— **Articles** —

On a certain symmetric property in the geometry of numbers

Makoto Nagata

Osaka University of Pharmaceutical Sciences, 4-20-1 Nasahara, Takatsuki, Osaka 569-1094, Japan

(Received September 20, 2011; Accepted November 17, 2011)

We present a symmetric property on S_3 in connection with the so-called Minkowski's first theorem in the geometry of numbers.

1 Motivation and Results

There is a theorem that is called the "Theorem of Blichfeldt" [1, p.42, Theorem 2] related to Minkowski's first theorem in the geometry of numbers. We regard Theorem 1 below as (a subset version of) the Theorem of Blichfeldt.

For two subsets A and B of an abelian group, we write $A-B=\{a-b|a\in A,\ b\in B\}$. Here we use the symbols $+$, $-$ and 0 in the usual sense. By taking account of the adelic geometry of numbers, we consider the following: Let G be a locally compact abelian group, and let Λ be a discrete (at most countable) subgroup of G such that G/Λ is compact. Let μ be the Haar measure on G, and let F be a measurable fundamental domain for G/Λ such that F is contained in a compact subset. Put $d(\Lambda)=\mu(F)$. Suppose that $d(\Lambda)>0$. Let A be a measurable set contained in a compact subset of G.

Theorem 1. *If $\mu(A)>d(\Lambda)$, then $\Lambda\cap(A-A)\neq\{0\}$.*

A century has passed since the geometry of numbers came into being. In this paper, we are hardly interested in what Theorem 1 means. That is, our interest is not the existence of lattice points in a measurable set itself. Rather, our interest is a symmetry in the statement. This requires an explanation.

Note that $\Lambda=\Lambda-\Lambda$, i.e., Λ is also a "set of difference" as well as $A-A$. If one puts these 2 sets of difference as $P_1=\Lambda-\Lambda$, $P_2=A-A$, then Theorem 1 says that $P_1\cap P_2\neq\{0\}$. Needless to say, of course, it also says that $P_2\cap P_1\neq\{0\}$. Thus there is a (trivial!) symmetry on S_2 for these 2 sets of difference, P_1 and P_2, in Theorem 1; i.e., for any $\tau\in S_2$, $P_{\tau(1)}\cap P_{\tau(2)}\neq\{0\}$. Here S_2 is the symmetric group on 2 elements.

Question. What about a (nontrivial, if possible) symmetry on S_3? Here S_3 is the symmetric group on 3 elements.

Our answer to this question is the following: Let X be a subset of G. We introduce $X-X$ as the third set of difference. Let $P_1=\Lambda-\Lambda$, $P_2=A-A$ and $P_3=X-X$.

Theorem 2. *If $\#X\cdot\mu(A)>d(\Lambda)$, then $(P_{\tau(1)}\cap P_{\tau(2)})\cup((P_{\tau(1)}-P_{\tau(2)})\cap P_{\tau(3)})\neq\{0\}$ for all $\tau\in S_3$. Here $\#X$ denotes the cardinality of X.*

If $\#X=1$, then $X-X=\{0\}$, so it is obvious that Theorem 2 implies Theorem 1. Conversely we show that Theorem 1 implies Theorem 2.

大阪薬科大学　e-mail: paideia@gly.oups.ac.jp

2 Proofs

We recall a proof of Theorem 1. The following intuitive proof is well-known as "the average method." Note that it shows that $(\Lambda-\Lambda)\cap(A-A)\neq\{0\}$.

Proof of Theorem 1. (cf. [1, p.48, Theorem 2]) Let $f: G\to\mathbb{R}$ be the characteristic function of A: $f(x)=1$ if $x\in A$, $f(x)=0$ otherwise. Then

$$\int_F \sum_{a\in\Lambda} f(a+x)d\mu(x) = \int_G f(x)d\mu(x) \quad (=\mu(A))$$

Thus

$$\mu(F)\sup_{x\in F}\sum_{a\in\Lambda} f(a+x) \geq \mu(A)$$

Since $\mu(F)=d(\Lambda)$ and since $\mu(A)>d(\Lambda)$, we have $\sup_{x\in F}\Sigma_{a\in\Lambda} f(a+x)>1$. That is, there exists $x\in F$ and there exist a, $b\in\Lambda$ with $a\neq b$ such that $a+x$, $b+x\in A$. Therefore, $a-b\in A-A$.

We use Lemma 1 below in our proof of Theorem 2. It is deduced from Theorem 1, which is the case of $N=1$.

Lemma 1. *Let G, Λ, μ, $d(\Lambda)$ be as in Theorem 1. Let $N\geq 2$ be a natural number, fixed. Consider different N points $x_1, \ldots, x_N\in G$ and consider measurable sets $A_1, \ldots, A_N$ which are contained in a compact subset of G. Here it is not necessary that $A_i\neq A_j$ for $i\neq j$, but it is necessary that $x_i\neq x_j$ for $i\neq j$.*

If $x_i-x_j\notin A_i-A_j$ for all i, j $(i\neq j)$ and if $\Sigma_{i=1}^N \mu(A_i)>d(\Lambda)$, then there exist i, j (it is not necessary that $i\neq j$) and there exists $z\in\Lambda\setminus\{0\}$ such that $z+(x_i-x_j)\in A_i-A_j$.

