SOLUTIONS OF THE FROBENIUS CLASS EQUATION IN ALTERNATING GROUPS

SHUKER MAHMOOD KHOLIL

UNIVERSITI SAINS MALAYSIA

2012

SOLUTIONS OF THE FROBENIUS CLASS EQUATION IN ALTERNATING GROUPS

by

SHUKER MAHMOOD KHOLIL

Thesis submitted in fulfillment of the
requirements for the degree of
Doctor of Philosophy in
Mathematics

2012

ACKNOWLEDGMENTS

First of all, I wish to express my great thanks to the Almighty Allah for enabling me to complete this work. Second, I would like to acknowledge the indispensable role of several people in planning, writing, and revising this project. In this regard, I would like to thank my supervisor Associate Professor Dr. Andrew Rajah for his patient guidance in helping me to do this research. His sound advice and positive energy always encouraged me to advance more in my research.

A big thank-you goes to the staff of the main office of The School of Mathematical Sciences for their cooperative spirit, assistance, and punctuality. Finally, I extend my profuse thanks to my parents, family, children, and friends for their prayers, love and support, especially my kind father who passed away while I was in the midst of doing my research.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

CHAPTER 2 PRELIMINARY RESULTS

CHAPTER 3 SOLUTIONS OF $x^d \in A(\beta)$ FOR EACH $\beta \in H_n{}^c$ AND $n > 1$

CHAPTER 4 SOLUTIONS OF $x^d \in A(\beta)$ FOR EACH $\beta \in H_n$ AND $n \notin \theta$

CHAPTER 5 SOLUTIONS OF $x^d \in A(\beta)$ FOR EACH $\beta \in H_n$ AND $n \in \theta$

CHAPTER 6 CONCLUSION

APPENDICES (PUBLICATIONS)

1. Mahmood, S., and Rajah, A. (2011), Solving the class equation $x^d = \beta$ in an alternating group for each $\beta \in H_n \cap C^\alpha$ and $n \notin \theta$, Journal of the Association of Arab Universities for Basic and Applied Sciences, Science Direct, **10**, p. 42-50.

2. Mahmood, S., and Rajah, A. (2011), The ambivalent conjugacy classes of alternating groups, Pioneer Journal of Algebra, Number Theory and its Applications, Vol. **1**, No **2**, p. 67-72.

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

β	permutation
$A(\beta)$	the conjugacy class in A_n of the permutation β
A_n	the alternating group on $\{1,2,...,n\}$
S_n	the symmetric group on $\{1,2,...,n\}$
C^{α}	the conjugacy class of S_n consisting of permutations with cycle type α
$C^{\alpha\pm}$	the two conjugacy classes of A_n arising from splitting class C^{α} of S_n
F_n	{C^{α} of S_n | the number of parts α_k of α with the property $\alpha_k \equiv 3$ (mod 4) is odd}
H_n	{ C^{α} of $S_n \mid n > 1$, with all parts α_k of α different and odd}
${H_n}^c$	the complement set of H_n
$A(1)$	the identity class in A_n
$\|G \wedge d\|$	the number of solutions of $x^d = e$ in G
C_d	the cyclic group of order d
$\Re$	finitely generated group
$G \iota S_n$	the wreath product of group G by S_n
$G \iota A_n$	the wreath product of group G by A_n
$\|G\|$	the order of group G
$\|A : B\|$	$\|A\| / \|B\|$
ker(sgn)	the kernel of sign function
K_h	an element K_h of h-th cycle factor
$\alpha(\beta)$	the cycle type $(\alpha_1(\beta), \alpha_2(\beta), ..., \alpha_{c(\beta)}(\beta))$ of β

$\alpha_i(\beta)$	the part i of $\alpha(\beta)$
$\alpha \vdash n$	α is a partition of n
$p(n)$	the number of partitions of n
$c_r^n(\beta)$	the number of cycles of length r of β
$z_{\alpha(\beta)}$	$\prod_{r=1}^{n} r^{c_r^n(\beta)}(c_r^n(\beta))!$
sgn	the sign function
$c(\beta)$	the number of pairwise disjoint cycle factors of β
$C_S(\beta)$	the centralizer in S_n of the permutation β
$C_A(\beta)$	the centralizer in A_n of the permutation β
$dcd_*(\beta)$	the non-trivial disjoint cycle decomposition of β
n_β	the number of (non-trivial) cycles in $dcd_*(\beta)$
$Supp(\beta)$	$\{i \in \{1,2,...,n\} \mid \beta(i) \neq i\}$
m_β	the number of the support of β
$p \mid a$	p divides a
$Ord_p(a)$	the largest integer number k such that $p^k \mid a$
$\beta \underset{A_n}{\approx} \lambda$	the permutation β is conjugate to λ in A_n
$\lvert Hom(A,B) \rvert$	the number of homomorphisms from A to B

PENYELESAIAN PERSAMAAN KELAS FROBENIUS DALAM KUMPULAN SELANG-SELI

Abstrak

Persamaan Frobenius $x^d = \beta$ bagi kumpulan terhingga telah diperkenalkan oleh G. Frobenius dan dikaji oleh ramai penyelidik lain berkaitan dengan beberapa jenis kumpulan terhingga termasuk kumpulan kitaran terhingga, kumpulan terhingga terjana-*m*, kumpulan-*p* terhingga, dan hasil darab lingkaran kumpulan terhingga.

Dalam penyelidikan ini, bilangan penyelesaian bagi persamaan kelas $x^d = \beta \in A(\beta)$ dalam suatu kumpulan selang-seli A_n diperoleh, dan didapati β meliputi $A(\beta)$ kelas konjugasi bagi β dalam A_n.

Dalam tesis ini, empat kes bagi penyelesaian kepada kelas persamaan $x^d = \beta$ dalam A_n dibincang. Pertamanya, persamaan kelas $x^d = \beta$ dalam A_n, $\beta \in H_n^{\,c} \bigcap C^\alpha$ untuk semua $n > 1$ diselesaikan; dan bilangan penyelesaian bagi persamaan ini dengan $H_n = \{ C^\alpha$ of $S_n | n > 1$, dengan semua bahagian α_k dari α berbeza dan ganjil, C^α kelas konjugasi $S_n \}$ diperoleh. Seterusnya, bilangan penyelesaian serta penyelesaian persamaan kelas $x^d = \beta$ dalam A_n, $\beta \in H_n \bigcap C^\alpha$ dan $n \notin \theta = \{1, 2, 5, 6, 10, 14\}$ diperoleh. Ketiga, persamaan kelas $x^d = A(1) = e$ dalam A_n diselesaikan dan didapati bilangan penyelesaian persamaan ini, $A(1)$ merupakan kelas konjugasi identiti dalam A_n. Akhirnya, persamaan kelas $x^d = \beta$ dalam A_n, $\beta \in H_n \bigcap C^\alpha$ dan $n \in \theta$, dan bilangan penyelesaian bagi persamaan ini diperoleh.

