70. On Complexes in a Finite Abelian Group. I

By Tamás SZŐNYI*) and Ferenc WETTL**)

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1988)

Let G be a finite abelian group, written additively, which will be fixed throughout this paper. We shall consider *complexes*, i.e. nonempty subsets of G. For $g \in G$ and two complexes A, B, we shall write

$$A+g=\{a+g \mid a \in A\},$$
$$A+B=\{a+b \mid a \in A,\ b \in B\},$$
$$A \circ B=\{a+b \mid a \in A,\ b \in B,\ a \neq b\}.$$

We were led to this latter operation $\circ$ in our geometric research [2] (see also [1]) on ovals in a finite projective plane, in which some of the results of the present paper were needed.

For a complex K, we shall write $|K|=k$, $|K \circ K|=m$. The object of this paper is to prove the following three theorems.

Theorem 1. *If $k=m>4$ for a complex K, then one of the two statements holds:*

(i) *K is a coset of a subgroup of G.*

(ii) *There exists an element g of G such that $K+g$ has only involutions and $(K+g) \cup \{0\}$ is a subgroup of G.*

Theorem 2. *If $K+K=K \circ K$, then one of the two statements holds:*

(i) *$K+K=K \circ K$ is a coset of a subgroup of G.*

(ii) $m \geq \frac{3}{2}k$.

Theorem 3. *If $|G|$ is odd and $K+K \neq K \circ K$, then*

$$m \geq \frac{k-3-\sqrt{5k^2-10k+9}}{2}=\frac{\sqrt{5}+1}{2}k-\frac{\sqrt{5}+3}{2}+0\left(\frac{1}{k}\right).$$

Let us begin with

Lemma 1. *K is a coset of a subgroup of G if and only if $k=|K+K|$.*

Proof. The only if part is obvious. Suppose now $k=|K+K|$. Let $a \in K$ and put $K-a=H$. Then clearly $0 \in H$, $|H|=k$ and $|H+H|=|K+K|=|H|$ and $H \subset H+H$ which implies $H=H+H$. Thus H is a subgroup of G and K is a coset of H.

Corollary. *If $k=m$ and $K \circ K=K+K$, then K is a coset of a subgroup of G.*

This corollary allows us to reformulate our Theorem 1 into the following form.

Theorem 1′. *Suppose $K+K \neq K \circ K$ and $k=m>4$. Then* (ii) *of Theo-*

---

*) Computer and Automation Institute, Hungarian Academy of Sciences.

**) Mathematical Department of Technical University, Budapest, Faculty of Transportation Engineering.

rem 1 holds.

This can be again reformulated as follows.

When $K+K\neq K\circ K$, K has an element a such that $2a$ can not be written as $b+c$, $b, c\in K$, $b\neq c$. Take such $a\in K$ and put $K'=K-a$. Then $0\in K'$, $0\notin K'\circ K'$, $|K'|=k$, $|K'\circ K'|=m$. Rewriting K for K', we see that the proof of Theorem 1′ can be reduced to that of

Theorem 1″. *Suppose*

$$(0)\qquad 0\in K \quad \textit{but} \quad 0\notin K\circ K.$$

If $k=m>4$, then $K\setminus\{0\}$ consists of involutions and there is an involution g of G such that $(K+g)\cup\{0\}$ becomes a subgroup of G.

In the following (until the end of the proof of this theorem except in the corollary to Lemma 3) we suppose always that our K satisfies (0). We introduce the following notations (for such K):

We put for $x\in K$, $x\neq 0$,

$$K_x=x+(K\setminus\{0, x\})$$

and for $u\in G$

$$K^u=\{x\in K\,|\,u\in K_x\}.$$

K^u consists of those elements of K for which $u=x+y$ has a solution with $x, y\in K$, $y\neq 0$, $x\neq y$. Obviously we have

$$0,\ x\in K_x\cup K^x,\quad |K_x|=k-2$$

and hence

$$|K_x\cap K|\geq (k-2)-(m-k+1)=2k-3-m.$$

Lemma 2. *Suppose that K (satisfying (0)) has no involution and $m\geq k$. Then $|K^u|\leq m-k+1$ for $u(\neq 0)\in K$.*

