COMBINATORIAL PROPERTIES OF THE ALTERNATING & DIHEDRAL GROUPS AND HOMOMORPHIC IMAGES OF FIBONACCI GROUPS

BASHIR ALI
B.Sc (Hons. unimaid), M.Sc. (unijos)
PGNS/UJ/12261/00

A thesis in the Department of MATHEMATICS Faculty of Natural Sciences

Submitted to the School of Postgraduate Studies, University of Jos, in partial fulfillment of the requirements for the award of the degree of DOCTOR OF PHILOSOPHY IN MATHEMATICS of the

UNIVERSITY OF JOS.

AUGUST, 2010

CERTIFICATION

This is to certify that this thesis examined and approved for the award of the degree of **DOCTOR OF PHILOSOPHY in MATHEMATICS**:

______________________________	______________________________
	Professor S.U. Momoh
External Examiner	**Internal Examiner**
______________________________	______________________________
Professor M.S. Audu	Professor U. W. Sirisena
Supervisor	**Head of Mathematics Department**
______________________________	______________________________
Professor Y. N. Lohdip	Professor U.A. Ibanga
Dean of Faculty of Natural Sciences	**Dean, School of Postgraduate Studies**

DECLARATION

I hereby declare that this work is the product of my own research efforts, undertaken under the supervision of Professor M. S. Audu and has not been presented elsewhere for the award of a degree or certificate. All sources have been duly distinguished and appropriately acknowledge.

BASHIR ALI

(PGNS/UJ/12261/00)

ACKNOWLEDGEMENT

I am deeply indebted to a number of people who have given me assistance and tremendous support throughout the course of this study.

I wish to thank my supervisor, Professor M. S. Audu who has patiently guided and corrected me throughout the duration of this work. It is his expert advice and assistance that have made this work a reality.

My sincere appreciation goes to the entire staff of the Department of Mathematics, in particular the current Head of Mathematics Departments University of Jos and Nigerian Defence Academy, Kaduna in persons of Prof. W. Sirisena and Dr.KB Yuguda. Similar thanks goes to the program co-coordinator, Dr. E Apine.

I am also grateful to the Nigerian Defence Academy, Kaduna, for allowing me to undertake this training leave.

I will like to thank Dr. A. Umar, Sultan Qaboos University, Oman. It is from him I learnt more about cambinatorics while I was a research fellow in the Department of Mathematical Sciences, King Fahd University of Petroleum and Minerals Dhahran. Similar thanks goes to Dr. B. Yushau for the invitation and the Department for granting me research visiting position.

My sincere appreciation also goes to my wife Murja Shafiu, my children: Rahmatullah, Fatima, Ummukhulsum, Aishatu and Hannatu, my parents, inlaws, and brothers, in particular Dr. Habu Ali for their continue support and prayers.

DEDICATION

I dedicate this work to my family, Abu Hamza Hadejia and to all those who may find it beneficial to their scope of study.

TABLE OF CONTENTS

CHAPTER ONE
INTRODUCTION

CHAPTER TWO
LITERATURE REVIEW

CHAPTER THREE
RESULTS

LIST OF TABLES

NOTATIONS

$H \leq G$	H is a subgroup G
$H \lhd G$	H is normal in G
Hg, gH	Left or right coset of H in G , $g \in G, H \leq G$
$\phi : G \to H$	ϕ is a mapping from G to H
$\mathrm{G} \cong \mathrm{H}$	Group G and H are isomorphic
$\ker\phi$	Kernel of ϕ
G/N	Quotient group of G by N
$g^{-1}Hg$	Conjugate of H by g, $g \in G, H \leq G$
$N_G(H)$	Normalizer of H in G
$C_G(H)$	Centralizer of H in G
$Z(G)$	Center of G
$Aut(H)$	Group of automorphisms of H
$\mathrm{Inn}(G)$	Group of inner automorphisms of G
$\mathrm{Im}(\rho)$	Image of homomorphism ρ
$\mathrm{H} \times \mathrm{K}$	Direct product of H and K
D_n	Dihedral group of Degree n
$\mathrm{A_n}$	Alternating group on n elements
k^g	Action of g on k
$\mathrm{G}^{(n)}$	The n^{th} derived group of G
$V_1 \oplus V_2$	Direct sum of Vector spaces V_1 *and* V_2
$Fix_m(G)$	Fixed-point space of G *on* M

$Ann(M)$	Annihilator of M
$rad\ R$	Jacobson radical of R
$\lvert G:H\rvert$	Index of $H\ \ in\ \ G$
α^G	Orbit of $\alpha\ \ under\ \ G$, $\alpha \in \Omega$
G_α	Stabilizer of $\alpha, \alpha \in \Omega$
$G_{(\Delta)}$	Pointwise stabilizer of a subset $\Delta\ of\ \Omega$
$G_{\{\Delta\}}$	Setwise stabilizer of a subset $\Delta\ of\ \Omega$
G^Δ	Constituent of G on Δ
B_n	Bell number B_n
$C(n,r)$	Binomial Coefficient
$C(n, n_1, n_2, \ldots n_k)$	Multinomial coefficients
C_n	n Catalan number
$d(n,k)$	Number of permutation on n-set X having k cycles
$f(N,r)$	Number of partitions of N in which each part represented fewer than r times
$g(N,r)$	Number of partitions of N having no part divisible by r
$p(n,r)$	Number of r permutations of collection of n distinct objects
$S(n,r)$	Sterling number of the first kind

$s(n,r)$	Sterling number of the second kind
$S(n,0)$	Singles sterling number
d_n	Number of derangements
$f(n+2)=f(n+1)+f(n)$ $f(0)=f(1)=1$	Recurrence of Fibonacci number
L_n, $L_1=1 \quad L_2=3$ $L_{n+2}=L_{n+1}+L_n$	Recurrence of Lucas number

Abstract

Let $X_n = \{1,2,\ldots,n\}$ be a finite n-element set and let S_n, A_n *and* D_n be the Symmetric, Alternating and Dihedral groups of X_n, respectively. In this thesis we obtained and discussed formulae for the number of even and odd permutations (of an $n-$element set) having exactly k fixed points in the alternating group and the generating functions for the fixed points. Further, we give two different proofs of the number of even and odd permutations (of an $n-$element set) having exactly k fixed points in the dihedral group, one geometric and the other algebraic. In the algebraic proof, we further obtain the formulae for determining the fixed points. We finally proved the three families; $F(2r,4r+2)$, $F(4r+3,8r+8)$ and $F(4r+5,8r+12)$ of the Fibonacci groups $F(m,n)$ to be infinite by defining Morphism between Dihedral groups and the Fibonacci groups.

CHAPTER ONE
INTRODUCTION

1.1 INTRODUCTION

The main aim of this chapter is to highlight a few concepts which are fundamental for the understanding of semigroup, group and combinatorial theoretical concepts. The results therein form the background of the study, which spell out the statement of the problem, objective and justification of the study.

Let $X_n = \{x_1, x_2, \ldots, x_n\}$ be a finite set, a permutation on X_n is a one-to-one mapping of X_n onto itself. The set of all permutations on n elements is denoted by S_n called symmetric group of degree n,and of order $n!$. The group S_n consists of both even and odd permutations depending on the length the permutation, even or odd. The set of all even permutations on X_n forms a group called the alternating group (A_n). Another subgroup of S_n comprising of both even and odd permutations is called the Dihedral group such that for all $x, y \in S_n, \quad x, y \in D_n \, iff \; x^n = y^2 = 1, xy = y^{-1}x$.

The arrangement of elements of the Alternating or Dihedral groups according to specified rule (the number of fixed points) is of particular interest. First, how many of such arrangements are possible and what is their recurrence and generating functions.

Another group which has similar structure to the dihedral group is the Fibonacci $F(r,n) =< a_1a_2 \cdots a_{n-1}a_n : a_1a_2 = a_3, a_2a_3 = a_4, \cdots a_{n-1}a_n = a_1 >$ where r is the number of relations and n is the number of generators, for what value of $r \,\&\, n$ is the group finite or infinite.

1.2 BACKGROUND OF THE STUDY

Let $X_n = \{1, 2, \ldots, n\}$ be a finite n-element set and let $P_n,\ O_n,\ S_n, D_n\ and\ A_n$ be the partial transformation semigroups, the submonoid of T_n consisting of all order preserving mappings of X_n, the symmetric, dihedral and alternating groups respectively. The combinatorial properties of S_n have been studied over long period and many interesting results have emerged. In particular, the number of permutations of X_n having exactly k fixed points and their generating functions are known.

The Dihedral group D_n, geometrically consists of all symmetries of a regular $n-gon$ $(n \geq 3)$, that is, n rotations through the angles $\frac{360^\circ}{n}x$ $(x = 0,1,2,\ldots,n-1)$ and n reflections through each of the n lines of symmetry of the regular n-gon. Algebraically, each element of D_n is either cyclic (preserve orientation) or ant-cyclic (reverse orientation). Catarino and Higgins (1999) introduced a new subsemigroup of X_n containing O_n which is denoted by OP_n and its elements are called orientation preserving mappings. Also, they introduced a Semigroup $P_n = OP_n \cup OR_n$ where OR_n denotes the collection of all orientation reversing mappings. They showed that the Dihedral Group is the maximal sub-Semigroup of $P_n = OP_n \cup OR_n$. Fernandes (2000) studied the monoid of orientation preserving partial transformations of a finite chain, concentrating in particular on partial transformations which are injective. However, the algebraic proof (along the lines of Catarino and Higgins (1999)) and the geometric proof, for the number (and properties) of even and odd permutations having exactly k fixed points in the Dihedral group D_n seem not to have been studied.

The Fibonacci group $F(2, n)$ is the group defined by the Presentation

$$< a_1 a_2, \cdots, a_n : a_1 a_2 = a_3 , a_2 a_3 = a_4 \cdots a_{n-1} a_n = a_1 , a_n a_1 = a_2 >$$

The study of these groups began in earnest after a question of Conway (1965) as to whether or not $F(2, 5)$ is cyclic of order 11, and it was quickly determined in (Conway, et al, 1965) that this was indeed the case, and also that $F(2, 1)$ and $F(2, 2)$ are trivial, $F(2, 3)$ is the quaternion group of order 8, $F(2, 4)$ is cyclic of order 5, and $F(2, 6)$ is infinite.

In a survey article Thomas (1989) gave a list of those parameters r and n for which the finiteness or infiniteness of the Fibonacci group $F(r,n)$ was still unknown. Since then, some of the unknown examples were proved infinite by Prishchepov (1998) using geometric methods, and some isolated difficult examples, such as $F(4,7)$, were proved infinite and automatic by computer programs written by Holt (1998), Christopher (1998), proved all of the outstanding cases except for two families of examples which were proved to be infinite by using geometric methods. The two families that remain unsettled are $F(7+5i,5)$ and $F(8+5i,5)$ for integers $i \geq 0$. The methods also apply to those examples that had previously been handled by computers. All these methods were not able to give a generalized result of testing the order of a Fibonacci group.

1.3 STATEMENT OF THE PROBLEM

Let

$$e(n,k) = \left|\{\alpha \in A_n : f(\alpha) = k\}\right|$$

$$e'(n,k) = \left|\{\alpha \in A_n' : f(\alpha) = k\}\right|$$

$$f(x) = \sum_{i \geq 0} e_i \frac{x^i}{i!}$$

be the number of even (odd) permutations in the alternating group and the generating functions for the fixed points. How many even (odd) permutations ($e(n,k)$ *or* $e'(n,k)$) of an $n-$element set having exactly k fixed points are in the alternating group and what is the generating functions for the fixed points.

Geometrically and Algebraically, How many even and odd permutations (of an $n-$element set) having exactly k fixed points are in the dihedral group and what are the fixed points.

To study Alternating and Dihedral groups, let α be a permutation of X_n, and $f(m\ ,n)$ be the number of permutations of X_n that can be expressed as a product of $r_i(m-i+1, i=1,2,\cdots, m-1)$ cycles. How many such permutations are there in X_n.

The Fibonacci groups $F(m\ ,n)$ defined as

$$F(m,\ n) = < a_1, a_2, \ldots, a_n | a_i a_{i+1} \cdots a_{i+m-1} = a_{i+m} \ \ i = 1,2,\ldots,m >$$

for what value of m *and* n is the Fibonacci group infinite or finite.

1.4 JUSTIFICATION OF THE STUDY

Since the combinatorial properties of $A_n \textit{ and } D_n$ have not been studied, it is our desire to consider the number of even and odd permutations (of an $n-$element set) having exactly k fixed points in the alternating & dihedral groups, the generating functions for the fixed points in the alternating group and the formulae for determining the fixed points in the dihedral group. Considering the combinatorial properties of the Dihedral group, we create morphism between the dihedral group and the Fibonacci group. The morphism will give us a new method of determining the finiteness or infiniteness of Fibonacci group.

It is our hope that the combinatorial properties of these groups will help in studying the nature (structure) of other permutation groups, and it is our hope that the new method of studying the finiteness or infiniteness of Fibonacci group will help in the study of unsettled problems.

1.5 OBJECTIVE OF THE STUDY

The objective of this research is to

1. Obtain the number of even (odd) permutations having exactly k fixed points in the alternating group, discuss the fixed points and the generating functions for the fixed points.

2. Give two different proofs one geometric and the other algebraic (in line with Catarino and Higgins 1999) of the number of even and odd permutations (of an $n-$element set) having exactly k fixed points in the dihedral group. In

the algebraic proof, we further obtain the formulae for determining the fixed points.

3. Prove the three families; $F(2r,4r+2)$, $F(4r+3,8r+8)$ and $F(4r+5,8r+12)$ of the Fibonacci groups $F(m\ ,n)$ to be infinite by defining Morphism between Dihedral groups and the Fibonacci groups.

4. Obtain the number of permutations of X_n that can be expressed as a product of $r_i\left(m-i+1, i=1,2,\cdots, m-1\right)$ cycles.

1.6 BASIC SEMIGROUP THEORY

Throughout unless otherwise explicitly indicated, the letter S denotes an arbitrary semigroup.

We call an algebraic structure $(S,\circ)$ that satisfies the closure property a groupoid, that is to say, if, $\forall\ x,\ y \in S,\ \ x\circ y \in S$. A semigroup S is a groupoid with an associative binary operation, that is to say, if

$$\forall\ x, y,\ z \in S, \qquad x\circ(y\circ\ z)=(x\circ\ y)\circ z.$$

If a semigroup S has the property that, for all $x\ ,y\in\ S,\ \ xy=yx$, we say that S is a commutative semigroup. If a semigroup S contains an element 1 with the property that $\forall\ x\in S,\ \ 1\circ x = x = x\circ 1.$ We say that 1 is an identity element of S, and that S is a semigroup with identity or a monoid. A semigroup S has at most one identity element. If S has no identity element, then an extra element 1 can be adjoined to S to form a monoid. We define $S\circ 1 = S = 1\circ S$ and $1\circ 1 = 1\ \forall\ \ s\in S$, thus $S\cup\{1\}$ is now a monoid. We refer to

$S^1 = S \cup \{1\}$ as a monoid obtained from S by adjoining an identity element if necessary.

If a semigroup S with at least two elements contains a unique element 0 (zero) such that, $\forall\ x \in S,\ 0 \circ x = x \circ 0 = 0$, we say that 0 is a zero element (or just a zero) of S and S is a semigroup with zero. If S has no zero element, then an extra element 0 can be adjoined to S, we define $S \circ 0 = 0 = 0 \circ S$ and $0 \circ 0 = 0$ $\forall\ s \in S.$ We refer to $S^0 = S \cup \{0\}$ as a semigroup obtained from S by adjoining zero if necessary. A semigroup with zero, sometimes written as S^0 such that $xy = 0\ \ \forall\ x, y \in S$ is called a null semigroup. A semigroup with zero is called a 0 group if and only if $\forall a \in S \setminus \{0\}\ \ aS = S$ and $Sa = S.$

A non-trivial example of semigroup are the so called left (right) zero semigroups. A non-empty set L such that $\forall\ a, b \in L,\quad ab = a,$ is called a left zero semigroup. Similarly, we define a right zero semigroup R such that $\forall a, b \in R,\ \ ab = b.$ Observe that for all a in L(R) we have $a^2 = aa = a$ such elements are called idempotent. A semigroup consisting entirely of idempotent elements is called a band (or Idempotent semigroup).

A non-empty subset $A\ of\ S$ is called a subsemigroup if it is closed with respect to multiplication, that is, if $a, b \in A,\ ab \in A$ a condition that can be expressed more compactly as $A^2 \subseteq A.$ The associative condition that holds throughout S certainly holds throughout A and so A is itself a semigroup. The sets $S,\ \{0\}, \{1\}\ and\ \{e\}$ are special subsemigroups of$S.$

A non empty subset A of S is called a left Ideal if $SA \subseteq A,$ a right ideal, if $AS \subseteq A,$ and two sided if it is both a left and a right ideal. Every ideal is a subsemigroup, but the converse is not true.

1.7 MONOGENIC (CYCLIC) SEMIGROUP

The concept of a cyclic semigroup is similar to that of group theory. Let S be a semigroup, and let $\{U_i : i \in I\}$ with $I \neq 0$ $\phi \neq T = \bigcap_{i \in I} U_i$ is a subsemigroup of $S.$ Let A be a non empty subset of $S,$ there is at least one subsemigroup of S containing $A,$ namely S itself. The intersection of all subsemigroups of S containing $A,$ is a subsemigroup of S we denote it by $\langle A \rangle$, and is a subsemigroup defined by two properties. (1) $A \subseteq A_j (j \in J).$ (2) If U is a subsemigroup of S containing $A,$ then $< A >= U_j$ for each j.

The subsemigroup $\langle A \rangle$ consists of all elements of S that can be expressed as a finite product of elements of $A.$ If $\langle A \rangle = S,$ we say that A is a set of generators or a generating set of S.

If A is finite, i.e. $A = \{ a_1, a_2, a_3, \ldots, a_n \}.$ Then we shall write $\langle A \rangle$ as $\langle a_1, a_2, \ldots, a_n \rangle$. In the case where $A = \{a\},$ a singleton set, when $< a > = \{ a \ , a^2, a^3, \cdots \}.$ If S is a monoid then we can equally talk of the subsemigroup of S generated $a,$ this will always contain 1, $< a >= \{1, a \ , a^2, a^3_{,} \cdots\}.$ we refer to $\langle a \rangle$ as a monogenic subsemigroup of S generated by the element $a.$ The order of a is the order of the subsemigroup $\langle a \rangle$.

If S is a semigroup in which there exist an element a such that $S = < a >$, then S is said to be a monogenic semigroup. A semigroup with only one generator is referred to as cyclic.

1.8 ORDERED SETS, SEMILATTICES AND LATTICES

A binary relation $\leq$ on a set X is called a partial order relation if the relation $\leq$ is an equivalence relation on X.

A partial order having the extra-property that for all $x, y \in X$, $x \leq y$ or $y \leq x$ will be called a total (or linear) order. A set with total order will be called a totally ordered set (or chain). A set with a partial order is called a poset.

1.9 GREEN'S EQUIVALENCE: REGULAR SEMIGROUP

In 1951, J.A. Green defined five equivalences $H, K, R, D, and\ J$.

These equivalences play a fundamental role in the semigroup theory.

Green's Equivalences: Let a be an element of a semigroup S. The smallest left ideal of S containing an element a is $Sa \cup \{a\}$, denoted by S^1a and is called the principal left ideal generated by a. An equivalence L on S is defined by the rule that $a\ L\ b$ if and only if $S^1a = S^1b$ Similarly, we define the equivalence R by the rule that $a\ R\ b$ if and only if $aS^1 = bS^1$.

An alternative (internal) characterization is;

Let $a, b, c,\ d\ \in S$. Then

(i) $a\ L\ b\ iff\ \exists\ x, y \in S^1 :\ xa = b,\ \ yb = a$

$a\ R\ b\ \ iff\ \exists\ \ u, v \in S^1\ :\ au = b,\ \ bv = a$

(ii) L *and* R are right and left congruence's respectively.

(iii) $L \cap R = H$ *and* $L \cup R = D$ The smallest equivalence containing both L *and* R.

The equivalence J is defined by the rule that

$a\ J\ b \Rightarrow S^1 a\, S^1 = S^1 b S^1$

$\Leftrightarrow \exists x, y, u, v \in S^1,\ xay = b,\ ubv = a.$

An element $a \in S$ is called regular; if there exists $x\ in\ S$ such that $a\,x\,a = a.$ Obviously, idempotents are regular. If every element of a semigroup S is regular, we say that S is a regular semigroup.

Groups are of course regular semigroups and also every rectangular band B is trivially regular, since $axa = a$ for all a, x in B

Every idempotent e in a semigroup S is right identity for Re(right regular D-class) and a left identity for $Le.$(left regular D-class) An element $a^{'}$ in S is called an inverse of a if $aa^{'}a = a,\ a^{'}a\, a^{'} = a^{'}.$

An element with an inverse is necessarily regular, if $a^{'}$ is an inverse of a then a is an inverse of $a^{'}$. Every regular element has an inverse, if there exist x in S such that $axa = a$ then, let $x^{'} = xax,\ ax^{'}a = a,\ x^{'}ax^{'} = x^{'}.$

An element a in S may have more than one inverse. Indeed, in a rectangular band every element is an inverse of every other element.

1.10 BASIC GROUP THEORY

Throughout, unless otherwise explicitly indicated, the letter G denotes an arbitrary group.