SOLUTIONS OF THE FROBENIUS CLASS EQUATION IN ALTERNATING GROUPS

ABSTRACT

The Frobenius equation $x^d = \beta$ in finite groups was introduced by G. Frobenius and studied by many others who dealt with several types of finite groups, including finite cyclic groups, $m-$generated finite groups, finite $p-$groups, and wreath products of finite groups.

In the current study, the number of solutions for the class equation $x^d = \beta \in A(\beta)$ in an alternating group A_n is found and it is observed that β ranges over $A(\beta)$ the conjugacy class of β in A_n.

In this thesis, four cases of solutions to the class equation $x^d = \beta$ in A_n are discussed. Firstly, the class equation $x^d = \beta$ in A_n, where $\beta \in H_n{}^c \bigcap C^\alpha$, for all $n > 1$ is solved and the number of solutions of the above equation with $H_n = \{ C^\alpha$ of $S_n | n > 1$, with all parts α_k of α different and odd} is found, where C^α is a conjugacy class of S_n. Next, the class equation $x^d = \beta$ in A_n where $\beta \in H_n \bigcap C^\alpha$ and $n \notin \theta = \{1,2,5,6,10,14\}$ is solved and the number of solutions is determined. Thirdly, the class equation $x^d = A(1) = e$ in A_n is solved and the number of solutions of this equation where $A(1)$ is the identity conjugacy class in A_n is determined. Finally, the class equation $x^d = \beta$ in A_n, where $\beta \in H_n \bigcap C^\alpha$ and $n \in \theta$ is solved and the number of its solutions is found.

CHAPTER 1

INTRODUCTION

1.0 Introduction

In Chapter 1, the main purpose of this thesis is explained; the steps and aims for the current work is recalled. Moreover, the literature survey about past studies of Frobenius equations in finite groups are also recalled.

1.1 Literature Survey

The Frobenius Theorem shows that for any positive integer d, the number of elements of a finite group G that satisfies the equation $x^d = 1$ is a multiple of $\gcd(d, |G|)$, the greatest common divisor of d and $|G|$ (see Ishihara et al., 2001). Let $x^d = 1$ be an equation in a finite group G. Then the number of solutions of the above equation is denoted by $|G \wedge d|$. (Chowla et al., 1952) proved that $\sum_{n=0}^{\infty} \frac{|G \wedge d|}{n!} x^n = \exp(\sum_{k|d} \frac{x^k}{k})$, where $G = S_n$, and $|S_0 \wedge d| = 1$.

The Frobenius Theorem was greatly generalized by (Hall, 1959) who proved that if G is a finite group of order k and C is a conjugacy class of cardinality m in G, then for each $a \in C$, the number of solutions of $x^d = a$ in G is a multiple of $\gcd(dm, k)$. (Lam, 1988) proved that the number of solutions of $x^{p^d} = a$ in a non-cyclic $p-$group G is a multiple of p^2, where $p > 2$ is a prime number. In another direction, the subset $W = \{x \in G \mid x^d = 1\}$ in any finite group G, where d is a divisor of the order of G is considered. The set W is a union of certain conjugacy classes of G including the identity conjugacy class. From the Frobenius Theorem (see Brauer, 1969; Khurana et al., 2005), $|G \wedge d| = hd$ for $h \geq 1$. However, (Rust, 1966) proved a conjecture of Frobenius for $G = A_n\ (n \geq 5)$ and showed that $h > 1$.

Let $\Re$ be a finitely generated group and $f^{\Re}$ a set of all subgroups B of $\Re$ the indices $|\Re : B|$ of which are finite. Wohlfahrt proved that $\sum_{n=0}^{\infty} \frac{|Hom(\Re, S_n)|}{n!} x^n = \exp(\sum_{B \in f^{\Re}} \frac{x^{|\Re:B|}}{|\Re:B|})$ (referred to as the Wohlfahrt formula) (see Takegahara, 2004), where the sum $\sum_{B \in f^{\Re}}$ is over all subgroups B of $\Re$ of finite index $|\Re : B|$, $|Hom(\Re, S_n)|$ is the number of homomorphisms from $\Re$ to S_n, and $|Hom(\Re, S_0)| = 1$. In fact, a cyclic group C_d of order d, $|Hom(C_d, G)|$ coincides with the number of solutions of $x^d = 1$in a finite group G.

(Takegahara, 2002) showed that $\sum_{n=0}^{\infty} \frac{|Hom(\Re, G \iota S_n)| x^n}{|G|^n n!} =$ $\exp(\sum_{B \in f^{\Re}} \frac{|Hom(B, G)| x^{|\Re:B|}}{|\Re:B||G|})$, where $G \iota S_n$ is the wreath product of finite group G with S_n, and $|Hom(\Re, G \iota S_0)| = 1$. The same has also been shown by (Okada, 1990), when $\Re$ is a finite cyclic group. Moreover, this condition has also been studied by (Mulle, 2000; Mulle and Shareshian, 2002).

(Berkovich, 1991) proved that if $k > 1$ and $p > 2$, then $|G \wedge p^k| \equiv 0 \bmod p^{k+p}$ where $|G \wedge p^k|$ is the number of the solutions of the equation $x^{p^k} = 1$ in a non-cyclic $p-$group G. This fact is a generalization of many results (see Berkovich, 1968; Berkovich, 1971).

(Mann and Martinez, 1996) proved that for any natural number $m, n \geq 1$, there exists a number $0 < k < 1$ such that if G is an m-generated finite group and $\frac{|G \wedge n|}{|G|} \geq k$, then $|G \wedge n| = |G|$ (i.e., $x^n = 1$ for an arbitrary $x \in G$). The inequality $Ord_p(|S_n \wedge p|) \geq [\frac{n}{p}] - [\frac{n}{p^2}]$ is also shown by (Grady and Newmanm, 1994), and (Katsurada et al., 2000), where $|S_n \wedge p|$ is the number of solutions of the equation $x^p = 1$ in symmetric group on n letters, and p is a prime number. $Ord_p(|S_n \wedge p|) = [\frac{n}{p}] - [\frac{n}{p^2}]$ provided that $n \equiv 0 \mod p^2$ (see Ishihara et al., 2001).

Let $G \iota A_n$ be the wreath product of a finite group G with A_n. The exponential generating function for the number of solutions in $G \iota A_n$ to the equation $x^d = 1$ was found by (Chigira, 1996) who proved that $\sum_{n=0}^{\infty} \frac{|G \iota A_n \wedge d|}{n!} x^n = \frac{1}{2} \{\exp(\sum_{k|d} \frac{(-|G|)^{k-1} |G \wedge (d/k)| x^k}{k}) + \exp(\sum_{k|d} \frac{|G|^{k-1} |G \wedge (d/k)| x^k}{k})\}$, where $|G \iota A_0 \wedge d| = 1$ and $|G \iota A_i \wedge d| = 0$ if $i < 0$.

