A group automorphism is a factor of a direct product of a zero entropy automorphism and a Bernoulli automorphism

by

Nobuo Aoki (Tokyo)

Abstract. Our aim is to show the title, that is, a compact metric abelian group X with an automorphism σ splits into a sum $X = X_1 + X_2$ of σ-invariant subgroups X_1 and X_2 such that (X_1, σ) has zero entropy and (X_2, σ) is Bernoullian.

§ 1. **Introduction.** The metrical and topological structures of affine transformations studied by many authors. It follows from Parry [12, 13] and Dani [6] that the metrical structure of an affine transformation of a compact abelian group has a relation to that of its automorphism part. For example, if an affine transformation of a compact abelian group is minimal, then its automorphism part has zero entropy. Further, an affine transformation is a Kolmogorov automorphism if and only if its automorphism part is so.

Concerning only with automorphisms of a compact metric abelian group, Rohlin proved in [15] that every ergodic automorphism of a compact metric abelian group is a Kolmogorov automorphism (hence Bernoullian [9] or [1]). After that the author [2] extended the result of [1] to a compact metric group.

Let X be a compact metric abelian group and σ be an automorphism of X, then it is known (cf. [1]) that there exists a σ-invariant subgroup X_2 such that the factor of σ on X/X_2 has zero entropy and the restriction of σ on X_2 is Bernoullian. However, it is unknown yet whether X contains a subgroup X_1 such that (X_1, σ) has zero entropy and X splits into a sum $X = X_1 + X_2$.

In this paper, we first prove that a compact metric abelian group X splits into a sum $X = X_0 + F$ of the connected component X_0 of the identity and a totally disconnected subgroup F, invariant with respect to a given automorphism of X. Our aim is to show that every automorphism of a compact metric abelian group is an algebraic factor of a direct product of a Bernoulli automorphism and an automorphism with zero entropy. This characterizes a metrical and topological structure (in the ergodic theory) of every automorphism.

The author wishes to express his heartily thanks to the referee for his kind advice and sugestions.

§ 2. Main results. Throughout this paper, we shall write the group operation by additive form. The identity of the group will be denoted by "0". To distinguish the direct sum of subgroups from the sum, we denote them by the symbols "$\oplus$" and "$+$" respectively. The direct product of two groups will be denoted by "$\otimes$". We shall call simply *automorphisms* continuous group automorphisms, and denote them by Greek letters σ and γ. Given an automorphism of a group, its restriction on a subgroup and the induced automorphism on a factor group will be denoted by the same symbol if there is no confusion. We shall call a *factor automorphism* the induced automorphism of a factor group.

The following is a main result of this paper.

THEOREM 1. *Every automorphism of a compact metric abelian group is an algebraic factor of a direct product of an automorphism with zero entropy and a Bernoulli automorphism.*

Proof. This is obtained easily from the following Theorem 2. Indeed, let X be as in Theorem 2 and σ be an automorphism of X. If Theorem 2 was established, then X contains the subgroups X_1 and X_2 in Theorem 2. Hence (X, σ) is an algebraic factor of $(X_1 \otimes X_2, \sigma\otimes\sigma)$.

THEOREM 2. *Let X be a compact metric abelian group and σ be an automorphism of X. Then X contains σ-invariant subgroups X_1 and X_2 such that*

(i) *(X_1, σ) has zero entropy,*

(ii) *(X_2, σ) is ergodic (and hence Bernoullian with respect to the normalized Haar measure) and*

(iii) *$X = X_1 + X_2$.*

In the remainder of this paper we shall prove Theorem 2.

§ 3. An auxiliary result. We shall show a result on a compact metric abelian group used in proving Theorem 2.

PROPOSITION 1. *Let X be a compact metric abelian group and X_0 be the connected component of the identity in X. If σ is an automorphism of X, then there exists a σ-invariant totally disconnected subgroup H such that $X = X_0 + H$.*

For the proof we need the following Lemma 1. Let G be a discrete countable abelian group and γ be an automorphism of G. We write

$$K_f = \sum_{-\infty}^{\infty} \gamma^j \langle f\rangle, \quad f \in G,$$

where $\langle f\rangle$ is a cyclic subgroup of G generated by f.

LEMMA 1 (Lemma 3.1 of [1]). *Let G and γ be as above. Assume that G_t is a γ-invariant torsion free subgroup. Then, for $g \in G$ there exists an integer $d>0$ such that $dK_g + G_t$ is a torsion free subgroup.*

We shall give here a proof for completeness. Let $\dot{g} = g + G_t \in G/G_t$, and $\dot{W}$ be the γ-invariant subgroup of G/G_t generated by $\dot{g}$. Under that action of γ, we can consider $\dot{W}$ to be a $\boldsymbol{Z}[x, x^{-1}]$-module ($\boldsymbol{Z}[x, x^{-1}]$ denotes the ring of polynomials in x and x^{-1} with integer coefficients). Let $\dot{V}$ be the torsion subgroup of $\dot{W}$. Then $\dot{V}$ is clearly a $\boldsymbol{Z}[x, x^{-1}]$-submodule of $\dot{W}$. Since $\boldsymbol{Z}[x, x^{-1}]$ is Noetherian, $\dot{V}$ is finitely generated under $\boldsymbol{Z}[x, x^{-1}]$, say by $v_1, \ldots, v_r$. If $d_j v_j = 0$ for non-zero integers d_j $(1 \leqslant j \leqslant r)$, and $d = d_1 \ldots d_r$, then $d\dot{V} = \{0\}$ in G/G_t, and so $d\dot{W}$ is torsion free. Since both $d\dot{W} = (dK_g + G_t)/G_t$ and G_t are torsion free, so is $dK_g + G_t$.

We denote by (G, γ) the dual of (X, σ) $((\gamma g)(x) = g(\sigma x), g \in G$ and $x \in X)$.

