38. *Properties of Ergodic Affine Transformations of Locally Compact Groups. III*

By Ryotaro SATO
Department of Mathematics, Josai University, Saitama

(Comm. by Kinjirô KUNUGI, M. J. A., Feb. 12, 1971)

Let G be an abelian group. An affine transformation S of G is a transformation of G onto itself of the form $S(x)=a+T(x)$, where $a \in G$ and T is an automorphism of G. In case G is a locally compact non-discrete topological group, it has been proved (cf. [1], [2], [3] and [4]) that if there exists a continuous affine transformation S of G which has a dense orbit then G is compact. In the present paper we shall study the structure of a discrete abelian group G which is covered by an orbit under an affine transformation S.

1. Theorems.

From now on, for simplicity, we say that an affine transformation S of G satisfies property $\mathcal{A}$ if $\{S^n(w); n=0, \pm 1, \pm 2, \cdots\}=G$ for some $w \in G$.

Theorem 1. *Let G be an infinite abelian group. If G has an affine transformation $S(x)=a+T(x)$ satisfying property $\mathcal{A}$ then G is isomorphic with the additive group Z of the integers, a is a generator, and T is the identity transformation.*

Theorem 2. *Let G be a finite abelian group with order r. If 4 does not divide r, and G has an affine transformation $S(x)=a+T(x)$ satisfying property $\mathcal{A}$ then G is isomorphic with the cyclic group $Z(r)$ of order r, and a is a generator.*

2. Proof of Theorem 1.

Lemma 1. *If G has an affine transformation $S(x)=a+T(x)$ satisfying property $\mathcal{A}$ then G is finitely generated.*

Proof. Since $\{S^n(0); n=0, \pm 1, \pm 2, \cdots\}=\{S^n(w); n=0, \pm 1, \pm 2, \cdots\}=G$, $T(a)=S^k(0)$ for some integer k. If $k=0$ (resp. 1, or 2) then it is easy to check that $G=\{0\}$ (resp. $G=\{na; n=0, \pm 1, \pm 2, \cdots\}$, or $G=\{0\}$). If $k \geqq 3$, we see that $T^k(a)$ is in the subgroup H generated by $\{a, T(a), \cdots, T^{k-1}(a)\}$. It follows at once that

$$a \in T(H) \subset H,$$

and hence $T(H)=H$, and $S(H)=H$. This clearly assures that $G=H$, the required conclusion. A similar argument also applies in the case $k<0$, and so G is finitely generated.

Lemma 2. *If the additive group $Z^p (p \geqq 1)$ has an affine transfor-*

mation $S(x)=a+T(x)$ satisfying property $\mathcal{A}$ then $p=1$, a is a generator, and T is the identity transformation.

Proof. The automorphism T of Z^p may be extended in a natural fashion to a linear transformation of the p-dimensional complex euclidean space C^p. Then from the matrix theory, T can be represented by a triangular matrix under some suitable basis $\{e_1, e_2, \cdots, e_p\}$ of C^p:

$$T=\begin{pmatrix} \lambda_1 & & & * \\ & \lambda_2 & & \\ & & \ddots & \\ O & & & \lambda_p \end{pmatrix}$$

Let $a=\alpha_1 e_1+\alpha_2 e_2+\cdots+\alpha_r e_r$, where $\alpha_r \neq 0$. It is easy to observe that if $n \geqq 1$,

$$S^n(0)=*e_1+\cdots+*e_{r-1}+\alpha_r(1+\lambda_r+\cdots+\lambda_r^{n-1})e_r$$

and

$$S^{-n}(0)=*e_1+\cdots+*e_{r-1}+(-1)\alpha_r(\lambda_r^{-1}+\lambda_r^{-2}+\cdots+\lambda_r^{-n})e_r$$

Case I. If $\lambda_r \neq 1$ then

$$S^n(0)=*e_1+\cdots+*e_{r-1}+\alpha_r\frac{1-\lambda_r^n}{1-\lambda_r}e_r,$$

for $n=0, \pm 1, \pm 2, \cdots$. Since $nS(0)=*e_1+\cdots+*e_{r-1}+n\alpha_r e_r \in Z^p$, and S satisfies property $\mathcal{A}$, it follows that

$$\{n\alpha_r\,;\, n=0, \pm 1, \pm 2, \cdots\} \subset \left\{\alpha_r\frac{1-\lambda_r^n}{1-\lambda_r}\,;\, n=0, \pm 1, \pm 2, \cdots\right\}.$$

This is obviously impossible.

Case II. If $\lambda_r=1$ then

$$S^n(0)=*e_1+\cdots+*e_{r-1}+n\alpha_r e_r$$

for $n=0, \pm 1, \pm 2, \cdots$. It follows at once that $S^n(0)=nS(0)$, and so $a=S(0)$ is a generator. The lemma now is clear.

We are now in a position to accomplish the proof of Theorem 1. By Lemma 1, $G=Z^p \oplus F$, where F is a finite abelian group. If we define an affine transformation S^* of $G/F=Z^p$ by

$$S^*(x+F)=S(x)+F,$$

S^* satisfies property $\mathcal{A}$, whence it follows from Lemma 2 that $p=1$, i.e., $G=Z \oplus F$, which is possible only if $F=\{0\}$. This establishes Theorem 1.