Let G be a non empty set, the algebraic structure $(G,*)$ is called a group if;

(i) G is a semigroup with respect to $*$

(ii) For all $g \in G \; \exists \; e \in G$ such that $g*e = e*g = g$, the element e is the identity element of G.

(iii) To every element $g \; in \, G$, there exist a unique element $g^{-1} \in G$ called the inverse of $g \; in \, G$ with the property that $g*g^{-1} = g^{-1}*g = e.$

Henceforth, unless otherwise explicitly indicated, our groups are multiplicative. If H is a subset of a group G such that the group operation of G is closed on H, then H is a subgroup of G and we write $H \leq G,$ we state that H is a subgroup of G if for all $x, y \in H,$ $x y^{-1} \in H.$

If the element e is the identity element of $G,$ the set $\{e\}$ is the smallest subgroup of G of order one. This and G itself are called the trivial (improper) subgroups of $G.$ Any other subgroup H of G is said to be a proper subgroup of G**.**

We say that G is commutative or abelian if every pair of its elements commutes, i.e. $\forall \; g_1, g_2$ in G. $g_1g_2 = g_2g_1$, otherwise it is non-abelian. By the cardinality of G we mean the number of elements of the set G which we called the order of G and is denoted by $|G|$ or $o(G)$.

The order of an element $g \in G$ is the least positive integer n, if one exists, such that $a^n = e,$ then g is said to be of order n, if no such n exist, then g is said to be of infinite or zero order.

Let $g \in G$, if the group G can be generated by an element $g \in G$ such that $G = \{g^n : n \in Z_+\}$ then G is said to be a cyclic group generated by g, and written as $\langle g \rangle = G.$ If g generates G then so is $g^{-1} \in G,$ and the order of g is equal to the order of $G.$ Thus, if the $0(G) = n$ *and* $0(g) = m$ Then m and n are relatively prime.

If $0(G) = p, p$ a prime number, then G is cyclic and has no proper subgroup.

1.11 PERMUTATION GROUP

Let $X_n = \{x_1, x_2, \ldots, x_n\}$ be a finite set of arbitrary elements, a permutation on X_n is a one-to-one mapping of X_n onto itself. The set of all permutations on X_n forms a group with respect to permutation multiplication (composition of mappings). The set of all permutations on n elements is denoted by S_n *or* $Sym(X_n)$ and called the symmetric group of degree n, the degree of S_n is the number of elements in the finite set permuted. The number of elements in a permutation on n elements is $n!$ and is the order of S_n $(i.e. |S_n| = n!)$. A Permutation group G is a subgroup of a symmetric group. Elements of permutation groups are denoted by lower case letters as well as elements of abstract groups.

The inverse permutation $\beta \in S_n$ is given by $\beta^{-1} \in S_n$, if β takes y into x and then β^{-1} permutation inverse of β takes the point x to y, $x\beta^{-1} = y$. The identity permutation on X_n is the identity mapping which leaves all points of X_n fixed, $i : x \to x$ $(x)i = x \; \forall x \in G$.

Any element $g \in Sym\left(X_{n}\right)$ can be written in $r - cycle,\ i.e.\ g = (x_1\ x_2\ \ldots\ x_r)$, such that x_1 *is* mapped *to* x_2, x_2 *is* mapped *to* $x_3\ \ldots\ x_{r-1}$ *and* x_r is mapped *to* x_1 and any other element of X_n to itself. The length of a cycle is the number of distinct elements (points) which occur in the cycle.

Each cycle can be decomposed uniquely into disjoint cycles. A cycle which interchanges only two points and fixes the rest is called a transposition. Every permutation can be written as a product of transpositions, $g = (x_1\ y_1)(x_2\ y_2)\cdots(x_n\ y_n)$.

An element $g \in Sym(X_n)$ is said to be even if it can be expressed as a product of even number of transpositions and odd if it can be expressed as a product of odd number of transpositions. A $t -$ cycle can be expressed as a product of $t-1$ transpositions; a $t -$ cycle is an even permutation if it has odd length and is odd if it has even length. A transposition is odd while the identity element is even by convention.

The set of all even permutations on X_n forms a group called the alternating group and denoted by $A_n,\ A^x\ or\ A_n(x): A_n := \{g \in Sym(X): g\ is\ even\}$.

We state that $|Sym(X): A_n| = 2\quad or\ |A_n| = \frac{n!}{2}$ and A_n is a normal subgroup of $Sym(X)$. Two permutations $\alpha\ and\ \beta\ \ in\ S_n$ are conjugate in S_n if and only if they have the same cycle. The cyclic form of the permutations $g^{-1}xg$ is obtained by replacing each point α in the cyclic form of x by α^g. Thus if $x = (578)(321)\qquad g = (152)(743)\ \ then\ g^{-1}xg = (5g, 7g, 8g, 3g, 2g, 1g) = (248)(715)$

1.12 TRANSFORMATIONS

The analogue to the symmetric group S_n of all permutations of a set X_n is the full transformations semigroup T_n consisting of all mappings from X_n into X_n. The operation in both cases is composition of mappings. Simple combinatorics yields $|S_n| = n! \quad |T_n| = n^n$

1.13 GROUP HOMOMORPHISM (SEMIGROUP MORPHISM)

Let Ψ be a mapping from a set M into a set N denoted as $\Psi : M \to N \ or \ \Psi : M \to M\Psi \ where \ m\Psi \ or \ \Psi(m)$ is the image of an element inΨ. A homomorphism from a group M to a group N is a mapping $\Psi : M \to N$ such that $(m_1 m_2)\Psi = m_1\Psi\, m_2\Psi$ for all $m_1, m_2 \in M$. In that case Ψ is said to preserve the respective operations in M and N. In the sense that if operation in M and N are $\bullet$ and $*$ respectively, then $(m_1 \bullet m_2)\Psi = m_1\Psi * m_2\Psi$. A homomorphism of a group into itself is called an endomorphism.

Let $\Psi : M \to N$ be a homomorphism of groups. We define the kernel of $\Psi\,(written \ \ker\Psi)$ as $\ker\,\Psi := \{\, m \in M : m\Psi = 1\}$ and it is a normal subgroup of M. The image of Ψ is $im\Psi := \{m\Psi \in \mathrm{N} : m \in M\,\}$ is a subgroup of N. The $\ker\Psi = 1$ if and only if the homomorphism Ψ is a one to one mapping. Every homomorphism $\Psi : M \to N$ gives rise to a natural factor group namely $G/\ker\varphi$. It can easily be verified that if N is normal in M, then each factor group M/N gives rise to the natural homomorphism $\Psi : M \to M/N$ defined by $im\Psi = N_m$ for all $m \in M \ with \ \ker\Psi = N$.

Let the mapping $\Psi : M \to N$ be a bijective (one to one and onto) homomorphism, then $\Psi^{-1} : N \to M$ is also a homomorphism and Ψ is said to be an isomorphism denoted as $M \cong N$ read as M is isomorphic to N. If $M \cong N$, then the order of M *and* N is the same, and the identity $e' \in N$ is the image of identity $e \in M$.

We state without proof the three main isomorphism theorems.

<u>1.13.1 The First Isomorphism Theorem</u>

If $\Psi : M \to N$ is a homomorphism of groups then $M/\ker \varphi \cong im\varphi$.

<u>1.13.2 The Second Isomorphism Theorem</u>

Let M be a subgroup of G and N a normal subgroup of G. Then $NM \leq G, \quad N \cap M \lhd M \text{ and } \left({}^{NM}\!/_{M}\right) \cong M/M \cap N$.

<u>1.13.3 The Third Isomorphism Theorem</u>

Let G be a group. If N is normal in G and $N \leq M \lhd G$, then

${}^{M}\!/_{N} \lhd {}^{G}\!/_{N} \text{ and } \left({}^{G}\!/_{N}\right) / \left({}^{M}\!/_{N}\right) \cong {}^{G}\!/_{M}$

An isomorphism of a group G into itself is said to be an automorphism of the group G. The mapping $\Psi : M \to M$ given by $m\Psi = m$ for all $m \in M$, is an automorphism *iff* M is an Abelian group.

1.14 DIRECT PRODUCTS

Let M and N be any two groups, the (external) direct product of M and N denoted by $M \times N$, is the set of ordered pairs (m, n), $m \in M$ *and* $n \in N$, with coordinate wise multiplication

$$(m_1, n_1)\,(m_2, n_2) = (m_1\, m_2,\ n_1\, n_2), \quad m_1, m_2 \in M,\ n_1, n_2 \in N.$$

The unit element is $(1,1)$, the inverse of (m,n) is (m^{-1},n^{-1}). The new group is known as the direct product $M\times N$ and it is routine to verify the axioms of a group.

A group G is said to be decomposable if its subgroups M *and* N are such that every element of G is expressible as a product mn with $m\in M$ *and* $n\in N$; every element of M commutes with every element of N and $M\cap N=1$. If not, it is said to be indecomposable.

The correspondence $(m,n)\to(n,m)$ shows that $M*N$ *and* $N*M$ are isomorphic. Let M *and* N be normal subgroups of G such that $G=M*N$, the mappings $\Psi:G\to M$ and $\Phi:G\to N$ defined by $\Psi:(m,n)\to m$ *and* $\Phi:(m,n)\to n$ *for all* $(m,n)\in G$ then Φ *and* Ψ are surjective homomorphism called projection of G *onto* M *and onto* N respectively.

We say that $\ker\Psi=1*N$ *and* $\ker\Phi=M*1$ if it is a subgroup of G such that $H\Psi=M$ *and* $H\Phi=N$. In that case G, is said to be the sub-direct product of M *and* N.

1.15 COSET

Let H be a subgroup of a group G and $a\in G$. The subset $Ha:=\{ha:h\in H\}$ is called a right coset of H in G (or residue classes modulo the subgroup) generated by a. Left cosets of H in G are defined in an analogous way.

Any two left (right) cosets of H in G are either disjoint or identical. If $a,b \in G,\ Ha = Hb\ \ iff\ \ ab^{-1} \in H,$ we say that a is congruent to $b\,\mathrm{mod}ulo\,H,$ symbolically, we write $a \equiv b(\mathrm{mod}\ H)\ iff\ ab^{-1} \in H.$

The relation, congruency, is an equivalence relation. Therefore, it partitions G into disjoint equivalence classes. The equivalence classes corresponding to $a \in G$ is defined as, $[a] = \{x \in G \mid x \equiv a \bmod H\}$. The number of distinct right (left) cosets of H in G is called the index of H in G, and will be denoted by $|G:H|$ or $[G:H]$, if G is a finite group we have $|G:H| = |G|/|H|$.

By Lagrange's theorem, the order of a subgroup of a finite group G divides the order of the group, for which we can show that $|G:H| = \frac{|G|}{|H|}$

Equally, the order of an element of a finite group divides the order of the group.

1.16 Normal Subgroup

Let N be a subgroup of a group $G.$ The subgroup N is normal in G, denoted as $N \lhd G,$ if and only if $gN = Ng$ for all $g \in G$ or equivalently $g^{-1}Ng = N\ for\ all\ g \in G$. The normalizer of H in G is denoted by $N(H) := \{g \in G \mid H^g = H\} = \{g \in G \mid Hg = gH\} \leq G$. We call G simple if its only normal subgroups are the trivial subgroups $\{e\}\ and\ G$.

If H is normal in G then the set $G/_H = \{gH \mid g \in G\}$ is called the factor or quotient group of $G\ by\ H$. The product on the set is defined by the rule

$$g_1H\ g_2H = g_1\,g_2H\ \ for\ all\ g_1, g_2 \in G.$$

The identity element of $G/_H$ is $H \; and \; g^{-1}H$ is the inverse of gH.

Let $g, a \in G$ the element $a^{-1}ga = g^a$ is known as the conjugate of $g \; by \; a \;\; if \;\; a^{-1}ga = b$. Then b is said to be conjugate to $g \; and \; b$ is also called the transform of $g \; by \; a,$ written as $a \sim b.$ The relation $\sim$ partition G into equivalence classes, and conjugate elements have the same order. We write $C(a) \; or \; [a]$ for the set of all elements conjugate to $a \in G$ called the conjugacy classes of $a.$

We defined the conjugate subgroups of G as if $M \; and \; N$ are two subgroups of a group $G.$ In that case, N is said to be conjugate to M if there exist an element $x \in G$ such that $N = x^{-1}Mx.$

If $N = x^{-1}Mx,$ then N is called the transform of $M \; by \; x.$ We write $N \sim M \;\; if \;\; N$ is conjugate to M. The relation $\sim$ on the sets of subgroups of G is also an equivalence relation as in elements in $G.$

The centralizer of $g \; in \, G$ is defined by $C_G(g) := \{g \in G : y^{-1}gy = g\}$

If the conjugacy class of g consist of just $g,$ then g is known as a self conjugate element. $C_G(g) = \{g \in G \mid \forall x \in G, \quad x^{-1}gx = g\}$

There is a one-one correspondence between the conjugacy class of $g \; in \, G$ and the set of right cosets of the centralizer of G and $|Cl_G(g)| = |G : C_G(g)|$

$$C_G(H) := \{x \in G \mid xh = hx \;\; for \; all \; h \in H\}$$

$$:= \{x \in G \mid h^x = h \;\; for \, all \;\; x \in H\} = \cap\{C_G(x) \mid x \in H\}$$

is a subgroup of G. Indeed, $C_G(H) = \cap\{C_G(x) | \; x \in H\} \leq G.$

If $H = G$ then $C_G(H)$ is called the centre of G and it is denoted as $Z(G)$.

$$Z(G) := \{g \in G \mid gx = xg \quad \forall x \in G\}$$

1.17 p - GROUPS

Throughout this section, p-denotes a prime number.

Let G be a group, such that every element of G has prime power order for some fixed prime p, then G is called a p-group.

Lagrange's theorem assures that in a given group G, certain types of subgroups do not exist; it however, provides a necessary condition for the existence of a subgroup. In 1875 Sylow provides a sufficient condition for the existence in a group of subgroups of certain orders. Suppose H is a proper subgroup of G and $0(H) = n$, $1 < n < p$, then n cannot divide p. Thus a group of prime order can have no proper subgroup, e.g. the alternating group of degree 4, A_4 has no subgroup of order 6 although 6 divides 12.

Let G be a finite group, such that $|G| = p^r s$ and r a natural number where p is a prime and $(p,s) = 1$. Each subgroup of order p^r in G is called a Sylow p-subgroup of G and if N is any p-subgroup of G then $H \subseteq x^{-1}N x$ for some $x \in G$.

We state without proof the three Sylow theorems.

1.17.1 Sylow's first theorem

Let G be a finite non-abelian group and $|G| = p^r m \ and \ (p,m) = 1$. Then for each $n \in Z$ such that $0 \le n \le r$, G has a subgroup of order p^n.

Thus, $|G| = p^r$ for some r if and only if the order of every element of G is a power of p.

1.17.2 Sylow's second theorem

In a finite group the Sylow p-subgroups (for a fixed prime p) are all conjugate and are isomorphic.

1.17.3 Sylow's third theorem

In a finite group the number of Sylow p-subgroups (for a fixed prime p) is congruent to 1 modulo p.

1.18 GROUP ACTIONS ON GROUPS

Let $M \ and\ N$ be groups. We say that M acts on N as a group if to each $m \in M$ and each $n \in N$, there corresponds a unique element $m \in M$ such that

$(i)\ \left(m^{n_1}\right)^{n_2} = m^{n_1 n_2}\ (ii)\ m^1 = m\ \ (iii)\ \left(n_1 n_2\right)^m = n_1^m n_2^m\ \forall\ m, m_1, m_2 \in M\ and\ n, n_1, n_2 \in N$

Let $M\ act\ on\ N$ as groups, then for each $m \in M$, there corresponds an automorphism $\Psi : N \to N^m\ of\ N$ and the mapping $\Psi : M \to \Psi_m$ is a homomorphism of $M\ \text{int}\, o\ Auto(N)$. We call Ψ the automorphism representation of M or simply action.

1.19 BASIC COMBINATORICS

Combinatorics could be described as the art of arranging objects according to specified rule. We want to know, first, whether a particular arrangement is possible at all. If so, in how many ways can it be done?

Combinatorics depends on two elementary rules. (i) *Disjunctive (or Sum)* rule; if $E_i(i = 1, 2, \ldots, k)$ are k events such that no two of them can occur at the same time, and if E_i can occur in n_i ways, then one of the k events can occur in $n_1+n_2+\ldots+n_k$ ways. (ii) Sequential or Product Rule; if an event can occur in m ways and a second event in n ways, and if the number of ways the second event occurs does not depend upon how the first event occurs, then the two events can occur simultaneously in mn ways. More generally, if $E_i\,(i=1,2,\ldots,k)$ are k events and if E_i can occur in n_1 ways, E_2 can occur in n_2 and E_k can occur in n_k ways (no matter how the previous $k-1$events occur), then the k events can occur simultaneously in $n_1\,n_2\,n_3\ldots n_k$ ways.

1.20 THE BINOMIAL THEOREM

Let n and k be non-negative integers, with $0\le k\le n.$ *T*he binomial coefficient $\binom{n}{k}$ is defined to be the number of $k-$element subsets of a set of n elements. This numbers is often written as ${}^nC_k$ or $\binom{n}{k}$ and read as n choose $k.$ It is called a binomial coefficient.

$$\binom{n}{k}=\frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots1}=\frac{n!}{k!(n-k)!}$$

where, $\binom{n}{0}=1$ is the empty set and $\binom{n}{n}=1.$

1.21 PERMUTATIONS AND COMBINATIONS

The number of selections of k objects from a set of n objects where repetition is allowed and order is significant is given by $n^k.$ If the order is not significant, it is given by $\binom{n+k-1}{k}.$

If the repetitions is not allowed and order is significant it is given by $n(n-1)\ldots(n-k+1)$. But if the order is not significant, it is given by $\binom{n}{k}$.

1.22 RECURRENCE RELATIONS AND GENERATING FUNCTIONS

1.22.1 Recurrence Relation

If $\langle a_0, a_1, \cdots, a_k, \cdots\rangle$ is a sequence of real numbers such that there is an equation relating to the term a_n $(for\ any\ n \geq n_0)$ to one or more of its predecessors in the sequence, then this equation is a recurrence relation obeyed by the sequence. For example, the sequence $\langle 0!, 1!, 2!, \cdots\rangle$ satisfies the recurrence relation $a_n = na_{n-1}$ $(n \geq 1)$.

Conversely, given this relation and the initial condition $a_0 = 1$, one can recover the entire sequence by iteration.

$$a_n = n[(n-1)a_{n-1}] = [n(n-1)(n-2)a_{n-3}] = \cdots = n(n-1)\cdots(1) = n!$$

The recurrence relation;

$$a_n = c_1 a_{n-1} + c_1 a_{n-1} + \cdots + c_1 a_{n-r} + f(n)$$

In which, C_i $(i = 1, 2, \ldots, r)$ are constants, with $C_i \neq 0$, is called a linear recurrence relation with constant coefficients of order r.

1.22.2 Generating Function

The sequence of real numbers $\langle a_o, a_1, a_2, \ldots\rangle$ and a dummy variable x, have ordinary generating functions as $g(x) = a_0 + a_1 x + a_2 x^2 + \ldots$ and exponential generating function as $G(x) = a_0 + a_1 \frac{x}{1!} + a_2 \frac{x^2}{2!} + \ldots.$

1.23 SOME SPECIAL NUMBERS

1.23.1 Bell Numbers

The Bell numbers B_n is the number of partitions of an n-set or the number of equivalence relations on an n-set (if R is an equivalence relation on X, then the equivalence classes of R form a partition of X and the converse is also true).

The recurrence and generating functions for Bell numbers is given by

$$B_n = \sum_{k=1} \binom{n-1}{k-1} B_{n-k}, \; for \; n \geq 1, \quad e^{x-1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n, \; for \; n \geq 1$$

1.23.2 Fibonacci numbers

In his book "Liberabaci" which appeared in 1202, the Italian mathematician Fibonacci gives this problem (the Rabbit Problem):

How many pairs of rabbit can be produced from a single pair in a year if every month each pair begets a new pair which from the second month on becomes productive?

Let us denote by $F(n)$ the number of pairs after n months starting from the beginning of a year. We see that in $n+1$ months there will be $F(n)$ pairs and as many more newly born pairs as there were at the end of the month $n-1$, which is to say, $F(n-1)$ pairs of rabbits. In other words, we have the recurrence relation

$$F(n+1) = F(n) + F(n-1) \; or \; F_{n+1} = F_n + F_{n-1}$$

Since, by hypothesis, $F(0)=1$ and $F(1)=2$.

We find, in succession, $F(2)=3$, $F(3)=5$, $F(4)=8$, etc. In particular, $F(12)=377$.

The numbers $F(n)$ are called Fibonacci numbers.

Fibonacci sequence $\langle 1, 2, 3, 5, 8, \ldots \rangle$, is defined by the recurrence relation

$$f_n = f(n-1) + f(n-2) \text{ or } f_n = f_{n-1} + f_{n-2}$$

Such that $f(0) = f(1) = 1$

Thus, the ordinary generating function of Fibonacci sequence is

$$\sum_{n=2}^{\infty} f(n)x^n = x\sum_{n=2}^{\infty} f(n-1)x^{n-1} + x^2\sum_{n=2}^{\infty} f(n-2)x^{n-2}$$

The Catalan and Bell numbers are two important sequences of numbers. They have several, apparently accidental, common properties.