(Goldmann and Russell, 2002) studied the computational complexity of solving systems of equations over a finite group G, where $x_1 . x_2 . x_3 ... x_h = 1_G$ is an equation over a finite group G, each x_i is either a variable, an inverted variable, or a group constant, and 1_G is the identity element of G. (Shen, 2010) proved that if $|G \wedge d|$ has no divisor 4 for all $d \geq 1$, then G is solvable.

1.2 Background of the Study

In the present work, the conjugacy classes of permutations in an alternating group are studied in detail. If there exist elements $b_1, b_2, ..., b_m$ in a finite group G such that for every $b_j \in \{b_i\}_{i=1}^m$, the conjugacy class of b_j in G is $\{b_i\}_{i=1}^m$, then for each positive integer d and $b_j \in \{b_i\}_{i=1}^m$, the collection of Frobenius equations $\{x^d = b_i\}_{i=1}^m$ in G is called the Frobenius class equation $x^d = b_j$ in G. Moreover, the class equation $x^d = \beta$ in A_n, where β ranges over the conjugacy class $A(\beta)$ in A_n and d is a positive integer is solved. Also the number of solutions - if any exists - is found (the main purpose of the present research is to solve and determine the number of solutions of the Frobenius class equation $x^d = \beta$ in A_n).

The Frobenius equation $x^d = \beta$ in a finite group has been studied by many mathematicians such as (Brauer, 1969), (Mann and Martinez, 1996), (Berkovich, 1991) and others. A study was introduced by (Taban, 2007) to solve the class equation $x^d = \beta$ in a symmetric group and explain the solutions using group-theoretic approach. This approach states that all pairs of permutations γ and β in a symmetric group are conjugates iff they have the same structure. However, this is not necessarily true in an alternating group. Therefore, in the current research, the conjugacy classes in an alternating group will be studied in detail, where the conjugacy class of β in A_n is denoted by $A(\beta)$.

1.3 Organization of the Thesis

The rest of this thesis is organized as follows: In Chapter 2, all the main definitions and results of the alternating group and conjugacy classes in a symmetric group that are required in our study are mentioned, including the $k-$cycle, cycle type, and support of permutation, among others. In this chapter, all the necessary basic propositions are also provided. The basic propositions in Chapter 2 are used in Chapter 3 to solve the class equation $x^d = \beta$ in A_n, and the number of solutions for each $n > 1$ and $\beta \in H_n{}^c \bigcap C^\alpha$ is found, where $H_n = \{C^\alpha$ of $S_n | n > 1$, with all parts α_k of α different and odd$\}$. In Chapter 4, the class equation $x^d = \beta$ in A_n, where $n \notin \theta = \{1,2,5,6,10,14\}$ and $\beta \in H_n \bigcap C^\alpha$ is solved and the number of solutions is determined. In Chapter 5, the solutions and number of solutions are found for the class equation $x^d = 1 \in A(1)$ in A_n, where $A(1)$ is the identity conjugacy class in the alternating group. In the same chapter, a new theorem and its corollary on the ambivalent conjugacy classes in A_n are introduced and proved. Also the solutions and number of solutions for the class equation $x^d = \beta$ in A_n for all $n \in \theta$ and $\beta \in H_n$ are considered. Finally, in Chapter 6 some suggestions for future research are laid out.

1.4 Objective of the Thesis

The goal of this thesis is to solve the class equation $x^d = \beta$ in A_n, where β ranges over the conjugacy class $A(\beta)$ in A_n, and d is a positive integer. Moreover, the number of solutions - if any exists - is determined. In a special case, $A(\beta) = C^\alpha(\beta)$, where $A(\beta)$ is a conjugacy class of the permutation β in an alternating group, and $C^\alpha(\beta)$ is a conjugacy class of the permutation β in a symmetric group, we have $A(\beta)$ is the ambivalent class in an alternating group. In another case where $A(\beta) \neq C^\alpha(\beta)$, we have the situation where $A(\beta)$ is not necessarily an ambivalent class in the alternating group. Hence, in the current work, four cases of the class equation $x^d = \beta$ in an alternating group are dealt with: two cases each when $A(\beta) = C^\alpha(\beta)$ and $A(\beta) \neq C^\alpha(\beta)$. These cases cover all probabilities for the class equation $x^d = \beta$ in an alternating group. The following class equations in A_n are solved, and the number of solutions is determined.

(1) $x^d = \beta$, where $\beta \in H_n{}^c \cap C^\alpha$ for all $n > 1$,

(2) $x^d = \beta$, where $\beta \in H_n \cap C^\alpha$ and A_n is not an ambivalent group,

(3) $x^d = e$, where e is the identity element, and

(4) $x^d = \beta$, where $\beta \in H_n \cap C^\alpha$ and A_n is an ambivalent group.

1.5 Methodology Flowchart

The flow of this thesis is explained by using the chart in Figure 1 to solve the class equation $x^d = \beta$ in A_n, where $\beta \in C^\alpha$ for some conjugacy classes in the symmetric group. Figure 2 describes the flow used to determine the number of solutions to the same class equation.

