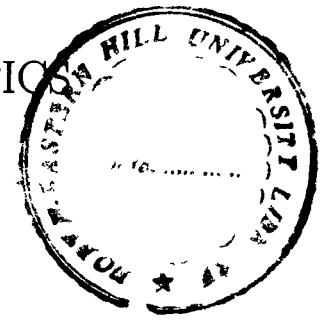
COMMUTATIVITY DEGREES OF FINITE GROUPS – A SURVEY

BY

RAJAT KANTI NATH
DEPARTMENT OF MATHEMATICS



SUBMITTED
IN PARTIAL FULFILMENT OF THE
REQUIREMENT OF THE DEGREE OF

MASTER OF PHILOSOPHY
IN
MATHEMATICS

TO

NORTH-EASTERN HILL UNIVERSITY
SHILLONG – 793022, INDIA
FEBRUARY, 2008

CERTIFICATE

I certify that the dissertation entitled "COMMUTATIVITY DEGREES OF FINITE GROUPS - A SURVEY" submitted by Mr. Rajat Kanti Nath in partial fulfilment of the requirement of the degree of Master of Philosophy in Mathematics is the outcome of a study undertaken by the candidate.

I certify that the sources from which ideas have been borrowed have been duly referred to.

The material in this dissertation has not been presented for the award of a degree in any university before.

This dissertation may be placed before the examiners for evaluation and necessary formalities. I certify that this dissertation is worthy of consideration by the examiners.

Ashish Kumar Das

Supervisor
Department of Mathematics
North-Eastern Hill University
Shillong – 793022

Place: Shillong.
20^{th} February, 2008.

NORTH-EASTERN HILL UNIVERSITY

February, 2008

DECLARATION

I, Rajat Kanti Nath, hereby declare that the subject matter in this dissertation is the record of work done by me, that the contents of this dissertation did not form basis of the award of any previous degree to me or to the best of my knowledge to anybody else, and that the dissertation has not been submitted by me for any research degree in any other university/institute.

This dissertation is being submitted to the North-Eastern Hill University for the degree of Master of Philosophy in Mathematics.

Rajat Kanti Nath
Signature of the Candidate

Countersigned by:

Signature of the Head

Head
Department of Mathematics,
North-Eastern Hill University
Shillong-7930022

Signature of the Supervisor

DR. A. K. DAS, READER
MATHS DEPT., NEHU,
SHILLONG-22, MEGHALAYA

ACKNOWLEDGEMENT

This work was carried out under the supervison of Dr. Ashish Kumar Das, Department of Mathematics, North-Eastern Hill University. I wish to express my sincere thanks and gratitude to him for his guidance and invaluable help during the preparation of this dissertation.

I express my gratitude to Dr. P. K. Saikia, Dr. S. Dutta and Dr. A. M. Buhphang, Department of Mathematics, N.E.H.U., for giving M. Phil. courses and also for providing me with lots of help and suggestions.

I also express my gratitude to Prof. H. K. Mukerjee and Prof. M. B. Rege, Department of Mathematics, N.E.H.U., for their help and suggestions.

I am also thankful to Mr. A. T. Singh and all other faculty members of the Department of Mathematics, N.E.H.U., for their help and cooperation.

I am very much indebted to all the Research Scholars and the office staffs of the Department of Mathematics, N.E.H.U., for extending all possible help to me.

I am grateful to all my relatives and friends for their support and for being my constant source of inspiration.

Finally, I am grateful to all my family members, especially my parents and my brother Probir, for giving me constant encouragement and providing me with unbelievable opportunities to continue my studies.

Rajat Kanti Nath

PREFACE

A student studying both probability and algebra might well ask the question "What is the probability that two group elements, chosen at random will commute?" The answer is given by what is known as commutativity degree of a group. The commutativity degree $\Pr(G)$ of a finite group G is defined as

$$\Pr(G) = \frac{\text{Number of ordered pairs } (x,y) \in G \times G \text{ such that } xy = yx}{\text{Total number of ordered pairs } (x,y) \in G \times G}.$$

Commutativity degree is a kind of measure for abelianness of a group. Obviously, if G is abelian then this probability is 1. An important formula for commutativity degree is $\Pr(G) = k(G)/|G|$, where $k(G)$ is the number of conjugacy classes of G, was established by W. H. Gustafson [18] using the technique used by P. Erdös and P. Turán [12], in their study on some problems of statistical group theory. One of the oldest known results on commutativity degree (going back at least to Miller, 1944 [39]) is that $\Pr(G) \leq 5/8$ for finite non-abelian groups which first appeared in print in 1973 when W. H. Gustafson [18] showed that an analogous bound holds for compact non-abelian groups.

In 1969, K. S. Joseph [29] made an elaborate study of this notion. Later, in 1979, D. J. Rusin [43] has been obtained an explicit computation of $\Pr(G)$ for finite groups G with $G' \leq Z(G)$ and also for groups with $G \cap Z(G) = \{1\}$.

He also gave some limiting conditions and classified all finite groups having commutativity degree greater than $11/32$. In fact this was the first classification of groups ever done in terms of commutativity degree. After quite sometime around 1995, P. Lescot [32] classified up to isoclinism, all finite groups for which commutativity degree is greater than or equal to $1/2$. It may be mentioned here that the concept of isoclinism between groups was introduced by Philip Hall [19]. Two groups G and H are said to be isoclinic if $G/Z(G)$ and $H/Z(H)$ are isomorphic, so also G' and H' (via. ϕ_1 and ϕ_2 respectively), and $a_H \circ (\phi_1 \times \phi_1) = \phi_2 \circ a_G$ where a_G (similarly a_H) is given by $a_G(xZ(G), yZ(G)) = [x, y] \quad \forall\, x, y \in G$.

After six years of this classification, in around 2001, P. Lescot [33] classified, up to isomorphism, all finite groups for which commutativity degree is greater than or equal to $1/2$.

The first decade of this millenium is a remarkable decade in the history of commutativity degree. After Lescot [33], in 2006, F. Barry, D. MacHale and Á. Ní Shé [1] studied some supersolvability and CLT (Converse of Lagranges Theorem) conditions for finite groups using commutativity degree. In the same year 2006, R. M. Guralnick and G. R. Robinson [17] pointed out some general properties of $\Pr(G)$ which have not been observed before. Also they pointed out that the solution of the (coprime) $k(GV)$-problem can yield quite strong information about commutativity degree. The (coprime) $k(GV)$-problem is to show that whenever p is a prime and G is a p'-group acting faithfully on the $G\mathbb{F}(p)$-module V, then $k(GV) \leq |V|$. This has re-

cently been solved in full generality in [16].

The original notion of commutativity degree was generalized in a number of ways. The first generalization has been done way back in around 1975, by Gary Sherman [46]. He studied the probability that an automorphism fixes a group element, which gives commutativity degree in a special case. In the next year 1976 D. Machale [37] made an study of 'commutativity degree in finite rings' denoted by $\Pr(R)$, which is anologous to 'commutativity degree in finite groups'. The concept of conjugacy in groups has no obvious analogue in rings even though there are many results for $\Pr(R)$ which are very similar to those for $\Pr(G)$, however, the methods of proofs are quite different. Then after 16 years, in 1994, J. L. Leavitt, G. J. Sherman and M. E. Walker [34] tried to relate this concept with rewriteability in finite groups, which is some kind of generalization of the notion of commutativity and they found a relation between 3-rewriteability and commutativity degree. However, lots of works are yet to be done in this direction.

Just a few years back, in around 1995, P. Lescot [32] defined 'multiple commutativity degree. Recently, in 2005, M. R. R. Moghaddam, K. Chiti and A. R. Salemkar [40] defined 'n^{th} nilpotency degree'. In 2007, A. Erfanian, R. Rezaei, and P. Lescot [13] defined 'relative commutativity degree' and 'relative n^{th} nilpotency degree'. These concepts are closely related to the concept of commutativity degree.

Most recently, in the beginning of the year 2008, M. R. Pournaki and

R. Sobhani [41] studied the 'probability that the commutator of two group elements is equal to a given element', which we call the 'g-commutativity degree'. In fact their work extends the results of Rusin [43].

In Chapter 1, we have collected some of the basic definitions, notations and conventions from the theory of groups, to be used in the succeeding chapters. We also recall the notion of characters of finite groups and list a few properties of group charaters including orthogonality relations.

In Chapter 2, we study the notion of commutativity degree of a finite group including its computations for some non-trivial classes of finite groups. Some of the important results are given bellow:

Theorem 2.1.8

(i) *Commutativity degree is a monotonically decreasing function. i.e., if H is a subgroup of G then $\Pr(G) \leq \Pr(H)$ with equality if and only if $C_G(g)H = G$.*

(ii) *Commutativity degree is a completely multiplicative function. i.e., if G and H are two finite groups then $\Pr(G \times H) = \Pr(G) \cdot \Pr(H)$.*

(iii) *For any normal subgroup N of G, $\Pr(G) \leq \Pr(G/N)\Pr(N)$. The equality holds if and only if $C(g \bmod N) = NC_G(g)$ for each $g \in G$.*

Theorem 2.2.3 *Let G be a non-abelian group and p is the least prime*

number which divides $|G|$, *then*

$$\Pr(G) \leq \frac{1}{p^2}\left(1 + \frac{p^2-1}{|G'|}\right)$$

In particular, we have $\Pr(G) \leq (p^2+p-1)/p^3$ with equality holding if and only if $G/Z(G)$ has order p^2.

Theorem 2.3.1 *Let* G *be a finite group such that* $\mathrm{cd}(G) = \{1, m\}$, $m > 1$, *then*

$$\Pr(G) = \frac{1}{|G'|}\left(1 + \frac{|G'|-1}{m^2}\right)$$

Proposition 2.4.8 *If* G *is a* p*-group with* $G' \leq Z(G)$, *then*

$$\Pr(G) = \frac{1}{|G'|}\left[1 + \sum \frac{(p-1)[G':K]/p}{p^{n(K)}}\right].$$

where the sum is over all subgroups K *of* G' *such that* G'/K *is non-trivial cyclic and* $n(K)$ *is a positive number associated to* K.

In Chapter 3 there are three sections. In the first section we study classification of groups having commutativity degree more than 11/32 [43]. In the next section we discuss the concept of isoclinism [19]. In this section we have studied properties of isoclinism between groups some of which are mentioned below

Lemma 3.2.3 *If* G *and* H *are isomorphic then they are isoclinic as well.*

Lemma 3.2.5 *Let* G *and* H *be two isoclinic groups; then* $\Pr(G) = \Pr(H)$.

Proposition 3.2.6 *Let* G *be any group (finite or infinite). Then there is a group* G_1 *isoclinic to* G *such that* $Z(G_1) \subseteq G_1'$. *If* G *is finite, so is any such* G_1.

one of the main objectives of this section is to give an alternative proof of the following result

Corollary 2.5.4 *Let G be a finite group such that $G' \cap Z(G) = \{1\}$; then there is a finite group K such that $\Pr(K) = \Pr(G)$, $K' \cong G'$ and $Z(K) = \{1\}$.*

Finally, in the last section of this chapter we study classification, up to isoclinism [32], of groups having commutativity degree at least $1/2$. Here the main result is

Theorem 3.3.1 *Let G be a finite group such that $\Pr(G) \geq \frac{1}{2}$, then G is isoclinic to exactly one of the following:*

(i) *trivial group $\{1\}$,*

(ii) *an extraspecial 2-group,*

(iii) *S_3, the symmetric group of three symbols.*

Also, in this section we study classification, up to isomorphism [33], of groups having commutativity degree at least $1/2$. Here the main result is

Theorem 3.3.6 *A finite group G has commutativity degree $\Pr(G) \geq \frac{1}{2}$ if and only if one of the following holds:*

(i) *G is abelian,*

(ii) *$G \cong P \times A$, where P is a 2-group such that $|P'| = 2$, and A is an abelian group of odd order,*

(iii) $G \cong G_m \times A$, *where* $m \geq 1$, A *is abelian and* $G_m = < \sigma, \tau | \sigma^3 = \tau^{2^m} = 1, \tau^{-1}\sigma\tau = \sigma^{-1} >$.

In Chapter 4, we study some conditions in terms of *commutativity degree* under which a finite group acquires certain special properties expressible in standard group-theoretic terms. The main objective of this section is to establish the following results:

Theorem 4.2.8

(i) *If the average size of a conjugacy class of* G *is less then 3, then* G *is both supersolvable and CLT;* A_4 *shows that this is the best possible result.*

(ii) *If* $|G|$ *is odd and average size of a conjugacy class of* G *is less then* $6\frac{9}{11}$, *then* G *is both supersolvable and CLT.* $G(75)$ *shows that this result is the best possible in both cases.*

In the last Chapter, we discuss various generalizations of the notion "commutativity degree of finite groups", like 'g-commutativity degree', 'multiple commutativity degree', 'n^{th} nilpotency degree', 'relative commutativity degree, 'relative n^{th} nilpotency degree', 'probability that an automorphism fixes a group element', 'Rewriteability in finite groups' etc. Finally we study 'commutativity degree of finite rings'- a concept that is analogous to 'commutativity degree of finite groups'.

Contents

List of Symbols

$\mathbb{Z}$	set of integers
$\mathbb{Z}^+$	set of positive integers
$\mathbb{N}$	$\mathbb{Z}^+ \cup \{0\}$, set of natural numbers
$\mathbb{Q}$	set of rational numbers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$H \leq G$	H is a subgroup of G
$H < G$	H is a proper subgroup of G
$H \subseteq G$	H is a subset of G
$H \subset G$	H is a proper subset of G
$H \trianglelefteq G$	H is a normal subgroup of G
$\|G : H\|$	index of H in G
G/N	factor group
HK	$\{hk \mid h \in H,\ k \in K\}$
$H \times K$	direct product of the groups H and K
$H \oplus K$	direct sum of the groups H and K
aH	$\{ah \mid h \in H\}$, left coset of H
$G \cong H$	G and H are isomorphic
$\langle a \rangle$	$\{a^n \mid n \in \mathbb{Z}\}$, the cyclic group generated by a
$\langle a_1, a_2, \cdots, a_n \rangle$	subgroup generated by $a_1, a_2, \cdots, a_n$

$o(g)$	order of g
$\|G\|$	order of the group G
$[x, y]$	$xyx^{-1}y^{-1}$, the commutator of x and y
$[H, K]$	$\langle\{[x, y] \mid x \in H, y \in K\}\rangle$
G'	$[G, G]$, the commutator subgroup or derived subgroup of G
y^g	gyg^{-1}, conjugate of y
$\mathrm{Cl}(g)$	conjugacy class of g
$k(G)$	number of conjugacy classes of G
$\mathrm{orb}(x)$	orbit of x
$\mathrm{stab}(x)$	stabilizer of x
$\mathrm{Aut}(G)$	automorphism group of G
$\mathrm{Inn}(G)$	inner automorphism group of G
$C_G(x)$	$\{y \in G : xy = yx\}$, centralizer of x in G
$N_G(H)$	normalizer of a subgroup H in G
χ	character
$\chi(1)$	degree of χ
$\mathrm{Irr}(G)$	set of all irreducible characters of G
$\mathrm{cd}(G)$	$\{\chi(1) : \chi \in \mathrm{Irr}(G)\}$, set of degrees of all irreducible characters of G
$\ker \chi$	$\{g \in G \mid \chi(g) = \chi(1)\}$, kernel of χ
$\det(A)$	determinant of A
$\mathrm{tr}(A)$	trace of A
$\mathrm{Ker}\,\phi$	kernel of the homomorphism ϕ

$\mathcal{G}$	set of all finite groups upto isomorphism
$\mathcal{G}_p$	set of all $G \in \mathcal{G}$ such that $\|G\|$ is divisible by the prime p but by no other smaller prime
G_p	p-group
$G_{p'}$	p'-group, group whose order is relatively prime to p
C_n	cyclic group of order n
D_n	dihedral group of order $2n$
Q_{2^n}	quaternion group of order 2^n, dicyclic group
S_n	symmetric group of degree n
A_n	alternating group of degree n
$G^{(i)}$	i^{th} derived subgroup of G
$\gamma_i(G)$	i^{th} term in descending central series of G
${}_nH$	$[x_1, x_2, \cdots, x_n]$ where $x_1, x_2, \cdots, x_n \in H$
$Z(G)$	center of the group G
$Z_n(G)$	n^{th} center of the group G
$GL(n, \mathbb{F})$	group of $n \times n$ non-singular matrices over the field $\mathbb{F}$
$M_n(\mathbb{F})$	algebra of $n \times n$ matrices over $\mathbb{F}$
$SL(n, \mathbb{F})$	$\{A \in M_n(\mathbb{F}) \mid \det(A) = 1\}$
$G\mathbb{F}(p)$	Galois field of p elements
$\mathbb{ISO}(G)$	$\{H \mid H$ is isoclinic to G with $Z(H) \leq H'\}$
$\mathbb{F}[G]$	group algebra of G over $\mathbb{F}$
$\text{inv}(G)$	invariant number of G

$\text{iso.exp}(G)$	isoclinic exponent of G
δ_{ij}	Kronecker delta function
G^n	direct product of n copies of G
$\prod_{i=1}^{n} G_i$	direct product of $G_1, G_2, \ldots, G_n$
$\bigoplus_{i=1}^{n} G_i$	direct sum of $G_1, G_2, \ldots, G_n$
$\text{diag}(G \times G)$	$\{(g,g) \mid g \in G\}$, diagonal of $G \times G$
$\Pr(G)$	commutativity degree of the group G
$\Pr(R)$	commutativity degree of the ring R
$\Pr_g(G)$	g-commutativity degree of the group G
$\Pr^n(G)$	n^{th} commutativity degree of the group G
$\Pr^{(n)}(G)$	n^{th} nilpotency degree of the group G
$\Pr(H,G)$	relative commutativity degree of a subgroup H of a group G.
$\Pr^{(n)}(H,G)$	n^{th} relative nilpotency degree of a subgroup H of a group G
$\Pr_n(G;S)$	S-rewriteability or n-rewriteability degree of a group G

Chapter 1

Preliminaries

In this chapter we recall some of the basic definitions, notations and conventions from the theory of groups, which will be used in the forth coming chapters. We would like to mention here that, unless stated otherwise, *all groups considered in this dissertation are to be assumed as finite groups.*

1.1 Group Action

Definition 1.1.1. Let G be a group and X be a set. Then G is said to *act* on X if $\forall\, g \in G$ and $\forall\, x \in X$ there exists an element $g.x \in X$, determined uniquely by g and x, such that the following conditions hold:

(i) $1.x = x \ \forall\, x \in X$, 1 being the identity element of G.

(ii) $(gh).x = g.(h.x) \ \forall\, x \in X$ and $\forall\, g, h \in G$.

Definition 1.1.2. If a group G acts on a set X then for each $x \in X$, the *orbit of* x denoted by $\mathrm{orb}(x)$ is defined to be the set $\{gx \in X | g \in G\}$.

Definition 1.1.3. If a group G acts on a set X then for each $x \in X$, the *stabilizer of* x denoted by $\text{stab}(x)$ is defined to be the subgroup $\{g \in G \mid gx = x\}$ of G.

Theorem 1.1.4. *Let a group G acts on a set X. Then, for each $x \in X$, the number of elements in the orbit of x equals the index of stabilizer of x, i.e.,*

$$|\,\text{orb}(x)| \;=\; [G : \text{stab}(x)].$$

1.2 Isomorphism Theorems

Theorem 1.2.1. (First Isomorphism Theorem) ([42], page 22)
Let $\phi : G \to H$ be a homomorphism with kernel K . Then K is a normal subgroup of G and $G/K \cong \text{Im}\,\phi$.

Theorem 1.2.2. (Second Isomorphism Theorem) ([42], page 25)
Let H and N be subgroups of G, and $N \trianglelefteq G$. Then

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

Theorem 1.2.3. (Third Isomorphism Theorem) ([42], page 26)
Let $K \subset H \subset G$, where both H and K are normal subgroups of G. Then H/K is a normal subgroup of G/K and

$$\frac{G/K}{H/K} \cong \frac{G}{H}.$$

Theorem 1.2.4. (Correspondence Theorem) ([3], page 98)
Let $\phi : G_1 \to G_2$ be a homomorphism of a group G_1 onto a group G_2. Then the following are true:

(i) $H_1 \leq G_1 \Rightarrow \phi(H_1) \leq G_2$.

(ii) $H_2 \leq G_2 \Rightarrow \phi^{-1}(H_2) \leq G_1$.

(iii) $H_1 \trianglelefteq G_1 \Rightarrow \phi(H_1) \trianglelefteq G_2$

(iv) $H_2 \trianglelefteq G_2 \Rightarrow \phi^{-1}(H_2) \trianglelefteq G_1$

(v) $H_1 < G_1$ *and* $H_1 \operatorname{Ker}\phi \Rightarrow H_1 = \phi^{-1}(\phi(H_1))$

(vi) *The mapping* $H_1 \to \phi(H_1)$ *is a 1-1 correspondace between the family of subgroups of* G_1 *containing* $\operatorname{Ker}\phi$ *and the family of subgroups of* G_2*; furthermore, normal subgroups of* G_1 *correspond to normal subgroups of* G_2.

Corollary 1.2.5. *Let* N *be a normal subgroup of* G. *Given any subgroup* H_1 *of* G/N, *there is a unique subgroup* H *of* G *such that* $H_1 = H/N$. *Further,* $H \trianglelefteq G$ *if and only if* $H/N \trianglelefteq G/N$.

1.3 Direct Products

Definition 1.3.1. If H and K are groups then the *(external) direct product* of H and K, denoted by $H \times K$, is the set of all ordered pairs (h, k), where $h \in H$ and $k \in K$, with the binary operation

$$(h, k)(h', k') = (hh', kk').$$

Theorem 1.3.2. ([42], page 29)
Let G *be a group with normal subgroups* H *and* K: *if* $H \cap K = \{1\}$ *and* $HK = G$, *then* $G \cong H \times K$.

Theorem 1.3.3. ([42], page 30)
Let $G = H \times K$, and let $H_1 \trianglelefteq H$ and $K_1 \trianglelefteq K$. Then $H_1 \times K_1 \trianglelefteq G$ and

$$\frac{G}{H_1 \times K_1} \cong \frac{H}{H_1} \times \frac{K}{K_1}.$$

Corollary 1.3.4. *If $G = H \times K$, then $G/(H \times \{1\}) \cong K$.*

1.4 Commutator Subgroup

Let $a,\ b$ be two elements of a group G, the *commutator* of a and b, denoted by $[a,\ b]$, is the element $aba^{-1}b^{-1}$. The *commutator subgroup* or *derived subgroup* of G, denoted by $[G,\ G]$ or G', is the subgroup of G generated by all the commutators in G.

Theorem 1.4.1. ([42], page 24)
The commutator subgroup is a normal subgroup, the quotient group G/G' is abelian, and if H is a normal subgroup of G for which G/H is abelian then G' is contained in H.

Few Commutator Identities:

There are many commutator identities that are quite useful. Few such commutator identities are given bellow.

Lemma 1.4.2. ([42], page 92)
If $x,\ y,\ z \in G$ then

(i) $[x,\ y]^{-1} = [y,\ x]$

(ii) $[x,\ yz] = [x,\ y][x,\ z]^y$

(iii) $[xy,\ z] = [y,\ z]^x[x,\ z]$

Lemma 1.4.3. Jacobi identity: ([42], page 93)
Let $x,\ y,\ z \in G$ *and* $[x,\ y,\ z] = [x,\ [y,\ z]]$ *then*

$$[x,\ y^{-1},\ z]^y[y,\ z^{-1},\ x]^z[z,\ x^{-1},\ y]^x = 1.$$

1.5 Conjugacy Classes

Let $x,\ y$ be two elements of a group G. We say that x is *conjugate* to y if $x^g = gxg^{-1} = y$ for some $g \in G$. The relation "x *is conjugate to* y *in* G" is an equivalence relation on G. The equivalence classes are called *conjugacy classes* of G. The conjugacy class of x is denoted by $\mathrm{Cl}(x)$.

Theorem 1.5.1. *The number of conjugates of* x *in* G *is* $[G : C_G(x)]$. *i.e.,* $|\mathrm{Cl}(x)| = |G : C_G(x)|$.

Lemma 1.5.2. ([42], page 53)
Let $k(G)$ *be the number of conjugacy classes of a finite group* G, *then*

$$k(G) = \frac{1}{|G|}\sum_{g\in G}|C_G(g)|.$$

Theorem 1.5.3. (Class Equation) ([42], page 57)
Let G *be a finite group, then*

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$$

where one x_i *is chosen from each conjugacy class having more than one element.*

1.6 Automorphism Groups

Definition 1.6.1. The set of all automorphisms of a group G, denoted by $\mathrm{Aut}(G)$ forms a group under the binary operation of composition. This group is said to be the *automorphism group* of G.

Definition 1.6.2. An automorphism α of G is said to be *inner* if it is conjugation by an element of G, i.e., $\alpha(x) = \phi_g(x) = gxg^{-1}$ for some $g \in G$; otherwise, α is *outer*.

The set of all inner automorphisms of G, denoted by $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

Theorem 1.6.3. (N/C Theorem) ([45], page 50)
Let G be a group and H is a subgroup, then $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

As an immediate corollary, we have

Corollary 1.6.4. $\mathrm{Inn}(G) \cong G/Z(G)$.

Corollary 1.6.5. *If $G \in \mathcal{G}_p$ and $|G'| = p$ then $G' \leq Z(G)$.*

Proof. By N/C Theorem 1.6.3, we have

$$|\frac{G}{C_G(G')}| \leq |\mathrm{Aut}(G')| = p - 1.$$

Also, $|G/C_G(G')|$ divides $|G|$ and since $G \in \mathcal{G}_p$ we have $|G/C_G(G')| = 1$. Hence $G' \leq Z(G)$. □

Definition 1.6.6. A group G is *complete* if $Z(G) = \{1\}$ and every automorphism of G is inner, i.e., $\mathrm{Aut}(G) = \mathrm{Inn}(G)$.

Theorem 1.6.7. ([45], page 450)
If H is a complete group and $H' < H$, then there is no group G such that $G' = H$.

1.7 Normal Series

Definition 1.7.1. A sequence $(G_0, G_1, \cdots, G_r)$ of subgroups of a group G is called a *normal series* of G if

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_{r-1} \trianglelefteq G_r.$$

The factors of a normal series are the quotient groups G_i/G_{i-1}, $1 \leq i \leq r$.

Definition 1.7.2. A composition series of a group G is a normal series $(G_0, G_1, \cdots, G_r)$ without repetition whose factors G_i/G_{i-1} are all simple groups. The factors G_i/G_{i-1} are called composition factors of G.

Note 1.7.3. We often refer to a normal series $(G_0, G_1, \cdots, G_r)$ by saying that

$$\{1\} = G_0 \subset G_1 \subset \cdots G_r = G$$

is a normal series of G.

Lemma 1.7.4. ([27], page 241)
Every finite group has a composition series.

Theorem 1.7.5. (Jordan-Hölder Theorem) ([27], page 241)
Any two composition series of a finite group are equivalent.

1.8 Solvable Groups

As the derived subgroup G' of a group G we define the nth derived subgroup of G, written as $G^{(n)}$, as follows:

$$G^{(1)} = G', \quad G^{(n)} = (G^{(n-1)})' \quad (n > 1).$$

Definition 1.8.1. A group G is said to be *solvable* if $G^{(k)} = \{1\}$ for some positive integer k.

Theorem 1.8.2. ([3], page 119)
A group G is solvable if and only if G has a normal series with abelian factors. Further, a finite group is solvable if and only if its composition factors are cyclic groups of prime orders.

Theorem 1.8.3. ([3], page 119)
Let G be a group. If G is solvable, then every subgroup of G and every homomorphic image of G are solvable.

Theorem 1.8.4. ([42], page 82)
Let N is a normal subgroup of G such that N and G/N are solvable, then G is solvable.

Corollary 1.8.5. *If H and K are solvable, then $H \times K$ is solvable.*

Corollary 1.8.6. *Every finite p-group is solvable.*

1.9 Nilpotent Groups

We define inductively the n^{th} *center* of a group G as follows. For $n = 1$, $Z_1(G) = Z(G)$. Consider the center of the quotient group $G/Z_1(G)$.

Because $Z(G/Z_1(G))$ is a normal subgroup of $G/Z_1(G)$, by Corollary 1.2.5 there is a unique normal subgroup $Z_2(G)$ of G such that

$$\frac{Z_2(G)}{Z_1(G)} = Z(G/Z_1(G)).$$

Thus, inductively we obtain a normal subgroup $Z_n(G)$ of G such that

$$\frac{Z_n(G)}{Z_{n-1}(G)} = Z(G/Z_{n-1}(G))$$

for every positive integer $n > 1$. $Z_n(G)$ is called the n^{th} center of G. Setting $Z_0(G) = \{1\}$, we have

$$\frac{Z_n(G)}{Z_{n-1}(G)} = Z(G/Z_{n-1}(G))$$

for every positive integer n. It follows immediately from the definition that

$$Z_n(G) = \{x \in G \mid xyx^{-1}y^{-1} \in Z_{n-1}(G) \ \forall \ y \in G\}.$$

Hence, $(Z_n(G))' \subset Z_{n-1}(G)$.

The ascending series

$$\{1\} = Z_0(G) \subset Z_1(G) \subset \cdots \subset Z_n(G) \subset \cdots$$

of subgroups of a group G is called the *upper central* series of G.

Definition 1.9.1. A group G is said to be *nilpotent* if $Z_m(G) = G$ for some m. The least such integer m is called the class of nilpotency of G.

Theorem 1.9.2. ([3], page 121) *A group G is nilpotent if and only if G has a normal series*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_m = G$$

such that $G_i/G_{i-1} \subset Z(G/G_{i-1})$ for all $i = 1, \cdots, m$.

Define a chain of subgroups $\gamma_i(G)$ inductively as follows:

$$\gamma_1(G) = G$$
$$\text{and} \quad \gamma_{i+1}(G) = [\gamma_i(G), G].$$

It is easy to see that $\gamma_{i+1}(G) \subset \gamma_i(G)$ and $\gamma_{i+1}(G)$ is a normal subgroup of G for all i. Thus, if $y \in \gamma_i(G)$, then x and y commute modulo $\gamma_{i+1}(G)$. Also

$$G = \gamma_1(G) \supset \gamma_(G) \supset \cdots .$$

is a normal series called *descending central series.*

Theorem 1.9.3. ([42], page 89)
For any group G, $Z_m(G) = G$ if and only if $\gamma_{m+1}(G) = \{1\}$. Moreover,

$$\gamma_{i+1}(G) \subset Z_{m-i}(G) \quad \textit{for all } i.$$

Now we are able to give an alternative definition for nilpotent group as follows

Definition 1.9.4. A group G is said to be *nilpotent* if $\gamma_{m+1}(G) = \{1\}$ for some m. The least such integer m is called the class of nilpotency of G.

Theorem 1.9.5. ([3], page 121)
Let G be a nilpotent group. Then every subgroup of G and every homomorphic image of G are nilpotent.

Theorem 1.9.6. ([42], page 90)
If G is nilpotent and $H \trianglelefteq G$, then G/H is nilpotent.

Theorem 1.9.7. ([42], page 91)

A direct product G of a finite number of nilpotent groups is nilpotent.

Theorem 1.9.8. ([42], page 91)

A group of order p^n, p prime, is nilpotent.

Theorem 1.9.9. ([42], page 91)

A finite group G is nilpotent if and only if it is the direct product of its Sylow subgroups.

1.10 Supersolvable Groups

Definition 1.10.1. A group G is said to be *supersolvable* if it has a series of subgroups A_i such that

$$\{1\} = A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots \subseteq A_r = G;$$

with $A_i \trianglelefteq G$ for each $i, 0 \leq i \leq r$, and each factor group A_{i+1}/A_i is cyclic for $0 \leq i \leq r-1$.

Remark 1.10.2. It is clear that if G is nilpotent, then G is supersolvable; but not conversely. Also if G is supersolvable then G is solvable; but not conversely. Thus for finite groups, we have the following hierarchy of classes of groups:

Cyclic $\Rightarrow$ Abelian $\Rightarrow$ Nilpotent $\Rightarrow$ Supersolvable $\Rightarrow$ Solvable .

Theorem 1.10.3. ([20], page 158)

Subgroups and the factor groups of a supersolvable groups are supersolvable.

Definition 1.10.4. A group is called CLT if it satisfies the converse of Lagranges Theorem.

We know that any finite abelian group is CLT. The following theorem says that every finite supersolvable group is CLT.

Theorem 1.10.5. ([44], page 144)
If G is finite supersolvable group of order n and $m|n$, then G has a subgroup of order m.

1.11 Möbius Function of a Poset

Definition 1.11.1. A *partially ordered set* or a *poset* is a set S together with a binary relation $a \geq b$ satisfying the following conditions:

(i) $a \geq a$ (reflexivity).

(ii) $a \geq b$ and $b \geq a$, then $a = b$ (anti-symmetry).

(iii) $a \geq b$ and $b \geq c$, then $a \geq c$ (transitivity).

Definition 1.11.2. A *lattice* is a partially ordered set in which any two elements have a least upper bound and greatest lower bound.