Proof of Proposition 1. Denote by G' the maximal torsion subgroup of G. For a character $g_0 \notin G'$, it follows that there is an integer $d_0 > 0$ such that $d_0 K_{g_0}$ is torsion free. Since X is metrizable, G must be countable. Using Lemma 1 inductively, we see that there exist positive integers $d_1, d_2, \ldots$ and characters $g_1, g_2, \ldots \notin G'$ such that $G'' = \sum_{j=0}^{\infty} d_j K_{g_j}$ is torsion free and G/G'' is a torsion group.

Let H denote the annihilator of G'' in X. Then H has the character group G/G''. Thus H is totally disconnected and σ-invariant. On the other hand, since X/X_0 is totally disconnected, $X/(X_0+H)$ must be connected and totally disconnected, that is, an identity group. The proof is completed.

§ 4. Proof of Theorem 2. In proving Theorem 2, we need the following propositions.

PROPOSITION 2. *Let X and σ be as in Theorem 2. If X is connected, then Theorem 2 is true for (X, σ).*

PROPOSITION 3. *Let X and σ be as in Theorem 2. If X is totally disconnected, then Theorem 2 is true for (X, σ).*

The group X is expressed as $X = X_0 + H$ with the notations of Proposition 1. If we hold Propositions 2 and 3, then the subgroups X_0 and H split into the sums $X_0 = X_1' + X_2'$ and $H = H_1 + H_2$ of subgroups such that X_1' and H_1 satisfy (i) and X_2' and H_2 satisfy (ii). Denote $X_1 = X_1' + H$ and $X_2 = X_2' + H$, then $X = X_1 + X_2$ since $X = X_0 + H$. Since (X_1, σ) is an algebraic factor of the direct product system $(X_1' \otimes H_1, \sigma\otimes\sigma)$, (X_1, σ) has zero entropy. Also (X_2, σ) is a factor of $(X_2' \otimes H_2, \sigma\otimes\sigma)$, so that (X_2, σ) is ergodic (and hence Bernoullian).

It will be remain only to show Propositions 2 and 3.

(I) Proof of Proposition 2. For the proof we prepare some results that suffice for our needs. As before let G be a countable discrete torsion free abelian group and γ be an automorphism of G. For $g \in G$ we shall denote by $p_g(x)$ a polynomial $p(x)$ with minimal degree such that $p(\gamma)g = 0$ for some $0 \neq p(x) \in \boldsymbol{Z}[x]$. We define subsets

$$G_A = [g \in G\colon\ p_g(\gamma)g = 0\}$$

(obviously G_A is a γ-invariant subgroup) and

$$G_B = \{g \in G_A\colon\ p_g(x) \text{ has only roots of unity}\},$$
$$G_C = \{g \in G_A\colon\ p_g(x) \text{ has not roots of unity}\}.$$

LEMMA 2. *G_B and G_C are γ-invariant subgroups, and $G_B \cap G_C = \{0\}$.*

Proof. It is obvious that G_B and G_C are γ-invariant. If f and g are in G_B, then $p_f(\gamma)f = p_g(\gamma)g = 0$. Since $p_f(\gamma)p_g(\gamma)(f+g) = 0$, a polynomial $p_{f+g}(x)$ divides $p_f(x)p_g(x)$ over Q (denoting the rational field). Thus $p_{f+g}(x)$ has only roots of unity, whence $f+g \in G_B$. It is easy to see that G_C is a subgroup and $G_B \cap G_C = \{0\}$.

LEMMA 3. *$G_A/(G_B \oplus G_C)$ is a torsion group.*

Proof. If $\operatorname{rank}(G_A) = r < \infty$, then G_A is imbeded in Q^r where Q^r is the r-dimensional vector space over Q. We can consider G_A to be a subset of Q^r. Then there is an extension of γ on Q^r (we denote it by the same symbol γ). The space Q^r has a direct sum splitting $Q^r = Q_B \oplus Q_C$ of γ-invariant subspaces where all the eigenvalues of $\gamma_{|Q_B}$ are only roots of unity and those of $\gamma_{|Q_C}$ are not roots of unity. Obviously, $G_B \subset Q_B$ and $G_C \subset Q_C$. Let $f \in G_A$, then $f = f_B + f_C$ with some $f_B \in Q_B$ and some $f_C \in Q_C$. Since Q^r is a divisible extension of G_A, $nf_B \in G_B$ and $nf_C \in G_C$ for some $n > 0$, hence $nf = nf_B + nf_C \in G_B \oplus G_C$. This shows that $G_A/(G_B \oplus G_C)$ is a torsion group.

If $\operatorname{rank}(G_A) = \infty$, it is easy to see that G_A contains a sequence

$$G_A^{(1)} \supset G_A^{(2)} \supset \ldots \supset \bigcup_n G_A^{(n)} = G_A$$

of γ-invariant subgroups such that $\operatorname{rank}(G_A^{(n)}) < \infty$ for all $n \geqslant 1$. Hence there exist subgroups $G_B^{(n)}$ and $G_C^{(n)}$ such that $G_B^{(n)} \subset G_B$ and $G_C^{(n)} \subset G_C$, and $G_A^{(n)}/(G_B^{(n)} \oplus G_C^{(n)})$ is a torsion group. We obtain at once the conclusion.

LEMMA 4. *If $g \notin G_A$, then the subgroup $K_g = \sum_{-\infty}^{\infty} \gamma^j \langle g \rangle$ splits into a (restricted) direct sum $K_g = \bigoplus_{-\infty}^{\infty} \gamma^j \langle f \rangle$.*

Proof. This follows from the fact that $p(\gamma)g \neq 0$ for all $0 \neq p(x) \in Z[x]$.

The set $\Gamma = \{g \in G\colon g \notin G_A\}$ is countable and $G_A + \Gamma = G$ holds. For $g_{i_1} \in \Gamma$, we denote by g_{i_2} a character $f \in \Gamma$ such that $K_{g_{i_1}} \cap K_f = \{0\}$, and by g_{i_3} a character $h \in \Gamma$ such that $K_{g_{i_1}} \oplus K_{g_{i_2}} \cap K_h = \{0\}$. Repeating this step, we get a sequence $\{K_{g_{i_n}}\}$ of subgroups and obviously

$$G_D = \bigoplus_{n \geqslant 1} K_{g_{i_n}}.$$

Then G_D is γ-invariant and $G_A \cap G_D = \{0\}$. We claim that G/G_D is not necessarily torsion free.

