DERIVATION OF CYCLE INDEX FORMULAS OF SEMIDIRECT PRODUCT GROUPS

Muthoka Geoffrey Ngovi (M.Sc.)
Reg No: I84/27038/2014
Department of Mathematics and Actuarial Science
Kenyatta University

A Thesis Submitted in Partial Fullfilment of the Requirements for the Award of the Degree of Doctor of Philosophy (Pure Mathematics) in the School of Pure and Applied Sciences of Kenyatta University

December, 2019

Declaration

This thesis is my original work and has not been presented for a degree award in any other university or for any other award.

Muthoka Geoffrey Ngovi (M.Sc)
I84/27038/2014

Signature__________________________ Date_____________

This thesis has been submitted for examination with our approval as university supervisors.

Prof. Ireri Kamuti Signature__________________________ Date_____________
Department of Mathematics and Actuarial Science

Dr. Mutie Kavila Signature__________________________ Date_____________
Department of Mathematics and Actuarial Science

Dedication

To my wife Emily, my daughter Daisy and my son Daylan; may you be inspired by this work.

Acknowledgements

I am greatly indebted to my supervisors Prof. I. Kamuti and Dr. M. Kavila who tirelessly inspired and guided me throughout this work. Their timely insights, encouragement and availability when I needed them did not only assist me complete this work but also inculcated in me intellectual values that will continue to influence my work.

I extend special thanks to my friends and colleagues Lao and Patrick for encouraging and challenging me throughout the period of this research.

My studies would not have been accomplished without the great moral and spiritual support from my beloved parents Mr. and Mrs. Mulandi, may the almighty God increase you and bless you abundantly.

Above all I thank the almighty God for the sound health and brain during the period of my studies; with whom all things have been possible.

Finally, I thank the National Research Fund for funding my research.

TABLE OF CONTENTS

LIST OF TABLES

ABBREVIATIONS AND NOTATIONS

A_n	- Alternating group of degree n
C_n	- Cyclic group of order n
D_n	- The dihedral group of order $2n$
$G = N \rtimes H$	- G is a semidirect product group of N by H
$\mathrm{N_G(H)}$	- Normalizer of subgroup H in G
$\|G\|$	- Order of a group G
C^g	- Conjugacy class of $g \in G$
S_n	- The symmetric group of degree n
$\mathbf{X}^{(r)}$	- Set of all unordered $r-$element subsets from $\mathrm{X} = \{1, 2, ..., \mathrm{n}\}$
$\mathbf{X}^{[r]}$	- Set of all ordered $r-$element subsets from $\mathrm{X} = \{1, 2, ..., \mathrm{n}\}$
$\sum_{\mathbf{d}\|\mathbf{n}}$	- Sum over the divisors d of n
$\sum_{\substack{\mathbf{d}\|\mathbf{n} \\ \mathbf{a}\nmid\mathbf{d}}}$	- Sum over the divisors d of n with d not divisible by a
$\langle (ab) \rangle$	- A cyclic group generated by a cycle of length two
$Aff(p)$	- The affine(p) group
$Aff_{\square}(p)$	- The affine square(p) group
$\mathbb{Z}_n$	- Group of integers modulo n
$\phi(d)$	- Euler's phi function
$\pi(\mathrm{x})$	- Numbers of fixed elements in permutation X
$C_G(g)$	- The centralizer of $g \in G$ in the group G

Abstract

The concept of the cycle index formulas of a permutation group was discovered in the year 1937. Since then cycle index formulas of several groups have been studied by different scholars. For instance the cycle index of the dihedral group D_n acting on the set of vertices of a regular $n-$gon is known and has been applied in enumeration of different mathematical structures. In this study the relationship between the cycle index formula of a semidirect product group and the cycle index formulas of the two subgroups which the group is a semidirect product of was established. In particular the cycle index formula of the dihedral group D_n of order $2n$ is expressed in terms of the cycle index formula of a cyclic group of order two C_2 and the cycle index formula of the cyclic group of order n, C_n; the cycle index formula of the symmetric group S_n is expressed in terms of the cycle index formula of the alternating group A_n and the cycle index formula of a group generated by a cycle of length two, $\langle (ab) \rangle$. The cycle index formula of an affine(p) group has been derived by considering the different cycle types of elements of the group and expressed in terms of the cycle index formula of $C_p = \{x + b, \ where \ b \in \mathbb{Z}_p\}$ and the cycle index formula of $C_{p-1} = \{ax, \ where \ 0 \neq a \in \mathbb{Z}_p\}$. We further extend this to affine(q) where q is a power of a prime p and to the affine square(p) and affine square(q) groups. Finally, the cycle index formula of a Frobenius group is expressed in terms of the cycle index formula of the Frobenius complement H and the cycle index formula of the Frobenius kernel M. The cycle index formulas which are known such as that of the dihedral group and the symmetric group were used and the groups whose cycle index formulas are not known such as the affine(p), affine square(p), affine(q) and affine square(q) group were first derived as part of the research. It was noted that for semidirect groups which are Frobenius such as the dihedral group D_n with an odd value of n, the affine groups and the affine square groups, we can fully express the cycle index of the group in terms of the cycle index formulas of the subgroups which the group is a semidirect of. However, for semidirect product groups which are not Frobenius such as the dihedral group D_n with an even value of n and the symmetric group S_n, the cycle index formula of the group cannot be expressed fully in terms of the cycle index formulas of the subgroups the group is a semidirect product of.

CHAPTER 1

INTRODUCTION

This chapter has six sections. Section 1.1 gives some background information of cycle index formulas and their applications. Section 1.2 provides the problem statement and its justification. In Section 1.3, we give the objectives of the study while in Section 1.4, we give the significance of the study. Definition of terms used throughout the thesis is done in Section 1.5 and preliminary results which are used in the thesis are given in Section 1.6.

1.1 Background information

Many problems in enumerative combinatorics reduce via Pólya's enumeration Theorem, (Pólya, 1937), to the determination of the cycle index of a certain group. The cycle index is therefore a very useful tool in enumeration. The concept of cycle index lies in a branch of mathematics called Enumeration Combinatorics which deals with questions of the form "how many elements are there in a given set?" These may include questions like: How many different isomers are there of a certain compound? How many in-equivalent mathematical structures are there with specified properties? It is essential to specify carefully what is meant by "different" or "equivalent" before attempting to find the number. Typically this is done by starting with an easily formed finite set X and then putting an equivalence relation on that set in such a way that two elements are regarded as different if and only if they belong to different equivalence classes. The number of different structures is equal to the number of equivalence classes. In many practical examples, the equivalence is defined in terms of the action of a finite group G on a set X.

In recent years, enumerative combinatorics, group theory and graph theory have given rise to a branch of Mathematics called Combinatorics, which in one of its branches deals with generation of cycle indices of different groups. These cycle indices are applied in enumeration of different objects such as different mathematical structures and chemical compounds. In general, the cycle index formula of any permutation group G acting on a set X with $|X| = n$ is a polynomial of the form; $P_{(G,X)}\left(x_1, x_2, \ldots, x_n\right) = \frac{1}{|G|}\sum_{g\in G} x_1^{\alpha_1(g)} x_2^{\alpha_2(g)} \ldots x_n^{\alpha_n(g)}$ where $\alpha_l(g)$ is the number of cycles of length l in the permutation g.

1.2 Problem statement and justification

In combinatorial mathematics a cycle index formula is a polynomial in several variables from which information on how a group G of permutations acting on a set say X can be simply read from its coefficients and exponents. Cycle index formulas have been studied for many years and the cycle index formulas of many permutation groups are known. If $G = N * H$, where $*$ is some binary operation on permutation groups, determination of the cycle index formula of G in terms of the cycle index of N and the cycle index of H has been done for many operations. For instance, the cycle index formulas of wreath product groups was studied and applied in chemical enumeration by Krishnamurthy (1985) and the cycle index formulas of internal direct product groups was studied by Kamuti (2012). By expressing the cycle index of a group in terms of the cycle index formulas of a binary operation of permutation groups, the resulting cycle index can be applied in counting of different objects which the original cycle index of the group can not count. For example, the cycle index formula of C_n cannot count isomers of organic compound but we can use the cycle index generated by the wreath product of C_n by C_{n+1} to count different isomers as demonstrated by Krishnamurthy (1985). For a large group, expressing its cycle index in terms of the cycle indices of simpler permutation groups makes its application easy. If $G = N \rtimes H$, a semidirect product; this study tries to find an expression of the cycle index of G in terms of the cycle index of N and H.

1.3 Objectives

1.3.1 General objective

To study the relationship between the cycle index formulas of semidirect product groups and the individual groups which the group is a semidirect product of.

1.3.2 Specific objectives

i. To express the cycle index formula of the dihedral group D_n, in terms of cycle index formula of a cyclic group of order two C_2, and the cyclic group C_n of order n.

ii. To express the cycle index formula of the symmetric group S_n, of degree n in terms of cycle index formula of the alternating group A_n and a group generated by a cycle of length two $\langle (ab) \rangle$.

iii. To express the cycle index formula of a Frobenius group in terms of cycle index formula of the Frobenius complement H and the Frobenius kernel M.

iv. To derive the cycle index formula of an affine(p) group and express it in terms of the cycle index formula of $C_p = \{x + b,\ where\ b \in \mathbb{Z}_p\}$ and the cycle index formula of $C_{p-1} = \{ax, \ where \ \ 0 \neq a \in \mathbb{Z}_p\}$ and extend the same to an affine(q) group where $q = p^r$ for some prime number p.

v. To derive the cycle index formula of an affine square(p) group and express it in terms of the cycle index formula of $C_p = \{x + b, \ where \ b \in \mathbb{Z}_p\}$ and the cycle index formula of $C_{\frac{p-1}{2}} = \{ax, \ where \ 0 \neq a \ is \ a \ square \ in \ \mathbb{Z}_p\}$ and extend the same to an affine square(q) group where $q = p^r$ for some prime p.

1.4 Significance

Combinatorics is a field that has generated a lot of interest from mathematicians, chemists and physicists across the world. Apart from its numerous applications in purely mathematical problems, there are many real life problems that have been solved by a combinatorial approach. Specific applications have been in enumerating chemical compounds, labelled and unlabelled graphs and self-complementing graphs; in addition to studying of crystal structure of nuclear magnetic resonance spectrography. For instance, cycle index formulas can be used to count the number of different graphs with a given number of vertices. In Chemistry, cycle index formulas can be used to count the number of isomers of a given organic compound. In real life applications, cycle index formulas can be used to get the number of different arrangements or permutations that a given number of objects can be arranged. For example, the number of ways in which a given number of beads can be arranged to form non identical necklaces can be evaluated using cycle indices.

This study extends some of the existing results in the area of combinatorial enumeration. By so doing, new results and concepts have been realized. In addition, the results of this study will provide valuable information to the combinatorists.

1.5 Definitions

Definition 1.5.1.

A permutation group is a group G whose elements are permutations of a given set X and whose group operation is the composition of permutations in G.

Definition 1.5.2.

A permutation of the form $(a_1 a_2 \ \ . \ . \ . \ a_k)$ is called a cycle of length k or a k-cycle. A 2-cycle is called a transposition.

Definition 1.5.3.

Cycles in a permutation are said to be disjoint if they have no elements in common.

Definition 1.5.4.

Let X be a set and G be a group. We say that G acts on a set X on the left if $\forall g \in G$ and $x \in X$ there exists a unique $gx \in X$ such that $\forall x \in X$ and $g_1, \ g_2 \in G$, $g_1 g_2 (x) = \ g_1(g_2 x)$ and $ex = x$, where e denotes the identity in G.

Remark: *The action of G from the right can be defined in a similar way.*

Definition 1.5.5.

Let g be an element of a group G. The conjugacy class of g in G is given by $\{xgx^{-1} | x \in G\}$.

Definition 1.5.6.

If a finite group G acts on a set X with n elements, each $g \in G$ corresponds to a permutation σ of X, which can be written uniquely as a product of disjoint cycles. If σ has α_1 cycles of length 1, α_2 cycles of length 2, . . . , α_n cycles of length n, we say that g corresponds to σ and hence g has cycle type $(\alpha_1,\ \alpha_2,\ .\ .\ .\ ,\ \alpha_n)$.

Definition 1.5.7.

If a finite group G acts on a set X, $|X| = n$, and $g \in G$ has cycle type $(\alpha_1,\ \alpha_2,\ .\ .\ .\ ,\ \alpha_n)$, we define the monomial of g to be $mon\,(g) = t_1^{\alpha_1} t_2^{\alpha_2}\ .\ .\ .\ t_n^{\alpha_n}$, where $t_1,\ t_2,\ .\ .\ .,\ t_n$ are distinct commuting indeterminates.

Definition 1.5.8.

The cycle index of the action of G on X is the polynomial (say over the rational field Q) in $t_1,\ t_2,\ .\ .\ .,\ t_n$ given by;

$$Z(G) = Z_{G,X}(t_1, t_2, \cdots, t_n) = \frac{1}{|G|} \sum_{g \in G}^{m} \{mon(g)\}$$

Note that if G has conjugacy classes $K_1, K_2,\ .\ .\ ., K_m$ with $g_i \in K_i$ then

$$Z(G) = \frac{1}{|G|} \sum_{i=1}^{m} |K_i|\, mon(g_i).$$

Definition 1.5.9.

Let G act on a set X, then X is partitioned into disjoint equivalence classes called orbits or transitivity classes of the action. For each $x \in X$, the orbit containing x is denoted by $orb_G(x)$.

Definition 1.5.10.

If the action of a group G on a set X has only one orbit, then we say that G acts transitively on X. In other words, G acts transitively on X if for every pair of points $x, y \in X$, there exists $g \in G$ such that $gx = y$.

Definition 1.5.11.

Let G act on a set X and let $x \in X$. The stabilizer of x in G, denoted by $Stab_G(x)$, is given by $Stab_G(x) = \{g \in G | gx = x\}$.

Definition 1.5.12.

Let G act on a set X. The set of elements of X fixed by g is called the fixed point set of g, denoted by $Fix(g)$ and is given by $Fix(g) = \{x \in X | gx = x\}$.

Definition 1.5.13.

Given any two sets X and Y which are not necessarily equal, we can form another set of ordered pairs $X \times Y = \{(x, y) | x \in X \text{ and } y \in Y\}$ called the Cartesian product of X and Y.

Definition 1.5.14.

Let H and K be any two groups and let $G = H \times K$ be such that $(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2)$ for all $h_1, h_2 \in H$ and $k_1, k_2 \in K$, then G is an external direct product group of H and K.

Definition 1.5.15.

Let H and K be normal subgroups of a group $G = H \times K$ and further let $H \cap K = \{e\}$, then G is an internal direct product group of H and K.

Definition 1.5.16.

A group G is said to be a semidirect product group of N by H if;

i. $N \lhd G$ *and* $H < G$

ii. $N \cap H = \{e\}$

iii. $NH = G$.

We symbolically express this as $G = N \rtimes H$.

Definition 1.5.17.

Consider the array of objects given by;

$(x_1, y_1)(x_1, y_2)(x_1, y_3)\cdots\ (x_1, y_q)$

$\vdots$

$(x_p, y_1)(x_p, y_2)(x_1, y_3)\cdots\ (x_p, y_q)$

Consider the set of all the permutations of these pq objects obtained by permuting within each row according to some $h \in H$ (not necessarily the same for each row) and then permuting the rows according to some $g \in G$. This set of permutation is the wreath product group of G by H denoted by $G[H]$. An element in $G[H]$ is denoted by $(g; h_1, h_2, \cdots, h_p)$.

Definition 1.5.18.

The group of symmetries of a regular $n-$gon (n rotational symmetries and n reflectional symmetries) is called the dihedral group and is denoted by D_n. This group is of degree n and order $2n$.

In general if $G = D_n$ *then,* $G = \langle a, b | a^n = b^2 = 1, ab = ba^{-1} \rangle$. *If* G *acts on the set* X *of vertices of a regular* n*-gon then* $N = C_n = \langle a \rangle$ *and* $H = C_2 = \langle b \rangle$, *and* $G = N \rtimes H$.

Definition 1.5.19.

Let $X = \{1, 2, 3, \ . \ . \ . \ , \ n\}$ *be a finite set. Then the group of all permutations of* X *is called the symmetric group on* n *elements and is denoted by* S_n. *This group is of order* $n!$.

Definition 1.5.20.

A Frobenius group is a group G *acting on a set* X *transitively in such a way that the stabilizer* H *of a point is non-trivial, but only the identity fixes two or more points. This means that* $H \cap (xHx^{-1}) = \{e\}$, *if* $x \in G \backslash H$.

Definition 1.5.21.

A geometrical substructure of the Euclidean space which generalizes some of the properties of the Euclidean space such that it is independent of the concepts of distance and measure of angles but maintains the properties related to parallelism and ratio of lengths for parallel line segments is referred to as an affine space.

An affine transformation is a function from an affine space to another affine space which preserves points, straight lines and planes.

The set of all invertible affine transformations from an affine space onto itself form a group G *over an affine space called the affine(p) group. The elements of the affine(p) group are all transformations of the form* $ax + b$ *where* a *is a non zero element in* $\mathbb{Z}_p$ *and* $b \in \mathbb{Z}_p$ *and thus the group is of order* $p(p-1)$. *The set* $C_p = \{x+b, \text{ where } b \in \mathbb{Z}_p\}$ *(translations) forms a normal cyclic subgroup of the affine group isomorphic to* $\mathbb{Z}_p$.