Theorem 1.11.3. (Möbius Inversion Formula) ([27], page 459)
For any partially ordered set S, there exists a unique function m (the Möbius Inversion Function*) from $S \times S$ to $\mathbb{Z}$ such that if A is any commutative group and f and g are functions from S to A such that*

$$g(y) = \sum_{\substack{s \in S \\ x \geq y}} f(x), \quad \textit{for all } y \in S$$

then

$$f(y) = \sum_{x \in S} m(y,x) g(x), \quad \textit{for all } y \in S.$$

Corollary 1.11.4. *Let f and g are functions from S to an abelian group A satisfying*

$$g(y) = \sum_{\substack{s \in S \\ x \leq y}} f(x), \quad y \in S.$$

Then

$$f(y) = \sum_{x \in S} \mu(y,x) g(x).$$

In particular, taking S to be the poset of subgroups of a $p-$group G we have the following:

Lemma 1.11.5. *Let G be a p-group and H, K be two subgroups of G. Then*

(i) $$m(K,H) = \begin{cases} 0, & \textit{if } K \textit{ is not normal in } H \\ m(1,H_0), & \textit{otherwise.} \end{cases}$$

(ii) $$m(1,H_0) = \begin{cases} (-1)^i p^{i(i-1)/2}, & \textit{if } H_0 \textit{ is an elementary abelian } p\textit{-group} \\ & \textit{of order } p^i; \\ 0, & \textit{otherwise.} \end{cases}$$

where $H_0 = H/K$ and m is the Möbius Inversion Function.

Lemma 1.11.6. ([27], page 465)

Let V be a vector space of dimension n over $G\mathbb{F}(p)$. If

$$\begin{bmatrix} n \\ j \end{bmatrix}$$

denotes the number of subgroups of order p^j (subspaces of dimension j) then

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1$$

and

$$\begin{bmatrix} n \\ j \end{bmatrix} = p^j \cdot \begin{bmatrix} n-1 \\ j \end{bmatrix} + \begin{bmatrix} n-1 \\ j-1 \end{bmatrix}.$$

1.12 Character Theory

Definition 1.12.1. Let $\mathbb{F}$ be a field and A be an $\mathbb{F}$-vector space which is also a ring with 1. Then A is said to be an $\mathbb{F}$-*algebra* if for $c \in \mathbb{F}$ and $x, y \in A$

$$(cx)y = c(xy) = x(cy).$$

Example 1.12.2. Let G be a finite group and $\mathbb{F}[G]$ be the set of all "formal" sums $\{\sum_{g \in G} a_g g \mid a_g \in \mathbb{F}\}$. Then $\mathbb{F}[G]$ has a $\mathbb{F}$-vector space structure in an obvious way. The elements of $\mathbb{F}[G]$ for which $a_g = 1$ and $a_h = 0$ if $h \neq g$ is identified with g. This identification embeds G into $\mathbb{F}[G]$ and in fact G is a basis for $\mathbb{F}[G]$. To define multiplication on $\mathbb{F}[G]$, we multiply the basis vectors according to their group multiplication and extend linearly to all of $\mathbb{F}[G]$. Then this defines the structure of an $\mathbb{F}$-algebra on $\mathbb{F}[G]$.

Definition 1.12.3. Let A and B be two $\mathbb{F}$-algebras. Then a mapping $\phi : A \to B$ is said to be an *algebra homomorphism* or an $\mathbb{F}$-*homomorphism* if the following satisfies

(i) $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in A$;

(ii) $\phi(1) = 1$;

(iii) ϕ is an $\mathbb{F}$-linear transformation.

Definition 1.12.4. Let A be an $\mathbb{F}$-algebra. A *representation* of A is an algebra homomorphism $\rho : A \to M_n(\mathbb{F})$. The integer n is called the *degree* of ρ.

Definition 1.12.5. Two representations ρ and σ of same degree n is said to be *similar* if there exists a non singular $n \times n$ matrix P such that

$$\rho(a) = P^{-1}\sigma(a)P \quad \forall \ a \in A.$$

Remark 1.12.6. 'Similarity' is an equivalence relation among representations of same degree.

Definition 1.12.7. Let G be a group and let $\mathbb{F}$ be a field. Then $\mathbb{F}$-representation of G is a homomorphism $\rho : G \to \mathrm{GL}(n, \mathbb{F})$ for some positive integer n.

Remark 1.12.8. An $\mathbb{F}$-representation $\bar{\rho}$ of $\mathbb{F}[G]$ determines an $\mathbb{F}$-representation ρ of G by restriction. Conversely, an $\mathbb{F}$-representation ρ of G determines an $\mathbb{F}$-representation $\bar{\rho}$ of $\mathbb{F}[G]$ by linear extension. i.e.,

$$\bar{\rho}\left(\sum_{g\in G} a_g g\right) := \sum_{g\in G} a_g \rho(g).$$

We shall use the same symbol to denote an $\mathbb{F}$-representation of G as well as the corresponding $\mathbb{F}$-representation of $\mathbb{F}[G]$.

Definition 1.12.9. Let A be an $\mathbb{F}$-algebra and let V be a finite dimensional vector space. Suppose for every $v \in V$ and $x \in A$ that a unique $vx \in V$ is defined. Then V is said to be an *A-module* if for all $x, y \in A$, $v, w \in V$, and $c \in \mathbb{F}$ the following satisfies

(i) $(v + w)x = vx + wx$,

(ii) $v(x + y) = vx + vy$,

(iii) $(vx)y = v(xy)$,

(iv) $(cv)x = c(vx) = v(cx)$,

(v) $v1 = v$.

Definition 1.12.10. Let V be an A-module. Then an A-invariant subspace W of V is said to be a *submodule* of V.

Definition 1.12.11. A nonzero A-module V is said to be *irreducible* if its only submodules are 0 and V, otherwise it is called *reducible.*

Fact 1.12.12. Let $\rho : A \to M_n(\mathbb{F})$ be a representation of the $\mathbb{F}$-algebra A. Let $V = M_{1\times n}(\mathbb{F})$. Clearly

$$v \in V,\ X \in M_n(\mathbb{F}) \Rightarrow vX \in V.$$

Then for $v \in V$, $a \in A$, $va := v\rho(a)$ gives an A-module structure to V.

Fact 1.12.13. Let M be an A-module. Let $\mathcal{B}$ is an $\mathbb{F}$ basis for M. For all $a \in A$ let $a_M : M \to M$ be the map $x \mapsto xa \ \forall \ a \in A$. Set $\rho(a) =$ matrix of a_M with respect to the basis $\mathcal{B}$. Then ρ defines a representation of A.

Remark 1.12.14. There is a natural one to one correspondence (as mentioned in Fact 1.12.12 and Fact 1.12.12) between isomorphism classes of A-modules and similarity classes of representations of A.

Definition 1.12.15. A representation $\rho : A \to M_n(\mathbb{F})$ is said to be *irreducible* if the corresponding A-module (as per Fact 1.12.12) is irreducible. Otherwise *reducible.*

Definition 1.12.16. Let ρ be an $\mathbb{F}$-representation of G. Then the $\mathbb{F}$-character χ of G afforded by ρ is the function given by $\chi(g) = \operatorname{tr} \rho(g)$.

We restrict our attention to the special case that the field $\mathbb{F} = \mathbb{C}$ and the word "character" will mean $\mathbb{C}$-character. Notice that $\chi(1) = \deg \rho$, we say that $\chi(1)$ is the *degree* of χ. Characters of degree 1 are called *linear character.*

Remark 1.12.17. Similar representations of a group G afford equal character and characters are constant on conjugacy classes of a group G.

Definition 1.12.18. Characters afforded by irreducible representations are called *irreducible characters.*

Lemma 1.12.19. ([25], page 16)
The number of similarity class of irreducible representations of a group G is equal to the number of conjugacy classes of G.

Lemma 1.12.20. ([25], page 16)

Let G be a group and $\mathrm{Irr}(G)$ *be the set of all irreducible characters of G. Then* $|\mathrm{Irr}(G)|$ *equals the number of conjugacy classes of G and*

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2.$$

Theorem 1.12.21. (First Orthogonality Relation) ([25], page 20)

The following holds for every finite group G

$$\frac{1}{|G|}\sum_{g \in G} \chi_i(g)\chi_j(g^{-1}) = \delta_{ij}.$$

Lemma 1.12.22. ([25], page 20)

Let ρ be a representation of a group G affording the character χ and let $g \in G$. Let $n = o(g)$, the order of g. Then

(i) *$\rho(g)$ is similar to a diagonal matrix* $\mathrm{diag}(\varepsilon_1, \cdots, \varepsilon_f)$, *where $f = \chi(1)$;*

(ii) $\varepsilon_i^n = 1$;

(iii) $\chi(g) = \sum \varepsilon_i$ *and* $|\chi(g)| \leq \chi(1)$;

(iv) $\chi(g^{-1}) = \overline{\chi(g)}$.

Theorem 1.12.23. (Second Orthogonality Relation) ([25], page 21)

Let G be a group and g, $h \in G$. Then

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = 0$$

if g is not conjugate to h in G. Otherwise the sum is equal to $|C_G(g)|$.

Definition 1.12.24. Let χ be a character of G. Then $\ker\chi = \{g \in G \mid \chi(g) = \chi(1)\}$.

Theorem 1.12.25. ([25], page 25)
Let G be a group with commutator subgroup G'. Then

(i) $G' = \cap\{\ker\chi \mid \chi \in \mathrm{Irr}(G),\ \chi(1) = 1\}$;

(ii) $|G : G'| =$ *the number of linear characters of* G.

Theorem 1.12.26. ([25], page 27)
Let χ be a character of a group G and let $Z = Z(\chi) = \{g \in G : |\chi(g)| = \chi(1)\}$. Let ρ be a representation of G which affords χ. Then

(i) $Z = \{g \in G | \rho(g) = \varepsilon I$ *for some* $\varepsilon \in \mathbb{C}\}$;

(ii) Z *is a subgroup of* G;

(iii) $\chi_Z = f^\lambda$ *for some linear character* λ *of* Z;

(iv) $Z/\ker\chi$ *is cyclic;*

(v) $Z/\ker\chi \subseteq Z(G/\ker\chi)$;

Furthermore, if $\chi \in \mathrm{Irr}(G)$, *then*

(vi) $Z/\ker\chi = Z(G/\ker\chi)$.

Theorem 1.12.27. ([25], page 28)
Let $\chi \in \mathrm{Irr}(G)$. Then $\chi(1)^2 \leq |G : Z(\chi)|$. The equality holds if and only if χ vanishes on $G \setminus Z(\chi)$.

Theorem 1.12.28. ([25], page 38)

For any $\chi \in \mathrm{Irr}(G)$, $\chi(1)$ *divides* $|G|$.

Theorem 1.12.29. (Frobenious) (See [47])

Let G *be a group and* $g \in G$. *Then the number of solutions of the equation* $[x, y] = g$ *in* G *is*

$$|G| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}.$$

Chapter 2

Commutativity Degree and its Computations

In probabilistic group theory one might ask the question "What is the probability that two group elements, chosen at random will commute?" The answer is given by what is known as commutativity degree of a group. Commutativity degree is a kind of measure for abelianness of a group. In this chapter we shall study the commutativity degree of a finite group in detail including its computations for some non trivial classes of finite groups.

2.1 Definition and elementary properties

From probability theory, the probability of occurance of an event A among several alternatives is given by

$$\Pr(A) = \frac{\text{Number of outcomes favorable to the event } A}{\text{Total number of possible outcomes}}.$$

Hence for a finite group G the probability $\Pr(G)$ that two group elements, chosen at random will commute with each other is given by

$$\Pr(G) = \frac{|\{(x,y) \in G \times G : xy = yx\}|}{|G \times G|} = \frac{|\mathcal{C}|}{|G|^2}$$

where $\mathcal{C} = \{(x,y) \in G \times G : xy = yx\}$. Clearly, a finite group G is abelian if and only if $\Pr(G) = 1$. Moreover, since the identity element 1 of a group commutes with every element of the group, and every element commutes with itself, we have $1 \times G \subset \mathcal{C}$, $G \times 1 \subset \mathcal{C}$ and $\mathrm{diag}(G \times G) \subset \mathcal{C}$ and any two of the sets $1 \times G$, $G \times 1$ and $\mathrm{diag}(G \times G)$ have only one element in common, viz. 1, we have

$$|\mathcal{C}| \geq |1 \times G| + |G \times 1| + |\,\mathrm{diag}(G \times G)| - 2 = 3|G| - 2.$$

Hence

$$\Pr(G) \geq \frac{3}{|G|} - \frac{2}{|G|^2}.$$

Thus for a non-abelian group G we have $(3/|G| - 2/|G|^2) \leq \Pr(G) < 1$.

The ratio $\Pr(G)$ is called the *Commutativity Degree* of G. This concept has been studied by several authors (eg. [29], [18], [36], [43], [32], [15] etc.) under various notations like $d(G)$, $p(G)$, $R(G)$, $mc(G)$ etc.

Further, note that a pair $(x,y) \in G \times G$ belongs to $\mathcal{C}$ if and only if $y \in C_G(x)$. So, $\mathcal{C} = \bigsqcup_{x \in G}(\{x\} \times C_G(x))$ whence $|\mathcal{C}| = \sum_{x \in G} |C_G(x)|$. Therefore by Lemma 1.5.2, we have $|\mathcal{C}| = |G| \cdot k(G)$ and hence we have the following proposition.

Proposition 2.1.1. *For a finite group G, $\Pr(G) = k(G)/|G|$.*

Let $\mathcal{G}$ be the collection of all finite groups (up to isomorphism) then commutativity degree can be thought as arithmetic function on $\mathcal{G}$ [10]. However, before looking at some of the properties of $\Pr(G)$ as an arithmetic function, we need to study some facts about conjugacy classes of the group G.

Lemma 2.1.2. *Let G be a finite group and H be a subgroup of G, then*

(i) $|C_G(g)| \leq [G : H]|C_H(g)|$ *with equality if and only if* $C_G(g)H = G$

(ii) $\sum_{g \in G} |C_H(g)| = \sum_{h \in H} |C_G(h)|$

Proof. (i) We know that $HC_G(x) \subseteq G$ for all x in G. So, $|HC_G(x)| \leq |G|$ and we have

$$\frac{|H||C_G(x)|}{|H \cap C_G(x)|} \leq |G|$$

$$\text{or, } \frac{|H|}{|H \cap C_G(x)|} \leq \frac{|G|}{|C_G(x)|}.$$

Thus

$$|H : C_H(x)| \leq |G : C_G(x)| \text{ for all } x \in G.$$

from which lemma follows. The equality part is clear.

(ii) It can be seen easily.

□

Further the second part of this lemma can be generalized for any two subsets of a group as follows

Lemma 2.1.3. *Let G be a finite group and H, K be subsets of G, then* $\sum_{g \in K} |C_H(g)| = \sum_{h \in H} |C_K(h)|$

Theorem 2.1.4. *Let G be a finite group and H be a subgroup of G, then*

(i) $k(H) < [G : H]k(G)$, *if* $H \neq G$

(ii) $k(G) \leq [G : H]k(H)$ *with equality if and only if* $C_G(g)H = G$

Proof. The proof of part (i) follows from Lemma 1.5.2 and the fact that $C_H(h) \subset C_G(h)$ and part (ii) follows from Lemma 2.1.2. □

Theorem 2.1.5. *Let G be a finite group and $N \trianglelefteq G$, then*

$$k(G) \leq k(G/N)k(N).$$

The equality holds if and only if $C(g \bmod N) = NC_G(g)$ for each $g \in G$

Proof. By Second Isomorphism Theorem 1.2.2, we have

$$\frac{C_G(g)}{C_N(G)} = \frac{C_G(g)}{N \cap C_G(g)} = \frac{NC_G(g)}{N} \subseteq C_{G/N}(Ng).$$

with equality if and only if $C(g \bmod N) = NC_G(g)$. Therefore,

$$|C_G(g)| \leq |C_{G/N}(Ng)||C_N(g)| \tag{2.1.a}$$

If $G = \bigsqcup_{i=1}^{k} Nh_i$ the coset decomposition of G then

$$\begin{aligned}
\sum_{g \in G} |C_G(g)| &= \sum_{i=1}^{k} \sum_{g \in Nh_i} |C_G(g)| \\
&\leq \sum_{i=1}^{k} \sum_{g \in Nh_i} |C_{G/N}(Ng)||C_N(G)| \quad \text{(by Equation 2.1.a)} \\
&= \sum_{i=1}^{k} |C_{G/N}(Ng)| \sum_{g \in Nh_i} |C_N(g)| \\
&= \sum_{i=1}^{k} |C_{G/N}(Ng)| \sum_{t \in N} |C_{Nh_i}(t)|
\end{aligned}$$

We have $C_{Nh_i}(t) = \{x \in Nh_i \mid xt = tx\} = \{x = nh_i \in Nh_i \mid h_i t h_i^{-1} \sim t \, in \, N\}$ Thus $C_{Nh_i}(t)$ is nonempty $\Leftrightarrow gtg^{-1}$ is conjugate to t in N, and in that case $C_{Nh_i}(t)$ is a coset of $C_N(t)$. Hence,

$|C_{Nh_i}(t)| \leq |C_N(t)|$ with equality $\Leftrightarrow gtg^{-1}$ is conjugate to t in N.

It follows that

$$\sum_{g \in G} |C_G(g)| \leq \sum_{i=1}^{k} |C_{G/N}(Ng)| \sum_{t \in N} |C_N(t)|$$

$$\Rightarrow |G| k(G) \leq |G : H| k(G/N) |N| k(N)$$

$$\Rightarrow k(G) \leq k(G/N) k(N)$$

with equality $\Leftrightarrow NC_G(g) = C(g \bmod N)$ holds and each G-class in N is an N-class. However, the latter statement is implied by $NC_G(g) = C(g \bmod N)$ taking $g \in N$ □

Corollary 2.1.6. *Let G be a finite group and $N \trianglelefteq G$. If*

$$k(G) = k(G/N) k(N), \tag{2.1.b}$$

then

$$k(L) = k(L/N) k(N) \tag{2.1.c}$$

for each subgroup $L \supset N$. Conversely, if $k(L) = k(L/N)k(N)$ for each subgroup $L = N\langle g, t \rangle$ with $[g, t] \in N$, then (2.1.b) holds.

Proof. The first statement follows from the fact that (2.1.b) for G implies (2.1.b) for L.

Let $t \in C(g \bmod N)$. Assuming (2.1.c) for $L = N\langle g, t\rangle$, we get $t \in C_L(g \bmod N) = NC_L(g) \subset NC_G(g)$. Thus if (2.1.c) holds for all such L, then $C(g \bmod N) \subset NC_G(g)$ for each g, from which (2.1.b) follows. □

Theorem 2.1.7. *If G and H are two finite groups then $k(G\times H) = k(G)k(H)$.*

Proof. Let S_G, S_H and $S_{G\times H}$ denotes the set of all conjugacy classes in the groups G, H and $G \times H$ respectively. Define a function f from $S_{G\times H}$ to $S_G \times S_H$ such that

$$f(\mathrm{Cl}((g,\ h))) = (\mathrm{Cl}(g),\ \mathrm{Cl}(h))$$

where

$$\begin{aligned}\mathrm{Cl}((g,\ h)) &= \{(g_1,\ h_1)(g,\ h)(g_1,\ h_1)^{-1} : (g_1,\ h_1) \in G \times H\}\\ &= \{(g_1 g g_1^{-1},\ h_1 h h_1^{-1}) : g_1 \in G,\ h \in H\}\\ &= \mathrm{Cl}(g) \times \mathrm{Cl}(h).\end{aligned}$$

This shows that f is a bijection. Hence,

$$|S_{G\times H}| = |S_G||S_H|$$

or, $k(G \times H) = k(G)k(H)$ which implies $\Pr(G \times H) = \Pr(G) \cdot \Pr(H)$. □

As an arithmetic function on $\mathcal{G}$, commutativity degree has the following properties.

Theorem 2.1.8. (i) *Commutativity degree is a monotonically decreasing function. i.e., if H is a subgroup of G then $\Pr(G) \leq \Pr(H)$ with equality if and only if $C_G(g)H = G$.*

(ii) *Commutativity degree is a completely multiplicative function. i.e., if* G *and* H *are two finite groups then* $\Pr(G \times H) = \Pr(G) \cdot \Pr(H)$.

(iii) *For any normal subgroup* N *of* G, $\Pr(G) \leq \Pr(G/N)\Pr(N)$. *The equality holds if and only if* $C(g \bmod N) = NC_G(g)$ *for each* $g \in G$.

Proof. Part (i) follows from Theorem 2.1.4, part (ii) follows from Theorem 2.1.7 and part (iii) follows from Theorem 2.1.5. □

Remark 2.1.9. One may note that if the equality holds in Theorem 2.1.8 part (iii) and N is abelian, then $N \subseteq Z(G)$.

2.2 Non-trivial upper bounds for $\Pr(G)$

Obviously 1 is an upper bound for $\Pr(G)$. However when G is non-abelian, there is a notable gap between $\Pr(G)$ and 1, as suggested by the following proposition.

Proposition 2.2.1. *If* G *is finite non-abelian group then* $\Pr(G) \leq \frac{5}{8}$ *with equality if and only if* $G/Z(G)$ *has order* 4.

Proof. Let $\mathcal{K}_1, \mathcal{K}_2, \cdots, \mathcal{K}_t$ be the conjugacy classes of noncentral elements of G. Then $|\mathcal{K}_i| \geq 2 \ \forall \ i = 1, 2, \cdots, t$.

By the Class Equation 1.5.3 of G, we have

$$|G| = |Z(G)| + |\mathcal{K}_1| + |\mathcal{K}_2| + \cdots + |\mathcal{K}_t| \geq |Z(G)| + 2t$$

or, $t \leq (|G| - |Z(G)|)/2$. Since G is non-abelian, $G/Z(G)$ is not cyclic and so $|G/Z(G)| \geq 4$, i.e., $|Z(G)| \leq |G|/4$. Hence $t \leq \frac{3}{8}|G|$ and so

$$k(G) = |Z(G)| + t \leq \frac{|G|}{4} + \frac{3}{8}|G|.$$

This, in view of Proposition 2.1.1, proves the proposition.

For the second part, let $\Pr(G) = 5/8$. Assume that $|G/Z(G)| > 4$. Then

$$\Pr(G) = \frac{k(G)}{|G|} = \frac{|Z(G)|}{|G|} + \frac{k(G) - |Z(G)|}{|G|}$$

which implies

$$\frac{3}{8} < \frac{k(G) - |Z(G)|}{|G|}.$$

Again by the Class Equation 1.5.3 of G, we have

$$|G| \geq 2(k(G) - |Z(G)|).$$

Now using both the inequalities, we get

$$\frac{|G| - k(G)}{|G|} > \frac{3}{8} \quad \text{gives} \quad \Pr(G) < 5/8.$$

Which is a contradiction. Hence $G/Z(G)$ has order 4.

Conversely, suppose that $|G/Z(G)| = 4$. For $a_1 \in G \setminus Z(G)$ $\exists\, a_2 \in G \setminus Z(G)$ such that $a_1a_2 \neq a_2a_1$. Therefore, we can write

$$G/Z(G) = \{Z(G), a_1Z(G), a_2Z(G), a_3Z(G)\}$$

where $a_3 = a_1a_2$ and $a_1^2,\ a_2^2,\ a_3^2 \in Z(G)$. Also if $x \in a_iZ(G)$ and $y \in a_jZ(G)$ then $xy \neq yx$. Thus $x,\ y \in G$ will commute if

(i) $x \in Z(G),\ y \in G,$

(ii) $x \in a_1Z(G)$, $y \in Z(G)$ or $y \in a_1Z(G)$,

(iii) $x \in a_2Z(G)$, $y \in Z(G)$ or $y \in a_2Z(G)$,

(iv) $x \in a_3Z(G)$, $y \in Z(G)$ or $y \in a_3Z(G)$.

Now

$$\begin{aligned}
|\mathcal{C}| &= |\{(x,\ y) \in G \times G : xy = yx\}| \\
&= |\{(x,\ y) \in G \times G : x \in Z(G),\ y \in G\}| \\
&\quad + 3[|\{(x,\ y) \in G \times G : x \in a_1Z(G),\ y \in Z(G)\}| \\
&\quad + |\{(x,\ y) \in G \times G : x \in a_1Z(G),\ y \in a_1Z(G)\}|] \\
&= |Z(G)||G| + 6|Z(G)|^2.
\end{aligned}$$

which gives $\Pr(G) = 5/8$. □

It is well-known that any non-abelian group of order 8 has exactly five conjugacy classes. So, $\Pr(G) = 5/8$ for non-abelian groups of order 8. There are only two non abelian groups of order eight viz. D_4, the dihedral group and and Q_8, the quaternion group. Thus $\Pr(D_4) = \Pr(Q_8) = 5/8$. This shows that the upper bound in Proposition 2.2.1 is the best possible one. This also shows that $\Pr(G)$ does not determine G up to isomorphism. Also Note that the class of finite non-abelian groups G such that $|G/Z(G)| = 4$ is quite big. For example, we may consider the groups $Q_8 \times A$ or $D_4 \times A$ where A is abelian group.

Theorem 2.2.2. *Let G be a finite non-abelian group. Then*

$$\Pr(G) \leq \frac{1}{4} + \frac{3}{4}\frac{1}{|G'|}.$$

Proof. By Lemma 1.12.20, we have

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 = |G : G'| + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1) \neq 1}} \chi(1)^2$$

$$\geq |G : G'| + (k(G) - |G : G'|) \cdot 2^2 = 4k(G) - 3|G : G'|$$

$$\Rightarrow k(G) \leq \frac{|G|}{4} + \frac{3}{4}\frac{|G|}{|G'|}$$

$$\Rightarrow \Pr(G) \leq \frac{1}{4} + \frac{3}{4}\frac{1}{|G'|}.$$

□

Further we have a more general result due to K. S. Joseph [29] given in the following theorem:

Theorem 2.2.3. *Let G be a non-abelian group and p be the least prime number which divides $|G|$, then*

$$\Pr(G) \leq \frac{1}{p^2}\left(1 + \frac{p^2 - 1}{|G'|}\right).$$

In particular, we have $\Pr(G) \leq (p^2 + p - 1)/p^3$ with equality holding if and only if $G/Z(G)$ has order p^2.

Proof. By Lemma 1.12.20, we have

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2$$

$$= |G : G'| + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1) \neq 1}} \chi(1)^2$$

Since $\chi(1)$ divides $|G|$ for all $\chi \in \mathrm{Irr}(G)$ we have $\chi(1) \geq p$. Therefore

$$|G| \geq |G : G'| + p^2(k(G) - |G : G'|)$$

which gives

$$\Pr(G) = \frac{k(G)}{|G|} \leq \frac{1}{p^2}\left(1 + \frac{p^2-1}{|G'|}\right).$$

Thus the first part of the result done.

For the particular case we have $\{1\} \neq G' \leq G$ and p is the least prime number which divides $|G|$ it follows that $|G'| \geq p$. Hence

$$\Pr(G) \leq \frac{1}{p^2}\left(1 + \frac{p^2-1}{p}\right) = \frac{p^2+p-1}{p^3}.$$

The proof of the last part is analogous to that of Theorem 2.2.1. □

Corollary 2.2.4. *Let G be a non-abelian group and p is the least prime number which divides $|G|$. If $\Pr(G) > 1/p$ then $|G'| = p$. i.e., $G' \cong C_p$.*

Proof. By Theorem 2.2.3, and using the hypothesis we have

$$\frac{1}{p} < \Pr(G) \leq \frac{1}{p^2}\left(1 + \frac{p^2-1}{|G'|}\right)$$

which gives $|G'| < p+1$. Hence $|G'| = p$. □

Theorem 2.2.5. *Let G be a non-abelian p-group then*

$$\Pr(G) \leq \frac{p^2+p-1}{p^3}.$$

Proof. Let $|G| = p^n$ then $|Z(G)| \leq p^{n-2}$; because $|Z(G)| \neq p^n$ and if $|Z(G)| = p^{n-1}$ then $|G|/|Z(G)| = p$, which is impossible since $G/Z(G)$ is not cyclic.

By the Class Equation 1.5.3 of G, we have

$$
\begin{aligned}
|G| &= |Z(G)| + \sum_{a \notin Z(G)} |\operatorname{Cl}(a)| \\
&\geq |Z(G)| + (k(G) - |Z(G)|)p \\
&= |Z(G)|(1-p) + pk(G) \\
\Rightarrow \quad pk(G) &\leq p^n + (p-1)|Z(G)| \\
&\leq p^n + (p-1)p^{n-2} \\
\Rightarrow \quad \Pr(G) &\leq \frac{p^2+p-1}{p^3}.
\end{aligned}
$$

□

Remark 2.2.6. Consider the set $V = \{\Pr(G) \mid G \text{ is a finite group}\}$. Clearly $V \subset [0,1]$. The above theorem says that 0 is a limit point of V ([43], [9]). So natural question arises

PROBLEM: What is the derived set (V') of V, i.e., the set of all limit points of V? In view of Proposition 2.2.1, is it true that $V' = [0, 5/8]$?

We conclude this section by stating the following interesting theorem. The proof can be found in [17].

Theorem 2.2.7. *Let G be a finite group with Fitting subgroup F. Then*

$$\Pr(G) \leq (\Pr(F))^{-1/2}|G:F|^{1/2} \leq |G:F|^{-1/2}.$$

2.3 Commutativity degree for groups having $|\operatorname{cd}(G)| = 2$

In this section we consider the groups having only two character degrees. Such groups are solvable and have been throughly investigated by Isaacs and Passman [23], [24]. In [41] Pournaki and Sobhani have computed the commutativity degree for these groups.

Theorem 2.3.1. *Let G be a finite group such that $\operatorname{cd}(G) = \{1, m\}$, $m > 1$, then*

$$\Pr(G) = \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{m^2}\right)$$

Proof. We have

$$|G| = \sum_{\chi \in \operatorname{Irr}(G)} \chi(1)^2 = |G : G'| + (k(G) - |G : G'|)m^2$$

which implies

$$\frac{k(G)}{|G|}m^2 = 1 + \frac{1}{|G'|}m^2 - \frac{1}{|G|}$$

and the theorem follows. □

By Theorem 1.12.27, we have the degree of an irreducible complex character can not exceed $|G : Z(G)|^{1/2}$ i.e., $\chi(1) \leq |G : Z(G)|^{1/2}$ $\forall$ $\chi \in \operatorname{Irr}(G)$. Finite groups for which this bound is attained are called groups of *central type* . In 1982 Howlett and Isaacs [22] proved that a finite group of central type must be solvable, but not necessarily nilpotent. Now in view of Theorem 2.3.1 we can state the following corollary.

Corollary 2.3.2. *Let G be a finite group such that $|\operatorname{cd}(G)| = 2$, then*

$$\Pr(G) \geq \frac{1}{|G'|}\left(1 + \frac{|G'| - 1}{|G : Z(G)|}\right)$$

The equality holds if and only if G is a group of central type.

Proposition 2.3.3. *Let G be a finite group such that $|G'| = p$, p a prime, and $G' \leq Z(G)$, then G is a group of central type with* $\operatorname{cd}(G) = \{1,\ |G : Z(G)|^{1/2}\}$.

Proof. Let χ be a non-linear irreducible complex character of G. Let $g \in G \setminus Z(G)$. So $g^{-1} \in G \setminus Z(G)$ Therefore there exists an element $x \in G$ such that $z := [g^{-1},\ x] \neq 1$. Since $|G'| = p$ is a prime, each non-trivial element of G' is a generator of G' and so $G' = \langle z \rangle$. Now consider ρ as a $\mathbb{C}$-representation of G affording χ. By Theorem 1.12.26, we have $\rho(z) = \varepsilon I$ for some $\varepsilon \in \mathbb{C}$. For $\varepsilon = 1$ we have $z \in \operatorname{Ker}\rho$ and therefore $G' \leq \operatorname{Ker}\rho$ which is a contradiction by Theorem 1.12.25 and hypothesis. Therefore $\varepsilon \neq 1$ and since

$$\chi(g) = \chi(xgx^{-1}) = \chi(gz) = \operatorname{tr}\rho(gz) = \operatorname{tr}(\rho(g)\rho(z)) = \operatorname{tr}(\varepsilon\rho(g)I) = \varepsilon\chi(g)$$

which forces $\chi(g) = 0$. Now by Theorem 1.12.27, we have $\chi(1)^2 = |G : Z(G)|$. Therefore G is a group of central type with just two irreducible complex character degrees, i.e., $\operatorname{cd}(G) = \{1,\ |G : Z(G)|^{1/2}\}$. □

2.4 Commutativity degree for groups having nipotance class 2

In this section we compute the value of $\Pr(G)$ for groups G having $G' \leq Z(G)$. However, we first develop certain group theoretic tools for this purpose.

Definition 2.4.1. For any element x of G we define $[G,x] = \{[g,x] \mid g \in G\}$.

Then $[G,x]$ is a subset of G' while for any subset H of G, $[G,H]$ is a subgroup generated by all $[G,x]$ with $x \in H$.

Definition 2.4.2. For any subset $H \subseteq G$, define

$$H^* = \{x \in G \ : \ [G,\ x] \subseteq H\}.$$

Obviously $H^* = (G' \cap H)^*$. Also if H is a normal subgroup then $H^*/H = Z(G/H)$. In particular, H^* is a subgroup of G.

The following lemma gives some properties for the operators $(\ )^*$ and $(\ )'$.

Lemma 2.4.3. *Let G be a group and H, H_1, H_2 are subsets G. Then*

(i) $\{1\}^* = Z(G)$

(ii) $(G')^* = G$

(iii) $H_1 \subseteq H_2$ *implies* $(H_1)^* \subseteq (H_2)^*$

(iv) $(H_1 \cap H_2)^* = (H_1)^* \cap (H_2)^*$

(v) $(H_1)^*(H_2)^* \leq (H_1H_2)^*$

(vi) $(H^*)' \subseteq H$ *but* $H \not\subseteq (H')^*$

(vii) $((H^*)')^* \subseteq H^*$ *but* $(H)^* \not\subseteq (H^*)')^*$

Definition 2.4.4. For any subgroup H of G define $\bar{H}$ as $\bar{H} = H^* - \bigcup_{K<H} K^*$ that is, $\bar{H}$ is the set of all elements for which $[G,\ x] = H$ precisely, and not for any proper subgroup. i.e., $\bar{H} = \{x \in G : [G,\ x] = H\}$.

