.

Let $M^1(X)$ be the convolution semigroup of probability distributions on X. For a distribution $\mu \in M^1(X)$ denote by $\widehat{\mu}(y) = \int_X (x, y) d\mu(x)$ its characteristic function. If H is a closed subgroup of Y and $\widehat{\mu}(y) = 1$ for $y \in H$, then $\widehat{\mu}(y + h) = \widehat{\mu}(y)$ for all $y \in Y$, $h \in H$. For $\mu \in M^1(X)$, we define the distribution $\bar{\mu} \in M^1(X)$ by the formula $\bar{\mu}(E) = \mu(-E)$ for any Borel set $E \subset X$. Observe that $\widehat{\bar{\mu}}(y) = \overline{\widehat{\mu}(y)}$. Let K be a compact subgroup of X. Note that the characteristic function of the Haar distribution m_K is of the form

$$\widehat{m}_K(y) = \begin{cases} 1, & y \in A(Y, K); \\ 0, & y \notin A(Y, K). \end{cases} \tag{1}$$

Denote by $I(X)$ the set of the idempotent distributions on X, i.e. the set of shifts of the Haar distributions m_K of compact subgroups K of X.

2. The main theorem

Let p be a prime number. We need some properties of the group of p-adic numbers Ω_p (see e.g. [7, §10]). As a set Ω_p coincides with the set of sequences of integers of the form $x = (\ldots, x_{-n}, x_{-n+1}, \ldots, x_{-1}, x_0, x_1, \ldots, x_n, \ldots)$, where $x_n \in \{0, 1, \ldots, p-1\}$, such that $x_n = 0$ for $n < n_0$, where the number n_0 depends on x. Correspond to each element $x \in \Omega_p$ the series $\sum_{k=-\infty}^{\infty} x_k p^k$. Addition and multiplication of series are defined in a natural way and define the operations of addition and multiplication in Ω_p. With respect to these operations Ω_p is a field. Denote by Δ_p a subgroup of Ω_p consisting of $x \in \Omega_p$ such that $x_n = 0$ for $n < 0$. This subgroup is called the group of p-adic integers. Elements of the group Δ_p we write in the form $x = (x_0, x_1, \ldots, x_n, \ldots)$. The family of subgroups $\{p^m \Delta_p\}_{m=-\infty}^{\infty}$ can be considered as an open basis at zero of the group Ω_p and defines a topology on Ω_p. With respect to this topology the group Ω_p is locally compact, noncompact, and totally disconnected. The character group Ω_p^* of the group Ω_p is topologically isomorphic to Ω_p, and the value of a character $y \in \Omega_p^*$ at an element $x \in \Omega_p$ is defined by the formula

$$(x, y) = \exp\left[2\pi i \left(\sum_{n=-\infty}^{\infty} x_n \left(\sum_{s=n}^{\infty} y_{-s} p^{-s+n-1} \right) \right) \right]$$

([7, (25.1)]).

Each automorphism $\alpha \in \mathrm{Aut}(\Omega_p)$ is the multiplication by an element $x_\alpha \in \Omega_p$, $x_\alpha \neq 0$, i.e. $\alpha g = x_\alpha g$, $g \in \Omega_p$. If $\alpha \in \mathrm{Aut}(\Omega_p)$, in order not to complicate notation, we will identify the automorphism α with the corresponding element x_α, i.e. when we write αg, we will suppose that $\alpha \in \Omega_p$. We note that $\widetilde{\alpha} = \alpha$. Denote by Δ_p^0 the subset of Δ_p, consisting of all invertible elements of Δ_p, $\Delta_p^0 = \{x = (x_0, x_1, \ldots, x_n, \ldots) \in \Delta_p : x_0 \neq 0\}$. Obviously, each element $g \in \Omega_p$ is represented in the form $g = p^k c$, where k is an integer, and $c \in \Delta_p^0$. It is obvious that the multiplication by c is a topological automorphism of the group $p^m \Delta_p$ for any integer m.

For a fixed prime p denote by $\mathbf{Z}(p^\infty)$ the set of rational numbers of the form

$$\left\{ \frac{k}{p^n} : k = 0, 1, \ldots, p^n - 1, n = 0, 1, \ldots \right\}$$

and define the operation in $\mathbf{Z}(p^\infty)$ as addition modulo 1. Then $\mathbf{Z}(p^\infty)$ is transformed into an Abelian group, which we consider in the discrete topology. Obviously, this group is topologically isomorphic to the multiplicative group of p^nth roots of unity, where n goes through the nonnegative integers, considering in the

discrete topology. For a fixed n denote by $\mathbf{Z}(p^n)$ the subgroup of $\mathbf{Z}(p^\infty)$ consisting of all elements of the form $\left\{ \frac{k}{p^n} : k = 0, 1, \ldots, p^n - 1 \right\}$. The group $\mathbf{Z}(p^n)$ is isomorphic to the multiplicative group of p^nth roots of unity.

Let $\alpha \in \mathrm{Aut}(\Omega_p)$, $\alpha = p^k c$, where $k \geq 0$, $c \in \Delta_p^0$. Let l be an integer. It is easy to see that α induces an epimorphism $\bar{\alpha}$ and c induces an automorphism $\bar{c}$ on the factor-group $\Omega_p / p^l \Delta_p$. Let

$$x = (\ldots, x_{-n}, x_{-n+1}, \ldots, x_{-1}, x_0, x_1, \ldots, x_n, \ldots) \in \Omega_p.$$

Define the mapping $\tau : \Omega_p / p^l \Delta_p \mapsto \mathbf{Z}(p^\infty)$ by the formula

$$\tau(x + p^l \Delta_p) = \sum_{n=-\infty}^{l-1} x_n p^{n-l}, \quad x + p^l \Delta_p \in \Omega_p / p^l \Delta_p. \tag{2}$$

Then τ is a topological isomorphism of the groups $\Omega_p / p^l \Delta_p$ and $\mathbf{Z}(p^\infty)$. Put

$$\widehat{\alpha} = \tau \bar{\alpha} \tau^{-1}, \quad \widehat{c} = \tau \bar{c} \tau^{-1}, \tag{3}$$

and observe that $\widehat{\alpha} = p^k \widehat{c}$, $\widehat{c} \in \mathrm{Aut}(\mathbf{Z}(p^\infty))$, and $\widehat{\alpha}$ is an epimorphism. If $c = (c_0, c_1, \ldots, c_n, \ldots) \in \Delta_p^0$, then the automorphism $\widehat{c}$ acts in the following way. Put $s_n = c_0 + c_1 p + c_2 p^2 + \cdots + c_{n-1} p^{n-1}$. The restriction of the automorphism $\widehat{c}$ to the subgroup $\mathbf{Z}(p^n) \subset \mathbf{Z}(p^\infty)$ is of the form $\widehat{c} y = s_n y$, $y \in \mathbf{Z}(p^n)$, i.e. $\widehat{c}$ acts in $\mathbf{Z}(p^n)$ as the multiplication by s_n.

We note that since Ω_p is a totally disconnected group, the Gaussian distributions on Ω_p are degenerated ([13, Ch. 4]), and the class of idempotent distributions on Ω_p can be considered as a natural analog of the class of Gaussian distributions.

