International Journal of Algebra, Vol. 5, 2011, no. 4, 183 - 187

Subgroup Structure of Finite n-Ary Groups

Awni Fayez Al-Dababseh[*a,b]

[a]Department of Mathematics, Faculty of Science, Hail University,
Hail 2440, Saudi Arabia

[b]Department of Mathematics and Statistics, Faculty of Science,
Al-Hussein Bin Tall University Ma'an, Jordan
*Awni69@yahoo.com

Abstract

In this paper, we establish some properties of subgroup structure of finite n-ary groups.

Mathematics Subject Classification: 20N15

Keywords: Finite n-ary group; Idempotent element; Derived group

1 Introduction

Let X be nonempty set. We remind that, the system $G =< X, () >$ with one n-ary operation $() : X^n \to X$ is called n-ary group [1], if it is associative and for all $a_1, a_2, ..a_{i-1}, a_{i+1}...a_n, a \in X$ the equation are

$$(a_1a_2.......a_{i-1}xa_{i+1}........a_n) = a \tag{1}$$

solvable in X(where $i = 1, 2, 3, ..., n$).

n-Ary groups inherit many properties from binary groups (there are invariant and semivariant subgroups) analogous by properties of invariant subgroups of groups in binary groups. On the other hand because for $n \geq 3$ n-ary group hasn't identity element in general case or have two, three and more identity element(see for example [2]), then the theory of n-ary groups is specific with respect to the group theory and theories algebraic systems of other types.

n-Ary groups as n-ary systems have many application in different branches. For example, in the theory of automata [3] n-ary semigroups and n-ary groups are used. Some n-ary structures induced by hypercube have application in error -correctung and error-detecting coding theory, cryptology, as well as in the theory of (t, m, s)-nets (see for example [4, 5]).

Subgroups structure one of the interesting approach of the theory of finite n-ary group. The aim of this paper to give some properties of n-ary subgroups.

2 Preliminaries

The sequence of elements $x_i, x_{i+1}, ..., x_j$ is denoted by ${x_i}^j$. In the case $j < i$ it is the empty symbol. The sequence of elements $x, x, .., x$ is denoted by x^k.

Definition 2.1 *Let G be n-ary group. Then, $x_1^{k(n-1)}$ is an identity if $\left(x\, x_1^{k(n-1)}\right) = \left(x_1^{k(n-1)} x\right) = x$ for all $x \in G$.*

Definition 2.2 *Let G be n-ary group and let $x \in G$. Then, the sequence of elements $\bar{x}$ of G is called an inverse of x if $x\bar{x}$ is an identity.*

Definition 2.3 *Let i be an element of n-ary group $< G, () >$. Then, i is called idempotent element if $(ii...i) = i$.*

Definition 2.4 *Let s be an integer and a is an element of n-ary group G. Then, the $s - th$ $n - adic$ power of the element a is the element $a^{[s]}$ of G such that :*

1. *If $s = 0$, then $a^{[s]} = a$.*
2. *If $s > 0$, then $a^{[s]} = (a^{s(n-1)+1})$.*
3. *If $s < 0$, then $a^{[s]}$ is the solution of $(xa^{-s(n-1)}) = a$, that is $(a^{[s]}a^{-s(n-1)}) = a$*

Definition 2.5 *n-ary group $G =< X, () >$ is called derived from the binary group $B =< X, * >$ if $(x_1^n) = x_1 * x_2 * ... x_n *$ for all sequence x_1^n in X^n.*

Theorem 2.6 *[1] n-ary group $G =< X, () >$ is derived from the binary group $B =< X, * >$ if and only if G has an identity element.*

Lemma 2.7 *[1] Let k_1 and k_2 are integer numbers and let a be an element of n-ary group G, then $\left(a^{[k1]}\right)^{[k2]} = a^{[k1k2(n-1)+k1+k2]}$*

Lemma 2.8 *[1] Let a be an element of n-ary group G with finite n-adic order m, then $a^{[s]} = a^{[r]}$ if and only if $s - r$ is a multiple of m.*

Lemma 2.9 *[1] Let a be an element of n-ary group G with finite n-adic order m, then $a^{[s]} = a$ if and only if s is a multiple of m.*

Lemma 2.10 *[1] Let a be an element of n-ary group G with finite n-adic order m, then $|\langle a\rangle| = \mathrm{m}$, and$\langle \mathrm{a}\rangle = \{\mathrm{a}^{[0]} = a, \mathrm{a}^{[1]}, ..., \mathrm{a}^{[\mathrm{m}-1]}\}$*

3 Main Results

In this section, we are going to prove the following

Theorem 3.1 *Let $G =< X, () >$ finite n-ary group, $|G| = g = rs$, where $gcd(r, s) = 1$ and $gcd(r, n-1) = 1$, and let G haven't any idempotent element ,then G have at least one subgroup which order divides s.*

Proof. Let c be any fixed element of n-ary group G and let $C =< c >$. Consider the following possible cases :