The set $C_{p-1} = \{ax,\ where\ \ 0 \neq a \in \mathbb{Z}_p\}$ *forms a cyclic group under multiplication and the affine group is a semidirect product of the two. An affine*(q) *group can be defined similarly for any* $q = p^r$.

The semidirect product of the cyclic subgroups $C_p = \{x + b,\ where\ b \in \mathbb{Z}_p\}$ *and* $C_{\frac{p-1}{2}} = \{ax,\ where\ \ a \text{ is a nonzero square in } \mathbb{Z}_p\}$ *of the affine group form another group known as the affine square group denoted as* $Aff_{\square}(p)$. *An* $Aff_{\square}(q)$ *can be defined similarly for any* $q = p^r$.

Definition 1.5.22.

A group G is metacyclic if it has a normal subgroup N such that the quotient group G/N *is cyclic.*

Definition 1.5.23.

An integer n is said to be a square free integer if its prime factorization has exactly one factor for each prime that appears in it.

Definition 1.5.24.

The Möbius function of any $n \ \in N$ *is given by,*

$$\mu(n) = \begin{cases} -1 & \text{if } n \text{ is a square free with an odd number of prime factors} \\ 0 & \text{if } n \text{ has a squared prime factor} \\ 1 & \text{if } n \text{ is a square free with an even number of prime factors.} \end{cases}$$

1.6 Preliminary results

In this section we give cycle indices of some finite permutation groups.

The proofs of Theorems 1.6.1, 1.6.2, 1.6.3, 1.6.4 and 1.6.5 are covered in Harary (1969).

Theorem 1.6.1.

Let S_n be the symmetric group of order $n!$. Then the cycle index of S_n acting on the set X of n elements is;

$$Z_{(S_n,X)} = \frac{1}{n!}\sum_j \frac{n!}{\prod_{k=1}^{n} k^{j_k} j_k!} t_1^{j_1} t_2^{j_2} \ . \ . \ . \ t_n^{j_n},$$

where the sum is taken over all partitions j of n.

Theorem 1.6.2.

Let A_n be the alternating group of order $\frac{n!}{2}$. Then the cycle index of A_n acting on the set X of n elements is;

$$Z_{(A_n,X)} = \frac{1}{n!}\sum_j \frac{n!\left[1+(-1)^{j_2+j_4+\ . \ . \ .}\right]}{\prod_{k=1}^{n} k^{j_k} j_k!} t_1^{j_1} t_2^{j_2} \ . \ . \ . \ t_n^{j_n},$$

where the sum is taken over all partitions j of n.

Theorem 1.6.3.

Let C_n be the cyclic group of permutations generated by $g = (12\ . \ . \ .\ n)$, then for each divisor d of n there are $\phi(d)$ permutations in C_n which have $\frac{n}{d}$ cycles of length d

and hence the cycle index of C_n acting on the set X of n elements is;

$$Z_{(C_n,X)} = \frac{1}{n}\sum_{d|n}\phi(d)t_d^{\frac{n}{d}}.$$

Theorem 1.6.4.

Let D_n be the dihedral group. Then the cycle index of D_n acting on the set X of the vertices of a regular $n-$gon is;

$$Z_{(D_n,X)} = \begin{cases} \frac{1}{2n}\left[\sum_{d|n}\{\phi\left(d\right)t_d^{\frac{n}{d}}\} + \frac{n}{2}t_1^2 t_2^{\frac{n-2}{2}} + \frac{n}{2}t_2^{\frac{n}{2}}\right] \text{if n is even} \\ \frac{1}{2n}\left[\sum_{d|n}\{\phi\left(d\right)t_d^{\frac{n}{d}}\} + nt_1 t_2^{\frac{n-1}{2}}\right] \text{if n is odd.} \end{cases}$$

Theorem 1.6.5.

Let x be a permutation with cycle type $(\alpha_1, \alpha_2, \alpha_3, . . ., \alpha_n)$. Then;

i. the number $\pi(x^l)$ of cycles of length one in x^l is $\sum_{i|l} i\alpha_i$.

ii. $\alpha_l = \frac{1}{l}\sum_{i|l}\pi\left(x^{\frac{l}{i}}\right)\mu(i)$ where μ is the Möbius function.

Theorem 1.6.6.

The length of a conjugacy class in G containing $g \in G$ is given by $|C^g| = \frac{|G|}{|C_G(g)|}$

CHAPTER 2

LITERATURE REVIEW

Profound influence on the future of combinatorics has been due to the contributions by Howard Redfield, George Pólya, De Bruijn and Frank Harary. Harary (1960) pointed out the work that was done by Redfield (1927) which showed the relationship between the theory of finite groups and enumerative combinatorics. This forms a basis of the study of cycle indices. However, Redfield's paper was almost ignored. The outstanding contributions to enumeration, which he had made, were not recognized until his death in 1944. In his paper, Redfield introduced the concept of group-reduced distributions (which we today call the cycle index of a permutation group). He used the concept of group-reduced distributions to count the number of in-equivalent configurations.

Pólya (1937), independently discovered the concept of the cycle index of a permutation group and gave it its present name. The researcher presented to the combinatorial world a powerful theorem which reduced to a matter of routine solution of a wide range of problems. This theorem contained within it the potential for growth and generalization in many directions. Pólya's Theorem relates to the enumeration of mathematical objects called configurations, which in abstract sense can be defined as mappings from a set D to a set R. The theorem states that the configuration counting series $F(x) = A_1x + A_2x^2 + A_3x^3 + \ . \ . \ .$ is obtained by substituting the figure counting series $f(x) = a_1x + a_2x^2 + a_3x^3 + \ . \ . \ .$ into the cycle index where a_i is the number of figures of weight i. This means that we replace every occurrence of indeterminate t_i in the cycle index by $f(x^i)$. By Pólya's Theorem, cycle index became a very powerful enumeration tool and hence the need for computing the cycle indices of permutation groups. The researcher used the cycle index to count graphs and chemical compounds.

After Pólya, several scholars have studied cycle indices of different permutation groups. Bruijn and Klarner (1969) extended and generalized Pólya's Theorem. This researchers' generalization consisted the introduction of another group, say H, which permutes the figures, in addition to the group G of permutations of boxes. Two configurations were then regarded as equivalent if one could be obtained from the other by permuting both boxes and figures by appropriate permutations. Subsequently, Bruijn and Klarner (1969) enumerated generalized graphs.

The ties between Pólya's Theorem and De Bruijn's Theorem were strengthened by Harary and Palmer (1966) by publication of their power group enumeration Theorem. Bruijn and Klarner (1969) answered the enumeration problem when two permutation groups A and B are involved with A acting on X and B on Y. Pólya's formula can be seen as a special case of the De Bruijn result with B being the identity group. The Power Group Enumeration Theorem gives the same outcome with the power group B^A as the permutation group acting on the set Y^X of functions. Like De Bruijn's Theorem, this relates to a set of mappings $f : D \to R$, with a group G acting on D and another group H acting on R. These mappings are treated in the same way as boxes in Pólya's Theorem and under the action of the two groups they are permuted among themselves in a rather complicated manner. Thus, the two groups G and H induce a group of permutations of the mappings, denoted by H^G

and called the 'power group'. The problem of enumerating mappings then reduces to that of finding the cycle index of this group, followed by the application of Pólya's Theorem. Harary and Palmer (1966) gave formulas for computing some of the cycle index in question, and hence solving of the De Bruijns type of problem, as well as some more general problems along the same lines. Harary and Palmer (1973) also gives more information on the power group enumeration Theorem.

Another theorem that can be used to solve problems similar to those which Pólya's Theorem applies is the Superposition Theorem studied by Read (1959) where he enumerated locally restricted graphs and the number of r-coloured graphs and non-separable graphs. The scope of this theorem is most easily seen in a graph theoretical setting, in which it relates to the number of non-isomorphic graphs that can be formed by superposing two graphs G_1 and G_2 on one and the same set of vertices. It turns out that the required number of superposition depends only on the cycle indices of the automorphism groups of G_1 and G_2. In fact, if these cycle indices are;

$$\frac{1}{|G_1|}\sum_{(j)} A_{(j)} t_1^{j_1} t_2^{j_2} \ldots t_p^{j_p}$$

and

$$\frac{1}{|G_2|}\sum_{(j)} B_{(j)} t_1^{j_1} t_2^{j_2} \ldots t_p^{j_p},$$

then the required number of superpositions is

$$\frac{1}{|G_1 G_2|}\sum_{(j)} A_{(j)} B_{(j)} t^{j_1 j_2 \ldots j_p . j_1! j_2! \ldots j_p!}.$$

Thus the Superposition Theorem can be used, among many other things to find individual coefficients in the counting series produced by Pólya's Theorem, De Bruijn's Theorem or the Power Group Enumeration Theorem, without having to find the whole series.

Pólya's Theorem has also been applied to the theory of music in determining the number of chords. To define this, one takes the n-scale to be the integers from 0 to $n-1$ under addition modulo n. There are translations $a \rightarrow a+i$, where $0 \leq i < n$. An equivalence class (that is, an orbit) is called a chord, and one wishes to determine for each $r < n$, the number of r-chords; that is, the number of orbits consisting of r elements. This is equivalent to colouring the n-vertices by two colours. We choose the vertices in the chord by colouring them by one colour and those which are not in it by other colour. The group is simply the cyclic group of order n whose cycle index is given in Theorem 1.6.3. In this case, we substitute $1+x^d$ for S_d and obtain the generating function whose coefficient of x^r is the number of r-chords. We obtain the number of r-chords to be

$$\frac{1}{n}\sum_{d|n}\phi(d)\binom{n/d}{r/d}$$

Sometimes, one allows for bigger group of transformations of the scale by allowing inversion $a \rightarrow -a$ also. Then, the group becomes the dihedral group D_n of order $2n$ formed by the rotations and reflection of a regular $n-$gon whose cycle index is given in Theorem 1.6.4.

It can be determined that the number of r-chords in this dihedral case is;

$$\frac{1}{2n}\sum_{d|(n,r)}\phi(d)\begin{pmatrix} n/d \\ r/d \end{pmatrix} + \frac{1}{2}\begin{pmatrix} [n/2] \\ [r/2] \end{pmatrix}, \text{ if } n \text{ is odd}$$

$$\frac{1}{2n}\sum_{d|(n,r)}\phi(d)\begin{pmatrix} n/d \\ r/d \end{pmatrix} + \frac{1}{2}\begin{pmatrix} n/2 \\ r/2 \end{pmatrix}, \text{ if } n \text{ and } r \text{ are even}$$

$$\frac{1}{2n}\sum_{d|(n,r)}\phi(d)\begin{pmatrix} n/d \\ r/d \end{pmatrix} + \frac{1}{2}\begin{pmatrix} \frac{n-2}{2} \\ [r/2] \end{pmatrix}, \text{ if } n \text{ is even and } r \text{ is odd.}$$

For more information on this, one can refer to Pólya and Read (1987).

Harary (1959) computed the cycle index of exponentiation of permutation groups. Harrison and High (1968) computed the cycle index of a product of permutation groups. Joseph (1981) studied the vector space cycle index. Several other cycle index formulas can be found in Krishnamurthy (1985). The cycle index formulas derived by Krishnamurthy were used while deriving the cycle index of the symmetric group, and the dihedral group.

Kamuti (1992) determined the cycle structure of elements of $PGL(2,q)$ and $PSL(2,q)$ acting on the cosets of their maximal subgroups. The method used to derive these cycle structures was used to derive the cycle indices of the affine group. The study devised general formulas for computation of cycle index formulas of the action of these groups. Harald (1997) derived the cycle indices of linear, affine, and projective groups. Jason (1999) derived the cycle indices for the finite classical groups.

Kamuti and Obong'o (2002) computed the cycle index of the reduced ordered triples group $S_n^{[3]}$ which was further extended by Kamuti and Njuguna (2004)) to cycle index of the reduced ordered $r-$group $S_n^{[r]}$. Kamuti (2004) expressed the cycle index formula of $G = H \rtimes K$ in terms of the cycle index of H and the cycle index of K. This study considered semidirect products of Frobenius groups only. Cameron (2007) studied the cycle index of the direct product permutation groups. Munywoki *et al.* (2010) studied the cycle indices of Frobenius groups. In their study, they considered a Frobenius group $G = M \rtimes H$ acting on a set X and expressed the cycle index of G in terms of the cycle indices of M and H and the resulting cycle was given as; $Z_{(G,X)} = \frac{1}{|H|}Z_{(M,X)} + Z_{(H,X)} - \frac{1}{|H|}Z_{(1,X)}$. This cycle will be used in deriving the cycle index of Frobenius group.

Jason *et al.* (2012) derived the cycle indices for finite orthogonal groups of even characteristic. Kamuti (2012) expressed the cycle index of the internal direct product of a group $G = M \times H$ in terms of the cycle index of M and cycle index of H. In his paper, he showed that if $G = M \times H$(internal direct product), $M \lhd G, H \lhd G$ $MH = G$ and $M \bigcap H = \{e\}$ then G acts on $S = G/H$, set of left cosets of H in G by left multiplication, that is if $x \in G$, $yH \in S$, then $x(yH) = xyH \in S$. There is a natural bijection between M and S, given by $u \to uH$ for each $u \in M$, however that does not determine equivalent actions of G on S and M. A more complicated action of G on M, which is equivalent to its action on S can be defined as follows. For each $x \in G$ then x can be written uniquely as $x = uh$ and each $s \in S$ can be written as $s = uH$, with $u \in M$ hence we have $xs = x(uH) = vhuH = vhuh^{-1}H = v.{}^huH$, where ${}^hu = huh^{-1} \in M$. Thus, we get an action of G on M that is a combination of conjugation and multiplication: $x = vh$ acts on u by $u \xrightarrow{x=vh} v.^{h}u$. Since x can be written uniquely as $x = uh$ with $u \in M,\ h \in H$, also each $s \in S = G/H$ can be written uniquely as $s = uH$ with $u \in M$. Then the action of $x = uh$ on $v \in M$ becomes $v \to u.^{h}v = uv$ (since elements of M and H commute). Thus, $mon(uh) = mon(u)$ for all u and h. So

$$\begin{aligned} Z_{(G,S)} &= |G|^{-1} \sum \{mon(uh) | u \in M, h \in H\} \\ &= |G|^{-1}|H| \sum \{mon(u) | u \in M\} \\ &= |M|^{-1} \sum \{mon(u) | u \in M\} \\ &= Z_{(M,S)} \end{aligned}$$

Vladimir and Kovijanic (2017) derived the cycle index of the automorphism group of $\mathbb{Z}_n$ which was given as;

$Z_{(U_n,\ \mathbb{Z}_n)} = Z_{(U_{p_1^{\alpha_1}},\ \mathbb{Z}_{p_1^{\alpha_1}})} \times Z_{(U_{p_2^{\alpha_2}},\ \mathbb{Z}_{p_2^{\alpha_2}})} \times\ \ldots\ \times Z_{(U_{p_s^{\alpha_s}},\ \mathbb{Z}_{p_s^{\alpha_s}})}$ where $U_n = Aut(\ \mathbb{Z}_n)$

Muthoka *et al.* (2015) derived the cycle index formulas for the dihedral group D_n acting on unordered 2−element subsets from $X = \{1, 2, ..., n\}$. The formulas were found to be;

$$Z_{\left(D_n, X^{(2)}\right)} = \frac{1}{2n}\left[\sum_{d|n} \phi\left(d\right) t_d^{\frac{n(n-1)}{2d}} + n t_1^{\frac{(n-1)}{2}} t_2^{\frac{(n-1)^2}{4}}\right]$$

for an odd value of n and

$$Z_{\left(D_n, X^{(2)}\right)} = \frac{1}{2n}\left[\sum_{d|n, 2|d} \phi\left(d\right) t_{\frac{d}{2}}^{\frac{n}{d}} t_d^{\frac{n(n-2)}{2d}} + \sum_{d|n, 2\nmid d} \phi\left(d\right) t_d^{\frac{n(n-2)}{2d}} + n t_1^{\frac{n}{2}} t_2^{\frac{n(n-2)}{4}}\right]$$

for even n.

Later Muthoka *et al.* (2016) extended this work to D_n acting on the ordered 2−element subsets from $X = \{1,2,...,n\}$. The formulas were found to be;

$$Z_{\left(D_n,X^{[2]}\right)} = \frac{1}{2n}\left[\sum_{d|n}\phi\left(d\right)t_d^{\frac{n(n-1)}{d}} + nt_2^{\frac{n(n-1)}{2}}\right]$$

for an odd value of n and,

$$Z_{\left(D_n,X^{[2]}\right)} = \frac{1}{2n}\left[\sum_{d|n,2|d}\phi\left(d\right)t_d^{\frac{n(n-1)}{2d}} + \sum_{d|n,2\nmid d}\phi\left(d\right)t_d^{\frac{n(n-1)}{d}} + \frac{n}{2}t_1^2t_2^{\frac{(n-1)(n-2)}{2}} + \frac{n}{2}t_2^{\frac{n(n-1)}{2}}\right]$$

for an even value of n.

Rotich (2016) worked on cycle indices, subdegrees and suborbital graphs of $PGL(2,q)$ acting on the cosets of its subgroups.