We consider the case of two independent random variables ξ_1 and ξ_2 with values in the group $X = \Omega_p$, i.e. we consider the linear forms $L_1 = \alpha_1 \xi_1 + \alpha_2 \xi_2$ and $L_2 = \beta_2 \xi_1 + \beta_2 \xi_2$, where $\alpha_j, \beta_j \in \mathrm{Aut}(X)$. Assume that the conditional distribution of the linear form $L_2 = \beta_2 \xi_1 + \beta_2 \xi_2$ given $L_1 = \alpha_1 \xi_1 + \alpha_2 \xi_2$ is symmetric. Our aim is to describe the possible distributions μ_j depending on α_j, β_j. Introducing the new independent random variables $\xi_j' = \alpha_j \xi_j$, $j = 1, 2$, we can suppose that $L_1 = \xi_1 + \xi_2$ and $L_2 = \delta_1 \xi_1 + \delta_2 \xi_2$, where $\delta_j \in \mathrm{Aut}(X)$. Note also that the conditional distribution of the linear form $L_2 = \delta_1 \xi_1 + \delta_2 \xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric if and only if the conditional distribution of δL_2, where $\delta \in \mathrm{Aut}(X)$, given L_1 is symmetric. It follows from this that we may assume that $L_2 = \xi_1 + \alpha \xi_2$, where $\alpha \in \mathrm{Aut}(X)$.

We can formulate now the main result of the article.

Theorem 1. *Let $X = \Omega_p$. Let $\alpha = p^k c$, where $k \in \mathbf{Z}$ and $c = (c_0, c_1, \ldots, c_n, \ldots) \in \Delta_p^0$, be an arbitrary topological automorphism of the group X. Then the following statements hold.*

1. *Let ξ_1 and ξ_2 be independent random variables with values in X and distributions μ_1 and μ_2. Assume that the conditional distribution of the linear form $L_2 = \xi_1 + \alpha \xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric. Then*

   1(i) *If $p > 2$, $k = 0$ and $c_0 \neq p - 1$, then $\mu_j = m_K * E_{x_j}$, where K is a compact subgroup of X and $x_j \in X$. Moreover, if $c_0 = 1$, then μ_1 and μ_2 are degenerate distributions.*

   1(ii) *If $p = 2$, $k = 0$, $c_0 = 1$ and $c_1 = 0$, then μ_1 and μ_2 are degenerate distributions.*

   1(iii) *If $p > 2$ and $|k| = 1$, then either $\mu_1 \in I(X)$ or $\mu_2 \in I(X)$.*

2. *If one of the following conditions holds:*

   2(i) *$p > 2$, $k = 0$, $c_0 = p - 1$;*

   2(ii) *$p = 2$, $k = 0$, $c_0 = c_1 = 1$;*

   2(iii) *$p = 2$, $|k| = 1$;*

   2(iv) *$p \geq 2$, $|k| \geq 2$,*

   then there exist independent random variables ξ_1 and ξ_2 with values in X and distributions μ_1 and μ_2 such that the conditional distribution of the linear form $L_2 = \xi_1 + \alpha \xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric whereas $\mu_1, \mu_2 \notin I(X)$.

It is easy to see that cases 1(i)–1(iii) and 2(i)–2(iv) exhaust all possibilities for p and α.

3. Lemmas

To prove Theorem 1 we need some lemmas.

Lemma 1 ([3], see also [4, §16])**.** *Let X be a second countable locally compact Abelian group, Y be its character group. Let ξ_1 and ξ_2 be independent random variables with values in X and distributions μ_1 and μ_2. Let α_j, β_j be continuous endomorphisms of X. The conditional distribution of the linear form $L_2 = \beta_1 \xi_1 + \beta_2 \xi_2$ given $L_1 = \alpha_1 \xi_1 + \alpha_2 \xi_2$ is symmetric if and only if the characteristic functions $\widehat{\mu}_j(y)$ satisfy the equation*

$$\widehat{\mu}_1(\widetilde{\alpha}_1 u + \widetilde{\beta}_1 v)\widehat{\mu}_2(\widetilde{\alpha}_2 u + \widetilde{\beta}_2 v) = \widehat{\mu}_1(\widetilde{\alpha}_1 u - \widetilde{\beta}_1 v)\widehat{\mu}_2(\widetilde{\alpha}_2 u - \widetilde{\beta}_2 v), \quad u, v \in Y. \quad (4)$$

Observe that in [3] this lemma is proved when $\alpha_j, \beta_j \in \mathrm{Aut}(X)$, but the proof is valid without any changes for the case when α_j, β_j are continuous endomorphisms.

Lemma 2. *Let $X = \Omega_p$, ξ_1 and ξ_2 be independent random variables with values in X and distributions μ_1 and μ_2 such that $\mu_j(y) \geq 0$, $j = 1, 2$. Let $\alpha = p^k c \in \mathrm{Aut}(X)$, where $k \in \mathbf{Z}$ and $c \in \Delta_p^0$. Assume also that $\alpha \neq -I$. If the conditional distribution of the linear form $L_2 = \xi_1 + \alpha \xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric, then there exists a closed subgroup $H \subset Y$, such that $\widehat{\mu}_j(y) = 1$ for $y \in H$, $j = 1, 2$.*

Proof. Taking into account that the conditional distribution of the linear form L_2 given L_1 is symmetric if and only if the conditional distribution of the linear form $\alpha^{-1} L_2$ given L_1 is symmetric, we may assume without loss of generality that $k \geq 0$. Apply Lemma 1. Since $X = \Omega_p$, we have $\widetilde{\alpha} = \alpha$, and hence equation (4) takes the form

$$\widehat{\mu}_1(u + v)\widehat{\mu}_2(u + \alpha v) = \widehat{\mu}_1(u - v)\widehat{\mu}_2(u - \alpha v), \quad u, v \in Y. \tag{5}$$

If $\alpha = I$, then put in equation (5) $u = v = y$. We get that $H = Y$, i.e. μ_1, and μ_2 are degenerate distributions. So, we will assume that $\alpha \neq I$. Since $\widehat{\mu}_1(0) = \widehat{\mu}_2(0) = 1$, we can choose a neighborhood at zero V of Y such that $\widehat{\mu}_j(y) > 0$ for $y \in V$, $j = 1, 2$. Obviously, we can assume that $V = p^l \Delta_p$ for some l. Since $k \geq 0$, we have $\alpha(p^l \Delta_p) \subset p^l \Delta_p$. Put $\psi_j(y) = -\log \widehat{\mu}_j(y)$, $y \in p^l \Delta_p$, $j = 1, 2$. It follows from (5) that the functions $\psi_1(y)$ and $\psi_2(y)$ satisfy the equation

$$\psi_1(u + v) + \psi_2(u + \alpha v) - \psi_1(u - v) - \psi_2(u - \alpha v) = 0, \quad u, v \in p^l \Delta_p. \tag{6}$$

We use the finite difference method to solve equation (6). Let $\psi(y)$ be a function on Y, and h be an arbitrary element of Y. Denote by Δ_h the finite difference operator

$$\Delta_h \psi(y) = \psi(y + h) - \psi(y).$$

Let k_1 be an arbitrary element of $p^l \Delta_p$. Put $h_1 = \alpha k_1$ and hence, $h_1 - \alpha k_1 = 0$. Substitute $u + h_1$ for u and $v + k_1$ for v in equation (6). Subtracting equation (6) from the obtained equation we find

$$\Delta_{l_{11}} \psi_1(u + v) + \Delta_{l_{12}} \psi_2(u + \alpha v) - \Delta_{l_{13}} \psi_1(u - v) = 0, \quad u, v \in p^l \Delta_p, \tag{7}$$

where $l_{11} = (\alpha + I)k_1$, $l_{12} = 2\alpha k_1$, $l_{13} = (\alpha - I)k_1$. Let k_2 be an arbitrary element of $p^l \Delta_p$. Put $h_2 = k_2$ and hence, $h_2 - k_2 = 0$. Substitute $u + h_2$ for u and $v + k_2$

for v in equation (7). Subtracting equation (7) from the obtained equation we arrive at

$$\Delta_{l_{21}}\Delta_{l_{11}}\psi_1(u+v) + \Delta_{l_{22}}\Delta_{l_{12}}\psi_2(u+\alpha v) = 0, \quad u,v \in p^l\Delta_p, \tag{8}$$