Lemma 2.4.5. *Let G be a group such that $G' \leq Z(G)$. Then $|H^*| = \sum_{K \leq H} |\bar{K}|$ for any $H \leq G'$.*

Proof. To prove the lemma it suffices to show that $H^* = \bigcup_{K \leq H} \bar{K}$ disjointly. Let $x \in \bigcup_{K \leq H} \bar{K}$ then $x \in \bar{K}$ for some $K \leq H$ implies $x \in K^*$. Then by Lemma 2.4.3 (iii), we have $x \in H^*$. Thus $\bigcup_{K \leq H} \bar{K} \subseteq H^*$.

Conversely, let $x \in H^*$. If $x \in \bar{H}$ then obvious, so let $x \notin \bar{H}$ then $x \in K^*$ for some $K < H$. Choose K such that K is minimal i.e., $|K|$ is smallest. Then $x \notin \bigcup_{L<K} L^*$. Otherwise, $x \in L^*$ where $L < K$. Which contradicts to the minimality of K. Therefore $x \in K^* - \bigcup_{L<K} L^* = \bar{K}$ for some $K \leq H$. Which implies $x \in \bigcup_{K \leq H} \bar{K}$. Thus $H^* \subseteq \bigcup_{K \leq H} \bar{K}$. Hence $H^* = \bigcup_{K \leq H} \bar{K}$.

Also $x \in \bar{K}$ for exactly one $K \leq H$ because $x \in \bar{K_1}$ and $x \in \bar{K_2}$ for two subsets K_1 and K_2 of H implies $x \in K_1^*$, $x \in K_2^*$ and $x \notin \bigcup_{L_1 \leq K_1} K_1^*$, $x \notin \bigcup_{L_2 \leq K_2} K_2^*$. Which implies $x \in K_1^* \cap K_2^* = (K_1 \cap K_2)^*$. Therefore, $x \in \bigcup_{L_1 \leq K_1} L_1^*$ and $x \in \bigcup_{L_2 \leq K_2} L_2^*$. Which is a contradiction. Hence $H^* = \bigcup_{K \leq H} \bar{K}$ disjointly. □

Lemma 2.4.6. *Let G be a p-group with $H \leq G'$. If $k(G)$ denotes the number of conjugacy classes in G then $k(G) = \sum_{H \leq G'} (|\bar{H}|/|H|)$.*

Proof. Let $H \leq G'$. For $x \in \bar{H}$ we write $S_x = \{gxg^{-1} | g \in G\}$. i.e., S_x is the set of all conjugates of x in G. Then it can be seen that $S_x = Hx$. Hence $|S_x| = |Hx| = |H|$. That is each element of $\bar{H}$ has $|H|$ numbers of conjugates. Also $S_x \subseteq \bar{H}$. Therefore the number of conjugacy class in $\bar{H}$ is $|\bar{H}|/|H|$. Again for any conjugacy class S_g of G we have $S_x \subseteq \bar{H_i}$ for some

$H_i \leq G'$. Otherwise assume $x, y \in S_g$ be such that $x \in \bar{H}_i$ and $y \in \bar{H}_j$ for some$H_i \leq G'$ and $H_j \leq G'$ where $H_i \neq H_j$. which implies $S_x \subseteq \bar{H}_i$ and $S_y \subseteq \bar{H}_i$. Since $S_x = S_y S_g$ so $H_i \cap H_j \neq \phi$ which contradicts to the fact that $H_i \cap H_j = \phi$. Hence, $k(G) = \sum_{H \leq G'} (|\bar{H}|/|H|)$, as required. □

We are now in a position to compute $\Pr(G)$ when G is of nilpotance class 2 i.e., $G' \leq Z(G)$. Since G nilpotent, we have, by Theorem 1.9.9,

$$G = G_2 \times G_3 \times \cdots,$$

where G_p is a p-group. So by Theorem 2.1.8(ii), we have

$$\Pr(G) = \Pr(G_2) \cdot \Pr(G_3) \cdots.$$

Therefore we need only to compute $\Pr(G_p)$ for each prime p such that $p \mid |G|$. So, without any loss we assume that G is a p-group with $G' \leq Z(G)$. In this case, the subset $[G,\ x]$ is actually a subgroup, since $[g_1,\ x][g_2,\ x] = [g_1 g_2,\ x]$. Thus we need only consider the subgroups of G'. Hence when we speak of H^* here, it will be assumed that H is a group. Since $H \leq Z(G)$ so $H \trianglelefteq G$; as noted earlier, H^* is a group. Since G is a p-group, both $|H|$ and $|H^*|$ are powers of p.

The following proposition gives a formula for computing $\Pr(G)$ for a p-group G with $G' \leq Z(G)$.

Proposition 2.4.7. *If G is a p-group with $G' \leq Z(G)$, then*

$$\Pr(G) = \frac{1}{|G|} \sum_{K \leq G'} \frac{|K^*|}{|K|} \begin{cases} 1, & \text{if } K = G' \\ 1 - \frac{1}{p}, & \text{if } G'/K \text{ is non trivial cyclic} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Using Theorem 2.1.1 and Lemma 2.4.6, we get

$$\Pr(G) = \frac{k(G)}{|G|} = \frac{1}{|G|}\sum_{H\leq G'}\frac{|\bar{H}|}{|H|}$$

Considering the lattice of subgroups of G' and taking $f = |(^-)|$ and $g = |(\ )^*|$ then applying Möbius Inversion Formula (Theorem 1.11.3), we get $|\bar{H}| = \sum_{K\leq H} m(K,\ H)|K^*|$. Therefore,

$$\begin{aligned}\Pr(G) &= \frac{1}{|G|}\sum_{H\leq G'}\frac{1}{|H|}\left(\sum_{K\leq H} m(K,\ H)|K^*|\right)\\ &= \frac{1}{|G|}\sum_{H\leq G'}\sum_{K\leq H}\left(\frac{m(K,\ H)}{|H|}|K^*|\right)\\ &= \frac{1}{|G|}\sum_{H\leq G'}|K^*|\left(\sum_{K\leq H\leq G'}\frac{m(K,\ H)}{|H|}\right).\end{aligned}$$

The lattice of subgroups of G' containing K is isomorphic to the lattice of subgroups of G'/K. Using this fact and Lemma 1.11.5(i), we get

$$\Pr(G) = \frac{1}{|G|}\sum_{K\leq G'}|K^*|\left(\sum_{H_0\leq(G'/K)}\frac{1}{|K|\cdot|H_0|}m(1,\ H_0)\right).$$

Again by Lemma 1.11.5(ii), the only terms that contribute to the above sum are those for which H_0 is an elementary abelian p-subgroup G'/K. If we let L be the subgroup of elements of order $\leq p$ in G'/K, then the above formula becomes

$$\Pr(G) = \frac{1}{|G|}\sum_{K\leq G'}\frac{|K^*|}{|K|}\left(\sum_{H_0\leq L}\frac{m(1,\ H_0)}{|H_0|}\right).$$

This L is isomorphic to a vector space of dimension n over $G\mathbb{F}(p)$. Thus, if $(C_p)^i$ denotes the direct product of i copies of the cyclic group of order p,

then by Lemma 1.11.6, we get

$$\sum_{H_0 \leq L} \frac{m(1,H_0)}{|H_0|} = \sum_{i=0}^{n} m(1,(C_p)^i) \cdot \frac{1}{p^i} \begin{bmatrix} n \\ i \end{bmatrix} = \sum_{i=0}^{n} (-1)^i p^{i(i-3)/2} \begin{bmatrix} n \\ i \end{bmatrix}$$

For $n = 0$, this comes out to 1, while for $n = 1$, it is $1 - (1/p)$. For $n \geq 2$, it becomes

$$\begin{aligned}
& (-1)^0 p^{0(0-3)/2} \begin{bmatrix} n \\ 0 \end{bmatrix} + \sum_{i=0}^{n-1} (-1)^i p^{i(i-3)/2} \begin{bmatrix} n \\ i \end{bmatrix} + (-1)^n p^{n(n-3)/2} \begin{bmatrix} n \\ n \end{bmatrix} \\
= \; & 1 + (-1)^n p^{n(n-3)/2} + \sum_{i=0}^{n-1} (-1)^i p^{i(i-3)/2} \left(p^i \begin{bmatrix} n-1 \\ i \end{bmatrix} + \begin{bmatrix} n-1 \\ i-1 \end{bmatrix} \right) \\
= \; & 1 + (-1)^n p^{(n(n-3))/2} + \sum_{i=0}^{n-1} (-1)^i p^{i(i-3)/2} \cdot p^i \begin{bmatrix} n-1 \\ i \end{bmatrix} \\
& - \sum_{i=0}^{n-2} (-1)^i p^{(i+1)(i-2)/2} \begin{bmatrix} n-1 \\ i \end{bmatrix} \\
= \; & 1 + (-1)^n p^{n(n-3)/2} - (-1)^0 p^{0(0-3)/2} \cdot p^0 \begin{bmatrix} n-1 \\ 0 \end{bmatrix} \\
& + (-1)^{n-1} p^{n(n-3)/2} \begin{bmatrix} n-1 \\ n-1 \end{bmatrix} + \sum_{i=0}^{n-1} (-1)^i p^{i(i-1)/2} \left(1 - \frac{1}{p}\right) \begin{bmatrix} n-1 \\ i \end{bmatrix} \\
= \; & \left(1 - \frac{1}{p}\right) \sum_{i=0}^{n-1} m(1,\ (C_p)^i) \cdot \begin{bmatrix} n-1 \\ i \end{bmatrix} \\
= \; & \left(1 - \frac{1}{p}\right) \sum_{H \leq (C_p)^{n-1}} m(1,\ H).
\end{aligned}$$

This last sum may be evaluated. Define a function on the subgroups of $(C_p)^{n-1}$ by

$$f(H) = \begin{cases} 1, & \text{if } H = \{1\} \\ 0, & \text{otherwise.} \end{cases}$$

Then define the function $g(H) = \sum_{K \leq H} f(K)$, which is identically equal to 1. If we apply the Möbius Inversion Formula (Theorem 1.11.3) to this pair of functions, we get $f(H) = \sum_{K \leq H} m(K, H)g(K)$. Since $n \geq 2$, $(C_p)^{n-1} \neq \{1\}$, so that

$$\begin{aligned} 0 &= f((C_p)^{n-1}) \\ &= \sum_{K \leq (C_p)^{n-1}} m(K,\ (C_p)^{n-1}) \cdot g(K) \\ &= \sum_{K \leq (C_p)^{n-1}} m(1,\ (C_p)^{n-1}/K) \cdot 1 \\ &= \sum_{H \leq (C_p)^{n-1}} m(1,\ H). \end{aligned}$$

Thus,

$$\sum_{H_0 \leq L} \frac{m(1,\ H_0)}{|H_0|} = \begin{cases} 1, & \text{if } n = 0 \\ 1 - \frac{1}{p}, & \text{if } n = 1 \\ 0, & n \geq 2. \end{cases}$$

First the case $n = 1$ we have $L = \{1\}$; this is equivalent to G'/K having no elements of order p, and hence that $K = G'$. Secondly, if $n = 1$ we have

$$\sum_{H_0 \leq L} \frac{m(1,\ H_0)}{|H_0|} = 1 - \frac{1}{p}.$$

This happens just when G'/K has a unique subgroup of order p; since it is already abelian, G'/K is cyclic and non trivial. Finally, if $n \geq 2$ (that is, all other cases), the sum is zero. Therefore, our formula for $\Pr(G)$ becomes

$$\Pr(G) = \frac{1}{|G|} \sum_{K \leq G'} \frac{|K^*|}{|K|} \begin{cases} 1, & \text{if } K = G' \\ 1 - \frac{1}{p}, & \text{if } G'/K \text{ is non trivial cyclic} \\ 0, & \text{otherwise.} \end{cases}$$

This completes the proof. □

We know that K^* is a subgroup of the p-group G. So K^* is also a p-group, i.e., $|K^*|$ is a power of p. Let us now define an integer $n(K)$ associated to K as follows:

$$|K^*| = \frac{|G|}{p^{n(K)}} \tag{2.4.a}$$

Next we note that the formula for $\Pr(G)$ mentioned in the above proposition can be re-written as

$$\Pr(G) = \frac{1}{|G|} \left[\frac{|(G\prime)^*|}{|G\prime|} + \sum_{\substack{G\prime/K \\ cyclic}} \frac{|K^*|}{|K|} \left(1 - \frac{1}{p}\right) \right]$$

Therefore, using Lemma 2.4.3(ii) and Equation 2.4.a, we get

$$\begin{aligned}\Pr(G) &= \frac{1}{|G'|}\sum_{\substack{G'/K\\ cyclic}}\frac{1}{|K|\cdot p^{n(K)}}\left(1-\frac{p-1}{p}\right)\\ &= \frac{1}{|G'|}\left[1+\sum_{\substack{G'/K\\ cyclic}}\frac{|G'|}{|K|\cdot p^{n(K)}}\left(1-\frac{p-1}{p}\right)\right]\\ &= \frac{1}{|G'|}\left[1+\sum_{\substack{G'/K\\ cyclic}}\frac{(p-1)[G':K]/p}{p^{n(K)}}\right].\end{aligned}$$

Thus we can restate Proposition 2.4.7 as follows

Proposition 2.4.8. *If G is a p-group with $G' \leq Z(G)$, then*

$$\Pr(G) = \frac{1}{|G'|}\left[1+\sum\frac{(p-1)[G':K]/p}{p^{n(K)}}\right].$$

where the sum is over all subgroup K of G' such that G'/K is non-trivial cyclic.

Lemma 2.4.9. *Let G be a p-group with $G' \leq Z(G)$ and K be a subgroup of G'. Define $n(K)$ as in Equation 2.4.a. Then $n(K) = 0$ if and only if $K = G'$.*

Proof. Let $n(K) = 0$ then $|K^*| = |G|/p^0 = |G|$ implies $K^* = G$. i.e., $\{x \in G : [G, x] \subseteq K\} = G$. Therefore, $G' = [G, G] \leq K$. Hence $K = G'$.

Conversely, let $K = G'$ then $K^* = (G')^* = G$ implies $|K^*| = |G|$ forces $n(K) = 0$. □

Now we look for some limiting conditions on the exponents $n(K)$. we write $n(K_i) = n_i$ when the subgroups are indexed. These are nonnegative integers, with $n(K) = 0$ iff $K = G'$ (by Lemma 2.4.9) Furthermore, since we know $K_1 \geq K_2$ implies $(K_1)^* \leq (K_2)^*$. Therefore, $|(K_1)^*| \leq |(K_2)^*|$ which forces $n_1 \geq n_2$.

Next if $K_i = K_j \cap K_k$ and $K_j, K_k \leq K_l$, then we have $(K_jK_k) \leq K_l$, so $(K_j^*K_k^*) \leq (K_jK_k)^* \leq K_l^*$ and $K_j^* \cap K_k^* = K_i^*$ (by Lemma 2.4.3(iv)). Hence,

$$\begin{aligned}\frac{|G|}{p^{n_l}} = |K_l^*| \geq |K_j^*K_k^*| = \frac{|K_j^*| \cdot |K_k^*|}{|K_j^* \cap K_k^*|} &= \frac{|K_j^*| \cdot |K_k^*|}{|K_i^*|} \\ &= \left(\frac{|G|}{p^{n_j}}\right) \cdot \left(\frac{|G|}{p^{n_k}}\right) / \left(\frac{|G|}{p^{n_i}}\right) \\ &= \frac{|G|}{p^{n_j+n_k-n_i}}\end{aligned}$$

Thus

$$\frac{|G|}{p^{n_l}} \geq \frac{1}{p^{n_j+n_k-n_i}}$$

which gives $n_jn_k \geq n_in_l$.

We also have the following proposition.

Proposition 2.4.10. *If H is a p-group with $H' \leq Z(H)$ and H' cyclic, then $H/Z(H) \cong \prod_i (C_{p^{n_i}} \times C_{p^{n_i}})$ with all $n_i \leq k$, and $n_1 = k$. (where, $p^k = |H'|$.) In particular, $[H : Z(H)]$ is a square, and is at least $|H'|^2$.*

Proof. We prove this by induction on the rank r of the abelian group $H/Z(H)$. The proposition is certainly true if $r = 0$. On the other hand, since $H/Z(H)$ is never cyclic since H is a nonabelian, therefore $r \neq 2$. Hence, we may assume $r \geq 1$. We write $H/Z(H) = \langle a_1Z(H)\rangle \times \langle a_2Z(H)\rangle \times \cdots \times \langle a_rZ(H)\rangle$.

Because H is generated by $Z(H)$ and the a_i, and $H' \leq Z(H)$, we have

$$H' = \langle [a_i,\ a_j] : 1 \leq i,\ j \leq r \rangle.$$

Since H' is cyclic of order p^k, this implies in particular that some $[a_i,\ a_j]$ has order p^k. Without loss of generality, we may assume that $c = [a_1,\ a_2]$ is such an element. Since $H' \leq Z(H)$ so $c \in Z(H)$, $[a_1^m,\ a_j] = [a_1,\ a_j]^m$. So since $[a_1,\ a_j]^{p^k} = 1$ for all j but $[a_1,\ a_2]^{p^{k-1}} \neq 1$ implies $a_1^{p^k} \in Z(H)$ but $a_1^{p^{k-1}} \notin Z(H)$. Therefore, $\langle a_1 Z(H) \rangle \cong C_{p^k}$. Similarly, $\langle a_2 Z(H) \rangle \cong C_{p^k}$.

Since c generates H', for each i and j we may write $[a_i,\ a_j] = c^{e_{ji}}$. Then if we set $b_i = a_i a_2^{-e_{1i}} a_1^{e_{2i}}$ for each $i > 2$, we compute

$$[a_1,\ b_i] = [a_1,\ a_i][a_1,\ a_2]^{-e_{1i}}[a_1,\ a_1]^{e_{2i}}$$

$$= c^{e_{1i}} c^{-e_{1i}} = 1$$

and similarly $[a_2,\ b_i] = 1$. Since $\langle a_i \rangle \cap \langle a_i,\ a_2 \rangle \leq Z(H)$, the order of $b_i Z(H)$ is the same as $a_i Z(H)$; from this it is easy to check that

$$H/Z(H) = \langle a_1 Z(H) \rangle \times \langle a_2 Z(H) \rangle \times \langle b_3 Z(H) \rangle \times \cdots \times \langle b_r Z(H) \rangle$$

Now let $K \leq H$ be the subgroup $K = \langle Z(H),\ b_3,\ b_4,\ \cdots,\ b_r \rangle$. It is clear that $Z(H) \subseteq Z(K)$; but conversely, since $H = \langle a_1,\ a_2 \rangle$ and $[a_1,\ b_i] = [a_2,\ b_i] = 1$, we have $Z(K) \subseteq Z(H)$. Thus we may use the inductive hypothesis on K:

(i) $K' \subseteq H'$, so K' is cyclic

(ii) $K' \subseteq H' \subseteq Z(H) = Z(K)$

(iii) $K \subseteq H$ is also a p-group

(iv) $K/Z(K) = K/Z(H) = \langle b_3 Z(H)\rangle \times \cdots \times \langle b_r Z(H)\rangle$ has rank $r-2 < r$.

So, we may assume $K/Z(K) \cong \prod_i (C_{p^{n_i}} \times C_{p^{n_i}})$ for some set of n_i. Thus,

$$\begin{aligned} H/Z(H) &= \langle a_1 Z(H)\rangle \times \langle a_2 Z(H)\rangle \times \langle b_3 Z(H)\rangle \times \cdots \times \langle b_r Z(H)\rangle \\ &\cong (C_{p^k} \times C_{p^k}) \times \prod_i (C_{p^{n_i}} \times C_{p^{n_i}}) \end{aligned}$$

as desired.

To prove the second part recall that $p^{n(K)}$ was defined so that $|K^*| = |G|/p^{n(K)}$. Thus

$$p^{n(K)} = \frac{|G|}{|K^*|} = \frac{|G/K|}{|K^*/K|} = [H : Z(H)]$$

where $H = G/K$ and $K^*/K = Z(G/K) = Z(H)$. Also $H' = KG'/K = G'/K$ which is cyclic for the subgroups K appearing in Proposition 2.4.8, and $H' \leq Z(G)/K \leq K^*/K = Z(H)$. Hence by Proposition 2.4.10, we have

$$\begin{aligned} H/Z(H) &\cong \prod_i (C_{p^{n_i}} \times C_{p^{n_i}}) \\ \Rightarrow |H/Z(H)| &= \prod_i |(C_{p^{n_i}} \times C_{p^{n_i}})| \end{aligned}$$

Therefore, $p^{n(K)} = \prod_i p^{2n_i} = p^{2\sum n_i} = (p^{\sum n_i})^2$. i.e., $n(K) = 2\sum n_i$. Hence all the $n(K)$ are even. Also $p^{n(K)} = [H : Z(H)]$ is a square and $p^{n(K)} = (p^{\sum n_i})^2 \geq (p^k)^2 = |H'|^2$, as required. □

Corollary 2.4.11. *Let G be a finite group such that $|G'| = p$ and $G' \leq Z(G)$, then*

(i) $|G : Z(G)| = p^{2s}$ *for some positive integer* s.

(ii) $\Pr(G) = \frac{1}{p}\left(1 + \frac{p-1}{|G : Z(G)|}\right)$.

Proof. By Corollary 1.6.5, and Corollary 2.2.4, we have

$$G = G_p \times G_{p'}$$

where $G_p' \leq Z(G)$ and $G_{p'}$ is abelian.

Also we have

$$\frac{G}{Z(G)} \cong \frac{G_p}{Z(G_p)}.$$

Therefore by Proposition 2.4.10, we have $|G_p/Z(G_p)| = p^{2s}$ for some positive integer s. Hence part (i) follows.

Part (ii) follows from Proposition 2.4.8 as well as Proposition 2.3.3. □

Remark 2.4.12. Note that part (ii) of Corollary 2.4.11, also follows from Theorem 2.3.1 and Proposition 2.3.3.

2.5 Commutativity degree for groups having $G' \cap Z(G) = \{1\}$

In the previous section we have considered groups G satisfying $G' \leq Z(G)$. Here, we turn to the opposite extreme i.e., $G' \cap Z(G) = \{1\}$. We need the following

Proposition 2.5.1. *If* $N \trianglelefteq G$ *and* $N \cap G' = \{1\}$, *then* $\Pr(G) = \Pr(G/N)$.

Proof. Let L be a subgroup of G such that $L = \langle N,\ g,\ h\rangle$ where $[g,\ h] \in N$. Then for all such L, L' is generated by conjugates of $[N,\ N]$, $[N,\ g]$, $[N,\ h]$ and $[g,\ h]$ while each of these lies in $N \cap G' = \{1\}$. Thus $L' = \{1\}$. i.e., L' is abelian. Therefore, $N \leq L$ and L/N are also abelian, so that

$$\Pr(L) = 1 = \Pr(L/N) \cdot \Pr(N)$$

which implies $k(L) = k(L/N)k(N)$. Hence by Corollary 2.1.6, we get $k(G) = k(G/N)k(N)$ from which proposition follows. □

By Theorem 2.1.8(i) and Proposition 2.5.1, we have the following corollary

Corollary 2.5.2. *If $N \trianglelefteq G$ then $\Pr(G/N) \geq \Pr(G)$. If $N \cap G' = \{1\}$, then equality holds.*

Remark 2.5.3. We may use Proposition 2.5.1, in our case to conclude that $\Pr(G) = \Pr(G/Z(G))$; moreover, $(G/Z(G))' = (G'Z(G))/Z(G) = (G' \times Z(G))/Z(G) \cong G'$ and also $Z(G/Z(G)) = Z(G)^*/Z(G) = (G' \cap Z(G))^*/Z(G) = Z(G)/Z(G)$. Thus, $\Pr(G) = \Pr(K)$ for some group with $K' \cong G'$ and $Z(K) = \{1\}$. Therefore, we must merely look for $\Pr(K)$ for all such groups K.

The above remark can be stated as the following corollary.

Corollary 2.5.4. *Let G be a finite group such that $G' \cap Z(G) = \{1\}$; then there is a finite group K such that $\Pr(K) = \Pr(G)$, $K' \cong G'$ and $Z(K) = \{1\}$.*

Proposition 2.5.5. *For any given G', there are at most a finite number of groups K with $K' \cong G'$ and $Z(K) = \{1\}$.*

Proof. Let $L = K/C_K(K') = N_K(K')/C_K(K')$ is isomorphic to a subgroup of $\mathrm{Aut}(K')$ (by N/C Theorem 1.6.3). Now $L' = K'C_K(K')/C_K(K')$, so that we have an abelian group

$$L/L' = \frac{K/C_K(K')}{K'C_K(K')/C_K(K')} \cong \frac{K}{K'C_K(K')};$$

if $n = \mathrm{rank}(L/L')$, then $K/K'C_K(K')$ can be generated by n elements $x_i(K'C_K(K'))$ with $x_i \in K$.

By Jacobi identity (1.4.3) we have $[C_K(K'),\ C_K(K')] \leq Z(K)$. In our case, this means that $[C_K(K')]' \leq Z(K) = \{1\}$, i.e., $C_K(K')$ is abelian; so if $y \in C_K(K')$ then $[K'C_K(K'),\ y] = \{1\}$. Since $K = \langle x_1,\ x_2, \cdots,\ x_n,\ K'C_K(K')\rangle$, this means that if $y \in C_K(K')$ commutes with each x_i $(1 \leq i \leq n)$ then $y \in Z(K) = \{1\}$.

Therefore, for $y_1,\ y_2 \in C_K(K')$, if $[y_1,\ x_i] = [y_2,\ x_i]$ for each i, then $y_1x_iy_1^{-1} = y_2x_iy_2^{-1}$, so that $y_2^{-1}y_1$ commutes with each x_i and hence from the above we have $y_2^{-1}y_1 = 1$, or $y_1 = y_2$. This tells us that $|C_K(K')|$ is equal to the number of values of the n-tuple $\{[y,\ x_i],\ 1 \leq i \leq n\}$ assumes as y ranges over $C_K(K')$, which is therefore at most

$$\prod_{i=1}^{n} |[C_K(K'),\ x_i]| \leq \prod_{i} |[K,\ x_i]| \leq |K'|^n.$$

Then, from $|K| = |C_K(K')| \cdot |K/C_K(K')|$, we have

$$|K| \leq |K'|^n \cdot |L| \leq |K'|^{|\mathrm{Aut}(K')|}\,|\mathrm{Aut}(K')|,$$

since $|L| \leq |\mathrm{Aut}(K')|$ and $n \leq |L/L'| \leq |L|$. Hence with a given commutator subgroup G', the orders of groups K with $K' \cong G'$ and $Z(K) = \{1\}$ are bounded by a function of G' alone. This justifies the claim that there are only a finite number of such groups. □

Remark 2.5.6. There are further restrictions when $Z(K) = \{1\}$. For example, no element x in K' except $x = 1$ can be fixed under each automorphism of $L \leq \mathrm{Aut}(K')$. Because for $x \in K'$ such that each automorphism of L fixes x we have $kxk^{-1} = x \ \forall \ k \in K$ implies $x = 1$. Furthermore, $L = K/C_K(K')$ is abelian iff $K' \leq C_K(K')$, i.e., iff K' is abelian. In that case, we must have $|K'|$ dividing $|C_K(K')|$. In particular, if $n = 1$, then $|K'| \leq |C_K(K')| \leq |K'|$, and so $K' = C_K(K')$.

Remark 2.5.7. There are some cases in which there are no K with $K' \cong G'$ and $Z(K) = \{1\}$. As noted before, this happens if there is an $x \in G' \setminus \{1\}$ fixed under each automorphism in $L \leq \mathrm{Aut}(K')$. One common case in which this occurs is when G' is isomorphic to C_{2^n}, $n \geq 1$; since G' has unique element of order 2, that element is fixed under all automorphisms, and hence must lie in $Z(G)$. This also happens if $G' \cong C_6$.

We may use these remarks (2.5.6 and 2.5.7) on a specific class of groups to get more detailed information than that supplied in Proposition 2.5.5 in the following Proposition.

Proposition 2.5.8. *If K' is cyclic of prime order p, and $Z(K) = \{1\}$, then $K = \langle a, b \ : \ a^p = b^n = 1, bab^{-1} = a^r \rangle$, where $n|(p-1)$ and $r^j \equiv 1 \bmod p$ if and only if $n|j$.*

Proof. Write $K' = \langle a \rangle$. Then $\mathrm{Aut}(K')$ is cyclic, so that $n = 1$ and $K' = C_K(K')$ as noted above. Further, $L \leq \mathrm{Aut}(K')$ is also cyclic, say $L = \langle bK' \rangle$. Let $|L| = n$ and note that n divides $|\mathrm{Aut}(K')| = p - 1$. Also $|L| = n$ implies $b^n \in K' = \langle a \rangle$, say $b^n = a^s$. If $s \neq 0$, then $\langle b \rangle = \langle b, a \rangle = K$, so K should

be cyclic , and then would not have trivial center. Thus we have $s = 0$, and $b^n = 1$. Next, note that $K' \trianglelefteq K$ implies $bab^{-1} = a^r$. If $r^j \equiv 1 \bmod p$, then $b^j ab^{-j} = a^{r^j} = a$, so b^j commutes with $\langle b \rangle$ and with $\langle a \rangle$, so $b^j \in Z(K) = \{1\}$, and $j \equiv 0 \bmod n$. □

Note that the groups in the above proposition are known as *metacyclic groups*. The following proposition gives us a formula for $\Pr(G)$ for this class of groups.

Proposition 2.5.9. *Let n and r be positive integers and let p be a prime number for which $n|(p-1)$ and $r^j \equiv 1 \bmod p$ if and only if $n|j$. Suppose that $G = \langle a, b \ : \ a^p = b^n = 1, bab^{-1} = a^r \rangle$, then*

$$\Pr(G) = \frac{n^2 + p - 1}{pn^2}.$$

Proof. It is easy to see that $|G'| = p$ and $\mathrm{cd}(G) = \{1,\ n\}$. Now the assertion holds by Theorem 2.3.1. □

Now consider a finite group G such that $|G'| = p$, a prime, and $G' \cap Z(G) = \{1\}$. We have $(G/Z(G))' \cong G'$. On the other hand, if we consider $Z(G/Z(G)) = H/Z(G)$ for some H, $Z(G) \leq H \leq G$, then $[G,\ H] \leq G' \cap Z(G) = \{1\}$ implies $H = Z(G)$ and we have $Z(G/Z(G)) = 1$. Therefore by Proposition 2.5.8, there is a positive integer n depending only on G for which $G/Z(G) = \langle a,\ b \ : \ a^p = b^n = 1,\ bab^{-1} = a^r \rangle$. The number n is called the *invariant number* of G and denoted by $\mathrm{inv}(G)$.

Finally, we can obtain the following proposition using the definition of invariant number and Proposition 2.5.9.

Proposition 2.5.10. *Let G be a finite group such that $|G'| = p$, where p a prime, and $G' \cap Z(G) = \{1\}$. Suppose that* $\mathrm{inv}(G) = n$. *Then*

$$\Pr(G) = \frac{n^2 + p - 1}{pn^2}.$$

Chapter 3

Classification of Groups using Commutativity Degree

In this chapter there are three sections. In the first section we study classification of groups having commutativity degree more than 11/32 [43]. In the next section we describe the concept of isoclinism [19] and finally, in the last section we study classification of groups up to isoclinism [32] as well as isomorphism [33] for groups having commutativity degree at least 1/2.

3.1 Groups having commutativity degree more than 11/32

In some cases it is possible to find the possible set of values of commutativity degree $\Pr(G)$ in a given interval. In 1979, David J. Rusin [43] has found the possible set of values of $\Pr(G)$ in the interval (11/32, 1] and classified all

finite groups for which the commutativity degree is greater than 11/32. i.e., for $\Pr(G) > 11/32$. In this section we study Rusin's Classification of Groups in terms of commutativity degree. By Theorem 2.2.2 of Chapter 2, we have

$$\Pr(G) \leq \frac{1}{4} + \frac{3}{4}\frac{1}{|G'|} \tag{3.1.a}$$

Equation 3.1.a enables us in principle to determine all possible values of $\Pr(G)$ greater than any fraction ρ_0, as long as $\rho_0 > 1/4$; in this situation one need to find all values of $\Pr(G)$ for those groups for which G' is one of the groups of order less than $3/(4\rho_0 - 1)$. If $\Pr(G) > 11/32$ then using Equation 3.1.a one has $|G'| < 8$. Thus we need only to consider those groups for which $G' = \{1\}$, C_2, C_3, C_4, $C_2 \times C_2$, C_5, C_6, S_3, and C_7.

$G' = \{1\}$ means G abelian, so $\Pr(G) = 1$. On the other hand $G' \cong S_3$ is impossible, by Theorem 1.6.7. Thus we need only to consider the seven remaining cases. It turns out that even for a given G', the different possibilities for $G' \cap Z(G)$ require separate discussions. Since $G' \cap Z(G)$ is a subgroup of G', we must investigate the following combinations:

G'	C_2	C_3	C_4	$C_2 \times C_2$	C_5	C_6	C_7
$G' \cap Z(G)$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$
	C_2	C_3	C_2	C_2	C_5	C_2	C_7
			C_4	$C_2 \times C_2$		C_3	
						C_6	

Table 3.1: possibilities for $G' \cap Z(G)$

Case 1. $G' < Z(G)$.

For $G' \cong C_p$ with p a prime, the only proper subgroup of G' is $\{1\}$, which has index p, so that by Proposition 2.4.8, one has $\Pr(G) = 1/p \cdot (1 + (p - 1)/p^{2n})$ for some n also $G/Z(G) \cong C_p^{2n}$ by Proposition 2.4.10. For $p = 2$, we have the infinite family of values $1/2 \cdot (1 + 1/2^{2n})$. For $p = 3$, only $n = 1$ gives a value ($= 11/27$) greater than $11/32$. For $p = 5$ and $p = 7$, all values of $\Pr(G)$ are too small.