More recently Peter and Jason (2017) studied some properties of the cycle polynomial of a permutation group. Muthoka (2017) derived the cycle index formulas for D_n acting on unordered triples and the resulting formulas were given as;

$$\begin{aligned} Z_{\left(D_n,X^{(3)}\right)} \quad = \quad & \frac{1}{2n}\Bigg[\sum_{d|n,3|d}\phi\left(d\right)b_{\frac{d}{3}}^{\frac{n}{d}}b_d^{\frac{n^2(n-3)}{6d}} + \sum_{d|n,3\nmid d}\phi\left(d\right)b_d^{\frac{n(n-1)(n-2)}{6d}} + \frac{n}{2}b_1^{n-2}b_2^{\frac{(n^2-4)(n-3)}{12}} \\ & + \frac{n}{2}b_2^{\frac{n(n-1)(n-2)}{12}}\Bigg] \end{aligned}$$

for an even value of n and

$$Z_{\left(D_n,X^{(3)}\right)} = \frac{1}{2n}\left[\sum_{d|n,3|d}\phi\left(d\right)b_{\frac{d}{3}}^{\frac{n}{d}}b_d^{\frac{n^2(n-3)}{6d}} + \sum_{d|n,3\nmid d}\phi\left(d\right)b_d^{\frac{n(n-1)(n-2)}{6d}} + nb_1^{\frac{n-1}{2}}b_2^{\frac{\left(n^2-1\right)(n-3)}{12}}\right]$$

for an odd value of n.

Rotich (2018) derived the cycle indices of $PGL(2,q)$ acting on the cosets of its subgroups by computing the disjoint cycle structures of elements G acting on the cosets of $H = D_{2(q-1)}$. The resulting cycle index was given to be;

$$Z(G) = \frac{1}{|G|}[t_1^{\frac{|G|}{|H|}} + (q^2-1)t_p^{p^{f-1}(q+1)} + \frac{q(q+1)}{2}\sum_{1\neq d|q-1}\phi(d)t_1^2 t_d^{\frac{(q-1)(q+2)}{d}} + \frac{q(q-1)}{2}\sum_{1\neq d|q+1}\phi(d)t_d^{\frac{q(q+1)}{d}}].$$

Kimani *et al.* (2019) derived the cycle index formula of $PSL(2,q)$ acting on the cosets of $PSL(2,e)$, where q is an even power of e. The resulting formulas were given to be;

$$\begin{aligned}
Z(G) = \frac{1}{q(q^2-1)}\Bigg[& t_1^{\frac{q\left(q^2-1\right)}{e\left(e^2-1\right)}} + \left(q^2-1\right) t_1^{\frac{q}{e}} t_2^{\frac{q\left(q^2-e^2\right)}{2e\left(e^2-1\right)}} \\
& + \frac{q(q+1)}{2} \sum_{\substack{1\neq d|q-1 \\ ul=j\neq q-1=v}} \phi(d)\, t_l^{\frac{q-1}{l(e-1)}} t_d^{\frac{(q-1)\left(q^2+q-e^2-e\right)}{de\left(e^2-1\right)}} \\
& + \frac{q(q+1)}{2} \sum_{\substack{1\neq d|q-1 \\ uh=v\neq q-1=j}} \phi(d)\, t_h^{\frac{q-1}{h(e+1)}} t_d^{\frac{(q-1)\left(q^2+q-e^2+e\right)}{de\left(e^2-1\right)}} \\
& + \frac{q(q+1)}{2} \sum_{\substack{1\neq d|q-1 \\ v,j\neq q-1 \\ \frac{ul}{j}=\frac{uh}{v}=1}} \phi(d)\, t_l^{\frac{q-1}{l(e-1)}} t_h^{\frac{q-1}{h(e+1)}} t_d^{\frac{(q-1)\left(q^2+q-2e^2\right)}{de\left(e^2-1\right)}} \\
& + \frac{q(q+1)}{2} \sum_{\substack{1\neq d|q-1 \\ j=v=q-1}} \phi(d) t_d^{\frac{q\left(q^2-1\right)}{de\left(e^2-1\right)}} \\
& + \frac{q(q-1)}{2} \sum_{1\neq d|q+1} \phi(d) t_d^{\frac{q\left(q^2-1\right)}{de\left(e^2-1\right)}} \Bigg],
\end{aligned}$$

when q is even and;

$$Z(G) = \frac{2}{q(q^2-1)}\left[t_1^{\frac{q(q^2-1)}{e(e^2-1)}} + \frac{(q^2-1)}{2} t_1^{\frac{2q}{e}} t_p^{\frac{q(q^2-2e^2+1)}{pe(e^2-1)}} + \frac{(q^2-1)}{2} t_p^{\frac{q(q^2-1)}{pe(e^2-1)}} \right.$$

$$+\frac{q(q+1)}{2} \sum_{\substack{1\neq d|\frac{q-1}{2} \\ \frac{ul}{j}=1, j\neq\frac{q-1}{2}=v}} \phi(d)\, t_l^{\frac{q-1}{l(e-1)}} t_d^{\frac{(q-1)(q^2+q-e^2-e)}{de(e^2-1)}}$$

$$+\frac{q(q+1)}{2} \sum_{\substack{1\neq d|\frac{q-1}{2} \\ \frac{uh}{v}=1, v\neq\frac{q-1}{2}=j}} \phi(d)\, t_h^{\frac{q-1}{h(e+1)}} t_d^{\frac{(q-1)(q^2+q-e^2+e)}{de(e^2-1)}}$$

$$+\frac{q(q+1)}{2} \sum_{\substack{1\neq d|\frac{q-1}{2} \\ \frac{ul}{j}=1=\frac{uh}{v}, v, j\neq\frac{q-1}{2}}} \phi(d)\, t_l^{\frac{q-1}{l(e-1)}} t_h^{\frac{q-1}{h(e+1)}} t_d^{\frac{(q-1)(q^2+q-2e^2)}{de(e^2-1)}}$$

$$+\frac{q(q+1)}{2} \sum_{1\neq d|\frac{q-1}{2}=j=v} \phi(d) t_d^{\frac{q(q^2-1)}{de(e^2-1)}}$$

$$\left. +\frac{q(q-1)}{2} \sum_{1\neq d|\frac{q+1}{2}} \phi(d) t_d^{\frac{q(q^2-1)}{de(e^2-1)}} \right],$$

when q is odd.

Several scholars have used the cycle index in enumeration of different objects and structures. Harary (1955) counted the number of linear, rooted and connected graphs. Read (1960) also enumerated locally restricted graphs and the number of r-coloured graphs on labeled vertices. Harary (1967) studied the applications of Pólya's Theorem to permutation groups. Robinson (1970) enumerated coloured graphs and non-separable graphs. Bruijn and Klarner (1969) enumerated generalized graphs. Enumeration of stable stereo, position isomers and poly-substituted alcohols was done by Balasubramanian (1979).

CHAPTER 3

THE CYCLE INDEX OF THE DIHEDRAL GROUP AS A SEMIDIRECT PRODUCT OF THE CYCLIC GROUP OF ORDER n BY A CYCLIC GROUP OF ORDER TWO

3.1 Introduction

Let $G = N \rtimes H$, then G is a semidirect product group if $N \triangleleft G$, $H < G, NH = G$ and $N \cap H = \{e\}$. The aim of this chapter is to express the cycle index of the dihedral group D_n in terms of the cycle index of the cyclic group C_n and that of a cyclic group of order two C_2. In this case the dihedral group can be written as $D_n = C_n \rtimes C_2$ since the dihedral group is a semidirect product of the two subgroups. This chapter has three sections. In Section 3.1, we give the introduction while in Section 3.2, we show that the dihedral group is a semidirect product of the cyclic group C_n and a cyclic group C_2. In Section 3.3, we express the cycle index formula of the dihedral group in terms of the cycle index formulas of C_n and C_2. In subsection 3.2.1 we consider an odd value of n and an even value of n is considered in subsection 3.2.2.

3.2 The dihedral group as a semidirect product group

Theorem 3.2.1.

The dihedral group is a semidirect product group of C_n and C_2.

Proof.

Let $N = C_n \triangleleft D_n$ and $H = C_2 < D_n$.

Clearly, $N \cap H = \{e\}$, where e is the identity element in D_n.

Since $|NH| = \frac{|N||H|}{|N \cap H|} = \frac{(n.2)}{1} = 2n = |D_n|$,

we deduce that, $D_n = NH = N \rtimes H \cong C_n \rtimes C_2$ □

3.3 Expressing the cycle index of D_n in terms of cycle index of C_n and C_2

We now use the above information to establish the relationship between the cycle index formulas of the dihedral group and that of a cyclic group of order two C_2 acting on n elements and the cyclic group of order n, C_n.

3.3.1 If n is even

Suppose that n is even. Then from Theorem 1.6.4 the cycle index is given by;

$$\begin{aligned} Z_{(D_n,X)} &= \frac{1}{2n}\left(\sum_{d|n} \phi(d)\, t_d^{\frac{n}{d}} + \frac{n}{2} t_1^2 t_2^{\frac{n-2}{2}} + \frac{n}{2} t_2^{\frac{n}{2}}\right) \\ &= \frac{1}{2} Z_{(N,X)} + \frac{1}{4}\left(t_1^2 t_2^{\frac{n-2}{2}} + t_2^{\frac{n}{2}}\right) \end{aligned}$$

Since $H = \langle b \rangle$ is equal to the stabilizer of a point, we have

$mon\,(b) = t_1^2 t_2^{\frac{n-2}{2}}$.

Since H is a reflection and $|H| = 2$ we have;

$Z_{(H,X)} = \frac{1}{2}\left(t_1^n + t_1^2 t_2^{\frac{n-2}{2}}\right)$

Therefore;

$Z_{(D_n,X)} = \frac{1}{2} Z_{(N,X)} + \frac{1}{2} Z_{(H,X)} + \frac{1}{4} t_2^{\frac{n}{2}} - \frac{1}{4} Z_{(1,X)}$

Thus;

$$Z_{(G,X)} = \frac{1}{2} Z_{(C_n,X)} + \frac{1}{2} Z_{(C_2,X)} + \frac{1}{4} t_2^{\frac{n}{2}} - \frac{1}{4} Z_{(1,X)} \qquad (3.1)$$

We note that the extra term $\frac{1}{4}t_2^{\frac{n}{2}}$ is a result of the fact that there are $\frac{n}{2}$ elements of G that are neither in N nor in a conjugate of H. We also note that $mon(ab) = t_2^{\frac{n}{2}}$ or the extra term could be defined in terms of $Z_{(K,X)}$ where $K = \langle (a\ b) \rangle$ of order 2.

Example 3.3.1

Let $n = 6$ and $X = \{1, 2, 3, 4, 5, 6\}$, then by Theorem 1.6.4 we have;

$$\begin{aligned}
Z_{(D_6,X)} &= \frac{1}{12}\left(t_1^6 + t_2^3 + 2t_3^2 + 2t_6 + 3t_1^2t_2^2 + 3t_2^3\right) \\
&= \frac{1}{12}\left(t_1^6 + t_2^3 + 2t_3^2 + 2t_6\right) + \frac{1}{4}t_1^2t_2^2 + \frac{1}{4}t_2^3 \\
&= \frac{1}{12}\left(t_1^6 + t_2^3 + 2t_3^2 + 2t_6\right) + \frac{1}{4}\left(t_1^6 + t_1^2t_2^2\right) + \frac{1}{4}t_2^3 - \frac{1}{4}t_1^6 \\
&= \frac{1}{2}.\ \frac{1}{6}\left(t_1^6 + t_2^3 + 2t_3^2 + 2t_6\right) + \frac{1}{2}.\ \frac{1}{2}\left(t_1^6 + t_1^2t_2^2\right) + \frac{1}{4}t_2^3 - \frac{1}{4}t_1^6 \\
&= \frac{1}{2}Z_{(C_6,X)} + \frac{1}{2}Z_{(C_2,X)} - Z_{(1,X)} + \frac{1}{4}t_2^3.
\end{aligned}$$

3.3.2 If n is odd

Suppose that n is odd.

Then from Theorem 1.6.4 the cycle index D_n is given by

$$\begin{aligned}
Z_{(D_n,X)} &= \frac{1}{2n}\left(\sum_{d|n}\phi(d)t_d^{\frac{n}{d}} + nt_1t_2^{\frac{n-1}{2}}\right) \\
&= \frac{1}{2n}\left(\{\sum_{d|n}\phi(d)t_d^{\frac{n}{d}}\} + nt_1t_2^{\frac{n-1}{2}}\right) \\
&= \frac{1}{2}\{\frac{1}{n}\sum_{d|n}\phi(d)t_d^{\frac{n}{d}}\} + \frac{1}{2}t_1t_2^{\frac{n-1}{2}} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{2}\{t_1^n + t_1t_2^{\frac{n-1}{2}}\} - \frac{1}{2}t_1^n \\
&= \frac{1}{2}Z_{(N,X)} + Z_{(H,X)} - \frac{1}{2}Z_{(1,X)} \\
&= \frac{1}{2}Z_{(C_n,X)} + Z_{(C_2,X)} - \frac{1}{2}Z_{(1,X)} \qquad (3.2)
\end{aligned}$$

Example 3.3.2

Let $n = 5$ and $X = \{1, 2, 3, 4, 5\}$ then by Theorem 1.6.4 we have;

$$\begin{aligned}
Z_{(D_5,X)} &= \frac{1}{10}\left(t_1^5 + 4t_5 + 5t_1t_2^2\right) \\
&= \frac{1}{10}\left(t_1^5 + 4t_5\right) + \frac{1}{2}t_1t_2^2 \\
&= \frac{1}{2}.\frac{1}{5}\left(t_1^5 + 4t_5\right) + \frac{1}{2}\left(t_1^5 + t_1t_2^2\right) - \frac{1}{2}t_1^5 \\
&= \frac{1}{2}Z_{(C_5,X)} + Z_{(C_2,X)} - \frac{1}{2}Z_{(1,X)}
\end{aligned}$$

CHAPTER 4

THE CYCLE INDEX OF THE SYMMETRIC GROUP AS A SEMIDIRECT PRODUCT GROUP OF THE ALTERNATING GROUP BY A CYCLIC GROUP OF ORDER TWO

4.1 Introduction

The aim of this chapter is to express the cycle index of the symmetric group S_n in terms of the cycle index of the alternating group A_n and that of a cyclic group of order two $C_2 = \langle (ab) \rangle$. In this case, the symmetric group can be written as $S_n = A_n \rtimes C_2$ since it is a semidirect product of the two subgroups. This chapter has four sections. In Section 4.1 we give the introduction while in Section 4.2 we show that the symmetric group is a semidirect product of the alternating group and a cyclic group C_2. In Section 4.3 we give some examples of cycle index formulas of the symmetric group for $n = 3, 4, 5, 6, 7$ and 8 which are used in Section 4.4 to come up with a general expression of the cycle index of symmetric group in terms of the alternating group and a cyclic group of order two.

4.2 The symmetric group as a semidirect product group

Theorem 4.2.1.

The symmetric group is a semidirect product group of A_n and $C_2 = \langle (ab) \rangle$.

Proof.

Let $N = A_n \lhd S_n$ and $H = C_2 = \langle (ab) \rangle < S_n$.

Clearly, $N \cap H = \{e\}$, where e is the identity element in S_n.

Since $|NH| = \frac{|N||H|}{|N \cap H|} = \frac{(\frac{n!}{2}.2)}{1} = n! = |S_n|$,

we deduce that, $S_n = NH = N \rtimes H \cong A_n \rtimes C_2$ □

4.3 Some examples

4.3.1 Cycle index of S_3

Suppose $X = \{1, 2, 3\}$ so that $n = 3$,

$G = S_3 = \{1, (123), (132), (12), (13), (23)\}$,

$N = A_3 = \{1, (123), (132)\}$ and

$H = C_2 = \{1, (12)\}$.

Then;

$Z_{(G,X)} = \frac{1}{6}\{t_1^3 + 2t_3 + 3t_1t_2\}$,

$Z_{(N,X)} = \frac{1}{3}\{ t_1^3 + 2t_3\}$ and

$Z_{(H,X)} = \frac{1}{2}\{t_1^3 + t_1t_2\}$.

Thus;

$$
\begin{aligned}
Z_{(G,X)} &= \frac{1}{6}\{t_1^3 + 2t_3 + 3t_1t_2\} \\
&= \frac{1}{2}\frac{1}{3}\{t_1^3 + 2t_3\} + \frac{1}{2}\{t_1^3 + t_1t_2\} - \frac{1}{2}t_1^3 \\
&= \frac{1}{2}Z_{(N,X)} + Z_{(H,X)} - \frac{1}{2}Z_{(1,X)} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{(3-2)!}Z_{(N,X)} - \frac{1}{2(3-2)!}Z_{(1,X)} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{(n-2)!}Z_{(N,X)} - \frac{1}{2(n-2)!}Z_{(1,X)}, \ \textit{where } n = 3.
\end{aligned}
$$

4.3.2 Cycle index of S_4

Suppose $X = \{1, 2, 3, 4\}$ so that $n = 4$. Then;

$$G = S_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (13), (14), (23),$$

$$(12), (24), (34), (12)(34), (13)(24), (14)(23), (1234), (1243), (1324), (1342),$$

$$(1432), (1423)\},$$

$$N = A_4 = \{1, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34),$$

$$(13)(24), (14)(23)\}$$

and $H = C_2 = \{1, (12)\}$.

