Journal of Algebra and Applications
ISSN: 2217-6764, URL: http://www.ilirias.com
Volume 5 Issue 1(2015), Pages 1-5.

CYCLIC GROUPS WITH HAJÓS PROPERTY, AN ELEMENTARY APPROACH

SÁNDOR SZABÓ

Abstract. There is a complete description of the finite abelian groups possessing the so-called Hajós property. The known proofs of this important classification result rely on cyclotomic fields or characters even in the particular case of cyclic groups. This paper provides an elementary proof for the cyclic case.

1. Introduction.

Let G be a finite abelian group. We will use multiplicative notation in connection with abelian groups. Let A, B be subsets of G. The product AB is defined by $AB = \{ab : \ a \in A, \ b \in B\}$. The product AB is direct if

$$a_1 b_1 = a_2 b_2, \ a_1, a_2 \in A, \ b_1, b_2 \in B$$

imply that $a_1 = a_2$, $b_1 = b_2$. If the product AB is direct and if it is equal to G, then we say that the equation $G = AB$ is a factorization of G. A subset A of G is called normalized if the identity element e of G belongs to A. A factorization $G = AB$ is called a normalized factorization if the factors A and B are both normalized.

For a subset A of G the notation $\langle A\rangle$ stands for the smallest subgroup of G that contains A, that is, $\langle A\rangle$ denotes the span of A in G. We say that a normalized subset A of G is a full-rank subset of G if $\langle A\rangle = G$. We say that a normalized factorization $G = AB$ is a full-rank factorization if A and B are both full-rank subsets of G.

A subset A of G is termed periodic if there is a $g \in G \setminus \{e\}$ such that $gA = A$. The element g is called a period of A. It is clear that if g, h are periods of A and $gh \neq e$, then gh is also a period of A. The periods of A together with the identity element form a subgroup H of G. In fact the subset A is a union of cosets modulo H and consequently there is a subset C of G for which the product CH is direct and $CH = A$. A factorization $G = AB$ is defined to be periodic if either A or B is periodic. We say that the finite abelian group G has the Hajós property if either $G = \{e\}$ or $G \neq \{e\}$ and each factorization of G is periodic. It turns out that if G has the Hajós property, then so does each subgroup of G.

2010 *Mathematics Subject Classification.* 20K01, 05B45, 52C22, 68R05.

Key words and phrases. direct product of subsets, factoring abelian groups into subsets, normalized, periodic, full-rank subsets, normalized, periodic full-rank factorizations, Hajós property of groups.

Submitted November 8, 2015. Published November 30, 2015.

Let $t_1, \dots, t_s$ be not necessarily distinct prime powers with $t_i \geq 2$. We will express the fact that G is a direct product of cyclic groups of orders $t_1, \dots, t_s$ by saying that the type of G is $(t_1, \dots, t_s)$. There is a complete classification of the finite abelian groups possessing the Hajós property. To describe this let us consider the following list of group types.

$$\begin{array}{llll}
(p^\alpha, q), & (p^2, q^2), & (p^2, q, r), & (p, q, r, s), \\
(p^3, 2, 2), & (p^2, 2, 2, 2), & (p, 2^2, 2), & (p, 2, 2, 2, 2), \\
(p, q, 2, 2), & (p, 3, 3), & (3^2, 3), & (2^\alpha, 2), \\
 & (2^2, 2^2), & (p, p). &
\end{array}$$

Here p, q, r, s are distinct primes and $\alpha \geq 3$. A group whose type is on the list has the Hajós property and each group that has the Hajós property is a subgroup of such a group. The above characterization of groups with Hajós property first appeared in [3]. This is one of the most frequently used results of the factorization theory of finite abelian groups. The first row of the list contains cyclic groups. This result first appeard in [2]. The multiplicative group of the non-zero elements of a finite field is cyclic and from this reason the classification of finite cyclic groups with Hajós property is widely applied and it is an important result on its own right.