where $l_{21} = 2k_2$, $l_{22} = (I+\alpha)k_2$. Let k_3 be an arbitrary element of $p^l\Delta_p$. Put $h_3 = -\alpha k_3$ and hence, $h_3 + \alpha k_3 = 0$. Substitute $u + h_3$ for u and $v + k_3$ for v in equation (8). Subtracting equation (8) from the obtained equation we find

$$\Delta_{l_{31}}\Delta_{l_{21}}\Delta_{l_{11}}\psi_1(u+v) = 0, \quad u,v \in p^l\Delta_p, \tag{9}$$

where $l_{31} = (I - \alpha)k_3$. Substituting $v = 0$ into (9), taking into account the expressions for l_{11}, l_{21}, l_{31} and the fact that k_1, k_2, k_3 are arbitrary elements of $p^l\Delta_p$, we find from (9) that there exists a subgroup $p^m\Delta_p \subset p^l\Delta_p$, where the function $\psi_1(y)$ satisfies the equation

$$\Delta_h^3\psi_1(y) = 0, \quad h,y \in p^m\Delta_p. \tag{10}$$

Taking into account that $p^m\Delta_p$ is a compact group, we conclude from (10) that $\psi_1(y) = const$, $y \in p^m\Delta_p$ ([4, §5]). Since $\psi_1(0) = 0$, we have $\psi_1(y) = 0$, for $y \in p^m\Delta_p$. This implies that $\widehat{\mu}_1(y) = 1$ for $y \in p^m\Delta_p$. For the distribution μ_2 we reason similarly and find a subgroup $p^n\Delta_p$ such that $\widehat{\mu}_2(y) = 1$ for $y \in p^n\Delta_p$. Put $H = p^m\Delta_p \cap p^n\Delta_p$. Lemma 2 is proved. $\qquad\square$

Lemma 3 ([1], see also [4, §17]). *Let X be a finite Abelian group containing no elements of order 2, α be an automorphism of X such that $I \pm \alpha \in \mathrm{Aut}(X)$. Let ξ_1 and ξ_2 be independent random variables with values in the group X and distributions μ_1 and μ_2. If the conditional distribution of the linear form $L_2 = \xi_1 + \alpha\xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric, then $\mu_j = m_K * E_{x_j}$, where K is a finite subgroup of X and $x_j \in X$, $j = 1, 2$.*

4. Proof of statements 1(i)–1(iii)

Before we begin the proof make the following remarks. It is obvious that the characteristic functions of the distributions $\bar{\mu}_j$ also satisfy equation (5). This implies that the characteristic functions of the distributions $\nu_j = \mu_j * \bar{\mu}_j$ satisfy equation (5) too. We have $\widehat{\nu}_j(y) = |\widehat{\mu}_j(y)|^2 \geq 0$, $j = 1, 2$. Hence, when we prove statements 1(i)–1(iii) we may assume without loss of generality that $\mu_j(y) \geq 0$, $j = 1, 2$, because μ_j and ν_j are idempotent distributions or degenerate distributions simultaneously.

Taking into account that the conditional distribution of the linear form L_2 given L_1 is symmetric if and only if the conditional distribution of the linear form $\alpha^{-1}L_2$ given L_1 is symmetric, we may assume without loss of generality that $k \geq 0$.

Put $f(y) = \widehat{\mu}_1(y)$, $g(y) = \widehat{\mu}_2(y)$ and write equation (5) in the form

$$f(u+v)g(u+\alpha v) = f(u-v)g(u-\alpha v), \quad u, v \in Y, \tag{11}$$

where $\alpha \in \mathrm{Aut}(Y)$, $\alpha = p^k c$, $k \geq 0$, $c \in \Delta_p^0$. We also assume that $f(y) \geq 0$, $g(y) \geq 0$. In fact we will study solutions of equation (11).

PROOF OF STATEMENTS 1(i) AND 1(ii). By Lemma 1, the characteristic functions $f(y)$ and $g(y)$ satisfy equation (11). Put

$$E = \{y \in Y : f(y) = g(y) = 1\}. \tag{12}$$

If either μ_1 or μ_1 is a nondegenerate distribution, then $E \neq \Omega_p$. Observe that in cases 1(i) and 1(ii) $\alpha \neq -I$. Then by Lemma 2, $E \neq \{0\}$. Thus, E is a nonzero proper closed subgroup of Ω_p, and hence $E = p^l \Delta_p$ for some l. It follows from (12) that

$$f(y+h) = f(y), \quad g(y+h) = g(y), \quad y \in Y, \ h \in p^l \Delta_p. \tag{13}$$

Taking into account (13), denote by $\bar{f}(y)$ and $\bar{g}(y)$ the functions induced by the functions $f(y)$ and $g(y)$ on the factor-group $Y/p^l \Delta_p$. Put $\widehat{f} = \bar{f} \circ \tau^{-1}$, where τ is defined by formula (2). We get from (11) that the functions $\widehat{f}(y)$ and $\widehat{g}(y)$ satisfy the equation

$$\widehat{f}(u+v)\widehat{g}(u+\widehat{\alpha}v) = \widehat{f}(u-v)\widehat{g}(u-\widehat{\alpha}v), \quad u, v \in \mathbf{Z}(p^\infty), \tag{14}$$

where $\widehat{\alpha}$ is defined by formula (3). It follows from (12) that

$$\{y \in \mathbf{Z}(p^\infty) : \widehat{f}(y) = \widehat{g}(y) = 1\} = \{0\}. \tag{15}$$

Statement 1(i). Assume first that $c_0 \neq 1$. Since $p > 2$, $k = 0$ and $c_0 \neq p - 1$, we have

$$I \pm \widehat{\alpha} \in \mathrm{Aut}(\mathbf{Z}(p^\infty)). \tag{16}$$

We note that for any n the restriction of any automorphism of the group $\mathbf{Z}(p^\infty)$ to the subgroup $\mathbf{Z}(p^n) \subset \mathbf{Z}(p^\infty)$ is an automorphism of the subgroup $\mathbf{Z}(p^n)$. Consider the restriction of equation (14) to the subgroup $\mathbf{Z}(p^n)$. Observe that

$(\mathbf{Z}(p^n))^* \cong \mathbf{Z}(p^n)$, and the group $\mathbf{Z}(p^n)$ contains no elements of order 2. Taking into account that (16) holds, we can apply Lemmas 1 and 3 to the group $\mathbf{Z}(p^n)$ and get that the restrictions of the characteristic functions $\widehat{f}(y)$ and $\widehat{g}(y)$ to the subgroup $\mathbf{Z}(p^n)$ take only two values: 0 and 1. Moreover, $\widehat{f}(y) = \widehat{g}(y)$ for $y \in \mathbf{Z}(p^n)$. Hence, the characteristic functions $\widehat{f}(y)$ and $\widehat{g}(y)$ on the group $\mathbf{Z}(p^\infty)$ take also only two values 0 and 1, and $\widehat{f}(y) = \widehat{g}(y)$ for $y \in \mathbf{Z}(p^\infty)$. Then the standard reasoning show that $\mu_j = m_K * E_{x_j}$, where K is a compact subgroup of X and $x_j \in X$.

Assume now that $c_0 = 1$. Since $k = 0$, the restriction of the automorphism $\widehat{\alpha}$ to $\mathbf{Z}(p) \subset \mathbf{Z}(p^\infty)$ is the identity automorphism. Hence, the restriction of equation (14) to $\mathbf{Z}(p)$ takes the form

$$\widehat{f}(u + v)\widehat{g}(u + v) = \widehat{f}(u - v)\widehat{g}(u - v), \quad u, v \in \mathbf{Z}(p). \tag{17}$$

Substituting here $u = v = y$, we get $\widehat{f}(2y)\widehat{g}(2y) = 1$, $y \in \mathbf{Z}(p)$. Since $p > 2$, this implies that

$$\widehat{f}(y) = \widehat{g}(y) = 1, \quad y \in \mathbf{Z}(p),$$

but this contradicts to (15). Thus, μ_1 and μ_2 are degenerate distributions.