Thus, $Z_{(G,X)}$ can be written as;

$Z_{(G,X)} = \frac{1}{24}\{t_1^4 + 8t_1t_3 + 3t_2^2 + 6t_1^2t_2 + 6t_4\}$,

$Z_{(N,X)} = \frac{1}{12}\{t_1^4 + 8t_1t_3 + 3t_2^2\}$

and $Z_{(H,X)} = \frac{1}{2}\{t_1^4 + t_1^2t_2\}$.

Thus;

$$
\begin{aligned}
Z_{(G,X)} &= \frac{1}{24}\{t_1^4 + 8t_1t_3 + 3t_2^2 + 6t_1^2t_2 + 6t_4\} \\
&= \frac{1}{24}\{t_1^4 + 8t_1t_3 + 3t_2^2\} + \frac{1}{24}\{6t_1^2t_2 + 6t_4\} \\
&= \frac{1}{2}\frac{1}{12}\{t_1^4 + 8t_1t_3 + 3t_2^2\} + \frac{1}{2}\frac{1}{2}\{t_1^4 + t_1^2t_2\} - \frac{1}{4}t_1^4 + \frac{1}{24}\{6t_4\} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{2}Z_{(H,X)} - \frac{1}{4}Z_{(1,X)} + \frac{1}{4}t_4 \\
&= \frac{1}{2}\ Z_{(N,X)} + \frac{1}{(4-2)!}Z_{(H,X)} - \frac{1}{2(4-2)!}Z_{(1,X)} + \frac{1}{24}\{6t_4\} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{(n-2)!}Z_{(H,X)} - \frac{1}{2(n-2)!}Z_{(1,X)} + \frac{1}{n!}\{6t_4\},\ \textit{where}\ n\ =\ 4.
\end{aligned}
$$

In this case, the extra term $\frac{1}{4!}\{6t_4\}$ is the contribution to $Z_{(G,X)}$ of the six odd permutations of X that are not transpositions. They are not in a conjugate of H and all of them form a single conjugacy class.

4.3.3 Cycle index of S_5

Suppose $X = \{1, 2, 3, 4, 5\}$, so that $n = 5$, $G = S_5$, N=A$_5$ and H=$\langle(12)\rangle$

Table 4.1: Cycle Types of Elements of S_5

Permutation Type	*Cycle Type*	*Corresponding Monomial*	*Corresponding No. of Elements in S_5*
(a)(b)(c)(d)(e)	(5,0,0,0,0)	t_1^5	1
(a)(bc)(de)	(1,2,0,0,0)	$t_1t_2^2$	15
(a)(b)(cde)	(2,0,1,0,0)	$t_1^2t_3$	20
(abcde)	(0,0,0,0,1)	t_5	24
(a)(b)(c)(de)	(3,1,0,0,0)	$t_1^3t_2$	10
(ab)(cde)	(0,1,1,0,0)	t_2t_3	20
(a)(bcde)	(1,0,0,1,0)	t_1t_4	30
TOTAL			$120 = \|S_5\|$

Thus;

$Z_{(G,X)}=\frac{1}{120}\{t_1^5+15t_1t_2^2+20t_1^2t_3+24t_5+10t_1^3t_2+20t_2t_3+30t_1t_4\}$,

$Z_{(N,X)} = \frac{1}{60}\{t_1^5 + 15t_1t_2^2 + 20t_1^2t_3 + 24t_5\}$ and

$Z_{(H,X)} = \frac{1}{2}\{t_1^5 + t_1^3t_2\}$.

Thus, $Z_{(G,X)}$ can be rewritten as;

$$\begin{aligned}
Z_{(G,X)} &= \frac{1}{120}\{t_1^5 + 15t_1t_2^2 + 20t_1^2t_3 + 24t_5\} + \frac{1}{120}\{10t_1^3t_2 + 20t_2t_3 + 30t_1t_4\} \\
&= \frac{1}{2}\frac{1}{60}\{t_1^5 + 15t_1t_2^2 + 20t_1^2t_3 + 24t_5\} + \frac{1}{6}\frac{1}{2}\{t_1^5 + t_1^3t_2\} - \frac{1}{12}t_1^5 \\
&\quad + \frac{1}{120}\{20t_2t_3 + 30t_1t_4\} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{6}Z_{(H,X)} - \frac{1}{12}Z_{(1,X)} + \frac{1}{5!}\{20t_2t_3+30t_1t_4\}
\end{aligned}$$

$$= \frac{1}{2}Z_{(N,X)} + \frac{1}{(5-2)!}Z_{(H,X)} - \frac{1}{2\,(5-2)!}Z_{(1,X)} + \frac{1}{5!}\{20t_2t_3{+}30t_1t_4\}$$
$$= \frac{1}{2}Z_{(N,X)} + \frac{1}{(n-2)!}Z_{(H,X)} - \frac{1}{2\,(n-2)!}Z_{(1,X)} + \frac{1}{n!}\{20t_2t_3{+}30t_1t_4\}$$

In this case $\frac{1}{5!}\{20t_2t_3{+}30t_1t_4\}$ is the contribution to $Z_{(G,X)}$ of the 50 odd permutations of X that are not transpositions. These permutations are not in a conjugate of H and form two conjugacy classes; one consisting of 20 elements and the other 30.

4.3.4 Cycle index of S_6

Suppose $X = \{1,2,3,4,5,6\}$ so that $G = S_6$, N $=A_6$ and $H = \langle(12)\rangle$.

Table 4.2: Cycle Types of Elements of S_6

Permutation Type	*Cycle Type*	*Corresponding Monomial*	*Corresponding No. of Elements in* S_6
(a)(b)(c)(d)(e)(f)	(6,0,0,0,0,0)	t_1^6	1
(a)(b)(cd)(ef))	(2,2,0,0,0,0)	$t_1^2t_2^2$	45
(a)(b)(c)(def)	(3,0,1,0,0,0)	$t_1^3t_3$	40
(abc)(def)	(0,0,2,0,0,0)	t_3^2	40
(a)(bcdef)	(1,0,0,0,1,0)	t_1t_5	144
(ab)(cdef)	(0,1,0,1,0,0)	t_2t_4	90
(a)(b)(c)(d)(ef)	(4,1,0,0,0,0)	$t_1^4t_2$	15
(a)(bc)(def)	(1,1,1,0,0,0)	$t_1t_2t_3$	120
(ab)(cd)(ef)	(0,3,0,0,0,0)	t_2^3	15
(a)(b)(cdef)	(2,0,0,1,0,0)	$t_1^2t_4$	90
(abcdef)	(0,0,0,0,0,1)	t_6	120
	TOTAL		$720 = \lvert S_6\rvert$

Thus;

$$
\begin{aligned}
Z_{(G,X)} &= \frac{1}{720}\{t_1^6 + 45t_1^2t_2^2 + 40t_1^3t_3 + 40t_3^2 + 144t_1t_5 + 90t_2t_4 + 15t_1^4t_2 \\
&\quad +120t_1t_2t_3 + 15t_2^3 + 90t_1^2t_4 + 120t_6\}, \\
Z_{(N,X)} &= \frac{1}{360}\{t_1^6 + 45t_1^2t_2^2 + 40t_1^3t_3 + 40t_3^2 + 144t_1t_5 + 90t_2t_4\} \textit{ and} \\
Z_{(H,X)} &= \frac{1}{2}\{t_1^6 + t_1^4t_2\}.
\end{aligned}
$$

Thus, $Z_{(G,X)}$ can be rewritten as;

$$
\begin{aligned}
Z_{(G,X)} &= \frac{1}{720}\{t_1^6 + 45t_1^2t_2^2 + 40t_1^3t_3 + 40t_3^2 + 144t_1t_5 + 90t_2t_4\} \\
&\quad + \frac{1}{720}\{15t_1^4t_2 + 120t_1t_2t_3 + 15t_2^3 + 90t_1^2t_4 + 120t_6\} \\
&= \frac{1}{2}\frac{1}{360}\{t_1^6 + 45t_1^2t_2^2 + 40t_1^3t_3 + 40t_3^2 + 144t_1t_5 + 90t_2t_4\} + \frac{1}{24}\frac{1}{2}\{t_1^6 + t_1^4t_2\} \\
&\quad - \frac{1}{48}t_1^6 + \frac{1}{720}\{120t_1t_2t_3 + 15t_2^3 + 90t_1^2t_4 + 120t_6\} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{24}Z_{(H,X)} - \frac{1}{48}Z_{(1,X)} + \frac{1}{6!}\{120t_1t_2t_3 + 15t_2^3 + 90t_1^2t_4 + 120t_6\} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{(6-2)!}Z_{(H,X)} - \frac{1}{2(6-2)!}Z_{(1,X)} + \frac{1}{6!}\{120t_1t_2t_3 + 15t_2^3 + 90t_1^2t_4 \\
&\quad +120t_6\} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{(n-2)!}Z_{(H,X)} - \frac{1}{2\,(n-2)!}Z_{(1,X)} \\
&\quad + \frac{1}{n!}\{120t_1t_2t_3 + 15t_2^3 + 90t_1^2t_4 + 120t_6\}, \textit{ where } n = 6.
\end{aligned}
$$

In this case, the extra $\frac{1}{6!}\{120t_1t_2t_3 + 15t_2^3 + 90t_1^2t_4 + 120t_6\}$ is the contribution, to $Z_{(G,X)}$ of the 345 odd permutations of X that are not transpositions. These permutations are not in a conjugate of H and form four conjugacy classes.

4.3.5 Cycle index of S_7

Suppose $X = \{1, 2, 3, 4, 5, 6, 7\}$ so that $n = 7$, $G = S_7$, $N = A_7$ and $H = \langle(12)\rangle$.

Table 4.3: Cycle Types of Elements of S_7

Permutation Type	*Cycle Type*	*Corresponding Monomial*	*Corresponding No. of Elements in* S_7
(a)(b)(c)(d)(e)(f)(g)	(7,0,0,0,0,0,0)	t_1^7	1
(a)(b)(c)(de)(fg)	(3,2,0,0,0,0,0)	$t_1^3t_2^2$	105
(a)(b)(c)(d)(efg)	(4,0,1,0,0,0,0)	$t_1^4t_3$	70
(ab)(cd)(efg)	(0,2,1,0,0,0,0)	$t_2^2t_3$	210
(a)(bcd)(efg)	(1,0,2,0,0,0,0)	$t_1t_3^2$	280
(a)(bc)(defg)	(1,1,0,1,0,0,0)	$t_1t_2t_4$	630
(a)(b)(cdefg)	(2,0,0,0,1,0,0)	$t_1^2t_5$	504
(abcdefg)	(0,0,0,0,0,0,1)	t_7	720
(a)(b)(c)(d)(e)(fg)	(5,1,0,0,0,0,0)	$t_1^5t_2$	21
(a)(bc)(de)(fg)	(1,3,0,0,0,0,0)	$t_1t_2^3$	105
(a)(b)(cd)(efg)	(2,1,1,0,0,0,0)	$t_1^2t_2t_3$	420
(a)(b)(c)(defg)	(3,0,0,1,0,0,0)	$t_1^3t_4$	210
(abc)(defg)	(0,0,1,1,0,0,0)	t_3t_4	420
(ab)(cdefg)	(0,1,0,0,1,0,0)	t_2t_5	504
(a)(bcdefg)	(1,0,0,0,0,1,0)	t_1t_6	840
TOTAL			$5040 = \lvert S_7\rvert$

Thus;

$$
\begin{aligned}
Z_(G,X) &= \frac{1}{5040}\{t_1^7 + 105t_1^3t_2^2 + 70t_1^4t_3 + 210t_2^2t_3 + 280t_1t_3^2 + 630t_1t_2t_4 + 504t_1^2t_5 \\
&\quad +720t_7 + 21t_1^5t_2 + 105t_1t_2^3 + 420t_1^2t_2t_3 + 210t_1^3t_4 + 420t_3t_4 + 504t_2t_5 \\
&\quad +840t_1t_6\}, \\
Z_{(N,X)} &= \frac{1}{2520}\{t_1^7 + 105t_1^3t_2^2 + 70t_1^4t_3 + 210t_2^2t_3 + 280t_1t_3^2 + 630t_1t_2t_4 + 504t_1^2t_5 \\
&\quad +720t_7\}
\end{aligned}
$$

and

$$
Z_{(H,X)} = \frac{1}{2}\{t_1^7 + t_1^5t_2\}.
$$

Thus, $Z_{(G,X)}$ can be written as;

$$
\begin{aligned}
Z_{(G,X)} &= \frac{1}{5040}\{t_1^7 + 105t_1^3t_2^2 + 70t_1^4t_3 + 210t_2^2t_3 + 280t_1t_3^2 + 630t_1t_2t_4 + 504t_1^2t_5 \\
&\quad +720t_7\} + \frac{1}{5040}\{21t_1^5t_2 + 105t_1t_2^3 + 420t_1^2t_2t_3 + 210t_1^3t_4 + 420t_3t_4 \\
&\quad +504t_2t_5 + 840t_1t_6\} \\
&= \frac{1}{2}\frac{1}{2520}\{t_1^7 + 105t_1^3t_2^2 + 70t_1^4t_3 + 210t_2^2t_3 + 280t_1t_3^2 + 630t_1t_2t_4 + 504t_1^2t_5 \\
&\quad +720t_7\} + \frac{1}{120}\frac{1}{2}\{t_1^7 + t_1^5t_2\} - \frac{1}{240}t_1^7 \\
&\quad +\frac{1}{5040}\{105t_1t_2^3 + 420t_1^2t_2t_3 + 210t_1^3t_4 + 420t_3t_4 + 504t_2t_5 + 840t_1t_6\} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{120}Z_{(H,X)} - \frac{1}{240}Z_{(1,X)} \\
&\quad +\frac{1}{7!}\{105t_1t_2^3 + 420t_1^2t_2t_3 + 210t_1^3t_4 + 420t_3t_4 + 504t_2t_5 + 840t_1t_6\}
\end{aligned}
$$

$$\begin{aligned} &= \frac{1}{2}Z_{(N,X)} + \frac{1}{(7-2)!}Z_{(H,X)} - \frac{1}{2(7-2)!}Z_{(1,X)} \\ &\quad + \frac{1}{7!}\{105t_1t_2^3 + 420t_1^2t_2t_3 + 210t_1^3t_4 + 420t_3t_4 + 504t_2t_5 + 840t_1t_6\} \\ &= \frac{1}{2}Z_{(N,X)} + \frac{1}{(n-2)!}Z_{(H,X)} - \frac{1}{2(n-2)!}Z_{(1,X)} \\ &\quad + \frac{1}{n!}\{105t_1t_2^3 + 420t_1^2t_2t_3 + 210t_1^3t_4 + 420t_3t_4 + 504t_2t_5 + 840t_1t_6\}, \end{aligned}$$

where $n = 7$.

In this case, the extra term $\frac{1}{7!}\{105t_1t_2^3 + 420t_1^2t_2t_3 + 210t_1^3t_4 + 420t_3t_4 + 504t_2t_5 + 840t_1t_6\}$ is the contribution to $Z_{(G,X)}$ of the 2,499 odd permutations of X that are not transpositions. These permutations are not in a conjugate of H and form some six conjugacy classes.

4.3.6 Cycle index of S_8

Suppose $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ so that $n = 8$, $G = S_8$, $N = A_8$ and $H = \langle(12)\rangle$.