Case 1: Let $C \neq G$ and let $|C| = g_1$, then g_1 is a divisor of g using Lagrange Theorem of n-ary groups [1]. It is clear that $g_1 > 1$, and g_1 can be written as $g_1 = r_1.s_1$ where r_1 is a factor of r and s_1 is a factor of s. It follows that, $gcd(r_1, s_1) = 1$ and $gcd(r_1, n-1) = 1$. We want to show that there exists an element c_1 in C such that $c_1^{[s_1]} = c_1$. Consider the linear congruence

$$s_1(n-1)y \equiv -s_1(\bmod g_1) \tag{2}$$

Since $gcd(s_1(n-1), g_1) = s_1$, then the congruence (2) has s_1 mutually incongruent solutions modulo g_1 . Let g_2 one of them . Then,

$$s_1(n-1)g_2 \equiv -s_1(\bmod g_1) \tag{3}$$

or $s_1(n-1)g_2 + s_1 = g_1.t$.

By lemma (2.7) and lemma (2.8) we get that,

$$(c^{[g_2]})^{[s_1]} = c^{[g_2 s_1(n-1)+s_1+g_2]} = c^{[g_1 t+g_2]} = c^{[g_2]} \tag{4}$$

This implies that ,there exists an element $c_1 = c^{[g_2]}$ in C such that $c_1 = c_1^{[s_1]}$. Let s_2 be the finite n-adic order of c_1 (the smallest positive integer such that: $c_1^{[s_2]} = c_1$), then by lemma (2.9) s_2 is a factor of s_1 so s. By lemma (2.10) the order of C is s_2. Hence G have a subgroup which order divides s.

Case 2: Let $C = G$. By Post Theorem [6] in G there exist uniquely cyclic subgroup with order s.

Example 3.2 *Let $X = \{1, a, a^2, a^3, b, ba, ba^2, ba^3\}$, and let $< X, . >$ be quaternion group. If we define on X n-ary operation $()$ such that $(x_1^n) = x_1 \cdot x_2 \cdots x_n \cdot a^2$, then $G =< X, () >$ is Hamiltonian n-ary group without idempotent elements. In [1], Rusakov show that the Hamiltonian n-ary group G have four subgroups with order two ($A =< 1 >, B =< a >, C =< b >, D =< ba >$) and six subgroups of order four ($< \{1, a, a^2, a^3\}, () >, < \{1, a^2, b, ba\}, () >, < \{1, a^2, ba, ba^2\}, () >, < \{a, a^3, b, ba^2\}, () >, < \{a, a^3, ba, ba^3\}, () >, < \{b, ba, ba^2, ba^3\}, () >$).*

Theorem 3.3 *Let $G =< X, () >$ be n-ary group with finite odd order and let n be an odd natural number also. If G has an identity element, then it is the unique idempotent element in G.*

Proof. Let $B =< X, * >$ be a binary group. If $|G| = 1$, then it is contains only the identity element, so contains an idempotent. Let $|G| = 2m+1, m \geq 1$ and let e be the identity element of G. If we defined the binary operation $*$ as follows

$$x_1 * x_2 = (x_1 x_2 e^n - 2) \quad \forall x_1 \ , x_2 \in X \tag{5}$$

Then we have $x*e = x$ which means that e is an identity element of the binary operation defined on B, so the group G is derived from the binary group B. Let e_1 be an idempotent element in G such that $e1 \neq e$. Since $({e_1}^n) = {e_1}^n = e_1$, then ${e_1}^{n-1} = e$. Contradiction, because the order of the element must divide the order of the group, so $e_1 = e$.

The following results are corollary's from Theorem (2.6)[7].

Corollary 3.4 *If the set of idempotent elements of a given n-ary group is non-empty, then it is a commutative n-ary subgroup.*

Corollary 3.5 *If i_1 and i_2 are idempotent elements of a ternary group $G =< X, () >$, then $< i_1, i_2, () >$ is a ternary subgroup of G.*

ACKNOWLEDGEMENTS.

The author thanks the administration of Al-Hussein Bin Tall University for granting him a sabbatical year during he developed this work.

References

[1] C.A. Rusakov, *Algebraic n-ary systems*, Minsk, Navuka Tehnika 1992.

[2] A. W. Dudek, K. Gtazek, Around the Hossz-Gluskin theorem for n-ary groups, *Discrete Mathematics,* **21** (2008) 4861 - 4876.

[3] J.W. Grzymala-Busse, Automorphisms of polyadic automata, *J. Assoc. Comput. Mach.* **16** (1969) 208 - 219.

[4] C. F. Laywine, G. L. Mullen, *Discrete Mathematics Using Latin Squares* Wiley, New York 1998.

[5] C. F. Laywine, G. L. Mullen, G. Whittle, D-dimensional hypercubes and the Euler and MacNeish conjectures, *Monatsh. Math.* **111** (1995) 223 - 238.

[6] E . L. Post, Polydic groups. *Trans. Amer.Math.Soc.* **48** 1940 208 - 350.

[7] A. W. Dudek, Idempotents in n-ary semigroups, *Southeast Asian Bulletion of Mathematics*, **25** (2001) 97 - 104.

Received: September, 2010