Statement 1(ii). Since $k = 0$, $c_0 = 1$ and $c_1 = 0$, the restriction of the automorphism $\widehat{\alpha}$ to the subgroup $\mathbf{Z}(4) \subset \mathbf{Z}(2^\infty)$ is the identity automorphism. Hence, the restriction of equation (14) to the subgroup $\mathbf{Z}(4)$ takes the form (17), where $u, v \in \mathbf{Z}(4)$. Substituting in (17) $u = v = y$, we get

$$\widehat{f}(2y)\widehat{g}(2y) = 1, \quad y \in \mathbf{Z}(4).$$

This implies that $\widehat{f}(y) = \widehat{g}(y) = 1$ for $y \in \mathbf{Z}(2)$, but this contradicts to (15). Thus, μ_1 and μ_2 are degenerate distributions. $\qquad\square$

The proof of statement 1(iii) is based on the proof of the following proposition which is of interest in its own right.

Proposition 1. *Let $X = \Omega_p$, ξ_1 and ξ_2 be independent random variables with values in X and distributions μ_1 and μ_2. Let $\alpha \in \mathrm{Aut}(X)$, and $\alpha \neq -I$. If the conditional distribution of the linear form $L_2 = \xi_1 + \alpha\xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric, then either μ_1 and μ_2 are degenerate distributions or there exists a closed subgroup $M \subset Y$, such that $\widehat{\mu}_j(y) = 0$ for $y \notin M$, $j = 1, 2$.*

PROOF. Let $\alpha = p^k c \in \mathrm{Aut}(X)$, where $k \in \mathbf{Z}$ and $c \in \Delta_p^0$. We can assume without loss of generality that $k \geq 0$. Otherwise we consider the linear form $L_2 = \alpha^{-1}\xi_1 + \xi_2$ instead of $L_2 = \xi_1 + \alpha\xi_2$. Taking into account that in cases 1(i) and 1(ii) of Theorem 1 Proposition 1 holds, it remains to consider the following cases:

1. $p \geq 2$, $k \geq 1$;
2. $p > 2$, $k = 0$, $c_0 = p - 1$;
3. $p = 2$, $k = 0$, $c_0 = c_1 = 1$.

Obviously, we can assume without loss of generality that $\widehat{\mu}_j(y) \geq 0$, $j = 1, 2$. Put $f(y) = \widehat{\mu}_1(y)$, $g(y) = \widehat{\mu}_2(y)$. We have $f(-y) = f(y)$ and $g(-y) = g(y)$. Reasoning as in the proof of statements 1(i)–1(ii) and retaining the same notation we arrive at equation (14). Set $\beta = I - \alpha$, $\gamma = I + \alpha$. Substituting into equation (14) $u = v = y$, we obtain

$$\widehat{f}(2y)\widehat{g}(\widehat{\gamma}y) = \widehat{g}(\widehat{\beta}y), \quad y \in \mathbf{Z}(p^\infty). \tag{18}$$

Substituting into equation (14) $u = \widehat{\alpha}y$, $v = y$, we get

$$\widehat{f}(\widehat{\gamma}y)\widehat{g}(2\widehat{\alpha}y) = \widehat{f}(\widehat{\beta}y), \quad y \in \mathbf{Z}(p^\infty). \tag{19}$$

1. $p \geq 2$, $k \geq 1$. Since $k \geq 1$, we have $\widehat{\beta}, \widehat{\gamma} \in \mathrm{Aut}(\mathbf{Z}(p^\infty))$. Put $\kappa = \beta\gamma^{-1}$. Equations (18) and (19) imply

$$\widehat{g}(\widehat{\kappa}y) = \widehat{f}(2\widehat{\gamma}^{-1}y)\widehat{g}(y), \quad y \in \mathbf{Z}(p^\infty), \tag{20}$$

and

$$\widehat{f}(\widehat{\kappa}y) = \widehat{f}(y)\widehat{g}(2\widehat{\alpha}\widehat{\gamma}^{-1}y), \quad y \in \mathbf{Z}(p^\infty). \tag{21}$$

Since $0 \leq \widehat{f}(y) \leq 1$, it follows from (20) that

$$\widehat{g}(\widehat{\kappa}y) \leq \widehat{g}(y), \quad y \in \mathbf{Z}(p^\infty).$$

This implies that for any natural n the inequalities

$$\widehat{g}(\widehat{\kappa}^n y) \leq \cdots \leq \widehat{g}(\widehat{\kappa}y) \leq \widehat{g}(y), \quad y \in \mathbf{Z}(p^\infty), \tag{22}$$

hold. Let $y \in \mathbf{Z}(p^\infty)$. Then $y \in \mathbf{Z}(p^l)$ for some l, and hence $\widehat{\kappa}y \in \mathbf{Z}(p^l)$. It follows from this that $\widehat{\kappa}^m y = y$ for some m, depending generally speaking on y. Substituting in (22) $n = m$ we get

$$\widehat{g}(\widehat{\kappa}y) = \widehat{g}(y), \quad y \in \mathbf{Z}(p^\infty). \tag{23}$$

Reasoning similarly, we obtain from (21) that

$$\widehat{f}(\widehat{\kappa}y) = \widehat{f}(y), \quad y \in \mathbf{Z}(p^\infty). \tag{24}$$

Assume that there exists a sequence of elements $y_n \in \mathbf{Z}(p^\infty)$ such that:

(a) the order of element y_n is equal to p^{i_n}, $i_n \to \infty$;

(b) $\widehat{g}(y_n) \neq 0$.

Then it follows from (20) and (23) that,

$$\widehat{f}(2\widehat{\gamma}^{-1}y_n) = 1. \tag{25}$$

Suppose that $p > 2$. Then (25) implies that $\widehat{f}(y) = 1$ for $y \in \mathbf{Z}(p^{i_n})$, because the order of the element $2\widehat{\gamma}^{-1}y_n$ is equal to p^{i_n}, and hence the element $2\widehat{\gamma}^{-1}y_n$ generates the subgroup $\mathbf{Z}(p^{i_n})$. If $p = 2$, then $\widehat{f}(y) = 1$ for $y \in \mathbf{Z}(2^{i_n-1})$, because the order of the element $2\widehat{\gamma}^{-1}y_n$ is equal to 2^{i_n-1}, and the element $2\widehat{\gamma}^{-1}y_n$ generates the subgroup $\mathbf{Z}(2^{i_n-1})$. Thus, for $p \geq 2$ we have $\widehat{f}(y) = 1$ for $y \in \mathbf{Z}(p^\infty)$, and equation (14) implies that

$$\widehat{g}(u + \widehat{\alpha}v) = \widehat{g}(u - \widehat{\alpha}v), \quad u, v \in \mathbf{Z}(p^\infty).$$

It follows from this that $\widehat{g}(2\widehat{\alpha}y) = 1$ for $y \in \mathbf{Z}(p^\infty)$, and hence $\widehat{g}(y) = 1$ for $y \in \mathbf{Z}(p^\infty)$, because $2\widehat{\alpha}$ is an epimorphism. We proved that μ_1, and μ_2 are degenerate distributions.

The similar reasoning shows that if there exists a sequence of elements $z_n \in \mathbf{Z}(p^\infty)$ such that:

(a) the order of the element z_n is equal to p^{j_n}, $j_n \to \infty$;

(b) $\widehat{f}(z_n) \neq 0$,

then μ_1, and μ_2 are also degenerate distributions.