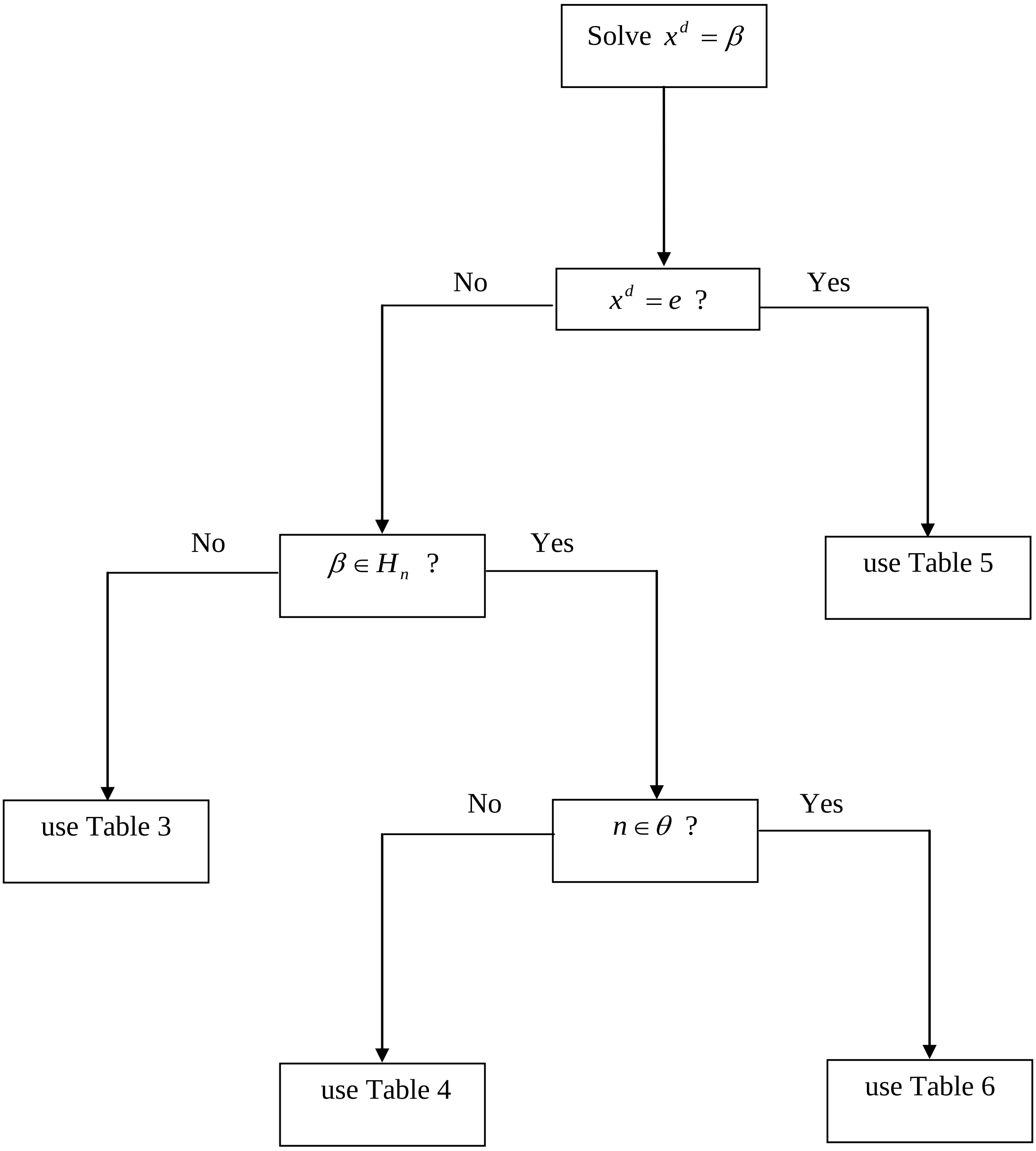

Figure 1 : Obtaining the solutions of $x^d = \beta$ in A_n

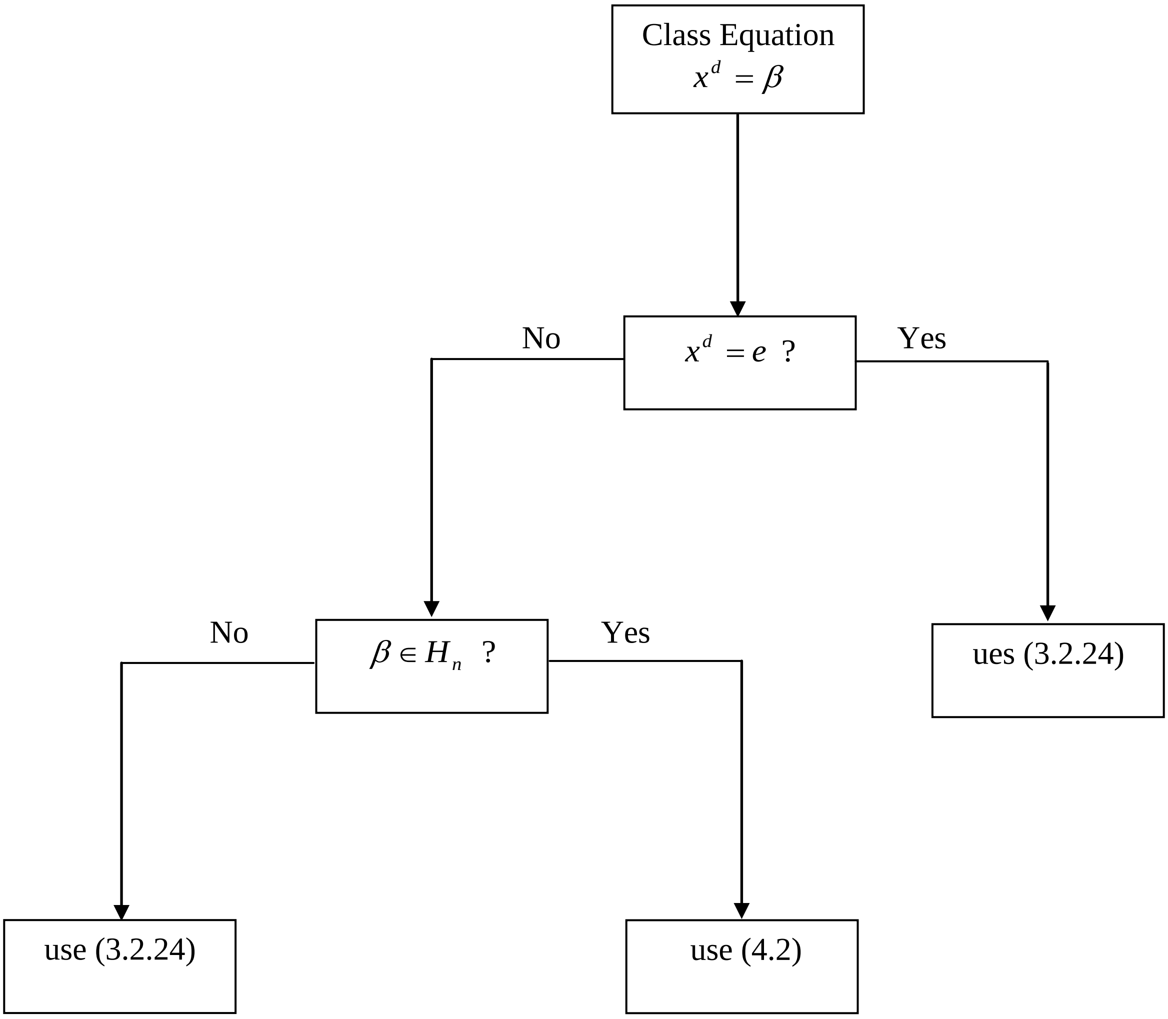

Figure 2 : Obtaining the number of solutions for the equation $x^d = \beta$ in A_n

CHAPTER 2

PRELIMINARY RESULTS

2.0 Introduction

In this chapter, the basic definitions and results of the conjugacy classes in the symmetric and alternating groups will be given. Several necessary basic definitions and results are also provided.

2.1 Basic Definitions and Preliminaries

2.1.1 Definition (Zeindler, 2010)

A partition α is a sequence of nonnegative integers $(\alpha_1, \alpha_2, ...)$ with $\alpha_1 \geq \alpha_2 \geq ...$ and $\sum_{i=1}^{\infty} \alpha_i < \infty$. The length $l(\alpha)$ and size $|\alpha|$ of α are defined as $l(\alpha) = Max\{i \in N \mid \alpha_i \neq 0\}$ and $|\alpha| = \sum_{i=1}^{\infty} \alpha_i$. Let $\alpha \vdash n = \{\alpha \ partition \mid |\alpha| = n\}$ for $n \in N$. An element of $\alpha \vdash n$ is called a partition of n, and α_i are the parts of α.