For $G' = C_6 \cong C_2 \times C_3$, we know that G is nilpotent, say $G = H_2 \times H_3$ where $H_2' = C_2$ and $H_3' = C_3$. By Proposition 2.4.8 and Theorem 2.1.8(ii), we have

$$\Pr(G) = \frac{1}{2} \cdot \left(1 + \frac{1}{2^{2n}}\right) \cdot \frac{1}{3}\left(1 + \frac{2}{3^{2m}}\right) \leq \frac{5}{8} \cdot \frac{11}{27} < \frac{11}{32}.$$

For $G' = C_4$, the only subgroups in the lattice are C_4, C_2 and $\{1\}$, by Proposition 2.4.8, we have

$$\Pr(G) = \frac{1}{4} \cdot \left(1 + \frac{1}{2^{2m}} + \frac{2}{2^{2n}}\right),$$

with

$$2^{2n} = \frac{|G|}{|\{1\}^*|} = \left|\frac{G}{Z(G)}\right| \geq [G' : \{1\}]^2 = 16,$$

and

$$2^{2m} \geq [G' : C_2]^2 = 4,$$

so that $\Pr(G) \leq 11/32$.

For $G' = C_2 \times C_2$, then by Proposition 2.4.8, we have

$$\Pr(G) = \frac{1}{4} \cdot \left(1 + \frac{1}{2^{2n_1}} + \frac{1}{2^{2n_2}} + \frac{1}{2^{2n_3}}\right).$$

Taking $n_1 \geq n_2 \geq n_3$ for definiteness, we must also have $n_2 + n_3 \geq n_1$, so that $\Pr(G) = 7/16$ $(n_1 = n_2 = n_3 = 1)$ and $25/64$ $(n_1 = 2, n_2 = n_3 = 1)$ are the only values greater than $11/32$.

Case 2. $G' \cap Z(G) = \{1\}$.

By Remark 2.5.6, we have seen that the unique element of order 2 of a group G must lie in the center of G. Thus $G' \cong C_2, C_4$ or C_6 gives contradiction in this case. This also rules out the combination $G' \cong C_6, G' \cap Z(G) \cong C_3$. If $G' = C_2 \times C_2$, then we may find that $G/Z(G) \cong A_4$ and $\Pr(G) = 1/3$.

The remaining cases are of the form $G' \cong C_p$ for p an odd prime; by Proposition 2.5.9, we have $\Pr(G) = (n^2 + p - 1)/n^2 p$ (where $n|p-1$). The only values of $\Pr(G)$ above $11/32$ for groups G in this case are $1/2$ ($G' \cong C_3$ and $G/Z(G) \cong S_3$), $2/5$ ($G' \cong C_5$ and $G/Z(G) \cong D_{10}$) and $5/14$, ($G' \cong C_7$ and $G/Z(G) \cong D_{14}$).

Case 3. Remaining combinations.

First, consider the case $|G'| = 4$ with $|G' \cap Z(G)| = 2$. For this case Rusin claims to have shown that $\Pr(G) = 1/4 \cdot (1 + 1/2^{2t} + 1/2 \cdot 1/2^{2s})$, with $2^{2s} = [C_G(G') : Z(C_G(G'))]$ and $2^{2t} = [H : Z(H)]$ where $H = G/(G' \cap Z(G))$; $s + 1 \geq t \geq 1$. The only value of this, exceeding $11/32$, is $7/16$.

The last case is $G' \cong C_6$ with $G' \cap Z(G) \cong C_2$. Again,Rusin claims to have shown that for such G, $\Pr(G) = 1/4 + 1/2^s$, $s \geq 3$. The only value of this, exceeding $11/32$, is $3/8$ (for $s = 3$).

Summary: If we summerize whatever has been studied so far, then we have the following possibilities for $\Pr(G) > 11/32$:

$\Pr(G)$	G'	$G' \cap Z(G)$	$G/Z(G)$
$\frac{1}{2} \cdot (1 + 2^{-2s})$	C_2	C_2	$(C_2)^{2s}$
$1/2 = .5000$	C_3	$\{1\}$	S_3
$7/16 = .4375$	C_4 or $C_2 \times C_2$	C_2	D_4
	$C_2 \times C_2$	$C_2 \times C_2$	${C_2}^3$ or ${C_2}^4$
$11/27 \approx .4074$	C_3	C_3	$C_3 \times C_3$
$2/5 = .4000$	C_5	$\{1\}$	D_5
$25/64 \approx .3906$	$C_2 \times C_2$	$C_2 \times C_2$	C_2^3 or C_2^4
$3/8 = .3750$	C_6	C_2	$C_2 \times S_3$ or T

Table 3.2: Possibilities for $\Pr(G)$ above $11/32$

(T being the nonabelian group of order 12 with $T \ncong A_4$, and $T \ncong C_2 \times S_3$.)

Remark 3.1.1. We have not discused the last column in the above table for all cases due to lack of resources. However, it definitely reveals the intuitive feeling that the groups having comparatively large centers are abelian.

3.2 Isoclinism Between Groups

In this section we study the concept of isoclinism, introduced by P. Hall [19].

Definition 3.2.1. Let G and H be two groups. Then, the pair (ϕ_1, ϕ_2) is said to be an isoclinism from G to H if

(i) ϕ_1 is an isomorphism from $G/Z(G)$ to $H/Z(H)$,

(ii) ϕ_2 is an isomorphism from G' to H', and

(iii) the diagram

$$\begin{array}{ccc} \frac{G}{Z(G)} \times \frac{G}{Z(G)} & \xrightarrow{\phi_1 \times \phi_1} & \frac{H}{Z(H)} \times \frac{H}{Z(H)} \\ \Big\downarrow a_G & & \Big\downarrow a_H \\ G' & \xrightarrow{\phi_2} & H' \end{array}$$

commutes, that is, $a_H \circ (\phi_1 \times \phi_1) = \phi_2 \circ a_G$ where a_G (similarly a_H) is given by $a_G(xZ(G), yZ(G)) = [x, y] \quad \forall\, x, y \in G$.

If there is an isoclinism from G to H, we say that G and H are *isoclinic*.

Remark 3.2.2. Isoclinism is an equivalence relation between groups.

Let us now study some properties of isoclinism between two groups.

Lemma 3.2.3. *If G and H are isomorphic then they are isoclinic as well.*

Proof. Let $\phi : G \to H$ be an isomorphism. Then ϕ induces isomorphisms $\phi_1 : G/Z(G) \to H/Z(H)$ given by $\phi_1(gZ(G)) = \phi(g)Z(H) \quad \forall \quad g \in G$ and $\phi_2 : G' \to H'$ given by $\phi_2(g) = \phi(g) \quad \forall \quad g \in G'$, so that the following diagram commutes:

$$\begin{array}{ccc} \frac{G}{Z(G)} \times \frac{G}{Z(G)} & \xrightarrow{\phi_1 \times \phi_1} & \frac{H}{Z(H)} \times \frac{H}{Z(H)} \\ \Big\downarrow a_G & & \Big\downarrow a_H \\ G' & \xrightarrow{\phi_2} & H' \end{array}$$

Noting that for $(\alpha, \beta) \in \frac{G}{Z(G)} \times \frac{G}{Z(G)}$ we may write $\alpha = g_1 Z(G)$, $\beta = g_2 Z(G)$, where $g_1, g_2 \in G$ and so

$$\begin{aligned} a_H \circ (\phi_1 \times \phi_1)(\alpha, \beta) &= a_H(\phi_1(\alpha), \phi_1(\beta)) \\ &= a_H(\phi(g_1)Z(H), \phi(g_2)Z(H)) \\ &= [\phi(g_1), \phi(g_2)] \\ &= \phi_2([g_1, g_2]) \\ &= \phi_2(a_G(\alpha, \beta)) \\ &= (\phi_2 \circ a_G)((\alpha, \beta)), \end{aligned}$$

which means that $a_H \circ (\phi_1 \times \phi_1) = \phi_2 \circ a_G$. □

Lemma 3.2.4. *Let G be a finite group and $N \trianglelefteq G$ such that $N \cap G = \{1\}$. Then G is isoclinic to G/N*

Proof. Since $(G/N)' \cong G'$ and $Z(G/N) = \{N\}$ so $(G/N)/Z(G/N) \cong G/N$. Hence the lemma follows. □

Lemma 3.2.5. *Let G and H be two isoclinic groups; then* $\Pr(G) = \Pr(H)$.

Proof. We have

$$\begin{aligned}\left|\frac{G}{Z(G)}\right|^2 \Pr(G) &= \frac{1}{|Z(G)|^2}|G|^2 \Pr(G) \\ &= \frac{1}{|Z(G)|^2}\left|\{(x,y) \in G \times G | xy = yx\}\right| \\ &= \frac{1}{|Z(G)|^2}\left|\{(x,y) \in G \times G | xyx^{-1}y^{-1} = 1\}\right| \\ &= \frac{1}{|Z(G)|^2}\left|\{(x,y) \in G \times G | a_G(xZ(G), yZ(G)) = 1\}\right| \\ &= \left|\{(\alpha,\beta) \in \left(\frac{G}{Z(G)}\right)^2 a_G(\alpha,\beta) = 1\}\right|.\end{aligned}$$

That is

$$\left|\frac{G}{Z(G)}\right|^2 \Pr(G) = \left|\{(\alpha,\beta) \in \left(\frac{G}{Z(G)}\right)^2 a_G(\alpha,\beta) = 1\}\right|. \tag{3.2.a}$$

Similarly,

$$\left|\frac{H}{Z(H)}\right|^2 \Pr(H) = \left|\{(\gamma,\delta) \in \left(\frac{H}{Z(H)}\right)^2 a_H(\gamma,\delta) = 1\}\right| \tag{3.2.b}$$

Let (ϕ_1, ϕ_2) be an isoclinism from G to H; then

$$\begin{aligned}&\{(\alpha,\beta) \in \left(\frac{G}{Z(G)}\right)^2 a_G(\alpha,\beta) = 1\} \\ = \;&\{(\alpha,\beta) \in \left(\frac{G}{Z(G)}\right)^2 \phi_2(a_G(\alpha,\beta)) = 1\} \\ = \;&\{(\alpha,\beta) \in \left(\frac{G}{Z(G)}\right)^2 a_H(\phi_1(\alpha),\phi_1(\beta)) = 1\} \\ = \;&\{(\gamma,\delta) \in \left(\frac{H}{Z(H)}\right)^2 a_H(\gamma,\delta) = 1\}.\end{aligned}$$

Thus, from Equation 3.2.a and Equation 3.2.b, it follows that

$$\left|\frac{G}{Z(G)}\right|^2 \Pr(G) = \left|\frac{H}{Z(H)}\right|^2 \Pr(H).$$

But $G/Z(G)$ and $H/Z(H)$ are isomorphic (via ϕ_1), hence $|G/Z(G)| = |H/Z(H)|$; the equality $\Pr(G) = \Pr(H)$ follows. □

Proposition 3.2.6. *Let G be any group (finite or infinite); then there is a group G_1 isoclinic to G such that $Z(G_1) \subseteq G_1'$. If G is finite, so is any such G_1.*

Proof. We have every group is a homomorphic image of a free group. Choose a free group F such that $\pi : F \to G$ be a surjective homomorphism. Consider the map $\phi : F \to G \times F/F'$ given by $\phi(x) = (\pi(x), xF')\ \forall x \in F$. Let $T = \phi(F)$.

Then

$$\begin{aligned} Z(T) &= \{(g,\bar{f}) \in T : [(g,\bar{f}),(h,\bar{k})] = 1 \ \forall \ (h,\bar{k}) \in T\} \\ &= \{(g,\bar{f}) \in T : [g,h] = 1 \text{ and } [\bar{f},\bar{k}] = 1 \ \forall \ (h,\bar{k}) \in T\} \\ &= \{(g,\bar{f}) \in T : g \in Z(G)\} \\ &= \{\phi(x) : x \in \pi^{-1}(Z(G))\} \\ &= \phi(A) \ \text{ where } \ A = \pi^{-1}(Z(G)). \end{aligned}$$

We have

$$\begin{aligned} T/T' = \phi(F)/\phi(F') &= \frac{F/\operatorname{Ker}\phi}{(F/\operatorname{Ker}\phi)'} \\ &= \frac{F/\operatorname{Ker}\phi}{F'\operatorname{Ker}\phi/\operatorname{Ker}\phi} \\ &= \frac{F}{F'\operatorname{Ker}\phi} \end{aligned}$$

but $\operatorname{Ker}\phi = \operatorname{Ker}\pi \cap F' \subseteq F'$.

Thus

$$T/T' \cong F/F'$$

is free abelian. Also $Z(T)/(Z(T) \cap T') \cong Z(T)T'/T'$, hence to a subgroup of T/T'; since subgroup of a free abelian group is free abelian therefore $Z(T)/(Z(T) \cap T')$ is also free abelian. We can thus find a free abelian subgroup B of $Z(T)$ such that

$$Z(T) = B \times (Z(T) \cap T').$$

B, as a subgroup of $Z(T)$, is normal in T; we intend to show that

$$G_1 = \frac{T}{B}$$

satisfies our requirements.

Let $C/B = Z(G_1) = Z(T/B)$; then

$$[C, T] \subseteq T' \cap B = T' \cap Z(T) \cap B = \{1\},$$

i.e., $C \subseteq Z(T)$. Also $\frac{Z(T)}{B} \subseteq Z\left(\frac{T}{B}\right) = \frac{C}{B}$ gives $Z(T) \subseteq C$. Therefore

$$Z\left(\frac{T}{B}\right) = \frac{Z(T)}{B}.$$

In particular,

$$Z(G_1) = \frac{Z(T)}{B} = \frac{B \times (Z(T) \cap T'}{B} \subseteq \frac{BT'}{B} = \left(\frac{T}{B}\right)' = G_1'.$$

Let us first define

$$\tau : \frac{G}{Z(G)} \to \frac{G_1}{Z(G_1)}$$

by

$$\tau(\alpha) = (\phi(f)B)Z(G_1),$$

where

$$\alpha = \pi(f)Z(G) \quad (f \in F).$$

If $\alpha = \pi(f_1)Z(G) = \pi(f_2)Z(G)$, then $\pi({f_1}^{-1}f_2) = \pi({f_1}^{-1})\pi(f_2) \in Z(G)$, hence ${f_1}^{-1}f_2 \in \pi^{-1}(Z(G)) = A$. Therefore

$$\phi(f_1)^{-1}\phi(f_2) = \phi({f_1}^{-1}f_2) \in \phi(A) = Z(T)$$

from which it follows that

$$(\phi(f_1)B)^{-1}(\phi(f_2)B) = (\phi(f_1)^{-1}\phi(f_2))B \in \frac{Z(T)}{B} = Z\left(\frac{T}{B}\right) = Z(G_1)$$

and $(\phi(f_1)B)Z(G_1) = (\phi(f_2)B)Z(G_1)$. We have proved that τ is well-defined; it is clearly a homomorphism of groups. Also for $(\phi(f)B)Z(G_1) \in \dfrac{G_1}{Z(G_1)}$ where $f \in F$ we have $\pi(f)Z(G) \in \dfrac{G}{Z(G)}$ such that

$$\tau(\pi(f)Z(G)) = (\phi(f)B)Z(G_1).$$

i.e., τ is surjective. Let $\alpha = \pi(f)Z(G) \in \operatorname{Ker}\pi$ then $\phi(f)B \in Z(G_1) = Z(T)/B$, i.e., $\phi(f) \in Z(T) = \phi(A)$. Therefore $\phi(f) = \phi(a)$, where $a \in A = \pi^{-1}(Z(G))$. It follows that

$$\pi(f) \subseteq Z(G)$$

and

$$\alpha = \pi(f)Z(G) = Z(G) = 1_{G/Z(G)},$$

i.e., τ is injective, therefore an isomorphism.

Obviously,

$$G_1' = \left(\frac{T}{B}\right)' = \frac{T'B}{B} \cong \frac{T'}{T' \cap B} \cong T' = \phi(F)' = G' \times \{1\} \cong G'$$

all the isomorphisms being canonical. We have in fact shown that

$$\sigma : G' \to G_1'$$

defined by

$$\forall x \in G' \quad \sigma(x) = (x, 1)B$$

is an isomorphism. where 1 is identified with $1_{F/F'}$, the identity element of F/F'. We shall establish that (τ, σ) is an isoclinism from G to G', thereby completing the proof of the proposition. It is now clearly enough to check condition (iii) in Definition 3.2.1. Then let $(\alpha, \beta) \in \left(\frac{G}{Z(G)}\right)^2$, with $\alpha = \pi(f_1)Z(G)$ $(f_1 \in F)$ and $\beta = \pi(f_2)Z(G)$ $(f_2 \in F)$. One has

$$\begin{aligned}
[a_{G_1} \circ (\tau \times \tau)](\alpha, \beta) &= a_{G_1}(\tau(\alpha), \tau(\beta)) \\
&= a_{G_1}((\phi(f_1)B)Z(G_1), (\phi(f_2)B)Z(G_1)) \\
&= [\phi(f_1)B, \phi(f_2)B] \\
&= ([\pi(f_1), \pi(f_2)], 1)B \\
&= \sigma([\pi(f_1), \pi(f_2)]) \\
&= \sigma(a_G(\alpha, \beta)) \\
&= [\sigma \circ a_G](\alpha, \beta).
\end{aligned}$$

Thus $a_{G_1} \circ (\tau \times \tau) = \sigma \circ a_G$, as claimed.

If G is finite, so are $G/Z(G)$ and hence $G_1/Z(G_1) \cong G/Z(G)$; but $Z(G_1) \subseteq G_1'$, so $|G; G_1|$ is finite. But $G_1' \cong G'$ is finite, so G_1 is also finite. □

Let G be a finite group. Consider the set $\mathbb{ISO}(G)$ defined by

$$\mathbb{ISO}(G) = \{H \mid H \text{ is a finite group isoclinic to } G \text{ such that } Z(H) \leq H'\}.$$

Then by Proposition 3.2.6, $\mathbb{ISO}(G)$ is non-empty. Let us state the following lemma which will be useful for further considerations.

Lemma 3.2.7. *Let G be a finite group such that $G' \leq Z(G)$. Then*

$$\mathbb{ISO}(G) = \{H : H \text{ is a finite group isoclinic to } G \text{ such that } Z(H) = H'\}.$$

Moreover, if $|G'| = p$, p prime, then $\{|H| : H \in \mathbb{ISO}(G)\} = \{p^n\}$ for some positive integer n.

Proof. If $H \in \mathbb{ISO}(G)$ then G and H are isoclinic. Let (φ, ψ) be an isoclinism from G to H. We have $Z(H) \leq H'$. By assumption $G' \leq Z(G)$ therefore $G/Z(G)$ is abelian and since $G/Z(G) \cong H/Z(H)$ (via φ), we obtain that $H/Z(H)$ is abelian which implies that $H' \leq Z(H)$. Hence we have $H' = Z(H)$. This proves the first part of the lemma.

For the proof of the second part of the lemma suppose that H and K be two elements of $\mathbb{ISO}(G)$. Then we have

$$|H/H'| = |H/Z(H)| = |K/Z(K)| = |K/K'|.$$

But $|H'| = |K'|$, so we have $|H| = |K|$ which implies that $\{|H| : H \in \mathbb{ISO}(G)\} = \{l\}$ for some positive integer l.

Now suppose that $|G'| = p$ and $H \in \mathbb{ISO}(G)$ then $|H'| = p$. If q $(\neq p)$ is a prime divisor of $|H|$, the nilpotency of H implies that the Sylow q-subgroup of H must lie in $Z(H) = H'$ which is a contradiction since $|H'| = p$. Therefore H must be a p-group and so $l = p^n$ for some positive integer n which completes the proof. □

Viewing the above lemma for the finite group G such that $|G'| = p$, p prime and $G' \leq Z(G)$, the positive integer n for which $\{|H| : H \in \mathbb{ISO}(G)\} = \{p^n\}$ is called *isoclinic exponent* of G and denoted by iso.exp(G).

Lemma 3.2.8. *Let S be a nonabelian simple group then any group G isoclinic to S is isomorphic to $S \times A$ for some abelian group.*

Proof. G is isoclinic to S implies $G' \cong S' \cong S$, therefore

$$G' \cap Z(G) \subseteq Z(G') = \{1\}.$$

But

$$\frac{G}{Z(G)} \cong \frac{S}{Z(S)} \cong S$$

is perfect, hence $G = G'Z(G) = G' \times Z(G) \cong S \times Z(G)$. The result follows with $A = Z(G)$. □

Lemma 3.2.9. *Let G be a group (finite or infinite) and H be a subgroup of G. If $G = HZ(G)$ then G and H are isoclinic, and if H is finite then the converse is also true.*

Proof. If $G = HZ(G)$ then for each $g \in G$ one has $g = hz$ for some $h \in H$ and $z \in Z(G)$. Now, for $h' \in Z(H)$ one has $h'g = h'(hz) = (h'h)z = h(h'z) = (hz)h' = gh'$ for all $g \in G$. Which implies $h' \in Z(G)$. Therefore $Z(H) \subseteq H \cap Z(G)$ and the other inclusion is trivial. Thus $Z(H) = H \cap Z(G)$ and

$$\frac{H}{Z(H)} = \frac{H}{H \cap Z(G)} \cong \frac{HZ(G)}{Z(G)} = \frac{G}{Z(G)},$$

the isomorphism $i_1 : H/Z(H) \to G/Z(G)$ being induced by the inclusion $i : H \to G$.

Furthermore, let $x,\ y \in G$; then $x = h_1 z_1 (h_1 \in H,\ z_1 \in Z(G))$ and $y = h_2 z_2 (h_2 \in H,\ z_2 \in Z(G))$, then $[x, y] = [h_1,\ h_2] \in H'$ and $G' = H'$. Let $1'_G$ be the identity mapping from G' to H'. It is clear that $(i_1,\ 1'_G)$ is an isoclinism from H to G.

Conversely, if H is isoclinic to G and is finite, then $G/Z(G) \cong H/Z(H)$ is also finite. But

$$\left|\frac{G}{Z(G)}\right| \geq \left|\frac{HZ(G)}{Z(G)}\right| = \left|\frac{H}{H \cap Z(G)}\right| \geq \left|\frac{H}{Z(H)}\right| = \left|\frac{G}{Z(G)}\right|.$$

Thus one has the equality all along, and so $G = HZ(G)$. □

Lemma 3.2.10. *Let G and H be two isoclinic finite groups, then*

$$|G' \cap Z(G)| = |H' \cap Z(H)|.$$

Proof. Since G and H are isoclinic, so $\frac{G}{Z(G)} \cong \frac{H}{Z(H)}$ implies $\left(\frac{G}{Z(G)}\right)' \cong \left(\frac{H}{Z(H)}\right)'$. But

$$\left(\frac{G}{Z(G)}\right)' = \frac{G'Z(G)}{Z(G)} \cong \frac{G'}{G' \cap Z(G)}$$

and similarly

$$\left(\frac{H}{Z(H)}\right)' \cong \frac{H'}{H' \cap Z(H)}.$$

Therefore

$$\frac{|G'|}{|G' \cap Z(G)|} = \frac{|H'|}{|H' \cap Z(H)|}.$$

Since $G' \cong H'$, it follows that $|G' \cap Z(G)| = |H' \cap Z(H)|$. □

Remark 3.2.11. We can use the Lemma 3.2.10, to give a new proof of Corollary 2.5.4 of Chapter 2 as follows:

By Proposition 3.2.6, there is a finite group K isoclinic to G such that $Z(K) \subseteq K'$. Then

$$|Z(K)| = |Z(K) \cap K'| = |Z(G) \cap G'| = |\{1\}| = 1,$$

by Lemma 3.2.10 and the hypothesis on G, i.e., $Z(K) = \{1\}$. Now the isoclinism between K and G implies $K' \cong G'$ and $\Pr(K) = \Pr(G)$ by Lemma 3.2.5. This proves Corollary 2.5.4.

3.3 Groups having commutativity degree at least $1/2$

In this section we consider the groups having commutativity degree at least $1/2$ and classify them upto isoclinism [32] as well as upto isomorphism [33].

3.3.1 Classification upto isoclinism

The main result here is the following

Theorem 3.3.1. *Let G be a finite group such that $\Pr(G) \geq \frac{1}{2}$, then G is isoclinic to exactly one of the following*

(i) *trivial group* $\{1\}$,

(ii) *an extraspecial* $2-$*group,*

(iii) S_3, *the symmetric group of three symbols .*

Proof. By Proposition 3.2.6, there is a group H isoclinic to G such that $Z(H) \subseteq H'$; now Lemma 3.2.5 implies that $\Pr(H) = \Pr(G) \geq \frac{1}{2}$. We may therefore assume that $Z(G) \subseteq G'$. Theorem 2.2.2 yields the bound

$$|G'| \leq \frac{3}{4\Pr(G) - 1} \leq \frac{3}{4 \cdot \frac{1}{2} - 1} = 3.$$

Let us consider two cases:

Case 1. $Z(G) \subset G'$

In this case one has $Z(G) = \{1\}$ (because $|G'| \in \{1, 2, 3\}$). Let

$$E = \{g \in G | \ |G : C_G(g)| = 2\},$$

let $n = |G|$ and $|E|$. Clearly $|G : C_G(1)| = 1$. Thus there are exactly $n - m - 1$ elements of G such that $|G : C_G(g)| \geq 3$, therefore

$$\begin{aligned}
\frac{n^2}{2} \leq |G|^2 \Pr(G) &= \sum_{x \in G} |C_G(x)| \\
&= |C_G(1)| + \sum_{x \in E} |C_G(x)| + \sum_{x \in G, |G:C_G(x)| \geq 3} |C_G(x)| \\
&\leq n + m \cdot \frac{n}{2} + (n - m - 1)\frac{n}{3} \\
&= \frac{2n}{3} + \frac{mn}{6} + \frac{n^2}{3},
\end{aligned}$$

i.e., $m \geq n-4$. If $n < 10$, the condition $\{1\} = Z(G) \subset G'$ forces $G \cong S_3$, and we are done. We may therefore assume $n \geq 10$, and thus $m \geq n-4 \geq n/2+1$. Now let $g \in E$ then by definition of E we have $|G : C_G(g)| = 2$, therefore $C_G(g) \trianglelefteq G$ and $G/C_G(g)$ is abelian (being order 2) i.e., $G' \subseteq C_G(g)$ and $g \in C_G(g)$. Thus we have shown that

$$E \subseteq C_G(G').$$

It follows that $|C_G(G')| \geq |E| = m > n/2$, implies $|G : C_G(G')| < 2$, i.e., $G = C_G(G')$ therefore $G' \subseteq Z(G)$, which is a contradiction. Hence $n \geq 10$ is not possible in this case.

Case 2. $Z(G) = G'$

In this case G is nilpotent. For each prime p, let G_p be the Sylow p-subgroup of G. If G_p is nonabelian, then by Theorem 2.1.8 (i) and Theorem 2.2.5, we have

$$\frac{1}{2} \leq \Pr(G) \leq \Pr(G_p) \leq \frac{p^2 + p - 1}{p^3}$$

i.e., $p^3 \leq 2p^2 + 2p - 2 < 2p(p+1)$ and $p^2 < 2p + 2$, hence $(p-1)^2 < 3 < 4$, i.e., $p < 3$, thus $p = 2$. Therefore G is the direct product of its Sylow 2-group G_2 and an abelian group, say H. i.e., $G = G_2 \times H$. Then $Z(G) = Z(G_2) \times H$ i.e., $G' = Z(G_2) \times H$ also $G' = G_2' \times \{1\}$, thus $G_2' \times \{1\} = Z(G_2) \times H$ forces $G_2' = Z(G_2)$ and $H = \{1\}$. That is G is a 2-group.

Now $|G'| \leq 3$ and $|G'|$ divides $|G|$ implies $Z(G) = G' = \{1\}$ or $|G'| = 2$. In the first case $G = \{1\}$ and in the second case $Z(G) = G'$ has order 2, i.e., G is an extraspecial 2-group. □

Corollary 3.3.2. *If* $\Pr(G) \geq \frac{1}{2}$, *one of the following holds:*

(i) G *is abelian and* $\Pr(G) = 1$.

(ii) $G/Z(G)$ *is an elementary abelian group of order* 2^{2m} *for some* $m \geq 1$, $|G'| = 2$, *and* $\Pr(G) = \frac{1}{2}(1 + 1/4^m) \leq \frac{5}{8}$.

(iii) G *is isoclinic to* S_3 *and* $\Pr(G) = \frac{1}{2}$.

Proof. By Theorem 3.3.1, G is isoclinic to $\{1\}$, an extraspecial 2-group, or S_3; the first case leads to (i), and the third one to (iii). Let G is isoclinic to

an extraspecial 2-group we may assume that G is an extraspecial 2-group. i.e., $G' = Z(G)$ has order 2. By Proposition 2.4.8 of Chapter 2, we have

$$\begin{aligned}\Pr(G) &= \frac{1}{2} \cdot \left(1 + \frac{1}{2^{2m}}\right), m \geq 1 \\ &= \frac{1}{2} \cdot \left(1 + \frac{1}{4^m}\right), m \geq 1\end{aligned}$$

where $2^{2m} = \frac{|G|}{|\{1\}^*|} = \frac{|G|}{|Z(G)|}$. Also by Proposition 2.4.10, we have $\frac{G}{Z(G)} \cong C_2^{2m}$. Thus $\frac{G}{Z(G)}$ is an elementary abelian group of order 2^{2m} for some $m \geq 1$. □

Some immediate consequences of Corollary 3.3.2 are

(i) If G is not abelian, then $\Pr(G) \leq \frac{5}{8}$.

(ii) If $\Pr(G) > \frac{1}{2}$, then G is nilpotent.

(iii) If $\Pr(G) = \frac{1}{2}$ and G is not nilpotent, then $G/Z(G) \cong S_3$ and $G' \cong C_3$.

(iv) If $\frac{1}{2} < \Pr(G) < 1$, then $\Pr(G) \in \{\frac{1}{2}(1 + 1/4^n) \mid n \in \mathbb{N}, n \geq 1\}$.

PROBLEM: Is it possible to classify (upto isoclinism) all finite groups for $\Pr(G) \geq \frac{1}{p}$, where p is any odd prime ?

3.3.2 Classification upto Isomorphism

In order to study the classification upto isomorphism, we need to develop some group theoretic tools.

Proposition 3.3.3. *Let p be a prime number, G an abelian r-group and u an element of G; then either*

(i) $\langle u \rangle$ *is a direct factor of* G, *or*

(ii) *For some* $v \in G$, $o(uv^p) < o(u)$.

Proof. We have $G = G_1 \times G_2 \times \cdots G_k$ where G_i's are finite cyclic p-groups. We may assume that $u \neq 1 \in G$ as in that case (i) holds trivially. Let $u = (u_1, u_2, \cdots u_k)$. Consider the set $S = \{i | 1 \leq i \leq k \text{ and } o(u_i) = o(u)\}$. Also note that $o(u) = \max\limits_{1 \leq i \leq k} \{o(u_i)\}$

Case 1. For all $i \in S, \langle u_i \rangle < G_i$

In this case u_i and hence u_i^{-1} are not generators of $G_i \ \forall \ i \in S$. Therefore for all $i \in S$ there exists $y_i \in G$ such that $u_i^{-1} = y_i^p$.

Let $v = (x_1, x_2, \cdots x_k)$ where

$$x_i = \begin{cases} y_i, & \text{if } i \in S \\ 1, & \text{if } i \notin S. \end{cases}$$

Then $uv^p = (u_1, u_2, \cdots u_k)(x_1^p, x_2^p, \cdots x_k^p) = (w_1, w_2, \cdots, w_k)$ where

$$w_i = \begin{cases} 1, & \text{if } i \in S \\ u_i, & \text{if } i \notin S. \end{cases}$$

Therefore

$$o(uv^p) = \max_{1 \leq i \leq k} \{o(w_i)\} = \max_{\substack{1 \leq i \leq k \\ i \notin S}} \{1, o(u_i)\} < o(u)$$

and so (ii) holds.

Case 2. There exists an $i \in S$ such that $\langle u_i \rangle = G_i$

Without any loss we may assume $\langle u_1 \rangle = G_1$. Let $H = \{1\} \times G_2 \times G_3 \times \cdots \times G_k$.

Since every $g_i \in G_i$ we have $(g_1, g_2, \cdots, g_k) = (g_1, 1, \cdots, 1)(1, g_2, \cdots, g_k)$ and $g_1 = u_1^m$ for some m, also $(u_1, 1, \cdots, 1) = (u_1, u_2, \cdots, u_k)(1, u_2^{-1} \cdots, u_k^{-1}) \in \langle u \rangle H$ therefore $G \subseteq \langle u \rangle H$. Hence $G = \langle u \rangle H$.