From what has been said it follows that if μ_1, and μ_2 are nondegenerate distributions, then there exists n such that $\widehat{f}(y) = \widehat{g}(y) = 0$ for $y \notin \mathbf{Z}(p^n)$. Proposition 1 in case 1 follows directly from this.

2. $p > 2$, $k = 0$, $c_0 = p - 1$. Since $p > 2$, we have $\widehat{\beta} \in \mathrm{Aut}(\mathbf{Z}(p^\infty))$. We find from equation (18) that

$$\widehat{g}(y) = \widehat{f}(2\widehat{\beta}^{-1}y)\widehat{g}(\widehat{\gamma}\widehat{\beta}^{-1}y), \quad y \in \mathbf{Z}(p^\infty). \tag{26}$$

Since $0 \leq \widehat{g}(y) \leq 1$, we find from (26) that

$$\widehat{g}(y) \leq \widehat{f}(2\widehat{\beta}^{-1}y), \quad y \in \mathbf{Z}(p^\infty). \tag{27}$$

Reasoning similarly we get from (19) that

$$\widehat{f}(y) = \widehat{f}(\widehat{\gamma}\widehat{\beta}^{-1}y)g(2\widehat{\alpha}\widehat{\beta}^{-1}y), \quad y \in \mathbf{Z}(p^\infty). \tag{28}$$

Taking into account that $0 \le \widehat{f}(y) \le 1$, this implies that

$$\widehat{f}(y) \le \widehat{g}(2\widehat{\alpha}\widehat{\beta}^{-1}y), \quad y \in \mathbf{Z}(p^\infty). \tag{29}$$

Inequalities (27) and (29) imply the inequalities

$$\widehat{g}(y) \le \widehat{f}(2\widehat{\beta}^{-1}y) \le \widehat{g}(4\widehat{\alpha}\widehat{\beta}^{-2}y),$$

$$\widehat{f}(y) \le \widehat{g}(2\widehat{\alpha}\widehat{\beta}^{-1}y) \le \widehat{f}(4\widehat{\alpha}\widehat{\beta}^{-2}y), \quad y \in \mathbf{Z}(p^\infty). \tag{30}$$

Reasoning as in the proof of case 1, we find from (30) that

$$\widehat{g}(y) = \widehat{g}(4\widehat{\alpha}\widehat{\beta}^{-2}y), \quad \widehat{f}(y) = \widehat{f}(4\widehat{\alpha}\widehat{\beta}^{-2}y), \quad y \in \mathbf{Z}(p^\infty). \tag{31}$$

We find from (30) and (31) that

$$\widehat{g}(y) = \widehat{f}(2\widehat{\beta}^{-1}y), \quad \widehat{f}(y) = \widehat{g}(2\widehat{\alpha}\widehat{\beta}^{-1}y), \quad y \in \mathbf{Z}(p^\infty). \tag{32}$$

It follows from (32) (28) and (26) that if $\widehat{g}(y_0) \ne 0$ for some $y_0 \in \mathbf{Z}(p^\infty)$, then $\widehat{g}(\widehat{\gamma}\widehat{\beta}^{-1}y_0) = 1$, and if $\widehat{f}(y_0) \ne 0$, then $\widehat{f}(\widehat{\gamma}\widehat{\beta}^{-1}y_0) = 1$. We complete the proof as in case 1.

3. $p = 2$, $k = 0$, $c_0 = c_1 = 1$. Put $\beta = 2\beta_1$, $\gamma = 2\gamma_1$. Then $\widehat{\beta}_1 \in \mathrm{Aut}(\mathbf{Z}(2^\infty))$, and $\widehat{\gamma}_1$ is an epimorphism. It follows from (18) that

$$\widehat{f}(y)\widehat{g}(\widehat{\gamma}_1 y) = \widehat{g}(\widehat{\beta}_1 y), \quad y \in \mathbf{Z}(2^\infty). \tag{33}$$

Similarly, we find from (19) that

$$\widehat{f}(\widehat{\gamma}_1 y)\widehat{g}(\widehat{\alpha} y) = \widehat{f}(\widehat{\beta}_1 y), \quad y \in \mathbf{Z}(2^\infty). \tag{34}$$

It follows from (33) and (34) that

$$\widehat{g}(y) = \widehat{f}(\widehat{\beta}_1^{-1}y)\widehat{g}(\widehat{\gamma}_1\widehat{\beta}_1^{-1}y), \quad \widehat{f}(y) = \widehat{f}(\widehat{\gamma}_1\widehat{\beta}_1^{-1}y)\widehat{g}(\widehat{\alpha}\widehat{\beta}_1^{-1}y), \quad y \in \mathbf{Z}(2^\infty).$$

Hence,

$$\widehat{g}(y) \le \widehat{f}(\widehat{\beta}_1^{-1}y), \quad \widehat{f}(y) \le \widehat{g}(\widehat{\alpha}\widehat{\beta}_1^{-1}y).$$

This implies that

$$\widehat{g}(y) \le \widehat{f}(\widehat{\beta}_1^{-1}y) \le \widehat{g}(\widehat{\alpha}\beta_1^{-2}y), \quad \widehat{f}(y) \le \widehat{g}(\widehat{\alpha}\widehat{\beta}_1^{-1}y) \le \widehat{f}(\widehat{\alpha}\widehat{\beta}_1^{-2}y).$$

We complete the proof as in case 2. Proposition 1 is proved completely. $\square$

PROOF OF STATEMENTS 1(iii). Observe that in case 1(iii) $\alpha \neq -I$. Reasoning as in the proof of statements 1(i) and 1(ii) and retaining the same notation we arrive at equation (14). Put

$$E_{\widehat{f}} = \{y \in \mathbf{Z}(p^\infty) : \widehat{f}(y) \neq 0\}, \quad E_{\widehat{g}} = \{y \in \mathbf{Z}(p^\infty) : \widehat{g}(y) \neq 0\},$$

$$B_{\widehat{f}} = \{y \in \mathbf{Z}(p^\infty) : \widehat{f}(y) = 1\}, \quad B_{\widehat{g}} = \{y \in \mathbf{Z}(p^\infty) : \widehat{g}(y) = 1\}.$$

Since $p > 2$ and $k = 1$, we have $2\widehat{\gamma}^{-1} \in \mathrm{Aut}(\mathbf{Z}(p^\infty))$. Moreover, since $k = 1$, obviously, (20), (21), (23) and (24) hold. Taking this into account, we find from (20) and (23) that $E_{\widehat{g}} \subset B_{\widehat{f}}$. Analogously, we find from (21) and (24) that $pE_{\widehat{f}} \subset B_{\widehat{g}}$. If μ_2 is a nondegenerate distribution, then $B_{\widehat{g}}$ is a proper subgroup of $\mathbf{Z}(p^\infty)$, and hence $B_{\widehat{g}} = \mathbf{Z}(p^n)$ for some n. Since $B_{\widehat{g}} \subset E_{\widehat{g}} \subset B_{\widehat{f}}$, it follows from (15) that $B_{\widehat{g}} = \{0\}$. If $B_{\widehat{f}} = \{0\}$, then $E_{\widehat{g}} \subset B_{\widehat{f}} = \{0\}$, and hence μ_2 is an idempotent distribution. If $B_{\widehat{f}} \neq \{0\}$, then $pB_{\widehat{f}} \subset pE_{\widehat{f}} \subset B_{\widehat{g}} = \{0\}$. This implies that $B_{\widehat{f}} = E_{\widehat{f}} = \mathbf{Z}(p)$, and hence μ_1 is an idempotent distribution. $\qquad\square$