2.1.2 Remark

Only the non-zero components of a partition are written. Any $\beta \in S_n$ is chosen and written as $\gamma_1 \gamma_2 \ldots \gamma_{c(\beta)}$ with γ_i disjoint cycles of length α_i, and $c(\beta)$ is the number of disjoint cycle factors, including the $1-$cycle of β. However, because disjoint cycles commute, assume that $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_{c(\beta)}$. Therefore, $\alpha = (\alpha_1, \alpha_2, ..., \alpha_{c(\beta)})$ is a partition of n (Zeindler, 2010).

2.1.3 Definition (Zeindler, 2010)

The partition $\alpha = \alpha(\beta) = (\alpha_1(\beta), \alpha_2(\beta), ..., \alpha_{c(\beta)}(\beta))$ is called the cycle type of the permutation β in S_n.

2.1.4 Definition (Zeindler, 2010)

Let α be a partition of n. Then $C^{\alpha} \subseteq S_n$ is defined to be the set of all elements with cycle type α.

2.1.5 Definition (Zeindler, 2010)

Let $\beta \in S_n$. Then $c_m^n(\beta)$ is defined to be the number of cycles of length m of β.

2.1.6 Remarks

(1) If $\beta \in C^{\alpha}$, then the conjugacy class C^{α} is denoted by $C^{\alpha}(\beta)$.

(2) The relationship between partition $\alpha = (\alpha_1, \alpha_2, ..., \alpha_{c(\beta)})$ and $c_m^n(\beta)$ is as follows: $c_m^n(\beta) = \left|\{i : \alpha_i = r\}\right|$ (Zeindler, 2010).

(3) The cardinality of each class C^{α} of β can be found as follows:

$$\left|C^{\alpha}\right| = \frac{n!}{z_{\alpha(\beta)}} \quad \text{with} \quad z_{\alpha(\beta)} = \prod_{r=1}^{n} r^{c_m^n(\beta)} (c_m^n(\beta))! \quad \text{and} \quad c_m^n(\beta) = \left|\{i : \alpha_i = r\}\right|$$

(Bump, 2004).

(4) If the cycle decomposition of an element $\beta \in S_n$ consists of c_i cycles of length i, where $0 \le c_i \le n$ for $1 \le i \le n$, then β has cycle type $\alpha = (n^{c_n}, (n-1)^{c_{n-1}}, ..., 1^{c_1})$. If $c_i = 0$ then i^{c_i} is omitted. For example, $\alpha = (4,4,2,1,1,1) = (4^2, 2, 1^3)$ (Beals et al., 2003).

(5) Generally if $\beta \in S_n$ let $c(\beta)$ be the number of pairwise disjoint cycle factors including the 1-cycle of β. Let l_h $(1 \le h \le c(\beta))$ be their lengths, and choose for each h an element k_h in the h-th cycle factor. Then $\beta = \prod_{h=1}^{c(\beta)} (k_h, \beta(k_h), \beta^2(k_h), ..., \beta^{l_h - 1}(k_h))$ (James and Kerber, 1984).

(6) The number $p(n)$ of partitions of n grows rapidly with n. For instance, $p(1) = 1$, $p(4) = 5$, and $p(20) =$ 627 (Andrews and Eriksson, 2004).

2.1.7 The Conjugate Relation (Ceccherini-Silberstein et al., 2010; Macdonald, 1995)

Let λ and β be two elements in S_n. Then λ is conjugate to β in S_n iff there exists $\gamma \in S_n$ such that $\beta = \gamma\lambda\gamma^{-1}$. Moreover, for every pair of λ, β in A_n, λ is conjugate to β in A_n iff there exists $\gamma \in A_n$ such that $\lambda = \gamma\beta\gamma^{-1}$. The conjugate relation on S_n is an equivalence relation, and the conjugacy class of $\beta \in S_n$ can be determined using the cycle type of β, given that each pair of λ and

β in S_n are conjugates iff they have the same cycle structure. If $\beta \in C^{\alpha}$, then $C^{\alpha} \subseteq S_n$, the conjugacy class of β in S_n. The number of the conjugacy classes of S_n is also equal to the number of partitions of n.

2.1.7 Notations and Results on Ambivalence

2.1.7.1 Remarks

(1) An ambivalent element of a group is the one which is conjugate to its inverse, and an ambivalent group is one in which all of its elements are ambivalent (Higgins et al., 1971).

(2) Considering that all elements in S_n with the same cycle decomposition are conjugates and $\beta^{-1} = (k_r, ..., k_2, k_1)$ for all $\beta = (k_1, k_2, ..., k_r) \in S_n$. Thus every permutation in S_n is conjugate to its inverse, and each element $\beta \in A_n$ has an element $t \in S_n$ taking $\beta \to \beta^{-1} = t\beta t^{-1}$. To show the ambivalence of β in A_n, the existence of some t in A_n such that $\beta^{-1} = t\beta t^{-1}$ must be shown (Herstein, 1965).

(3) Every symmetric group is an ambivalent group. However, this is not true for the alternating groups. Assuming that $\theta = \{1,2,5,6,10,14\}$, then ($A_n, n \in \theta$), which are ambivalent groups, whereas ($A_n, n \notin \theta$) are non-ambivalent groups (Parkinson, 1973).

2.1.7.2 Proposition (Parkinson, 1973)

The non-ambivalent elements of A_n are precisely the elements λ with cycle decomposition $\{\alpha_1, \alpha_2, ..., \alpha_m\}$ satisfying the following three restrictions:

(i) $\alpha_i = \alpha_j \Rightarrow i = j$,

(ii) Each α_i is odd, and

(iii) $\frac{1}{2}(n-m)$ is odd.

2.1.7.3 Proposition (Armeanu, 1996).

If N is a normal subgroup of an ambivalent group G, then G/N is an ambivalent group.

2.1.7.4 Proposition (James and Kerber, 1984)

If the conjugacy class C^{α} of elements with cycle type α splits into two conjugacy classes of A_n, denoted by $C^{\alpha\pm}$, then A_n is an ambivalent group iff each of $C^{\alpha\pm}$ in A_n are ambivalent.

2.1.9 Some Results on Permutations (Ceccherini-Silberstein et al., 2010; Bump, 2004).

(1) $(k_1, k_2, ..., k_r) \in A_n \Leftrightarrow r$ is odd.

(2) $\beta \in A_n \Leftrightarrow n - c(\beta)$ is even, so $\operatorname{sgn}(\beta) = (-1)^{n - c(\beta)}$.

(3) $|\beta| = lcm\{\alpha_i(\beta) : 1 \le i \le c(\beta)\}$, the order of β is equal to the least common multiple of the set $\{\alpha_i(\beta) : 1 \le i \le c(\beta)\}$.

(4) Let $C_S(\beta) = \{\gamma \in S_n \mid \beta\gamma = \gamma\beta\}$ be a centralizer group of β in S_n, then $|C_S(\beta)| = z_{\alpha(\beta)}$ with $z_{\alpha(\beta)} = \prod_{r=1}^{n} r^{c_m^n(\beta)}(c_m^n(\beta))!$ and $c_m^n(\beta) = |\{i : \alpha_i = r\}|$.

2.1.10 Example

Let $n = 5$. Then we have the following table.