LEMMA 5. *For any $\dot{g} \in G/G_D$, there exists $0 \neq p(x) \in Z[x]$ such that $p(\gamma)\dot{g} = 0$ (the identity of G/G_D).*

Proof. This follows from the definition of G_D.

LEMMA 6. *Let X be a compact connected metric abelian group, σ be an automorphism of X and (G, γ) be the dual of (X, σ). If $G = G_B$ (that is, for any $f \in G$, $p_f(\gamma)f = 0$ and $p_f(x)$ has only roots of unity), then (X, σ) has zero entropy.*

Proof. We notice that G is torsion free. Let G_g denote a subgroup generated by $\{\gamma^j g\colon -\infty < j < \infty\}$ for any $g \in G$. Since $p_g(\gamma)g = 0$, the rank of G_g is finite. We have that $p_g(x)$ is monic and its constant term is ± 1 since it has only roots of unity and $p_g(x) \in Z[x]$. Therefore it follows that G_g is finitely generated. Since G is countable, G contains a sequence $G_1 \subset G_2 \subset \ldots$ of γ-invariant subgroups such that $\bigcup G_n = G$ and for any $n \geqslant 1$, G_n is finitely generated. If X_n is the annihilator of G_n in X, then X_n is σ-invariant and X/X_n is a finite-dimensional torus. Since every polynomial $p_g(x)$ has only roots of unity, $(X/X_n, \sigma)$ has zero entropy (cf. see p. 168 of [17]). Hence (X, σ) has also zero entropy since $X_n \searrow \{0\}$.

THEOREM A (§ 6 of [16]). *Let σ be an automorphism of a compact metric abelian group X. If N is a σ-invariant subgroup of X, then $h(\sigma) = h(\sigma_{|X/N}) + h(\sigma_{|N})$ (the notation $h(\sigma)$ means the Kolmogorov entropy).*

From now on we shall prove Proposition 2. For the proof we must use Proposition 3 that is proved later on. As before let (G, γ) be the dual of (X, σ). Since X is connected and metrizable, G is a countable discrete torsion free abelian group. We have

$$G \supset G_A \oplus G_D \supset G_B \oplus G_C \oplus G_D.$$

Denote by $\operatorname{ann}(X, G')$ the annihilator of a subgroup G' of G in X, and put

$$Y_1 = \operatorname{ann}(X, G_C \oplus G_D) \quad \text{and} \quad X_2 = \operatorname{ann}(X, G_B).$$

Then we get

$$Y_1 + X_2 = \operatorname{ann}(X, \{G_C \oplus G_D\} \cap G_B) = \operatorname{ann}(X, \{0\}) = X.$$

It follows that (X_2, σ) is ergodic and $(X/X_2, \sigma)$ has zero entropy. For, the character group of X_2 is G/G_B and $\gamma_{|G/G_B}$ has no finite orbits except the identity. If $\dot{g} = g + G_B \in G/G_B$ and $\gamma^k(g + G_B) = \gamma^k g + G_B = g + G_B$ for some $k \neq 0$, then $(\gamma^k - I)g \in G_B$ and so $p_{(\gamma^k - I)g}(\gamma)(\gamma^k - I)g = 0$. Since $p_{(\gamma^k - I)g}(x)$ has only roots of unity, so is $p_{(\gamma^k - I)g}(x)(x^k - 1)$. Hence $g \in G_B$ and so $\dot{g}$ is the identity of G/G_B. Therefore (X_2, σ) is ergodic. The character group of X/X_2 is G_B. Hence by Lemma 6, $(X/X_2, \sigma)$ has zero entropy. It is easy to see that X_2 is the maximal subgroup satisfying the above conditions (by using Theorem A).

Using Proposition 1, we see that there are σ-invariant subgroups Z and H such that Z is connected, H is totally disconnected and

$$Y_1 = Z + H.$$

If we hold Proposition 3, then H contains σ-invariant subgroups H_1 and H_2 such that (H_1, σ) has zero entropy, (H_2, σ) is ergodic and

$$H = H_1 + H_2.$$

To get the splitting as in Theorem 2, let $(G^{(z)}, \gamma)$ be the dual of (Z, σ), then $G^{(z)}$ is the factor group of $G/(G_C \oplus G_D)$, which is the character group of Y_1. Hence by

Lemma 5, for any $g \in G^{(z)}$ there is $0 \neq p(x) \in Z[x]$ such that $p(\gamma)g = 0$. As before, define γ-invariant subgroups

$$G_B^{(z)} = \{g \in G^{(z)}: p_g(x) \text{ has only roots of unity}\},$$
$$G_C^{(z)} = \{g \in G^{(z)}: p_g(x) \text{ has not roots of unity}\}.$$

Then $G^{(z)}/(G_B^{(z)} \oplus G_C^{(z)})$ is a torsion group (Lemma 3). Since $G^{(z)}$ is torsion free, there exists the minimal divisible extension $(\bar{G}^{(z)}, \gamma)$ of $(G^{(z)}, \gamma)$ (see § 23 of [11] and [1]). It is easy to see that $\bar{G}^{(z)} = \bar{G}_B^{(z)} \oplus \bar{G}_C^{(z)}$ where $\bar{G}_B^{(z)} = \{g \in \bar{G}^{(z)}: mg \in G_B^{(z)}$ for some $m \neq 0\}$ and $\bar{G}_C^{(z)}$ is defined in the same way. Obviously, for $g \in \bar{G}_B^{(z)}$ a polynomial $p_g(x)$ has only roots of unity and for $f \in \bar{G}_C^{(z)}$ a polynomial $p_f(x)$ has not roots of unity.