1.23.3 The Catalan Numbers

The Catalan Numbers are $1,\ 2,\ 5,\ 14,\ \ 42,\ \ldots$ and appear in many guises. For example, in how many ways can sums of n terms be bracketed so that it can be calculated by adding two terms at a time? (Five possibilities)

The recurrence relations for the Catalan numbers is given by

$$C_n = \sum_{i=1}^{n-1} C_i \ \ C_{n-i}, \quad n > 1.$$

Here $C_n(1 \le i \le n)$ is the number of ways of bracketing a sum of n terms.

The Catalan numbers C_n is $C_n = \frac{1}{n}\binom{2n-1}{n-1}$,

The generating functions for Catalan numbers is given as

$$C(x) = C_0 + C_1x_1 + C_2x_2 + \cdots$$

1.23.4 Sterling Numbers

Let n *and* k be positive integers with $k \leq n,$ the sterling number of the first kind, $s(n,k)$ is defined by the rule that $(-1)^{n-k} s(n,k)$ is the number of permutations of $\{1, 2, \ldots, n\}$ with k-cycle.

The sterling numbers of the second kind $S(n, k)$ is the number of partitions of $\{1, \ldots, n\}$ with k (non-empty) parts.

The recurrence relation is given by $S(n+1,k) = S(n,k-1) - nS(n,k)$ such that $S(n,0) = S(n,1) = 0$ *for all n.*

1.23.5 Proposition

(a) $\sum_{k=1}^{n}(-1)^{n-1} S(n,k) = \sum_{k=1}^{n}|S(n,k)| = n!;$ (b) $\sum_{k=1}^{n} S(n,k) = B_n,$ n^{th} Bell numbers.

$S(n,n) = S(n,k) = 1, S(n+1,k) = -nS(n,k) + S(n,k-1), and\ S(n+1,k) = kS(n,k) + S(n,k-1)$

1.24 DERANGEMENTS

A derangement of $\{1, 2, \ldots, n\}$ is a permutation of this set which leaves no point fixed. Let $d(n)$ be the number of derangements of $\{1 ,\ldots, n\}$. Any derangement moves the point n to some point $i < n$ (fixed no point of n). Thus, $d(n)$ is given as three terms recurrence relation.

$$d(n) = (n-1)d(n-1) + d(n-2). \quad d(0) = 1,\ d(1) = 0.$$

$$d(n) = n!\left(\sum_{i=0}^{n}\frac{(-1)^i}{i!}\right)$$

This is the nearest integer to $\frac{n!}{e}$ $for\ n \geq 1,$ where e is the base of natural logarithms.

CHAPTER TWO
LITERATURE REVIEW

2.1 TRANSITIVE PERMUTATION GROUPS

Let G be a permutation group on Ω and Δ a subset of Ω, Δ is said to be a fixed block of G if $\Delta^G = \Delta \ or \ \Delta \cap \Delta^G \neq \phi$.

The union and intersection of any two fixed blocks is a fixed block. Every group $G \ in \ \Omega$ has two trivial fixed blocks $\phi \ and \ \Omega$

2.1.1 Orbit 0f $\alpha \ in \ G$

The fixed block $\Delta \neq \phi$ is called an orbit or set of transitivity of G on Ω, denoted by $\alpha^G \ or \ \alpha G$, where αG is defined as

$$\alpha^G := \{\alpha^g \mid g \in G\}, \ \alpha \in \Omega$$

A group G acting on a set Ω is said to be a transitive permutation group if it has only one orbit i.e. $\alpha^G = \Omega$.Thus, for all $\alpha, \beta \in \Omega$ there exists $g \in G$ such that $\alpha^g = \beta$. A group which is not transitive is called intransitive. A group G acting transitively on a set Ω is said to act regularly if $\alpha^G = 1$ for each $\alpha \in \Omega$, that is only the identity fixes any point. The number of elements in α^G is called the length of the orbit.

A relation $\sim \ in \ \Omega$ defined by the rule, $\alpha \sim \beta \Rightarrow \alpha^g = \beta \ \forall g \in G$, $\alpha, \beta \in \Omega \ with \ \alpha g = \beta$ is an equivalence relation.

The orbits of G partition Ω, for let $\Delta_1, \Delta_2, \Delta_3, \ldots, \Delta_S$ be the orbits of $G \ on \ \Omega$ then G induces a permutation group G^Ω on Δ and Δ is a disjoint union of orbits $\Delta = \bigcup_{i=1}^{s} \Delta_I$. Moreover, $G \leq \prod_{i=1}^{s} G^{\Delta_I}$ and we say that G is a direct product of the groups $G^{\Delta_1}, G^{\Delta_2}, \ldots, G^{\Delta_S}$. If also, each G^{Δ_I} $(i = 1, 2, \ldots, s.)$ is isomorphic to a group H (possibly $H \leq G$). We say that G is a sub-direct product of H.

A subset $\Delta \, of \, \Omega$ is said to be $G-$invariant if for all $g \in G, \; \beta \in \Delta$ and $\beta^g = s$ implies $\beta^g \in \Delta$

2.1.2 Some Properties of Orbits $\alpha^G \; in \; G$

1. Each point $\alpha \in \Omega$ lies in exactly one orbit $\Delta \; of \; G, \; \Delta = \beta^G$.
2. Two points $\alpha \neq \beta$ lies in the same orbit β^G if and only if $\alpha = \beta^g$ for some $g \in G$.
3. Let $\alpha, \beta \in \Omega. \; If \; \beta \in \alpha^G, \; then \; \alpha^G = \beta^G. \; Otherwise \; \beta^G \cap \alpha^G = \phi..$
4. A non-empty subset $\Delta \; of \; \Omega$ is an orbit *iff* it is a minimal $G-$invariant subset.
5. Any G invariant subset of Ω is a disjoint union of orbits.

2.1.3 Stabilizer of $\alpha \in \Omega \; in \; G$

Let $g \in G$ and $\alpha \in \Omega.$, the stabilizer of $\alpha \; in \; G$, denoted as G_α is defined as

$$G_\alpha = \{g \in G \mid g\alpha = \alpha\}$$

The set of elements of G which fix a specified point $\alpha \; in \; \Omega..$

2.1.4 Some Properties of $G_\alpha, \; of \; \alpha \; in \; G$

1. The stabilizer $G_\alpha \; of \; \alpha \; in \; G$ is a subgroup of G.

2. $\left|\alpha^G\right| = \left|G : G_\alpha\right|$ where α^G is the orbit containing α, $\left|G : G_\alpha\right|$ is the index of G_α *in* G, *and* G is transitive, then $\left|\alpha^G\right| = \left|\Omega\right| = n = \left|G : G_\alpha\right|$

3. Let $\alpha \in \Omega$ *and* $h, k \in G$ *then* $\alpha^h = \alpha^k$ *iff* $hk^{-1} \in G_\alpha$.

4. If $\alpha^h = \beta, \alpha \in \Omega$, $h \in G$ *then* $G_\alpha = G_\beta$ implies that $h^{-1}G_\alpha h = G_\beta$,

5. $\left|\alpha^G\right|\left|G\right| = G_\alpha$, $\left|G\right| = n$.

<u>2.1.5 The Transitive Constituents</u> G^Δ

Let G be a permutation group on Ω, $G \leq Sym(\Omega)$. We say that a set $\Delta \subseteq \Omega$ is a fixed block of G or is fixed by G if $\Delta^G = \Delta$ *or* $\Delta^G \cap \Delta = \phi$.

Then each $g \in G$ induces a permutation on Δ which is denoted by g^Δ. We call the totality of g^{Δ}`s formed for all $g \in G$ the constituent G^Δ *of* G *on* Δ $(e.g.\, G = G^\Omega)$. clearly, G^Δ is a permutation group on Δ.

2.2 REGULAR AND SEMI-REGULAR GROUPS

A permutation group G *on* Ω is called semi-regular if for each $\alpha \in \Omega$ we have that $G_\alpha = 1$.

Thus, a faithful $G - set$ is regular if it is transitive and only the identity of G has fixed points (that is $G_\alpha = 1$)

1. Every regular group is also semi-regular; subgroups and constituent of semi-regular groups are semi-regular. The identity element is semi-regular.

2. In semi-regular groups all orbits have the same length and the length is the order of G, for $\left|\alpha^G\right|\left|G_\alpha\right| = \left|G\right|$. *If* $G_\alpha = 1$ *then* $\left|\alpha^G\right| = \left|G\right|$ (Wielandt, 1964).

3. If a Semi-regular group G of order n has m orbits then $m|G_a| = n.$

4. Caley Representation of a permutation Group G. Every transitive Abelian group is regular and G is its own centralizer.

5. The centralizer of every semi-regular group is transitive.

2.3 THE SUBGROUPS $G_{(\Delta)}$ and $G_{\{\Delta\}}$.

Let the group G acts on a set Ω *and* $\Delta \subseteq \Omega,$ we define the point wise stabilizer $G_{(\Delta)}$ *of* Δ as

$$G_{(\Delta)} = \{g \in G : \alpha g = \alpha \quad \forall\, \alpha \in \Delta\}$$

The set wise stabilizer of Δ is defined as

$$G_{\{\Delta\}} = \{\, g \in G : \alpha g \in \Delta \quad \forall\, \alpha \in \Delta\}$$

2.3.1 Some Properties of $G_{(\Delta)}$ *and* $G_{\{\Delta\}}$

(1) $G_{(\Delta)}$ *and* $G_{\{\Delta\}}$ are subgroups of G .

(2) $G_{(\Delta)}$ is normal in G.

(3) The factor group $G/G_{(\Delta)}$ is the group of permutations induced by G *on* Δ

2.3.2 Burnside Lemma (wielandt, 1964)

Burnside found the number of orbits in the action of G *on* $\Omega,$ although the work originated from Cauchy in 1845 and Frobenius in 1887.

Let the group G act on a finite set $\Omega,$ the number of orbits say n *of* G in the action of G on a finite set Ω is given by

$$n = \frac{1}{|G|} \sum f(t),$$

where $f(t)$, is the number of points of G fixed by α, $f(t)=\{\alpha \in \Omega : \alpha^{g}=\alpha\}$ set of fixed points of G.

Let G be a transitive permutation group on Ω, the number of orbits $n(\alpha)$ *of* G_{α} *in* Ω is given by

$$n(\alpha)=\frac{1}{|G|}\sum_{g\in G} f^{2}(g)$$

and it is called the rank of the transitive group G *on* Ω.. If the permutation group G is semi-regular then $n(\alpha)=\frac{1}{|G|}n$

2.4 PRIMITIVE GROUPS

A subset Δ *of* Ω is said to be a set of imprimitivity (Blocks) if for each $g \in G$ either $\Delta^{g}=\Delta$ *or* Δ^{g} *and* Δ are disjoint. The set $\{1\}$ and the empty set $\{\phi\}$ are called the trivial sets of imprimitivity.

Let G be a transitive permutation group. If G has only non-trivial blocks then G is said to be an imprimitive group. Otherwise it is primitive on Ω.

2.4.1 Some Properties of Primitive Permutation Groups

1. If $|\Omega|=|G|$ then G is a trivial group.
2. Every doubly transitive group G is primitive.
3. Let $\alpha \in \Omega$, $|\Omega|>1$. A transitive group G *on* Ω is primitive if and only if G_{α} is a maximal subgroup of G.
4. If G is primitive on Ω and $\alpha \neq \beta \in \Omega$, then either $G_{\alpha} \neq G_{\beta}$ *or* G is a group of prime degree or equivalently $G=\langle G_{\alpha}, G_{\beta}\rangle$.

5. Every transitive permutation group of prime degree is primitive.

2.5 MULTIPLY TRANSITIVE GROUPS

Let G be a permutation group on Ω and k a natural number with $1 \leq k \leq n = |\Omega|$. We say that $G\ is\ k-ply$ transitive or $k-fold$ transitive $(on\ \Omega)$ if for every two k tuples $\alpha_1,\ldots,\alpha_k$ and $\beta_1, \ldots, \beta_k$ of points of Ω $(with\ \alpha_i \neq \alpha_j,\ \beta_i \neq \beta_j\ for\ i \neq j)$, there exists $g \in G$ which takes α_i $\operatorname{int} o$ β_i $(i = I,\ldots,k)$. The transitive group introduced in 2.1 is the same as 1-fold transitivity. We call a group multiply transitive if it is at least 2-transitive. Every $(k+1)-fold$ transitive group is also $k-fold$ transitive. Every group having a $k-fold$ transitive subgroup is itself $k-fold$ transitive.

Whereas there are numerous nontrivial doubly and triply transitive groups, only two nontrivial quadruply transitive and two nontrivial quintuply transitive groups are known (Mathew, 1861, 1873).Their degrees are 11, 23 and 12, 24 respectively. It is not known if there are nontrivial $k-fold$ transitive groups for $k > 7$ (Dixon, 1996).

2.6 CLASSIFICATION OF TRANSITIVE GROUPS

The problem of classifying subgroups of the symmetric group is one of the oldest problems of group theory; it is in fact the subject of the 1858 prize question of the Academic des sciences: Academic des sciences (1857):

By the beginning of the 20th century, a series of articles had appeared which classified the transitive groups up to degree 15. The classification for the higher degree culminates in the papers of Cole (1895), miller (1896, 1898) and Kuhn (1904). A full history of these endeavors can be found in Short (1992, Appendix A, pp. 122-124).

With the advent of computers, starting in the early 1980's the classifications up to degree 15 were redone by Butler and McKay (1983), Royle (1987), Butter (1993).

A complete list of these groups with names and properties can be found in Conwey et al. (1998).

2.7 CLASSIFICATION OF PRIMITIVE GROUPS

The primitive groups up to degree 17 were already classified by Jordan (1872). Sims (1970) published a list up to degree 20 and later extended it up to degree 50. Solvable primitive groups of degree <256 were classified by Short (1992), Eick and Halfling (2003) classified all affine groups of degree up to 1000.

The O'Nan-Scoh theorem, Scoh (1980) gave the classification of finite simple groups (Gorenstein,1982) essentially reduced the problem of classifying primitive groups to the classification of maximal subgroups of simple groups and to the problem of classifying irreducible matrix groups.

Dixon and Martimer (1988) classified the non-affine primitive groups up to degree 999. This classification was made explicit by Thieben (1997), which also gives the non-soluble affine groups up to degree 255. The techniques used do not stop at this degree but should be able to classify primitive groups up to several thousands if such a classification was desired.

In particular, a classification of transitive groups only needs to classify the imprimitive groups.

2.8 CONSTRUCTING TRANSITIVE PERMUTATION GROUPS

Alexander Hulpke (1999) presented a new algorithm to classify all transitive subgroups of the symmetric group up to conjugacy. It has been used to determine the transitive groups of degree up to 30.

In his article, Hulpke described a method to construct the transitive groups of given degree n. That is to classify the transitive subgroups of S_n up to conjugacy. The algorithm has been used successfully to verify the lists of groups of degrees up to 15 and to construct the hitherto unclassified groups of degree 16-30. These calculations were done in computer algebra system GAP 4(GAP, 2002).

2.9 TRANSITIVE $p-$ GROUPS OF DEGREE p^m

Let p be a prime number. The classification of transitive $p-$groups of degree p^m $(m \geq 2)$ when the group is abelian is well-known.

We state, without proof, the result in the Lemma which follows:

2.9.1 Lemma (Audu, 1988b)

If $\pi(m)$ is the number of partitions of the natural number m then there are, up to equivalence, $\pi(m)$ different number of faithful transitive $p-$groups of degree p^m whose centre has order p^m.

For non-abelian transitive $p-$groups of degree p^2, we have the following:

2.9.2 Theorem (Audu, 1988c)

There are $(2p-1)$ different $p-$groups of G of order p^2. Two of these are Abelian of the $(2p-3)$ non-Abelian Group, we have that $(p-2)$ of them have exponent p while the remaining $(p-1)$ of them have exponent p^2. As such the groups are distinguishable by their exponent and order.

Apine, (2000) classified transitive and faithful $p-$groups of degree p^3 whose centre is elementary abelian of rank two.

2.10 CLOCKWISE (ANTI-CLOCKWISE) ORIENTATION

Let $X_n = \{1, 2 ,..., n\}$ be a set with standard ordering. A map $\alpha : X_n \to X_n$ is order decreasing if $x\alpha \leq x$, for all x in X_n. If $x \leq y \Rightarrow x\alpha \leq y\alpha$, then α is said to be order preserving for all x, y in X_n. Let $A = (a_1, a_2, ..., a_s)$ be a finite sequence from the chain X_n. We say that A is cyclic or has clockwise orientation if there exist not more than one subscript i such that $a_i > a_{i+1}$ where a_{s+1} denotes a_1. We say that $A = (a_1, a_2, ..., a_s)$ is anti-cyclic or has anticlockwise orientation if there exists no more than one subscript i such that $a_i < a_{i+1}$. Note that a sequence A is cyclic if and only if A is empty or there exist $i \in \{0,1,...,s-1\}$ such that $a_{i+1} \leq a_{i+2} \leq \cdots \leq a_s \leq a_1 \leq \cdots \leq a_i$, is unique unless the sequence is a constant.

2.10.1 Remark

(i) Let A be any cyclic (anti-cyclic) sequence. Then A is anti-cyclic (cyclic) if and only if A has no more than two distinct values.

If $A = (a_1, a_2, ..., a_t)$ is any sequence then we denote by A^r sequence

$(a_t, a_{t-1}, \ldots, a_1)$, Called the reversed sequence of A.

(ii) Let $A = (a_1, a_2, \ldots, a_t)$ be any sequence from X_n. Then A is cyclic (anti-cyclic) if and only if A^τ is anti-cyclic (cyclic).

(iii) If $(a_1, a_2, \ldots, a_t)$ is a cyclic (anti-cyclic) then, so is

(a) The sequence. $(a_{i_1}, a_{i_2}, \ldots, a_{i_r})\ (i_1 < i_2 < \cdots < i_r)$

(b) $(a_j, a_{j+1}, \ldots a_t, a_{1,} \ldots, a_{j-1})$ *for all* $1 \le j \le t.$

(iv) For non-constant $\alpha \in OP_n, \alpha$ is an order-preserving mapping if and only if $1\alpha < n\alpha$.

2.11 ORIENTATION PRESERVING (REVERSING) MAPPINGS

Catarino and Higgins (1999) introduced a new subsemigroup of X_n containing O_n which is denoted by OP_n and its element are called orientation preserving mappings. Also, they introduced a semigroup $P_n = OP_n \cup OR_n$ where OR_n denotes the collection of all orientation reversing mappings. Fernandes (2000) studied the monoid of orientation preserving partial transformations of a finite chain, concentrating in particular on partial transformations which are injective. He study several structural properties of the monoids of all injective orientation preserving partial transformations on a chain $POPI_n$. He establishes descriptions for the ideals and for the congruencies of these monoids and show that $POPI_n$ is a 2-generated semigroup, for all $n \in \mathrm{N}$. He finally gives a presentation for these monoids.

2.11.1 Orientation Preserving Mapping

Let $\alpha \in T_n$, we say that α is orientation-preserving mapping on X_n if the sequence $(1\alpha, 2\alpha, \cdots, n\alpha)$ is cyclic. From 2.10 above, this sequence is then cyclic with respect to $\leq_k$ for all $0 \leq k \leq n-1$. The collection of all orientation-preserving mapping on X_n will be denoted by OP_n.

2.11.2 Lemma (Fernandes, 2000)

Let $\alpha \in OP_n$ and $(b_1, \cdots, b_t)$ be a cyclic sequence of members of X_n. The sequence $(b_1\alpha, \cdots, b_t\alpha)$ is also cyclic.

2.11.3 Remark

Catarino and Higgins (1999) regarded the members of X_n as being placed clockwise around the circumference of a circle so that the integer i lies between $i-1$ *and* $i+1$ (reduced modulo n) any sequence of 3 distinct members (i, j, k) is cyclic or anti-cyclic. Let $\alpha \in OP_n$ *and* (i, j, k) be any triple of 3 distinct members of X_n. If the entries are distinct, then the triple $(i\alpha, j\alpha, k\alpha)$ defines the same orientation as (i, j, k).

2.11.4 Lemma (Catarino and Higgins, 4.6, 1999)

Every $\alpha \in O_n$ has fixed point.

Proof

Let $\alpha \in O_n$ and $A = \{x \in X : x \leq x\alpha\}$. Note that $1 \in A$ *and so* A is not-empty. Let $a = \max A$. Hence $a \leq a\alpha$ as $a \in A$, and $a\alpha \leq a(a\alpha)$ as $\alpha \in O_n$. Thus $a\alpha \in A$ and $a\alpha \leq a$ by maximality of a, therefore $a = a\alpha$ as required.

2.11.5 Lemma (Catarino and Higgins, 4.7, 1999)

Let $\alpha = a^k f a^k$ where $f \in O_n$ and $0 \leq k \leq n-1$. Then $x \in f(\alpha)$ if and only if $x - k \in F(f)$. In particular, if $x \in H$, then $\mathrm{F}(\alpha) \neq \phi$.

2.11.6 Remark

Catarino and Higgins (1999) gave some results on the fixed point of OP_n, we list some of the results as in Lemma 4.7, 4.8 & theorem 4.9 of Catarino and Higgins (1999). Let $\alpha \in OP_n$. then;

(i) The diagraph of α cannot have a non-trivial cycle and a fixed point.