Table 1. Cardinality of Conjugacy Classes in S_5.

$p(n)$ **Partition**	β **Representative**	$C^{\alpha}(\beta)$ **Class**	$\lvert C^{\alpha}(\beta)\rvert$ **Cardinality of $C^{\alpha}(\beta)$**
1,1,1,1,1	(1)	$[1^5]$	1
1,1,1,2	(12)	$[1^3,2]$	10
1,1,3	(123)	$[1^2,3]$	20
1,4	(1234)	[1,4]	30
5	(12345)	[5]	24
1,2,2	(12)(34)	$[1,2^2]$	15
2,3	(12)(345)	[2,3]	20
			120=5!

Note that S_5 has seven conjugacy classes because there are seven partitions of the number 5. Note as well that $\lambda = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 2 & 6 \end{pmatrix}$ are elements in S_6. Hence, λ and β can be represented as a product of pairwise disjoint cycles, as shown in the following diagram:

$\lambda = (1\ 2\ 3\ 4\ 5)$	(6)
5	1

$\beta = (1\ 3\ 5\ 2\ 4)$	(6)
5	1

Then, $\lambda \in [1,5]$ and $\beta \in [1,5]$, so λ and β are conjugates in S_6, but are not conjugates in A_6. Therefore any pair of conjugate permutations λ and β in S_n are not necessarily conjugate permutations in the alternating group A_n too.

2.1.11 Explanations of Some Facts

(1) Since A_n is a normal subgroup of S_n, a conjugacy class C^{α} of S_n is either contained in A_n or in $S_n \setminus A_n$. If $C^{\alpha} \subseteq A_n$, then C^{α} is either an A_n-class or splits into two A_n-classes. The order of a conjugacy class $C^{\alpha}(\beta)$ is equal to the index of the centralizer $C_S(\beta)$ of β in S_n. Considering that for the centralizer $C_A(\beta)$ of β in A_n, $C_A(\beta) = C_S(\beta) \cap A_n$, which is a subgroup of index ≤ 2 in $C_S(\beta)$, then either $C^{\alpha} \subseteq A_n$ is an A_n-class C^A itself, that is, $C^{\alpha}(\beta) = C^A(\beta)$ or $C^{\alpha}(\beta)$ splits into exactly two A_n- classes of the same order $\frac{|C^{\alpha}(\beta)|}{2}$. The conjugacy class $C^{\alpha}(\beta)$ splits (for $n > 1$) iff $C_A(\beta) = C_S(\beta)$, that is, iff $C_S(\beta)$ contains no odd permutations. $C_S(\beta)$ contains an odd permutation if β contains a cycle factor of even length (which is then an odd element of $C_S(\beta)$) or if β contains two cycle factors of the same odd length, that is, $\beta = \ldots (k_h, \beta(k_h), \ldots, \beta^r(k_h))(k_j, \beta(k_j), \ldots, \beta^r(k_j))$. Thus

$\lambda = (k_h, k_j)(\beta(k_h), \beta(k_j)) \ldots ((\beta^r(k_h), \beta^r(k_j)) \in C_S(\beta) \setminus A_n$. Conversely, if β consists of cycle factors of pairwise different odd lengths, then $C_S(\beta)$ is generated by these cycle factors and is contained in A_n (James and Kerber, 1984).

(3) The symmetric group S_n is generated by two elements $\{(1,2),(1,2,\ldots,n)\}$ (Boerner, 1970). Moreover, S_n is generated by transpositions $\{(1,2),(2,3),\ldots,(n-1,n)\}$, whereas A_n is generated by $3-$cycles if $n \geq 3$(Passmen, 1968).

2.2 Known Results

2.2.1 Proposition (Mazurov, 2005)

If X is the set of all $3-cycles$ $(i,j,k) \in A_n$, where $n \geq 5$ and $i \neq j \neq k \neq i$, then X is a conjugacy class in A_n such that $\langle X \rangle = A_n$. For any non-commuting $x, y \in X$, $\langle x, y \rangle$ is isomorphic to A_4 or A_5.

2.2.2 Remark (Herzog et al., 2004)

If q is a rational number, then $[q] = k$, where k is the unique integer satisfying $k \leq q < k+1$.

2.2.3 Proposition (Bertram and Herzog, 2001)

Each $\beta \in A_n, n \geq 1$ is a product of three $l-$cycles in S_n iff l is odd, and either $\left[\frac{n}{2}\right] \leq l \leq n$ or $n = 7$ and $l = 3$.

2.2.4 Remark (Herzog et al., 2008)

Let $k, l \geq 2$ be integers. Then $n = n(k,l)$ is denoted to be the largest integer such that every permutation in A_n is a product of k cycles of length l. For each $\beta \in S_n - \{e\}$, where e is an identity element in S_n. $dcd_*(\beta)$ is denoted as the non-trivial disjoint cycle decomposition of β by, which represents β as a product of disjoint cycles of length greater than 1. n_β is designated as the number of (non-trivial) cycles in $dcd_*(\beta)$, and $m_\beta = |\text{supp}(\beta)|$ is designated as the number of the support of β where supp(β) $= \{i \in \{1,2,...,n\} \mid \beta(i) \neq i\}$.

2.2.5 Proposition (Herzog et al., 2004)

Let $\beta \in S_n$ and $l_1, l_2 \in N,$ where $n \geq l_1 \geq l_2 \geq 2$. Then $\beta = C_1C_2$, where C_1 ,C_2 are cycles in S_n of lengths l_1, l_2, respectively, iff either $n_\beta = 2$, l_1, l_2 are the lengths of the cycles in $dcd_*(\beta)$, and $l_1 + l_2 = m_\beta$, or the following conditions hold:

(1) $l_1 + l_2 = m_\beta + n_\beta + 2s$ for some $s \in N \bigcup \{0\}$, and

(2) $l_1 - l_2 \leq m_\beta - n_\beta$.

2.2.6 Lemma (James and Kerber, 1984)

$C^{\alpha\pm}$ of A_n are ambivalent iff the number of parts α_k of α with the property $\alpha_k \equiv 3$ (mod 4) is even.

2.2.7 Lemma (James and Kerber, 1984)

$C^{\alpha}(\beta)$ splits into two A_n-classes of equal order iff $n > 1$, and the non-zero parts of $\alpha(\beta)$ are different and odd. (In every other case $C^{\alpha}(\beta)$ does not split).

2.2.8 Lemma (Taban, 2007)

Let $[a^r]$ be a conjugacy class in a symmetric group S_n. If p is a prime number such that $p \mid a$, then the solution of $x^p \in [a^r]$

(1) is $[(ap)^{\frac{r}{p}}]$ if $p \mid r$, or

(2) does not exist if p does not divide r.

