Open Journal of Discrete Mathematics, 2011, 1, 136-138
doi:10.4236/ojdm.2011.13017 Published Online October 2011 (http://www.SciRP.org/journal/ojdm)

An Application of Cyclotomic Polynomial to Factorization of Finite Abelian Groups*

Khalid Amin
University of Bahrain, *Department of Mathematics*, *Sakhir*, *Kingdom of Bahrain*
E-mail: *kamin@sci.uob.bh*
Received June 21, 2011; *revised July* 25, 2011; *accepted August* 21, 2011

Abstract

A finite abelian group G is said to have the Hajós-k-property (k>1) if from any decomposition $G = A_1 A_2 ... A_K$ of G into a direct product of its subsets, it follows that one of these subsets A_i is periodic, meaning that there exists a nonidentity element g in G such that $gA_i = A_i$. Using some properties of the cyclotomic polynomials, we will show that the cyclic groups of orders p^α and groups of type (p^2, q^2), where p and q are primes have this property. We also include a partial result about groups of type (p^α, q^β), where p and q are distinct primes and α, β are integers ≥ 1.

Keywords: Factorization of Finite Abelian Groups, Hajós Property

1. Introduction

Let G be a finite abelian group with identity element e. If G is a direct product of cyclic groups of orders $m_1, m_2, \cdots, m_r$, we say that G is of type $(m_1, m_2, \cdots, m_r)$. If $A_1, A_2, \cdots, A_k$ are subsets of G such that each element g of G can be expressed in a unique way as $g = a_1 a_2 \cdots a_k$, where $a_i \in A_i$, we write $G = A_1 A_2, \cdots A_k$ and say that we have a *factorization* of G. If in addition each contains the identity element G, we say that we have a *normalized factorization* of G. We will use $|A_i|$ to denote the number of elements of A_i. Similarly $|g|$ will donate the order of the element g of G. A subset A of G is called *periodic* if there is a non-identity element g in G such that $gA = A$.

The topic of factorizations of abelian groups arose when Hajós [2] solved a conjecture by H. Minkowski [3] concerning lattice tiling after transforming it into a theorem about finite abelian groups. For reference, we state this theorm below:

If $G = A_1 A_2, \cdots A_k$ is a factorization of a finite abelian group G, where each of the subsests is of the form $\{e, a, a, \cdots a^r\}$, then at least one of these subsets is a subgroup of G.

L. Rédei [4] generalized this to:

If $G = A_1 A_2, \cdots A_k$ is a factorization of a finite abelian group G, where each of the subsets has a prime number of elements and contains the identity e, then at least one of these subsets is a subgroup of G.

A. Sands [5] classified groups with Hajós-2-proprty which we list below:

$$(p^\alpha, q), (p^2, q^2), (p^2, q, r), (p, q, r, s)$$
$$(p^3, 2, 2), (p^2, 2, 2, 2), (p, 2^2, 2), (p, 2, 2, 2, 2)$$
$$(p, q, 2, 2), (p, 3, 3), (3^2, 3), (2^\alpha, 2)$$
$$(2^2, 2^2), (p, p)$$

where p, q, r and s are primes and $\alpha \geq 1$ is an integer.

2. Preliminaries

Let G be a cyclic group of order n, with generator g. Let us write $G = \sum_{i=0}^{n-1} g^i$. Similarly, for a subset $A = \{g^{\alpha_1}, g^{\alpha_2}, \cdots, g^{\alpha_r}\}$ of G, we write $A = \sum_{i=0}^{r} g^{\alpha_i}$.

Then we can write

$$A_1 A_2 \cdots A_k = \left(\sum_{i=1}^{\eta_1} g^{\alpha_i}\right)\left(\sum_{i=1}^{\eta_2} g^{\alpha_i}\right) \cdots \left(\sum_{i=1}^{\eta_2} g^{\alpha_i}\right),$$

Where multiplication is carried out in the group ring $Z(G)$. Thus, when multiplication is carried out we regard A_i as polynomials in g provided that addition of

*Mathematics Subject Classification: 20K01

the indices is carried out module *n*. *i.e.* polynomials are multiplied $mod\left(g^n-1\right)$.

Now, if we replace *g* by *x* and write $A_i(x)=\sum_{i=1}^{r_i}x^{\alpha_i}$ then from the relation $G=A_1A_2,\cdots A_k$, then we get:

$$G(x)=A_1(x)A_2(x)...A_k(x)\bmod(x^n-1)$$

As $\left(x^{n-1}+\cdots x+1\right)$ is a factor of x^n-1, it follows that each irreducible divisor of $\left(x^{n-1}+\cdots x+1\right)$ will divide one of the polynomials $A_i(x)$. These irreducible polynomials are the *cyclotomic polynomials* whose roots are the *d*-th *primitive* roots of unity where $d\,|\,n$ and $d>1$.

At some stage in this work, we shall need the following facts about the cyclotomic polynomials.

1) The *n*-th cyclotomic polynomial is usually denoted by $\Phi_n(x)$ and is given by:

$$\Phi_n(x)=\prod_{d|n}\left(1-x^{\frac{n}{d}}\right)^{\mu(d)}$$

2) The $\Phi_n(x)'s$ have integer coefficients *i.e.* $\Phi_n(x)\in Z(x)$ and they are irreducible and relatively prime.