(ii) Let $\alpha \in OP_n$, the diagraph of α cannot have two cycles of different length.

(iii) Let $\alpha \in OP_n$ if $F(\alpha) \neq \phi$ then the diagraph of α is a forest and each component C associated with α is a fixed point of α is an interval.

(iv) Let $\alpha \in OP_n$, such that $F(\alpha) \neq \phi$. Let C be any component of α, then $C\ \alpha \subseteq C$, there exist $i, j \in X$ such that $c = [i, j]$, *and* α restricted to c is an order preserving with respect to $\leq_{i-1}$.

2.11.7 Orientation-Reversing Mapping

Let $\alpha \in T_n$, we say α is an orientation-reversing mapping on X_n if the sequence $(1\alpha, 2\alpha, \cdots, n\alpha)$ is anti-cyclic, the collection of all orientation-reversing mappings on X_n is denoted by OR_n.

Let $\gamma \in OR_n$, γ is a reflection where by $i \to n + i - 1(i \in X)$. and $(1\gamma, 2\gamma, \ldots, n\gamma) = (n, n-1, \ldots, 1)$ for $\gamma \in OR_n$ is anti-cyclic.

2.11.8 Remark

If Γ_λ, Γ_γ are involutions in T_n which map OP_n *onto* OR_n and OR_n *onto* OP_n, then $(OR_n)^2 = (OP_n)^2 = OP_n$, $P_n = OP_n \cup OR_n$ is a submonoid of T_n

$OP_n \cup OR_n = \{\alpha \in OP_n : |X| \le 2\}.$

<u>2.11.9 Lemma</u> (Catarino and Higgins, 5.2, 1999)

Let $\alpha \in OP_n$ be such that $|X_\alpha| = t$ *for some* $3 \le t \le n$ and H_∞ be the class H class containing ∞. Then $|H_\infty| = 2t$

<u>2.11.10 Theorem</u> (Catarino & Higgins, 5.9, 1999)

For $t \ge 3$ the maximal subgroups of $D_t^{o_n}$ are the dihedral groups of order $2t$.

2.12 COMBINATORIAL PROPERTIES OF TRANSFORMATION SEMIGROUPS AND SYMMETRIC GROUPS

Let the binomial coefficient $\binom{n}{r}$ be denoted as $C(n,r)$. Higgins (1992a) presented the following results

(i) $\sum_{k=0}^{n} c(n,k)c(m,k) = c(m+n,\ k)$ *for* $n \le m$

(ii) $\sum_{k=0}^{n} c(2k,k)c(2n-2k,n-k) = 4^n$

(iii) $\sum_{k=1}^{n} C_{k-1}C_{n-k} = C_n$

Gomes and Howie (1987) were the first to study PO_n (excluding the identity map) and among other things they computed the order of PO_n as

$$|PO_n| = \sum_{r=0}^{n} \binom{n}{r}\binom{n+r-1}{r}$$

However, from the computational point of view, this result is not satisfactory if one were to compute higher orders of PO_n. In view of this, Laradji and Umar (2007) computed the order of $PC_n \, as \, \gamma_n$, the double Schroeder number, also obtain the recurrence.

$$f(n,r,k) = \left|\{\alpha \in PO_n \middle| \; |Dom\alpha| = r \wedge \max(\operatorname{Im}\alpha) = k\}\right|$$

They defined $f(n,r,k)$ in terms of I_n as

$$or = \left|\{\alpha \in I_n : \; |im\alpha| = r(= Dom\alpha) \wedge \; f(\alpha) = k\}\right|$$

$$f(n,o,k) = \begin{cases} 1 & k = 0 \\ 0 & k > 0 \end{cases}$$

$$f(n,r,0) = \begin{cases} 1 & r = 0 \\ 0 & r > 0 \end{cases}$$

and $f(n,r,1) = \binom{n}{r}(1 \le r \le n)$, $f(n,r,k) = \binom{n}{k} f(n-k, \; r-k, 0)$.

We have $f(n,r,k) = \binom{n}{r}\binom{k+r-2}{k-1}$ $for \; n \ge 0, \, k > 0$

For a given (partial) mapping or transformation $\alpha : y \subseteq X \to X.$, we denote the set of fixed points by $f(\alpha) = \{x \in y : x\alpha = x\}$ its Domain $Y \; by \; Dom\alpha$ and its image set by $\operatorname{Im}\alpha.$

Let $f(n,n)$ be the number of derangements of an $n-$element set, and it is well known that

$$f(n,n) = (n-1)f(n-1, \; n-1) + f(n-2, \; n-2) = nf(n-1, \; n-1) + (-1)^n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}$$

with $f(n,r) = 1$. However, $f(n,r)$ may also be expressed as

$$f(n,r) = \binom{n}{r} C(n,r)$$

where $C(n,r)$ is the number of partial one to one mapping without fixed points and having a fixed domain, say $\{x_1, x_2, \ldots, x_r\} \le X_n$ *and* $c(n,0)=1$ *and* $c(n,n)= f(n,n)$ generally we have:

2.12.1 Proposition (Laradji and Umar, 2004b)

$$C(n,r) = rC(n-1,\, r-1) + C(n-1,\, r)\ (1 \le r < n)$$

$$C(n,r) = r!\sum_{m=0}^{r}\binom{n-m}{r-m}\frac{(-1)^m}{m!} \quad (0 \le r < n)$$

Laradji and Umar (2006) obtain the generating function a_n of symmetric inverse semigroup, such that

$$a_n = n!\sum_{m=0}^{n}\frac{(-1)^m}{m!}\ \lambda_{n-m}\,, \qquad f(x) = \sum_{n\ge 0} a_n \frac{x^n}{n!} = \frac{e^{\frac{x^2}{1-x}}}{1-x}\,.$$

2.12.2 Proposition

Let $f_k(x)$ be the exponential generating function for

$$a_{n,k} = \binom{n}{k} a_{n-k} \ \textit{then}\ \ f(x) = \frac{x^k e^{\frac{x^2}{1-x}}}{k!(1-x)}$$

CHAPTER THREE
RESULTS

3.1 RESULT ONE

SOME COMBINATORIAL PROPERTIES OF THE ALTERNATING GROUP

Let $X_n = \{1, 2, \ldots, n\}$ be a finite n-element set and let $S_n, I_n,$ *and* A_n be as defined, the combinatorial properties of S_n have been studied over long period and many interesting results have emerged. In particular, the number of permutations of (X_n) having exactly k fixed points and their generating functions are known.

In this section we obtain and discuss formulae for the number of even permutations (of an n-element set) having exactly k fixed points. Moreover, we obtain generating functions for these numbers. We also obtain similar results for the number of odd permutations.

We list some combinatorial results, (some may be found in chapter two and one), that we shall need later in our proofs.

<u>3.1.1 Result</u>

Let d_n be as defined. Then

$$d_n = n!\sum_{i=0}^{n}\frac{(-1)^i}{i!} = (n-1)(d_{n-1} + d_{n-2}) = nd_{n-1} + (-1)^n, where\ d_0 = 1$$

3.1.2 Result

The principle of inclusion-exclusion says that

Suppose that X_n is some set of objects and P is a set of properties. For $R \subseteq P$, let $N_=(R)$ be the number of objects in X_n that have exactly the properties in R and non of the properties in $R \subseteq P$,

$$\mathrm{N}_=(R) = \sum_{R \subseteq Q \subseteq P} (-1)^{|Q/\ R\ |} N \geq (Q),$$

3.1.3 Result

Let A_n and n are as defined in chapter one, then,

$$A_n = \frac{n!}{2}(n \geq 2), where\ |A_0| = 1 = |A_1|.$$

3.1.4 Result

Let $d(x,k) = \sum_{n \geq 0} \frac{d(n,k)}{n!} x^n$. Then $d(x,k)$ converges for $|x| < 1$ to the functions $\frac{x^k e^{-x}}{k!(1-x)}$.

3.1.5 Corollary

Let $d(x) = \sum_{n \geq 0} \frac{d(n)}{n!} x^n$. Then $d(x)$ converges for $|x| < 1$ to the function

$$\frac{e^{-x}}{(1-x)}.$$

3.2 EVEN AND ODD PERMUTATIONS

We defined the number of k fixed points in an even permutation of n-elements.

$$e(n,k) = |\{\alpha \in A_n : f(\alpha) = k\}|, \tag{3.1}$$

where $f(\alpha) = |\{x \in X_n : x\alpha = x\}|$. Then it is not difficult to see that

$$e(n,k) = \binom{n}{k} e(n-k,0) = \binom{n}{k} e_{n-k}. \qquad (3.2)$$

Thus to compute $e(n,k)$ it is sufficient to compute $e\,(n,0) = e_n$. However, note that e_n is the number of even permutations without fixed points; that is, the number of even derangements. Now we have

3.2.1 Theorem

Let e_n be as defined in (3.2). Then $e_o = 1, e_1 = 0,$ and for all $n \geq 2,$ we have

$$e_n = \frac{n!}{2} \sum_{i=0}^{n-2} \frac{(-1)^i}{i!} + (-1)^{n-1}(n-1).$$

Proof

By the Inclusion-Exclusion Principle we see that

$$e_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} |A_{n-i}| = \sum_{i=0}^{n-2} (-1)^i \binom{n}{i} |A_{n-i}| + (-1)^{n-1} n + (-1)^n$$

$$= \sum_{i=0}^{n-2} (-1)^i \frac{n!}{(n-i)!i!} . \frac{(n-i)!}{2} + (-1)^{n-1}(n-1)$$

$$= \frac{n!}{2} \sum_{i=0}^{n-2} \frac{(-1)^i}{i!} + (-1)^{n-1}(n-1).$$

The number e_n satisfies some recurrence similar to those of d_n in Result 3.1.1

3.2.2 Proposition

Let e_n be as defined in (3.2). Then

$(a)\ e_n=(n-1)\left(e_{n-1}+e_{n-2}+(-1)^{n-1}(n-1)\right),\quad e_0=1,\ e_1=0;$

$(b)\ e_n=ne_{n-1}+(-1)^{n-1}(n-2)(n+1)/2,\quad e_0=1.$

Proof

(a) Using theorem 3.2.1 and algebraic manipulations successively we have $e_n=\frac{n!}{2}\sum_{i=0}^{n-2}\frac{(-1)^i}{i!}+(-1)^{n-1}(n-1)$

$$=(n-1)\left[\frac{\{(n-1)+1\}(n-2)!}{2}\sum_{i=0}^{n-2}\frac{(-1)^i}{i!}\right]+(-1)^{n-1}(n-1)$$

$$=(n-1)\left[\frac{(n-1)(n-2)!}{2}\sum_{i=0}^{n-2}\frac{(-1)^i}{i!}+\frac{(n-2)!}{2}\sum_{i=0}^{n-2}\frac{(-1)^i}{i!}\right]+(-1)^{n-1}(n-1)$$

$$=(n-1)\left[\begin{array}{l}\frac{(n-1)!}{2}\sum_{i=0}^{n-3}\frac{(-1)^i}{i!}+\frac{(n-1)!}{2}\frac{(-1)^{n-2}}{(n-2)!}+\frac{(n-2)!}{2}\sum_{i=0}^{n-4}\frac{(-1)^i}{i!}\\ \\ +\frac{(n-2)!}{2}\frac{(-1)^{n-3}}{(n-3)!}+\frac{(n-2)!}{2}\frac{(-1)^{n-2}}{(n-2)!}\end{array}\right]+(-1)^{n-1}(n-1)$$

$$=(n-1)\left[\begin{array}{l}\frac{(n-1)!}{2}\sum_{i=0}^{n-3}\frac{(-1)^i}{i!}+\frac{(-1)^{n-2}}{2}(n-1)+\frac{(n-2)!}{2}\sum_{1=0}^{n-4}\frac{(-1)^i}{i!}\\ \\ +\frac{(-1)^{n-3}}{2}(n-2)+\frac{(-1)^{n-2}}{2}\end{array}\right]+(-1)^{n-1}(n-1)$$

$$= (n-1)\left[\frac{(n-1)!}{2}\sum_{i=0}^{n-3}\frac{(-1)^{i}}{i!} + \frac{(n-2)!}{2}\sum_{i=0}^{n-4}\frac{(-1)^{i}}{i!} + (-1)^{n-2}\right] + (-1)^{n-1}(n-1)$$

$$= (n-1)\left[\frac{(n-1)!}{2}\sum_{i=0}^{n-3}\frac{(-1)^{i}}{i!} + \frac{(-1)^{n-2}(n-2)}{1} + \frac{(n-2)!}{2}\sum_{i=0}^{n-4}\frac{(-1)^{!}}{i!} + \frac{(-1)^{n-3}(n-3)}{1}\right]$$

$$+ (-1)^{n-1}(n-1)$$

$$= (n-1)(e_{n-1} + e_{n-2}) + (-1)^{n-1}(n-1),$$

as required.

(b) As in (a) above, using Theorem 3.2.1 and algebraic manipulations successively we have

$$e_n = \frac{n!}{2}\sum_{i=0}^{n-2}\frac{(-1)^{i}}{i!} + (-1)^{n-1}(n-1)$$

$$= n\left[\frac{(n-1)!}{2}\sum_{i=0}^{n-3}\frac{(-1)^{i}}{i!} + \frac{(n-1)!}{2}\frac{(-1)^{n-2}}{(n-2)!}\right] + (-1)^{n-1}(n-1)$$

$$= n\left[\frac{(n-1)!}{2}\sum_{i=0}^{n-3}\frac{(-1)^{i}}{i!} + \frac{(n-1)}{2}(-1)^{n-2}\right] + (-1)^{n-1}(n-1)$$

$$= n\left[\frac{(n-1)!}{2}\sum_{i=0}^{n-3}\frac{(-1)^{i}}{i!} + (-1)^{n-2}(n-2) - \frac{(-1)^{n-2}}{2}(n-3)\right] + (-1)^{n-1}(n-1)$$

$$= ne_{n-1} + (-1)^{n-1}\frac{1}{2}n(n-3) + (-1)^{n-1}(n-1)$$

$$= ne_{n-1} + (-1)^{n-1}\frac{1}{2}(n-2)(n+1),,$$

as required.

We now turn our attention to finding the number of odd permutations with k fixed points. Let

$$e'(n,k) = \left|\{\alpha \in A'_n : f(\alpha) = k\}\right|, \qquad (3.3)$$

Then it is not difficult to see that

$$e'(n,k) = \binom{n}{k} e'(n-k,\, 0) = \binom{n}{k} e'_{n-k} \qquad (3.4)$$

As in the even case above, to compute $e'(n,k)$ it is sufficient to compute $e'(n,0) = e'_n$. Also, note that e'_n is the number of odd permutations without fixed points. That is, the number of odd derangements. We can certainly deduce results for e'_n in exactly the same manner as above; however, we shall take advantage of Theorem 3.2.1 and result 3.1.1, since it is clear that

$$e'_n = d_n - e_n$$

$$= n!\sum_{i=0}^{n}\frac{(-1)^i}{i!} - \left[\frac{n!}{2}\sum_{i=0}^{n-2}\frac{(-1)^i}{i!} + (-1)^{n-1}(n-1)\right]$$

$$= \frac{n!}{2}\sum_{i=0}^{n-2}\frac{(-1)^i}{i!}.$$

Thus we have proved the following result

3.2.3 Theorem

Let e'_n be as defined by (3.4). Then

$$e'_n = \frac{n!}{2}\sum_{i=0}^{n-2}\frac{(-1)^i}{i!}.$$

3.2.4 Proposition

Let e'_n be as defined in (3.4), respectively. Then

$(a)\ e'_n = (n-1)(e'_{n-1} + e'_{n-2}) + (-1)^n(n-1),\ e'_0 = e'_1 = 0;$

$(b)\ e'_n = ne'_{n-1} + (-1)^n n(n-1)/2,\ e'_0 = 0.$

Proof

It follows directly from result 3.1.1 and proposition 3.2.2

3.2.5 Proposition

Let e_n *and* e'_n be as defined in (3.1) and (3.3), respectively. Then

$$(a)\ e_n = \frac{1}{2}\left[d_n - (-1)^n(n-1)\right],\ d_0 = 1;$$

$$(b)\ e'_n = \frac{1}{2}\left[d_n + (-1)^n(n-1)\right],\ d_0 = 1.$$

Proof

(a) Using Theorem 3.2.1 and algebraic manipulations successively we have

$$e_n = \frac{n!}{2}\sum_{i=0}^{n-2}\frac{(-1)^i}{i!} + (-1)^{n-1}(n-1)$$

$$= \frac{n!}{2}\sum_{i=0}^{n}\frac{(-1)^i}{i!} - \frac{n!}{2}\left[\frac{(-1)^{n-1}}{(n-1)!} + \frac{(-1)^n}{n!}\right] + (-1)^{n-1}(n-1)$$

$$= \frac{1}{2}d_n - \frac{(-1)^{n-1}n}{2} + \frac{(-1)^{n-1}}{2} + \frac{(-1)^{n-1}2(n-1)}{2}$$

$$= \frac{1}{2}\left[d_n + (-1)^{n-1}(n-1)\right]$$

$$= \frac{1}{2}\left[d_n - (-1)^{n}(n-1)\right]$$

as required.

(b) Using Theorem 3.2.1 and algebraic manipulations successively we have

$$e_n' = \frac{n!}{2}\sum_{i=0}^{n-2}\frac{(-1)^i}{i!}$$

$$= \frac{n!}{2}\sum_{i=0}^{n}\frac{(-1)^i}{i!} - \frac{n!}{2}\left[\frac{(-1)^{n-1}}{(n-1)!} + \frac{(-1)^n}{n!}\right]$$

$$= \frac{1}{2}\left[d_n - (-1)^{n-1}n + (-1)^{n-1}\right]$$

$$= \frac{1}{2}\left[d_n + (-1)^{n}(n-1)\right]$$

as required.

3.2.6 Remarks

The sequence $e(n,k)$ and $e'(n,k)$ with the exception of $e_n = e(n,0)$ are not yet listed in Sloane's encyclopedia of integer sequence (N.J.A Sloane, 2005).

For some selected values $e(n,k)$ and $e'(n,k)$ see Tables $1.e(n,k)$ and $2.e'(n,k)$, respectively.

1. $e\left(n,k\right)$

k n	0	1	2	3	4	5	6	7	$\sum e\left(n,k\right)$
0	1								1
1	0	1							1
2	0	0	1						1
3	2	0	0	1					3
4	3	8	0	0	1				12
5	24	15	20	0	0	1			60
6	130	144	45	40	0	0	1		360
7	930	910	504	105	70	0	0	1	2520

2. $e'(n,k)$

k n	0	1	2	3	4	5	6	7	$\sum e'(n,k)$
0	0								0
1	0	0							0
2	1	0	0						1
3	0	3	0	0					3
4	6	0	6	0	0				12
5	20	30	0	10	0	0			60
6	135	120	90	0	15	0	0		360
7	924	945	420	210	0	21	0	0	2520

3. $e(n)+e'(n)-d_n$

n	$e(n)$	$e'(n)$	d_n	$e(n)+e'(n)-d_n$
0	1	0	1	0
1	0	0	0	0
2	0	1	1	0
3	2	0	2	0
4	3	6	9	0
5	24	20	44	0
6	130	135	265	0
7	930	924	1854	0
8	7413	7420	14833	0
9	66752	66744	133496	0
10	667476	667485	1334961	0
11	7342290	7342289	14684570	0
12	88107415	88107426	176214841	0

3.3 GENERATING FUNCTIONS

3.3.1 Proposition

Let $f(x)$ be the exponential generating function for e_n. then using proposition 3.2.5, result 3.1.4 and algebraic manipulations successively we see that

$$f(x) = \sum_{i\geq 0} e_i \frac{x^i}{i!} = \sum_{i\geq 0} \frac{1}{2}\left[d_i - (-1)^i (i-1)\right]\frac{x^i}{i!}$$

$$= \frac{1}{2}\sum_{i\geq 0} d_i \frac{x^i}{i!} - \frac{1}{2}\sum_{i\geq 0} (-1)^i (i-1)\frac{x^i}{i!}$$

$$= \frac{1}{2}\frac{e^{-x}}{1-x} + \frac{x}{2}\sum_{i\geq 1}(-1)^{i-1}\frac{x^{i-1}}{(i-1)!} + \frac{1}{2}\sum_{i\geq 0}(-1)^i \frac{x^i}{i!}$$

$$= \frac{1}{2}\frac{e^{-x}}{1-x} + \frac{x}{2}e^{-x} + \frac{1}{2}e^{-x}$$

$$= \frac{\left(1 - x^2/2\right)}{1-x}e^{-x}$$

3.3.2 Proposition

Let $f_k(x)$ be the exponential generating function for $e_{i,k} = \binom{i}{k} e_{i-k}$. *Then* $f_k(x) = \frac{x^k\left(1 - x^2/2\right)e^{-x}}{k!(1-x)}$.

Proof

$$\text{Lhs} \quad = f_k(x) = \sum_{i \geq k} \frac{\begin{pmatrix} i \\ k \end{pmatrix} e_{i-k} \bullet x^i}{i!}$$

$$= \sum_{i \geq k} \frac{e_{i-k} . x^i}{k!(i-k)!}$$

$$= \frac{x^k}{k!} \sum_{i \geq k} \frac{e_{i-k} . x^{i-k}}{(i-k)!}$$

$$= \frac{x^k}{k!} f(x) = \frac{x^k(1 - x^2/2)e^{-x}}{k!(1-x)} = rhs,$$

as required.