The known proofs of the classification result on groups with Hajós property are relying on the theory of cyclotomic polynomials and cyclotomic fields or alternatively on characters of finite abelian groups. We will show that for the cyclic case the classification can be accomplished using only elementary group theoretical techniques.

2. Preliminaries.

The next observation is well-known. When we want to decide if a factorization $G = AB$ of a finite abelian group G is periodic we may focus our attention on normalized factorizations. To see why let us choose $a \in A$, $b \in B$. Multiplying the factorization $G = AB$ by $a^{-1}b^{-1}$ we get the normalized factorization $G = Ga^{-1}b^{-1} = (Aa^{-1})(Bb^{-1})$. Note that a subset A of G is periodic if and only if (Aa^{-1}) is periodic.

Let G be a finite abelian group whose order is devisible by a prime p. There are unique subgroups H and K of G such that the order of H is a power of p and the order of K is relatively prime to p further $G = HK$ is factorization of G. Consequently each element $g \in G$ can be uniquely written as a product $g = hk$, where $h \in H$ and $k \in K$. In what follows we will say that h is the p-part of the element g. Note that when G is a p-group, then $H = G$ and $K = \{e\}$ hold.

We will use the following result several times.

Lemma 2.1. *Let $G = AB$ be a normalized factorization of the finite cyclic group G such that $|A| = p$ is a prime. Then the factorization is periodic.*

Proof. Since G is a cyclic group, it has a unique subgroup L of order p. Let A' be the set of the p-parts of the elements of A. It is a corollary of Proposition 3 of [4] that in the factorization $G = AB$ the factor A can be replaced by A' to get the normalized factorization $G = A'B$. From $|G| = |A||B|$, $|G| = |A'||B|$ it follows that $|A| = |A'|$. In other words the p-parts of the elements of A are pair-wise distinct. In particular, the p-part of each element $a \in A \setminus \{e\}$ is distinct from e. Therefore p is a divisor of $|a|$ for each $a \in A \setminus \{e\}$.

If $|a| = p$ for each $a \in A \setminus \{e\}$, then $A = L$ and consequently A is periodic. Thus we may assume that $|a| \neq p$ for some $a \in A \setminus \{e\}$. Set $C = \{e, a, a^2, \dots, a^{p-1}\}$. By Lemma 3 of [6], in the factorization $G = AB$ the factor A can be replaced by C to get the normalized factorization $G = CB$. From the proof of Lemma 1 of [5] we know that a^p is a period of B. □

The following result is Theorem 3 of [7]. For easier reference we state it as a lemma.

Lemma 2.2. *Let p, q be distinct primes and let G be a finite abelian group whose p-component and q-component are cyclic. If $G = AB$ is a normalized factorization of G such that $|A| = p^\alpha q^\beta$, then the factorization is not full-rank.*

We defined products and direct products of subsets only for two subsets. However, even if one works with factorizations involving two subsets factorizations involving more factors occur inevitably. So we extend our definitions. The product of the subsets $A_1, \dots, A_n$ of G is equal to

$$\{a_1 \cdots a_n : \ a_1 \in A_1, \dots, a_n \in A_n\}.$$

The product $A_1 \cdots A_n$ is direct if

$$a_{1,1} \cdots a_{1,n} = a_{2,1} \cdots a_{2,n}, \ a_{1,1}, a_{2,1} \in A_1, \dots, a_{1,n}, a_{2,n} \in A_n$$

imply $a_{1,1} = a_{2,1}, \dots, a_{1,n} = a_{2,n}$. This extended version will be used only once with $n = 4$.

3. Two propositions.

In this section we will show that the cyclic groups on the list in Section 1 have the Hajós property.

Proposition 3.1. *Let G be a finite abelian group of type (p^α, q), where p, q are distinct primes, $\alpha \geq 1$. Then each factorization of G is periodic.*

Proof. Let $G = AB$ be a factorization of G. We may assume that the factorization is normalized. We may choose the notations such that $|A| = p^\lambda$, $\lambda \geq 1$ and $|B| = p^\mu q$, $\mu \geq 0$.