Let $(\bar{Z}, \sigma)$ be the dual of $(\bar{G}^{(z)}, \gamma)$, then $\bar{Z}$ splits into a direct sum

$$\bar{Z} = \bar{Z}_B \oplus \bar{Z}_C$$

of σ-invariant subgroups where $\bar{Z}_B = \operatorname{ann}(\bar{Z}, \bar{G}_C^{(z)})$ and $\bar{Z}_C = \operatorname{ann}(\bar{Z}, \bar{G}_B^{(z)})$. Since $\bar{Z}_B$ has the character group $\bar{G}_B^{(z)}$, from Lemma 6 it follows that $(\bar{Z}_B, \sigma)$ has zero entropy. On the other hand, the character group $\bar{G}_C^{(z)}$ of $\bar{Z}_C$ has no periodic points under γ except the identity, so that $(\bar{Z}_C, \sigma)$ is ergodic.

Let $K = \operatorname{ann}(\bar{Z}, G^{(z)})$, then K is σ-invariant and $\bar{Z}/K$ is isomorphic to Z. Since $\bar{Z}/K$ and Z have the same character group $G^{(z)}$ on which actions of γ coincide, (Z, σ) is isomorphic to $(\bar{Z}/K, \sigma)$. Therefore Z is expressed as

$$Z = Z_1 + Z_2$$

of σ-invariant subgroups where Z_1 and Z_2 are factors of $\bar{Z}_B$ and $\bar{Z}_C$, respectively. From the maximality of X_2, $Z_2 + H_2 \subset X_2$. Let us put $X_1 = Z_1 + H_1$, then (X_1, σ) has zero entropy, and $X = X_1 + X_2$.

In order to conclude the proof of Proposition 2 and get Theorem 2, we have to show Proposition 3.

(II) Proof of Proposition 3. For the proof we need the following results.

THEOREM B (11.1 of [16]). *Let σ be an automorphism of a compact totally disconnected metric abelian group X. Then there exists in X a σ-invariant subgroup K such that $(X/K, \sigma)$ has zero entropy and (K, σ) is Bernoullian (with respect to the normalized Haar measure).*

Let X be a compact metric abelian group and X split into a direct sum $X = \bigoplus_{-\infty}^{\infty} H_i$ where $H_i = H$, $i = 0, \pm 1, \ldots$ The automorphism σ of X defined by $\sigma\{h_n\} = \{h_{n+1}\}$ will be called a *Bernoulli group automorphism.* A Bernoulli group automorphism having a group of states which is different from the identity and having no proper non-trivial subgroups will be called a *simple Bernoulli group automorphism.*

THEOREM C (11.5 of [16]). *Let X be a compact totally disconnected metric abelian group and σ be an automorphism of X. Let H be an open subgroup of X such that $\bigcap \sigma^n H = \{0\}$. If X/H is simple, then X is finite or σ is a simple Bernoulli group automorphism of X.*

The following is a reform of Theorem 11.7 in [16]. In compact totally disconnected metric abelian groups, the statement of the theorem is not certain (see [3]).

LEMMA 7. *Let X be a compact totally disconnected metric abelian group. If σ is an ergodic automorphism of X, then X contains a sequence*

$$X = F_0 \supset F_1 \supset \ldots$$

of σ-invariant subgroups such that $\bigcap F_n = \{0\}$ and for any $n \geq 0$, there is a sequence

$$F_n = F_{n,0} \supset F_{n,1} \supset \ldots \supset \bigcap_i F_{n,i} = F_{n+1}$$

of σ-invariant subgroups such that for any $i \geq 1$, $\sigma_{|F_n/F_{n,i}}$ is a simple Bernoulli group automorphism.

Proof. Since X is totally disconnected, X contains a sequence $X = A_0 \supset A_1 \supset \ldots$ of open subgroups such that $\bigcap A_n = \{0\}$. Writing $H_n' = \bigcap_k \sigma^k A_n$ for any $n \geq 0$, by Theorem B there is a subgroup H_n of H_n' such that $(H_n'/H_n, \sigma)$ has zero entropy and (H_n, σ) has completely positive entropy. The sequence $\{H_n\}$ decreases and $\bigcap H_n = \{0\}$. Without loss of generality we may assume that the sequence contains no repetitions.

We fix the integer n and carry out a recursive construction of the sequence

$$H_n = F_{n,0} \supset F_{n,1} \supset \ldots \supset F_{n+1}$$

of σ-invariant subgroups, imposed the following conditions: for any $i \geq 0$,

$$F_{n,i} \supset F_{n,i,1} \supset \ldots \supset \bigcap_j F_{n,i,j} = F_{n,i+1}$$

such that for any $j \geq 1$, $\sigma_{|F_{n,i}/F_{n,i,j}}$ is a simple Bernoulli group automorphism.

Assume that the subgroups $F_{n,0} \supset F_{n,1} \supset \ldots \supset F_{n,i}$ satisfy all the conditions that we have imposed and $F_{n,i} \supsetneqq H_{n+1}$. Then $F_{n,i}$ contains an open proper subgroup B such that $B \supset H_{n+1}$ and $F_{n,i}/B$ is simple. Put $H = \bigcap \sigma^k B$, then $\sigma_{|F_{n,i}/H}$ is a simple Bernoulli group automorphism (Theorem C), and $h(\sigma_{|F_{n,i}/H}) = \log p$ where p is some prime. By Theorem B there is a subgroup $F_{n,i+1}$ of H such that $(H/F_{n,i+1}, \sigma)$ has zero entropy and $(F_{n,i+1}, \sigma)$ has completely positive entropy.