<u>3.3.3 Proposition</u>

Let $g_k(x)$ be the exponential generating function for $e^i(i, k) = \begin{pmatrix} i \\ k \end{pmatrix} e'_{i-k}.$ *Then* $g_k(x) = \frac{x^k(x^2/2)e^{-x}}{k!(1-x)}.$

Proof

From the obvious fact that $d(i, k) = e(i,k) + e'(i,k),$ result 3.1.4 and proposition 3.3.2 it follows that

$$\frac{x^k e^{-x}}{k!(1-x)} = \sum_{i \geq k} d(i,k) \frac{x^i}{i!} = \sum_{i \geq r} [e(i,r) + e'(i,r)] \frac{x^i}{i!}$$

$$= \sum_{i \geq k} e(i,k)\frac{x^i}{i!} + \sum_{i \geq k} e'(i,k)\frac{x^i}{i!}$$

$$= \frac{x^k \left(1 - x^2/2\right)e^{-x}}{k!(1-x)} + g_k\,(x).$$

hence the result follows.

3.4 NUMBER OF PERMUTATIONS WITH A GIVEN CYCLE STRUCTURE

Let $X_{mn} = \{a_1, a_2, \ldots, a_{mn}\}$, where $m \geq 2$ *and* $n \geq 1$, then we immediately see that

3.4.1 Lemma

Let $X_n = \{a_1, a_2, \ldots, a_n\}$. The number of ways in which a permutation α of $X_4 = \{a_1, a_2, a_3, a_4\}$ can be expressed as a product of two transpositions is 3.

Proof

$\alpha = (a_1\, a_2)(a_3\, a_4)$, $\quad (a_1\, a_3)(a_2\, a_4)$ *and* $(a_1\, a_4)(a_2\, a_3)$

3.4.2 Lemma

The number of ways in which a permutation α of X_6 can be expressed as a product of three transpositions is 15

Let the first transposition be $(a_1\, x)$ then $x \in \{a_2, a_3, a_4, a_5, a_6\}$, and the other 4 elements can be written as two transpositions in 3 ways. Then we have 15 possible ways.

3.4.3 Lemma

The number of ways in which permutations α *of* X_{2n} can be expressed as a product of n transpositions is

$$f(n,2)=\frac{(2n)!}{2n\cdot 2(n-2)\cdots 4\cdot 2}=\frac{(2n)!}{2^n\cdot n!}.$$

Proof

The proof is by induction. If the first transposition is $(a_1 x)$, $x\in\{a_2,a_3,\ldots,a_{2n}\}$ then there are $(2n-1)$ possibilities for x. The remaining $2n-2$ elements can be expressed as a product of transpositions in $(2n-3)(2n-5)\cdots 3\cdot 1$ ways. Then we have $(2n-1).(2n-3)(2n-5)\cdots 3\cdot 1$ possible ways.

3.4.4 Lemma

The number of permutation α of X_{mr} that can be expressed as a product of r m-cycles is $f(r,m)=\frac{(mr)!}{m^r\, r!}$.

3.4.5 Theorem

Let α be a permutation of X_n, *with* $r_i(m-i+1)-cylcles$ $(i=1,2,\cdots,m-1)$. the number of such permutations is

$$\frac{n!}{m^{r_1}r_1!(m-1)^{r_2}r_2!\cdots 2^{r_{m-1}}r_{m-1}!}=\frac{n!}{\prod_{i=0}^{m-2}(m-i)^{r_{i+1}}(r_{i+1})!}$$

Proof

First note that $mr_1+(m-1)r_2+\cdots+3r_{m-2}+2r_{m-1}=n$. Now choose mr_1 elements from X_n to form r_1 $m-$cycles. This can be done in $\binom{n}{mr_1}$ ways, and these mr_1 elements can be expressed as a product of r_1 $m-$cycles in

$f(r_1,m)$. Next choose $(m-1)r_2$ elements from the remaining $n-mr_1$ elements to form the r_2 $(m-1)-cycles$. This can be done in $\binom{n-mr_1}{(m-1)r_2}$ ways and these $(m-1)r_2$ elements can be expressed as a product of r_2 $(m-1)-cycles$, in $f(r_2, m-1)$ ways. We continue in this way until we reach the last $2\,r_{m-1}$ elements which can be expressed as a product of r_{m-1} $2-cycles\ in$ $f(r_{m-1}, 2)$ ways. Multiplying all the possibilities gives

$$\binom{n}{mr_1} f(r_1, m).\binom{n-mr_1}{(m-1)r_2} f(r_2,m-1) \cdots \binom{2r_{m-1}}{2r_{m-1}} f(r_{m-1}, 2).$$

This simplifies to the required result by using Lemma 3.4.4 and algebraic manipulations.

3.5 RESULT 2

SOME COMBINATORIAL PROPERTIES OF THE DIHEDRAL GROUP

We investigate certain combinatorial properties of the Dihedral group D_n, we give two different proofs of the main result; one geometric and the other algebraic. We now consider the geometric approach.

First, recall that the dihedral group D_n consists of all symmetries of a regular $n-gon$ $(n \geq 3)$, that is, n rotations through the angles $\frac{360^\circ}{n}x$ $(x = 0,1,2,\ldots,n-1)$ and n reflections through each of the n lines of symmetry of the regular n-gon.

We shall denote the set of rotations and reflections by Rot_n and $\operatorname{Re} f_n$, respectively.

Next we establish a sequence of results that will lead to the proof of the main result.

3.5.1 Results

Rot_n is a cyclic subgroup of D_n, in fact $Rot_n = <\alpha>$, where $\alpha = (12\cdots n)$ is the first rotation through angle $\frac{360^0}{n}$, in a clock-wise direction (same direction as the labeling of the corners of the regular $n-$ gon).

3.5.2 Result

If n is odd, $Rot_n \leq A_n$.

Proof

If n is odd, $\alpha = (12\cdots n)$ is a cycle of odd length and α and all its powers are even permutations.

3.5.3 Result

For all α in Rot_n, $f(\alpha) = 0$, except the identity e for which $f(e) = n$.

3.5.4 Result

If n is even, there are exactly $\frac{n}{2}$ even permutations and exactly $\frac{n}{2}$ odd permutations in Rot_n.

Proof

If n is even, then $\alpha = (12\cdots n)$ is a cycle of even length and so

$\alpha, \alpha^3, \alpha^5, \cdots, \alpha^{n-1}$ are all odd permutations, while $\alpha^2, \alpha^4, \cdots, \alpha^n$ are all even permutations.

To obtain the corresponding results for $\operatorname{Re} f_n,$ we observe that if n is even then there are two types of lines of symmetry (of the regular n-gon): one through the midpoints of a pair of opposite sides and the other through a pair of opposite vertices. The former gives rise to $\frac{n}{2}$ derangements while the latter gives rise to $\frac{n}{2}$ permutations each having exactly two fixed points.

And if n is odd, all lines of symmetry are through a vertex and the midpoint of its opposite side. This gives rise to n permutation each having exactly one fixed point. Thus we have:

3.5.5 Result

If n is even, there are exactly $\frac{n}{2}$ derangements and $\frac{n}{2}$ permutations each having exactly two fixed points, in $\operatorname{Re} f_n$.

3.5.6 Result

If n is odd, $f(\alpha) = 1$ for all α in $\operatorname{Re} f_n$.

3.5.7 Result

If $n = 4k,$ there are exactly $\frac{n}{2}$ even derangements and exactly $\frac{n}{2}$ odd permutations each having exactly two fixed points in $\operatorname{Re} f_n$.

Proof

For the even derangements we consider reflections through the midpoints of a pair of opposite sides, which give rise to $\frac{4k}{2}=2k$ transpositions (an even number of transpositions).

For the odd permutation each with two fixed points, we consider reflections through the other type of line of symmetry, which give rise to $\frac{4k-2}{2}=2k-1$ transpositions (an odd number of transpositions).

3.5.8 Result

If $n=4k+2$, there are exactly $\frac{n}{2}$ odd derangements and exactly $\frac{n}{2}$ even permutations each having two fixed points in $\operatorname{Re} f_n$.

Proof

This is similar to that of Result 3.5.7, above. Two further results whose proofs are similar to that for Result 3.5.7 above are.

3.5.9 Result

If $n=4k+1$, then there are n even permutations each having a unique fixed point in $\operatorname{Re} f_n$.

3.5.10 Result

If $n=4k+3$, then there are n odd permutations each having a unique fixed point in $\operatorname{Re} f_n$.

3.6 NUMBER OF FIXED POINTS

Now as in the Alternating group, we define equivalence on D_n by the equality of number of fixed points and consider:

$$f(n,k)=\left|\left\{\alpha\in D_n \mid f(\alpha)=k\right\}\right|. \tag{3.5}$$

Then it is clear that $f(n,n)=1$ since the identity permutation is the only one with n fixed points.

3.6.1 Proposition

Let $f(n,k)$ be as defined in (3.5).

Then we have

$$(a)\ f(n,\ 0)=\begin{cases} n-1, & if\ \ n\ is\ odd, \\ \dfrac{3n}{2}-1, & if\ \ n\ is\ even. \end{cases}$$

$$(b)\ f(n,\ 1)=\begin{cases} n, & if\ \ n\ is\ odd, \\ 0, & if\ \ n\ is\ even. \end{cases}$$

$$(c)\ f(n,\ 2)=\begin{cases} 0, & if\ \ n\ is\ odd, \\ \dfrac{n}{2}, & if\ \ n\ is\ even. \end{cases}$$

$$(d)\, f(n,\ 3)=f(n,4)=\cdots=f(n,n-1)=0.$$

Proof

(a) If n is odd, there are $n-1$ derangements from Rot_n, by Result 3.5.3 and there are no derangements from $\mathrm{Re}\,f_n$, by Result 3.5.6.

If n is even, there are again $n-1$ derangement from Rot_n by Result 3.5.3 and there are $\frac{n}{2}$ derangements from $\mathrm{Re}\,f_n$, by Results 3.5.3. The proofs for (b) and (c) are similar to that for (a) above.

(d) This result follows directly from (a), (b) and (c) together with the fact that $f(\mathrm{n},\mathrm{n})=1$

3.7 EVEN AND ODD PERMUTATIONS

Let $e(n,k)=\left|\{\alpha \in D_n \cap A_n : f(\alpha)=k\}\right|$ (3.6)

Then clearly we see that $e(n,\, n)=1$. Less obvious is the following result.

3.7.1 Proposition

Let $e(n,k)$ be as defined in (3.6).

Then we have

$$(a)\; e(n,\,0)=\begin{cases} n-1, & if\ n\ is\, odd, \\ \frac{n}{2}-1, & if\ n=4k+2, \\ n-1, & othewise. \end{cases}$$

$$(b)\; e(n,\,1)=\begin{cases} n, & if\ n=4k+1, \\ 0, & othewise. \end{cases}$$

$$(c)\; e(n,2)=\begin{cases} \frac{n}{2}, & if\ n=4k+2, \\ 0, & othewise. \end{cases}$$

$(d)\; e(n,2)=e(n,4)=\cdots=e(n,n-1)=0.$

Proof

(a) If n is odd, then there are $n-1$ even derangements, by Results 3.5.2 and 3.5.3, all from Rot_n. Note that there are no derangements from $\operatorname{Re} f_n$ by Result 3.5.6.

If $n=4k+2$, then there are $\frac{n}{2}-1$ even derangements from Rot_n, by Result 3.5.3 and Result 3.5.4. There are no even derangements if $n=4k+2$ from $\operatorname{Re} f_n$ by Result 3.5.8.

Finally, if $n=4k$, then there are $\frac{n}{2}-1$ even derangements from $Rot_{n,}$ by Results 3.5.3 and 3.5.4. Moreover there are $\frac{n}{2}$ even derangements from $\operatorname{Re} f_n$, by Results 3.5.7.

The proof for (b) and (c) are similar to that for (a) above, while (d) follows directly from proposition 3.6.1 (d).

We now turn our attention to odd permutations.

First, let

$$e'(n,k)=\left|\{\alpha \in D_n - A_n \mid f(\alpha)=k\}\right| \qquad (3.7).$$

Then it is clear that

$$f(n,k)=e(n,k)+e'(n,k). \qquad (3.8).$$

and since $e(n,n)=1=f(n,n)$

It follows that $e'(n,n)=0.$ In general, we have

3.7.2 Proposition

Let $e'(n,k)$ be defined as in (3.7).

Then we have

$$(a)\ e'(n,0)=\begin{cases} 0, & if\ \ n\ is\ odd, \\ n, & if\ \ n=4k+2, \\ \frac{n}{2}, & otherwise. \end{cases}$$

$$(b)\ e'(n\ ,1)=\begin{cases} n, & if\ \ n=4k+3, \\ 0, & otherwise. \end{cases}$$

$$(c)\ e'(n,2)=\begin{cases} \frac{n}{2}, & if\ \ n=4k, \\ 0, & otherwise. \end{cases}$$

$(d)\, e'(n,\, 3) = e'(n,\, 4) = \cdots = e'(n,\, n-1) = 0.$

Proof

All the results follow directly from proposition 3.6.1 and equations (3.7) and (3.8).

3.8 THE SUBGROUP OF ORIENTATION PRESERVING (REVERSING) MAPPINGS

Let X_n denote the set $\{1, 2, \cdots, n\}$ considered with standard ordering and let T_n, P_n and O_n be the full transformation semigroup, the partial transformation semigroup and the submonoid of T_n consisting of all order preserving mappings of X_n, respectively. Another closely related algebraic structure to O_n and P_n are S_n and D_n the symmetric and dihedral groups on the set X_n, respectively.

Catarino and Higgins (1999) introduced a new subsemigroup of X_n containing O_n which is denoted by OP_n and its elements are called orientation preserving mappings. Also, they introduced a semigroup $P_n = OP_n \cup OR_n$ where OR_n denotes the collection of all orientation reversing mappings. Fernandes (2000) studied the monoid of orientation preserving partial transformations of a finite chain, concentrating in particular on partial transformations which are injective. Here, we consider the subgroup of orientation preserving bijective mappings. In particular, we pay attention to a subgroup the Dihedral group D_n of the order $2n$ defined as $D_n = \{x, y \mid x^n = 1,\, y^2 = 1 \quad xy = x^{-1}y\}.$

We have in sections 3.5-3.7 give a geometric proof for the number of even and odd permutations having exactly k fixed points in the Dihedral group D_n. However, the algebraic proof of this result along the lines of Catarino and Higgins (1999) seem not to have been studied.

At the end of this introductory section we gather some known results that we shall need in later sections.

The semigroup of all order-preserving self maps of X_n consist of all maps $\alpha : X_n \to X_n$ with the property that $x \le y \Rightarrow x\alpha \le y\alpha$. A map α is order decreasing if $x\alpha \le x$ for all x in X_n. Let $A = (a_1, a_2, \ldots, a_s)$ be a finite sequence from the chain X_n. We say that A is cyclic or has clockwise orientation if there exist not more than one subscript i such that $a_i > a_{i+1}$ where a_{s+1} denotes a_1. We say that $A = (a_1, a_2, \ldots, a_s)$ is anti-cyclic or has anticlockwise orientation if there exists no more than one subscript i such that $a_i < a_{i+1}$. Note that a sequence A is cyclic if and only if A is empty or there exist $i \in \{0,1,\ldots,s-1\}$ such that $a_{i+1} \le a_{i+2} \le \cdots \le a_s \le a_1 \le \cdots \le a_i$. i is unique unless the sequence is a constant.

3.8.1 Result

Let A be any cyclic (anti-cyclic) sequence. Then A is anti-cyclic (cyclic) if and only if A has no more than two distinct values.

If $A = (a_1, a_2, \ldots, a_t)$ is any sequence then we denote by A^r sequence $(a_t, a_{t-1}, \ldots, a_1)$, called the reversed sequence of A.

3.8.2 Result

Let $A=(a_1,a_2,\ldots,a_t)$ be any sequence from X_n. Then A is cyclic (anti-cyclic) if and only if A^τ is anti-cyclic (cyclic).

3.8.3 Result

If $(a_1,a_2\ldots,a_t)$ is cyclic (anti-cyclic) then so is

(a) the sequence. $(a_{i_1},a_{i_2},\ldots,a_{i_r})$ $(i_1<i_2<\cdots<i_r)$

(b) and the sequence $(a_j,a_{j+1},\ldots a_t,a_{,1}\ldots,a_{j-1})$, for all $1\le j\le t$.

3.8.4 Result

For non-constant $\alpha\in OP_n$, α is an order-preserving mapping if and only if $1\alpha<n\alpha$.

3.8.5 Result

Any restriction of a member of OPD_n (ORD_n) is also a member of OPD_n (ORD_n)

3.8.6 Result

Let $\alpha\in OPD_n$ and let $(a_1\ldots a_m)$, $m\ge 1$ be any cyclic sequence of members of X_n, then the sequence $(a_1\alpha\ldots a_m\alpha)$ is also cyclic. Similarly $((a_1\alpha)\alpha\ldots(\alpha_m\alpha)\alpha)$is cyclic.

3.8.7 Result [11, lemma 4.8]

Let $\alpha\in OPD_n$.Then the digraph of α cannot have a non-trivial cycle and a fixed point.

3.8.8 Result [11, lemma 4.9]

Let $\alpha \in OPD_n$. Then the digraph of α cannot have two cycles of different length.

3.8.9 Result

The maximum subgroup of D_n is OPD_n and is cyclic of order n; OPD_n is a cyclic subgroup and every subgroup of OPD_n is also cyclic of order less than or equal to n.

3.8.10 Result

If n is a natural number; then OPD_n is a subgroup of D_n and ORD_n is an inverse of OPD_n.

3.9. SUBGROUP OF ORIENTATION PRESERVING MAPPINGS

We shall give the algebraic proof of the results established in section 3.5. We first consider the subgroup $OPD_{n.}$

3.9.1 Lemma

The set of all $\alpha \in OPD_n$ forms a cyclic subgroup of D_n.

Proof

Every subgroup of a cyclic group of order less than or equal to the order of the group is a cyclic subgroup. Let $\alpha \in OPD_n$, by Result 3.8.5 and Result 3.8.6 the sequence $(a_1\alpha \quad a_2\alpha \quad \cdots a_m\alpha)$ is cyclic and if $\tau \in OPD_n$ then $(a_1\alpha\tau \;\; a_2\alpha\tau \cdots a_m\alpha\tau)$ is also cyclic.

3.9.2 Lemma

Every $\alpha \in \mathrm{OPD}_n$ is either a derangement or an identity.

Proof

It is clear from Results 3.8.7 and 3.8.8 that every $\alpha \in \mathrm{OPD_n}$ cannot have a non trivial cycle and a fixed point and the digraph of α cannot have two cycles of different length and lemma 3.9.1 implies the result.

3.9.3 Lemma

If n is odd, the set of all $\alpha \in \mathrm{OPD_n}$ forms a cyclic subgroup of A_n of order n .

Proof

Since every, $\alpha(\neq e) \in OPD_n$ is a derangement, and α is of odd length. Then every permutation of odd length is even and a product of even or odd number of even permutations is even. Hence $\mathrm{OPD_n}$ is a set of even permutation and Lemma 3.9.1 and $A_n = \{\alpha \in S_n | \ \alpha \ is \ even\}$ implies the result.

3.9.4 Theorem

If n is even, there are exactly $\frac{n}{2}$ even permutations and exactly $\frac{n}{2}$ odd permutations in $\mathrm{OPD_n}$.

Proof

Every $\alpha_n^m \in OPD_n \ \ 1 \le m \le n$ is defined as,

$$\alpha_n^m = \prod_{i=1}^{n} (i, \ m+i) = (i \ \ i+m \quad i+2m \ \cdots \ i+n-m)$$

Let $|T_k|$ be the length of one of the cycles of α_n^m and $|a^m|$be the number of disjoint cycles in α_n^m. If n is even we first consider even values of m, $m = n = 2k$ and then carry out the induction process of the proof.

First consider $m = n = 2k$, we have,

Case I. $m = n = 2k$

$$\alpha^{n} = (1\ 1+n\ \ 1+2n\ \ 1+3n \cdots 1+n-n) = (1),$$

implies that α^{n} has n fixed points.

Case II. $m = n-2$

$$\alpha^{n-2} = (1\ \ n-1\ \ n-3\ \ n-5 \cdots n-(n-3) = 3)(2\ \ n\ \ n-2\ \ n-4 \cdots n-(n-4) = 4)$$

$$\cdots (k\ \ k+(n-2)\ \ k+2(n-2)\ \ k+3(n-2)\ \cdots\ n-(n-k)-2) = k+2)$$

To determine the nature of the permutation α^{n-2}, we only need to determine the length of one of the cycles in the product of disjoint cycles of α^{n-2}.

Now, let

$$T_1 = (1\ \ n-1\ \ n-3\ \ n-5 \cdots (n-(n-3)))$$

be one of the cycles of α^{n-2}.

$$|T_1| = \frac{n}{n-(n-3)-1} = \frac{n}{2}$$

Since by Result 3.8.8, any $\alpha^{m} \in OPD_n$ cannot have two cycles of different length in α^{n-2}, we can only have $n \left| \frac{n}{2} \right.$ cycles each of length $\frac{n}{2}$, which is a product of even number of odd (even) length cycles. Hence α^{n-2} is a product of even number of even (odd) length cycles.