5. Proof of statements 2(i)–2(iv)

Taking into account that the conditional distribution of the linear form L_2 given L_1 is symmetric if and only if the conditional distribution of the linear form $\alpha^{-1}L_2$ given L_1 is symmetric, we may assume without loss of generality that $k \geq 0$, and hence the restriction of $\alpha \in \mathrm{Aut}(\Omega_p)$ to the subgroup Δ_p is a continuous endomorphism of Δ_p. We retain the notation α for this restriction. We will construct in cases 2(i)–2(iv) independent random variables ξ_1 and ξ_2 with values in Δ_p and distributions μ_1 and μ_2 such that the conditional distribution of the linear form $L_2 = \xi_1 + \alpha\xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric, whereas $\mu_1, \mu_2 \notin I(\Delta_p)$. Considering ξ_j as independent random variables with values in Ω_p, we prove statements 2(i)–2(iv). Taking into account Lemma 1 it suffices to construct non-idempotent distributions μ_j on the group Δ_p such that their characteristic functions satisfy equation (5). We note that the groups $\mathbf{Z}(p^\infty)$ and Δ_p are the character groups of one another, and the value of a character $y = \frac{l}{p^n} \in \mathbf{Z}(p^\infty)$ at an element $x = (x_0, x_1, \ldots, x_n, \ldots) \in \Delta_p$ is defined by the formula

$$(x, y) = \exp\left\{\left(x_0 + x_1 p + \cdots + x_{n-1}p^{n-1}\right)\frac{2\pi i l}{p^n}\right\}.$$

Moreover, any topological automorphism of the group Δ_p is the multiplication by an element of Δ_p^0. For $c = (c_0, c_1, \ldots, c_n, \ldots) \in \Delta_p^0$, the restriction of the

automorphism $\widetilde{c} \in \text{Aut}(\mathbf{Z}(p^\infty))$ to the subgroup $\mathbf{Z}(p^n) \subset \mathbf{Z}(p^\infty)$ is of the form $\widetilde{c}y = s_n y$, $y \in \mathbf{Z}(p^n)$, where $s_n = c_0 + c_1 p + c_2 p^2 + \cdots + c_{n-1} p^{n-1}$. Observe also that $\widetilde{\alpha} = p^k \widetilde{c}$, and

$$A(\mathbf{Z}(p^\infty), p^l \Delta_p) = \mathbf{Z}(p^l). \tag{35}$$

Put $f(y) = \widehat{\mu}_1(y)$, $g(y) = \widehat{\mu}_2(y)$. In these notation equation (5) takes the form

$$f(u+v)g(u+\widetilde{\alpha}v) = f(u-v)g(u-\widetilde{\alpha}v), \quad u, v \in \mathbf{Z}(p^\infty). \tag{36}$$

Statement 2(i). Consider on the group Δ_p the distribution $\mu = am_{\Delta_p} + (1 - a)m_{p\Delta_p}$, where $0 < a < 1$. It follows from (1) and (35) that the characteristic function $\widehat{\mu}(y)$ is of the form

$$\widehat{\mu}(y) = \begin{cases} 1, & y = 0; \\ 1 - a, & y \in \mathbf{Z}(p); \\ 0, & y \notin \mathbf{Z}(p). \end{cases} \tag{37}$$

Let us check that the characteristic functions $f(y) = g(y) = \widehat{\mu}(y)$ satisfy equation (36). Consider 3 cases:

1. $u, v \in \mathbf{Z}(p)$. Since $c_0 = p - 1$, we have $\widetilde{\alpha}y = -y$ for $y \in \mathbf{Z}(p)$, and the restriction of equation (36) to the subgroup $\mathbf{Z}(p)$ takes the form

$$f(u+v)g(u-v) = f(u-v)g(u+v), \quad u, v \in \mathbf{Z}(p). \tag{38}$$

Since $f(y) = g(y)$, (38) holds.

2. Either $u \in \mathbf{Z}(p)$, $v \notin \mathbf{Z}(p)$, or $u \notin \mathbf{Z}(p)$, $v \in \mathbf{Z}(p)$. Then $u \pm v \notin \mathbf{Z}(p)$. This implies that $f(u \pm v) = 0$, and hence both sides of equation (36) are equal to zero.

3. $u, v \notin \mathbf{Z}(p)$. If $u + v, u + \widetilde{\alpha}v \in \mathbf{Z}(p)$, then

$$(I - \widetilde{\alpha})v \in \mathbf{Z}(p). \tag{39}$$

Since $p > 2$, $k = 0$ and $c_0 = p - 1$, we have $I - \alpha \in \text{Aut}(\Delta_p)$, and hence $I - \widetilde{\alpha} \in \text{Aut}(\mathbf{Z}(p^\infty))$. Then (39) implies that $v \in \mathbf{Z}(p)$, contrary to the assumption. Thus, either $u + v \notin \mathbf{Z}(p)$ or $u + \widetilde{\alpha}v \notin \mathbf{Z}(p)$, and the left-hand side of equation (36) is equal to zero. Similarly we check that the right-hand side of equation (36) is also equal to zero. Thus, (36) holds.

Statement 2(ii). Consider on the group Δ_2 the distribution $\mu = am_{\Delta_2} + (1-a)m_{2\Delta_2}$, where $0 < a < 1$. Then the characteristic function $\widehat{\mu}(y)$ is represented

by formula (37) for $p = 2$. Let us check that the characteristic functions $f(y) = g(y) = \widehat{\mu}(y)$ satisfy equation (36). Since $k = 0$ and $c_0 = c_1 = 1$, the restriction of the automorphism $\widetilde{\alpha} \in \mathrm{Aut}(\mathbf{Z}(2^\infty))$ to the subgroup $\mathbf{Z}(2^n) \subset \mathbf{Z}(2^\infty)$ is of the form $\widetilde{\alpha}y = my$, $y \in \mathbf{Z}(2^n)$, where $m = 1 + 2 + c_2 2^2 + \cdots + c_{n-1} 2^{n-1} = 4l - 1$. Consider 3 cases: 1. $u, v \in \mathbf{Z}(2)$; 2. either $u \in \mathbf{Z}(2)$, $v \notin \mathbf{Z}(2)$ or $u \notin \mathbf{Z}(2)$, $v \in \mathbf{Z}(2)$; 3. $u, v \notin \mathbf{Z}(2)$. In cases 1 and 2 the reasoning is the same as in case 2(i).

Consider case 3, i.e. assume that $u, v \notin \mathbf{Z}(2)$, and prove first that if $u + v, u + \widetilde{\alpha}v \in \mathbf{Z}(2)$, then $u - v, u - \widetilde{\alpha}v \in \mathbf{Z}(2)$, and (36) holds. To prove this note that the inclusions $u + v, u + \widetilde{\alpha}v \in \mathbf{Z}(2)$ are possible only in the following cases.

(a) $u + v = 0$ and $u + \widetilde{\alpha}v = 0$. This implies that $(\widetilde{\alpha} - I)v = (m - 1)v = 2(2l - 1)v = 0$. Hence, $v \in \mathbf{Z}(2)$, but this contradicts to the assumption.

(b) $u + v = \frac{1}{2}$ and $u + \widetilde{\alpha}v = \frac{1}{2}$. The reasoning is the same as in case (a).

(c) $u + v = 0$ and $u + \widetilde{\alpha}v = \frac{1}{2}$. This implies that $(\widetilde{\alpha} - I)v = (m - 1)v = 2(2l - 1)v = \frac{1}{2}$. It follows from this that either $v = \frac{1}{4}$, $u = \frac{3}{4}$, or $v = \frac{3}{4}$, $u = \frac{1}{4}$. In both cases $u - v = \frac{1}{2}$, $u - \widetilde{\alpha}v = u - mv = 0$, and hence (36) holds.

(d) $u + v = \frac{1}{2}$, $u + \widetilde{\alpha}v = 0$. The reasoning is the same as in case (c).