2.2.9 Lemma (Taban, 2007)

Let p be a prime number and $[a^r]$ a conjugacy class of a symmetric group. If p does not divide a, then the solution of $x^p \in [a^r]$ is

(1) $[a^r]$ if $1 \le r < p$, or

(2) $[a^r], [a^{r-p}, (ap)], [a^{r-2p}, (ap)^2], \ldots, [a^{r-mp}, (ap)^m]$ if $m \le r \le (m+1)p.$

2.2.10 Lemma (Taban, 2007)

If p and q are distinct primes and $p \mid a, q \mid a$ where $[a^r]$ is a conjugacy class of a symmetric group, then the solution of $x^{pq} \in [a^r]$

(1) is $[(pqa)^{\frac{r}{pq}}]$ if $pq \mid r$, or

(2) does not exist if pq does not divide r.

2.2.11 Lemma (Taban, 2007)

Let p and q be distinct primes and $[a^r]$ a conjugacy class of a symmetric group. If $p \mid a$ and q does not divide a, then the solution of $x^{pq} \in [a^r]$

(1) is $[(pa)^i, (pqa)^j]$, where i and j are solutions of the equation $i + qj = \frac{r}{p}$ if $p \mid r$, or

(2) does not exist if p does not divide r.

2.2.12 Lemma (Taban, 2007)

Let p and q be distinct primes and $[a^r]$ a conjugacy class in S_n. If p does not divide a and q does not divide a, then the solution of $x^{pq} \in [a^r]$ is $[a^i, (pa)^j, (qa)^k, (pqa)^l]$, where i, j, k and l are non-negative integers and solutions of the equation $i + pj + qk + pql = r$.

2.2.13 Lemma (Taban, 2007)

If $p \mid a$ and $r = p^l r_0$ where $l < n$ and $\gcd(r_0, p) = 1$, where $[a^r]$ is a conjugacy class of a symmetric group, then there is no solution for $x^{p^n} \in [a^r]$.

2.2.14 Lemma (Taban, 2007)

If $p \mid a$ and $p \mid b$, where $[a^r, b^s]$ is a conjugate class in S_n, then the solution of $x^p \in [a^r, b^s]$

(2) is $[(ap)^{\frac{r}{p}}, (bp)^{\frac{s}{p}}]$ if $p \mid r$ and $p \mid s$, or

(3) does not exist if otherwise.

2.2.15 Lemma (Taban, 2007)

If p does not divide ab, where $[a^r, b^s]$ is a conjugacy class in S_n, then the solution of $x^p \in [a^r, b^s]$ is $[a^i, b^j, (pa)^k, (pb)^l]$, where $i + pk = r$ and $j + pl = s$.

2.2.16 Lemma (Taban, 2007)

If $p \mid a$ and p does not divide b, where $[a^r, b^s]$ is a conjugacy class in S_n, then the solution of $x^p \in [a^r, b^s]$ is $[b^i, (pa)^j, (pb)^k]$, where $pj = r$ and $i + pk = s$.

2.2.17 Lemma (Taban, 2007)

For the solution of $x^d \in [a^r, b^s]$, if there is no solution for $x^d \in [a^r]$ or $x^d \in [b^s]$, then there is no solution for $x^d \in [a^r, b^s]$.

2.2.18 Lemma (Taban, 2007)

If $p \mid a$, where $[a^r]$ is a conjugacy class of a symmetric group, then the solution of $x^{p^m} \in [a^r]$

(1) is $[(p^m a)^{\frac{r}{p^m}}]$ if $p^m \mid r$, or

(2) does not exist if p^m does not divide r.

2.2.19 Lemma (Taban, 2007)

If p does not divide a, where $[a^r]$ is a conjugacy class of a symmetric group, then the solution of $x^{p^m} \in [a^r]$ is $[a^{r_1}, (p^m a)^{r_2}, (p^2 a)^{r_3}, \ldots, (p^m a)^{r_{m+1}}]$, where $r_1, r_2, \ldots, r_{m+1}$ are the solutions of the equation $r_1 + pr_2 + p^2 r_3 + \cdots + p^m r_{m+1} = r$.

2.2.20 Lemma (Taban, 2007)

If p and q are distinct primes, $p \mid a$ and $q \mid a$, where $[a^r]$ is a conjugacy class of a symmetric group, then the solution of $x^{p^m q^n} \in [a^r]$

(1) is $[(p^m q^n a)^{\frac{r}{p^m q^n}}]$ if $p^m q^n \mid r$, or

(2) does not exist if $p^m q^n$ does not divide r.

2.2.21 Lemma(Taban, 2007)

If p and q are distinct primes, $p \mid a$ and q does not divide a, where $[a^r]$ is a conjugacy class of a symmetric group, then the solution of $x^{p^m q^n} \in [a^r]$

(1) is $[(p^m a)^{r_1}, (qp^m a)^{r_2}, (q^2 p^m a)^{r_3}, ..., (q^n p^m a)^{r_{m+1}}]$, where $r_1, r_2, ..., r_{m+1}$ are the solutions of the equation $r_1 + qr_2 + q^2 r_3 + \cdots + q^n r_{m+1} = \dfrac{r}{p^m}$ if $p^m \mid r$, or

(2) does not exist if p^m does not divide r.

2.2.22 Lemma (Taban, 2007)

If p and q are distinct primes, and p and q do not divide a, where $[a^r]$ is a conjugacy class of a symmetric group, then the solution of $x^{p^m q^n} \in [a^r]$ is

$$[a^{s_{1,1}}, (pa)^{s_{1,2}}, ..., (p^m a)^{s_{1,m+1}}, (qa)^{s_{2,1}}, (pqa)^{s_{2,2}}, ..., (p^m qa)^{s_{2,m+1}}, (q^2 a)^{s_{3,1}}, (pq^2 a)^{s_{3,2}},$$
$$..., (p^m q^2 a)^{s_{3,m+1}}, ..., (q^n a)^{s_{n+1,1}}, (pq^n a)^{s_{n+2,2}}, (p^2 q^n a)^{s_{n+1,3}}, ..., (p^m q^n a)^{s_{n+1,m+1}}]$$

where $s_{i,j}$, $1 \le i \le n+1,\ 1 \le j \le m+1$ are solutions of

$$\begin{pmatrix} s_{1,1} & s_{1,2} & . & . & . & s_{1,m+1} \\ s_{2,1} & s_{2,2} & . & . & . & s_{2,m+1} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ s_{n+1,1} & s_{n+1,2} & . & . & . & s_{n+1,m+1} \end{pmatrix} \begin{pmatrix} 1 \\ p \\ p^2 \\ . \\ . \\ . \\ p^m \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \\ r_3 \\ . \\ . \\ . \\ r_{n+1} \end{pmatrix}$$

and r_i, $1 \le i \le n+1$ are solutions of the equation $r_1 + qr_2 + q^2 r_3 + \cdots + q^n r_{n+1} = r$.

2.2.23 Lemma (Taban, 2007)

If $p_1, p_2, ..., p_m$ are distinct primes such that $p_i \mid a$, $\forall i = 1,...,m$ and $p_j^{n_j}$ does not divide r for some ($1 \le j \le m$), where $[a^r]$ is a conjugacy class of a symmetric group, then there is no solution for $x^{{p_1}^{n_1} {p_2}^{n_2} \dots {p_m}^{n_m}} \in [a^r]$.