Proof. We show first the equivalence between $(A_i-x_i)\cap(A_j-x_j)\neq\emptyset$ and $x_i-x_j\in A_i-A_j$ for $i\neq j$. Here A_i-x_i means $A_i-\{x_i\}$.

If there exists $x\in(A_i-x_i)\cap(A_j-x_j)$, then there also exists $a_i\in A_i$; and there exists $a_j\in A_j$ such that $a_i-x_i=x=a_j-x_j$. Therefore $x_i-x_j=a_i-a_j\in A_i-A_j$. Conversely, if $x_i-x_j\in A_i-A_j$, then there exists $a_i\in A_i$; and there also exists $a_j\in A_j$ such that $x_i-x_j=a_i-a_j$. Put $x:=a_i-x_i=a_j-x_j$, then $x\in(A_i-x_i)\cap(A_j-x_j)$.

Now, on the assumptions of Lemma 1, we have $(A_i-x_i)\cap(A_j-x_j)=\emptyset$ for $i\neq j$. Let A be a disjoint union $\sqcup_{i=1}^N(A_i-x_i)$. Then $\mu(A)=\Sigma_{i=1}^N \mu(A_i-x_i)=\Sigma_{i=1}^N\mu(A_i)>d(\Lambda)$. By Theorem 1, there exists $z\in\Lambda\setminus\{0\}$ such that $z\in A-A$. That is, there exist x, $y\in A$ such that $z=x-y$. Thus, there exist i, j (it is not necessary that $i\neq j$) such that $x\in A_i-x_i$, $y\in A_j-x_j$; and so there exist $a_i\in A_i$ and also $a_j\in A_j$ such that $x=a_i-x_i$, $y=a_j-x_j$. Therefore $z+(x_i-x_j)\in A_i-A_j$.

Proof of Theorem 2. If $\#X=1$, then $P_3=\{0\}$ and then Theorem 2 follows from Theorem 1. Now we assume that $\#X\geq 2$. Note that $P_i=-P_i$ for $i=1, 2, 3$.

Since $\#X\cdot\mu(A)>d(\Lambda)$, one can take $\{x_1, \ldots, x_N\}\subset X$ with $N\cdot\mu(A)>d(\Lambda)$. Let each $A_1, \ldots, A_N$ (in Lemma 1) be A. Then $\Sigma_{i=1}^N\mu(A_i)>d(\Lambda)$.

(Case 1) τ is the identity, that is, $\tau=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$: If $(P_1\setminus\{0\})\cap P_2\neq\emptyset$, then we have nothing to do. Assume that $(P_1\setminus\{0\})\cap P_2=\emptyset$.

If $x_i-x_j\notin A-A=P_2$ for all i, j $(i\neq j)$, then, by Lemma 1, there exist $z\in P_1\setminus\{0\}$, p, q (it is not necessary that $p\neq q$) and $b\in P_2$ such that $-z=b-(x_p-x_q)\in P_1\setminus\{0\}$. That is, $x_p-x_q=b+z$. If $p=q$, then $b+z=0$ and then $P_1\setminus\{0\}\ni -z=b\in P_2$, which contradicts to the assumption $(P_1\setminus\{0\})\cap P_2=\emptyset$. Thus, we have $p\neq q$. Therefore, $P_1-P_2\ni z+b=x_p-x_q\in P_3$ and, by $x_p-x_q\neq 0$, $(P_1-P_2)\cap P_3\neq\{0\}$.

If there exist i, j $(i\neq j)$ such that $x_i-x_j\in P_2$, then $P_3\ni x_i-x_j\in P_2\subset P_1-P_2$ and, by $x_i-x_j\neq 0$, $(P_1-P_2)\cap P_3\neq\{0\}$.

(Case 2) $\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$: Assume that $P_2\cap P_3=\{0\}$.

Note that $P_2 \cap P_3 \supset \{0\}$. Then $x_i - x_j \notin A - A$ for i, j $(i \neq j)$. By Lemma 1, there exist i, j (it is not necessary that $i \neq j$) such that $(\Lambda \setminus \{0\}) \cap (A-A) - \{x_i - x_j\} \neq \emptyset$. Therefore $(P_2 - P_3) \cap P_1 \neq \{0\}$.

(Case 3) $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$: If $P_3 \cap P_2 \neq \{0\}$, then, by $0 \in P_1$, $\{0\} \neq P_3 \cap P_2 \subset (P_1 - P_3) \cap P_2$. Thus, we can assume that $P_2 \cap P_3 = \{0\}$. By Case 2, we have $(P_2 - P_3) \cap P_1 \neq \{0\}$. That is, there exist $z \in P_1 \setminus \{0\}$, $b \in P_2$, $y \in P_3$ such that $z = b + y$.

If $b = 0$, then $0 \neq z = y$, meaning that $P_1 \cap P_3 \neq \{0\}$.

If $b \neq 0$, then, by $P_2 \ni b = z - y \in P_1 - P_3$, $(P_1 - P_3) \cap P_2 \neq \{0\}$. In either case, we have $(P_1 \cap P_3) \cup ((P_1 - P_3) \cap P_2) \neq \{0\}$.

(Case 4) The case of $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \left(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right)$ follows from Case 1 (resp. Cases 2, 3).

References

[1] P. M. Gruber, C. G. Lekkerkerker *Geometry of Numbers* North-Holland Mathematical Library, Vol. 37 1987 (2nd ed.)