Let (G, γ) be the dual of $(F_{n,i}/F_{n,i+1}, \sigma)$. Since $h(\sigma_{|F_{n,i}/F_{n,i+1}}) = \log p$ (by Theorem A), G is a p-group. For, if G is not a p-group then G splits into a direct sum $G = \bigoplus_{a \geq 1} G^{(a)}$ of γ-invariant prime groups $G^{(a)}$ (p. 137 of [11]). Hence $F_{n,i}/F_{n,i+1}$ splits into a direct sum $F_{n,i}/F_{n,i+1} = \bigoplus_{a \geq 1} F^{(a)}$ where $F^{(a)}$ is a σ-invariant subgroup with character group $G^{(a)}$. Since each $(F^{(a)}, \sigma)$ is ergodic (Bernoullian), if q is a prime and $G^{(a)}$ is a q-group then $h(\sigma_{|F^{(a)}}) \geq \log q$ (by Theorem B). On the other hand, let G_H be the annihilator of $H/F_{n,i+1}$, then G_H is the character group of $F_{n,i}/H$. Since $F_{n,i}/H = \bigoplus_{-\infty}^{\infty} \sigma^j(F'/H)$ where F'/H is a p-cyclic group, G_H is annihilated by multiplication by p and hence $G_H \subset G^{(b)}$ for some b. This is inconsistent with $h(\sigma_{|F_{n,i}/F_{n,i+1}}) = \log p$.

It is easy to see that G is annihilated by multiplication by the prime p. Indeed, let G_m be the subgroup of G being annihilated by multiplication by p^m for $m = 1, 2$. Then $G_1 \subset G_2 \subset G$ and $\gamma_{|G_2/G_1}$ has no finite orbits except the identity. For $m = 1, 2$, if $\dot{K}_m$ is the annihilator of G_m in $F_{n,i}/F_{n,i+1}$, then $F_{n,i}/F_{n,i+1} = \dot{K}_0 \supset \dot{K}_1 \supset \dot{K}_2$ and for $m = 0, 1$, $(\dot{K}_m/\dot{K}_{m+1}, \sigma)$ is ergodic. Hence by Theorem C, $h(\sigma_{|\dot{K}_m/\dot{K}_{m+1}}) \geq \log p$ for $m = 0, 1$. But, since $h(\sigma_{|F_{n,i}/F_{n,i+1}}) = \log p$, we get $G = G_1$.

Therefore we can consider G to be a $Z/pZ[x, x^{-1}]$-module ($Z/pZ[x, x^{-1}]$ denotes the ring of polynomials in x and x^{-1} with coefficients in the field Z/pZ). We claim that γ has no finite orbits except the identity. Since $Z/pZ[x, x^{-1}]$ is a principal ideal domain, there is a sequence $G_1 \subset G_2 \subset \dots$ of free $Z/pZ[x, x^{-1}]$-modules such that $\bigcup G_i = G$ and for $i \geq 1$, G_i is of the form

$$G_i = Z/pZ[\gamma, \gamma^{-1}]g_i = \bigoplus_{-\infty}^{\infty} \gamma^n \langle g_i \rangle$$

for some $g_i \in G_i$. If $F_{n,i,j}/F_{n,i+1}$ is the annihilator of G_j in $F_{n,i}/F_{n,i+1}$ then $F_{n,i,j} \subset F_{n,i}$ and for $j \geq 1$, $\sigma_{|F_{n,i}/F_{n,i,j}}$ is a simple Bernoulli group automorphism.

It remains to show that there is an integer $i(n)$ such that $F_{n,i(n)} = H_{n+1}$. Put $\tilde{X} = X/H'_{n+1}$ and $\tilde{A} = A_{n+1}/H'_{n+1}$, then $\tilde{A}$ is open in $\tilde{X}$ and $\bigvee \sigma^k \varrho = \varepsilon$ where ϱ is the finite group partition of $\tilde{X}$ consisting of the cosets of $\tilde{A}$ and ε is the partition of $\tilde{X}$ into single points. Hence $(\tilde{X}, \sigma)$ has finite entropy. On the other hand,

$$h(\sigma_{|F_{n,i}/F_{n,i+1}}) \geq \log 2$$

and by Theorem A,

$$\sum_i h(\sigma_{|F_{n,i}/F_{n,i+1}}) \leq h(\sigma_{|X/H_{n+1}}) = h(\sigma_{|X/H'_{n+1}}) + h(\sigma_{|H'_{n+1}/H_{n+1}}) = h(\sigma_{\tilde{X}}) < \infty .$$

Therefore our requirement was obtained.

For the subgroups $\{F_{n,i}\}$ ($i = 0, 1, \dots, i(n)$ and $n = 0, 1, \dots$), we write $F_{n,i} = F_k$ where $k = \sum_{m=0}^{n-1} i(m) + i$. Obviously, the sequence $\{F_k\}$ satisfies all the required conditions.

LEMMA 8. *Let X be a compact totally disconnected metric abelian group and σ be an automorphism of X. If $h(\sigma) < \infty$, then $h(\sigma) = \log n$ where n is some integer.*

Proof. Let $\{A_m\}$ be a decreasing sequence of open subgroups such that $\bigcap A_m = \{0\}$ and ϱ_m be the finite group partition of X consisting of the cosets of A_m. Then, $h(\sigma, \varrho_m) = \lim_{n\to\infty} H(\varrho_m | \bigvee_1^n \sigma^{-i}\varrho_m) = \log|\varrho_m|$ (the notation $|E|$ means the cardinality of a set E). Since $\varrho_m \nearrow$ and $\bigvee \varrho_m$ is the partition of X into single points, we get $h(\sigma) = \lim_m h(\sigma, \varrho_m)$. But since $h(\sigma) < \infty$, there is $m > 0$ such that $h(\sigma) = h(\sigma, \varrho_m)$ and so $h(\sigma) = \log|\varrho_m|$.

Let σ be an automorphism of a compact metric abelian group X. We shall call σ *expansive* if there exists an open neighborhood U of the identity in X such that $0 \neq x \in U$ implies $\sigma^n x \notin U$ for some integer n. Some obvious examples of expansive automorphisms are a Bernoulli group automorphism and an automorphism

of a finite-dimensional torus such that all the eigenvalues of the matrix corresponding to the automorphism are off the unit circle.