3. Proof of Theorem 2.

Lemma 3. *Let G be a finite abelian group with order $r \geqq 2$, and $S(x)=a+T(x)$ an affine transformation of G satisfying property $\mathcal{A}$. Then the subgroup $H=\{x \in G\,;\, T(x)=x\}$ is a non-trivial cyclic subgroup generated by $x_0=a+T(a)+\cdots+T^{k-1}(a)$, where k denotes the period of a under T. Moreover if p denotes the order of x_0 then $r=pk$.*

Proof. In case $T(a)=a$, the lemma is clear, so we study the case $T(a) \neq a$. Since $k<r$, we see that $x_0=a+T(a)+\cdots+T^{k-1}(a) \neq 0$. Let

$n=ik+j$, where $0 \leqq i < p$ and $0 < j < k$. Then

$$S^n(0)=ix_0+(a+T(a)+\cdots+T^{j-1}(a)).$$

Therefore

$$T(S^n(0))-S^n(0)=T^j(a)-a\neq 0,$$

from which $H=\{x_0, 2x_0, \cdots, px_0\}$ and $r=pk$.

Lemma 4. *Let G be a finite abelian group with order r which has an affine transformation $S(x)=a+T(x)$ satisfying property $\mathcal{A}$, and let $H=\{x \in G; T(x)=x\}$. If 4 does not divide r, and G/H is cyclic then G is cyclic and a is a generator.*

Proof. The proof proceeds by induction on r. If $r \leqq 3$, the lemma is clear. Now suppose that if $1 \leqq s < r$, and 4 *does not divide* s then the lemma is true.

If $T(a)=a$, the proof is trivial, and so we suppose that $T(a)\neq a$. Let k be the period of a under T and p the order of $x_0=a+T(a)+\cdots+T^{k-1}(a)$. Define an affine transformation S^* of G/H as follows:

$$S^*(x+H)=S(x)+H.$$

Since S^* has property $\mathcal{A}$, the order of $a+H \in G/H$ is the greatest in the orders of the elements in the cyclic G/H, whence $a+H$ generates G/H. Clearly G is generated by $\{a, x_0\}$, and so there exist two positive integers m and n such that m devides n, and $G=Z(m)\oplus Z(n)$, where $Z(m)$, $Z(n)$ denote cyclic groups of order m, n, respectively. An elementary calculation shows that the order of a equals n.

If $ka=0$ then the order of a equals k by virtue of Lemma 3, and so G is isomorphic with the direct product group $H\oplus H_1$, where H_1 denotes the cyclic group generated by a. Hence $G=Z(p)\oplus Z(k)$. Let $T(a)=\lambda x_0+\mu a$. Then an easy calculation shows that

$$S^k(0)=\lambda(1+(1+\mu)+\cdots+(1+\mu+\cdots+\mu^{k-2}))x_0 + (1+\mu+\cdots+\mu^{k-1})a=x_0\neq 0.$$

From the property of S^* of $G/H=Z(k)$ it follows that

$$1+(1+\mu)+\cdots+(1+\mu+\cdots+\mu^{k-2})=1+2+\cdots+(k-1)$$

$(\text{mod } k)$. Let $k=hp$. Then the above relation holds only if $p=2$, and so $r=4h$, which contradicts the hypothesis that 4 *does not divide* r. Thus $ka\neq 0$. Let $ka=tx_0 \in H$, where $0<t<p$.

In case t, p are relatively prime, it follows easily that the order of a equals $r=pk$, whence a is a generator. In case t, p are not relatively prime, let q be the order of $ka=tx_0$. Then the order of a equals qk, and so $r=pk=(p/q)qk=(p/q)n=mn$. Therefore $p=qm>m$. Let $x_0=(\alpha, \beta)\in Z(m)\oplus Z(n)=G$. Then $mx_0=(0, m\beta)\neq(0,0)$. If H_2 denotes the subgroup generated by mx_0 then clearly G/H_2 is not cyclic. However from the construction of H_2, G/H_2 has an affine transformation satisfying property $\mathcal{A}$, which contradicts the hypothesis of induction.

By virtue of the above two lemmas, the proof of Theorem 2 is now easy. It proceeds by induction on r. If $1 \leqq r \leqq 3$, the theorem is clear. Now suppose that if $1 \leqq s < r$ and 4 *does not divide* s, then the theorem is true.

In case $T(a)=a$, the proof is trivial, and so we suppose that $T(a) \neq a$. In this case, the subgroup $H=\{x \in G; T(x)=x\}$ is a non-trivial cyclic subgroup by virtue of Lmma 3. By the hypothesis of induction, G/H is cyclic, whence by Lemma 4, G is cyclic and a is a generator. The proof is completed.

4. Counter-examples.

1) In Theorem 2, the hypothesis that 4 *does not divide* r is not omitted. In fact, let G be the direct product group $Z(2) \oplus Z(2n)$ of cyclic groups with orders 2 and $2n$, respectively, where n is an odd integer. Define an affine transformation S of G by

$$S(x, y)=(0, 1)+(x+y, y)$$

It is easy to check that S satisfies property $\mathcal{A}$. But obviously G is not cyclic.

2) There exists an affine transformation $S(x)=a+T(x)$ satisfying property $\mathcal{A}$, but T is not the identity transformation. To see this, let G be the cyclic group $Z(16)$ of order 16, and define an affine transformation S of G as follows: $S(x)=1+5x$. A routine calculation shows that S satisfies property $\mathcal{A}$, but $T(x)=5x$ is not the identity transformation.

References

[1] R. Sato: Continuous affine transformations of locally compact totally disconnected groups. Proc. Japan Acad., **46**, 143–146 (1970).

[2] ——: Correction to the paper "Continuous affine transformations of locally compact totally disconnected groups" (to appear).

[3] ——: On locally compact abelian groups with dense orbits under continuous affine transformations. Proc. Japan Acad., **46**, 147–150 (1970).

[4] ——: Properties of ergodic affine transformations of locally compact groups. I, II. Proc. Japan Acad., **46**, 231–235, 236–238 (1970).