Slightly modifying the notation of De Bruijn [1], we also define for a divisor *d* of *n*, the polynomial

$$\Phi_{n,d}(x)=\frac{1-x^n}{1-x^{\frac{n}{d}}}=1+x^{\frac{n}{d}}+x^{2\frac{n}{d}}+\cdots+x^{(d-1)\frac{n}{d}}$$

3. Results

Before we embark on showing our results, we must mention that all factorizations can be assumed to be normalized, for if $G=A_1A_2,\cdots A_k$ is a factorization of G, then since each A_i is non-empty, there exists an element a_i is $A_i, 1\le i\le k$. Multiplying *G* by $g=\left(a_1a_2,\cdots a_k\right)^{-1}$, we get that $G=gG=a_1^{-1}A_1a_2^{-1}A_2,\cdots a_k^{-1}A_k$, which is clearly normalized.

Theorem 3.1 Let *p* be a prime. If *G* is a cyclic group of order $n=p^\alpha$, then *G* has the Hajos-*k*-proprty, for all *k*, $1<k\le\alpha$.

Proof Let *G* be generated by *g* and consider the factorization $G=A_1A_2,\cdots A_k$ of *G*. Our previous discussion leads to the following congruence relation:

$$G(x)\equiv A_1(x)A_2(x)\cdots A_k(x)\,mod\left(x^n-1\right).$$

Now, $\Phi_n(x)$ divides some $A_i(x)$. But

$$\Phi_n(x)=\Phi_{p^\alpha}(x)=\frac{x^{p^\alpha}-1}{x^{p^{\alpha-1}}-1}.$$

Thus, $\frac{x^{p^\alpha}-1}{x^{p^{\alpha-1}}-1}$ divides $A_i(x)$. It follows that A_i is periodic with period $g^{p^{\alpha-1}}$ □

As an illustration, consider a cyclic group $G=\langle g\rangle$ of order $8=2^3$. Let $A=\left\{e,g,g^4,g^5\right\}$ and $B=\left\{e,g^2\right\}$. Then it is easy to verify that $AB=G$ is a factorization of *G* and that *A* is periodic with period $g^4=g^{2^{3-1}}$.

We shall use the following theorem by De Bruijn [1] in showing our next result.

If $n=p^\alpha q^\beta$, *where* p, q *are distinct primes and* $\alpha,\beta\ge1$, $F(x)\in Z[x]$ *and* $\Phi_n(x)$ *divides* $F(x)$, *then* $F(x)=g(x)\Phi_{n,p}(x)+h(x)\Phi_{n,q}(x)$ *for some polynomials* $g(x),\ h(x)\in Z[x]$.

Theorem 3.2 If *G* is of type $\left(p^2,q^2\right)$, where *p* and *q* are distinct primes, then *G* has the Hajos-*k*-property, for all *k*, $1<k\le4$.

Proof Consider a factorization $G=A_1A_2,\cdots A_k$ of *G*. The case $k=4$ is true by Redei's theorem. The case $k=3$, is true by Redei theorem and Theorem 2 of Sands [5]. Thus, we only need detail the case $k=2$. Say $G=A_1A_2$ in which both factors contain *pq* elements. Again by our previous discussion, we obtain the relation

$$G(x)\equiv A_1(x)A_2(x)\bmod(x^n-1),$$

where $n=p^2q^2$. It follows that $\Phi_n(x)$ divides $A_1(x)A_2(x)$. Since A_1 and A_2 contain the same number of elements, we may and shall assume that $\Phi_n(x)$ divides $A_1(x)$. Then, by De Bruijn's result above, we get that

$$A_1(x)=f(x)\Phi_{n,p}(x)+g(x)\Phi_{n,q}(x).$$

Therefore,

$$A_1(x)=f(x)\frac{x^n-1}{x^{\frac{n}{p}}-1}+g(x)\frac{x^n-1}{x^{\frac{n}{q}}-1}.$$

Now:

$$A_1(1)=pq=pf(1)+qg(1)$$

Therefore, either $f(1)=q$ and $g(1)=0$, or $f(1)=0$ and $g(1)=p$. In the first case, $g(x)=0$, and $\frac{x^n-1}{x^{n/p}-1}$ divides $A_1(x)$ in which case A_1 is periodic with period $g^{n/p}$. In the second case, $f(x)=0$ and $\frac{x^n-1}{x^{n/q}-1}$ divides $A_1(x)$ and so A_1 is periodic with period $g^{n/p}$. □

Corollary 3.1 If *G* is of type $\left(p^\alpha,q^\beta\right)$, where *p* and *q* are distinct primes, and α,β are integers ≥1, then *G*

has the Hajós-k-property, where $k = (\alpha + \beta)/2$.

4. References

[1] N. G. De Bruijn, "On the Factorization of Finite Cyclic Groups," *Indagationes Mathematicae*, Vol. 15, No.4, 1953, pp. 370-377.

[2] G. Hajos, "Uber Einfache und Mehrfaache Bedekung des n-Dimensionales Raumes Mit Einem Wurfelgitter," *Mathematics Zeitschrift*, Vol. 47, No. 1, 1942, pp. 427-467. doi:10.1007/BF01180974

[3] H. Minkowski, "Diophantische Approximationen," Teuner, Leipzig, 1907.

[4] L. Redei, "Ein Beitrag Zum Problem Der Faktorisation Von Endlichen Abelschen Gruppen," *Acta Mathematics Hungarica*, Vol. 1, No. 2-4, 1950, pp. 197-207. doi:10.1007/BF02021312

[5] A. Sands, "Factorization of Finite Abelian Groups," *Acta Mathematics Hungarica*, Vol. 13, No. 1-2, 1962, pp. 153-169. doi:10.1007/BF02033634