Reasoning similarly we verify that if $u - v, u - \widetilde{\alpha}v \in \mathbf{Z}(2)$, then $u + v, u + \widetilde{\alpha}v \in \mathbf{Z}(2)$, and (36) holds.

Statement 2(iii). Consider on the group Δ_2 the distributions $\mu_1 = am_{2\Delta_2} + (1 - a)m_{4\Delta_2}$ and $\mu_2 = am_{\Delta_2} + (1 - a)m_{2\Delta_2}$, where $0 < a < 1$. It follows from (1) and (35) that that the characteristic function $\widehat{\mu}_1(y)$ is of the form

$$\widehat{\mu}_1(y) = \begin{cases} 1, & y \in \mathbf{Z}(2); \\ 1 - a, & y \in \mathbf{Z}(4); \\ 0, & y \notin \mathbf{Z}(4). \end{cases}$$

Moreover, the characteristic function $\widehat{\mu}_2(y)$ is represented by formula (37) for $p = 2$. Let us check that the characteristic functions $f(y) = \widehat{\mu}_1(y)$ and $g(y) = \widehat{\mu}_2(y)$ satisfy equation (36). Consider 3 cases:

1. $u, v \in \mathbf{Z}(4)$. Obviously, we can assume that $u \neq 0$, $v \neq 0$. Since either $c_0 = 1$, $c_1 = 0$ or $c_0 = c_1 = 1$, the restriction of the automorphism $\widetilde{c}$ to the subgroup $\mathbf{Z}(4)$ is of the form: either $\widetilde{c}y = y$ or $\widetilde{c}y = -y$, $y \in \mathbf{Z}(4)$. Thus, the restriction of equation (36) to the subgroup $\mathbf{Z}(4)$ either takes the form

$$f(u + v)g(u + 2v) = f(u - v)g(u - 2v), \quad u, v \in \mathbf{Z}(4), \tag{40}$$

or

$$f(u + v)g(u - 2v) = f(u - v)g(u + 2v), \quad u, v \in \mathbf{Z}(4). \tag{41}$$

Consider equation (40). Equation (41) can be considered analogously.

(a) $u = v = \frac{1}{2}$. Then $u \pm v = 0$, $2v = 0$. Hence, $f(u \pm v) = 1$, $g(u \pm 2v) = g(u)$ and (40) holds.

(b) $u = \frac{1}{2}$, $v \in \{\frac{1}{4}, \frac{3}{4}\}$. Then $f(u \pm v) = f(v)$. Since $u \pm 2v = 0$, we have $g(u \pm 2v) = 1$, and (40) holds.

(c) $u \in \{\frac{1}{4}, \frac{3}{4}\}$, $v = \frac{1}{2}$. Then $f(u \pm v) = f(u)$. Since $2v = 0$, we have $g(u \pm 2v) = g(u)$, and (40) holds.

(d) $u, v \in \{\frac{1}{4}, \frac{3}{4}\}$. This implies that $u \pm 2v \notin \mathbf{Z}(2)$. Hence $g(u \pm 2v) = 0$, and both sides of equation (40) are equal to zero.

2. Either $u \in \mathbf{Z}(4)$, $v \notin \mathbf{Z}(4)$ or $u \notin \mathbf{Z}(4)$, $v \in \mathbf{Z}(4)$. Then $u \pm v \notin \mathbf{Z}(4)$. Hence $f(u \pm v) = 0$ and both sides of equation (40) are equal to zero.

3. $u, v \notin \mathbf{Z}(4)$. If $u + v \in \mathbf{Z}(4)$ and $u + \widetilde{\alpha}v \in \mathbf{Z}(2)$, then

$$(I - \widetilde{\alpha})v \in \mathbf{Z}(4). \tag{42}$$

Since $k = 1$, we have $I - \alpha \in \mathrm{Aut}(\Delta_2)$, and hence $I - \widetilde{\alpha} \in \mathrm{Aut}(\mathbf{Z}(2^\infty))$. Then (42) implies that $v \in \mathbf{Z}(4)$, contrary to the assumption. Hence, either $u + v \notin \mathbf{Z}(4)$ or $u + \widetilde{\alpha}v \notin \mathbf{Z}(2)$. This implies that the left-hand side of equation (36) is equal to zero. Reasoning analogously, we verify that the right-hand side of equation (36) is also equal to zero. Thus, (36) holds.

Statement 2(iv). Consider on the group Δ_p the distributions $\mu_1 = am_{p^{k-1}\Delta_p} + (1-a)m_{p^k\Delta_p}$ and $\mu_2 = am_{\Delta_p} + (1-a)m_{p^{k-1}\Delta_p}$, where $0 < a < 1$. It follows from (1) and (35) that the characteristic functions $\widehat{\mu}_1(y)$ and $\widehat{\mu}_2(y)$ are of the form

$$\widehat{\mu}_1(y) = \begin{cases} 1, & y \in \mathbf{Z}(p^{k-1}); \\ 1-a, & y \in \mathbf{Z}(p^k) \setminus \mathbf{Z}(p^{k-1}); \\ 0, & y \notin \mathbf{Z}(p^k). \end{cases}$$

$$\widehat{\mu}_2(y) = \begin{cases} 1, & y = 0; \\ 1-a, & y \in \mathbf{Z}(p^{k-1}) \setminus \{0\}; \\ 0, & y \notin \mathbf{Z}(p^{k-1}). \end{cases} \tag{43}$$

Let us check that the characteristic functions $f(y) = \widehat{\mu}_1(y)$ and $g(y) = \widehat{\mu}_2(y)$ satisfy equation (36). Consider 3 cases:

1. $u, v \in \mathbf{Z}(p^k)$. Since $\alpha = p^k c$, we have $\widetilde{\alpha}v = 0$, and hence the restriction of equation (36) to the subgroup $\mathbf{Z}(p^k)$ takes the form

$$f(u + v)g(u) = f(u - v)g(u), \quad u, v \in \mathbf{Z}(p^k). \tag{44}$$

(a) $u \in \mathbf{Z}(p^{k-1})$. Then $f(u \pm v) = f(v)$, and equation (44) holds.

(b) $u \in \mathbf{Z}(p^k)\backslash\mathbf{Z}(p^{k-1})$. Then $g(u) = 0$, and both sides of equation (44) are equal to zero.

2. Either $u \in \mathbf{Z}(p^k)$, $v \notin \mathbf{Z}(p^k)$ or $u \notin \mathbf{Z}(p^k)$, $v \in \mathbf{Z}(p^k)$. Then $u \pm v \notin \mathbf{Z}(p^k)$. This implies that $f(u \pm v) = 0$, and both sides of equation (36) are equal to zero.

3. $u, v \notin \mathbf{Z}(p^k)$. If $u + v \in \mathbf{Z}(p^k)$, $u + \widetilde{\alpha}v \in \mathbf{Z}(p^{k-1})$, then

$$(I - \widetilde{\alpha})v \in \mathbf{Z}(p^k). \tag{45}$$

Since $k \geq 1$, we have $I - \alpha \in \mathrm{Aut}(\Delta_p)$, and hence $I - \widetilde{\alpha} \in \mathrm{Aut}(\mathbf{Z}(p^\infty))$. Then (45) implies that $v \in \mathbf{Z}(p^k)$, contrary to the assumption. Hence, either $u + v \notin \mathbf{Z}(p^k)$ or $u + \widetilde{\alpha}v \notin \mathbf{Z}(p^{k-1})$. This implies that the left-hand side of equation (36) is equal to zero. Reasoning analogously, we verify that the right-hand side of equation (36) is also equal to zero. Thus, (36) holds. Theorem 1 is proved.