Now

$$|G| = |\langle u \rangle H| = \frac{|\langle u \rangle||H|}{|\langle u \rangle \cap H|} = \frac{o(u)|H|}{|\langle u \rangle \cap H|}$$
$$= \frac{o(u_1)|H|}{|\langle u \rangle \cap H|} = \frac{|G_1||G_2| \cdots |G_k|}{|\langle u \rangle \cap H|} = \frac{|G|}{|\langle u \rangle \cap H|}.$$

Which forces $\langle u \rangle \cap H = \{1\}$. *Hence* $\langle u \rangle$ *is a direct factor of* G. *i.e.,* (i) holds. □

Let p and q denote prime numbers such that $q|p-1$. Then there exists, up to isomorphism, one and only one non abelian group of order pq, which is

$$D_{pq} =< \sigma, \tau | \sigma^p = \tau^q = 1, \tau^{-1}\sigma\tau = \sigma^\lambda >$$

where $\lambda \not\equiv 1(\mathrm{mod}p)$ but $\lambda^q \equiv 1(\mathrm{mod}p)$. Let $\theta \in \{1, 2, \cdots, q-1\}$ and $m \geq 1$, we define a new group $T_{p,q,m,\theta}$ by generators and relations in the following way

$$T_{p,q,m,\theta} =< \pi, \tau | \pi^p = \tau^{q^m} = 1, \tau^{-1}\pi\tau = \pi^{\lambda^\theta} > .$$

Then $|T_{p,q,m,\theta}| = pq^m$ and $\tau^q \in Z(T_{p,q,m,\theta})$, therefore

$$C =< \tau^q > \trianglelefteq\ T_{p,q,m,\theta}.$$

But

$$\frac{T_{p,q,m,\theta}}{C} =< \bar{\pi}, \bar{\tau} | (\bar{\pi})^p = (\bar{\tau})^q = 1, (\bar{\tau})^{-1}\bar{\pi}\bar{\tau} = (\bar{\pi})^{\lambda^\theta} >$$

is isomorphic to D_{pq}, hence has center trivial, therefore $Z(T_{p,q,m,\theta}) \subseteq C$ and

$$Z(T_{p,q,m,\theta}) = C.$$

Thus it follows that

$$\frac{Z(T_{p,q,m,\theta}}{Z(T_{p,q,m,\theta})} \cong D_{pq}.$$

Conversely, one has

Theorem 3.3.4. *If the group G is such that $G/Z(G) \cong D_{pq}$, then there exists $\theta \in \{1, 2, \cdots, q-1\}$, $m \geq 1$ and a finite abelian group A, such that $G \cong T_{p,q,m,\theta} \times A$.*

Proof. Let r be a prime and R be a Sylow r-subgroup of G. Then $RZ(G)/Z(G)$ is a Sylow subgroup of $(G/Z(G)) \cong D_{pq}$. Since $\left|\frac{RZ(G)}{Z(G)}\right| = p$ or q therefore cyclic. Also $\frac{RZ(G)}{Z(G)} \cong \frac{R}{R \cap Z(G)}$ hence $\frac{R}{R \cap Z(G)}$ is cyclic. But $R \cap Z(G) \subseteq Z(R)$ therefore $R/Z(R)$ is cyclic hence R is abelian. Thus we have seen that all Sylow subgroups of G are abelian. Hence by Taunt's result [48], we have $G' \cap Z(G) = \{1\}$. Then

$$G' \cong \frac{G'}{G' \cap Z(G)} \cong \frac{G'Z(G)}{Z(G)} = \left(\frac{G}{Z(G)}\right)' \cong (D_{pq})' = < \sigma >,$$

that has order p; let π be an element of G' sent to σ by the above sequence of isomorphisms. Then $G' = < \pi >$ has order p.

As $(G/Z(G)) \cong D_{pq}$ is not abelian so $G' \nsubseteq Z(G)$, i.e., $\pi \notin Z(G)$; therefore one can find $t \in G$ such that $\pi t \neq t\pi$, i.e., $t^{-1}\pi t \neq \pi$.

But $< \pi > = G' \trianglelefteq G$, so $t^{-1}\pi t \in < \pi >$. i.e., $t^{-1}\pi t$ is a power of π, say π^n with $n \equiv 1 (\mathrm{mod} p)$.

But $t^{-1}\pi t = \pi^n$ implies $(t^{-1}\pi t)Z(G) = \pi^n Z(G)$. we may write $\bar{t}^{-1}\sigma\bar{t} = \sigma^n$ putting $tZ(G) = \bar{t}$ and $\pi Z(G) = \sigma$.

But the conjugates of σ in D_{pq} are of the form σ^{λ^u}. Therefore $\sigma^n = \sigma^{\lambda^u}$ for some $u \in \{0, 1, 2, \cdots, q-1\}$ and $n \equiv \lambda^u (\mathrm{mod}\, p)$. Therefore $t^{-1}\pi t = \pi^n =$

π^{λ^u}, with $u \neq 0$ (as $t^{-1}\pi t \neq \pi$) and hence $q \nmid u$. Let $o(t) = q^m\gamma$ where $q \nmid \gamma$ then $(t^\gamma)^{-1}\pi t^\gamma = \pi^{\lambda^{u\gamma}}$ and $u\gamma \not\equiv 0(\mathrm{mod}q)$. Let θ denotes the remainder in the division of $u\gamma$ by q. Setting $\tau = t^\gamma$ we see that

$$\tau^{-1}\pi\tau = \pi^{\lambda^\theta} \tag{3.3.a}$$

and $o(\tau) = q^m$. If one had $m = 0$ then would follow $\tau = 1, \pi = \pi^{\lambda^\theta}$, i.e., $\lambda^\theta \equiv 1(\mathrm{mod}p)$, i.e., $q \mid \theta$, a contradiction; therefore $m \geq 1$.

Among all $\tau \in G$ of q-power order q^m such that 3.3.a hold, let us choose one corresponding to the minimal possible value of m; it is clear that $H = < \pi, \tau >$ is isomorphic to $T_{p,q,m,\theta}$. We may write

$$pq = |D_{pq}| = \left|\frac{G}{Z(G)}\right| \geq \left|\frac{HZ(G)}{Z(G)}\right| = \left|\frac{H}{H \cap Z(G)}\right| = \left|\frac{H}{Z(H)}\right| \left|\frac{Z(H)}{H \cap Z(G)}\right|$$

$$= \left|\frac{T_{p,q,m,\theta}}{Z(T_{p,q,m,\theta})}\right| \left|\frac{Z(H)}{H \cap Z(G)}\right| = pq \left|\frac{Z(H)}{H \cap Z(G)}\right| \geq pq,$$

as $H \cap Z(G) \subseteq Z(H)$; therefore we have equality all along. In particular, $G = HZ(G)$ and $Z(H) = H \cap Z(G)$. But $\tau^q \in Z(H)$ therefore $\tau^q \in Z(G)$, and $o(\tau^q) = \frac{1}{q}o(\tau) = q^{m-1}$. Applying now Proposition 3.3.3 to $r = q$, $G = Z(G)_q$ (the q-component of $Z(G)$), and $u = \tau^q$, we obtain that either:

(a) $< \tau^q >$ is a direct factor of $Z(G)_q$ or

(b) For some $v \in Z(G)_q$, $o(\tau^q v^q) < o(\tau^q)$.

If (b) would hold, we would have

$$o(\tau v) \leq q\, o(\tau^q v^q) \leq o(\tau^q) = q^{m-1},$$

hence $o(\tau v) = q^r$ for some $r \leq m-1$ and $(\tau v)^{-1}\pi(\tau v) = v^{-1}(\tau^{-1}\pi\tau)v = \tau^{-1}\pi\tau = \pi^{\lambda^\theta}$, which contradicts to the minimality of m. Therefore (a) holds,

$$Z(G)_q =< \tau^q > \times B$$

for some (abelian) group B, and

$$\begin{aligned} G = HZ(G) &= < H, Z(G) > = < \pi, \tau, Z(G)_q, Z(G)_{q'} > \\ &= < \pi, \tau, \tau^q, B, Z(G)_{q'} > = < \pi, \tau, B, Z(G)'_q > \\ &= < \pi, \tau > \times B \times Z(G)_{q'} \cong T_{p,q,m,\theta} \times B \times Z(G)'_q. \end{aligned}$$

Thus we have proved that $G \cong T_{p,q,m,\theta} \times A$, where $A = B \times Z(G)_{q'}$. □

Corollary 3.3.5. *If $G/Z(G) \cong S_3$, then $G \cong G_m \times A$ for some $m \geq 1$, where A is an abelian group and $G_m =< \sigma, \tau | \sigma^3 = \tau^{2^m} = 1, \tau^{-1}\sigma\tau = \sigma^{-1} >$.*

Proof. Let us apply Theorem 3.3.4 with $p = 3$, $q = 2$; then $D_6 \cong S_3$ and it follows that $G \cong T_{3,2,m,\theta} \times A$ for some $m \geq 1$, $\theta \in \{1\}$ and some abelian group A, that is

$$G \cong T_{3,2,m,1} \times A.$$

But it is clear that

$$T_{3,2,m,1} =< \pi, \tau | \pi^3 = \tau^{2^m} = 1, \tau^{-1}\pi\tau = \pi^{-1} >$$

where $\lambda \not\equiv 1(\text{mod}3)$ but $\lambda^2 \equiv 1(\text{mod}3)$ therefore $\lambda \equiv -1(\text{mod}3)$. Thus $T_{3,2,m,1} \cong G_m$. Hence $G \cong G_m \times A$. □

Theorem 3.3.6. *A finite group G has commutativity degree $\Pr(G) \geq \frac{1}{2}$ if and only if one of the following holds:*

(i) *G is abelian.*

(ii) *$G \cong P \times A$, where P is a 2-group such that $|P'| = 2$, and A is an abelian group of odd order,*

(iii) *$G \cong G_m \times A$, where $m \geq 1$, A is abelian and $G_m =< \sigma, \tau | \sigma^3 = \tau^{2^m} = 1, \tau^{-1}\sigma\tau = \sigma^{-1} >$.*

Proof. By Corollary 3.3.2, one of the following hold

(1) G is abelian

(2) $G/Z(G)$ is an elementary abelian group of order 2^{2m} for some $m \geq 1$, and $|G'| = 2$

(3) G is isoclinic to S_3, and in particular

$$\frac{G}{Z(G)} \cong \frac{S_3}{Z(S_3)} \cong S_3.$$

But (1) is the same as (i), and (3) yields (iii) via Corollary 3.3.5. In case (2), $G' \subseteq Z(G)$, so G is nilpotent and hence it is the direct product of its Sylow subgroups. By necessity the odd order ones are abelian, so is their product A, and the Sylow 2-subgroup P verifies $|P'| = 2$, with $G \times A$.

Conversely, it is obvious that $\Pr(G) = 1 \geq \frac{1}{2}$ in case (i), and that

$$\Pr(G) = \Pr(G_m \times A) = \Pr(G_m)\Pr(A) = \frac{1}{2} \cdot 1 = \frac{1}{2}$$

in case (iii). In case (ii), $|G'| = 2$, therefore each conjugacy class of G has order at most two; but $\Pr(G) = k(G)/|G|$, where $k(G)$ denotes the number of conjugacy classes in G . Let $C_1 = \{1\}, C_2, \cdots, C_{k(G)}$ be the various conjugacy

classes in G. Then

$$|G| = \sum_{i=1}^{k(G)} |C_i| = 1 + \sum_{i=2}^{k(G)} |C_i| \leq 1 + 2(k(G) - 1) = 2k(G) - 1 < 2k(G),$$

therefore

$$\Pr(G) = \frac{k(G)}{|G|} > \frac{1}{2}.$$

□

Remark 3.3.7. Blackburn has enumerated, in [4], all the p-groups whose commutator subgroups have order p.

PROBLEM: Is it possible to classify (upto isomorphiism) all finite groups G for $\Pr(G) \geq \frac{1}{p}$, where p is any odd prime ?

Chapter 4

Supersolvability Conditions Using Commutativity Degree

In this chapter we study some conditions in terms of *commutativity degree* under which a finite group acquires certain special properties expressible in standard group-theoretic terms.

4.1 Prerequisites

In this section we study some group-theoretic results involving supersolvability and some other standard terms.

Lemma 4.1.1. *If G' is cyclic, then G is supersolvable.*

Proof. Let G' be cyclic therefore it is supersolvable. Let

$$\{1\} = A_0 \subseteq A_1 \subseteq A_2 \cdots \subseteq A_k = G'$$

be a normal series in which each factor group is cyclic. Again since G/G' is abelian so is supersolvable. Let

$$\frac{\{1\}}{G'} \subseteq \frac{B_1}{G'} \subseteq \frac{B_2}{G'} \subseteq \cdots \subseteq \frac{B_l}{G'} = \frac{G}{G'}$$

be a normal series such that $\frac{B_{i+1}/G'}{B_i/G'} \cong \frac{B_{i+1}}{B_i}$ is cyclic forall $1 \leq i \leq l$. Where B_i's are normal subgroups of G containing G' (by Correspondence Theorem 1.2.4) also $B_{i+1} \subseteq B_i$. Hence,

$$\{1\} = A_0 \subseteq A_1 \subseteq A_2 \cdots \subseteq A_k = G' \subseteq B_1 \subseteq B_2 \cdots \subseteq B_l = G$$

is a normal series in which every factor is cyclic. Therefore, G is supersolvable. □

Lemma 4.1.2. *G is supersolvable if and only if $\frac{G}{Z(G)}$ supersolvable.*

Proof. By Theorem 1.10.3, it is clear that $\frac{G}{Z(G)}$ supersolvable. Now suppose that $\frac{G}{Z(G)}$ supersolvable. Let

$$\frac{A_0}{Z(G)} \trianglelefteq \frac{A_1}{Z(G)} \cdots \trianglelefteq \frac{A_r}{Z(G)}$$

be a normal series where $A_0 = Z(G)$, $A_r = G$, $\frac{A_i}{Z(G)} \trianglelefteq \frac{G}{Z(G)}$ for $0 \leq i \leq r$ and $\frac{A_{i+1}}{Z(G)}/\frac{A_i}{Z(G)}$ is cyclic for $0 \leq i \leq r-1$.
By the Third Isomorphism Theorem 1.2.3, $\frac{A_{i+1}}{A_i}$ is also cyclic.
Now $Z(G)$ being finite abelian group , is supersolvable, so let

$$\{1\} = B_0 \trianglelefteq B_1 \trianglelefteq \cdots \trianglelefteq B_n = Z(G)$$

be a normal series for $Z(G)$ with $B_i \trianglelefteq Z(G)$, $0 \leq i \leq n$ and $\frac{B_{i+1}}{B_i}$ is cyclic for $0 \leq i \leq n-1$.

It is now clear that

$$\{1\} = B_0 \trianglelefteq B_1 \trianglelefteq \cdots \trianglelefteq B_n = Z(G) \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq G$$

is a normal series for G in which each subgroup is normal in G, because central subgroups are normal and $\frac{A_i}{Z(G)} \trianglelefteq \frac{G}{Z(G)}$ if and only if $A_i \trianglelefteq G$. Moreover, the required factor groups are cyclic, so G is supersolvable. □

Further this lemma can be strengthened to the following

Lemma 4.1.3. *Let $N \trianglelefteq G$ and suppose that N and G/N are both supersolvable. If every normal subgroup of N is normal in G, then G is supersolvable.*

Note that both A_4 and $G(75)$, the unique nonabelian group of order 75 shows that N and G/N, which are both supersolvable, but G is not supersolvable.

Lemma 4.1.4. *If* $\mathrm{Aut}(G)$ *is supersolvable, then G is supersolvable.*

Proof. Since $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ therefore $\mathrm{Inn}(G)$ is supersolvable (by Theorem 1.10.3). Also $\mathrm{Inn}(G) \cong \frac{G}{Z(G)}$. Therefore $\frac{G}{Z(G)}$ is supersolvable so by Lemma 4.1.2, G is supersolvable. □

The quaternion group Q_8 of order 8 shows that the converse of this result is false since Q_8 is supersolvable but $\mathrm{Aut}(Q_8) \cong S_4$ is not supersolvable.
We note that 'supersolvable' in Lemma 4.1.4 can not be replaced by 'CLT' because $S_4 \cong \mathrm{Aut}(A_4)$ is CLT but A_4 is NCLT.
However, it can be shown that $\frac{G}{Z(G)}$ CLT implies G CLT, but again the converse is false, since $A_4 \times C_2$ is CLT but $\frac{A_4 \times C_2}{Z(A_4 \times C_2)} \cong A_4$ is NCLT.

Lemma 4.1.5. *If $\frac{G'}{G' \cap Z(G)}$ is cyclic, then G is supersolvable.*

Proof. We have

$$\left(\frac{G}{Z(G)}\right)' = \frac{G'Z(G)}{Z(G)} \cong \frac{G'}{G' \cap Z(G)}.$$

Since $\frac{G'}{G' \cap Z(G)}$ is cyclic, so is $\left(\frac{G}{Z(G)}\right)'$. Thus by Lemma 4.1.1, $\frac{G}{Z(G)}$ is supersolvable, so by Lemma 4.1.2, G is supersolvable. □

A group G is called *incompetent* if there does not exists any group K such that $G \cong K'$.

Lemma 4.1.6. *If G has a cyclic, characteristic, non-central subgroup, then G is incompetent.*

Proof. See [38]. □

Lemma 4.1.7. *If $G \in \mathcal{G}_p$ and $G' \cong C_p \times C_p$, where p is an odd prime, then G is nilpotent.*

Proof. First of all we show that if for any prime q which divides $|G|$ Sylow q-subgroup $G_q \subseteq C_G(G')$, then $G_q \trianglelefteq G$.
Now $G_q \subseteq C_G(G')$ implies that $G' \subseteq C_G(G_q)$.
Then

$$G' \subseteq C_G(G_q) \subseteq N_G(G_q)$$

implies that $N_G(G_q) \trianglelefteq G$. Now G_q is a Sylow q-subgroup of G, so G_q is a Sylow q-subgroup of $N_G(G_q)$.

The Frattini argument now implies that

$$G = N_G(G_q)N_G(G_q) = N_G(G_q),$$

so $G_q \trianglelefteq G$.

Next, $\frac{N_G(G')}{C_G(G')}$ can be embedded in $\mathrm{Aut}(G')$, which has order $p(p-1)^2(p+1)$. Since p is odd, $(p-1)^2$ and $(p+1)$ are both even and relatively prime to p; also

$$((p-1)^2(p+1), |G|) = 1,$$

since $G \in \mathcal{G}_p$, so $\left|\frac{G}{C_G(G')}\right| = 1$ or p.

If $\left|\frac{G}{C_G(G')}\right| = 1$, $C_G(G') = G$, so $G' \subseteq Z(G)$ and G is nilpotent of class 2.

If $\left|\frac{G}{C_G(G')}\right| = p$, then $G_q \subseteq C_G(G')$ for all primes $q \neq p$, so $G_q \trianglelefteq G$.

Thus every Sylow subgroup of G is normal in G, so G is nilpotent, as claimed. □

Remark 4.1.8. (i) G is in fact isomorphic to $G_p \times A$, where A is an abelian p'-group.

(ii) Lemma 4.1.7 does not necessarily hold for $p = 2$, with A_4 being an obvious counterexample.

Lemma 4.1.9. *Let $|G|$ be odd and suppose that $\frac{1}{|G'|} > \frac{1}{25}(= 0.0400)$. Then G is supersolvable.*

Proof. We have $|G|$ odd and $|G'|$ is an odd number less than 25. If $|G'| = 1$ or a prime number, then G is supersolvable by Lemma 4.1.1. If $|G'| = 15$, again G' is cyclic and we are done. If $|G'| = 9$, then either G' is cyclic or $G' \cong C_3 \times C_3$. Since $|G|$ is odd, $G \in \mathcal{G}_3$ and, by Lemma 4.1.7, G is supersolvable. Finally, if $|G'| = 21$, then either G' is cyclic or G' is the unique nonabelian group of this order. But this group has a cyclic, characteristic, non central subgroup, contradicting Lemma 4.1.6. □

This result is the best one possible because $|G(75)'| = 25$ and $G(75)$ is not supersolvable.

Lemma 4.1.10. *If* $|Z(G)| = 1$, *then* $|G| \leq |G'||\operatorname{Aut}(G')|$. *Moreover, if* $|G' \cap Z(G)| = 1$, *then* $\left|\frac{G}{Z(G)}\right| \leq |G'||\operatorname{Aut}(G')|$.

Proof. We have

$$|G| = \left|\frac{G}{C_G(G')}\right| |C_G(G')|.$$

Since $\left|\frac{G}{C_G(G')}\right| \leq |\operatorname{Aut}(G')|$ (by N/C Theorem 1.6.3) it is sufficient to show that $C_G(G') \leq G'$.

Again by Jacobi identity (1.4.3), we have

$$[C_G(G'), C_G(G')] \leq Z(G) = \{1\}$$

Hence $C_G(G')$ is abelian. Therefore,

$$C_G(G') = P_1 \times P_2 \times \cdots \times P_k$$

where P_i's are Sylow p-subgroups of $C_G(G')$.

Let P be any Sylow p-subgroup of $C_G(G')$. Then $P \trianglelefteq C_G(G')$. Which implies $P \trianglelefteq G$.

Now consider the following cases:

Case 1. $p \nmid |G : G'|$

Assume $P \not\leq G'$. Then there exists some $x \in P$ such that $x \notin G'$. i.e., xG' is non identity in G/G'.

But $o(xG') \mid o(x)$ so $o(xG')$ is a nonzero power p. Which is a contradiction. Hence $P \leq G'$.

Case 2. $p \mid |G : G'|$

Let H/G' be a p-Sylow subgroup of G/G' and Q/G' be its complement then $G = HQ$ and $H \cap Q = G'$. We have H/G' acts on $C_P(Q)$ by the action $\phi(hG', x) = hxh^{-1}$. i.e., $\phi : H/G' \times C_P(Q) \to C_P(Q)$. Then by Fitting lemma (or by [31], 8.4.2), we have

$$P = [P, Q] \times C_P(Q) \tag{4.1.a}$$

Let θ be an orbit of this action. Let $\theta = \text{orb}(x)$ for $x \in C_P(Q)$. Then

$$\theta = \{hxh^{-1} \mid h \in H\}$$

Now

$$|\theta| \mid |H/G'|$$

$$\Rightarrow |\theta| \text{ is a power of} p$$

$$\Rightarrow p \mid |\theta| \text{ if} |\theta| > 1.$$

If $C_P(Q) \neq \{1\}$ then $p \mid |C_P(Q)|$. Also

$$|C_P(Q)| = \sum_{\theta} |\theta| = 1 + \sum_{\substack{\theta \\ \theta \neq \text{orb}(1)}} |\theta|$$

Since $p \mid |C_P(Q)|$ and $p \nmid 1$ so $p \nmid \sum_{\substack{\theta \\ \theta \neq \text{orb}(1)}} |\theta|$ there exists at least one orbit, say $\text{orb}(y)$ such that $y \neq 1$ and $|\text{orb}(y)| = 1$

$$i.e., \ \text{orb}(y) = \{y\},$$

$$i.e., \ \{hyh^{-1} \mid h \in H\} = \{y\},$$

$$i.e., \ hyh^{-1} = y \quad \forall \ h \in H,$$

$$i.e., \ hy = yh \quad \forall \ h \in H.$$

Thus $y \in C_P(H)$ and

$$1 \neq y \in C_P(H) \cap C_P(Q) \subseteq C_P(HQ) = C_P(G) \subset Z(G) = \{1\}.$$

Which is a contradiction. Hence $C_P(Q) = \{1\}$ and so by Equation 4.1.a, we have $P = [P, Q] \leq G'$ and we are done.

For the second part, given $G' \cap Z(G) = \{1\}$ which implies $(G/Z(G))' \cong G'$ and $Z(G/Z(G)) \cong \{1\}$. Hence by the first part, we have

$$\left|\frac{G}{Z(G)}\right| \leq \left|\left(\frac{G}{Z(G)}\right)'\right| |\operatorname{Aut}(G')|$$

which gives the required result. □

4.2 Main Results

In this section we study the main results which provide us with sufficient conditions for a group to be supersolvable or CLT. Here we begin with few lemmas.

Lemma 4.2.1. *If $G' \cong C_2 \times C_2$, then either*

(i) *G is nilpotent or*

(ii) $\Pr(G) = \frac{1}{3}$, *with* $\frac{G}{Z(G)} \cong A_4$ *and* $G' \cap Z(G) = \{1\}$.

Proof. Let $G' \cong C_2 \times C_2$ then since $G' \cap Z(G) \leq G'$ therefore $G' \cap Z(G) \cong C_2 \times C_2$, C_2 or $\{1\}$.

If $G' \cap Z(G) \cong C_2 \times C_2$ then $G' \leq Z(G)$, so G is nilpotent (of class 2).

If $G' \cap Z(G) \cong C_2$, then

$$\left(\frac{G}{Z(G)}\right)' \cong \frac{G'}{G' \cap Z(G)} \cong C_2.$$

By Corollary 1.6.5, $\frac{G}{Z(G)}$ is nilpotent of class 2 so G is nilpotent (of class 3).

Finally, suppose that $G' \cap Z(G) \cong \{1\}$. By Lemma 4.1.10, we have

$$\left|\frac{G}{Z(G)}\right| \leq |G'||\operatorname{Aut}(G')| = 4.6 = 24.$$

Now, since $G' \cap Z(G) \cong \{1\}$, $\frac{G}{Z(G)}$ is non-nilpotent so, by [6], the only possibility is $\frac{G}{Z(G)} \cong A_4$.

Then $\frac{1}{3} = \Pr(A_4) = \Pr(\frac{G}{Z(G)}) = \Pr(G)$, by Corollary 2.5.2 . □

Lemma 4.2.2. *If $G' \cong Q_8$, the quaternion group of order 8, then* $\Pr(G) \leq \frac{1}{3}$

Proof. By a result of Burnside [7], G can not be a 2-group. Now G can not be nilpotent either, because then $G = G_2 \times A$, where A is abelian of odd order, and then $Q_8 \cong G' = {G_2}'$, which is a contradiction.

Now we consider $G' \cap Z(G)$, which is a characteristic abelian subgroup of Q_8. Thus $G' \cap Z(G) \cong C_2$, with $G' \cap Z(G) \cong \{1\}$ being ruled out because Q_8 has a unique involution which is central in G.

Thus

$$\left(\frac{G}{Z(G)}\right)' \cong \frac{G'}{G' \cap Z(G)} \cong C_2 \times C_2$$

By Lemma 4.2.1, either $\frac{G}{Z(G)}$ is nilpotent, which is not possible, or $\Pr(\frac{G}{Z(G)}) = \frac{1}{3}$.

Then $\frac{1}{3} = \Pr(\frac{G}{Z(G)}) \geq \Pr(G)$, as desired, by Corollary 2.5.2. □

Remark 4.2.3. Using a deeper result of Joseph [29], Barry, MacHale and Shé [1] has shown, if $G' \cong Q_8$, then

$$\Pr(G) = \frac{1}{6} + \frac{1}{2^{2s+1}}s \geq 1,$$

so the maximum value that $\Pr(G)$ can have is $\frac{7}{24} < \frac{1}{3}$, is realized when $G \cong SL(2,3)$

Now we are in a position to study the main results of this chapter.

Theorem 4.2.4. *If* $\Pr(G) > \frac{1}{3}(= 0.3333...)$, *then* G *is supersolvable.*

Proof. If G is abelian then G is supersolvable. We may assume that G is non-abelian. Now $\frac{p^2+p-1}{p^3} < \frac{1}{3}$ for $p \geq 5$, so we may assume by second part of Theorem 2.2.3 that $G \in \mathcal{G}_p$ for $p = 2$ or 3.

If $p = 3$, by Corollary 2.2.4 , $|G'| = 3$, so G is supersolvable by Lemma 4.1.1. Thus we may assume that $p = 2$.

By first part of Theorem 2.2.3, we have $\frac{1}{3} < \Pr(G) \geq \frac{1}{4}(1 + \frac{3}{|G'|})$ which means that $|G'| < 9$.

If $G' \cong C_2$, C_3, C_4, C_5, C_6, C_7 or C_8 then by Lemma 4.1.1, G is supersolvable. Thus we are left with the following possibilities for G':

$$C_2 \times C_2,\ S_3,\ D_4,\ C_4 \times C_2,\ Q_8, \text{ and } C_2 \times C_2 \times C_2.$$

If $G' \cong C_2 \times C_2$ then by Lemma 4.2.1, G is nilpotent hence supersolvable.

S_3 and D_4 are eliminated by Lemma 4.1.6; and Q_8 is eliminated by Corollary 2.2.4.

We are left with the cases $G' \cong C_4 \times C_2$ and $C_2 \times C_2 \times C_2$, which we consider in turn.

(i) If $G' \cong C_4 \times C_2$, then

$$G' \cap Z(G) \cong C_4 \times C_2,\ C_4,\ C_2 \times C_2,\ C_2 \text{ or } \{1\}.$$

If $G' \cap Z(G) \cong C_4 \times C_2$, then G is nilpotent of class 2 and hence supersolvable. If $|G' \cap Z(G)| = 4$, then $\left|\frac{G'}{G' \cap Z(G)}\right| = 2$. Therefore,

$$\frac{G'}{G' \cap Z(G)} \cong C_2,$$

so by Lemma 4.1.5, G is supersolvable.

If $G' \cap Z(G) \cong C_2$, then

$$\left(\frac{G}{Z(G)}\right)' \cong \frac{G'}{G' \cap Z(G)}$$

is either cyclic of order 4 or $C_2 \times C_2$. If $\left(\frac{G}{Z(G)}\right)'$ is cyclic, then G is supersolvable by Lemma 4.1.5.

If

$$\left(\frac{G}{Z(G)}\right)' \cong C_2 \times C_2,$$

then by Lemma 4.2.1, $\frac{G}{Z(G)}$ is nilpotent, and we are done, or $\Pr(\frac{G}{Z(G)}) = \frac{1}{3}$. Then by Corollary 2.5.2, we have

$$\frac{1}{3} = \Pr(\frac{G}{Z(G)}) \geq \Pr(G) > \frac{1}{3},$$

which is a contradiction.

The case $G' \cong C_4 \times C_2$ and $G' \cap Z(G) = \{1\}$ does not arise, since $C_4 \times C_2$ has a unique element of order 2 and hence central in G.

(ii) Let $G' \cong C_2 \times C_2 \times C_2$. Then

$$G' \cap Z(G) \cong C_2 \times C_2 \times C_2,\ C_2 \times C_2,\ C_2 \text{ or } \{1\}.$$

If $|G' \cap Z(G)| = 8$, 4 or 2 as in (i), the result follows.

We are left with the case where $G' \cap Z(G) \cong \{1\}$.

Let G be a minimum counterexample to the theorem with $\Pr(G) > \frac{1}{3}$ and G non-supersolvable.

If $Z(G)$ is non-trivial then, $\Pr(\frac{G}{Z(G)}) > \frac{1}{3}$ and $\left|\frac{G}{Z(G)}\right| < |G|$, so $\frac{G}{Z(G)}$ is supersolvable. But by Lemma 4.1.2, G is supersolvable, which is a contradiction.

We may thus assume that $Z(G)$ is trivial, so by Lemma 4.1.10, we have

$$|G| \leq |G'||\operatorname{Aut}(G')| = 8.168 = 1344.$$

But using GAP [49], Barry, MacHale and Shé [1] has found that there are no groups G with the properties:

(i) $G' \cong C_2 \times C_2 \times C_2$

(ii) $Z(G) = \{1\}$

(iii) $\Pr(G) > \frac{1}{3}$

(iv) $|G| \leq 1344$.

This completes the proof. □

Since $\Pr(A_4) = \frac{1}{3}$, the above result is the best one possible.

Theorem 4.2.5. *If* $\Pr(G) > \frac{1}{3}$, *then* G *is CLT.*

Proof. Simply note that Theorem 1.10.3, G is supersolvable and so by Theorem 1.10.5, G is CLT. □

Again, A_4 shows that this result is the best possible.

Theorem 4.2.6. *If $|G|$ is odd and $\Pr(G) > \frac{11}{75}(= 0.1466...)$, then G is supersolvable.*

Proof. Suppose $G \in \mathcal{G}_p$ for $p \geq 11$. Then, by Theorem 2.2.3, we have

$$\Pr(G) \leq \frac{11^2 + 11 - 1}{11^3} = \frac{131}{1331} = 0.09842... < 0.141666... = \frac{11}{75},$$

which is a contradiction.

Thus $G \in \mathcal{G}_p$ for $p = 3, 5$ or 7.

If $p = 7$,

$$\frac{11}{75} < \Pr(G) \leq \frac{1}{49}\left[1 + \frac{48}{|G'|}\right]$$

gives $|G'| < 7.7586...$, so $|G'| = 7$ and G is supersolvable by Lemma 4.1.1.

If $p = 5$,

$$\frac{11}{75} < \Pr(G) \leq \frac{1}{25}\left[1 + \frac{24}{|G'|}\right]$$

gives $|G'| < 9$, so $|G'| = 5$ or 7 and G is supersolvable by Lemma 4.1.1.

Thus, $p = 3$,

$$\frac{11}{75} < \Pr(G) \leq \frac{1}{9}\left[1 + \frac{8}{|G'|}\right].$$

This gives $|G'| < 25$, and the result now follows from Lemma 4.1.9. □

Again, this result is the best possible because $G(75)$ has exactly 11 conjugacy classes and is not supersolvable.

Theorem 4.2.7. *If $|G|$ is odd and $\Pr(G) > \frac{11}{75}$, then G is CLT.*

Proof. Simply note that Theorem 4.2.6, G is supersolvable and so by Theorem 1.10.5, G is CLT. □

The NCLT group $G(75)$ again shows this result is the best one possible. Theorems 4.2.4-4.2.7 can be expressed in the following striking form.

Theorem 4.2.8. (i) *If the average size of a conjugacy class of G is less then 3, then G is both supersolvable and CLT; A_4 shows that this is the best possible result.*

(ii) *If $|G|$ is odd and average size of a conjugacy class of G is less then $6\frac{9}{11}$, then G is both supersolvable and CLT. $G(75)$ shows that this result is the best possible in both cases.*

Chapter 5

Generalized Commutativity Degree

In this chapter we shall study various generalizations of the notion "commutativity degree of finite groups", like 'g-commutativity degree', 'multiple commutativity degree', 'n^{th} nilpotency degree', 'relative commutativity degree, 'relative n^{th} nilpotency degree', 'probability that an automorphism fixes a group element', 'Rewriteability in finite groups' etc. Finally we shall study 'commutativity degree of finite rings'- a concept that is analogous to 'commutativity degree of finite groups'.