Table 4.4: Cycle Types of Elements of S_8

Permutation Type	*Cycle Type*	*Corresponding Monomial*	*Corresponding No. of Elements in* S_8
(a)(b)(c)(d)(e)(f)(g)(h)	(8,0,0,0,0,0,0,0)	t_1^8	1
(a)(b)(c)(d)(e)(f)(hg)	(6,1,0,0,0,0,0,0)	$t_1^6t_2$	28
(a)(b)(c)(d)(e)(fgh)	(5,0,1,0,0,0,0,0)	$t_1^5t_3$	112
(a)(b)(c)(d)(efgh)	(4,0,0,1,0,0,0,0)	$t_1^4t_4$	420
(a)(b)(c)(d)(ef)(gh)	(1,2,0,0,0,0,0,0)	$t_1^4t_2^2$	210
(a)(b)(c)(defgh)	(3,0,0,0,1,0,0,0)	$t_1^3t_5$	1344
(a)(b)(c)(de)(fgh)	(3,1,1,0,0,0,0,0)	$t_1^3t_2t_3$	1120
(a)(b)(cdefgh)	(2,0,0,0,0,1,0,0)	$t_1^2t_6$	3360
(a)(b)(cd)(efgh)	(2,1,0,1,0,0,0,0)	$t_1^2t_2t_4$	2520
(a)(b)(cd)(ef)(gh)	(2,3,0,0,0,0,0,0)	$t_1^2t_2^3$	420
(a)(b)(cde)(fgh)	(2,0,2,0,0,0,0,0)	$t_1^2t_3^2$	1120
(a)(bcdefgh)	(1,0,0,0,0,0,1,0)	t_1t_7	5760
(a)(bc)(de)(fgh)	(1,2,1,0,0,0,0,0)	$t_1t_2^2t_3$	1680
(a)(bcd)(efgh)	(1,0,1,1,0,0,0,0)	$t_1t_3t_4$	3360
(a)(bc)(defgh)	(1,1,0,0,1,0,0,0)	$t_1t_2t_5$	4032
(ab)(cd)(ef)(gh)	(0,4,0,0,0,0,0,0)	t_2^4	105
(ab)(cd)(efgh)	(0,2,0,1,0,0,0,0)	$t_2^2t_4$	1260
(ab)(cde)(fgh)	(0,1,2,0,0,0,0,0)	$t_2t_3^2$	1120
(ab)(cdefgh)	(0,1,0,0,0,1,0,0)	t_2t_6	3360
(abc)(defgh)	(0,0,1,0,1,0,0,0)	t_3t_5	2688
(abcd)(efgh)	(0,0,0,2,0,0,0,0)	t_4^2	1260
(abcdefgh)	(0,0,0,0,0,0,0,1)	t_8	5040
	TOTAL		$40320 = \lvert S_8\rvert$

Thus;

$$
\begin{aligned}
Z_{(G,X)} &= \frac{1}{40320}\{t_1^8 + 28t_1^6t_2 + 112t_1^5t_3 + 420t_1^4t_4 + 210t_1^4t_2^2 + 1344t_1^3t_5 + 1120t_1^3t_2t_3 \\
&+3360t_1^2t_6 + 2520t_1^2t_2t_4 + 420t_1^2t_2^3 + 1120t_1^2t_3^2 + 5760t_1t_7 + 1680t_1t_2^2t_3 \\
&+3360t_1t_3t_4 + 4032t_1t_2t_5 + 105t_2^4 + 1260t_2^2t_4 + 1120t_2t_3^2 + 3360t_2t_6 \\
&+2688t_3t_5 + 1260t_4^2 + 5040t_8\}, \\
Z_{(N,X)} &= \frac{1}{20160}\{t_1^8 + 112t_1^5t_3 + 210t_1^4t_2^2 + 1344t_1^3t_5 + 2520t_1^2t_2t_4 + 1120t_1^2t_3^2 \\
&+5760t_1t_7 + 1680t_1t_2^2t_3 + 105t_2^4 + 3360t_2t_6 + 2688t_3t_5 + 1260t_4^2\} \textit{ and} \\
Z_{(H,X)} &= \frac{1}{2}\{t_1^8 + t_1^6t_2\}.
\end{aligned}
$$

Thus, $Z_{(G,X)}$ can be written as;

$$
\begin{aligned}
Z_{(G,X)} &= \frac{1}{40320}\{t_1^8 + 112t_1^5t_3 + 210t_1^4t_2^2 + 1344t_1^3t_5 + 2520t_1^2t_2t_4 + 1120t_1^2t_3^2 + 5760t_1t_7 \\
&+1680t_1t_2^2t_3 + 105t_2^4 + 3360t_2t_6 + 2688t_3t_5 + 1260t_4^2\} \\
&+\frac{1}{40320}\{28t_1^6t_2 + 420t_1^4t_4 + 1120t_1^3t_2t_3 + 3360t_1^2t_6 + 420t_1^2t_2^3 + 3360t_1t_3t_4 \\
&+4032t_1t_2t_5 + 1260t_2^2t_4 + 1120t_2t_3^2 + 5040t_8\} \\
&= \frac{1}{2}\frac{1}{20160}\{t_1^8 + 112t_1^5t_3 + 210t_1^4t_2^2 + 1344t_1^3t_5 + 2520t_1^2t_2t_4 + 1120t_1^2t_3^2 + 5760t_1t_7 \\
&+1680t_1t_2^2t_3 + 105t_2^4 + 3360t_2t_6 + 2688t_3t_5 + 1260t_4^2\} + \frac{1}{720}\frac{1}{2}\{t_1^8 + 28t_1^6t_2\} \\
&-\frac{1}{1440}t_1^8 + \frac{1}{40320}\{420t_1^4t_4 + 1120t_1^3t_2t_3 + 3360t_1^2t_6 + 420t_1^2t_2^3 + 3360t_1t_3t_4 \\
&+4032t_1t_2t_5 + 1260t_2^2t_4 + 1120t_2t_3^2 + 5040t_8\} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{720}Z_{(H,X)} - \frac{1}{1440}Z_{(1,X)} + \frac{1}{8!}\{420t_1^4t_4 + 1120t_1^3t_2t_3 + 3360t_1^2t_6 \\
&+420t_1^2t_2^3 + 3360t_1t_3t_4 + 4032t_1t_2t_5 + 1260t_2^2t_4 + 1120t_2t_3^2 + 5040t_8\}
\end{aligned}
$$

$$= \frac{1}{2}Z_{(N,X)} + \frac{1}{(8-2)!}Z_{(H,X)} - \frac{1}{2(8-2)!}Z_{(1,X)}$$
$$+\frac{1}{8!}\{420t_1^4t_4 + 1120t_1^3t_2t_3 + 3360t_1^2t_6 + 420t_1^2t_2^3 + 3360t_1t_3t_4 + 4032t_1t_2t_5$$
$$+1260t_2^2t_4 + 1120t_2t_3^2 + 5040t_8\}$$
$$= \frac{1}{2}Z_{(N,X)} + \frac{1}{(n-2)!}Z_{(H,X)} - \frac{1}{2(n-2)!}Z_{(1,X)} + \frac{1}{n!}\{420t_1^4t_4 + 1120t_1^3t_2t_3$$
$$+3360t_1^2t_6 + 420t_1^2t_2^3 + 3360t_1t_3t_4 + 4032t_1t_2t_5 + 1260t_2^2t_4$$
$$+1120t_2t_3^2 + 5040t_8\},\ where\ n = 8.$$

In this case, the extra term $\frac{1}{8!}\{420t_1^4t_4 + 1120t_1^3t_2t_3 + 3360t_1^2t_6 + 420t_1^2t_2^3 + 3360t_1t_3t_4 + 4032t_1t_2t_5 + 1260t_2^2t_4 + 1120t_2t_3^2 + 5040t_8\}$ is the contribution, to $Z_{(G,X)}$ of the 20,132 odd permutations of X that are not transpositions. These permutations are not in a conjugate of H and form some nine conjugacy classes.

4.4 Cycle index of S_n

In this section we generalize the formulas obtained in Section 4.3 to obtain the cycle index formula of S_n in terms of the cycle index formulas of A_n and C_2.

Theorem 4.4.1.

Let $X = \{1, 2, \ldots, n\}$ so that $G = S_n$, $N = A_n$ and $H = \langle(12)\rangle$. Then,

$$Z_{(G,X)} = \frac{1}{2}Z_{(N,X)} + \frac{1}{(n-2)!}Z_{(H,X)} - \frac{1}{(n-2)!}Z_{(1,X)} + \frac{1}{n!}\{k\},$$

where k is the sum of monomials of the odd permutations that are not transpositions.

Proof.

The cycle type of the identity permutation, which is even, is $(n, 0, 0 \ldots, 0)$ while that of a transposition (ab), which is odd, is $(n-2,1,0,0,\ldots,0)$. So $mon\,(e) = t_1^n$ and $mon(ab) = t_1^{n-2}t_2$. Now, if p is the sum of monomials of the non-trivial even permutations of X, then by definition, $Z_{(N,X)} = \frac{2}{n!}\{t_1^n + p\}$.

Also, $Z_{(H,X)} = \frac{1}{2}\{t_1^n + t_1^{n-2}t_2\}$. The conjugacy class of (ab) has $\frac{n!}{(n-2)!1^{n-2}1!2^1} = \frac{n!}{2(n-2)!}$ elements. Finally, suppose k is the sum of the monomials of odd permutations of X that are not transpositions.

Then,

$$
\begin{aligned}
Z_{(G,X)} &= \frac{1}{n!}\sum_{g\in G}\{mon\,(g)\} \\
&= \frac{1}{n!}\sum_{g\in N}\{mon\,(g)\} + \frac{1}{n!}\sum_{g\notin N}\{mon\,(g)\} \\
&= \frac{1}{n!}\{t_1^n + p\} + \frac{1}{n!}\left(\frac{n!}{2\,(n-2)!}t_1^{n-2}t_2 + k\right) \\
&= \frac{1}{2}\left(\frac{2}{n!}\{t_1^n + p\}\right) + \frac{1}{2\,(n-2)!}\;t_1^{n-2}t_2 + \frac{1}{n!}\{k\} \\
&= \frac{1}{2}\left(\frac{2}{n!}\{t_1^n + p\}\right) + \frac{1}{(n-2)!}\left(\frac{1}{2}\{t_1^n + t_1^{n-2}t_2\}\right) - \frac{1}{2\,(n-2)!}t_1^n + \frac{1}{n!}\{k\} \\
&= \frac{1}{2}Z_{(N,X)} + \frac{1}{(n-2)!}Z_{(H,X)} - \frac{1}{2\,(n-2)!}Z_{(1,X)} + \frac{1}{n!}\;k\,.
\end{aligned}
$$

In this case note that the cycle index of S_n cannot be expressed fully in terms of the cycle index of $N = A_n$ and $H = \langle(12)\rangle$ since we have some odd permutation of X that are not transpositions which do not belong to either of the subgroups. □

CHAPTER 5

THE CYCLE INDEX OF THE AFFINE(q) GROUP AS A SEMIDIRECT PRODUCT OF THE ELEMENTARY ABELIAN GROUP P_q BY THE CYCLIC GROUP C_{q-1}

5.1 Introduction

In this chapter we derive the cycle index formula of the affine(p) group and express it in terms of the cycle index formulas of the cyclic groups C_p and C_{p-1}. Similarly, if $q = p^r$ the affine(q) group can be written as $Aff(q) = P_q \rtimes C_{q-1}$ since the affine(q) group is a semidirect product of the two subgroups. We also derive the cycle index of the affine(q) group and express it in terms of the cycle index of the elementary abelian group P_q and the cyclic subgroup C_{q-1}.

This chapter has four sections. In Section 5.1 we give an introduction while in Section 5.2 we show that the affine(q) group is a semidirect product of the elementary abelian group P_q and the cyclic subgroup C_{q-1}. In Section 5.3 we derive the cycle index of the affine(p) group and express it in terms of the cycle indices of the cyclic groups C_p and C_{p-1} while in Section 5.4 we derive the cycle index of the affine(q) group and express it in terms of the cycle indices of the elementary abelian group P_q and the cyclic group C_{q-1}.

5.2 The affine(q) group as a semidirect product group

Theorem 5.2.1.

The affine(q) group is a semidirect product group of the elementary abelian group P_q and the cyclic group C_{q-1}.

Proof.

Let $N = P_q \lhd Aff(q)$ and $H = C_{q-1} < Aff(q)$.

Clearly, $N \cap H = \{e\}$, where e is the identity element in $Aff(q)$.

Since $|NH| = \frac{|N||H|}{|N \cap H|} = \frac{q(q-1)}{1} = q(q-1) = |Aff(q)|$,

we deduce that, $Aff(q) = NH = N \rtimes H \cong P_q \rtimes C_{q-1}$. □

5.3 The cycle index of the affine(p) group

Lemma 5.3.1.

Let $g \in Aff(q)$ be such that g fixes only one element in $GF(q)$, then $C_G(g) = C_{q-1}$.

Proof.

Since the Affine(q) group acts transitively on $GF(q)$ (Kangogo, 2015), then the stabilizers of each of the elements in $GF(q)$ are conjugate and only intersect at the identity so it is enough to find the centralizer of any one element. The elements of $Aff(q)$ which fix $0 \in GF(q)$ are of the form $\alpha x + 0$ where $\alpha \in GF(q)$. This can be written as; $M = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$.

A general element of $Aff(q)$ is of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ such that $a \neq 0$ and

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}.$$

Now $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & -\alpha b + b \\ 0 & 1 \end{pmatrix}$.

For the element $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ to centralize $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ then, $-\alpha b + b = 0$, implying $b(1-\alpha) = 0 \Rightarrow b = 0$ or $\alpha = 1$.

If $\alpha = 1$, then $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ is the identity which is centralized by every element of the group and so the centralizers of $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ are of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ where $0 \neq a \in GF(q)$ thus the centralizer has order $q-1$ which is a cyclic multiplicative group C_{q-1} of order $q-1$. □

Lemma 5.3.2.

Let $g \in Aff(q)$ be such that g does not fix any element in $GF(q)$, then $C_G(g) = P_q$.

Proof.

Since the Affine(q) group acts transitively on $GF(q)$ (Kangogo, 2015), then the stabilizers of each of the elements in $GF(q)$ are conjugate and only intersect at the identity so it is enough to find the centralizer of any one element. The elements of $Aff(q)$ which do not fix any element of $GF(q)$ are of the form $x + \alpha$ where $\alpha \in GF(q)$. This can be written as; $M = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$.

A general element of $Aff(q)$ is of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ such that $a \neq 0$ and

$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}$.

Now $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha a \\ 0 & 1 \end{pmatrix}$.

For the element $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ to centralize $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ then, $\alpha a = \alpha$, implying $\alpha(a-1) = 0 \Rightarrow \alpha = 0$ or $a = 1$.

If $\alpha = 0$, then $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ is the identity which is centralized by every element of the group and so the centralizers of $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ are of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ where $b \in GF(q)$ thus the centralizer has order q which is the elementary abelian group P_q. □

Theorem 5.3.1.

Let p be a prime, the cycle index formula of the affine(p) group G acting on the p elements of $\mathbb{Z}_p$ is given by;

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^p + (p-1)\, t_p + p \sum_{1 \neq d | (p-1)} \phi(d) t_1 t_d^{\frac{p-1}{d}} \right)$$

where $|G| = p\,(p-1)$, $\phi(d)$ is the Euler's phi function and X the p elements of the field $\mathbb{Z}_p$.

Proof.

The elements of the $Aff(p)$ group are partitioned into I (the identity element), τ_1 (the set of elements that fix one element on the field $\mathbb{Z}_p$) and τ_0 (the set of elements that do not fix any element of $\mathbb{Z}_p$). To derive the cycle index formula we need to find the number of τ_0 and τ_1 elements and the respective cycle types.

Let $g \in \tau_1$, then by Lemma 5.3.1 $C_G(g) = C_{p-1}$ and by Theorem 1.6.6;

$$|C^g| = \frac{p(p-1)}{(p-1)} = p, \tag{5.1}$$

where C^g is the conjugacy class in G containing g.

Let $g \in \tau_0$, then by Lemma 5.3.2 $C_G(g) = C_p$ and by Theorem 1.6.6;

$$\Rightarrow |C^g| = \frac{p(p-1)}{p} = p - 1. \tag{5.2}$$

$N_G(C_{p-1}) = C_{p-1}$, implying there are $\frac{p(p-1)}{(p-1)} = p$ conjugate cyclic groups C_{p-1} in G. These cyclic groups intersect only at the identity thus,

$$|\tau_1| = (p-2)\,p. \tag{5.3}$$

We find the number of elements in τ_0 by subtracting the number of elements τ_1 and the identity from the order of G.

We have,

$|\tau_0| = [p\,(p-1) - (p-2)\,p - 1] = p - 1 = |C^g|$ by Equation 5.2 implying that all the elements in τ_0 are conjugate in G and are of order p.

Therefore;

$$Z_{(G,X)} = \frac{1}{|G|}(t_1^p + (p-1)\,.monomial\ of\ an\ element\ in\ \tau_0$$
$$+p(sumation\ of\ all\ monomials\ of\ the\ nontrivial\ elements\ in\ cyclic$$
$$subgroups\ C_{p-1}))$$

That is,

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^p + (p-1)\,.mon(x) + p\sum_{g\in C_{p-1}\setminus\{I\}} mon(g)\right), \tag{5.4}$$

where $x \in \tau_0$.

Let $x \in \tau_0$. Then $\pi(x) = 0$.

It follows from Theorem 1.6.5 that, $\pi(x^p) = p$ and if $l < p$, $\pi\left(x^l\right) = 0$.

Now if $0 < l < p$ then,

$$\begin{aligned}
\alpha_l &= \frac{1}{l}\sum_{i|l}\pi\left(x^{\frac{l}{i}}\right)\mu(i) \\
&= \frac{1}{l}\sum_{i|l}0\mu(i) = 0 \text{ and} \\
\alpha_p &= \frac{1}{p}\sum_{i|p}\pi\left(x^{\frac{p}{i}}\right)\mu(i) \\
&= \frac{1}{p}\left[\pi(x^p) - \pi(x)\right] \\
&= \frac{1}{p}\left[p - 0\right] = \frac{p}{p} = 1
\end{aligned}$$

The resulting monomial is;

$$t_p. \tag{5.5}$$

If $g \in \tau_1$ and l <d where d is the order of g, then

$$\pi(g) = 1, \pi\left(g^d\right) = p \; and \; \pi\left(g^l\right) = 1$$

$$\begin{aligned}
\alpha_l &= \frac{1}{l}\sum_{i|l} \pi\left(g^{\frac{l}{i}}\right)\mu(i) \\
&= \frac{1}{l}\sum_{i|l} (1)\mu(i) \\
&= \frac{1}{l}\sum_{i|l} \mu(i) = 0 \\
\alpha_d &= \frac{1}{d}\sum_{i|d} \pi\left(g^{\frac{d}{i}}\right)\mu(i) \\
&= \frac{1}{d}\left[\pi\left(g^d\right)\mu(1) + \sum_{1\neq i|d} \pi\left(g^{\frac{d}{i}}\right)\mu(i)\right] \\
&= \frac{1}{d}\left[\pi\left(g^d\right) + \sum_{i|d} \mu(i) - \pi(g)\right] \\
&= \frac{1}{d}[p-1] = \frac{p-1}{d}.
\end{aligned}$$

Thus the resulting monomial is;

$$t_1 t_d^{\frac{p-1}{d}} \tag{5.6}$$

Substituting for $mon(x)$ (in 5.5) and $mon(g)$ (in 5.6) in Equation 5.4 we get;

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^p + (p-1)\,t_p + p\sum_{1\neq d|(p-1)} \phi(d) t_1 t_d^{\frac{p-1}{d}}\right)$$

.