Case III. $m = n-4$

$$\alpha^{n-4} = (1\ \ n-3\ \ n-7\ \ n-11 \cdots n-(n-5)) \cdots (4\ \ n\ \ n-4 \cdots n-(n-8))$$

Then, the length of one of the cycles, says $T_1 = (1\ n-3 \cdots n-(n-5))$ of the permutation α^{n-4} is $\frac{n}{4}$.

By a similar argument as in case 1, we have $|\alpha^{n-4}| = 4$, Thus for any value of n the permutation α^{n-4} is a product of four (even) numbers of even (odd) length cycles. Hence α^{n-4} is an even permutation for $\frac{n}{4}$ even (odd).

Case IV. We now consider a general case for $m = n - m_k$

$$m_k = \{2, 4, \ldots, n-2\}$$

$$\alpha^{n-m_k} = \prod_{i=1}^{m_k} (i\ \ n-m_k+i\ \ n-2m_k+i\ \ n-3m_k+i \cdots m_k+i)$$

Lets denotes one of the cycles of α^{n-m_k} by T_K,

$$T_K = (1\ \ n-m_k+1\ \ \ n-2m_k+1\ \ n-3m_k+1 \cdots m_k+1)$$

such that the length of T_k is $|T_k| = \frac{n}{m_k}$.

By similar argument as in cases I-III, for $\frac{n}{m_k}$ even (odd), the permutation α^{n-m_k} is a product of m_k (an even number) of even (odd) length cycles.

It is clear that for $n = 2k$ there are $\frac{n}{2}$ even numbers and $\frac{n}{2}$ odd numbers.

We conclude from case I-IV, that if $n = 2k$ (even)and $m = 2k$, then there are $\frac{n}{2}$ even permutations.

We now pay attention to the remaining $\frac{n}{2}$ permutations. By a similar argument as in the case of $m=2k$ we consider, $m=n-m_{\tau}$, m_{τ} is an odd number, $m_{\tau}=\{1,\ 3,\ldots,n-1\}$ such that for any cycle, say, T_{τ} of $\alpha^{n-m_{\tau}}$ we have $|T_{\tau}|=\dfrac{n}{m_{\tau}}$.

Since n is even and m_{τ} is odd we consider two cases:

Case I. m_{τ} does not divides n.

Then $\alpha^{n-m_{\tau}}$ is a cyclic permutation of length n, n – even.

Case II. m_{τ} divides n

Let $n=m_{\tau}d$ .Since n is even and m_{τ} is odd, then it is clear that d is an even number. $\alpha^{n-m_{\tau}}$ is a product of m$_{\tau}$ cycles each of length d, is a product of odd number of even length cycle.

Finally, we conclude that if n is even, then for any value of m satisfying case I & II α^{m} is an odd permutation, and there are $\frac{n}{2}$ m_{τ}'s in n .

3.10 SUBGROUP OF ORIENTATION REVERSING MAPPINGS

We can now give the algebraic proof of the results established in section 3.5. We consider ORD_n.

Throughout sections 3.10 and 3.11, $m, n\ and\ k \in$ N, (set off natural numbers) $n>m>k$, $0\le k\le\dfrac{m-1}{2}$, and $0\le m\le n-2$. If $m=2k+1$ then $0\le k\le\dfrac{m+1}{2}$ and $0\le m\le n-2$. Let $\rho\in ORD_n$, we say ρ is an orientation-reversing bijective mapping on X_n, if the sequence $(1\rho, 2\rho, \cdots, n\rho)$ is anti-cyclic, the collection of all orientation-reversing bijective mappings on X_n is denoted by ORD_n.

We define a reflection $\rho_m \in ORD_n$ by $i \to 1-i-m+1$ $(i \in X_n)$ with $\rho = \rho_0 : i \to n+1-i$ such that $(1\rho\ , 2\rho,\ \cdots,\ n\rho) = (n,\ n-1,\ \cdots,\ 1)$ and is anti-cyclic. Thus, for every $\alpha^m \in OPD_n$ there exist an equivalence $\alpha^m\rho$ in ORD_n,. that is there exist an isomorphism between the subgroup OPD_n and ORD_n

<u>3.10.1 Lemma</u>

If $n=2k+1$, we consider two cases of $\rho_m = \alpha^m\rho$

(i) If $m = 2k$, ρ_m has a fixed point at $i = \frac{n+1}{2} - \frac{m}{2}$

(ii) If $m=2k+1$, then ρ_m $(0 \le m \le n-1)$ has a fixed point at $i = n - \frac{m+1}{2}$

Proof

We prove the assertions by induction on m, there are several cases to be examine. First recall that for all $\rho_m \in ORD_n$,

$$\rho_m = \alpha^m\rho = \prod_{i=1}^{\frac{n+1}{2}} (i, n-m-i+1)$$

Case 1. $m = 0$ $(m = 0 \bmod n)$

$$\rho = \rho_0 = \prod_{i=1}^{\frac{n+1}{2}} (i,\ n-i+1)$$

$$\begin{array}{ccc} 1 & \to & n \\ 2 & \to & n-1 \\ \vdots & \to & \vdots \\ \frac{n-1}{2} & \to & \frac{n+3}{2} \\ \frac{n+1}{2} & \to & \frac{n+1}{2} \\ \vdots & \to & \vdots \\ n-1 & \to & 2 \\ n & \to & 1 \end{array}$$

The fixed point is at

$$\rho_0 \to i = \frac{1}{2}(n-0+1) \Rightarrow i = \frac{1}{2}(n-m+1),\ m=0$$

$$\rho_0 = (1\ \ n)(2\ n-1)\cdots\left(\frac{n-1}{2}\ \ \frac{n+3}{2}\right)\left(\frac{n+1}{2}\ \ \frac{n+1}{2}\right)$$

Similarly, we consider the next even natural number, $m=2$

$$\rho_2 = (1\ \ n-2)(2\ \ n-3)\ \cdots\ \left(\frac{n-1}{2}\ \ \frac{n-1}{2}\right)\left(\frac{n+1}{2}\ \ \frac{n-3}{2}\right)\ \cdots\ (n-1\ \ n)$$

ρ_2 has a fixed point at

$$i = \frac{1}{2}(n-2+1) \Rightarrow i = \frac{1}{2}(n-m+1),\ m=2$$

Case 11, We now assume that the result holds for all values of m up to $2k$.

$$\rho_{2k} = (i\ n-i-2k+1).$$

$$\rho_{2k} = (1\ \ n-2k)(2\ \ n-2k-1)\cdots\left(\frac{n-2k-1}{2}\ \ \frac{n-2k+3}{2}\right)\left(\frac{n-2k+1}{2}\ \ \frac{n-2k+1}{2}\right)$$

$$\cdots\left(\frac{n-1}{2}\ \ \frac{n-2(2k-1)+1}{2}\right)\left(\frac{n+1}{2}\ \ \frac{n-2(2k-1)-1}{2}\right)\cdots(n\ \ n-2k+1)$$

ρ_{2k} has a fixed point at

$$2k \to i = \frac{1}{2}(n-2k+1) \Rightarrow i = \frac{1}{2}(n-m+1), \quad m = 2k.$$

Case 111, finally, we consider the next even natural number after $2k$, $m = 2(k+1)$.

$$\rho_{2(k+1)} = (i \quad n-i-2k-1)$$

$$\rho_{2(k+1)} = (1 \quad n-2(k+1))(2 \quad n-2(k+1)-1)\cdots\left(\frac{n-2(k+1)+1}{2} \quad \frac{n-2(k+1)+1}{2}\right)$$

$$\left(\frac{n-2(k+1)-1}{2} \quad \frac{n-2(k+1)+3}{2}\right)\cdots\left(\frac{n-1}{2} \quad \frac{n-2(2(k+1))+3}{2}\right)\left(\frac{n+1}{2} \quad \frac{n-2(2(k+1))+1}{2}\right)$$

The fixed point is at

$$i = \frac{1}{2}(n-2(k+1)+1) \Rightarrow i = \frac{1}{2}(n-m+1), m = 2(k+1)$$

The result is true for $m=2(k+1)$, hence it is true for all $m-$ even and $n-$ odd.

(ii).By a similar argument as in (i) above. Here, we consider m, $n=2k+1$.

$$\rho_m = \alpha^m \rho = \prod_{i=1}^{\frac{n+1}{2}} (i, n-m-i+1).$$

Case 1. $m=1.\ n-odd$.

$$\rho_1 = \prod_{i=1}^{\frac{n-1}{2}} (i \quad n-i)$$

$$\begin{array}{ccc} 1 & \to & n-1 \\ 2 & \to & n-2 \\ \vdots & \to & \vdots \\ n-1 & \to & 1 \\ n & \to & n \end{array}$$

The fixed point is at

$$i = \frac{1}{2}(n-1+1) \quad \Rightarrow i = \frac{1}{2}(n-m+1), \; m=1 \quad for \quad n > m$$

Since n and m are odd natural numbers and $0 \le m < n-1$ n-odd (the operation is orientation) we have $i = n\,(\frac{n}{2} = n, we\,have\,2n = n)$.

$$\rho_1 = (1\ \ n-1)(2\ \ n-2)\cdots\left(\frac{n-1}{2}\ \ \frac{n+1}{2}\right)\left(\frac{n+3}{2}\ \ \frac{n-3}{2}\right)\cdots(n-1\ \ 1)(n\ \ n)$$

Similarly, for $n-odd$**,** we consider the next odd natural number, $m{=}3$

$$\rho_3 = (1\ \ n-3)(2\ \ n-4)\cdots\left(\frac{n-3}{2}\ \ \frac{n-7}{2}\ \right)\cdots(n-1\ \ n-1)(n\ \ n-2)$$

The fixed point is at

$$i = \frac{1}{2}n - \frac{3+1}{2}, m = 3 \ and \ n-odd$$

by a similar argument as in the case of $m{=}1$, $\frac{1}{2}n = n$ we have

$$i = n - \frac{3+1}{2} \Rightarrow i = n - \frac{m+1}{2}, \ m = 3, \ n-odd\,\textbf{.}$$

Case 11, we assume that the result holds true for all values of $m=2k+1,\ n-odd$ **.**

$$\rho_{m(=2k+1)}=\alpha^{2k+1}\rho=\prod_{i=1}^{\frac{n-1}{2}}(i,\ n-i-2k)$$

$$\rho_{m(=2k+1)}=(1\ \ n-(2k+1))(2\ \ n-(2k+1)-1)\cdots\left(\frac{n-(2k+1)-1}{2}\ \ \frac{n-(2k+1)+3}{2}\right)\cdots$$

$$\left(n-\frac{(2k+1)-1}{2}\ \ n-\frac{(2k+1)+3}{2}\right)\left(n-\frac{(2k+1)+1}{2}\ \ n-\frac{(2k+1)+1}{2}\right)\ \cdots$$

$$(n-1\ \ n-(2k+1)+2)(n\ \ n-(2k+1)+1)$$

Similarly, for $m=2k+1$ the fixed point is at

$$i=n-\frac{(2k+1)+1}{2}\Rightarrow i=n-\frac{m+1}{2},m=2k+1\ \ n>m,\ n-odd\ \textbf{.}$$

Case III. $n-odd$ and $m=2k+3$, the next odd natural number after $2k+1$.

$$\rho_{m(=2k+3)}=\alpha^{2k+3}\rho=\prod_{i=1}^{\frac{n-2}{2}}(i,\ n-i-2k-2)$$

$$\rho_m=\alpha^{2k+3}\rho=(1\ \ n-(2k+3))(2\ \ n-(2k+3)-1)\cdots\left(\frac{n-(2k+3)-1}{2}\ \ \frac{n-(2k+3)+3}{2}\right)$$

$$\left(n-\frac{(2k+3)-1}{2}\ \ n-\frac{(2k+3)+3}{2}\right)\left(n-\frac{(2k+3)+1}{2}\ \ n-\frac{(2k+3)+1}{2}\right)\cdots$$

$$(n-1\ \ n-(2k+3)+2)(n\ \ n-(2k+3)+1)$$

by a similar argument as in cases I-II the fixed point is at

$$i = n - \frac{(2k+3)+1}{2} \Rightarrow i = n - \frac{m+1}{2}, \quad m = 2k+3, \quad n > m, \; n - odd \; .$$

The induction process proves that the result holds true for any value of $m{=}2k{+}1.$

3.10.2 Lemma

If n is even, then we have two cases for ρ_m

(i) If $m{=}2k$, ρ_m has no fixed point.

(ii) If $m{=}2k{+}1$, ρ_m has two fixed points at $i = \frac{1}{2}(n - m + 1)$ and $i = n - \frac{m+1}{2}$.

Proof

(i) For n-even we prove the assertion in a similar way we prove Lemma 3.10.1, by considering $m{=}2k$ and n - even.

Case I. Consider $m{=}0$ and $2.$

$$\rho \; = \alpha^0 \rho = \prod_{i=1}^{n} (i, \; n - i + 1)$$

$$\begin{array}{ccc}
1 & \rightarrow & n \\
2 & \rightarrow & n-1 \\
\vdots & \rightarrow & \vdots \\
\frac{n-2}{2} & \rightarrow & \frac{n+4}{2} \\
\frac{n}{2} & \rightarrow & \frac{n+2}{2} \\
\frac{n+2}{2} & \rightarrow & \frac{n}{2} \\
\vdots & \rightarrow & \vdots \\
n-1 & \rightarrow & 2 \\
n & \rightarrow & 1
\end{array}$$

If i is a fixed point, then

$$\rho_0 \to i = \frac{n+1}{2}$$

If $i = \frac{n+1}{2}$ is a fixed point, then it is clear that $n+1$ is odd, since n is even, it implies that $i = \frac{n+1}{2}$ does not exist in N (set of natural numbers) or ρ. Hence or otherwise, if $i = \frac{n+1}{2}$ is a fixed point, then, $0 \to i = n \neq 1$

$$\rho = \rho_0 = (1\ n)(2\ \ n-1)\cdots\left(\frac{n-2}{2}\ \ \frac{n+4}{2}\right)\left(\frac{n}{2}\ \ n+1\right)$$

If $m{=}2,\ \rho_2 = \alpha^2\rho = (i,\ n-i-1)$

If i is a fixed point, then $i = \frac{n-1}{2}$, does not exist in N (set of natural numbers) or ρ. since, by similar argument as in $m{=}0, n$ is an even natural number; $n{-}1$ is odd $\frac{n-1}{2} \notin \mathrm{N}$. If we assume that $\frac{n-1}{2} = n-1$ as in the other case, an odd number, that is $i{=}\ n{-}1$ is a fixed point, it implies that

$$i = n-(n-1)-1 = n \neq n-1$$

Hence ρ_2 doesn't have a fixed point.

$$\rho_2 = (1\ \ n-2)(2\ \ n-3)\cdots\left(\frac{n-4}{2}\ \ \frac{n+2}{2}\right)\left(\frac{n-2}{2}\ \ \frac{n}{2}\right)\cdots(n\ \ n-1)$$

Case II. Assume that the result is true for $m{=}2k$,

$$\rho_{2k} = (i,\ n-i-2k+1)$$

If $i = \frac{1}{2}(n-2k+1)$ is a fixed point, then it is clear that $n-(2k-1)$ is odd, since n is even and $2k-1$ is odd. It implies that $\frac{n-(2k-1)}{2}$ does not exist in N (set of natural numbers) or ρ. Hence or otherwise, if we assume that

$$i = \frac{n-(2k-1)}{2} = n-(2k-1),$$

is a fixed point, then

$$2k \to i = n-(n-(2k-1))-2k+1 = n \neq n-(2k-1)$$

$$\rho_{2k} = (1,\ n-2k)(2\ \ n-2k-1)\cdots\left(\frac{n-2k}{2}\quad \frac{n-2k+2}{2}\right)\cdots$$

$$(n-1\ \ n-2k+2)(n\quad n-2k+1)$$

Case III. $m = 2(k+1)$, the next even natural number after $2k$,

$$\rho_{m(=2(k+1))} = \alpha^{2(k+1)}\rho = (i,\ n-i-2k-1)$$

$$\rho_{m(=2(k+1))} = (1\ \ n-2(k+1))(2\quad n-2(k+1)-1)\cdots$$

$$\left(\frac{n-2(k+1)}{2}\quad \frac{n-2(k+1)+2}{2}\right)\cdots(n-1\quad n-2(k+1)+2)(n\ \ n-2(k+1)+1)$$

$$i = \frac{n-2(k+1)+1}{2} \Rightarrow i = \frac{n-m+1}{2},\ m = 2(k+1)$$

does not exist as a fixed point in ρ_m, by a similar argument as in the cases I&II above $n=m+1$ is odd, which implies that $\frac{n-m+1}{2}$ does not exist in N $(or\ \rho = 2(k+1))$ Hence or otherwise, if

$$i = \frac{n-m+1}{2} = n-m+1$$

then

$$2k+1 \to i = n-(n-m+1)-2k-1 = n \neq n-m+1$$

implies that $n-2(k+1)+1$ is not a fixed point.

The induction process proves that the result is true for any value of $m=2k,\ n$-even.

(ii) If n even and $m=2k+1$ then we consider various cases of m in a similar way as in (i) above.

Case 1. $m=1$.

$$\rho_1=\alpha^1\rho=\prod_{i=0}^{\frac{n}{2}}(i,\ n-i)$$

$$\begin{array}{ccll}
1 & \to & n-1 & \\
2 & \to & n-2 & \\
\vdots & \to & \vdots & \\
\dfrac{n-2}{2} & \to & \dfrac{n+2}{2} & \\
\dfrac{n}{2} & \to & \dfrac{n}{2} & \textit{is the first fixed point} \\
\vdots & \to & \vdots & \\
n-1 & \to & 1 & \\
n & \to & n & \textit{is the second fixed point}
\end{array}$$

$$\rho_1=(1\ \ n-1)(2\ \ n-2)\ \cdots\ \left(\frac{n-2}{2}\ \ \frac{n+2}{2}\right)\left(\frac{n}{2}\ \frac{n}{2}\right)\ \cdots\ (n\ \ n)$$

$i=\dfrac{n}{2}$ is the first fixed point of ρ_1 when n is even and $m=2k+1$. If one point is fixed, then we have $n-1$ elements left. Since $m=2k+1$, then by a similar argument as in Lemma 3.10.1 for n and m - odd. We have second fixed point at

$$n-\frac{1+1}{2}\Rightarrow i=n-\frac{m+1}{2},\ m=1.$$

Similarly, if $m=3$,

$$\rho_3=\prod_{i=1}^{\frac{n}{2}}(i,\ n-i-2)$$

$$\rho_3=\alpha^3\rho=(1\quad n-3)(2\quad n-4)\cdots\left(\frac{n-2}{2}\quad\frac{n-2}{2}\right)\left(\frac{n}{2}\,\frac{n-4}{2}\right)\ \cdots\ (n-1\quad n-1)(n\quad n-2)$$

$$i=\frac{1}{2}(n-3+1)$$

is a fixed point.

By a similar argument as in the case I above, the other fixed point is at

$$i=n-\frac{3+1}{2}=n-1\Rightarrow i=n-\frac{m+1}{2},\quad m=3.$$

Case II. $m=2k+1.$

Let's assume that the result is true for all values of m up to $m=2k+1.$

$$\rho_{2k+1}=\prod_{i=1}^{\frac{n}{2}}(i,\ n-i-2k)$$

$$\rho_{2k+1}=(1\quad n-(2k+1))(2\quad n-(2k+1)+1)\ \cdots\ \left(\frac{n-(2k+1)-1}{2}\quad\frac{n-(2k+1)+3}{2}\right)$$

$$\left(\frac{n-(2k+1)+1}{2}\quad\frac{n-(2k+1)+1}{2}\right)\ \cdots\ \left(n\ -\ \frac{(2k+1)-1}{2}\quad n\ -\ \frac{(2k+1)+3}{2}\right)$$

$$\left(n\ -\ \frac{(2k+1)+1}{2}\quad n\ -\ \frac{(2k+1)+1}{2}\right)\cdots(n-1\quad n-(2k+1)+2)(n\quad n-(2k+1)+1)$$

$$i=\frac{n-(2k+1)+1}{2}\ \Rightarrow\ i=\frac{n}{2}\ -\ \frac{m+1}{2},\quad m=2k+1$$

is a fixed point.

By similar argument as in the cases I&II above

$$i = n - \frac{m+1}{2}$$

is the second fixed point.

Case III. $m=2k+3$, the next odd natural number after $2k+1$

$$\rho_{2k+3} = (1 \quad n-(2k+3))(2 \quad n-(2k+3)-1)\cdots\left(\frac{n-(2k+3)-1}{2} \quad \frac{n-(2k+3)}{2}\right)$$

$$\left(\frac{n-(2k+3)+1}{2} \quad \frac{n-(2k+3)+1}{2}\right)\cdots\left(n - \frac{(2k+3)-1}{2} \quad n - \frac{(2k+3)+3}{2}\right)$$

$$\left(n - \frac{(2k+3)+1}{2} \quad n - \frac{(2k+3)+1}{2}\right)\cdots(n-1 \quad n-2k-1)(n \quad n-2k-2)$$

The first point is at

$$i = \frac{n-(2k+3)+1}{2} \Rightarrow i = \frac{n}{2} - \frac{m+1}{2}, \quad m = 2k+3.$$

By a similar argument as in the above cases 1 & 11, the second fixed point is at

$$i = n - \frac{(2k+3)+1}{2} \Rightarrow i = n - \frac{m+1}{2}, \quad m = 2k+3.$$

The induction process shows that if$n$ is even and $m=2k+1$ the permutation ρ_m has two fixed points at

$$i = \frac{1}{2}(n - m + 1) \text{ and } n - \frac{m+1}{2}$$

3.10.3 Lemma

If n is even and $m-$odd for every $\rho \in ORD_n$ there are exactly $\frac{n}{2}$ derangements and $\frac{n}{2}$ permutations each having exactly two fixed points in ORD_n.