5.1 g-commutativity degree

Let G be a finite group and g be an element of G. The *g- commutativity degree*, $\Pr_g(G)$ is the probability that the commutator of two randomly chosen

elements of G is equal to g. More precisely,

$$\Pr_g(G) = \frac{|D_g|}{|G|^2}$$

where $D_g = \{(x, y) \in G \times G \mid [x, y] = g\}$. It is clear that $\Pr_1(G)$ (for $g = 1$) is equal to $\Pr(G)$ the probability that two randomly chosen elements of G commute, and therefore $\Pr_g(G)$ is a generalization of $\Pr(G)$. This generalization is due to M. R. Pournaki and R. Sobhani [41]. In this section we study some formula to compute the g-commutativity degree. Obviously for $g \in G \setminus G'$, we have $\Pr_g(G) = 0$. Therefore we assume that $g \in G'$. Note that there are several examples of groups G in [30] where $\Pr_g(G) = 0$ even when g belongs to G'.

We now start with the following theorem which gives us a character theoratic formula for $\Pr_g(G)$.

Theorem 5.1.1. *Let G be a finite group and let $g \in G'$, then*

$$\Pr_g(G) = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}.$$

Proof. For a given $g \in G'$ consider the set $D_g = \{(x, y) \in G \times G \mid [x, y] = g\}$. Therefore we have $\Pr_g(G) = |D_g|/|G|^2$. On the other hand by Theorem 1.12.29, the number of solutions of the equation $[x, y] = g$ in G, i.e.,

$$|D_g| = |G| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}.$$

Therefore we obtain

$$\Pr_g(G) = \frac{|D_g|}{|G|^2} = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}.$$

This completes the proof. □

Let us note that if we consider $g = 1$ in the above theorem, then we get

$$\Pr_1(G) = \frac{1}{|G|}\sum_{\chi\in \mathrm{Irr}(G)}\frac{\chi(1)}{\chi(1)} = \frac{1}{|G|}\sum_{\chi\in \mathrm{Irr}(G)} 1 = \frac{|\,\mathrm{Irr}(G)|}{|G|} = \frac{k(G)}{|G|}.$$

Since the quantity $\Pr_1(G)$ is the usual commutativity degree $\Pr(G)$, therefore Theorem 5.1.1 is a generalization of the well known result $\Pr(G) = k(G)/|G|$. Let us now compute $\Pr_g(G)$ for finite groups with just two irreducible complex character degrees.

Theorem 5.1.2. *Let G be a finite group such that $\mathrm{cd}(G) = \{1, m\}$, $m > 1$, then*

$$\Pr_g(G) = \begin{cases} \frac{1}{|G'|}\left(1 - \frac{1}{m^2}\right) & \text{if } g \neq 1, \\ \frac{1}{|G'|}\left(1 + \frac{|G'|-1}{m^2}\right) & \text{if } g = 1. \end{cases}$$

Proof. The case $g = 1$ has given in Chapter 2 Theorem 2.3.1. We assume that $g \neq 1$. By Second Orthogonality Relation 1.12.23 for g, we have

$$0 = \sum_{\chi\in \mathrm{Irr}(G)} \chi(g)\chi(1) = \sum_{\substack{\chi\in \mathrm{Irr}(G)\\ \chi(1)=1}} \chi(g)\chi(1) + \sum_{\substack{\chi\in \mathrm{Irr}(G)\\ \chi(1)>1}} \chi(g)\chi(1).$$

In the case that χ is linear, we have $G' \leq \ker\chi$ and therefore $g \in \ker\chi$. Hence $\chi(g) = \chi(1)$. Also the number of all linear irreducible complex characters of G is equal to $|G : G'|$. So

$$\sum_{\substack{\chi\in \mathrm{Irr}(G)\\ \chi(1)=1}} \chi(g)\chi(1) = \sum_{\substack{\chi\in \mathrm{Irr}(G)\\ \chi(1)=1}} \chi(1)^2 = \sum_{\substack{\chi\in \mathrm{Irr}(G)\\ \chi(1)=1}} 1 = |G : G'|.$$

Also by assumption, $\chi(1) = m$ holds for each non-linear irreducible complex character χ of G. Therefore we get

$$\sum_{\substack{\chi\in \mathrm{Irr}(G)\\ \chi(1)>1}} \chi(g)\chi(1) = m\sum_{\substack{\chi\in \mathrm{Irr}(G)\\ \chi(1)>1}} \chi(g).$$

Hence

$$|G : G'| + m \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1)>1}} \chi(g) = 0$$

which implies

$$\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1)>1}} \chi(g) = -\frac{|G : G'|}{m}.$$

By Theorem 5.1.1, we have

$$\begin{aligned}
\mathrm{Pr}_g(G) &= \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \\
&= \frac{1}{|G|} \left(\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1)=1}} \frac{\chi(g)}{\chi(1)} + \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1)>1}} \frac{\chi(g)}{\chi(1)} \right) \\
&= \frac{1}{|G|} \left(\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1)=1}} 1 + \frac{1}{m} \sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1)>1}} \chi(g) \right) \\
&= \frac{1}{|G|} \left(|G : G'| + \frac{1}{m}(-\frac{|G : G'|}{m}) \right) \\
&= \frac{1}{|G'|} \left(1 - \frac{1}{m^2} \right).
\end{aligned}$$

This completes the proof. □

Since $\chi(1) \leq |G : Z(G)|^{1/2} \quad \forall \quad \chi \in \mathrm{Irr}(G)$ we can state the following corollary in view of the above theorem.

Corollary 5.1.3. *Let G be a finite group such that $|\mathrm{cd}(G)| = 2$. If $g \in G'$*

is non-identity then

$$\Pr_g(G) \leq \frac{1}{|G'|}\left(1 - \frac{1}{|G : Z(G)|}\right).$$

The equality holds if and only if G is a group of central type.

Finite groups with just two irreducible complex character degrees are non-abelian, so for such groups G the index of center is greater than or equal to 4. Therefore we can obtain the following corollary.

Corollary 5.1.4. *Let G be a finite group of central type such that $|\operatorname{cd}(G)| = 2$. If $g \in G'$ is non-identity then*

$$\Pr_g(G) \geq \frac{3}{4}\frac{1}{|G'|}.$$

We now study some explicit formulae to compute $\Pr_g(G)$ for groups with $|G'|$ is prime and $G' \leq Z(G)$.

Theorem 5.1.5. *Let G be a finite group such that $|G'| = p$, p prime and let $G' \leq Z(G)$. If $g \in G'$, then*

$$\Pr_g(G) = \begin{cases} \frac{1}{p}\left(1 - \frac{1}{|G:Z(G)|}\right) & \text{if } g \neq 1, \\ \frac{1}{p}\left(1 + \frac{p-1}{|G:Z(G)|}\right) & \text{if } g = 1. \end{cases}$$

Moreover, if $g \in G'$ is non-identity, then $\Pr_g(G) \geq \frac{3}{4p}$. Also $\Pr_1(G) = \frac{1}{4} + \frac{3}{4p}$.

Proof. The case $g = 1$ is same as Proposition 2.3.3 and the result in the other case follows from Theorem 5.1.2 and Corollary 5.1.4. □

Lemma 5.1.6. *Let G and H be two isoclinic finite groups and let (φ, ψ) be an isoclinism from G to H. If $g \in G'$ then*

$$\Pr_g(G) = \Pr_{\psi(g)}(H).$$

Proof. Since (φ, ψ) be an isoclinism from G to H, φ is an isomorphism from $G/Z(G)$ to $H/Z(H)$ and ψ is an isomorphism from G' to H'. Also the following diagram commutes.

$$\begin{array}{ccc} \frac{G}{Z(G)} \times \frac{G}{Z(G)} & \xrightarrow{\varphi \times \varphi} & \frac{H}{Z(H)} \times \frac{H}{Z(H)} \\ \Big\downarrow a_G & & \Big\downarrow a_H \\ G' & \xrightarrow{\psi} & H' \end{array}$$

We have

$$\begin{aligned} \left|\frac{G}{Z(G)}\right|^2 \mathrm{Pr}_g(G) &= \frac{1}{|Z(G)|^2}|G|^2 \mathrm{Pr}_g(G) \\ &= \frac{1}{|Z(G)|^2}|\{(x,y) \in G^2 : [x,y] = g\}| \\ &= \frac{1}{|Z(G)|^2}|\{(x,y) \in G^2 : a_G(xZ(G), yZ(G)) = g\}| \\ &= |\{(\alpha,\beta) \in \left(\frac{G}{Z(G)}\right)^2 : a_G(\alpha,\beta) = g\}|. \end{aligned}$$

Since ψ is an isomorphism, the last quantity is equal to

$$|\{(\alpha,\beta) \in \left(\frac{G}{Z(G)}\right)^2 : \psi(a_G(\alpha,\beta)) = \psi(g)\}|,$$

and the commutativity diagram implies that the above quantity is equal to

$$|\{(\alpha,\beta) \in \left(\frac{G}{Z(G)}\right)^2 : a_H(\varphi(\alpha), \varphi(\beta))) = \psi(g)\}|.$$

But φ is an isomorphism, so we get

$$\begin{aligned}
\left|\frac{G}{Z(G)}\right|^2 \mathrm{Pr}_g(G) &= |\{(\alpha,\beta) \in \left(\frac{G}{Z(G)}\right)^2 : a_H(\varphi(\alpha),\varphi(\beta))) = \psi(g)\}| \\
&= |\{(\gamma,\delta) \in \left(\frac{H}{Z(H)}\right)^2 : a_H(\gamma,\delta) = \psi(g)\}| \\
&= \frac{1}{|Z(H)|^2}|\{(x,y) \in H^2 : a_H(xZ(H), yZ(H)) = \psi(g)\}| \\
&= \frac{1}{|Z(H)|^2}|\{(x,y) \in H^2 : [x,y] = \psi(g)\}| \\
&= \frac{1}{|Z(H)|^2}|H|^2 \mathrm{Pr}_{\psi(g)}(H) \\
&= \left|\frac{H}{Z(H)}\right|^2 \mathrm{Pr}_{\psi(g)}(H).
\end{aligned}$$

But $G/Z(G)$ and $H/Z(H)$ are isomorphic (via φ), hence $\left|\frac{G}{Z(G)}\right| = \left|\frac{H}{Z(H)}\right|$ and the equality $\mathrm{Pr}_g(G) = \mathrm{Pr}_{\psi(g)}(H)$ follows. □

Proposition 5.1.7. *Let G be a finite group such that $|G'| = p$, p prime and let $G' \leq Z(G)$. Suppose that iso.exp$(G) = n$. If $g \in G'$, then*

$$\mathrm{Pr}_g(G) = \begin{cases} \frac{1}{p}\left(1 - \frac{1}{p^{n-1}}\right) & \text{if } g \neq 1, \\ \frac{1}{p}\left(1 + \frac{p-1}{p^{n-1}}\right) & \text{if } g = 1. \end{cases}$$

Proof. Let $H \in \mathbb{ISO}(G)$. Therefore G and H are isoclinic. Let (φ,ψ) be an isoclinism from G to H. By assumption $p^n = |H|$.

Since $G' \leq Z(G)$ and $H \in \mathbb{ISO}(G)$ Lemma 3.2.7 implies that $H' = Z(H)$. Now using Lemma 5.1.6 and Theorem 5.1.5, we have

$$\begin{aligned}\Pr_g(G) &= \Pr_{\psi(g)}(H) \\ &= \begin{cases} \frac{1}{p}\left(1 - \frac{1}{|H:Z(H)|}\right) & \text{if } g \neq 1, \\ \frac{1}{p}\left(1 + \frac{p-1}{|H:Z(H)|}\right) & \text{if } g = 1. \end{cases} \\ &= \begin{cases} \frac{1}{p}\left(1 - \frac{1}{p^{n-1}}\right) & \text{if } g \neq 1, \\ \frac{1}{p}\left(1 + \frac{p-1}{p^{n-1}}\right) & \text{if } g = 1. \end{cases}\end{aligned}$$

This completes the proof. □

Let us turn to the opposite extreme where $|G'|$ is prime and $G' \cap Z(G) = \{1\}$. The following proposition gives a generalization of Proposition 2.5.9 of Chapter 2.

Proposition 5.1.8. *Let n and r be positive integers and let p be a prime number for which $n|(p-1)$ and $r^j \equiv 1 \bmod p$ if and only if $n|j$. Suppose that $G = \langle a, b \,:\, a^p = b^n = 1, bab^{-1} = a^r \rangle$. If $g \in G'$, then*

$$\Pr_g(G) = \begin{cases} \frac{n^2-1}{pn^2} & \text{if } g \neq 1, \\ \frac{n^2+p-1}{pn^2} & \text{if } g = 1. \end{cases}.$$

Proof. It is easy to see that $|G'| = p$ and $\mathrm{cd}(G) = \{1,\ n\}$. Now the assertion holds by Theorem 5.1.2. □

Proposition 2.5.10 of Chapter 2 also can be generalized as the following proposition using the definition of invariant number and Proposition 5.1.8.

Proposition 5.1.9. *Let G be a finite group such that $|G'| = p$, where p a prime, and $G' \cap Z(G) = \{1\}$. Suppose that* $\mathrm{inv}(G) = n$. *If $g \in G'$, then*

$$\mathrm{Pr}_g(G) = \begin{cases} \frac{n^2-1}{pn^2} & \text{if } g \neq 1, \\ \frac{n^2+p-1}{pn^2} & \text{if } g = 1. \end{cases}.$$

Next we study few upper bounds for $\mathrm{Pr}_g(G)$. The following proposition gives us an upper bound for this quantity depending only on the number of conjugacy classes of G.

Proposition 5.1.10. *Let G be a finite group and let $g \in G'$. Then* $\mathrm{Pr}_g(G) \leq \mathrm{Pr}(G)$. *Moreover, the equality holds if and only $g = 1$.*

Proof. By Lemma 1.12.22 (iii), we have $|\chi(g)| \leq \chi(1)$ for each $\chi \in \mathrm{Irr}(G)$. Therefore Theorem 5.1.1 gives

$$\begin{aligned} \mathrm{Pr}_g(G) &= \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \leq \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(g)|}{\chi(1)} \\ &\leq \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} 1 = \frac{|\mathrm{Irr}(G)|}{|G|} = \frac{k(G)}{|G|} = \mathrm{Pr}(G). \end{aligned}$$

It is obvious that the equality holds if and only if $|\chi(g)| = \chi(1)$ for each $\chi \in \mathrm{Irr}(G)$ or equivalently $g = 1$. □

Proposition 5.1.11. *Let G be a finite group and let g be a non-identity element of G'. Then* $\mathrm{Pr}_g(G) < 1/2$.

Proof. Assume that $g \neq 1$. If $\mathrm{Pr}_g(G) \geq 1/2$ then by Proposition 5.1.10, we have

$$\mathrm{Pr}_1(G) = \frac{k(G)}{|G|} > \mathrm{Pr}_g(G) \geq \frac{1}{2}$$

or $\Pr_1(G) > \frac{1}{2}$. Therefore by Corollary 3.3.2, we have $|G| = 2^{2s+1}$, $|G'| = 2$ and $\frac{G}{Z(G)} \cong \mathbb{Z}_2^{2s}$ for some positive integer s. In this case $G' \leq Z(G)$. Therefore by Theorem 5.1.5, we have

$$\Pr_g(G) = \frac{1}{2}\left(1 - \frac{1}{2^{2s}}\right) < \frac{1}{2}$$

which is a contradiction. Therefore $\Pr_g(G) < 1/2$. □

Proposition 5.1.12. *For any $\epsilon \in \mathbb{R}$ with $\epsilon > 0$, there exists a finite group G and $g \in G$ such that $1/2 - \epsilon < \Pr_g(G) < 1/2$.*

Proof. Let s be a positive integer such that $s > -\frac{1}{2}\log_2 2\epsilon$. Consider a finite group of order 2^{2s+1} such that $|G'| = 2$ and $\frac{G}{Z(G)} \cong \mathbb{Z}_2^{2s}$. Let g be an non-identity element of G'. Then $1/2 - \epsilon < \Pr_g(G) < 1/2$, as required. □

Further we can generalize $\Pr_g(G)$ also. Let $H \subseteq G'$ and $D_H = \{(x, y) \in G \times G \mid [x, y] \in H\}$. Then the probability that the commutator of any two group element belonging to H, denoted by $\Pr_H(G)$ is equal to $|D_H|/|G|^2$. i.e.,

$$\Pr_H(G) = \frac{|D_H|}{|G|^2}.$$

Remark 5.1.13. If $H = \{g\}$ then $\Pr_H(G) = \Pr_g(G)$ and if $H = G'$ then $\Pr_{G'}(G) = 1$. Obviously if $H \nsubseteq G'$ then $\Pr_H(G) = 0$.

PROBLEM: To study $\Pr_H(G)$ for any subset H of G' in detail.

5.2 Multiple Commutativity Degree

Let $n \in \mathbb{N} := \mathbb{Z}^+ \cup \{0\}$. The n^{th} *commutativity degree* of a finite group G is defined as

$$\Pr^n(G) = \frac{|C^{(n+1)}(G)|}{|G|^{n+1}}$$

where

$$C^{(n+1)}(G) = \{(x_1, x_2, \cdots, x_{n+1}) \in G^{n+1} \mid x_i x_j = x_j x_i,\ 1 \leq i,\ j \leq n+1\};$$

G^{n+1} being the direct product of $(n+1)$ copies of G.

Clearly, $\Pr^0(G) = 1$ and $\Pr^1(G) = \Pr(G)$.

Lemma 5.2.1. *Let $\{g_1, g_2, \cdots, g_{k(G)}\}$ be a complete set of representatives of the conjugacy classes of a group G, then*

$$\Pr^{n+1}(G) = \frac{1}{|G|}\sum_{i=1}^{k(G)} \frac{1}{|\operatorname{Cl}(g_i)|^n}\Pr^n(C_G(g_i)) \quad \forall n \in \mathbb{N}.$$

Proof. We have

$$\begin{aligned}
&|G|^{n+2}\Pr^{n+1}(G) \\
&= \left|\{(x_1, \cdots x_{n+2}) \in G^{n+2} : x_i x_j = x_j x_i,\ 1 \leq i,\ j \leq n+2\}\right| \\
&= \sum_{x \in G} \left|\{(x_1, \cdots x_{n+1}) \in C_G(x)^{n+1} : x_i x_j = x_j x_i,\ 1 \leq i,\ j \leq n+1\}\right| \\
&= \sum_{x \in G} |C_G(x)|^{n+1}\Pr^n(C_G(x)) \\
&= \sum_{i=1}^{k(G)} |G : C_G(g_i)||G(g_i)|^{n+1}\Pr^n(C_G(g_i)) \\
&= \sum_{i=1}^{k(G)} |\operatorname{Cl}(g_i)| \left(\frac{|G|}{|\operatorname{Cl}(g_i)|}\right)^{n+1} \Pr^n(C_G(g_i))
\end{aligned}$$

$$= |G|^{n+1} \sum_{i=1}^{k(G)} \frac{1}{|\operatorname{Cl}(g_i)|^n} \Pr^n(C_G(g_i)).$$

Hence, the lemma follows. □

Lemma 5.2.2. *Let G and H are two isoclinic groups, then*

$$\Pr^n(G) = \Pr^n(H) \quad \forall n \in \mathbb{N}.$$

Proof. The argument is exactly parallel to the argument given in the proof of Lemma 3.2.5. □

Theorem 5.2.3. *Let G be a non-abelian group, then*

$$\Pr^n(G) \leq \frac{3 \cdot 2^n - 1}{2^{2n+1}} \quad \forall n \in \mathbb{N}.$$

Moreover, equality holds if and only if G is isoclinic to Q_8.

Proof. We use induction on n. For $n = 0$ the inequality is obvious since $\Pr^0(G) = 1$. Let us assume $\Pr^n(G) \leq (3 \cdot 2^n - 1)/2^{2n+1}$ and then using Lemma 5.2.1, choosing the g_i in such a way that $Z(G) = \{g_1, \cdots, g_{|Z(G)|}\}$. We get

$$\begin{aligned}
\Pr^{n+1}(G) &= \frac{1}{|G|} \sum_{i=1}^{k(G)} \frac{1}{|\operatorname{Cl}(g_i)|^n} \Pr^n(C_G(g_i)) \\
&= \frac{|Z(G)|}{|G|} \Pr^n(G) + \frac{1}{|G|} \sum_{i=|Z(G)|+1}^{k(G)} \frac{1}{|\operatorname{Cl}(g_i)|^n} \Pr^n(C_G(g_i)) \\
&\leq \frac{1}{|G : Z(G)|} \frac{3 \cdot 2^n - 1}{2^{2n+1}} + \frac{1}{|G|} \frac{1}{2^n} (k(G) - |Z(G)|).
\end{aligned}$$

But $k(G) = |G| \Pr(G) \leq \frac{5}{8}|G|$ and $|G : Z(G)| \geq 4$ because $G/Z(G)$ is not cyclic. Therefore

$$\begin{aligned}
\Pr^{n+1}(G) &\leq \frac{1}{|G : Z(G)|}\frac{3 \cdot 2^n - 1}{2^{2n+1}} + \frac{1}{2^n}\left(\frac{5}{8} - \frac{1}{|G : Z(G)|}\right) \\
&= \frac{5}{8 \cdot 2^n} + \frac{1}{|G : Z(G)|}\frac{1}{2^{2n+3}}(3 \cdot 2^{n+2} - 4 - 2^{n+3}) \\
&= \frac{5}{2^{n+3}} + \frac{2^{n+2} - 4}{2^{2n+3}|G : Z(G)|} \\
&\leq \frac{5}{2^{n+3}} + \frac{2^{n+2} - 4}{4 \cdot 2^{2n+3}} \\
&= \frac{5 \cdot 2^n + 2^n - 1}{2^{2n+3}} \\
&= \frac{3 \cdot 2^{n+1} - 1}{2^{2(n+1)+1}}
\end{aligned}$$

and the inequality is proved at rank $n + 1$. This computation also makes clear that, for a given $n \geq 1$, equality at rank $n + 1$ implies equality at rank n. Therefore, if, for a given $n \geq 1$,

$$\Pr^n(G) = \frac{3 \cdot 2^n - 1}{2^{2n+1}},$$

then $\Pr(G) = \Pr^1(G) = \frac{5}{8}$. Therefore, by Corollary 3.3.2, G is isoclinic to an extraspecial group of order 2^{2n+1}, where $\frac{1}{2}(1 + 1/4^m) = \frac{5}{8}$, that is $m = 1$. G is therefore isoclinic to either the dihedral group of order 8 D_4, or to the quaternion group Q_8. But these two group are isoclinic, hence G is isoclinic to Q_8 in any case.

Conversely, if G is isoclinic to Q_8, one may assume that $G = Q_8$ since $\Pr(G) = \Pr(Q_8)$. Then $|G; Z(G)| = 4$, $\Pr^0(G) = 1$, and $C_G(x)$ is abelian and of index 2 for all $x \in G \setminus Z(G)$; therefore, in the previous computation,

equality holds all along, which permits us to prove by induction on n that

$$\Pr^n(Q_8) = \frac{3 \cdot 2^n - 1}{2^{2n+1}} \quad \forall n \in \mathbb{N}.$$

□

As in Section 5.1, let us consider a group G and an element $g \in G$. Define

$$\Pr_g^n(G) = \frac{|D_g^{(n)}|}{|G|^{n+1}}$$

where $D_g^{(n)} = \{(x_1, \cdots, x_{n+1}) \in G^{n+1} \mid [x_i, x_j] = g, 1 \leq i, j \leq n+1\}$.

PROBLEM: To study $\Pr_g^n(G)$ in detail.

Similarly for any subset H of G' we can define $\Pr_H^n(G)$ as

$$\Pr_H^n(G) = \frac{|D_H^{(n)}|}{|G|^{n+1}}$$

where $D_H^{(n)} = \{(x_1, \cdots, x_{n+1}) \in G^{n+1} \mid [x_i, x_j] \in H, 1 \leq i, j \leq n+1\}$.

PROBLEM: To study $\Pr_H^n(G)$ in detail.

5.3 n^{th} Nilpotency Degree

For $n \geq 1$, let us define

$$\Pr^{(n)}(G) = \frac{|\{(x_1, x_2, \cdots, x_{n+1}) \in G^{n+1} | [x_1, x_2, \cdots, x_{n+1}] = 1\}|}{|G|^{n+1}}.$$

It is a natural generalization of $\Pr(G)$ and called the n^{th} *nilpotency degree.* Clearly, $\Pr^{(1)}(G) = \Pr(G)$. It is also easy to see that

$$\begin{aligned}\Pr^{(n)}(G) &= \frac{1}{|G|^{n+1}} \sum_{x_1 \in G} \cdots \sum_{x_n \in G} |C_G([x_1, x_2, \cdots, x_{n+1}])| \\ &= \frac{1}{|G|^n} \sum_{x_1 \in G} \cdots \sum_{x_n \in G} \frac{|C_G([x_1, x_2, \cdots, x_{n+1}])|}{|G|}\end{aligned}$$

Some results on n^{th} nilpotency degree are available in [40]. We state the following theorem without proof. The proof can be found in [40].

Theorem 5.3.1. *If G is a finite NC-group, then*

$$\Pr^{(n+1)}(G) = \frac{1}{|G|}\sum_{g\in G} \Pr^{(n)}\left(\frac{G}{C_G(g)}\right).$$

Note 5.3.2. By a NC-group we mean a finite group in which the centralizer of each element is a normal subgroup. It follows from the main result of Levi [35] that such a group is nilpotent of class at most 3.

Remark 5.3.3. It is obvious that

$$\Pr^{(n)}(G) \leq \Pr^{(n+1)}(G) \text{ for all } n \geq 1.$$

Now as a consequence of Theorem 5.3.1, we have the following theorem.

Theorem 5.3.4. *Let G be a finite NC-group and N be a normal subgroup of G , then*

$$\Pr^{(n)}(G) \leq \Pr^{(n)}\left(\frac{G}{N}\right)\Pr^{(n)}(N)$$

and the equality holds if $N \cap \gamma_{n+1}(G) = \{1\}$.

As mentioned earlier, if G is a NC-group, then G is nilpotent of class at most 3. So, Theorem 5.3.1 and 5.3.4 trivially hold for such groups. So, they have a limited scope. Let us study some upper bounds for $\Pr^{(n)}(G)$ available in [13], without any strong condition like NC-group.

Theorem 5.3.5. *Let G be a group. Then for every $n \geq 1$,*

$$\Pr^{(n+1)}(G) \leq \frac{1}{2}\left(1 + \Pr^{(n)}\left(\frac{G}{Z(G)}\right)\right).$$

Proof. We have

$$\begin{aligned}
|G|^{n+2}\Pr^{(n+1)}(G) &= |\{(x_1, x_2, \cdots, x_{n+1}, x_{n+2}) \in G^{n+2} | [x_1, x_2, \cdots, x_{n+2}] = 1\}| \\
&= \sum_{x_1 \in G} \cdots \sum_{x_{n+1} \in G} |C_G([x_1, x_2, \cdots, x_{n+1}])| \\
&= \sum_{x_1 \in G} \cdots \sum_{x_{n+1} \in G} \sum_{[x_1, x_2, \cdots, x_{n+1}] \in Z(G)} |C_G([x_1, x_2, \cdots, x_{n+1}])| \\
&\quad + \sum_{x_1 \in G} \cdots \sum_{x_{n+1} \in G} \sum_{[x_1, x_2, \cdots, x_{n+1}] \notin Z(G)} |C_G([x_1, x_2, \cdots, x_{n+1}])| \\
&\leq |G|^{n+1}\Pr^{(n)}\left(\frac{G}{Z(G)}\right)|G| \\
&\quad + \left(|G|^{n+1} - |G|^{n+1}\Pr^{(n)}\left(\frac{G}{Z(G)}\right)\right)\frac{|G|}{2} \\
&= \frac{|G|^{n+2}}{2}\left(1 + \Pr^{(n)}\left(\frac{G}{Z(G)}\right)\right).
\end{aligned}$$

from which the result follows. □

Theorem 5.3.6. *Let G be a finite group. Then for every $n \geq 1$,*

$$\Pr^{(n+1)}(G) \leq \frac{1}{2^n}\left(2^n - 1 + \Pr\left(\frac{G}{Z_n(G)}\right)\right).$$

Proof. We may proceed by induction on n. If $n = 1$, then the proof is clear by Theorem 5.3.5. Now, suppose that the theorem is true for n. To prove it for $n + 1$, we remark that

$$Z_{n-1}\left(\frac{G}{Z(G)}\right) = \frac{Z_n(G)}{Z(G)}.$$

So, by the induction hypothesis we see that

$$\begin{aligned}
\Pr^{(n)}\left(\frac{G}{Z(G)}\right) &\leq \frac{1}{2^{n-1}}\left(2^{n-1} - 1 + \Pr\left(\frac{G/Z(G)}{Z_{n-1}(G/Z(G))}\right)\right) \\
&= \frac{1}{2^{n-1}}\left(2^{n-1} - 1 + \Pr\left(\frac{G}{Z_n(G)}\right)\right).
\end{aligned}$$

Therefore, by Theorem 5.3.5, we have

$$\begin{aligned}\Pr^{(n+1)}(G) &\leq \frac{1}{2}\left(1+\frac{1}{2^{n-1}}\left(2^{n-1}-1+\Pr\left(\frac{G}{Z_n(G)}\right)\right)\right)\\ &= \frac{1}{2^n}\left(2^n-1+\Pr\left(\frac{G}{Z_n(G)}\right)\right).\end{aligned}$$

□

Theorem 5.3.7. *Let G be a finite group which is not nilpotent of class at most n. Then*

$$\Pr^{(n)}(G) \leq \frac{2^{n+2}-3}{2^{n+2}}.$$

Proof. Since G is not nilpotent of class n, $G/(Z_{n-1}(G))$ cannot be abelian. Thus $\Pr(G/(Z_{n-1}(G))) \leq 5/8$ by Proposition 2.2.1 and using Theorem 5.3.6, we have

$$\Pr^{(n)}(G) \leq \frac{1}{2^{n-1}}\left(2^{n-1}-1+\frac{5}{8}\right) = \frac{2^{n+2}-3}{2^{n+2}}.$$

as required. □

Example 5.3.8. Let G be the dihedral group of order 2^{n+2}, i.e.,

$$G = D_{2^{n+2}} = \langle a, b \mid a^{2^{n+1}} = b^2 = 1, bab = a^{-1}\rangle.$$

Then we have $Z(D_{2^{n+2}}) = \langle a^{2^n}\rangle = \{1, a^{2^n}\}$ and $\gamma_n(G) = \langle a^{2^{n-1}}\rangle = \{1, a^{2^{n-1}}, a^{2^n}, a^{3(2^{n-1})}\}$. Thus, we can see that if $[x_1, x_2, \cdots, x_n] \notin Z(G)$, then $[x_1, x_2, \cdots, x_n] = a^{2^{n-1}}$ or $a^{3(2^{n-1})}$ and so $|C_G([x_1, x_2, \cdots, x_n])| = |G|/2$ in this case. Hence we have, by induction over n:

$$\Pr^{(n)}(G) = \frac{1}{2}\left(1+\Pr^{(n-1)}\left(\frac{G}{Z(G)}\right)\right) = \frac{2^{n+2}-3}{2^{n+2}}.$$

This example confirms that the bound given in Theorem 5.3.7 is the best possible. Also the following theorem gives a better upper bound than Theorem 5.3.7, if $Z(G) = \{1\}$.

Theorem 5.3.9. *Let G be a finite group with $G \neq 1$ and $Z(G) = \{1\}$. Then for every $n \geq 1$*

$$\Pr^{(n)}(G) \leq \frac{2^n - 1}{2^n}.$$

Proof. Since $Z(G) = \{1\}$, so $Z_n(G) = \{1\}$ for all $n \geq 1$. Thus G is not nilpotent and therefore $\Pr(G) \leq 1/2$, by second consequence of Corollary 3.3.2. Hence the proof follows from Theorem 5.3.6 by induction on n. □

Note that $\Pr^{(n)}(G)$ can be further generalized to

$$\Pr_g^{(n)}(G) = \frac{|\{(x_1, x_2, \cdots, x_{n+1}) \in G^{n+1} | [x_1, x_2, \cdots, x_{n+1}] = g\}|}{|G|^{n+1}}.$$

for $n \geq 1$ where $g \in G$.

and

$$\Pr_H^{(n)}(G) = \frac{|\{(x_1, x_2, \cdots, x_{n+1}) \in G^{n+1} | [x_1, x_2, \cdots, x_{n+1}] \in H\}|}{|G|^{n+1}}.$$

for $n \geq 1$ where $H \leq G$.

PROBLEM: To study $\Pr_g^{(n)}(G)$ and $\Pr_H^{(n)}(G)$ in detail.

5.4 Relative Commutativity Degree

In this section, we study some properties of the relative commutativity degree of a subgroup H in a given group G [13].

Definition 5.4.1. The *relative commutativity degree* of the subgroup H in the group G, which is denoted by $\Pr(H,G)$, is by definition the ratio

$$\Pr(H,G) = \frac{|\{(x,y) \in H \times G : xy = yx\}|}{|H||G|}.$$

It is clear that if $H = G$, then $\Pr(H,G) = \Pr(G)$ and if G is abelian, then $\Pr(H,G) = 1$ as well. Let us restate Lemma 2.1.2 (i) which plays an important role in the comparison of $\Pr(H,G)$ with $\Pr(G)$ and $\Pr(H)$.