In the $\alpha = 1$ case $|A| = p$, $|B| = q$. Now Lemma 2.1 is applicable and gives that either A or B is periodic. We may assume that $\alpha \geq 2$ and we start an induction on $|G|$. By Lemma 2.2, either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$.

Let us deal with the $\langle B \rangle \neq G$ case first. Set $H = \langle B \rangle$. If B is periodic, then there is nothing to prove. Thus we may assume that B is not periodic. If $B = H$, then B is a subgroup distinct from $\{e\}$ and so B is periodic. Thus we may assume that $B \neq H$. Choose an element $a \in A$. Multiplying the factorization $G = AB$ by a^{-1} provides the normalized factorization $G = Ga^{-1} = (Aa^{-1})B$. Restricting this factorization to H we get the normalized factorization $H = G \cap H = (Aa^{-1} \cap H)B$. Considering the cardinalities yields $|H| = |Aa^{-1} \cap H||B|$. It follows that $|Aa^{-1} \cap H| = p^\gamma$ with some $\gamma \geq 0$. As $B \neq H$, we get $\gamma \geq 1$.

By the inductive assumption on $|G|$ from the factorization $H = (Aa^{-1} \cap H)B$ we get that either $Aa^{-1} \cap H$ or B is periodic. Only $Aa^{-1} \cap H$ can be periodic. Let g be a period of $Aa^{-1} \cap H$. As $|g|$ divides $|Aa^{-1} \cap H| = p^\gamma$ we may assume that $|g| = p$. The group G has a unique subgroup L of order p. Since $Aa^{-1} \cap H$ is a normalized subset of H, it follows that $g \in (Aa^{-1} \cap H)$ and so $\langle g \rangle = L \subseteq (Aa^{-1} \cap H)$. This means that

$$L \subseteq \bigcap_{a \in A} Aa^{-1}.$$

By Lemma 3 of [1], A is periodic.

Let us turn to the $\langle A \rangle \neq G$ case. If A is periodic, then there is nothing to prove and so we may assume that A is not periodic. Set $H = \langle A \rangle$. If $A = H$, then A is a subgroup of G and in particular A is periodic. Thus we may assume that $A \neq H$.

Let us choose an element $b \in B$. Multiplying the factorization $G = AB$ by b^{-1} we get the normalized factorization $G = Gb^{-1} = A(Bb^{-1})$. Restricting this factorization to H yields the normalized factorization $H = G \cap H = A(Bb^{-1} \cap H)$.

If q does not divide $|H|$, then H is a p-group and the equality $|H| = |A||Bb^{-1} \cap H|$ shows that q does not divide $|Bb^{-1} \cap H|$. By the inductive assumption on $|G|$ from the factorization $H = A(Bb^{-1} \cap H)$ we can conclude that either A or $Bb^{-1} \cap H$ is periodic. Only $Bb^{-1} \cap H$ can be periodic. Let g be a period of $Bb^{-1} \cap H$. We may assume that $|g| = p$ and as before it follows that B is periodic.

For the remaining part of the proof we may assume that q divides $|H|$. Let A' be the set of the p-parts of the elements of A. It is a consequence of Proposition 3 of [4] that in the factorization $H = A(Bb^{-1} \cap H)$ the factor A can be replaced by A' to get the normalized factorization $H = A'(Bb^{-1} \cap H)$. If A' is not periodic, then arguing as before we get that B is periodic. Thus we may assume that A' is periodic. Using that $|A'| = p^{\lambda}$ we get that L is a direct factor of A', that is, there is a normalized subset C of G such that the product CL is direct and $CL = A'$. By the inductive assumption on $|G|$ from the factorization $H = A(Bb^{-1} \cap H)$ it follows that either A or $Bb^{-1} \cap H$ is periodic. Only $Bb^{-1} \cap H$ can be periodic. Let g be a period of $Bb^{-1} \cap H$. We may assume that $|g| = p$ or $|g| = q$.