LEMMA 9. *Let X and σ be as in Lemma 8. If (X, σ) is expansive and $h(\sigma) = 0$, then X is finite.*

Proof. Assume that X is infinite (whence it is not discrete). Let U be an expansive neighborhood of the identity for (X, σ). Then U contains a non-trivial open subgroup N. Since $h(\sigma) = 0$, it is easy to see that $\bigcap_{n=0}^{\infty} \sigma^n N = \bigcap_{n=1}^{\infty} \sigma^n N$. Indeed, if $\bigcap_0^k \sigma^n N \subsetneqq \bigcap_1^k \sigma^n N$ for all $k > 0$, then it follows that $|X/\bigcap_0^k \sigma^n N| \geq 2^k$ for all $k > 0$. Let $\varrho(N)$ be the partition of X consisting of the cosets of N, then $\varrho(N)$ is a finite measurable partition and $\bigvee_0^k \sigma^n \varrho(N) = \varrho(\bigcap_0^k \sigma^n N)$ holds. Since $|\varrho(\bigcap_0^k \sigma^n N)| \geq 2^k$, by definition we have $h(\sigma) \geq \lim_{k\to\infty} (1/(k+1)) \log 2^k = \log 2$. But, since $h(\sigma) = 0$, we get the requirement.

Hence $N \subset \bigcap_{n=1}^{k} \sigma^n N$ for some k. If $N' = \bigcap_{n=1}^{k} \sigma^n N$, then $\sigma N' = N'$. But, $\{0\} \neq N' \subset N \subset U$, which is a contradiction.

LEMMA 10. *Let X and σ be as in Lemma 8. If σ is a simple Bernoulli group automorphism of X, then every σ-invariant proper subgroup is finite.*

Proof. Let K be a σ-invariant proper subgroup. Since $h(\sigma) = \log p$ for some prime p, $h(\sigma_{|X/K}) = \log p$ by Lemma 8. Hence $h(\sigma_{|K}) = 0$ (by Theorem A). Since (K, σ) is expansive, K is finite by Lemma 9.

LEMMA 11. *Let X and σ be as in Lemma 8. Assume that Y_2 is a σ-invariant subgroup such that $\sigma_{|Y_2}$ is a simple Bernoulli group automorphism and $(X/Y_2, \sigma)$ has zero entropy. If Y_2 is open in X, then X contains a σ-invariant subgroup Y_1 such that (Y_1, σ) has zero entropy and $X = Y_1 + Y_2$.*

Proof. Since $\sigma_{|Y_2}$ is a simple Bernoulli automorphism, $Y_2 = \bigoplus_{i=-\infty}^{\infty} \sigma^i W$ where W is a p-cyclic group (p is some prime). Hence $px = 0$ for any $x \in Y_2$. Since Y_2 is open, X contains a finite subgroup F such that $X = Y_2 + F$. Since F is finite, there is the smallest non-negative integer n such that $K \subsetneqq X$ and $X = \{\bigoplus_{i=0}^{n} \sigma^i W\} + K$ where $K = \{\bigoplus'_{i \neq 0,1,\dots,n} \sigma^i W\} + F$. Thus X/K is simple (indeed, by the choice of n we have $X/K = (\sigma^n W + K)/K \cong \sigma^n W$). Let $Y_1 = \bigcap_{-\infty}^{\infty} \sigma^i K$, then X/Y_1 is infinite. For, if X/Y_1 is finite, then $(Y_1 + Y_2)/Y_1 \cong Y_2/(Y_1 \cap Y_2)$ is also finite. Since $Y_1 \cap Y_2 \subsetneqq Y_2$, $Y_1 \cap Y_2$ is finite by Lemma 10, whence Y_2 is finite. This is impossible.

Since X/K is simple and X/Y_1 is infinite, $\sigma_{|X/Y_1}$ is a simple Bernoulli group automorphism (by Theorem C). Hence the entropy of $(X/(Y_1 + Y_2), \sigma)$ is zero and positive if $X/(Y_1 + Y_2)$ is non-trivial. We have therefore $X = Y_1 + Y_2$ where $h(\sigma_{|Y_1}) = 0$.

LEMMA 12. *Let σ be an automorphism of a compact metric abelian group X and H be a σ-invariant subgroup ($\sigma H = H$) of X. If (X, σ) and $(X/H, \sigma)$ are expansive, then (X, σ) is expansive.*

Proof. Let $\dot{U}$ and U' be expansive neighborhoods for $(X/H, \sigma)$ and (H, σ), respectively. Obviously, $\dot{U} = \{x+H\colon x \in V\}$ and $U' = H \cap V$ where U and V are suitable neighborhoods of X. Letting $W = U \cap V$, we have $\bigcap_{-\infty}^{\infty} \sigma^j W = \bigcap_{-\infty}^{\infty} \sigma^j W \cap H = \bigcap_{-\infty}^{\infty} \sigma^j(W \cap H) = \{0\}$ since $\bigcap_{-\infty}^{\infty} \sigma^j(W+H) = H$. Therefore W is an expansive neighborhood for (X, σ).

LEMMA 13. *Let X be a compact totally disconnected metric abelian group. If σ is a Bernoulli group automorphism of X and if $h(\sigma)<\infty$, then for any σ-invariant subgroup H, $(X/H, \sigma)$ is expansive.*

Proof. As before let (G, γ) be the dual of $(X/H, \sigma)$. By assumption, G is expressed as $G = \sum_{-\infty}^{\infty} \gamma^n G_1$ where G_1 is a finite group. Since G is a torsion group, G_1 splits into a finite direct sum $G_1 = \bigoplus_{j=1}^{k} G_{1,j}$ of prime groups $G_{1,j}$. Hence,

$$G = \sum_{-\infty}^{\infty} \gamma^n \{\bigoplus_{j=1}^{k} G_{1,j}\} = \bigoplus_{j=1}^{k} G^{(j)}$$

where $G^{(j)} = \sum_{-\infty}^{\infty} \gamma^n G_{1,j}$ for $1 \leqslant j \leqslant k$. Then X/H splits into a direct sum

$$X/H = \bigoplus_{j=1}^{k} \dot{X}_j$$

where each $\dot{X}_j$ is a subgroup with character group $G^{(j)}$.