Lemma 5.4.2. *Let H be a subgroup of G. Then*

$$|H : C_H(x)| \leq |G : C_G(x)| \text{ for all } x \in G.$$

Theorem 5.4.3. *Let H be a subgroup of G. Then*

$$\Pr(G) \leq \Pr(H,G) \leq \Pr(H).$$

Proof. We have

$$\begin{aligned}\Pr(H,G) &= \frac{1}{|H||G|}\sum_{x\in G} |\{y \in H : y \in C_G(x)\}| \\ &= \frac{1}{|H||G|}\sum_{x\in G} |C_H(x)| \geq \frac{1}{|G|^2}\sum_{x\in G} |C_G(x)| = \Pr(G)\end{aligned}$$

by Lemma 5.4.2. Similarly,

$$\begin{aligned}\Pr(H,G) &= \frac{1}{|H||G|}\sum_{y\in H} |\{x \in G : x \in C_G(y)\}| \\ &= \frac{1}{|H||G|}\sum_{y\in H} |C_G(y)| \leq \frac{1}{|H|^2}\sum_{y\in H} |C_H(y)| = \Pr(H)\end{aligned}$$

as required. □

It also follows from the above computation that $\Pr(H,G) = \Pr(H)$ if and only if

$$G = HC_G(x) \quad \forall x \in H \tag{5.4.a}$$

From (5.4.a), one can see that $\Pr(H,G) = \Pr(H)$ implies $H \trianglelefteq G$, and when H is abelian, that $H \subseteq Z(G)$. It also follows from the above reasoning that $\Pr(H,G) = \Pr(G)$ if and only if

$$G = HC_G(x) \quad \forall x \in G \tag{5.4.b}$$

But (5.4.b) implies (5.4.a), i.e.,$\Pr(H,G) = \Pr(G)$ implies $\Pr(H,G) = \Pr(H)$ (hence $\Pr(G) = \Pr(H)$). However, the converse is not true, e.g., if G is non-abelian and $H \subseteq Z(G)$, then $1 = \Pr(H) = \Pr(H,G) > \Pr(G)$. For example, if $G = D_4 = \langle a, b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle$ and $H = Z(D_4) = \langle a^2 \rangle$, then we have $\Pr(G) = 5/8$ and $\Pr(H,G) = \Pr(H) = 1$. Also, one may see that if $H \subseteq Z(G)$, then $\Pr(H,G) = \Pr(H) = 1$ and if $HZ(G) = G$, then $\Pr(G) = \Pr(H,G) = \Pr(H)$. The following lemma gives a sufficient condition for the above inequality to be strict.

Lemma 5.4.4. *Let H be a subgroup of G which is not normal. Then*

$$\Pr(G) < \Pr(H,G) < \Pr(H).$$

Proof. The result is implicit in the above discussions concerning conditions (5.4.a) and (5.4.b). □

The converse of Lemma 5.4.4 is not true. For instant, if $G = S_4$ and $H = A_4$, then we have

$$\Pr(G) = \frac{5}{24} < \Pr(H,G) = \frac{1}{4} < \Pr(H) = \frac{1}{3}.$$

Now we are able to give better upper and lower bounds for $\Pr(G)$ and $\Pr(H,G)$.

Theorem 5.4.5. *Let H be a subgroup of G and p be the smallest prime number dividing $|G|$. Then*

(i) $\dfrac{|Z(G)|}{|G|} + \dfrac{p(|G| - |Z(G)|)}{|G|^2} \leq \Pr(G) \leq \dfrac{|Z(G)| + |G|}{2|G|}$;

(ii) $\dfrac{|Z(G) \cap H|}{|H|} + \dfrac{p(|H| - |Z(G) \cap H|)}{|H||G|} \leq \Pr(H,G) \leq \dfrac{|Z(G) \cap H| + |H|}{2|H|}$.

Proof. (i) We have

$$\begin{aligned} |G|^2 \Pr(G) &= \sum_{x \in G} |C_G(x)| \\ &= \sum_{x \in Z(G)} |C_G(x)| + \sum_{x \in G - Z(G)} |C_G(x)| \\ &= |Z(G)||G| + \sum_{x \in G - Z(G)} |C_G(x)|. \end{aligned}$$

It is easy to see that if x is not in the center of G, then $p \leq |C_G(x)| \leq \frac{|G|}{2}$. So,

$$p(|G| - |Z(G)|) \leq \sum_{x \in G - Z(G)} |C_G(x)| \leq (|G| - |Z(G)|)\frac{|G|}{2}.$$

Hence

$$|Z(G)||G| + p(|G| - |Z(G)|) \leq |G|^2 \Pr(G) \leq |Z(G)||G| + (|G| - |Z(G)|)\frac{|G|}{2},$$

and so

$$\frac{|Z(G)|}{|G|} + \frac{p(|G| - |Z(G)|)}{|G|^2} \leq \Pr(G) \leq \frac{|Z(G)| + |G|}{2|G|}.$$

(ii) Set $K = Z(G) \cap H$. Then we have

$$|G||H| \Pr(H,G) = \sum_{x \in H} |C_G(x)| = \sum_{x \in K} |C_G(x)| + \sum_{x \in H-K} |C_G(x)|$$
$$= |K||G| + \sum_{x \in H-K} |C_G(x)|.$$

The rest of the proof is similar to the proof of part (i). □

We can see that equality may be attained in Theorem 5.4.5. For example, suppose that $H = Z(G)$, then we have

$$1 = \Pr(H,G) = \frac{|H| + |H|}{2|H|}.$$

The following theorem is a consequence of Theorem 5.4.5, and gives some upper bounds for $\Pr(H,G)$.

Theorem 5.4.6. *Let G be a non-abelian group and H be a subgroup. Then*

(i) $\Pr(H,G) = 1$ *if* $H \subseteq Z(G)$,

(ii) $\Pr(H,G) \leq \frac{3}{4}$ *if* $H \not\subseteq Z(G)$; *in fact* $\Pr(H,G) \leq \frac{5}{8}$ *if H is non-abelian.*

Proof. (i) Follows immediately from the definition of $\Pr(H,G)$.

(ii) Since $H \not\subseteq Z(G)$, $Z(G) \cap H \subsetneq H$ and so $|Z(G) \cap H| \leq \frac{1}{2}|H|$. The first inequality now follows from Theorem 5.4.5(ii). The second inequality follows from Theorem 5.4.3, noting that $\Pr(H) \leq 5/8$ if H is non-abelian.

□

The above bounds are in general the best. For, if $G = D_4 = \langle a, b \mid a^4 = b^2 = 1, (ab)^2 = 1\rangle$ and $H = \langle a\rangle$ then $\Pr(H, G) = 3/4$. Moreover, if $G = D_4 \times \mathbb{Z}_2$ and $H = D_4 \times \{1\}$, then $\Pr(H, G) = 5/8$. Note that, by (5.4.a), $\Pr(G \times \{1\}, G \times A) = \Pr(G)$ for any two groups G and A.

Theorem 5.4.7. *Let $H_1 \leq H_2 \leq G$. Then*

$$\Pr(H_1, H_2) \geq \Pr(H_1, G) \geq \Pr(H_2, G).$$

Proof. Since $H_1 \leq H_2 \leq G$, by Lemma 5.4.2 we have

$$|H_1 : C_{H_1}(x)| \leq |H_2 : C_{H_2}(x)| \leq |G : C_G(x)|,$$

for all $x \in G$. Thus

$$\begin{aligned}\Pr(H_1, H_2) &= \frac{1}{|H_1||H_2|}\sum_{x\in H_1} |C_{H_2}(x)| = \frac{1}{|H_1|}\sum_{x\in H_1}\frac{|C_{H_2}(x)|}{|H_2|} \\ &\geq \frac{1}{|H_1|}\sum_{x\in H_1}\frac{|C_G(x)|}{|G|} = \frac{1}{|H_1||G|}\sum_{x\in H_1}|C_G(x)| = \Pr(H_1, G).\end{aligned}$$

Similarly, we can prove that $\Pr(H_1, G) \geq \Pr(H_2, G)$. □

The following lemma plays a crucial role in the proof of Theorem 5.4.9.

Lemma 5.4.8. *Let H and N be two subgroups of G such that $N \leq H$ and $N \trianglelefteq G$. Then*

$$\frac{C_H(x)N}{N} \leq C_{H/N}(Nx), \text{ for all } x \in G.$$

Moreover, the equality holds if $N \cap [H, G] = \{1\}$.

Proof. Assume that $y \in C_H(x)$. Then we have

$$NxNy = N(xy) = N(yx) = NyNx \quad \text{or} \quad Ny \in C_{H/N}(Nx)$$

and this implies that

$$\frac{C_H(x)N}{N} \leq C_{H/N}(Nx).$$

Now if $N \cap [H,G] = \{1\}$, then for every $Ny \in C_{H/N}(Nx)$ we have $xyx^{-1}y^{-1} \in N \cap [H,G] = 1$. Therefore, $y \in C_H(x)$ and so $Ny \in (C_H(x))N/N$. □

Theorem 5.4.9. *Let H and N be two subgroups of G such that $N \trianglelefteq G$ and $N \leq H$. Then*

$$\Pr(H,G) \leq \Pr\left(\frac{H}{N}, \frac{G}{N}\right) \Pr(N).$$

If $N \cap [H,G] = \{1\}$, then the equality holds.

Proof. We have

$$\begin{aligned}
|H||G| \Pr(H,G) &= |\{(x,y) \in H \times G \mid xy = yx\}| \\
&= \sum_{y \in G} |C_H(y)| = \sum_{S \in G/N} \sum_{y \in S} \frac{|C_H(y)|}{|N \cap C_H(y)|} |C_N(y)| \\
&= \sum_{S \in G/N} \sum_{y \in S} \frac{|C_H(y)N|}{|N|} |C_N(y)| \\
&\leq \sum_{S \in G/N} \sum_{y \in S} |C_{H/N}(Ny)||C_N(y)| \quad \text{(by Lemma 5.4.8)} \\
&= \sum_{S \in G/N} |C_{H/N}(S)| \sum_{y \in S} |C_N(y)| \\
&= \sum_{S \in G/N} |C_{H/N}(S)| \sum_{y \in S} |\{x \in N \mid xy = yx\}| \\
&= \sum_{S \in G/N} |C_{H/N}(S)| \sum_{x \in N} |C_G(x) \cap S|.
\end{aligned}$$

If $C_G(x) \cap S \neq \phi$, then $S = Nx_0$ where $x_0 \in C_G(x) \cap S$. Therefore,

$$S \cap C_G(x) = Nx_0 \cap C_G(x) = Nx_0 \cap C_G(x)x_0 = (N \cap C_G(x))x_0 = C_N(x)x_0,$$

and so $|S \cap C_G(x)| = |C_N(x)x_0| = |C_N(x)|$. On the other hand if $C_G(x) \cap S = \phi$, then $|C_G(x) \cap S| < |C_N(x)|$. So, in either case,

$$|C_G(x) \cap S| \leq |C_N(x)|$$

Therefore,

$$\begin{aligned} |H||G| \Pr(H,G) &\leq \sum_{S \in G/N} |C_{H/N}(S)| \sum_{x \in N} |C_N(x)| \\ &= \left|\frac{H}{N}\right| \left|\frac{G}{N}\right| \Pr\left(\frac{H}{N}, \frac{G}{N}\right) |N|^2 \Pr(N). \end{aligned}$$

Hence

$$\Pr(H,G) \leq \Pr\left(\frac{H}{N}, \frac{G}{N}\right) \Pr(N).$$

Now, if $N \cap [H,G] = \{1\}$, then by Lemma 5.4.8

$$\frac{C_H(y)N}{N} \leq C_{H/N}(Ny) \quad \text{for all } y \in G.$$

Also $C_G(x) \cap S \neq \phi$ for all $x \in N$ and for all $S \in G/N$. Thus, all the inequalities may be changed into equalities. Hence

$$\Pr(H,G) = \Pr\left(\frac{H}{N}, \frac{G}{N}\right).$$

This completes the proof. □

Theorem 5.4.10. *Let H be a subgroup of G. Then*

(i) $H/(Z(G) \cap H) \cong \mathbb{Z}_2$ *if* $\Pr(H,G) = \frac{3}{4}$,

(ii) $H/(Z(G) \cap H) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ *if* $\Pr(H,G) = \frac{5}{8}$ *and H is non-abelian.*

Proof. (i) Suppose that $\Pr(H,G) = \frac{3}{4}$, then by Theorem 5.4.5(ii), $\Pr(H,G) \leq (|Z(G) \cap H| + |H|)/2|H|$. Thus we have

$$\frac{3}{4} \leq \frac{|Z(G) \cap H| + |H|}{2|H|} \quad \text{and so} \quad \frac{|H|}{|Z(G) \cap H|} \leq 2.$$

If $|H|/(|Z(G) \cap H|) = 1$, then we have $H \subseteq Z(G)$, whence $\Pr(H,G) = 1$, a contradiction. Therefore,$|H|/(|Z(G) \cap H|) = 2$. Hence

$$\frac{H}{Z(G) \cap H} \cong \mathbb{Z}_2.$$

(ii) Suppose that $\Pr(H,G) = \frac{5}{8}$, then

$$\frac{5}{8} \leq \frac{|Z(G) \cap H| + |H|}{2|H|} \quad \text{and so} \quad \frac{|H|}{|Z(G) \cap H|} \leq 4.$$

Since H is not abelian, $H/(Z(G) \cap H)$ is not cyclic. Therefore, we have

$$\frac{H}{Z(G) \cap H} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

and the proof of the theorem is completed. □

Note that the second part of Proposition 2.2.1 also follows by taking $H = G$ in part (ii) above.

Proposition 5.4.11. *Let* $G = D_{2n} = \langle a, b \mid a^n = b^2 = (ab)^2 = 1 \rangle$ *and* $H = \langle a \rangle$. *Then*

$$\Pr(H,G) = \begin{cases} \frac{n+2}{2n} & n \text{ even}, \\ \frac{n+1}{2n} & n \text{ odd}. \end{cases}$$

Proof. We know that

$$\begin{aligned} \Pr(H,G) &= \frac{1}{|H||G|} \sum_{x \in H} |C_G(x)| \\ &= \frac{1}{|H||G|} \left(\sum_{x \in H \cap Z(G)} |C_G(x)| + \sum_{x \in H - H \cap Z(G)} |C_G(x)| \right). \end{aligned}$$

If $x \in H \cap Z(G)$ then $|C_G(x)| = |G|$, and if $x \in (H - H \cap Z(G))$ then $|C_G(x)| = |G|/2$. Now, assume that n is even. Then $|Z(G) \cap H| = 2$, and we have

$$\begin{aligned}\Pr(H,G) &= \frac{1}{|H||G|}\left(|G||Z(G)\cap H| + \frac{|G|}{2}(|H| - |Z(G)\cap H|)\right) \\ &= \frac{|H| + |Z(G)\cap H|}{2|H|} = \frac{n+2}{2n}.\end{aligned}$$

If n is odd then $|Z(G)\cap H| = 1$, and so $\Pr(H,G) = (n+1)/2n$, as above. □

Similarly we have

Proposition 5.4.12. *Let* $G = Q_{2^n} = \langle a, b \mid a^{2^{n-1}} = 1,\ a^{2^{n-2}} = b^2,\ b^{-1}ab = a^{-1}\rangle$ *and* $H = \langle a\rangle$. *Then* $\Pr(H,G) = (2^{n-1} + 2)/2^n$ *for all positive integers* n.

It may be mentioned here that $\Pr(H,G)$ can be further generalized to

$$\Pr_g(H,G) = \frac{|\{(x,y) \in H \times G : [x,y] = g\}|}{|H||G|}.$$

where $g \in G$ and

$$\Pr_K(H,G) = \frac{|\{(x,y) \in H \times G : [x,y] \in K\}|}{|H||G|}.$$

where K is a subgroup of G'.

PROBLEM: To study $\Pr_g(H,G)$ and $\Pr_K(H,G)$ in detail.

5.5 Relative n^{th} Nilpotency Degree

In this section we study a generalization of $\Pr(H,G)$ called the relative n^{th} nilpotency degree. We start with the following definition.

Definition 5.5.1. Let H be a subgroup of G. The *relative* n^{th} *nilpotency degree* of H in G, which is denoted by $\Pr^{(n)}(H,G)$, is defined to be the ratio

$$\Pr^{(n)}(H,G) = \frac{|\{(x_1, x_2, \cdots, x_n, y) \in H^n \times G \,|[x_1, x_2, \cdots, x_n, y] = 1\}|}{|H|^n|G|}.$$

It is clear that $\Pr^{(1)}(H,G) = \Pr(H,G)$ and if $H = G$ then $\Pr^{(n)}(H,G) = \Pr^{(n)}(G)$.

Lemma 5.5.2. *Let H be a subgroup of G then*

$$\Pr^{(n)}(H,G) \leq \Pr^n(G) \quad \textit{for all } n \geq 1.$$

Proof. We have

$$\begin{aligned}
\Pr^{(n)}(H,G) &= \frac{1}{|H|^n|G|} \sum_{x_1 \in H} \cdots \sum_{x_n \in H} |C_G([x_1, x_2, \cdots, x_n])| \\
&= \frac{1}{|H|^n} \sum_{x_1 \in H} \cdots \sum_{x_n \in H} \frac{|C_G([x_1, x_2, \cdots, x_n])|}{|G|} \\
&\leq \frac{1}{|H|^n} \sum_{x_1 \in H} \cdots \sum_{x_n \in H} \frac{|C_H([x_1, x_2, \cdots, x_n])|}{|H|} \\
&= \frac{1}{|H|^{n+1}} \sum_{x_1 \in H} \cdots \sum_{x_n \in H} |C_H([x_1, x_2, \cdots, x_n])| \\
&= \Pr^{(n)}(H).
\end{aligned}$$

□

It may be noted here that the sequence $\{\Pr^{(n)}(H,G)\}_{n \geq 1}$ is monotonically increasing for any finite group G and each subgroup H of G, because

$$\begin{aligned}
\Pr^{(n+1)}(H,G) &= \frac{1}{|H|^{n+1}|G|}\sum_{x_1\in H}\cdots\sum_{x_{n+1}\in H}|C_G([x_1,x_2,\cdots,x_{n+1}])| \\
&= \frac{1}{|H|^{n+1}|G|}\sum_{x_1\in H}\cdots\sum_{x_{n+1}\in H}\sum_{[x_1,x_2,\cdots,x_{n+1}]=1}|C_G([x_1,x_2,\cdots,x_{n+1}])| \\
&\quad + \frac{1}{|H|^{n+1}|G|}\sum_{x_1\in H}\cdots\sum_{x_{n+1}\in H}\sum_{[x_1,x_2,\cdots,x_{n+1}]\neq 1}|C_G([x_1,x_2,\cdots,x_{n+1}])| \\
&\geq \frac{1}{|H|^{n+1}|G|}(|H|^{n+1})\Pr^{(n)}(H)|G| \\
&= \Pr^{(n)}(H) \geq \Pr^{(n)}(H,G).
\end{aligned}$$

Theorem 5.5.3. *Let H be a subgroup of G. Then, for every $n \geq 1$,*

$$\Pr^{(n+1)}(H,G) \leq \frac{1}{2}\left(1+\Pr^{(n)}\left(\frac{H}{H\cap Z(G)}\right)\right).$$

Proof. We have

$$\begin{aligned}
& |H|^{n+1}|G|\Pr^{(n+1)}(H,G) \\
= \;& |\{(x_1,x_2,\cdots,x_{n+1},y)\in H^{n+1}\times G \mid [x_1,x_2,\cdots,x_{n+1},y]=1\}| \\
= \;& \sum_{x_1\in H}\cdots\sum_{x_{n+1}\in H}|C_G([x_1,x_2,\cdots,x_{n+1}])| \\
= \;& \sum_{x_1\in H}\cdots\sum_{x_{n+1}\in H}\sum_{[x_1,x_2,\cdots,x_{n+1}]\in Z(G)\cap H}|C_G([x_1,x_2,\cdots,x_{n+1}])| \\
& \quad + \sum_{x_1\in G}\cdots\sum_{x_{n+1}\in H}\sum_{[x_1,x_2,\cdots,x_{n+1}]\notin Z(G)\cap H}|C_G([x_1,x_2,\cdots,x_{n+1}])| \\
\leq \;& |H|^{n+1}\Pr^{(n)}\left(\frac{H}{Z(G)\cap H}\right)|G| \\
& \quad + \left(|H|^{n+1}-|H|^{n+1}\Pr^{(n)}\left(\frac{H}{Z(G)\cap H}\right)\right)\frac{|G|}{2} \\
= \;& \frac{|H|^{n+1}|G|}{2}\left(1+\Pr^{(n)}\left(\frac{H}{Z(G)\cap H}\right)\right).
\end{aligned}$$

Hence the result follows. □

Note that Theorem 5.5.3 is a generalization of Theorem 5.3.5. The next theorem is a slight improvement of Theorem 5.3.4.

Theorem 5.5.4. *Let G be a finite group, H and N be subgroups of G such that $N \trianglelefteq G$ and $N \subseteq H$. Then*

$$\Pr^{(n)}(H, G) \leq \Pr^{(n)}\left(\frac{H}{N}, \frac{G}{N}\right).$$

Moreover, if $N \cap [_nH, G] = \{1\}$ then the equality holds.

Proof.

$$\begin{aligned}
& |H|^n|G|\Pr^{(n)}(H,G) \\
= \; & |\{(x_1, x_2, \cdots, x_n, y) \in H^n \times G \mid [x_1, x_2, \cdots, x_n, y] = 1\}| \\
= \; & \sum_{x_1 \in H} \cdots \sum_{x_n \in H} |C_G([x_1, x_2, \cdots, x_n])| \\
= \; & \sum_{x_1 \in H} \cdots \sum_{x_n \in H} \frac{|C_G([x_1, x_2, \cdots, x_n])N||C_N([x_1, x_2, \cdots, x_n])|}{|N|} \\
\leq \; & \sum_{x_1 \in H} \cdots \sum_{x_n \in H} |C_{G/N}([Nx_1, Nx_2, \cdots, Nx_n])||C_N([x_1, x_2, \cdots, x_n])| \\
= \; & \sum_{S_1 \in H/N} \sum_{x_1 \in S_1} \cdots \sum_{S_n \in H/N} \sum_{x_n \in S_n} |C_{G/N}([S_1, S_2, \cdots, S_n])||C_N([x_1, x_2, \cdots, x_n])| \\
= \; & \sum_{S_1 \in H/N} \cdots \sum_{S_n \in H/N} |C_{G/N}([S_1, S_2, \cdots, S_n])| \sum_{x_1 \in S_1} \cdots \sum_{x_n \in S_n} |C_N([x_1, x_2, \cdots, x_n])| \\
\leq \; & |N|^{n+1} \sum_{S_1 \in H/N} \cdots \sum_{S_n \in H/N} |C_{G/N}([S_1, S_2, \cdots, S_n])| \\
= \; & \left|\frac{H}{N}\right|^n \left|\frac{G}{N}\right| \Pr^{(n)}\left(\frac{H}{N}, \frac{G}{N}\right) |N|^{n+1} \\
= \; & |H|^n|G|\Pr^{(n)}\left(\frac{H}{N}, \frac{G}{N}\right).
\end{aligned}$$

Therefore,

$$\Pr^{(n)}(H,G) \leq \Pr^{(n)}\left(\frac{H}{N}, \frac{G}{N}\right).$$

Again, $[N, {}_nH] \subseteq N$, and so if $N \cap [{}_nH, G] = \{1\}$ then $[N, {}_nH] \cap [{}_nH, G] = \{1\}$ forcing $[N, {}_nH] = \{1\}$. This implies that $N \subseteq C_H([x_1, x_2, \cdots, x_n]) \subseteq C_G([x_1, x_2, \cdots, x_n])$, where $x_1, x_2, \cdots, x_n \in H$. Furthermore

$$\frac{C_G([x_1, x_2, \cdots, x_n])}{N} = C_{G/N}([Nx_1, Nx_2, \cdots, Nx_n]).$$

Hence by the same argument as in the first part we get the second part of the Theorem. □

Applying Theorem 5.5.4 with $H = G$, we get the following corollary.

Corollary 5.5.5. *If $N \trianglelefteq G$ then $\Pr^{(n)}(G) \leq \Pr^{(n)}(G/N)$.*

The following theorem is a generalization of Theorem 5.4.6

Theorem 5.5.6. *Let H be a proper subgroup of G. Then, for every $n \geq 1$,*

(i) $\Pr^{(n)}(H,G) = 1$ *if* $H \subseteq Z_n(G)$,

(ii) $\Pr^{(n)}(H,G) = 1$ *if* $H \nsubseteq Z_n(G)$ *and* $H/(Z(G) \cap H)$ *is nilpotent of class at most* $n-1$,

(iii) $\Pr^{(n)}(H,G) \leq (2^{n+2} - 3)/(2^{n+2})$ *if* $H \nsubseteq Z_n(G)$ *and* $H/(Z(G) \cap H)$ *is not nilpotent of class at most* $n-1$. .

Proof. (i) Follows immediately from definition.

(ii) It is clear that if $H/(Z(G)\cap H)$ is nilpotent of class at most $n-1$, then for elements $\bar{x_1}, \bar{x_2}, \cdots, \bar{x_n}$ in $H/(Z(G)\cap H)$, we have $[\bar{x_1}, \bar{x_2}, \cdots, \bar{x_n}] = \bar{1}$. So, $C_G([x_1, \cdots, x_n]) = G$, and by the same argument as in Theorem 5.5.3, we have

$$\begin{aligned}
&|H|^n|G|\Pr^{(n)}(H,G) \\
&\quad = |\{(x_1, x_2, \cdots, x_n, y) \in H^n \times G \mid [x_1, x_2, \cdots, x_n, y] = 1\}| \\
&\quad = \sum_{x_1 \in H} \cdots \sum_{x_n \in H} |C_G([x_1, x_2, \cdots, x_n])| \\
&\quad = |H|^n|G|.
\end{aligned}$$

Hence, $\Pr^{(n)}(H,G) = 1$.

(iii) Since $H/(Z(G)\cap H)$ is not nilpotent of class at most $n-1$, so

$$\Pr^{(n-1)}(H/(Z(G)\cap H)) \leq (2^{n+1}-3)/(2^{n+1}). \quad \text{(by Theorem 5.3.7)}$$

Now, by Theorem 5.5.3 we have

$$\begin{aligned}
\Pr^{(n)}(H,G) &\leq \frac{1}{2}\left(1 + \Pr^{(n-1)}\left(\frac{H}{H\cap Z(G)}\right)\right) \\
&\leq \frac{1}{2}\left(1 + \frac{2^{n+1}-3}{2^{n+1}}\right) = \frac{2^{n+2}-3}{2^{n+2}}.
\end{aligned}$$

□

It may be mentioned here that $\Pr^{(n)}(H,G)$ can be further generalized to

$$\Pr_g^{(n)}(H,G) = \frac{|\{(x_1, x_2, \cdots, x_n, y) \in H^n \times G \,|[x_1, x_2, \cdots, x_n, y] = g\}|}{|H|^n|G|}.$$

where $g \in G$ and

$$\Pr_K^{(n)}(H,G) = \frac{|\{(x_1, x_2, \cdots, x_n, y) \in H^n \times G \,|[x_1, x_2, \cdots, x_n, y] \in K\}|}{|H|^n|G|}.$$

where K is a subgroup of G.

PROBLEM: To study $\Pr_g^{(n)}(H,G)$ and $\Pr_K^{(n)}(H,G)$ in detail.

5.6 Probability that an Automorphism Fixes a Group Element

Let G be a finite group acting on a finite set Ω. Define

$$\mathrm{Fix}(G,\Omega) = \{(g,\omega) \in G \times \Omega | g\omega = \omega\}.$$

Then the probability that an element of G leaves an element of Ω fixed is defined to be the ratio

$$\Pr_G(\Omega) = \frac{|\,\mathrm{Fix}(G,\Omega)|}{|G||\Omega|}.$$

We have

$$\begin{aligned} |\,\mathrm{Fix}(G,\Omega)| &= \sum_{\omega\in\Omega} |\{g \in G \mid g\omega = \omega\} = \sum_{\omega\in\Omega} |\,\mathrm{stab}(\omega)| \\ &= \sum_{\omega\in\Omega} |G : \mathrm{orb}(\omega)| = \sum_{i=1}^{k} |G : \mathrm{orb}(\omega_i)||\,\mathrm{orb}(\omega_i)| \end{aligned}$$

where $\{\omega_1, \omega_2, \cdots, \omega_k\}$ is a set of representatives of the distinct orbits of Ω under the action of G, and we have $|\,\mathrm{Fix}(G,\Omega)| = k.|G|$.

Thus $\Pr_G(\Omega) = k/|\Omega|$ the ratio of the number of orbits in Ω under the action of G to the order of Ω.

If G acts on itself by conjugation then one has $k = k(G)$. In which case $\Pr_G(G) = k(G)/|G|$ gives the usual commutativity degree $\Pr(G)$.

Let $\Omega = G$ and $A = \mathrm{Aut}(G)$ then $\mathrm{Pr}_A(G)$ is the probability that an automorphism fixes a group element. In 1975, Gary Sherman [46] studied $\mathrm{Pr}_A(G)$ for a finite abelian group G and found few fruitful results. Let us study those results where G is a finite abelian group and $A = \mathrm{Aut}(G)$.

Theorem 5.6.1. $\mathrm{Pr}_A(G) = 1$ *if and only if* $G = \mathbb{Z}_2$.

Proof. It is trivial that $\mathrm{Pr}_A(\mathbb{Z}_2) = 1$. Conversely, if $\mathrm{Pr}_A(G) = 1$, then G is an elementary abelian 2-group since the automorphism $x \to -x$ must be the identity mapping. Viewing G as a $\mathbb{Z}_2$-space it follows that any two nontrivial elements of G are in the same orbit. Thus, $2/2^j = 1$ where $|G| = 2^j$. This implies $j = 1$; i.e., $G = \mathbb{Z}_2$. □

Theorem 5.6.2. $\mathrm{Pr}_A(G) \leq 3/4$ *if* $G \neq \mathbb{Z}_2$.

Proof. Let F is the subgroup of trivial orbits and $O_1, O_2, \cdots, O_r$ be the nontrivial orbits of G. Then we have

$$|G| = |F| + |O_1| + \cdots + |O_r|.$$

Hence, $(|G| - |F|)/2 \geq r$ since $|O_i| \geq 2$ for $i = 1, 2, \cdots, r$. From $k = r + |F|$ where k is the number of orbits of G, we get $k \leq (|G| + |F|)/2$.
If $G \neq \mathbb{Z}_2$, then $F \neq G$ and therefore $|G : F| \geq 2$. i.e., $|F| \leq |G|/2$. Thus $k \leq (3/4) \cdot |G|$, so $\mathrm{Pr}_A(G) \leq 3/4$ as required. □

Note that the above bound is the best possible as $\mathrm{Pr}_A(\mathbb{Z}_4) = 3/4$.

A routine verification gives the following theorem:

Theorem 5.6.3. *If* $G \cong \bigoplus_{i=1}^{s} G_i$, *then*

$$\Pr_A(G) \leq \prod_{i=1}^{s} \Pr_{A_i}(G_i),$$

where $A_i = \mathrm{Aut}(G_i)$, $1 \leq i \leq s$. *Equality holds if each* G_i *is a Sylow subgroup of* G.

In view of the above theorem, to obtain a bound for $\Pr_A(G)$ it suffices to obtain a bound for the Sylow subgroups. Note that for $|G| = p^n$ and G elementary abelian, we have $\Pr_A(G) = 2/p^n$ since G is a $\mathbb{Z}_p$-space. Also for $|G| = p^n$ and G cyclic, there is at least one element of order p^m for $m = 0, 1, 2, \cdots, n$. As elements in the same orbit must have equal orders, G has at least $n+1$ orbits. Since elements of the same order can be written as powers of elements with orders prime to p, the elements of a particular order form an orbit. Thus $\Pr_A(G) = (n+1)/p^n$ when G is cyclic. Gary Sherman [46] also established a general bound for $\Pr_A(G)$ when G is a p-group. The following is useful in establishing the bound.

Lemma 5.6.4. *Let* n *be a positive integer greater than* 1. *The maximum value of* $\prod_{i=1}^{k} n_i$, *for* $\sum_{i=1}^{k} n_i = n$, *is* $3^{(n-i)/3} \cdot 2^{i/2}$, *where*

$$\begin{aligned} i &= 4 \quad \text{if} \quad n \equiv 1 (\mathrm{mod} 3) \\ i &= 2 \quad \text{if} \quad n \equiv 2 (\mathrm{mod} 3) \\ i &= 0 \quad \text{if} \quad n \equiv 0 (\mathrm{mod} 3). \end{aligned}$$

Proof. The maximum occurs when no $n_i = 1$. Further, $(m-2) \cdot 2 > m$ if and only if $m > 4$. Thus each $n_i > 4$ can be replaced by $(n_i - 2) + 2$ in

the partition and the associated product will be increased. If some $n_i = 4$, replacing it by $2+2$ leaves the product unchanged. If $2+2+2$ occurs in the partition, replacing it by $3+3$ increases the product. Hence the maximum occurs when each n_i is a two or a three. The conclusion of the lemma follows immediately. □

Thus we observe that the maximum product associated with the partitions of n is smaller than the corresponding product obtained from m if $n < m$.

Proposition 5.6.5. *If* $|G| = p^n$, *then* $\Pr_A(G) \leq 2 \cdot (3/p^2)^{n/2}$.