Proof

If n even is ($n=4k$ *or* $(4k+2)$), it is clear that there are $\frac{n}{2}$ even numbers of $m's$' in n, and $\frac{n}{2}$ odd numbers of $m's$ in n. If $m=2k+1$ there are $\frac{n}{2}$ odd $m's$' in n. It implies that there are $\frac{n}{2}$ permutations with two fixed points in n by Lemma 3.10.2 Similarly, by the same argument $m=2k$ and Lemma 3.10.2 there are $\frac{n}{2}$ derangements in n.

3.10.4 Result

If n is odd, $f(\rho_m)=1$ for all m, $\rho_m \in ORD_n$.

Proof

This result follows from Lemma 3.10.1

3.10.5 Result

Let $n=4k+2$, if $m=2k$ then there are exactly $\frac{n}{2}$ odd derangements and if $m=2k+1$ then there are exactly $\frac{n}{2}$ even permutations each having exactly two fixed points, for every $\rho_m \in ORD_n$.

Proof

If $n=4k+2$, there are exactly $\frac{n}{2}$ derangements and exactly $\frac{n}{2}$ permutation with two fixed points by Lemma 3.10.3 since $\rho \in ORD_n$ cannot have two cycles of different length from Result 3.8.8.

Now, if $m = 2k$, ρ_m is a derangement by Lemma 3.10.2 and can be written as a product of $\frac{(4k+2)-0}{2} = 2k+1$ transpositions, a product of an odd number of transpositions, odd permutations.

If $m = 2k+1$ then each $\rho_m \in ORD_n$ has two fixed points as given by Lemma 3.10.2 and can be written as a product of $\frac{4k+2-2}{2} = 2k$ transpositions, a product of even number of transpositions, an even permutation.

3.10.6 Result

Let $n = 4k$, if $m = 2k$ then, there are exactly $\frac{n}{2}$ even derangements, and if $m = 2k+1$ there are exactly $\frac{n}{2}$ odd permutations each having two fixed points, for every $\rho_m \in ORD_n$.

Proof

By a similar argument as in the proof of Result 3.10.5 above, if $n = 4k$ and $m = 2k$, for every $\rho_m \in ORD_n$ can be written as a product of $\frac{4k-0}{2} = 2k$, an even number of transpositions, an even permutation. (Lemma 3.10.2)

If $n = 4k$, and $m = 2k+1$ each ρ_m has two fixed points, and can be written as a product of $\frac{(4k-2)-0}{2} = 2k-1$ transpositions, an odd permutation.

3.10.7 Result

If $n = 4k+1$, then there are $n-$ even permutations each having a unique fixed point in ORD_n.

3.10.8 Result

If $n=4k+3,$ then there are $n-$ odd permutations each having a unique fixed point in ORD_n.

The proof of the above two results is similar to that of Results 3.10.5 and 3.10 6 above.

3.10 9 Remark

Let $f(n,k)$ and $f(n,n)$ be as defined above. We give the algebraic proof of proposition 3.6.1.

Proof

If n is odd there are $n-1$ derangements from OPD_n by Lemma 3.9.2 We observe that in ORD_n there are no derangement if n is odd, by Lemma 3.10.4

If n is even there are $n-1$ derangements from OPD_n by Lemma 3.9.2 and $\frac{n}{2}$ derangements from Lemma 3.10.3.

The proofs for (b) and (c) are similar to that for (a) above.

3.11 EVEN AND ODD PERMUTATIONS

3.11.1 Proposition

Let $e(n,k)$ and $e(n,n)$ be as defined in equation (3.7), we give the algebraic proof of proposition 3.7.1.

Proof

If n is odd, then all $\alpha \in OPD_n$ by Lemma 3.9.3 are even derangements except the identity element. There is no derangement in ORD_n for n-odd by Lemmas 3.10.1 and 3.10.4.

If $n=4k+2$, then there are $\frac{n}{2}-1$ even derangements from OPD_n by Lemmas 3.9.2 & 3.9.4. InORD_n, we consider two cases of m, $m=2k+1$ and $m=2k$. In both cases, there is no even derangement from Results 3.10.5.

If $n=4k$, there are $\frac{n}{2}-1$ even derangement from Theorem 3.9.4 in OPD_n. Note that in ORD_n we consider two cases of m. If $m=2k$, then there are $\frac{n}{2}$ even derangements from Result 3.10.6. There is no even derangement for $m=2k+1$.

The proof for (b) and (c) are similar to that for (a) above, while (d) follows directly from proposition 3.6.1(d).

<u>3.11.2 Proposition</u>

Let $f(n,n)$, $f(n,k)$, $e(n,n)$,$e(n,k)$, $e'(n,n)$ and $e'(n,k)$ be as defined in section 3.7, the algebraic proof of proposition 3.7.2 follows directly from the algebraic proof of proposition 3.6.1 given above.

4. $e(n,k)$

k \ n	0	1	2	3	4	5	6	7	8	9	$\sum e(n,k)$
0	1										1
1	0	1									1
2	0	0	1								1
3	2	0	0	1							3
4	3	0	0	0	1						4
5	4	5	0	0	0	1					10
6	2	0	3	0	0	0	1				6
7	6	0	0	0	0	0	0	1			7
8	7	0	0	0	0	0	0	0	1		8
9	8	9	0	0	0	0	0	0	0	1	18

5. $e'(n,k)$

n \ k	0	1	2	3	4	5	6	7	8	9	$\sum e'(n,k)$
0	0										0
1	0	0									0
2	0	0	0								0
3	0	3	0	0							3
4	2	0	2	0	0						4
5	0	0	0	0	0	0					0
6	6	0	0	0	0	0	0				6
7	0	7	0	0	0	0	0	0			7
8	4	0	4	0	0	0	0	0	0		8
9	0	0	0	0	0	0	0	0	0	0	0

3.12 DIHEDRAL GROUPS AS HOMOMORPHIC IMAGES

We proved the three families: $F(2r,4r+2)$, $F(4r+3,8r+8)$ and $F(4r+5,8r+12)$ of the Fibonacci groups $F(m\ ,n)$ to be infinite by defining morphism between dihedral groups and the Fibonacci groups.

The dihedral group denoted by D_n is usually defined as

$$D_n =< x,y \mid x^n = y^2 = 1,\ yx^{-1} = xy > .$$

It is easy to prove the following:

<u>3.12.1 Lemma</u>

For all $k = 0,1,2,\ldots,n-1$ we have;

(a) $x^{-k} = x^{n-k}$; (d) $(x^k y)^2 = 1$;

(b) $y^{-1} = y$; (e) $x^k y x^k = y$;

(c) $yx^k = x^{n-k} y$; (f) $yxy = x^{-1} = x^{n-1}$.

Thus we may write the elements of D_n uniquely as x^k or $x^k y$, for $k = 0,1,2,\ldots,n-1$.

$$F(m,\ n) =< a_1, a_2, \ldots, a_n | a_i a_{i+1} \cdots a_{i+m-1} = a_{i+m} \quad i = 1,2,\ldots,m >$$

where subscripts are taken modulo n if necessary. The following lemma seems to be useful:

<u>3.12.2 Lemma</u>

For all $k > 0$ and $m \geq 2$ $\qquad a_{m+k} = a_{k-1}^{-1} a_{m+k-1}^2$

Proof

$$a_{m+k} = a_k a_{k+1} \cdots a_{m+k-1}$$

$$= a_{k-1}^{-1}\left(a_{k-1} a_k a_{k+1} \cdots a_{m+k-2}\right) a_{m+k-1}$$

$$= a_{k-1}^{-1} a_{m+k-1}^{2}$$

3.13 THE FIBONACCI GROUP $F(2r,\ 4r+2)$

Consider the Fibonacci group

$$F(2r,\ 4r+2) = < a_1, a_2, \ldots, a_{4r+2} \,|\, a_i a_{i+1} \cdots a_{i+2r} = a_{i+2r+1} \quad i = 1,2,\ldots,4r+2 >$$

where subscripts are taken modulo $4r+2$ if necessary. The following lemma seems to be useful:

3.13.1 Lemma

For all $k \geq 0$ and $r \geq 2$, $\quad a_{2r+k} = a_{k-1}^{-1} a_{2r+k-1}^{2}$

Proof

$$a_{2r+k} = a_k a_{k+1} \cdots a_{2r+k-1}$$

$$= a_{k-1}^{-1} \left(a_{k-1} a_k a_{k+1} \cdots a_{2r+k-2} \right) a_{2r+k-1}$$

$$= a_{k-1}^{-1} a_{2r+k-1}^{2}$$

3.13.2 Proposition

There exist a morphism from $F(2r, 4r+2)\ onto\, D_n\ (n \geq 3)$. Hence $F(2r, 4r+2)$ is infinite.

We shall prove this result by a sequence of lemmas and observations which we record as equations. First, we define a mapping from the first $2r$ generators of $F(2r, 4r+2)$ onto the two generators of D_n by

$$a_1 \to x \qquad \text{and} \qquad a_i \to y \qquad (i = 2,\ldots,2r) \qquad (3.9).$$

Then we immediately see that for $r \geq 1$

$$a_{2r+1} = a_1 a_2 \cdots a_{2r} \to xy^{2r-1} = xy \qquad (3.10).$$

and using lemma 3.13.1, we deduce that

$$a_{2r+2} = a_1^{-1}a_{2r+1}^2 \to x^{-1}(xy)^2 = x^{-1} = x^{n-1} \qquad (3.11).$$

$$a_{2r+3} = a_2^{-1}a_{2r+2}^2 \to y^{-1}(x^{n-1})^2 = yx^{n-2} = x^2y \qquad (3.12)$$

More generally, we have

3.13.3 Lemma

For $4 \le i \le 2r+1,\ r \ge 2$. $\quad a_{2r+i} \to y$

Proof

The proof is by induction.

Basis step: By Lemma 3.13.1 and (3.12), we see that

$$a_{2r+4} = a_3^{-1}a_{2r+3}^2 \to y^{-1}(x^2y)^2 = y^{-1} = y.$$

Induction step: suppose that $a_{2r+k} \to y \quad (k = 4,5,\ldots,2r)$.

Then using Lemma 3.13.1 again, we see that

$$a_{2r+k+1} = a_k^{-1}a_{2r+k}^2 \to y^{-1}y^2 = y^{-1} = y.$$

as required.

3.13.4 Lemma

For $r \ge 1$ we have;

$(a)\ a_{4r+2} \to xy;$

$(b)\ a_{4r+3} \to x;$

$(c)\ a_{4r+i} \to y \qquad (4 \le i \le 2r+2).$

Proof

We shall henceforth use Lemma 3.13.1, equations (3.9) to (3.12) whenever necessary without mentioning.

$(a)\ a_{4r+2} = a_{2r+1}^{-1}a_{4r+1}^2 \to (xy)^{-1}y^2 = xy.$

(b) $a_{4r+3} = a_{2r+2}^{-1}a_{4r+2}^{2} \rightarrow (x^{n-1})^{-1}(xy)^{2} = x$

(c) This is by induction.

Basis step:

$$a_{4r+4} = a_{2r+3}^{-1}a_{4r+3}^{2} \rightarrow (x^{2}y)^{-1}x^{2} = x^{2}yx^{2} = y. \qquad (by\ (b)).$$

Induction step: suppose that $a_{4r+k} \rightarrow y \ \ (k = i = 4,5,\ldots,2r+1)$.

Then

$$a_{4r+k+1} = a_{2r+k}^{-1}a_{4r+k}^{2} \rightarrow y^{-1}y^{2} = y,$$

as required.

It is now clear from Lemma 3.13.3, Lemma 3.13.4 and equations (3.10) to (3.12) that the map: $\rightarrow$ defined from the first $2r$ generators of $F(2r,4r+2)$ onto the two generators of D_n by $a_1 \rightarrow x$ and $a_i \rightarrow y \ (i = 2,\ldots,2r)$ as in (3.9) is indeed a morphism onto D_n.

3.14 THE FIBONACCI GROUP $F(4r+3,\ 8r+8)$

Consider the Fibonacci group

$$F(4r+3,\ 8r+8) = < a_1, a_2, \ldots, a_{8r+8} \big| a_i a_{i+1} \cdots a_{i+4r+2} = a_{i+4r+3} \ \ i = 1,2,\ldots,8r+8 >,$$

where subscripts are taken modulo $8r+8$ if necessary.

As in the case of the Fibonacci group $F(2r,\ 4r+2)$ we state the corresponding lemmas in $F(4r+3,\ 8r+8)$.

<u>3.14.1 Lemma</u>

For all $k \geq 5$ and $r \geq 0$.

(a). $a_{4r+k} = a_{k-4}^{-1}a_{4r+k-1}^{2}$;

(b). $a_{6r+k} = a_{2r+k-4}^{-1}a_{6r+k-1}^{2}$;

(c). $a_{8r+k} = a_{4r+k-4}^{-1} a_{8r+k-1}^{2}$.

Proof

$$(a)\ a_{4r+k} = a_{k-3}a_{k-2} \cdots a_{4r+k-2}a_{4r+k-1}$$

$$= a_{k-4}^{-1}(a_{k-4}a_{k-3} \cdots a_{4r+k-2})a_{4r+k-1}$$

$$= a_{k-4}^{-1}a_{4r+k-1}^{2}.$$

. $$(b)\ a_{6r+k} = a_{2r+k-3}a_{2r+k-2} \cdots a_{6r+k-1}$$

$$= a_{2r+k-4}^{-1}(a_{2r+k-4}a_{2r+k-3} \cdots a_{6r+k-2})a_{6r+k-1}$$

$$= a_{2r+k-4}^{-1}a_{6r+k-1}^{2}.$$

$$(c)\ a_{8r+k} = a_{4r+k-3}a_{4r+k-2} \cdots a_{8r+k-2}a_{8r+k-1}$$

$$= a_{4r+k-4}^{-1}(a_{4r+k-4}a_{4r+k-3} \cdots a_{8r+k-2})a_{8r+k-1}$$

$$= a_{4r+k-4}^{-1}a_{8r+k-1}^{2}.$$

3.14.2 Proposition

There exist a morphism from $F(4r+3,\ 8r+8)$ onto D_n $(for\,all\,n \geq 3)$.Hence $F(4r+3,\ 8r+8)$ is infinite.

We carry out the proof in a similar way to that for $F(2r,\,4r+2)$. We consider the case of $r=0$ first, then $r \geq 1$.

We define a mapping from the first 3 generators of $F(3,\ 8)$ onto the two generators of D_n by

$$a_1, a_3 \to x \qquad \text{and} \qquad a_2 \to y \tag{3.13}$$

Then we immediately see that

$$a_4 = a_1 a_2 a_3 \to xyx = y \qquad (3.14)\,.$$

We shall henceforth use lemma 3.14.1 and equations (3.13) and (3.14) whenever necessary without mentioning.

3.14.3 Lemma

If $k \geq 5$ then

(a). $a_5, a_7 \to x^{n-1}$;

(c). $a_6, a_8 \to x^2 y$.

Proof

$$(a)\ a_k = a_{k-4}^{-1} a_{k-1}^2$$

$$a_5 = a_1^{-1} a_4^2 \to x^{n-1} y^2 = x^{n-1}.$$

The proof of a_7 follows from the same argument

$$(b)\ a_k = a_{k-4}^{-1} a_{k-1}^2$$

$$a_6 = a_2^{-1} a_5^2 \to y^{-1} \left(x^{n-1}\right)^2 = x^2 y\ .$$

The proof of a_8 follows from the same argument

3.14.4 Lemma

If $k \geq 5$ we have;

(a) $a_9, a_{11} \to x$;

$(b)$$a_{12}, a_{10} \to y$.

Proof

$$(a)\ a_k = a_{k-4}^{-1} a_{k-1}^2$$

$$a_9 = a_5^{-1} a_8^2 \to (x^{n-1})^{-1} \left(x^2 y\right)^2 = x.$$

The proof of a_{11} follows from the same argument

$(b)\ a_k = a_{k-4}^{-1}a_{k-1}^2$

$$a_{10} = a_6^{-1}a_9^2 \to \left(x^2y\right)^{-1}x^2 = y$$

The proof of a_{12} follows from the same argument.

It is now clear from lemmas 3.14.3 and 3.14.4 and equations (3.13) and (3.14) that the map:$\to$ defined from the first 3 generators of $F(3,8)$ onto the three generators of D_n is indeed morphism onto D_n.

We define a mapping from the first $4r+3$ generators of $F(4r+3,\ 8r+8)$ onto the two generators of D_n by

$$a_1, a_{2r+3} \to x \quad \text{and} \qquad a_i \to y \ \ i = 2,3,\ldots,2r+2,2r+4,\ldots,4r+3. \qquad (3.15)$$

Then we immediately see that

$$a_{4r+4} = a_1 a_2 \cdots a_{4r+3} = xy^{2r+1}xy^{2r} \ = \ y \qquad (3.16).$$

We shall henceforth use lemma 3.14.1 and equations (3.15) to (3.16) whenever necessary without mentioning. to prove Lemmas 3.14.5 and 3.14.6.

3.14.5 Lemma

For $r \geq 1$,

$(a)\ a_{4r+5} \to x^{n-1};$

$(b)\ a_{4r+6} \to x^2y;$

$(c)\ a_{4r+i} \to \ y \qquad\qquad 7 \leq i \leq 2r+6.$

Proof

$(a)\ a_{4r+k} = a_{k-4}^{-1}a_{4r+k-1}^2$

$$a_{4r+5} = a_1^{-1}a_{4r+9}^2 \to x^{-1}\left(y\right)^2 = x^{n-1}.$$

(b) $a_{4r+k} = a_{k-4}^{-1} a_{4r+k-1}^{2}$.

$$a_{4r+6} = a_{2}^{-1} a_{4r+5}^{2} \to y^{-1}\left(x^{n-1}\right)^{2} = x^{2}y.$$

(c) We carry out the proof by induction.

Basis step: By Lemma 3.14.1, (3.15) and (b) above

$$a_{4r+7} = a_{3}^{-1} a_{4r+6}^{2} \to y^{-1}\left(x^{2}y\right)^{2} = y.$$

Induction step: suppose that $a_{4r+k} \to y \quad (i = k = 7, 8, \ldots, 2r+5)$.

Then using Lemma 3.14.1 again, we see that

$$a_{4r+k+1} = a_{k-3}^{-1} a_{4r+k}^{2} \to y^{-1}y^{2} = y,$$

as required.

<u>3.14.6 Lemma</u>

$(a)\, a_{6r+7} \ \to\ x^{n-1}$;

$(b)\, a_{6r+8} \ \to\ x^{2}y$;

$(c)\, a_{6r+i} \ \to\ y \quad (9 \le i \le 2r+8)$.

Proof

(a). $a_{6r+k} = a_{2r+k-4}^{-1} a_{6r+k-1}^{2}$

$$a_{6r+7} = a_{2r+3}^{-1} a_{6r+6}^{2} \to x^{-1}\left(y\right)^{2} = x^{n-1}.$$

(b). $a_{6r+k} = a_{2r+k-4}^{-1} a_{6r+k-1}^{2}$

$$a_{6r+8} = a_{2r+4}^{-1} a_{6r+7}^{2} \to y^{-1}\left(x^{n-1}\right)^{2} = x^{2}y.$$

(c). The assertion may be proved by induction on $i = k$.

Basis step: for $k = i = 9$ we see that

$$a_{6r+k} = a_{2r+k-4}^{-1} a_{6r+k-1}^{2}$$

$$a_{6r+9} = a_{2r+5}^{-1}a_{6r+8}^{2} \to y^{-1}\left(x^2y\right)^2 = y.$$

Induction step: suppose that $a_{6r+k} \to y \quad 9 \le k \le 2r+7$

Then using Lemma 3.14.1 again, we see that

$$a_{6r+k+1} = a_{(2r-3)+k}^{-1}a_{6r+k}^{2}$$

since $k \ge 9$ it is clear that $(2r-3)+k \ge 2r+3$ and any number say $a_m > a_{2r+3} \to y$ from (3.15) also, $a_{6r+k} \to y$ from the induction step, hence

$$a_{6r+k+1} = a_{(2r-3)+k}^{-1}a_{6r+k}^{2} \to y^{-1}y^2 = y$$

as required.

<u>3.14.7 Lemma</u>

$(a)\, a_{8r+i} \;\to\; x \quad i = 9,\ 0r\ \ 2r+11;$

$(b)\, a_{8r+j} \;\to\; y \quad j = 10,11,\ldots,2r+10,2r+12,\ldots,4r+11;$

Proof

We shall apply lemma 3.14.1, (3.15) and (3.16) to prove (a) and (b).