Let $G^{(j)}$ be a p-group and G'_m be a subgroup of $G^{(j)}$ being annihilated by multiplication by p^m for $m \geqslant 1$. Then there is an integer $a>0$ such that

$$G'_1 \subset G'_2 \subset \ldots \subset G'_a = G^{(j)}$$

since $G_{1,j}$ is a finite group. It is easy to see that for $1 \leqslant m \leqslant a$, $\gamma_{|G'_{m+1}/G'_m}$ has no finite orbits except the identity. Since $G^{(j)} = \sum_{-\infty}^{\infty} \gamma^n G_{1,j}$ and $G_{1,j}$ is finite, each G'_{m+1}/G'_m is finitely generated under $Z/pZ[x, x^{-1}]$, and so G'_{m+1}/G'_m is expressed as

$$G'_{m+1}/G'_m = Z/pZ[\gamma, \gamma^{-1}]\dot{g}_1 \oplus \ldots \oplus Z/pZ[\gamma, \gamma^{-1}]\dot{g}_b$$
$$= (\bigoplus_{-\infty}^{\infty} \gamma^n\langle\dot{g}_1\rangle) \oplus \ldots \oplus (\bigoplus_{-\infty}^{\infty} \gamma^n\langle\dot{g}_b\rangle)$$

for some $\dot{g}_1, \ldots, \dot{g}_b \in G'_{m+1}/G'_m$.

Let $\dot{X}_{G'_m}$ be the annihilator of G'_m in $\dot{X}_j$. Obviously, $\dot{X}_{G'_1} \supset \dot{X}_{G'_2} \supset \ldots \supset \dot{X}_{G'_a} = \{0\}$. For $m \geqslant 1$, $\dot{X}_{G'_m}$ is σ-invariant and $\sigma_{|\dot{X}_{G'_m}/\dot{X}_{G'_{m+1}}}$ is a simple Bernoulli automorphism.

From this together with Lemma 12, we get that $(\dot{X}_j, \sigma)$ is expansive. Therefore $(X/H, \sigma)$ is expansive and the proof is completed.

LEMMA 14. *Under the notations and the assumption of Lemma 11, if Y_2 is not open in X, then X contains a σ-invariant subgroup F such that (F, σ) has zero entropy and Y_2+F is open in X.*

Proof. Since $\sigma_{|Y_2}$ is a simple Bernoulli automorphism, obviously $h(\sigma_{|Y_2}) \geqslant \log 2$. Hence X contains an open subgroup L such that if $F_L = \bigcap_{-\infty}^{\infty} \sigma^i L$ then $(Y_2+F_L)/F_L$ is non-trivial. For, assume that $Y_2 \subset F_L$ for all open subgroups L. Then $Y_2 = \bigcap F_L = \{0\}$, which is a contradiction. Obviously $h(\sigma_{|X/(Y_2+F_L)}) = 0$ since $h(\sigma_{|X/Y_2}) = 0$. By theorem A,

$$h(\sigma_{|Y_2}) = h(\sigma) = h(\sigma_{|X/(Y_2+F_L)}) + h(\sigma_{|(Y_2+F_L)/F_L}) + h(\sigma_{|F_L}).$$

Hence, $h(\sigma_{|F_L}) = 0$. We write $\tilde{X} = \bigoplus_{i=-\infty}^{\infty} V_i$ where $V_i = X/L$ for $i = 0, \pm 1, \ldots$ Let $\tilde{P}$ be the cannonical projection from X/F_L onto X/L and $\tilde{\sigma}$ be a Bernoulli group automorphism of $\tilde{X}$. Define the map $\psi\colon X/F_L \to \tilde{X}$ by

$$\psi(\dot{x}) = \{P\sigma^i \dot{x}\}_{-\infty}^{\infty}, \quad \dot{x} \in X/F_L.$$

Then ψ is an isomorphism from X/F_L on some subgroup of $\tilde{X}$ and $\psi^{-1}\tilde{\sigma}\psi = \sigma$ on X/F_L holds. Since $\tilde{\sigma}$ is the Bernoulli group automorphism of $\tilde{X}$ and $h(\tilde{\sigma})<\infty$, $\big(\tilde{X}/\psi((Y_2+F_L)/F_L), \tilde{\sigma}\big)$ is expansive by Lemma 13 and $\big(\psi(X/F_L)/\psi((Y_2+F_L)/F_L), \tilde{\sigma}\big)$ is also expansive, whence so is $(X/(Y_2+F_L), \sigma)$. Since $h(\sigma_{|X/(Y_2+F_L)}) = 0$, $X/(Y_2+F_L)$ is finite by Lemma 9 and Y_2+F_L is open in X.

Proposition 3 now is proved as follows. Let X_2 be a subgroup of the group X such that $(X/X_2, \sigma)$ has zero entropy and (X_2, σ) has completely positive entropy (see Theorem B). Using Lemma 7, we see that X_2 contains a sequence

$$X_2 = X_{2,0} \supset X_{2,1} \supset \ldots$$

of σ-invariant subgroups such that $\bigcap X_{2,n} = \{0\}$ and for any $n \geqslant 0$ there is a sequence $X_{2,n} \supset X_{2,n,1} \supset \ldots$ of σ-invariant subgroups such that $\bigcap_j X_{2,n,j} = X_{2,n+1}$ and for any $j>0$, $\sigma_{|X_{2,n}/X_{2,n,j}}$ is a simple Bernoulli group automorphism.