2.2.24 Lemma (Taban, 2007)

If $p_1, p_2, ..., p_m$ are distinct primes such that $p_i \mid a$ and $p_i^{n_i} \mid r$ for each

($1 \le i \le m$), where $[a^r]$ is a conjugacy class of a symmetric group, then the solution of $x^{{p_1}^{n_1} {p_2}^{n_2} \dots {p_m}^{n_m}} \in [a^r]$ is $[({p_1}^{n_1} ... {p_m}^{n_m} a)^{\frac{r}{{p_1}^{n_1} \dots {p_m}^{n_m}}}]$.

2.2.25 Lemma (Taban, 2007)

If $p_1, p_2, ..., p_m$ are distinct primes and for some $1 \le i \le m$, $p_i \mid a$ and $p_i^{n_i}$ does not divide r, where $[a^r]$ is a conjugacy class of a symmetric group, then there is no solution for $x^{{p_1}^{n_1} {p_2}^{n_2} \dots {p_m}^{n_m}} \in [a^r]$.

2.2.26 Lemma (Taban, 2007)

If p_i, $1 \le i \le m$ and q are distinct primes and $p_i \mid a$, $p_i^{n_i} \mid r$ for each $1 \le i \le m$ and q does not divide a, where $[a^r]$ is a conjugacy class of a symmetric group, then the solution of $x^{q^k {p_1}^{n_1} {p_2}^{n_2} \dots {p_m}^{n_m}} \in [a^r]$ is $[({p_1}^{n_1} ... {p_m}^{n_m} a)^{r_1}, (q{p_1}^{n_1} ... {p_m}^{n_m} a)^{r_2}, ..., (q^k {p_1}^{n_1} ... {p_m}^{n_m} a)^{r_{k+1}}]$ where r_i , $1 \le i \le k+1$ are solutions of the equation $r_1 + qr_2 + \cdots q^k r_{k+1} = \dfrac{r}{p_1^{n_1} \cdots p_m^{n_m}}$.

2.2.27 Theorem (Taban, 2007)

If $\beta \in [A^a, B^b, ..., T^t]$ is a conjugacy class in a symmetric group S_n, then $\beta^d \in [\Omega^{ra}, \phi^{sb}, ..., \psi^{tm}]$ where $\gcd(d, A) = r$, $\gcd(d, B) = s, ..., \gcd(d, T) = m$ and $A = \Omega r$, $B = \phi s$,..., $T = \psi m$.

2.2.28 Corollary

Let $[B_1, B_2, ..., B_m]$ be a conjugacy class in a symmetric group S_n. If d is a positive integer such that $\gcd(d, B_i) = 1, (1 \le i \le m)$, then the solution of $x^d \in [B_1, B_2, ..., B_m]$ in S_n is $[B_1, B_2, ..., B_m]$.

Proof

Let $T = \{C^\alpha \text{ of } S_n \mid \text{ if } \lambda \in C^\alpha, \text{ then } \lambda^d \in [B_1, B_2, ..., B_m]\}$ be a solutions set of $x^d \in [B_1, B_2, ..., B_m]$ in S_n. For each $[A_1^{r_1}, A_2^{r_2}, ..., A_k^{r_k}] \in T$, assume $\gcd(d, A_j) = t_j$, and $A_j = \Omega_j t_j$, where $(1 \le j \le k)$. Let $\lambda \in [A_1^{r_1}, A_2^{r_2}, ..., A_k^{r_k}]$, then $\lambda^d \in [\Omega_1^{r_1 t_1}, \Omega_2^{r_2 t_2}, ..., \Omega_k^{r_k t_k}]$ by (2.2.27). However, $\lambda^d \in [B_1, B_2, ..., B_m]$. Hence $[\Omega_1^{r_1 t_1}, \Omega_2^{r_2 t_2}, ..., \Omega_k^{r_k t_k}] = [B_1, B_2, ..., B_m]$, thus we have:

(1) $m = k$.

(2) $1 = r_j t_j$, then $r_j = t_j = 1$ for all $(1 \le j \le m)$.

(3) $B_i = \Omega_i$, then $B_i = A_i$ for all $(1 \le j \le m)$.

Finally, from (1), (2), and (3) we have $[A_1^{r_1}, A_2^{r_2}, ..., A_k^{r_k}] = [B_1, B_2, ..., B_m]$. Then the solutions set of $x^d \in [B_1, B_2, ..., B_m]$ in S_n is $T = \{[B_1, B_2, ..., B_m]\} = [B_1, B_2, ..., B_m]$. □

2.2.29 Remarks

(1) If $x^d \in [B_1^{b_1}, B_2^{b_2}, \ldots, B_m^{b_m}]$, then the solution for every part of $x^d \in [B_1^{b_1}]$, $x^d \in [B_2^{b_2}]$,…, and $x^d \in [B_m^{b_m}]$ can be found separately, and then all the solutions can be collected to find the solution of $x^d \in [B_1^{b_1}, B_2^{b_2}, \ldots, B_m^{b_m}]$ in S_n. Moreover, if there is no solution for at least one of the parts, then there is no solution of $x^d \in [B_1^{b_1}, B_2^{b_2}, \ldots, B_m^{b_m}]$ in S_n.

(2) Theorem (2.2.27) gives all conjugacy classes of the form $[T_1^{t_1}, T_2^{t_2}, \ldots, T_m^{t_m}]$ which belong to the solutions set of $x^d \in [B_1^{r_1 t_1}, B_2^{r_2 t_2}, \ldots, B_m^{r_m t_m}]$ in S_n, where $\gcd(d, T_1) = r_1$, $\gcd(d, T_2) = r_2, \ldots, \gcd(d, T_m) = r_m$ and $T_1 = B_1 r_1$, $T_2 = B_2 r_2, \ldots, T_m = B_m r_m$. But this does not give all the solutions of $x^d \in [B_1^{r_1 t_1}, B_2^{r_2 t_2}, \ldots, B_m^{r_m t_m}]$ in S_n except when $t_1 = t_2 = \cdots = t_m = 1$ and $r_1 = r_2 = \cdots = r_m = 1$.

2.2.30 Example:

Find all conjugacy classes of the form $[T_1^{t_1}, T_2^{t_2}]$ which belong to the solutions set of $x^8 \in [1^4, 3]$ in S_7.

Solution:

Assume $d = 8,\quad r_1 t_1 = 4,\quad r_2 t_2 = 1,\quad B_1 = 1,\quad B_2 = 3,\quad T_1 = B_1 r_1 = \dfrac{4}{t_1},\quad T_2 = B_2 r_2 = \dfrac{3}{t_2}$, where $\gcd(d, T_1) = r_1$, and $\gcd(d, T_2) = r_2$. Now, we have to find the values of t_1 and t_2 which satisfy (1) and (2), where

$$(1)\ \gcd(d, T_1) = r_1 \Rightarrow \gcd(8, \frac{4}{t_1}) = \frac{4}{t_1} \Rightarrow t_1 = \{1,2,4\}.$$