Proof. Suppose the invariants of G are $m_1, m_2, \cdots, m_k, 1, \cdots, 1,$ where $\sum_{i=1}^{k} m_i = m$ and $i < j$ implies $m_i \geq m_j$. Let H denote the summands of G of order p and K denote the summands of G of order at least p^2. Thus $G \cong H \oplus K$. Then by Theorem 5.6.3, we get

$$\Pr_A(G) \leq \Pr_A(H) \cdot \Pr_A(K) \leq \left(\frac{2}{p^{n-m}}\right) \cdot \left(\prod_{i=1}^{k} \frac{m_i + 1}{p^{m_i}}\right)$$

Thus

$$\Pr_A(G) \leq (2/p^n) \cdot \prod_{i=1}^{k} (m_i + 1). \tag{5.6.a}$$

Since $\sum_{i=1}^{k} (m_i + 1) = m + k$, maximizing k maximizes the sum. The largest value for k occurs when the m_i's are smallest (all twos, except for one three if m is odd). Taking k' to be the integer of $\{m/2, (m-1)/2\}$ and applying Lemma 5.6.4, to Equation 5.6.a, we have

$$\Pr_A(G) \leq \frac{2}{p^n} \cdot 3^{(m+k')/3} \leq \frac{2}{p^n} \cdot 3^{(m+\frac{1}{2}m)/3} \leq \frac{2}{p^n} \cdot 3^{m/2} \leq 2 \cdot \left(\frac{3}{p^2}\right)^{n/2}.$$

as required. □

Proposition 5.6.6. *If $0 < \rho < 1$, there is only a finite number of finite abelian groups G with $\Pr_A(G) \geq \rho$.*

Proof. We may choose a positive integer N and a prime q both so large that $2 \cdot (3/4)^{N/2} < \rho$ and $2 \cdot (3/q^2)^{1/2} < \rho$. If $\Pr_A(G) \geq \rho$ and p^j divides $|G|$, where p is a prime, then $j < N$ and $p < q$. This condition imposes an upper bound on the order of G. Hence the result follows. □

Proposition 5.6.7. *If $\{G_n\}$ is a sequence of finite abelian groups for which $|G_n| \to \infty$ as $n \to \infty$, then $\Pr_A(G_n) \to 0$ as $n \to \infty$.*

Proof. Since $\{\Pr_A(G_n)\}$ is bounded above by 1, the limit superior of $\{\Pr_A(G_n)\}$ is finite. Indeed, $\limsup \Pr_A(G_n) = 0$, otherwise we contradict Proposition 5.6.6. Thus

$$0 \leq \liminf \Pr_A(G_n) \leq \limsup \Pr_A(G_n) = 0.$$

□

We would like to conclude this section by stating one problem posed by Gary Sherman [46].

PROBLEM: Suppose G is finite group (not necessary abelian) and S is the set of its subgroups. Let G acts on S by conjugation and consider $\Pr_G(S)$. It is clear that $\Pr_G(S) = 1$ if and only if each subgroup of G is normal. This is equivalent to G being abelian or Hamiltonian. The problem then is to determine if there exists some real number ρ, where $o < \rho < 1$, for which $\Pr_G(S) \leq \rho$ when G is neither abelian nor Hamiltonian. Sherman

conjectured that $\rho = 2/3$. If this conjecture is true, the bound is sharp since $\Pr_{S_3}(S) = 2/3$.

5.7 Rewriteability in Finite Groups

The notion of rewriteability has its origin in automata theory and currently is of considerable interest in group theory [5].

Let $S \subseteq S_n - \{1\}$; i.e., S is a non-empty set of nontrivial permutations of $\{1, 2, \cdots, n\}$. An n-tuple $(x_1, x_2, \cdots, x_n)$ of elements of G is called *S-rewriteable* or *n-rewriteable* if $x_1 x_2 \cdots x_n = x_{\sigma(1)} x_{\sigma(2)} \cdots x_{\sigma(n)}$ for some $\sigma \in S$.

Leavitt, Sherman and Walker [34] generalized the usual $\Pr(G)$ by setting

$$\Pr_n(G; S) = \frac{|Rw_n(G; S)|}{|G|^n}$$

where

$$Rw_n(G; S) = \{(x_1, x_2, \cdots, x_n) \in G^n \mid (x_1, x_2, \cdots, x_n) \text{ is } S\text{-rewriteable}\}.$$

We call $\Pr_n(G; S)$ as *S-rewriteability* or *n-rewriteability degree* of G. The case $n = 2$ gives $\Pr_2(G : S) = \Pr(G)$, however we shall write $\Pr_2(G : S) := \Pr_2(G)$ and $Rw_2(G : S) := Rw_2(G)$.

By the above definition, a group G is said to be 3-*rewriteable* if $xyz \in \{xzy, yzx, yxz, zxy, zyx\}$ for all $x, y, z \in G$. Let us first study few available results for 3-rewriteable groups. Using a result of Curzio, Longobard and Maj ([8] Theorem 3) Leavitt, Sherman and Walker [34] have established the following result. However first we shall discuss the proof given by Lescot [32].

Theorem 5.7.1. *The following conditions on a finite group G are equivalent*

(i) *The order of the commutator subgroup of* G *is one or two, i.e.,* $|G'| \leq 2$.

(ii) *The order of each conjugacy class of* G *is one or two, i.e.,* $|\operatorname{Cl}(x)| \leq 2 \ \forall x \in G$.

(iii) *The order of the centralizer of each element of* G *is* $|G|$ *or* $|G|/2$, *i.e.,* $|C_G(x)| \in \{|G|, |G|/2\} \ \forall x \in G$.

(iv) G *is 3-rewriteable, i.e.,* $xyz \in \{xzy, yzx, yxz, zxy, zyx\} \ \forall \ x, y, z \in G$.

(v) $\Pr(G) > 1/2$.

Proof. (i) $\Rightarrow$ (ii) Each $c \in \operatorname{Cl}(x)$ can be written as $c = yxy^{-1}$ therefore $c = (yxy^{-1}x^{-1})x \in G'x$ and $\operatorname{Cl}(x) \subseteq G'x$. Thus

$$|\operatorname{Cl}(x)| \leq |G'x| = |G'| \leq 2.$$

(ii) $\Rightarrow$ (iii) Clear because

$$|\operatorname{Cl}(x)| = |G : C_G(x)| \ \forall x \in G.$$

(iii) $\Rightarrow$ (iv) Let $(x, y, z) \in G^3$ then $C_G(y)$ has at most two right cosets in G. If $x \in C_G(y)$ then $xyz = yxz$; if $z \in C_G(y)$ then $xyz = xzy$. We may therefore assume that $xC_G(y) = G \setminus C_G(y) = zC_G(y)$, therefore $z^{-1}x \in C_G(y)$. If $xyz \neq yzx$ then $yzC_G(x) = G \setminus C_G(x)$, therefore $y \in yzC_G(x)$, i.e., $z \in C_G(x)$. It follows that

$$z^{-1}xy = yz^{-1}x = yxz^{-1}$$

$$or, \quad xyz = zyx.$$

(iv) $\Rightarrow$ (v) Let us apply the hypothesis to a triple (x, y, x^2); we get

$$xyx^2 \in \{xx^2y, yxx^2, yx^2x, x^2xy, x^2yx\} \ \forall (x, y) \in G \times G,$$

therefore $xy = yx$ or $yx^2 = x^2y$, thus in any case $x^2 \in Z(G)$. Therefore $G/Z(G)$ is a group in which every element has square 1, i.e., an elementary abelian 2-group. By Proposition 3.2.6, there is a group H isoclinic to G and such that $Z(H) \subseteq H'$. Also

$$\frac{H}{Z(H)} \cong \frac{G}{Z(G)}$$

is then elementary abelian, therefore $H' \subseteq Z(H)$ and

$$H' = Z(H).$$

For each $h \in H$, the map $\phi_h : H/Z(H) \to H'$ defined by

$$\phi_h(uZ(H)) = [h, u] \ \forall u \in H$$

(i.e., $\phi_h = a_H(hZ(H)), .)$ is a morphism of groups from $H/Z(H)$ to H', therefore, for $u \in H, [h, u] = \phi_h(uZ(H))$ has order 2. H', being abelian and generated by elements of order 2, is therefore an elementary abelian 2-group.

We now note that condition (iv) can be rewritten as

$$[x, y] = 1, \ [y, z] = 1, \ [x, yz] = 1, \ [xy, z] = 1, \text{ or } \ xyz = zyx,$$

i.e.,

$$[x, y] = 1, \ [y, z] = 1, \ [x, y][x, z]^y = 1, \ [y, z]^x[x, z] = 1, \text{ or } [x, y][x, z]^y[y, z] = 1$$

for all $(x, y, z) \in G^3$.

It follows that condition (iv) holds also for H since $G' \leq Z(G)$; consequently $H' \subseteq Z(H)$. Now the reasoning ([8], pp141-142), gives

$$|H'| \leq 2$$

Therefore $Z(H) = H'$ has order 1 or 2, i.e., $H = \{1\}$ or H is an extraspecial 2-group. By Corollary 3.3.2, we have

$$\Pr(G) = \{1\} \cup \{\frac{1}{2}\left(1 + \frac{1}{4^n}\right) | n \in \mathbb{N}, n \geq 1\}$$

and thus $\Pr(G) = \Pr(H) > \frac{1}{2}$.

(v) $\Rightarrow$ (i) By Theorem 2.2.2, we have

$$|G'| \leq \frac{3}{4\Pr(G) - 1} < \frac{3}{\frac{4}{2} - 1} = 3,$$

thus $|G'| \leq 2$. □

Now we discuss the proof by Leavitt Sherman and Walker [34]. The following lemmas are useful to organize the proof.

Lemma 5.7.2. *If x and y are elements of G for which $|G : C_G(x)| = 2$ and $C_G(y) \cap (G \setminus C_G(x)) \neq \phi$, then $G : C_G(xy) \geq [G : C_G(y)]$.*

Proof. The conjugacy class of y, $\mathrm{Cl}(y)$ may be written as $\{y^{g_1}, y^{g_2}, \cdots, y^{g_n}\}$ where $\{g_1, g_2, \cdots, g_n\}$ is a complete set of right representatives for $C_G(y)$ in G. Moreover, we may choose each coset representative $C_G(x)$. Otherwise $C_G(y)g_i \subseteq G \setminus C_G(x)$, which means that $G \setminus C_G(x) = C_G(x)g_i$ since $|G : C_G(x)| = 2$. Therefore $C_G(y)g_i \subseteq C_G(x)g_i$ and so $C_G(y) \subseteq C_G(x)$, a contradiction. The conclusion follows because the mapping $y^{g_i} \to xy^{g_i}$ embeds $\mathrm{Cl}(y)$ in $\mathrm{Cl}(xy)$. □

Let us consider the following subsets of G

$$X = \{x \in G |\ |G : C_G(x)| \geq 3\},$$
$$Y = \{x \in G |\ |G : C_G(x)| = 2\},$$
$$Z = \{x \in G |\ |G : C_G(x)| = 1\},\ \text{the center of } G.$$

Lemma 5.7.3. *If at least* $3 \cdot |Z|$ *elements of* G *have centralizers of index at least* 3, *then* $\Pr(G) \leq 1/2$.

Proof. Observe that

$$\begin{aligned} |Rw_2(G)| = k(G) \cdot |G| &\leq (|X|/3 + |Y|/2 + |Z|) \cdot |G| \\ &= (|Z| + (|X| - 3 \cdot |Z|)/3 + |Y|/2 + |Z|) \cdot |G| \\ &\leq (|Z| + (|X| - 3 \cdot |Z|)/2 + |Y|/2 + |Z|) \cdot |G| \\ &= (|X| + |Y| + |Z|) \cdot |G|/2 \\ &= |G|^2/2. \end{aligned}$$

Thus $\Pr(G) \leq 1/2$ as claimed. □

Lemma 5.7.4. *If* G *is not* 3*-rewriteable, then* $|G : Z| \geq 6$.

Proof. If $|G : Z|$ is 1, 2, 3 or 5 then G is abelian since G/Z is cyclic. If $|G : Z| = 4$ and x is a noncentral element, then $Z \subset C_G(x) \subset G$ implies $|G : C_G(x)| = 2$; i.e., G is 3-rewriteable. □

It is not necessary to invoke the characterization of 3-rewriteability to complete the Lemma 5.7.4. If $|G : Z| = 4$, then $G/Z \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Thus $G = Z \cup xZ \cup yZ \cup xyZ$. The only triple products from G whose 3-rewriteability

we might question have from $(xz_1)(yz_2)(xyz_3)$ or $(xz_1)(xyz_2)(yz_3)$. But, notice that $(xz_1)(yz_2)(xyz_3) = (xyz_3)(xz_1)(yz_2)$ and that $(xz_1)(xyz_2)(yz_3) = (yz_3)(xz_1)(xyz_2)$ because $x^2 \in Z$. This proof makes Lemma 5.7.4, which is an analogue of the fact that $|G : Z| \geq 4$ for nonabelian G.

Now we are able to give an elementary proof of Theorem 5.7.1. Theorem 5.7.1 can be restate as the following

Theorem 5.7.5. *A finite group G is 3-rewriteable if and only if* $\Pr(G) > 1/2$.

Proof. Assume that G is not 3-rewriteable. Then note that $X \neq \phi$. Choose $g \in X$ and set $n = |G : C_G(g)|$. Then $Z \cup Zg \subseteq C_G(g)$ and $(Z \cup Zg) \cap Y = \phi$. Thus

$$|C_G(g) \cap Y| \leq |G|/n - 2|Z|$$

and so

$$|(G \setminus C_G(g)) \cap Y| \geq |Y| - |G|/n + 2 \cdot |Z|.$$

If $x \in (G \setminus C_G(g)) \cap Y$, then $|G : C_G(x)| = 2$ and $C_G(g) \cap (G \setminus C_G(x)) \neq \phi$ implies, by Lemma 5.7.2, that $|G : C_G(xg)| \geq |G : C_G(g)| \geq 3$. Therefore $(G \setminus C_G(g)) \cap Y \subseteq X$; in fact $(G \setminus C_G(g)) \cap Y \subseteq X \setminus Zg$ as $Zg \subseteq X \cap C_G(g)$. Thus

$$|X| - |Z| = |X \setminus Zg| \geq |(G \setminus C_G(g)) \cap Y| \geq |Y| - |G|/n + 2 \cdot |Z|;$$

i.e.,

$$|X| \geq |Y| - |G|/n + 3 \cdot |Z|. \tag{5.7.a}$$

In view of Lemma 5.7.3 and (5.7.a) we are done if $|Y| \geq |G|/3$, so assume that $|Y| < |G|/3$. In this case Lemma 5.7.4 implies that $|X| > |G|/2$ and, therefore, $|X| > 3 \cdot |Z|$. The theorem is proved. □

Corollary 5.7.6. *If G is not 3-rewriteable, then at least $|G| \cdot (n-1)/2n + |Z|$ elements of G have centralizers of index at least 3 where n is the greatest centralizer index among the elements of G. In particular, more than $1/3$ of the elements of G have centralizers of index at least 3.*

Proof This follows directly from (5 7 a) by substituting $|G| - |X|$ for $|Y| + |Z|$. □

Note that Theorem 5.7.5 can formulate in terms of conjugacy classes and conditional probability as follows

Theorem 5.7.7. *Each conjugacy class of a finite group G has order one or two if and only if the average conjugacy class order is less than 2.*

Theorem 5.7.8. *For a given y the probability of commuting x and y ,for each x, is at least $1/2$ if and only if $\Pr(G) > 1/2$.*

The bound $1/2$ for 3-rewriteability is sharp in two senses.

(i) $\Pr(G) = 1/2$ *if and only if* $G/Z \cong S_3$.

(ii) *There exists a sequence, $\{G_n\}$, of 3-rewriteable groups such that* $\Pr(G_n) \downarrow 1/2$

A result of Ito [26] says that groups in which each conjugacy class is of order one or p, for a fixed prime p, must be the direct product of a p-group with this property and an abelian group. Thus, if G is 3-rewriteable we may write $G \cong T \times A$, where T is a 3-rewriteable 2-group and A is abelian And

$$\Pr(G) = \Pr(T \times A) = \Pr(T) \cdot \Pr(A) = \Pr(T).$$

Therefore we may restrict our attention to 2-groups.

Consider the quaternion group of order eight.

$$Q_8 = \langle x, y, z | x^2 = y^2 = z^2 = xyx^{-1}y^{-1} = xzx^{-1}z^{-1} = 1, yzy^{-1}z^{-1} = x \rangle.$$

The relevant fact are;

$$|Q_8| = 8 = 2^3,$$

$$Z = Q_8' = \{1, x\},$$

$$k(Q_8) = 5 = |Z| + (|G| - |Z|)/2 = (|G| + |Z|)/2,$$

$$\Pr(Q_8) = 5/8 = 1/2 + |Z|/(2 \cdot |G|).$$

Leavitt, Sherman and Walker [34] generalize by taking G_n to be an (extraspecial 2-group) generated by $x_1, x_2, \cdots, x_{2n+1}$ subject to the relations

$$x_i^2 = 1 \text{ for } 1 \leq i \leq 2n+1,$$

$$x_i x_j x_i^{-1} x_j^{-1} = \begin{cases} x_1 & \text{for } i \text{ even and } j = i+1, \\ 1 & \text{otherwise.} \end{cases}$$

Then $|G| = 2^{2n+1}$ and $Z = G_n' = \{1, x_1\}$ so that $\Pr(G_n) = 1/2 + 1/2^{2n+1}$.

Now we study bounds for $\Pr_n(G; S)$. The following lemma generalizes Theorem 2.2.3

Lemma 5.7.9. *If $n \geq 2$ and $\sigma \in S_n - \{id\}$, then $|Rw_n(G; \{\sigma\})| \leq k(G) \cdot |G|^{n-1}$.*

Proof. The proof is by induction on n. The case for $n = 2$ gives

$$|Rw_2(G; \{\sigma\})| = |\{(x, y) \in G^2 | xy = yx\}| = k(G) \cdot |G|.$$

Assume that the results holds for $n-1$.

If $\sigma(n)=n$, then $x_1x_2\cdots x_n = x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(n)}$ if and only if $x_1x_2\cdots x_{n-1} = x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(n-1)}$. Therefore $|Rw_n(G;\{\sigma\})| = |Rw_{n-1}(G;\{\hat{\sigma}\})|\cdot|G|$ where $\hat{\sigma}$ is σ restricted to $\{1,2,\cdots,n-1\}$. Thus in this case the induction hypothesis yields the result.

If $\sigma(n)<n$, say $\sigma(n)=m$, then $x_1x_2\cdots x_n = x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(n)}$ if and only if ${x_n}^{-1}x_{\sigma(j-1)}^{-1}\cdots x_{\sigma(1)}^{-1}x_1x_2\cdots x_n = x_{\sigma(j+1)}x_{\sigma(j+2)}\cdots x_m$ where $\sigma(j)=n$. Let $g = x_{\sigma(j-1)}^{-1}x_{\sigma(j-2)}^{-1}\cdots x_{\sigma(1)}^{-1}x_1x_2\cdots x_{n-1}$ and $h = x_{\sigma(j+1)}x_{\sigma(j+2)}\cdots x_m$. Notice that $|\{x_n|{x_n}^{-1}gx_n = h\}|$ is $|C_G(g)|$ or 0 for fixed $x_1,x_2,\cdots,x_{n-1}$ and that g varies over G as x_m varies over G. Thus

$$\begin{aligned}
|Rw_n(G;\{\sigma\})| &\le \sum_{x_1}\cdots\sum_{x_m}\cdots\sum_{x_{n-1}}|C_G(g)| \\
&= \sum_{x_1}\cdots\sum_{x_{n-1}}\left(\sum_{x_m}|C_G(g)|\right) \\
&= \sum_{x_1}\cdots\sum_{x_{n-1}}\left(\sum_{g}|C_G(g)|\right) \\
&= \sum_{x_1}\cdots\sum_{x_{n-1}}(k(G)\cdot|G|) \\
&= (k(G)|G|^{n-1}.
\end{aligned}$$

This completes the proof. □

It follows from Theorem 2.2.3 and Lemma 5.7.9 that

$$\Pr_n(G;S) = |Rw_n(G;S)|/|G|^n \le |S|\cdot\Pr(G) \le |S|(p^2+p-1)/p^3 \quad (5.7.b)$$

Since $(p^2+p-1)/p^3 \downarrow 0$ as $p\to\infty$ we may use equation (5.7.b) to conclude that, for $|S|$ fixed and sufficiently large p, "5/8-like" bound exists for

$\Pr_n(G;S)$. Leavitt, Sherman and Walker [34] showed that random sampling of the "S-rewriteability hypercube" of various groups suggests such bounds exists independent of p.

Lastly we conclude this section by a conjecture of Leavitt, Sherman and Walker [34].

Conjecture 5.7.10. *If G is not S-rewriteable then there exists $\rho_n(S) < 1$, independent of G, such that $\Pr_n(G;S) \leq \rho_n(S) < 1$.*

Specifically, if $p \geq 7$, then $\Pr_3(G; S_3 - \{id\}) \leq 275/343$. However, CAYLEY [21] suggests $\Pr_3(G; S_3 - \{id\}) \leq 17/18$. Thus for 3-rewriteability their conjecture is:

If G is not 3-rewriteable, then $\Pr_3(G; S_3 - \{id\}) \leq \rho_3(S_3 - \{id\}) = 17/18$.

If this conjecture proves to be true, then the 17/18 bound is sharp because $\Pr_3(S_3; S_3 - \{id\}) = 17/18$.

We conclude by mentioning that if G is non-abelian finite simple group then $\Pr_3(G; S_3 - \{id\}) \leq 5/12$. This follows from equation (5.7.b) because $\Pr(G) \leq \Pr(A_5)$ [11] and $\Pr(A_5) = 1/12$. It seems likely that the bound is actually 27/100 because CAYLEY[21] shows $\Pr(A_5, S_3 - \{id\})$ to be 27/100.

5.8 Commutativity in Finite Rings

In 1976 Machale [37] considered the problem of finding the probability $\Pr(R)$ that a pair of elements in a finite ring R commute with each other. He defined $\Pr(R)$ to be $\frac{1}{|R|^2}\sum_{x\in R}|C_R(x)|$, where $C_R(x)$ is the subring $\{r \in R : xr = rx\}$ of R. By Theorem 2.1.1 for finite group G we have $\Pr(G) = \frac{1}{|G|^2}\sum_{x\in G}|C_G(x)| =$

$k(G)/|G|$, where $k(G)$ is the number of conjugacy classes in the group G. The concept of conjugacy in groups has no obvious analogue in rings even though there are many results for $\Pr(R)$ very similar to $\Pr(G)$, however, the methods of proof will be somewhat different. Let us study few such results first studied by Machale [37].

Lemma 5.8.1. *If R is a non-commutative ring, then $R/Z(R)$ is not cyclic (additive) group.*

Proof. Let R be a non-commutative ring and $R/Z(R)$ is cyclic group generated by $Z(R)+r$. Then

$$R = Z(R) \cup (Z(R)+r) \cup 2(Z(R)+r) \cup \cdots \cup n(Z(R)+r) \cup \cdots$$

$$R = Z(R) \cup (Z(R)+r) \cup (Z(R)+2r) \cup \cdots \cup (Z(R)+nr) \cup \cdots$$

Typical elements of R may now be expressed as z_1+nr and z_2+mr where $z_1, z_2 \in Z(R)$ and m and n are integers. But these elements clearly commute, which contradicts the hypothesis. Hence the result follows. □

Corollary 5.8.2. *If R is a non-commutative ring, then $|R : Z(R)|$ can not be a prime number.*

Theorem 5.8.3. *If R is a non-commutative ring, then $\Pr(R) \leq 5/8$, with equality if and only if $|R : Z(R)| = 4$.*

Proof. Since R is a non-commutative ring by Corollary 5.8.2, we have $|R : Z(R)| \geq 4$.i.e., $|Z(R)| \leq (1/4)|R|$. Also for $x \in Z(R)$ we have $|R : C_R(x)| =$

1. Therefore at least three quarters of the elements of R satisfy $|R : C_R(x)| \geq 2$. Thus,

$$\Pr(R) = \frac{1}{|R|^2}\sum_{x\in R} |C_R(x)| \leq \frac{1}{4} + \frac{3}{4}\cdot\frac{1}{2} = \frac{5}{8}$$

If $\Pr(R) = 5/8$ then clearly $|R : Z(R)| = 4$. Assume therefore that $|R : Z(R)| = 4$, in which case $R/Z(R)$ is the direct sum of two cyclic groups $\langle Z(R) + a\rangle$ and $\langle Z(R) + b\rangle$. Now each non-central x has centralizer of index 2 in R and so $\Pr(R) = 5/8$ as required. □

The following rings of matrices over $G\mathbb{F}(2)$ show that the bound $\Pr(R) \leq 5/8$ for non-commutative rings is the best possible.

(i) $$\left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

(ii) $$\left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid \forall\ a, b, c \in G\mathbb{F}(2) \right\}$$

The above mentioned result is a special case of the following theorem whose proof is exactly analogous:

Theorem 5.8.4. *Let R be a non-commutative ring and p is the least prime number which divides $|R|$, then*

$$\Pr(R) \leq \frac{p^2 + p - 1}{p^3}.$$

The equality holds if and only if $|R : Z(R)| = p^2$.

Machale also observed that any subring of a finite ring is at least as commutative as the ring itself. This can be express by the following theorem.

Theorem 5.8.5. *If H is a subring of R then* $\Pr(R) \leq \Pr(H)$.

Proof. Since for any r in R, $C_H(r)$ is a subring of $C_R(r)$ it follows that

$$|C_R(r)| \leq |R : H||C_H(r)|.$$

Thus

$$\sum_{r\in R}|C_R(r)| \leq |R : H|\sum_{r\in R}|C_H(r)| = |R : H|\sum_{h\in H}|C_R(h)| \leq |R : H|^2\sum_{h\in H}|C_H(h)|.$$

It follows that $\Pr(R) \leq \Pr(H)$. □

We conclude this chapter and also the dissertation by the following remark.

Remark 5.8.6. Though the notion of commutativity degree of a finite group has been generalized in many different ways yet classification of groups using these generalized notions is far from completion.

Bibliography

[1] F. Barry, D. MacHale and Á. Ní Shé, *Some supersolvability conditions for finite groups*, Math. Proc. of the Royal Irish Acad. **106A** (2) (2006), 163–177.

[2] S. M. Belcastro and G. J. Sherman, *Counting Centralizers in Finite Groups* , Math. Magazine, **67(5)** (1994), 366-374.

[3] P. B. Bhattacharya, S. K. Jain, S. R. Nagpal *"Basic abstract algebra"*, second edition, Cambridge University Press, Cambridge, 1997.

[4] S. Blackburn, *Groups of Prime Power Order with Derived Subgroup of Prime Order*, J. Algebra **219**,(1999) , 625-657.

[5] R. D. Blyth and D. J. S. Robinson, *Recent progress on rewriteability in groups* , *Proceedings of the 1987 Singapore Group Theory conference*, de Gruyter, Berlin, 1989, 77-86.

[6] J. Burns, G. Ellis, D. Machale, P. Ó Murchuú, R. Sheehy and J. Wiegold, *Lower central series of groups with small upper central factors*, Proceedings of the Royal Irish Academy **97A** (1997), 113-122.

[7] W. Burnside, " *Theory of groups of finite order*, Dover Publication, New York, 1955.

[8] M. Curzio, P. Longobardi and M. Maj, *Su di un problema combinatorio in teoria dei gruppi*, Atti. Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur, **8 74** (1983), 136-142.

[9] A. K. Das, *On group elements having square roots*, Bull. Iranian Math. Soc., **31(2)**, (2005), 33-36.

[10] A. K. Das, *On arithmetic functions of finite groups*, Bull. Austral. Math. Soc. **75** (2007), 45–58.

[11] J. D. Dixon, Problem 176, Canad. Math. Bull., **16** (1973), 302.

[12] P. Erdös and P. Turán, *On some problems of a statistical group theory IV*, Acta. Math. Acad. Sci. Hung. **19** (1968), 413–435.

[13] A. Erfanian, R. Rezaei, and P. Lescot, *On the Relative Commutativity Degree of a Subgroup of a Finite Group*, Communications in Algebra, **35:12** (2007), 4183-4197.

[14] P. X. Gallagher, *The number of conjugacy classes in a finite group*, Math. Z. **118** (1970), 175–179.

[15] J. A. Gallian, *"Contemporary Abstract Algebra "*, 2nd edition D. C. Heath, 1990

[16] R. Gluck, K. Magaard, U. Riese, P. Schmid, *The solution of the $k(GV)$-problem* , J. Algebra **279** (2004), 694-719.

[17] R. M. Guralnick, G. R. Robinson, *On the commuting probability in finite groups* , J. Algebra **300** (2006), 509-528.

[18] W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034.

[19] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940), 130-141.

[20] M. Hall, *The Theory of Groups*, "The Macmillan Company", New York, 1967.

[21] D. F. Holt, *The CAYLAY group theory system*, Notices of the American Mathematical Society, **35** (1988). No. 8, 1135-1140.

[22] R. B. Howlett, I. M. Isaacs, *On Groups of Central Type*, Math. Z. **179** (1982), no. 4, 555-569.

[23] I. M. Isaacs, D. S. Passman, *A Characterization of Groups in Terms of the Degree of Their Characters*, Pacific J. Math. **15** (1965), 877-903.

[24] I. M. Isaacs, D. S. Passman, *A Characterization of Groups in Terms of the Degree of Their Characters II*, Pacific J. Math. **24** (1968), 467-510.

[25] I. M. Isaacs, *"Character Theory of Finite Groups"*, Dover Publications, Inc., New YorK, 1994.

[26] N. Itô, *On finite groups with given conjugate types*, Nagita Math. J., **6** (1953), 17-28.

[27] N. Jacobson, *"Basic Algebra I"*, W. H. Freeman and Co., San Francisco, 1974.

[28] K. Joseph, *Several conjectures on commutativity in algebraic structures*, Amer. Math. Monthly **84** (1977), 550–551.

[29] K. S. Joseph, *Commutativity in non-abelian groups.* Ph. D. thesis, University of California, Los Angeles (1969).

[30] L. C. Kappe, R. F. Morse, *On commutators in groups*, Group St Andrews 2005, Vol. 2, 531-558, London Math. Soc. Lecture Note series (No. 340), Cambridge Univ. Press, Cambridge, 2007.

[31] H. Kurzweil, B. Stellmacher, *The Theory of Finite Groups, An Introduction*, "Springer", UTX, New York, 2004.

[32] P. Lescot, *Isoclinism classes and commutativity degrees of finite groups*, J. of Algebra, **177** (1995), 847–869.

[33] P. Lescot, *Central extensions and commutativity degree*, Comm. Algebra, **29(10)** (2001), 4451-4460.

[34] J. L. Leavitt, G. J. Sherman and M. E. Walker, *Rewriteability in finite groups*, Amer. Math. Monthly **99** (1992), 446–452.

[35] F. W. Levi, *Groups in which the commutator operation satisfies certain algebraic conditions*, J. Indian Math. Soc. **(N. S.) 6** (1942), 87-97.

[36] D. MacHale, *How commutative can a non-commutative group be?*, Math.Gaz. LVIII (1974), 199–202.

[37] D. MacHale, *Commutativity in finite rings*, Amer. Math. Monthly **83** (1976), 30–32.

[38] D. Machale and P.Ó Murchuú , *Commutator subgroups of groups with small central factor groups*, Proceedings of the Royal Irish Academy **93A** (1993), 123-9.

[39] G. A. Miller, *Relative number of non-invariant operators in a group* , Proc. Nat. Acad. Sci. USA. **30(2)** (1944), 25-28.

[40] M, R. R. Moghaddam, K. Chiti, A. R. Salemkar, *n-Isoclinism classes and n-nilpotency degree of finite groups*, Algebra Colloquium **12(2)** (2005), 225-261.

[41] M. R. Pournaki, R. Sobhani *Probability that the Commutator of two Group Elements is Equal to a given Element*, J. Pure and Applied Algebra, **212** (2008), 727-734.

[42] J. J. Rotman, *An Introduction to the Theory of Groups*, 3rd edition, Allyn and Bacon, Inc, 1984.

[43] D. J. Rusin, *What is the probability that two elements of a finite group commute?*, Pacific J. Math., **82** (1979), 237–247.

[44] E. Schenkman, *"Group Theory"*, Van Nostrand, Princeton, N. J., 1965.

[45] W. R. Scott, *"Group Theory"*, Dover Publications, Inc., New YorK, 1987.

[46] G. Sherman, *What is the probability an automorphism fixes a group element?*, Amer. Math. Monthly **82** (1975), 261–264.

[47] T. Tambour, *On the number of solutions of some equations in finite groups* Research Reports in Mathematics, Dept. of Mathematics, Stockholm University, 1998.

[48] D. R. Taunt, *On A-Groups*, Proc. Camb. Phil. Soc., **45** (1949), 24-42.

[49] The GAP Group, *GAP - Groups, Algorithms, and Programming*, Version **4.2** Aachen-St Andrews, 1999, available at `http://www-gap.dcs.st-and.ac.uk/ gap`.

BRIEF BIO-DATA

1. Name:	RAJAT KANTI NATH
2. Sex:	Male
3. Date of birth:	2^{nd} February, 1982.
4. Father's Name:	Mr. Bharat Chandra Nath
5. Nationality:	Indian
6. Permanent Address:	Vill - Suripara, P.O. - Dhanpur Dist. - Dhubri, Assam, Pin - 783 337.
7. Academic Qualification:	M. Sc. in Mathematics, Tezpur University.
8. Awards and Achievements:	(i) Gold Medal in M.Sc. (ii) Certificate of Appreciation by Govt. of India.

9. Seminar/Workshop attended:

(i) Symposium on *Some recent advances in Mathematics*, organised by the Department of Mathematics, NEHU Shillong, from 4^{th} to 5^{th} April, 2007.

(ii) North East School on *Computational geometry*, jointly organised by ISI Kolkata, and St. Anthony's College, Shillong, from 1^{st} to 3^{rd} November, 2007.

(iii) Advanced Instructiional School on *Algebraic and analytic number theory*, organised by HRI Allahabad, from 3^{rd} to 28^{th} December, 2007.

(iv) *CMFT Workshop 2008*, organised by IASST Guwahati, from 3^{rd} to 10^{th} January, 2008.