Since $\sigma_{|X_2/X_{2,0,1}}$ is a simple Bernoulli group automorphism and

$$((X/X_{2,0,1})/(X_2/X_{2,0,1}), \sigma)$$

has zero entropy, by Lemmas 11 and 14 there is a σ-invariant subgroup M_1 of X such that

$$X = M_1 + X_2 \quad \text{and} \quad h(\sigma_{|M_1/X_{2,0,1}}) = 0.$$

Since $X_{2,0,j} \searrow X_{2,1}$, by Theorem A we have that for $k \geqslant 1$,

$$h(\sigma_{|X_{2,0}/X_{2,0,k}}) = h(\sigma_{|X_{2,0}/X_{2,0,1}}) + \sum_{j=2}^{k} h(\sigma_{|X_{2,0,j-1}/X_{2,0,j}}).$$

Notice that $\sigma_{|X_{2,0}/X_{2,0,k}}$ and $\sigma_{|X_{2,0}/X_{2,0,1}}$ are simple Bernoulli group automorphisms. Then by Lemma 8, we get $\sum_{j=2}^{k} h(\sigma_{|X_{2,0,j-1}/X_{2,0,j}}) = 0$ and so $h(\sigma_{|X_{2,0,1}/X_{2,0,k}}) = 0$. Since k is arbitrary, $h(\sigma_{|X_{2,0,1}/X_{2,1}}) = 0$ and hence $h(\sigma_{|M_1/X_{2,1}}) = 0$ (by Theorem A).

Since $\sigma_{|X_{2,1}/X_{2,1,1}}$ is a simple Bernoulli group automorphism and

$$((M_1/X_{2,1,1})/(X_{2,1}/X_{2,1,1}), \sigma)$$

has zero entropy, by the same argument we can find a σ-invariant subgroup M_2 of M_1 such that

$$M_1 = M_2+X_{2,1} \quad \text{and} \quad h(\sigma_{|M_2/X_{2,1,1}}) = 0 .$$

Since $X_{2,1} \subset X_2$, we get $M_1+X_2 = M_2+X_2 = X$. It is easy to see that

$$h(\sigma_{|X_{2,1,1}/X_{2,2}}) = 0 \quad \text{and} \quad h(\sigma_{|M_2/X_{2,2}}) = 0 .$$

Hence $((M_2/X_{2,1,1})/(X_{2,2}/X_{2,2,1}), \sigma)$ has zero entropy and $\sigma_{|X_{2,2}/X_{2,2,1}}$ is a simple Bernoulli group automorphism, so that M_2 contains a σ-invariant subgroup M_3 such that

$$M_2 = M_3+X_{2,2} \quad \text{and} \quad h(\sigma_{|M_3/X_{2,2,1}}) = 0 .$$

Obviously, $X = M_3+X_2$. Since $h(\sigma_{|X_{2,2,1}/X_{2,3}}) = 0$, we get $h(\sigma_{|M_3/X_{2,3}}) = 0$.

Continuing inductively this process, we have a sequence $M_1 \supset M_2 \supset \ldots$ of σ-invariant subgroups such that for any $n>1$,

$$X = M_n+X_2 \quad \text{and} \quad h(\sigma_{|M_n/X_{2,n}}) = 0 .$$

Put $X_1 = \bigcap M_n$, then $X = X_1+X_2$, and since $X_1/(X_{2,n} \cap X_1) \cong (X_{2,n}+X_1)/X_{2,n}$ is a subgroup of $M_n/X_{2,n}$, $h(\sigma_{|X_1}) = 0$ by Theorem A. The proof of Proposition 3 is completed.

Added in proof. An extension of the result of [9] (or [1]) to compact metric groups had already done by G. Miles and K. Thomas, Advances in Math. Supplementary Studies 2 (1978), pp. 207–249.

References

[1] N. Aoki, *A simple proof of the Bernoullicity of ergodic automorphisms on compact abelian group*, Israel J. Math. 38 (1981), pp. 189–198.

[2] — *The Bernoullicity of ergodic automorphisms of compact groups*, preprint.

[3] — *Zero-dimensional group automorphisms having a dense orbit*, to appear in J. Math. Soc. Japan.

[4] — and I. Kubo, *A number theoretical lemma and its application to the ergodic theory*, to appear.

[5] N. Bourbaki, *Elements de Mathematique Algebra*, Hermann, Paris, 1964.

[6] S. G. Dani, *Spectrum of an affine transformation*, Duke Math. J. 44 (1977), pp. 129–155.

[7] P. R. Halmos, *Lecture notes on ergodic theory*, Math. Soc. Japan, 1956.

[8] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademische Verlagsgesellschaft, Leipzig, 1923.

[9] D. Lind, *The structure of skew products with ergodic group automorphisms*, Israel J. Math. 3 (1977), pp. 205-248.

[10] S. Lang, *Algebra*, Addison-Welsey, 1972.

[11] A. G. Kurosch, *The Theory of Groups*, I, II, Chelsea, New York, 1960.

[12] W. Parry, *On the coincidence of three invariant σ-algebras associated with an affine transformation*, Proc. Amer. Math. Soc. 17 (1966), pp. 1297–1302.

[13] — *Ergodic properties of affine transformations and flows on nilmanifolds*, Amer. J. Math. 91 (1969), pp. 751–771.

[14] L. Pontrjagin, *Topological Groups*, Princeton Univ. Press, Princeton 1946.

[15] V. A. Rohlin, *Metric properties of endomorphisms of compact commutative groups*, Amer. Math. Soc. Trans. 64 (1967), pp. 244–272.

[16] S. A. Yuzvinskii, *Metric properties of endomorphisms of compact groups*, Amer. Math. Soc. Trans. 66 (1968), pp. 63–98.

[17] P. Walters, *Ergodic Theory*, Lecture Notes in Math. 458, Springer-Verlag, 1975.

[18] B. Weiss, *The isomorphisms problem in ergodic theory*, Bull. Amer. Math. Soc. 87 (1972), pp. 668–684.

DEPARTMENT OF MATHEMATICS
TOKYO METROPOLITAN UNIVERSITY
Tokyo

Accepté par la Rédaction le 7. 1. 1980