Let $X = \Delta_p$. We remind that each automorphism $\alpha \in \mathrm{Aut}(\Delta_p)$ is the multiplication by an element $c_\alpha \in \Delta_p^0$. Let ξ_1 and ξ_2 be independent random variables with values in the group Δ_p. Then we can consider ξ_j as independent random variables with values in the group Ω_p. Moreover, it is obvious that the multiplication by an element $c \in \Delta_p^0$ is a topological isomorphism of the group Ω_p. This implies that statements 1(i) and 1(ii) in Theorem 1 are also valid for the group Δ_p. Taking into account that in the proof of statements 2(i) and 2(ii) in Theorem 1 the corresponding independent random variables take values in the subgroup $\Delta_p \subset \Omega_p$, we conclude that the following theorem holds.

Theorem 2. *Let $X = \Delta_p$. Let $\alpha = c = (c_0, c_1, \ldots, c_n, \ldots) \in \Delta_p^0$ be an arbitrary topological automorphism of the group X. Then the following statements hold.*

1. *Let ξ_1 and ξ_2 be independent random variables with values in X and distributions μ_1 and μ_2. Assume that the conditional distribution of the linear form $L_2 = \xi_1 + \alpha\xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric. Then*

   1(i) *If $p > 2$ and $c_0 \neq p - 1$, then $\mu_j = m_K * E_{x_j}$, where K is a compact subgroup of X and $x_j \in X$. Moreover, if $c_0 = 1$, then μ_1 and μ_2 are degenerate distributions.*

   1(ii) *If $p = 2$, $c_0 = 1$ and $c_1 = 0$, then μ_1 and μ_2 are degenerate distributions.*

2. *If one of the following conditions holds:*

   2(i) *$p > 2$, $c_0 = p - 1$;*

   2(ii) *$p = 2$, $c_0 = c_1 = 1$,*

then there exist independent random variables ξ_1 and ξ_2 with values in X and distributions μ_1 and μ_2 such that the conditional distribution of the linear form $L_2 = \xi_1 + \alpha\xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric whereas $\mu_1, \mu_2 \notin I(X)$.

Remark 1. Assume that in Theorem 1 $p > 2$, $k = 0$, $c_0 \neq 1$ and $c_0 \neq p - 1$. This implies in particular, that $I - \alpha \in \mathrm{Aut}(\Delta_p)$, and hence

$$I - \widetilde{\alpha} \in \mathrm{Aut}(\mathbf{Z}(p^\infty)). \tag{46}$$

Let ξ_1 and ξ_2 be independent identically distributed random variables with values in Δ_p and distribution m_{Δ_p}. We check that the conditional distribution of the linear form $L_2 = \xi_1 + \alpha\xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric. By Lemma 1, it suffices to verify that the characteristic functions $f(y) = g(y) = \widehat{m}_{\Delta_p}(y)$ satisfy equation (36). It follows from (1) that

$$\widehat{m}_{\Delta_p}(y) = \begin{cases} 1, & y = 0; \\ 0, & y \neq 0. \end{cases}$$

Obviously, it suffices to check that equation (36) holds when $u \neq 0$, $v \neq 0$. Thus, assume that $u \neq 0$, $v \neq 0$. If $u + v = 0$ and $u + \widetilde{\alpha}v = 0$, then $(I - \widetilde{\alpha})v = 0$. Taking into account (46), this implies that $v = 0$, contrary to the assumption. Thus, either $u + v \neq 0$ or $u + \widetilde{\alpha}v \neq 0$, and hence the left-hand side of equation (36) is equal to zero. Reasoning analogously we show that the right-hand side of equation (36) is also equal to zero. So, equation (36) holds. This example shows that statement 1(i) in Theorem 1 can not be strengthened to the statement that both μ_1 and μ_2 are degenerate distributions.

Assume that conditions 1(iii) of Theorem 1 hold, i.e. $p > 2$ and $|k| = 1$. We can assume without loss of generality that $k = 1$. Let ξ_1 and ξ_2 be independent random variables with values in the group Δ_p and distributions $\mu_1 = am_{\Delta_p} + (1 - a)m_{p\Delta_p}$, where $0 < a < 1$, and $\mu_2 = m_{\Delta_p}$. Then the characteristic functions $f(y) = \widehat{\mu}_1(y)$ and $g(y) = \widehat{\mu}_2(y)$ are defined by formulas (43) for $k = 1$. Obviously, the proof that the characteristic functions $f(y)$ and $g(y)$ satisfy equation (36), given in the proof of statement 2(iv), remains true for $k = 1$ too. Thus, statement 1(iii) can not be strengthened to the statement that both distributions $\mu_1, \mu_2 \in I(X)$.

Remark 2. Compare Theorem 1 with Heyde's characterization theorem for two independent random variables on the real line $X = \mathbf{R}$. It is easy to see that this theorem can be formulated in the following way. Let ξ_1 and ξ_2 be independent random variables with values in the group $X = \mathbf{R}$ and distributions μ_1 and μ_2.

Let $\alpha \neq -I$. If the conditional distribution of the linear form $L_2 = \xi_1 + \alpha\xi_2$ given $L_1 = \xi_1 + \xi_2$ is symmetric, then μ_j are Gaussian. Thus, on the real line the only condition $\alpha \neq -I$, obviously, necessary, is sufficient for characterization of the Gaussian distribution.

It follows from Theorem 1 that on the group of p-adic numbers $X = \Omega_p$ the state of affairs is more complicated. On the one hand, much more severe constrains for α (conditions 1(i) for $p > 2$ and 1(ii) for $p = 2$) are necessary and sufficient for characterization of the idempotent distribution. On the other hand, there exist α (satisfying conditions 1(iii)) such that 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 the only one of the distributions μ_j is idempotent. This effect is absent on the real line.

References

[1] G. M. FELDMAN, On the Heyde theorem for finite Abelian groups, *J. Theoretical Probab.* **17** (2004), 929–941.

[2] G. M. FELDMAN, On the Heyde theorem for discrete Abelian groups, *Studia Math.* **177** (2006), 67–79.

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

[4] G. FELDMAN, Functional equations and characterization problems on locally compact Abelian groups, Vol. 5, EMS Tracts in Mathematics, *European Mathematical Society (EMS), Zurich*, 2008.

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

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

[7] E. HEWITT and K. A. ROSS, Abstract Harmonic Analysis, **1**, *Springer-Verlag, Berlin, Gottingen, Heildelberg*, 1963.

[8] C. C. HEYDE, Characterization of the normal low by the symmetry of a certain conditional distribution, *Sankhya, Ser. A.* **32** (1970), 115–118.

[9] A. M. KAGAN, YU. V. LINNIK and C. R. RAO, Characterization Problems in Mathematical Statistics, Wiley Series in Probability and Mathematical Statistics, *John Wiley & Sons, New York – London – Sydney*, 1973.

[10] M. V. MYRONYUK, Heyde's characterization theorem for discrete Abelain groups, *J. of Austral. Math. Soc.* **88** (2010), 93–102.

[11] M. V. MYRONYUK, The Heyde theorem on $\boldsymbol{a}$-adic solenoids, *Colloquium Mathematiquim* **132** (2013), 195–210.

[12] M. V. MYRONYUK and , G. M. FEL'DMAN, On a characterization theorem on finite abelian groups, *Siberian Math. J.* **46** (2005), 315–324.

[13] K. P. Parthasarathy, Probability measures on metric spaces, *Academic Press*, *New York and London*, 1967.

GENNADIY FELDMAN
MATHEMATICAL DIVISION
B. VERKIN INSTITUTE
FOR LOW TEMPERATURE PHYSICS
AND ENGINEERING OF
THE NATIONAL ACADEMY
OF SCIENCES OF UKRAINE
47, LENIN AVE, KHARKOV, 61103
UKRAINE

E-mail: feldman@ilt.kharkov.ua