□

Example 5.3.1

Let $p = 17$, $|G| = 272$

Therefore, possible values of d are; 2, 4, 8 and 16.

$\phi(2) = 1$, $\phi(4) = 2$, $\phi(8) = 4$, and $\phi(16) = 8$

By Theorem 5.3.1, we have;

$$Z_{(G,X)} = \frac{1}{272}\left(t_1^{17} + 16t_{17} + 17t_1t_2^8 + 34t_1t_4^4 + 68t_1t_8^2 + 136t_1t_{16}\right).$$

5.3.1 Expressing the cycle index of the Affine(p) group in terms of the cycle indices of the cyclic groups C_p and C_{p-1}

The equation in Theorem 5.3.1 can be simplified as;

$$\begin{aligned} Z_{(G,X)} &= \frac{1}{p\,(p-1)}\left(t_1^p + (p-1)\,t_p\right) + \frac{1}{p\,(p-1)}\left(pt_1^p + p\sum_{1\neq d|(p-1)} \phi(d)t_1t_d^{\frac{p-1}{d}}\right) - \frac{1}{(p-1)}t_1^p \\ &= \frac{1}{(p-1)}Z_{(C_p,X)} + \frac{1}{(p-1)}\left(t_1^p + \sum_{1\neq d|(p-1)} \phi(d)t_1t_d^{\frac{p-1}{d}}\right) - \frac{1}{(p-1)}t_1^p \\ &= \frac{1}{(p-1)}Z_{(C_p,X)} + Z_{(C_{p-1},X)} - \frac{1}{(p-1)}t_1^p \\ &= \frac{1}{|C_{p-1}|}Z_{(C_p,X)} + Z_{(C_{p-1},X)} - \frac{1}{|C_{p-1}|}Z_{(1,X)}. \end{aligned} \tag{5.7}$$

Example 5.3.2

Let $p = 11$, then $G\ is\ Aff(11)$ and $X = \{0,1,2,3,4,5,6,7,8,9,10\}$.

Then the cycle index of G acting on X is;

$Z_{(G,X)} = \frac{1}{110}\left(t_1^{11} + 10t_{11} + 11\sum_{1\neq d|10} \phi(d)t_1t_d^{\frac{10}{d}}\right)$ (from Theorem 5.3.1),

which can be simplified as;

$$\begin{aligned} Z_{(G,X)} &= \frac{1}{11\,(10)}\left(t_1^{11} + 10t_{11}\right) + \frac{1}{11\,(10)}\left(11t_1^{11} + 11\sum_{1\neq d|10} \phi(d)t_1t_d^{\frac{10}{d}}\right) - \frac{1}{10}t_1^{11} \\ &= \frac{1}{10}Z_{(C_{11},X)} + Z_{(C_{10},X)} - \frac{1}{10}t_1^{11} \\ &= \frac{1}{10}Z_{(C_{11},X)} + Z_{(C_{10},X)} - \frac{1}{10}Z_{(1,X)}\ (from\ Equation\ 5.7). \end{aligned}$$

5.4 The cycle index of the affine(q) group

Theorem 5.4.1.

Let p be a prime and $q = p^r$. The cycle index formula of the affine(q) group G acting on the q elements of $GF(q)$ is given by;

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^q + (q-1)\,t_p^{\frac{q}{p}} + q\sum_{1\neq d|(q-1)} \phi(d) t_1 t_d^{\frac{q-1}{d}}\right),$$

where $|G| = q\,(q-1)$, $\phi(d)$ is the Euler's phi function and X the q elements of the $GF\,(q)$.

Proof.

The elements of the $Aff(q)$ group are partitioned into $I,\ \tau_1$ (the set of elements that fix one element in the field $GF(q)$ and τ_0 (the set of elements that do not fix any element of $GF(q)$). To derive the cycle index formula we need to find the number of τ_0 and τ_1 elements and the respective cycle types.

Let $g \in \tau_1$, then from Lemma 5.3.1 $C_G(g) = C_{q-1}$ and by Theorem 1.6.6;

$$\Rightarrow |C^g| = \frac{q(q-1)}{(q-1)} = q, \tag{5.8}$$

where C^g is the conjugacy class in G containing g.

Let $g \in \tau_0$, then from Lemma 5.3.2 $C_G(g) = P_q$ and by Theorem 1.6.6;

$$\Rightarrow |C^g| = \frac{q(q-1)}{q} = q - 1 \tag{5.9}$$

$N_G(C_{q-1}) = C_{q-1}$, implying there are $\frac{q(q-1)}{(q-1)} = q$ conjugate cyclic groups C_{q-1} in G.

These cyclic groups intersect only at the identity thus;

$$|\tau_1| = (q-2)\,q. \tag{5.10}$$

We find the number of τ_0 elements by subtracting the number of τ_1 elements and the identity from the order of G.

We have,

$|\tau_0| = [q(q-1) - (q-2)\,q - 1] = q - 1 = |C^g|$ by 5.9. Implying all elements in τ_0 are conjugate in G and are of order p.

Therefore;

$$\begin{aligned} Z_{(G,X)} &= \frac{1}{|G|}(t_1^q + (q-1).monomial\ of\ an\ element\ in\ \tau_0 \\ &\quad +q(sumation\ of\ all\ monomials\ of\ the\ nontrivial\ elements\ in\ cyclic \\ &\quad subgroups\ C_{q-1})) \end{aligned}$$

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^q + (q-1)\,.mon(x) + q\sum_{g\in C_{q-1}\setminus\{I\}} mon(g)\right), \tag{5.11}$$

where $x \in \tau_0$

Let $x \in \tau_0$, then $\pi(x) = 0$.

It follows from Theorem 1.6.5 that $\pi(x^p) = q$ and

if $l < p$, $\pi\left(x^l\right) = 0$.

Now if $0 < l < p$ then,

$$\begin{aligned}
\alpha_l &= \frac{1}{l}\sum_{i|l}\pi\left(x^{\frac{l}{i}}\right)\mu(i) \\
&= \frac{1}{l}\sum_{i|l}0\mu(i) = 0 \\
\alpha_p &= \frac{1}{p}\sum_{i|p}\pi\left(x^{\frac{p}{i}}\right)\mu(i) \\
&= \frac{1}{p}\left[\pi(x^p) - \pi(x)\right] \\
&= \frac{1}{p}\left[q-0\right] = \frac{q}{p}
\end{aligned}$$

Therefore the resulting monomial is;

$$t_p^{\frac{q}{p}}. \tag{5.12}$$

$$If\ g \in \tau_1,\ then\ \pi(g) = 1, \pi\left(g^d\right) = q\ and \pi\left(g^l\right) = 1$$

$$when\ l < d$$

$$\begin{aligned}
\alpha_l &= \frac{1}{l}\sum_{i|l}\pi\left(g^{\frac{l}{i}}\right)\mu(i) \\
&= \frac{1}{l}\sum_{i|l}(1)\mu(i) \\
&= \frac{1}{l}\sum_{i|l}\mu(i) = 0
\end{aligned}$$

$$\begin{aligned}\alpha_d &= \frac{1}{d}\sum_{i|d}\pi\left(g^{\frac{d}{i}}\right)\mu\left(i\right)\\ &= \frac{1}{d}\left[\pi\left(g^{d}\right)\mu(1)+\sum_{1\neq i|d}\pi\left(g^{\frac{d}{i}}\right)\mu\left(i\right)-\pi\left(g\right)\right]\\ &= \frac{1}{d}\left[\pi\left(g^{d}\right)-\pi\left(g\right)\right]=\frac{1}{d}\left[q-1\right]=\frac{q-1}{d}\end{aligned}$$

Thus the resulting monomial is;

$$t_1 t_d^{\frac{q-1}{d}} \tag{5.13}$$

Substituting for $mon(x)$ (in 5.12) and $mon(g)$ (in 5.13) in Equation 5.11 we get;

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^q + (q-1)\,t_p^{\frac{q}{p}} + q\sum_{1\neq d|(q-1)}\phi(d)t_1 t_d^{\frac{q-1}{d}}\right).$$

□

Example 5.4.1

Let $p=3,\ r=3\ \Rightarrow q=3^3,\ X=GF(27)$ and $|G|=702$.

Possible values of d are; 2, 13 and 26. Therefore;

$\phi\,(2)=1$, $\phi\,(13)=12$ and $\phi\,(26)=12$.

By Theorem 5.4.1, we have;

$$Z_{(G,X)} = \frac{1}{702}\left(t_1^{27}+26t_3^9+27t_1t_2^{13}+324t_1t_{13}^2+324t_1t_{26}\right).$$

5.4.1 Expressing the cycle index formula of the affine(q) group in terms of the cycle indices of the elementary abelian group P_q and the cyclic group C_{q-1}

The equation in Theorem 5.4.1 can be simplified as;

$$
\begin{aligned}
Z_{(G,X)} &= \frac{1}{|G|}\left(t_1^q + (q-1)\,t_p^{\frac{q}{p}} + q\sum_{1\neq d|(q-1)}\phi(d)t_1t_d^{\frac{q-1}{d}}\right)\\
&= \frac{1}{q\,(q-1)}\left(t_1^q + (q-1)\,t_p^{\frac{q}{p}}\right) + \frac{1}{q\,(q-1)}\left(qt_1^q + q\sum_{1\neq d|(q-1)}\phi(d)t_1t_d^{\frac{q-1}{d}}\right)\\
&\quad -\frac{1}{(q-1)}t_1^q\\
&= \frac{1}{(q-1)}Z_{(P_q,X)} + \frac{1}{(q-1)}\left(t_1^q + \sum_{1\neq d|(q-1)}\phi(d)t_1t_d^{\frac{q-1}{d}}\right) - \frac{1}{(q-1)}t_1^q\\
&= \frac{1}{(q-1)}Z_{(P_q,X)} + Z_{(C_{q-1},X)} - \frac{1}{(q-1)}t_1^q\\
&= \frac{1}{|C_{q-1}|}Z_{(P_q,X)} + Z_{(C_{q-1},X)} - \frac{1}{|C_{q-1}|}Z_{(1,X)}. \qquad (5.14)
\end{aligned}
$$

Example 5.4.2

Let $p = 2,\ r = 3\ \Rightarrow q = 2^3,\ X = GF(8)$ and $|G| = 56$. Then the cycle index of G acting on X is;

$Z_{(G,X)} = \frac{1}{56}\left(t_1^8 + 7t_2^4 + 8\sum_{1\neq d|7}\phi(d)t_1t_d^{\frac{7}{d}}\right)$ (from Theorem 5.4.1,) which can be simplified as;

$$\begin{aligned} Z_{(G,X)} &= \frac{1}{8\,(7)}\left(t_1^8 + 7t_2^4\right) + \frac{1}{8\,(7)}\left(8t_1^8 + 8\sum_{1\neq d|7}\phi(d)t_1t_d^{\frac{7}{d}}\right) - \frac{1}{7}t_1^8 \\ &= \frac{1}{7}Z_{(P_8,X)} + Z_{(C_7,X)} - \frac{1}{7}t_1^8 \\ &= \frac{1}{7}Z_{(P_8,X)} + Z_{(C_7,X)} - \frac{1}{7}Z_{(1,X)}\ (\textit{from Equation}\ 5.14). \end{aligned}$$

CHAPTER 6

THE CYCLE INDEX OF THE AFFINE SQUARE(q) GROUP AS A SEMIDIRECT PRODUCT OF THE ELEMENTARY ABELIAN GROUP P_q AND THE CYCLIC GROUP $C_{\frac{q-1}{2}}$

6.1 Introduction

The set $P_q = \{x + b,\ where\ b \in GF(q)\}$ forms a normal subgroup of the affine(q) group and the set $C_{\frac{q-1}{2}} = \{ax,\ where\ a\ is\ a\ non\ zero\ square\ in\ GF(q)\}$ forms a cyclic subgroup of the affine(q) under multiplication. The semidirect product of the two groups P_q and $C_{\frac{q-1}{2}}$ forms a group known as the affine square(q) group denoted by $Aff_{\square}(q)$. The elements of $Aff_{\square}(q)$ are of the form $\{ax + b\ such\ that\ b \in GF(q)\ and\ a\ is\ a\ non\ zero\ square\ in\ GF(q)\}$. In this case, the affine square(q) group can be written as $Aff_{\square}(q) = P_q \rtimes C_{\frac{q-1}{2}}$ since it is a semidirect product of the two subgroups.

This chapter has four sections. In Section 6.1 we give an introduction while in Section 6.2 we show that the affine square(q) group is a semidirect product of the elementary abelian group P_q and the cyclic subgroup $C_{\frac{q-1}{2}}$. In Section 6.3 we derive the cycle index of the affine square(p) group and express it in terms of the cycle indices of the cyclic groups C_p and $C_{\frac{p-1}{2}}$ while in Section 6.4 we derive the cycle index of the affine square(q) group and express it in terms of the cycle indices of the elementary abelian group P_q and the cyclic group $C_{\frac{q-1}{2}}$. The proofs of these cycle indices will be similar to the proofs in chapter five.

6.2 The affine square(q) group as a semidirect product group

Theorem 6.2.1.

The affine square(q) group is a semidirect product group of the elementary abelian group P_q and the cyclic group $C_{\frac{q-1}{2}}$.

Proof.

Let $N = P_q \triangleleft Aff_{\square}(q)$ and $H = C_{\frac{q-1}{2}}$.

Clearly, $N \cap H = \{e\}$, where e is the identity element in $Aff_{\square}(q)$.

Since $|NH| = \frac{|N||H|}{|N \cap H|} = \frac{q(\frac{q-1}{2})}{1} = q(\frac{q-1}{2}) = |Aff_{\square}(q)|$,

we deduce that, $Aff_{\square}(q) = NH = N \rtimes H \cong P_q \rtimes C_{\frac{q-1}{2}}$ □

6.3 The cycle index of the affine square(p) group

Lemma 6.3.1.

Let $g \in Aff_{\square}(q)$ be such that g fixes only one element in $GF(q)$, then $C_G(g) = C_{\frac{q-1}{2}}$.

Proof.

Since the Affine square(q) group acts transitively on $GF(q)$ (Kangogo, 2015), then the stabilizers of each of the elements in $GF(q)$ are conjugate and only intersect at the identity so it is enough to find the centralizer of any one element. The elements of $Aff_{\square}(q)$ which fix $0 \in GF(q)$ are of the form $\alpha x + 0$ where $\alpha \in GF(q)$. This can be written as; $M = \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$.

A general element of $Aff_{\square}(q)$ is of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ such that a is a non zero square element of $GF(q)$ and $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}$.

Now $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & -\alpha b + b \\ 0 & 1 \end{pmatrix}$.

For the element $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ to centralize $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ then, $-\alpha b + b = 0$, implying $b(1-\alpha) = 0 \Rightarrow b = 0$ or $\alpha = 1$.

If $\alpha = 1$, then $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ is the identity which is centralized by every element of the group and so the centralizers of $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ are of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ where a is a non zero square element in $GF(q)$ thus the centralizer has order $\frac{(q-1)}{2}$ which is a cyclic multiplicative group $C_{\frac{(q-1)}{2}}$ of order $\frac{(q-1)}{2}$. □

Lemma 6.3.2.

Let $g \in Aff_{\square}(q)$ be such that g does not fix any element in $GF(q)$, then $C_G(g) = P_q$.

Proof.

Since the Affine square(q) group acts transitively on $GF(q)$, then the stabilizers of all elements in $GF(q)$ are conjugate and only intersect at the identity so it is enough to find the centralizers of any one element. The elements of $Aff_{\square}(q)$ which do not fix any element of $GF(q)$ are of the form $x + \alpha$ where $\alpha \in GF(q)$. This can be written as; $M = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$.

A general element of $Aff_{\square}(q)$ is of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ such that a is a non zero square element in $GF(q)$ and $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix}$.

Now $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha a \\ 0 & 1 \end{pmatrix}$.

For the element $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ to centralize $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ then, $\alpha a = \alpha$, implying $\alpha(a-1) = 0 \Rightarrow \alpha = 0$ or $a = 1$.

If $\alpha = 0$, then $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ is the identity which is centralized by every element of the group and so the centralizers of $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ are of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ where $b \in GF(q)$ thus the centralizer has order q which is the elementary abelian group P_q. $\square$

Theorem 6.3.1.

Let $p > 2$ be a prime, the cycle index formula of the affine square(p) group G acting on the p elements of $\mathbb{Z}_p$ is given by;

$$Z_{(G,X)} = \frac{1}{|G|} \left(t_1^p + (p-1)\, t_p + p \sum_{1 \neq d \mid \frac{p-1}{2}} \phi(d) t_1 t_d^{\frac{p-1}{d}} \right),$$

where $|G| = \frac{1}{2}p(p-1)$, $\phi(d)$ is the Euler's phi function and X the p elements of the filed $\mathbb{Z}_p$.