Proof. We have $K^u\cap K_u=\varnothing$, because from $x\in K^u\cap K_u$ would follow $u-x\in K$ (since $x\in K_u$) and $x-u\in K$ (since $x\in K^u$). Since K has no involution, $x-u\neq u-x$, but $0=(x-u)+(u-x)\in K\circ K$ in contradiction to (0). As $K^u\cup K_u\subset (K\circ K)\setminus\{u\}$, we obtain $m-1\geq |K^u\cup K_u|+|K^u\cap K_u|=|K^u|+|K_u|$ $=|K^u|+(k-2)$, whence conclusion.

Lemma 3. *If K (satisfying (0)) contains no involution, then $m\geq$ $(3/2)k-2$.*

Proof. We count $N=|\{(u, K_x)\,|\,u\in K_x\}|$ in two different ways. In counting first x and then $u\in K_x$, we see $N=(k-1)(k-2)$. If one counts first u and then x with $u\in K_x$, one obtains

$$N=\sum_{u\in K\circ K}|K^u|=\sum_{u\in (K\circ K)\cap K}|K^u|+\sum_{u\in (K\circ K)\setminus K}|K^u|$$
$$\leq (k-1)(m-k+1)+(m-k+1)(k-1)$$

in virtue of Lemma 2, as $|(K\circ K)\cap K|=k-1$, $|K^u|\leq m-k+1$, $|(K\circ K)\setminus K|=$ $m-k+1$, $|K^u|\leq k-1$, whence conclusion.

Corollary. *If K contains no involution and $k=m>4$, then $K\circ K=$ $K+K$, so that (in virtue of Corollary to Lemma 1) K is a coset of a subgroup of G.*

Remark. The following example shows that the number 4 in the above corollary can not be replaced by a smaller number. In this example, we have $k=m=4$, K contains no involution and is not a coset of any subgroup of G: $G=Z/12Z$, $K=\{1, 5, 7, 11\}$, $K\circ K=\{0, 4, 6, 8\}$.

Proof of Theorem 1''. We suppose that K satisfies (0) (so that $K\circ K\neq K+K$) and $m=k>4$. Put $K\backslash\{0\}=L$. As $K\ni 0$, we have $K\circ K\supset L$ and since $m=k$, $(K\circ K)\backslash L$ consists of just one element, denoted w, and from $x, y\in K$, $x\neq y$ follows $x+y\in L\subset K$ or $x+y=w$, an argument which will be repeatedly used in the following.

By the above corollary, K contains an involution, denoted a ($\neq 0$). Put $I_K=\{x\in K\,|\,2x=0\}$. We have $K\supset I_K\supset\{0, a\}$. Now we shall prove $K=I_K$ in showing that $K\backslash I_K\neq\varnothing$ leads to a contradiction.

An element x of $K\backslash I_K$ will be called *improper* if $a+x\in K$ and either $2x$ or $a+2x\in K$. We shall show that an improper element should exist, if $K\backslash I_K\neq\varnothing$.

Let x be any element of $K\backslash I_K$. Then $x\in K$ and $2x\neq 0$. We have $a\in K$ and $2a=0$, so that $a\neq x$. If $a+x\in K$ and $a+2x\neq w$, then x is improper, because $a+2x=(a+x)+x\in K$ since x, $a+x\in K$ and $x\neq a+x$.