(a) *If* $k = i = 9$

$$a_{8r+k} = a_{4r+k-4}^{-1}a_{8r+k-1}^{2}$$

$$a_{(8r+8)+1} = a_{4r+5}^{-1}a_{8r+8}^{2} \to \left(x^{n-1}\right)^{-1}\left(x^2y\right)^2 = x.$$

If $k = i = 2r+10$

$$a_{8r+(2r+10)} = a_{4r+(2r+10)-4}^{-1}a_{8r+(2r+9)}^{2}$$

$$a_{8r+(2r+10)} = a_{4r+(2r+10)-4}^{-1}a_{8r+(2r+9)}^{2} \to (y)^{-1}(y)^2 = y$$

If $k = i = 2r+11$

$$a_{8r+(2r+11)} = a_{4r+(2r+11)-4}^{-1}a_{8r+(2r+10)}^{2}$$

$$a_{8r+(2r+11)} = a^{-1}_{4r+(2r+11)-4}a^{2}_{2r+2} \to \left(x^{n-1}\right)^{-1}(y)^2 = x$$

$(b)\, a_{8r+j} \;\; \to \; y \qquad j = 10,11,\ldots,2r+10,2r+12,\ldots,4r+11$

The proof is by induction.

$$a_{8r+k} = a^{-1}_{4r+k-4}a^{2}_{8r+k-1}.$$

Basis step: For *If* $k = j = 10$ we have,

$$a_{(8r+8)+2} = a^{-1}_{4r+6}a^{2}_{(8r+8)+1} \to \left(x^2y\right)^{-1}(x)^2 = y$$

Induction step: suppose that $a_{8r+k} \to y$ for $k = 10,11,\ldots 2r+10,2r+12,\ldots,4r+11$

$$a_{8r+k+1} = a^{-1}_{4r+k-3}a^{2}_{8r+k}$$

.

From Lemma 3.14.5, $a_{4r+i} \to y \quad 7 \le i \le 2r+6$ thus,

$$a_{4r+i-3} \to y \quad 10 \le i \le 2r+9$$

$$a_{8r+k+1} = a^{-1}_{4r+k-3}a^{2}_{8r+k} \to y^{-1}y^2 = y$$

as required.

It is now clear from lemmas 3.14.5 to 3.14.7 and equations (3.13) to (3.16) that the map:→ defined from the first 2 generators of $F(4r+3,\, 8r+8)$ onto the two generators of D_n is indeed morphism onto D_n

3.15 THE FIBONACCI GROUP $F(4r+5,\ 8r+12)$

Consider the Fibonacci group

$$F(4r+5,\ 8r+12) = < a_1, a_2, \ldots, a_{8r+12} \left| a_i a_{i+1} \cdots a_{i+4r+4} = a_{i+4r+5} \right. \; i = 1,2,\ldots,8r+12 >$$

where subscripts are taken modulo $8r+12$ if necessary.

3.15.1 Lemma

For all $k > 5$ and $r \geq 0$.

(a). $a_{4r+k} = a_{k-6}^{-1} a_{4r+k-1}^{2}$;

(b). $a_{6r+k} = a_{2r+k-6}^{-1} a_{6r+k-1}^{2}.$;

(c) $a_{8r+k} = a_{4r+k-6}^{-1} a_{8r+k-1}^{2}..$

Proof

We proof this lemma in a similar way we prove lemma 3.14.3.

(a). $a_{4r+k} = a_{k-5} a_{k-4} \cdots a_{4r+k-2} a_{4r+k-1}$

$= a_{k-6}^{-1} (a_{k-6} a_{k-5} \cdots a_{4r+k-2}) a_{4r+k-1}$

$= a_{k-6}^{-1} a_{4r+k-1}^{2}.$

. (b) $a_{6r+k} = a_{2r+k-5} a_{2r+k-4} \cdots a_{6r+k-1}$

$a_{6r+k} = a_{2r+k-6}^{-1} (a_{2r+k-6} a_{2r+k-5} \cdots a_{6r+k-2}) a_{6r+k-1}$

$= a_{2r+k-6}^{-1} a_{6r+k-1}^{2}.$

. (c) $a_{8r+k} = a_{4r+k-5} \cdots a_{8r+k-2} a_{8r+k-1}$

$= a_{4r+k-6}^{-1} (a_{4r+k-6} a_{4r+k-5} \cdots a_{8r+k-2}) a_{8r+k-1}$

$= a_{4r+k-6}^{-1} a_{8r+k-1}^{2}.$

We now give the main result of this section.

3.15.2 Proposition

There exist a morphism from $F(4r+5,\ 8r+12)$ onto $D_n\ (for\,all\ \ n \geq 3)$.

Hence $F(4r+5,\ 8r+12)$.is infinite.

We carry out the proof in a similar way we prove $F(4r+3,\, 8r+8)$ We consider the case of $r=0$ first, then $r \geq 1$.

We define a mapping from the first 5 generators of $F(5,12)$ onto the two generators of D_n by

$$a_1, a_3 \to x \text{ and } a_i \to y \qquad i = 2,4,5 \qquad (3.17).$$

Then we immediately see that

$$a_6 = a_1 a_2 a_3 a_4 a_5 \to xyxy^2 = y^3 = y. \qquad (3.18).$$

3.15.3 Lemma

If $r=0$ then, the following mappings hold in $F(5,12)$

(a). $a_7, a_9 \to x^{n-1}$;

(b). $a_8, a_{10} \to x^2 y$;

(c). $a_{11}, a_{12} \to y$.

Proof

We shall apply Lemma 3.15.1 to prove (a) and (b)

$$(a) a_k = a_{k-6}^{-1} a_{k-1}^2$$

$$a_7 = a_1^{-1} a_6^2 \to x^{-1}(y)^2 = x^{n-1}.$$

The proof of a_9 follows from the same argument

$$(b) a_k = a_{k-6}^{-1} a_{k-1}^2$$

$$a_8 = a_2^{-1} a_7^2 \to y^{-1}\left(x^{n-1}\right)^2 = x^2 y.$$

The proof of a_{10} follows from the same argument

$$(d) a_k = a_{k-6}^{-1} a_{k-1}^2$$

$$a_{11} = a_5^{-1} a_{10}^2 \to y^{-1}\left(x^2 y\right)^2 = y.$$

The proof of a_{12} follows from the same argument

3.15.4 Lemma

If $r = 0$ then the following mappings hold in $F(5,12)$

(a) $a_{13}, a_{15} \to x$

(b) $a_k \to \ y \quad k = 14,16 \ and \ 17$

Proof

$$(a) a_k = a_{k-6}^{-1} a_{k-1}^2$$

$$a_{13} = a_7^{-1} a_{12}^2 \to \left(x^{n-1}\right)^{-1} (y)^2 = x.$$

The proof of a_{15} follows from the same argument

$$(b) a_k = a_{k-6}^{-1} a_{k-1}^2$$

$$a_{14} = a_8^{-1} a_{13}^2 \to \left(x^2 y\right)^{-1} x^2 = y.$$

The proof of a_k, $k = 16 \ and \ 17$ follows from the same argument

We now consider the case of $r \geq 1$.We define a mapping from the first $4r+5$ generators of $F(4r+5,\ 8r+12)$ onto the two generators of D_n

$$a_1, a_{2r+3} \to x \quad \text{and} \quad a_i \to y \quad i = 2,3,\ldots,2r+2,2r+4,\ldots,4r+5. \qquad (3.19).$$

Then we immediately see that

$$a_{4r+6} = a_1 a_2 \cdots a_{4r+5} \to xy^{2r+1} xy^{2r+2} = y^{4r+3} = y. \qquad (3.20).$$

3.15.5 Lemma

For $r \geq 1$.

(a) $a_{4r+7} \to x^{n-1}$

$(b)\ a_{4r+8} \rightarrow x^2 y$

$(c)\ a_{4r+i} \rightarrow y \quad 9 \leq i \leq 2r+8$

Proof

We shall apply lemma 3.15.1 and equation (3.19) and (3.20) to prove (a) (b) and (c)

$(a)\ a_{4r+k} = a_{k-6}^{-1} a_{4r+k-1}^2$

$a_{4r+7} = a_1^{-1} a_{4r+6}^2 \rightarrow x^{-1}(y)^2 = x^{n-1}$

$(b) a_{4r+k} = a_{k-6}^{-1} a_{4r+k-1}^2$

$a_{4r+8} = a_2^{-1} a_{4r+7}^2 \rightarrow y^{-1}(x^{n-1})^2 = x^2 y$

(c)We use induction on $i = k$.

Basis step: By lemma 3.15.1 and equation (3.19) and (3.20), we see that for $k = 9$

$$a_{4r+9} = a_3^{-1} a_{4r+8}^2 \rightarrow y^{-1}(x^2 y)^2 = y.$$

Induction step: suppose that $a_{4r+k} \rightarrow y \quad 9 \leq k \leq 2rt+7.$

Then using Lemma 3.15.1 again, we see that

$$a_{4r+k+1} = a_{k-5}^{-1} a_{4r+k}^2 \rightarrow y^{-1} y^2 = y,$$

as required.

<u>3.15.6 Lemma</u>

For $r \geq 1$

$(a)\, a_{6r+9} \rightarrow x^{n-1}$

$(b)\, a_{6r+10} \rightarrow x^2 y$

$(c)\ a_{6r+i} \ \rightarrow\ y \qquad 11 \le i \le 2r+12$

Proof

We shall apply lemma 3.15.1 and equation (3.19) and (3.20) to prove (a) (b) and (c)

(a) $a_{6r+9} = a_{2r+3}^{-1} a_{6r+8}^{2} \rightarrow x^{-1}(y)^2 = x^{n-1}$

(b) $a_{6r+10} = a_{2r+4}^{-1} a_{6r+9} \rightarrow y^{-1}(x^{n-1})^2 = x^2 y$

(c) the assertion may be proved by induction on $i = k$.

Basis step: for $k = 11$ we see that

$$a_{6r+11} = a_{2r+5}^{-1} a_{6r+10}^{2} \rightarrow y^{-1}(x^2 y)^2 = y.$$

Induction step: suppose that $a_{6r+k} \rightarrow y \quad 11 \le k \le 2r+11$

Then using Lemma 3.15.1 again, we see that

$$a_{6r+k+1} = a_{(2r-5)+k}^{-1} a_{6r+k}^{2}$$

Since $k > 10$ it is clear that $(2\text{r}-5)+\text{k} > 2\text{r}+3$ also $a_{6r+k} = x^{n-1}$, hence

$$a_{6r+k+1} = a_{(2r-5)+k}^{-1} a_{6r+k}^{2} \rightarrow y^{-1} y^2 = y.$$

as required.

<u>3.15.7 Lemma</u>

$(a)\ a_{8r+i} \ \rightarrow\ x \quad i = 13,\ and\ \ 2r+15$

$(b)\ \ a_{8r+j} \ \rightarrow\ y \quad j = 14, 15, \ldots, 2r+14, 2r+16, \ldots, 4r+17$

Proof

We shall apply lemma 3.15.1 and equation (3.19) and (3.20) to prove (a) and (b).

(a) $If \;\; i=k=13$

$$a_{8r+k} = a_{4r+k-6}^{-1}a_{8r+k-1}^{2}.$$

$$a_{8r+13} = a_{4r+7}^{-1}a_{8r+12}^{2} \rightarrow \left(x^{n-1}\right)^{-1}(y)^{2} = x$$

$If \;\; i=2r+15$

$$a_{8r+(2r+15)} = a_{4r+(2r+15)-6}^{-1}a_{8r+2r+14}^{2}$$

$$= a_{6r+9}^{-1}a_{2r+2}^{2} \rightarrow \left(x^{n-1}\right)^{-1}(y)^{2} = x$$

(c) Here we use induction on $j=k$.

Basis step: For $j=14$ we have,

$$a_{8r+k} = a_{4r+k-6}^{-1}a_{8r+k-1}^{2}.$$

$$a_{8r+14} = a_{4r+14}^{-1}a_{(8r+14)-1}^{2}$$

$$a_{(8r+12)+2} = a_{4r+8}^{-1}a_{(8r+12)+1}^{2} \rightarrow \left(x^{2}y\right)^{-1}x^{2} = y.$$

Induction step: suppose that $a_{8r+j} \rightarrow y \quad j=14,15,\ldots,2r+14,2r+16,\ldots,4r+16$

$$a_{8r+k+1} = a_{4r+k-6}^{-1}a_{8r+k}^{2}$$

From Lemma 3.15.5, $a_{4r+j} \rightarrow y \quad 9 \le j \le 2r+8$ thus,

$$a_{4r+j-6} \rightarrow y \quad 15 \le j \le 2r+14$$

$$a_{8r+k+1} = a_{4r+k-6}^{-1}a_{8r+k}^{2} \rightarrow y^{-1}y^{2} = y.$$

as required.

CHAPTER FOUR
SUMMARY OF RESULTS, CONTRIBUTIONS AND AREAS FOR FURTHER RESEACH

4.1 SUMMARY OF RESULTS

We have, in this thesis, accomplished the following:

1. We obtained and discussed formulae for the number of even permutations (of an n-element set) having exactly k fixed points in the alternating group.

2. We obtained generating functions for the number of even permutations having exactly k fixed points in alternating group.

3. We also obtained similar results (as in 1 and 2 above) for the number of odd permutations having exactly k fixed points and their generating functions in the alternating group.

4. We give a geometric proof for the number of even (odd) permutations (of an n-element set) having exactly k fixed points in the dihedral group.

5. We give an algebraic proof in line of Catarino and Higgins (1999) for the number of even (odd) permutations having exactly k fixed points, in the dihedral group.

6. We proved the three families: $F(2r,4r+2)$, $F(4r+3,8r+8)$ and $F(4r+5,8r+12)$ of the Fibonacci groups $F(m,n)$ to be infinite by defining morphism between Dihedral groups and the Fibonacci groups.

7. We give an alternative prove of the Cauchy's formula $f(m,n)$ for be the number of permutations of X_n that can be express as a product of $r_i(m-i+1, i=1,2,\cdots,m-1)$ cycles.

4.2 CONTRIBUTIONS TO KNOWLEDGE

1. We obtained and discussed formulae for the number of even and odd permutations (of an $n-$element set) having exactly k fixed points in the alternating group and the generating functions for the fixed points.

2. We give two different proofs of the number of even and odd permutations (of an $n-$element set) having exactly k fixed points in the dihedral group, one geometric and the other algebraic. In the algebraic proof, however, we further obtain the formulae for determining the fixed points.

3. We proved the three families; $F(2r,4r+2)$, $F(4r+3,8r+8)$ and $F(4r+5,8r+12)$ of the Fibonacci groups $F(m\,,n)$ to be infinite by defining Morphism between Dihedral groups and the Fibonacci groups.

4. We give an alternative prove of the Cauchy's formula for the number permutations with a given cycle structure.

4.3 AREAS FOR FURTHER RESEACH

1. The new method we introduced may be tested for the two families $F(7+5i,5)$ and $F(8+5i,5)$ for integers $i \geq 0$ that remain unsettled by creating morphism between the Fibonacci groups and a suitable permutation group

2. There is room for further research in the determination of more combinatorial properties of the permutation groups we discussed and other permutation groups.

3. The study of classification of transitive p groups of degree say p^m in line with Audu (1986a) can be considered, by obtaining the number of k fixed

points and the generating functions for the fixed points of transitive p groups of degree say p^m.

4. The study of permutations as even(odd) according to its length can be considered using number of fixed points.

5. The number of even (odd) permutations with a given cycle structure.

6. The number of cycle structures in a given permutation.

REFERENCES

Apine, E. (2000) On Transitive p-Groups of Degree p^2 or p^3. PhD *Thesis University of Jos.*

Audu, M. S. (1986a). Generating sets for transitive permutation groups of prime-power order. *Abacus* 17 (2): 22-26.

Audu, M. S. (1988b). The structure of the permutation modules for transitive p-groups of degree p^2. *Journal of Algebra* 17:227-239.

Audu, M. S. (1988c). The structure of the permutation modules for transitive abelian groups of prime-power order. *Nigerian Journal of Mathematics and Applications* 17: 1-8.

Audu, M. S. (1988d). The number of transitive p-groups of degree p^2. *Advances in Modeling and Simulation Enterprises Review* 7(4): 9-13.

Audu, M. S. (1989e). Groups of prime-power order acting on models over a modular field. *Advances in Modeling and Simulation Enterprises Review* 9 (4): 1-10.

Audu, M. S. (1991f). On transitive permutation groups. *Afrikan Mathematika Journal of African Mathematical Union* 4(2): 155-60.

Audu, M. S., Momoh, S. U. & Apine, E. (1994). On the classification of transitive p-groups of degree p^3. *Nigerian Journal of Mathematics and Applications* 7:1-12.

Ali, B. & Umar, A. (Accepted 20008). Some combinatorial properties of the alternating groups. *South East Asian mathematical Ass. Bull.* In press.

Balakrishnan, V.K. (1995). Combinatorics: Including Concepts of Graph. Theory Schaum's Outline Series, McGraw Hill Inc.

C. M. Campbell and P. P. Campbell Search techniques and epimorphisms between certain groups and Fibonacci groups *CIRCA Technical Report University of St Andrews* 2004/10(2004).

Catarino, P.M. & Higgins, P.M. (1999). The monoid of orientation-preserving mappings on a chain. *Semigroup Forum* 58:190-206.

Catarino, P.M. (2000). Monoids of orientation-preserving transformations of a finite chain and their presentation. *Semigroup Forum* 60:262-276.

Cemeron, P. J. (1999).Oligomorphic Permutation Groups. Cambridge: University Press, 159P.

Cemeron, P. J. (2001). Combinatorics Topics Techniques Algorithm, Cambridge: University Press.

Cemeron, P. J. (2000). Sequences realized by oligomorphic permutation groups. *Journal. Integer Sequence* 30:1.5.

Comlet, L. (1974). Advanced Combinatorics the Art of Finite and Infinite Expansions. Dordrecht, Holland: D. Reidel Publishing Company.

Conwal, H. (1965) Advanced problem 5327, *Amar. Math. Monthly* 72:915.

Conwal, J. H. et al, (1967) Solution to advanced problem 5327, *Amer. Math Monthly* 74: 91–93.

Campbell, C. M., Campbell, P. P., Doughe, H. & Roberson, E. F. (2002) On the Fibonacci length of powers of dihedral groups, *Journal of Pure and Applied Algebra* 57 – 73.

Elick, B. & Hofling, B. (2003). The soluble primitive permutation groups of degree at most 6560. *LMSS Computorial Mathematics* 6:29-39.

Feller, W. (1968). An Introduction to Probability Theory and its Applications.3rd edn, Witey.

Fernandes, V.H. (1997). Semigroups of order preserving mappings on a finite chain: a new class of divisions. *Semigroup Forum* 54:230-236.

Fernandes, V.H. (2000). The monoid of all injective orientation preserving partial transformations on a finite chain. *Communications in Algebra* 28(7): 3401-3426.

Fernandes, V.H. (2003).The monoid of all injective order preserving transformations, of a finite chain. *Semigroup Forum 65:56-70.*

GAP Groups. *http://www.gap-system.org. Algorithms and Programming* Version 4.3, 2002.

Gallia, J. A. (1998). Contemporary Abstract Algebra. Boston/New York: Houghton Mittlin.

Gorenstein, D. (1985). Finite Simple Groups: An Introduction to Their Classification. New York: Plenum Press, 333p.

Gregory, B. (1993). The transitive groups of degree fourteen and fifteen. *Journal of Symbolic Computation* 16 (4):13-422.

Gregory, B. & John, M. (1993). The transitive groups of degree up to 11. *Communication I n Algebra* 11: 863-911.

Gomes, G. S. S. & Howie J. M. (1992). On the ranks of certain semigroups of order-preserving transformations. *Semigroup Forum* 45:272-282.

Hans, U. B. & Bettina, E. (1999). The groups of order at most 1000 except 512 and 768. *Journal of Symbolic Computation* 27 (4):405-413.

Higgins, P. M. (1992a). Techniques of Semigroup Theory. Oxford: University Press.

Higgins, P. M. (1993b). Combinatorial results for semigroups of order preserving mappings. *Mathematics Proceedings of London Philosophical Society* 113:281-296.

Howie, J. M. (1995). Fundamentals of Semigroup Theory. Oxford: Claredon Press.

Howie, J. M. Combinatorial and Arithmetical Aspects of the Theory of Transformation Semigroups. *Lectures gives at university* of *LIBS,* 1990.

Hulpke, A. (2004). Constructing transitive permutation groups. J*ournal of Symbolic Computation 89-112.*

Laradji, A. & Umar, A. (2007). Combinatorial results for the symmetric inverse semigroups.*Semigroup Forum* (75):221-236.

Laradji, A. & Umar, A. (2004b). Combinatorial results for semigroups of order decreasing partial transformations. *Journal of Integer Sequence 7(4): 3- 8.*

Laradji, A. & Umar, A. (2004d). On the number of decreasing and order-preserving partial transformations. *Technical report No. 312, Department of Mathematical Science, KFUPM, Saudi Arabia.*

Liu, G. L. (1968) Introduction to Combinatorial Mathematics. New York: Mc Graw Hill Company.

Momoh, S. U. (1999) Representation of p-Groups and Transitivity of Groups. *PhD. Thesis, University of Jos*.

Odlyzko, A. M. (1995).Asymptotic Enumeration Methods: Handbook Combinatorics 1&2:1063-1229 Amsterdam: Elsevier.

Problem E2354, (1972) *America Math. Monthly* 79,394.

Umar, A. (1997). Some remarks about Fibonacci groups Semigroups. *Communications in Algebra*, Mercel Dekier, Inc. 25 (12): 3973–3977.

Sloane, J.A. The on-line Encyclopedia of Integer Sequences, http://www.research.alt.com.njas/sequences/.