Proof.

The elements of the $Aff_{\square}(q)$ group are partitioned into I (the identity element), τ_1 (the set of elements that fix one element on the field $\mathbb{Z}_p$) and τ_0 (the set of elements that do not fix any element of $\mathbb{Z}_p$). To derive the cycle index formula we need to find the number of τ_0 and τ_1 elements and the respective cycle types.

Let $g \in \tau_1$. Then from Lemma 6.3.1 $C_G(g) = C_{\frac{p-1}{2}}$ and by Theorem 1.6.6;

$$\Rightarrow |C^g| = \frac{p\frac{p-1}{2}}{\frac{p-1}{2}} = p, \tag{6.1}$$

where C^g is the conjugacy class in G containing g.

Let $g \in \tau_0$. Then from Lemma 6.3.2 $C_G(g) = C_p$ and by Theorem 1.6.6;

$$\Rightarrow |C^g| = \frac{p\frac{p-1}{2}}{p} = \frac{p-1}{2}. \tag{6.2}$$

The subgroup $N_G\left(C_{\frac{p-1}{2}}\right) = C_{\frac{p-1}{2}}$, implying there are $\frac{\frac{1}{2}p(p-1)}{\frac{1}{2}(p-1)} = p$ conjugate cyclic groups $C_{\frac{p-1}{2}}$ in G.

These cyclic groups intersect only at the identity.

Thus;

$$|\tau_1| = \left(\frac{p-1}{2} - 1\right) p \tag{6.3}$$

We find the number of elements in τ_0 by subtracting the number of elements τ_1 and the identity from the order of G.

$$|\tau_0| = \left[p\left(\frac{p-1}{2}\right) - \left(\frac{p-1}{2} - 1\right)p - 1\right] = p - 1 \tag{6.4}$$

Therefore, since the length of a conjugacy class of $g \in \tau_0$ is $\frac{p-1}{2}$ from Equation 6.2 and the number of τ_0 elements is $p-1$ from 6.4, then there are two conjugacy classes of elements in τ_0 and each element in τ_0 is of order p.

Therefore;

$$\begin{aligned} Z_{(G,X)} \quad = \quad & \frac{1}{|G|}[t_1^p + \frac{p-1}{2}.mon(x_1) + \frac{p-1}{2}.mon(x_2) \\ & +p(\textit{summation of all monomials of the nontrivial elements in cyclic} \\ & \textit{subgroups } C_{\frac{p-1}{2}})], \end{aligned}$$

where x_1 and x_2 are representatives of elements in the first and the second conjugacy classes respectively. Since all τ_0 elements are of order p then they will have the same monomial and thus $Z_{(G,X)}$ can be written as;

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^p + (p-1).mon(x) + p\sum_{g \in C_{p-1}\backslash\{I\}} mon(g)\right) \tag{6.5}$$

where $x \in \tau_0$.

Let $x \in \tau_0$. Then $\pi\left(x\right) = 0$.

It follows by Theorem 1.6.5 that $\pi\left(x^p\right) = p$ and

if $l < p$, $\pi\left(x^l\right) = 0$.

Now if $0 < l < p$ then,

$$\begin{aligned}\alpha_l &= \frac{1}{l}\sum_{i|l}\pi\left(x^{\frac{l}{i}}\right)\mu(i)\\ &= \frac{1}{l}\sum_{i|l}0\mu(i) = 0\end{aligned}$$

and

$$\begin{aligned}\alpha_p &= \frac{1}{p}\sum_{i|p}\pi\left(x^{\frac{l}{i}}\right)\mu(i)\\ &= \frac{1}{p}\left[\pi\left(x^p\right) - \pi\left(x\right)\right]\\ &= \frac{1}{p}\left[p - 0\right] = \frac{p}{p} = 1\end{aligned}$$

The resulting monomial is;

$$t_p \tag{6.6}$$

If $g \in \tau_1$, then $\pi(g) = 1$, $\pi\left(g^d\right) = p$ where d is the order of g and

$\pi\left(g^l\right) = 1$

when $l < d$

$$\begin{aligned}\alpha_l &= \frac{1}{l}\sum_{i|l}\pi\left(g^{\frac{l}{i}}\right)\mu(i)\\ &= \frac{1}{l}\sum_{i|l}(1)\mu(i)\\ &= \frac{1}{l}\sum_{i|l}\mu(i) = 0\end{aligned}$$

$$
\begin{aligned}
\alpha_d &= \frac{1}{d}\sum_{i|d}\pi\left(g^{\frac{d}{i}}\right)\mu\left(i\right)\\
&= \frac{1}{d}\left[\pi\left(g^{d}\right)\mu(1)+\sum_{1\neq i|d}\pi\left(g^{\frac{d}{i}}\right)\mu\left(i\right)-\pi\left(g\right)\right]\\
&= \frac{1}{d}\left[\pi\left(g^{d}\right)-\pi\left(g\right)\right]\\
&= \frac{1}{d}\left[p-1\right]=\frac{p-1}{d}
\end{aligned}
$$

Thus the resulting monomial is;

$$t_1 t_d^{\frac{p-1}{d}} \tag{6.7}$$

Substituting for $mon(x)$ (in 6.6) and $mon(g)$ (in 6.7) in Equation 6.5 we get;

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^p + (p-1)\,t_p + p\sum_{1\neq d|\frac{p-1}{2}}\phi(d)t_1 t_d^{\frac{p-1}{d}}\right).$$

□

Example 6.3.1

Let $p = 13$, $|G| = 78$ where $G = Aff_{\square}(13)$.

Possible values of d are; $2,\ 3\ and\ 6$.

$\phi\left(2\right) = 1$, $\phi\left(3\right) = 2$ and $\phi\left(6\right) = 2$.

Substituting in Theorem 6.3.1 we have;

$$Z_{(Aff_{\square}(13),X)} = \frac{1}{78}\left(t_1^{13} + 12t_{13} + 13t_1t_2^6 + 26t_1t_3^4 + 26t_1t_6^2\right)$$

.

6.3.1 Expressing the cycle index of the Affine square(p) group in terms of the cycle index of the cyclic groups C_p and $C_{\frac{p-1}{2}}$

The equation in Theorem 6.3.1 can be simplified as;

$$\begin{aligned}
Z_{(G,X)} &= \frac{1}{|G|}\left(t_1^p + (p-1)\,t_p + p\sum_{1\neq d|\frac{p-1}{2}} \phi(d)t_1 t_d^{\frac{p-1}{d}}\right)\\
&= \frac{1}{\frac{1}{2}p(p-1)}\left[t_1^p + (p-1)\,t_p\right] + \frac{1}{\frac{1}{2}p(p-1)}\left(pt_1^p + p\sum_{1\neq d|\frac{p-1}{2}} \phi(d)t_1 t_d^{\frac{p-1}{d}}\right) - \frac{1}{\frac{p-1}{2}}t_1^p\\
&= \frac{1}{\frac{p-1}{2}}Z_{(C_p,X)} + \frac{1}{\frac{p-1}{2}}\left(t_1^p + \sum_{1\neq d|\frac{p-1}{2}} \phi(d)t_1 t_d^{\frac{p-1}{d}}\right) - \frac{1}{\frac{p-1}{2}}t_1^p\\
&= \frac{1}{\frac{p-1}{2}}Z_{(C_p,X)} + Z_{(C_{\frac{p-1}{2}},X)} - \frac{1}{\frac{p-1}{2}}t_1^p\\
&= \frac{1}{\left|C_{\frac{p-1}{2}}\right|}Z_{(C_p,X)} + Z_{(C_{\frac{p-1}{2}},X)} - \frac{1}{\left|C_{\frac{p-1}{2}}\right|}Z_{(1,X)}. \qquad (6.8)
\end{aligned}$$

Example 6.3.2

Let $p = 11$, then G is $Aff_{\Box}(11)$ and $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and

$Z_{(G,X)} = \frac{1}{55}\left(t_1^{11} + 10t_{11} + 11\sum_{1\neq d|5}\phi(d)t_1 t_d^{\frac{10}{d}}\right)$ (from Theorem 6.3.1)

This can be simplified as;

$$\begin{aligned}
Z_{(G,X)} &= \frac{1}{11\,(5)}\left(t_1^{11} + 10t_{11}\right) + \frac{1}{11\,(5)}\left(11t_1^{11} + 11\sum_{1\neq d|5}\phi(d)t_1 t_d^{\frac{10}{d}}\right) - \frac{1}{5}t_1^{11}\\
&= \frac{1}{5}Z_{(C_{11},X)} + Z_{(C_5,X)} - \frac{1}{10}t_1^{11}\\
&= \frac{1}{10}Z_{(C_{11},X)} + Z_{(C_{10},X)} - \frac{1}{5}Z_{(1,X)}\ (from\ Equation\ 6.8).
\end{aligned}$$

6.4 The cycle index of the affine square(q) group

Theorem 6.4.1.

Let $p > 2$ be a prime and $q = p^r$, the cycle index formula of the affine square(q) group G acting on the q elements of $GF(q)$ is given by;

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^q + (q-1)\, t_p^{\frac{q}{p}} + q \sum_{1 \neq d | \frac{q-1}{2}} \phi(d) t_1 t_d^{\frac{q-1}{d}} \right),$$

where $|G| = \frac{1}{2}q(q-1)$, $\phi(d)$ is the Euler's phi function and X the q elements of the $GF(q)$.

Proof.

The elements of the $Aff_{\square}(q)$ group are partitioned into I (the identity element), τ_1 (the set of elements that fix one element on the field $GF(q)$) and τ_0 (the set of elements that do not fix any element of $GF(q)$). To derive the cycle index formula we need to find the number of τ_0 and τ_1 elements and the respective cycle types.

Let $g \in \tau_1$. Then from Lemma 6.3.1 $C_G(g) = C_{\frac{q-1}{2}}$ and by Theorem 1.6.6;

$$\Rightarrow |C^g| = \frac{\frac{1}{2}q(q-1)}{\frac{1}{2}(q-1)} = q \tag{6.9}$$

where C^g is the conjugacy class in G containing g.

Let $g \in \tau_0$, then from Lemma 6.3.2 $C_G(g) = P_q$ and by Theorem 1.6.6;

$$\Rightarrow |C^g| = \frac{\frac{1}{2}q(q-1)}{q} = \frac{q-1}{2}. \tag{6.10}$$

The subgroup $N_G\left(C_{\frac{q-1}{2}}\right) = C_{\frac{q-1}{2}}$, implying there are $\frac{\frac{1}{2}q(q-1)}{\frac{1}{2}(q-1)} = q$ conjugate cyclic groups $C_{\frac{q-1}{2}}$ in G.

These cyclic groups intersect only at the identity.

Thus;

$$|\tau_1| = \left(\frac{q-1}{2} - 1\right) q. \tag{6.11}$$

We find the number of τ_0 elements by subtracting the number of τ_1 elements and the identity from the order of G.

It follows that;

$$|\tau_0| = \left[q\frac{q-1}{2} - \left(\frac{q-1}{2} - 1\right) q - 1\right] = q - 1. \tag{6.12}$$

Since the length of a conjugacy class of $g \in \tau_0$ is $\frac{q-1}{2}$ from Equation 6.10 and the number of τ_0 elements are $q-1$ from 6.12, then there are two conjugacy classes of elements in τ_0 but each element in τ_0 is of order q.

Therefore;

$$\begin{aligned} Z_{(G,X)} &= \frac{1}{|G|}(t_1^q + \frac{q-1}{2}.mon(x_1) + \frac{q-1}{2}.mon(x_2) \\ &\quad +q(summation\ of\ all\ monomials\ of\ the\ nontrivial\ elements\ in\ cyclic \\ &\quad subgroups\ C_{\frac{q-1}{2}})), \end{aligned}$$

where x_1 and x_2 are representatives of elements in the first and the second conjugacy classes respectively but since all τ_0 are of order p then they will have the same monomial and thus $Z_{(G,X)}$ can be written as;

$$\begin{aligned} Z_{(G,X)} &= \frac{1}{|G|}(t_1^q + (q-1).monomial\ of\ an\ element\ in\ \tau_0 \\ &\quad +q(summation\ of\ all\ monomials\ of\ the\ nontrivial\ elements\ in\ cyclic \\ &\quad subgroups\ C_{\frac{q-1}{2}})). \end{aligned}$$

That is,

$$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^q + (q-1)\,.mon(x) + q\sum_{g\in C_{q-1}\setminus\{I\}} mon(g)\right), \tag{6.13}$$

where $x \in \tau_0$.

Let $x \in \tau_0$, then $\pi(x) = 0$

It follows from Theorem 1.6.5 that,

$\pi(x^p) = q$ and

if $l < p$, $\pi\left(x^l\right) = 0$

Now if $0 < l < p$ then,

$$\begin{aligned} \alpha_l &= \frac{1}{l}\sum_{i|l} \pi\left(x^{\frac{l}{i}}\right)\mu(i) \\ &= \frac{1}{l}\sum_{i|l} 0\mu(i) = 0 \end{aligned}$$

and

$$\begin{aligned}
\alpha_p &= \frac{1}{p}\sum_{i|p}\pi\left(x^{\frac{p}{i}}\right)\mu(i)\\
&= \frac{1}{p}\left[\pi(x^p)-\pi(x)\right]\\
&= \frac{1}{p}\left[q-0\right]=\frac{q}{p}.
\end{aligned}$$

Therefore the resulting monomial is;

$$t_p^{\frac{q}{p}}. \qquad (6.14)$$

If $g\in\tau_1$, then $\pi(g)=1$,

$\pi\left(g^d\right)=q$ where d is the order of g,

$\pi\left(g^l\right)=1$ when $l<d$

$$\begin{aligned}
\alpha_l &= \frac{1}{l}\sum_{i|l}\pi\left(g^{\frac{l}{i}}\right)\mu(i)\\
&= \frac{1}{l}\sum_{i|l}(1)\mu(i)\\
&= \frac{1}{l}\sum_{i|l}\mu(i)=0.
\end{aligned}$$

$$\begin{aligned}
\alpha_d &= \frac{1}{d}\sum_{i|d}\pi\left(g^{\frac{d}{i}}\right)\mu(i)\\
&= \frac{1}{d}\left[\pi\left(g^{d}\right)\mu(1)+\sum_{1\neq i|d}\pi\left(g^{\frac{d}{i}}\right)\mu(i)-\pi(g)\right]\\
&= \frac{1}{d}\left[\pi\left(g^{d}\right)-\pi(g)\right]\\
&= \frac{1}{d}\left[q-1\right]=\frac{q-1}{d}.
\end{aligned}$$

Thus the resulting monomial is;

$$t_1 t_d^{\frac{q-1}{d}}. \tag{6.15}$$

Substituting for $mon(x)$ (in 6.14) and $mon(g)$ (in 6.15) in Equation 6.13 we get;

$Z_{(G,X)} = \frac{1}{|G|}\left(t_1^q + (q-1)\,t_p^{\frac{q}{p}} + q\sum_{1\neq d|\frac{q-1}{2}}\phi(d)t_1 t_d^{\frac{q-1}{d}}\right).$ $\square$

Example 6.4.1

Let $p=5,\ r=2\ \Rightarrow q=5^2,\ X=GF(25)$ and $|G|=300$.

Possible values of d are; 2, 3,4, 6 and 12.

Then

$\phi(2)=1$, $\phi(3)=2$, $\phi(4)=2$, $\phi(6)=2$ and $\phi(12)=4$.