If $|g| = p$, then L is a direct factor of $Bb^{-1} \cap H$. This means that there is a normalized subset D of G such that the product DL is direct and $DL = (Bb^{-1} \cap H)$. Using $H = A'(Bb^{-1} \cap H)$ we get the normalized factorization $H = (CL)(DL)$. This leads to the contradiction that the product LL is direct.

Therefore we may assume that $|g| = q$. The group G has a unique subgroup M of order q. From $\langle g \rangle = M \subseteq (Bb^{-1} \cap H)$ we get

$$M \subseteq \bigcap_{b \in B} Bb^{-1}.$$

By Lemma 3 of [1], B is periodic. □

Proposition 3.2. *Let G be a cyclic group such that $|G|$ is a product of four not necessarily distinct primes. Then each factorization of G is periodic.*

Proof. Let $G = AB$ be a factorization of G. We may assume that the factorization is normalized and $|A| \neq 1$, $|B| \neq 1$. If one of $|A|$, $|B|$ is a prime, then by Lemma 2.1, either A or B is periodic. For the rest of the proof we may assume that $|A|$, $|B|$ are both products of two not necessarily distinct primes. By Lemma 2.2, either $\langle A \rangle \neq G$ or $\langle B \rangle \neq G$. By symmetry we may assume that $\langle A \rangle \neq G$.

If A is periodic, then there is nothing to prove and so we may assume that A is not periodic. Set $H = \langle A \rangle$. If $A = H$, then A is periodic. Therefore we assume that $A \neq H$. Let us choose an element $b \in B$. Multiplying the factorization $G = AB$ by b^{-1} we get the normalized factorization $G = Gb^{-1} = A(Bb^{-1})$. Restricting this factorization to H gives the normalized factorization $H = G \cap H = A(Bb^{-1} \cap H)$.

From $|H| = |A||Bb^{-1} \cap H|$, $B \neq H$, $H \neq G$ it follows that $|Bb^{-1} \cap H| = p$ is a prime.

The group G has a unique subgroup L of order p. By Lemma 2.1, from the factorization $H = A(Bb^{-1} \cap H)$ we get that either A or $Bb^{-1} \cap H$ is periodic. Only $Bb^{-1} \cap H$ can be periodic. Now $L = (Bb^{-1} \cap H)$. This gives that

$$L \subseteq \bigcap_{b \in B} Bb^{-1}.$$

By Lemma 3 of [1], B is periodic. $\square$

Acknowledgments. The authors would like to thank the anonymous referee for his/her comments that helped us improve this article.

References

[1] K. Corrádi and S. Szabó, Factoring by subsets of cardinality of a prime or a power of a prime, *Communications in Algebra*, **19** (1991), 1585–1592.

[2] A. D. Sands, On the factorisation of finite abelian groups, *Acta Math. Acad. Sci. Hungar.* **8** (1957), 65–86.

[3] A. D. Sands, On the factorisation of finite abelian groups II, *Acta Math. Acad. Sci. Hungar.* **13** (1962), 153–169.

[4] A. D. Sands, Replacement of factors by subgroups in the factorization of abelian groups, *Bull. London Math. Soc.*, **32** (2000), 297–304.

[5] S. Szabó, An elementary proof of Hajós' theorem through a generalization, *Mathematica Japonica* **40** (1994), 1–9.

[6] S. Szabó, Factoring an infinite abelian group by subsets, *Periodica Mathematica Hungarica*, **40** (2000), 135–140.

[7] S. Szabó, Completing codes and the Rédei property of groups, *Theoretical Computer Science* **359** (2006), 449–454.

Sándor Szabó
Institute of Mathematics and Informatics University of Pécs Ifjúság u. 6 7624 Pécs, HUNGARY
E-mail address: sszabo7@hotmail.com