Suppose $a+x\in K$ but $a+2x=w$. Then x is still improper, if $2x\in K$. Suppose therefore $2x\notin K$. As $k\geq 5$, $K\backslash\{0, a, x, a+x\}\neq\varnothing$ and we can take an element $y\in K\backslash\{0, a, x, a+x\}$. Then x, $y\in K$, $x\neq y$, and $x+y\neq a+2x=w$ (because $y\neq a+x$) so that $x+y\in L\subset K$ and $a+(x+y)=(a+x)+y\in K$ as $a+x$, $y\in K$, $a+x\neq y$, and $a+(x+y)\neq a+2x=w$ (because $x\neq y$). We have furthermore $2x+y=x+(x+y)\in K$ as x, $x+y\in K$, $x\neq x+y$ (because $y\neq 0$) and $2x+y\neq a+2x=w$ (because $y\neq a$), and $2(x+y)=(2x+y)+y\in K\circ K$ as $2x+y$, $y\in K$, $2x+y\neq y$ (because $2x\neq 0$). We have also $a+2(x+y)=(a+x+y)+(x+y)\in K\circ K$ as $a+x+y$, $x+y\in K$ and $a+x+y\neq x+y$. Thus both $2(x+y)$ and $a+2(x+y)\in K\circ K$. As these are different elements, one of them should be in K, and $x+y$ is improper. The existence of an improper element is thus shown in case $a+x\in K$.

Suppose now $a+x=w$. As $k\geq 5$, we can take an element y of $K\backslash\{0, a, x\}$. Then a, $y\in K$ and $a+y\neq a+x=w$. Therefore $a+y\in L\subset K$. If $2y=x$, we have $0\neq 2y\in K$ and y is improper. If $2y\neq x$, then $a+2y\neq a+x=w$ and $a+2y=(a+y)+y\in K\circ K$, so that $a+2y\in L\subset K$. Thus y is improper if $2y\neq 0$. In case $2y=0$, put $z=x+y$. We have x, $y\in K$, $x\neq y$ and $x+y\neq a+x=w$, therefore $z\in L\subset K$. Furthermore $2z=2x\neq 0$ and $a+z=a+(x+y)\in L\subset K$ as a, $x+y\in K$ and $(a+x)+y\neq a+x=w$, and $a+2z=(a+z)+z\in L\subset K$ as $a+z$, $z\in K$, $a+z\neq z$ and $a+2z=a+2x\neq a+x=w$. Thus z is improper, and we have shown the existence of an improper element in all cases.

Now let j be any natural number, and consider the following three properties of an improper element x:

$$A_j:\quad jx\neq 0 \quad\text{and}\quad a+jx\neq 0,$$
$$B_j:\quad jx\in K \quad\text{or}\quad a+jx\in K,$$
$$C_j:\quad jx\in K\circ K \quad\text{and}\quad a+jx\in K\circ K.$$

It is clear that C_j implies A_j and B_j. We see that C_{j+2} follows from A_j

and B_{j+1}. In fact

$$(j+2)x=x+(j+1)x=(a+x)+\{a+(j+1)x\}\in K\circ K$$

because $x\neq(j+1)x$, $a+x\neq a+(j+1)x$ in virtue of A_j, and x, $(j+1)x\in K$ or $(a+x)$, $a+(j+1)x\in K$ in virtue of B_{j+1} and the improperness of x,

$$a+(j+2)x=(a+x)+(j+1)x=x+\{a+(j+1)x\}\in K\circ K$$

holds for the same reason.

It is easy to see that A_j, B_j hold for $j=1, 2$ for any improper element x, whence C_3, C_4, $\cdots$ and A_3, A_4, $\cdots$ should follow which implies a contradiction because A_n can not hold if n is the order of x. Thus we have proved $K=I_K$. We see also that w is an involution because $w=u+v$, u, $v\in I_K$.

To complete the proof of our theorem, put $H=(K+w)\cup\{0\}$ and let us show that H is a subgroup of G. Using $K=I_K$, it is easily seen that $K+w=L\cup\{w\}=K\circ K$. Let x, $y\in H$. If x or $y=0$ or $x=y$, it is clear that $x+y\in H$. Otherwise we can write $x=x_0+w$, $y=y_0+w$, x_0, $y_0\in K$, $x_0\neq y_0$. Then $x+y=x_0+y_0\in K\circ K\subset H$, which shows that H is closed under addition.

(to be continued.)

References

[1] G. Korchmáros: Una generalizzazione del teorema di F. Buekenhout sulle ovali pascaliane. Boll. U. M. I., (5) 18-B, pp. 673–687 (1981).

[2] F. Wettl: On the nuclei of a point set of a finite projective plane. Journal of Geometry, **30**, 157–163 (1987).