Substituting in Theorem 6.4.1, we have;

$$Z_{(Aff_{\square}(25),X)} = \frac{1}{300}\left(t_1^{25}+24t_5^5+25t_1t_2^{12}+50t_1t_3^8+50t_1t_4^6+50t_1t_6^4+100t_1t_{12}^2\right).$$

6.4.1 Expressing the cycle index of the Affine square(q) group in terms of the cycle indices of the elementary abelian group P_q and the cyclic group $C_{\frac{q-1}{2}}$

The equation in Theorem 6.4.1 can be simplified as;

$$\begin{aligned}
Z_{(G,X)} &= \frac{1}{|G|}\left(t_1^q + (q-1)\,t_p^{\frac{q}{p}} + q\sum_{1\neq d|\frac{q-1}{2}} \phi(d) t_1 t_d^{\frac{q-1}{d}}\right) \\
&= \frac{1}{q\left(\frac{q-1}{2}\right)}\left(t_1^q + (q-1)\,t_p^{\frac{q}{p}}\right) + \frac{1}{q\left(\frac{q-1}{2}\right)}\left(qt_1^q + q\sum_{1\neq d|\frac{q-1}{2}} \phi(d) t_1 t_d^{\frac{q-1}{d}}\right) - \frac{1}{\frac{q-1}{2}} t_1^q \\
&= \frac{1}{\frac{q-1}{2}} Z_{(P_q,X)} + \frac{1}{\frac{q-1}{2}}\left(t_1^q + \sum_{1\neq d|\frac{q-1}{2}} \phi(d) t_1 t_d^{\frac{q-1}{d}}\right) - \frac{1}{\frac{q-1}{2}} t_1^q \\
&= \frac{1}{\frac{q-1}{2}} Z_{(P_q,X)} + Z_{(C_{\frac{q-1}{2}},X)} - \frac{1}{\frac{q-1}{2}} t_1^q \\
&= \frac{1}{\left|C_{\frac{q-1}{2}}\right|} Z_{(P_q,X)} + Z_{(C_{\frac{q-1}{2}},X)} - \frac{1}{\left|C_{\frac{q-1}{2}}\right|} Z_{(1,X)}. \qquad (6.16)
\end{aligned}$$

Example 6.4.2

Let $p = 3,\ r = 2\ \Rightarrow q = 3^2,\ X = GF(9)$ and $|G| = 36$ and

$Z_{(G,X)} = \frac{1}{36}\left(t_1^9 + 8t_3^3 + 9\sum_{1\neq d|4} \phi(d) t_1 t_d^{\frac{8}{d}}\right)$ (from Theorem 6.4.1)

which can be simplified as;

$$\begin{aligned}
Z_{(G,X)} &= \frac{1}{9\,(4)}\left(t_1^9 + 8t_3^3\right) + \frac{1}{9\,(4)}\left(9t_1^9 + 9\sum_{1\neq d|7} \phi(d) t_1 t_d^{\frac{7}{d}}\right) - \frac{1}{4} t_1^9 \\
&= \frac{1}{4} Z_{(P_9,X)} + Z_{(C_4,X)} - \frac{1}{4} t_1^9 \\
&= \frac{1}{4} Z_{(P_9,X)} + Z_{(C_4,X)} - \frac{1}{4} Z_{(1,X)}\ (from\ Equation\ 6.16).
\end{aligned}$$

CHAPTER 7

THE CYCLE INDEX OF THE FROBENIUS GROUP AS A SEMIDIRECT PRODUCT OF THE FROBENIUS COMPLEMENT *H* BY THE FROBENIUS KERNEL *M*

7.1 Introduction

A Frobenius group G is a group that acts on a set X transitively such that the stabilizer H of a point is nontrivial but only the identity element fixes two or more points. This collection of elements H of a Frobenius group G form a subgroup of G known as the Frobenius complement. This implies that $H \cap (xHx^{-1}) = \{e\}$. Given $x \in G \backslash H$, we define the set of all elements of G having no fixed points as $M^* = G \backslash \cup \{xHx^{-1} | x \epsilon G\}$. The set $M = M^* \cup \{e\}$ is a normal subgroup of G called the Frobenius kernel. The group G is a semidirect product of M by H written as $G = M \rtimes H$. The aim of this chapter is to express the cycle index formula of the Frobenius group in terms of cycle index of the Frobenius complement H and that of the Frobenius kernel M. This chapter has two sections. In Section 7.1 we give an introduction of the Frobenius group as a semidirect group. In Section 7.2 we express the cycle index of the Frobenius group in terms of the cycle indices of the Frobenius complement and the Frobenius kernel.

7.2 The cycle index of the Frobenius group

Let the cycle indices of the permutation groups H and M acting on the set X be $Z_{(H,X)}$ and $Z_{(M,X)}$ respectively. We need to express the cycle index of the Frobenius group G acting on X in terms of $Z_{(H,X)}$ and $Z_{(M,X)}$.

Theorem 7.2.1.

The cycle index formula of a Frobenius group G in terms of the cycle indices of the Frobenius kernel M and the Frobenius complement H is;

$Z_{(G,X)} = \frac{1}{|H|}Z_{(M,X)} + Z_{(H,X)} - \frac{1}{|H|}Z_{(1,X)}.$

Proof.

Let $x \in G$, be such that $x \neq$ e, then $x \in M$ or is a member of some conjugate of H. Since G acts on the set X transitively, then its action on X is equivalent to its action on the cosets of H in G.

From Theorem 1.6.5, the number of cycles of length l in a permutation x is given by $\alpha_l = \frac{1}{l}\sum_{i|l}\pi\left(x^{\frac{i}{l}}\right)\mu(i)$ where μ is the Möbius function.

It is enough to find the cycle of $x \in M$ and $x \in H$.

(i) If $x \in M$ then $|Fix(x)| = 0$ since x fixes no element by definition of M. Thus, $\pi\left(x^l\right) = 0$ unless $l = |x|$.

In the case when $l = |x|$ then,

$$\begin{aligned} \alpha_l &= \frac{1}{l}\sum_{i|l}\pi\left(x^{\frac{l}{i}}\right)\mu(i) \\ &= \frac{1}{l}\pi\left(x^l\right)\mu(1) \\ &= \frac{1}{|x|}\ \frac{|G|}{|H|} \end{aligned}$$

Thus $mon\ x = t_{|x|}^{\frac{|M|}{|x|}}$.

Thus, the contribution to the cycle index of G by the elements of M is;

$$\sum_{x \epsilon M} t_{|x|}^{\frac{|M|}{|x|}} \tag{7.1}$$

(ii) Let $x \epsilon H$ such that $x \neq e$, then from the definition, x fixes an element in $\frac{G}{H}$. If we first consider x^l such that $l \neq |x|$, then; $\pi\left(x^l\right) = 1$ for $1 < l < |x|$.

Now,

$$\begin{aligned}
\alpha_l &= \frac{1}{l}\sum_{i|l} \pi\left(x^{\frac{l}{i}}\right)\mu(i) \\
&= \frac{1}{l}\sum_{i|l} \mu(i) = 0.
\end{aligned}$$

If $l = |x|$, then;

$$\begin{aligned}
\alpha_{|x|} &= \frac{1}{|x|}\sum_{i||x|} \pi\left(x^{\frac{|x|}{i}}\right)\mu(i) \\
&= \frac{1}{|x|}\left[|M| + \sum_{1<i||x|} \pi\left(x^{\frac{|x|}{i}}\right)\mu(i)\right] \\
&= \frac{1}{|x|}\left[|M| + \sum_{i||x|} \mu(i) - 1\right] \\
&= \frac{1}{|x|}\left[|M| - 1\right] \ \ since \sum_{i||x|} \mu(i) = 0
\end{aligned}$$

So $mon\ x = t_1 t_{|x|}^{\frac{1}{|x|}[|M|-1]}$.

In this case we have excluded the identity element since it is contained in both

H and M and was considered in M. Since there are $|M| = \frac{|G|}{|H|}$ conjugates of H in G, the contribution to the cycle index of G by the non–identity elements of H and its conjugates is;

$$|M| \sum_{1 \neq x \in H} t_1 t_{|x|}^{\frac{1}{|x|}[|M|-1]} \tag{7.2}$$

Therefore by summing Equations 7.1 and 7.2 we get the cycle index of G as;

$$Z_{(G,X)} = \frac{1}{|G|} \left[\sum_{x \in M} t_{|x|}^{\frac{|M|}{|x|}} + |M| \sum_{1 \neq x \in H} t_1 t_{|x|}^{\frac{1}{|x|}[|M|-1]} \right] \tag{7.3}$$

$$Z_{(G,X)} = \frac{1}{|H|\,|M|} \sum_{x \in M} t_{|x|}^{\frac{|M|}{|x|}} + \frac{1}{|H|} \sum_{x \in \ H} t_1 t_{|x|}^{\frac{|M|-1}{|x|}} - \frac{1}{|H|} t_1^{|M|}$$

Thus, the cycle index of G in terms of the cycle index of M and H is;

$$Z_{(G,X)} = \frac{1}{|H|} Z_{(M,X)} + Z_{(H,X)} - \frac{1}{|H|} Z_{(1,X)}. \tag{7.4}$$

□

CHAPTER 8

CONCLUSION AND RECOMMENDATIONS FOR FURTHER RESEARCH

8.1 Introduction

This chapter has three sections. In Section 8.1 we give an introduction while the conclusion is given in Section 8.2. Finally, in Section 8.3 we suggest some areas for further research.

8.2 Conclusion

The purpose of this study was to express the cycle index formulas of different semidirect product groups in terms of the cycle index formulas of the subgroups the groups are semidirect product of.

In Chapter three we expressed the cycle index formula of the dihedral group D_n in terms of the cycle index formulas of the cyclic group C_n and a cyclic group of order two C_2, where the resulting cycle indices were given as; $Z_{(G,X)} = \frac{1}{2}\ Z_{(C_n,X)} + Z_{(C_2,X)} - \frac{1}{2}\ Z_{(1,X)}$ for an odd value of n and $Z_{(G,X)} = \frac{1}{2} Z_{(C_n,X)} + \frac{1}{2} Z_{(C_2,X)} + \frac{1}{4} t_2^{\frac{n}{2}} - \frac{1}{4} Z_{(1,X)}$ for an even value of n.

In Chapter four we expressed the cycle index formula of the symmetric group S_n in terms of the cycle index formulas of the alternating group A_n and a cyclic group of order two C_2, where the resulting cycle index was given as;

$Z_{(G,X)} = \frac{1}{2} Z_{(N,X)} + \frac{1}{(n-2)!} Z_{(H,X)} - \frac{1}{2(n-2)!} Z_{(1,X)} + \frac{1}{n!}\ k$, where k is the set of monomials of the odd permutation of X that are not transpositions.

In Chapter five we expressed the cycle index formula of the affine(p) group in terms of the cycle index formulas of the cyclic group C_p and a cyclic group C_{p-1} and extended the same to a general $q = p^r$, where the resulting cycle indices were given as; $Z_{(Aff(p),X)} = \frac{1}{|C_{p-1}|} Z_{(C_p,X)} + Z_{(C_{p-1},X)} - \frac{1}{|C_{p-1}|} Z_{(1,X)}$, for the affine($p$) group and $Z_{(Aff(q),X)} = \frac{1}{|C_{q-1}|} Z_{(P_q,X)} + Z_{(C_{q-1},X)} - \frac{1}{|C_{q-1}|} Z_{(1,X)}$ for the affine(q) group.

In Chapter six we expressed the cycle index formula of the affine square(p) group in terms of the cycle index formulas of the cyclic group C_p and a cyclic group $C_{\frac{p-1}{2}}$ and extended the same to a general $q = p^r$ where the resulting cycles were given as; $Z_{(Aff_{\square}(p),X)} = \frac{1}{\left|C_{\frac{p-1}{2}}\right|} Z_{(P_q,X)} + Z_{(C_{\frac{p-1}{2}},X)} - \frac{1}{\left|C_{\frac{p-1}{2}}\right|} Z_{(1,X)}$, for the affine square($p$) and $Z_{(Aff_{\square}(q),X)} = \frac{1}{\left|C_{\frac{q-1}{2}}\right|} Z_{(P_q,X)} + Z_{(C_{\frac{q-1}{2}},X)} - \frac{1}{\left|C_{\frac{q-1}{2}}\right|} Z_{(1,X)}$ for the affine square(q).

Lastly in Chapter seven we expressed the cycle index formula of a Frobenius group G in terms of the cycle index formulas of the Frobenius complement and the Frobenius kernel and the resulting cycle was given as $Z_{(G,X)} = \frac{1}{|H|} Z_{(M,X)} + Z_{(H,X)} - \frac{1}{|H|} Z_{(1,X)}$. It was noted that for semidirect groups which are Frobenius such as the dihedral group D_n with an odd value of n, the affine group and the affine square groups, we can fully express the cycle index of the groups in terms of the cycle index formulas of the subgroups it is a semidirect product of. However, for semidirect product groups which are not Frobenius such as the dihedral group D_n with an even value of n and the symmetric group, the cycle index formula of the group cannot be expressed fully in terms of the cycle index formulas of the subgroups it is a semidirect product of.

8.3 Recommendations for further research

Now that a general expression for the cycle indices of semidirect product groups which are Frobenius in terms of the cycle indices of their kernels and complements has been found in this study, further study can be done to find applications of the resulting expressions.

A similar research can also be done for other semidirect product groups which have not been considered such as the split metacyclic groups, in the hope of getting an expression of cycle indices for another family of semidirect product or an expression of the cycle indices of all the semidirect product groups.

References

Balasubramanian, K. (1979). Enumeration of stable stereo and isomers of polysubstituted alcohols. *Annals New York Acad. Sc*, **319**:33–36.

Bruijn, D. N. and Klarner, D. A. (1969). Enumeration of generalized graphs. *Koninkl. Nederl Akademia van wetenschappen, proceedings series*, **A72(1)**:1–9.

Cameron, P. J. (2007). Permutation groups. *London Math. Soc. Student Texts 45, Cambridge University Press, Cambridge.*

Harald, F. (1997). Cycle indices of linear, affine and projective groups. *Linear Algebra and Its Applications*, **263**:133–156.

Harary, F. (1955). The number of linear directed rooted and connected graphs. *Transactions of the American Mathematics Society*, **78**:445–463.

Harary, F. (1959). Exponential of permutation groups. *Amer Math. Monthly*, **66**:572–575.

Harary, F. (1960). Seminar on graph theory, holt, rinehart and winston. *Academic Press, New York.*

Harary, F. (1967). *Applications of Pólya's Theorem to permutation groups,. Ed. 4. Academic Press, New York.*

Harary, F. (1969). Graph theory. *Addison-Wesley Publishing Company, Academic Press, New York.*

Harary, F. and Palmer, E. (1966). Power group enumeration Theorem. *Journal of Combinarial Theory*, **1**:157–173.

Harary, F. and Palmer, E. (1973). Graphical enumeration. *Academic press, New York.*

Harrison, M. A. and High, R. G. (1968). Cycle index of a product of permutation groups. *Combinatorial Theory*, **4**:277–299.

Jason, F. (1999). Cycle indices for the finite classical groups. *Journal of Group Theory*, **2**:251-289.

Jason, F., Saxl, J. and Pham, H. (2012). Cycle indices for finite orthogonal groups of even characteristic. *Trans. Amer. Math. Soc*, **364**:2539-2566.

Joseph, P. S. (1981). The cycle structure of a linear transformation over a finite field. *Linear Algebra Appl*, **36**:141–155.

Kamuti, I. N. (1992). Combinatorial formulas, invariants and structures associated with primitive permutation representations of $PGL(2, q)$ and $PSL(2, q)$. *PhD, Mathematical studies Southampton University, U.K.*

Kamuti, I. N. (2004). On the cycle index of Frobenius groups. *East Africa Journal of Physical Sciences*, **5(2)**:81–84.

Kamuti, I. (2012). Cycle index of internal direct product groups. *International mathematical forum*, **7**:1491–1494.

Kamuti, I. and Obong'o, J. O. (2002). The derivation of cycle index *of* $S_n^{[3]}$. *Quaestiones Mathematicae*, **25**:437–444.

Kamuti, I. N. and Njuguna, L. N. (2004). On the cycle index of the reduced ordered r-groups. *East Africa Journal of Physical Sciences*, **5(2)**:99–108.

Kangogo, M. R. (2015). Ranks and subdegrees of the cyclic group, the dihedral group and the affine group and associated suborbital graphs. *PhD thesis, Kenyatta University.*

Kimani, P., Kamuti, I. and Rimberia, J. (2019). Cycle index formula for $G = PGL(2, q)$ acting on the cosets of $PSL(2, e)$ where q is an even power of e. *International Journal of Scientific Research and Innovative Technology*, **1**:1–10.

Krishnamurthy, V. (1985). Combinatorics: Theory and application. *Affiliated East-West Press Private Limited, New Delhi.*

Munywoki, M., Kamuti, I. and Kivunge, B. (2010). Cycle indices of Frobenius groups. *International Electronic Journal of Pure and Applied Mathematics*, **3**:339–344.

Muthoka, G. (2017). Derivation of cycle index formulas for dihedral group acting on unordered triples. *International Journal of Science and Research*, **6**:3235.

Muthoka, G., Kamuti, I., Hussain, L. and Patrick, K. (2015). Cycle index formulas of dihedral group acting on unordered pairs. *Journal of Mathematical Theory and Modeling*, **5**:11–21.

Muthoka, G., Kamuti, I., Kimani, P. and Hussein, L. (2016). Cycle index formulas for acting on ordered pairs. *International Journal of Science and Research*, **4**:1980–1983.

Peter, J. and Jason, S. (2017). The cycle polynomial of permutation group. *The electronic journal of combinatorics*, **25**:116.

Pólya, G. (1937). Combinatorische anzahlbestimmungen für gruppen, graphen und chemische verbindungen. *Acta Mathematics*, **68**:145–254.

Pólya, G. and Read, R. C. (1987). Combinatorial enumeration of groups, graphs and chemical compounds. *Springer-Verlag, New York.*

Read, R. C. (1959). The enumeration of locally restricted graphs I. *Journal of London Mathematics*, **34**:417–436.

Read, R. C. (1960). The enumeration of locally restricted graphs II. *Journal of London Mathematics*, **49**:344–351.

Redfield, J. H. (1927). The theory of group-reduced distributions; Amer. *Journal of London Mathematics*, **49**:433–455.

Robinson, R. W. (1970). The enumeration of non-separable graphs. *Journal of Combinatorial Theory*, **4**:181–190.

Rotich, S. K. (2016). Cycle indices, subdegrees and suborbital graphs of $PGL(2, q)$ acting on the cosets of its subgroups. *PhD thesis, Kenyatta University.*

Rotich, S. K. (2018). Cycle indices of $PGL(2, q)$ acting on the cosets of its subgroups. *International Journal of Scientific Research and Innovative Technology*, **4**:26–37.

Vladimir, B. and Kovijanic, V. (2017). The cycle index of the automorphism group of Z_n. *de L'Institut Mathematique, Nouvelle Série*, **101**:99–108.