A STUDY OF FINITE GROUPS IN TERMS OF THEIR ORDER CLASSES

SARBANI KONWAR

DEPARTMENT OF MATHEMATICS
NORTH-EASTERN HILL UNIVERSITY
SHILLONG – 793022, INDIA

A STUDY OF FINITE GROUPS IN TERMS OF THEIR ORDER CLASSES

BY

SARBANI KONWAR
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
AUGUST, 2010

CERTIFICATE

I certify that the dissertation entitled "A STUDY OF FINITE GROUPS IN TERMS OF THEIR ORDER CLASSES" submitted by Ms. Sarbani Konwar 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
Email: akdas@nehu.ac.in

Place: Shillong.
10^{th} August, 2010.

NORTH-EASTERN HILL UNIVERSITY

August, 2010

DECLARATION

I, Sarbani Konwar, 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.

Signature of the Candidate

Countersigned by:

Signature of the Head

Signature of the Supervisor

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. K. K. Singh and Dr. S. Dutta, Department of Mathematics, N.E.H.U., 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 support.

I am also thankful to Dr. A. M. Buhphang, 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 Mathematics Department, 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 for giving me constant encouragement and providing me with unbelievable opportunities to continue my studies.

Sarbani Konwar

PREFACE

In 1988, J.P. Zhang [27], in 1989, W. Feit and G.M. Seitz [7], and in 1991, R. W. van der Waall and A. Bensaid [24] independently settled the well-known Syskin problem [17]. Syskin problem asserts that if G is a finite group in which any two elements having the same order are conjugates, then G must be either a trivial group or the cyclic group C_2 or the symmetric group S_3. Since then several authors have investigated similar problems. In 1994, C. Li [15] has studied all finite groups in which any two elements of the same order are conjugates or inverse conjugates. Given a finite group G and an element $x \in G$, the set $OS_G(x) = \{y \in G : o(y) = o(x)\}$ is called the order class of x in G. Most often, when there is no ambiguity, we write $OS(x)$ in place of $OS_G(x)$. Since any two conjugates have the same order, the above mentioned property of a finite group G that any two elements having the same order are conjugates can also be restated by saying that the number of order classes and the number of conjugacy classes are same. In 2006, X. Du and W. Shi [6] have studied all finite groups in which the number of conjugacy classes exceeds the number of order classes by one. Keeping in mind the fact that the size of each conjugacy class divides the order of a finite group, C. E. Finch and L. Jones [8] have considered finite abelian groups in which the size of each order class divides the order of the group and called such groups as groups having perfect order subsets. They demonstrated several methods for the construction of finite abelian groups having perfect order subsets and also established a curious connection between such groups and

Fermat numbers i.e. numbers of the form $2^{2^n}+1$, $n \geq 0$. In 2003, the same authors [9] considered some of their results for finite non-abelian groups also. In 2003, S. Libera and P. Tlucek [16] have also given some examples of finite non-abelian groups having perfect order subsets. Recently A. K. Das [4] considered arbitrary finite groups having perfect order subsets, and obtained some interesting results along with a number of classes of non-abelian finite groups having perfect order subsets using the idea of semidirect product of finite groups.

In Chapter 1, we have collected some basic definitions and some results form the theory of groups which have been used in the forthcoming chapters. We also recall some results from the theory of numbers.

Let σ be a set of primes. A natural number n is called a *σ-number* if n is a product of primes chosen from the set σ. A finite group G is said to be *σ-order conjugate* or *σ-OC* if, whenever a σ-number n is the order of some element of G, all elements of order n are conjugate in G. In particular G is said to be *order conjugate* (or *OC*) if $\sigma \supseteq \pi(G)$, the set of primes dividing the order of G. In Chapter 2, we study some properties of σ-OC and OC-groups. Some of the significant results are given below.

Lemma 2.2.1 *Let G be a σ-OC group. Let x and y be p-elements of G where $p \in \sigma$. Assume that $N \trianglelefteq G$ and in the factor group $\bar{G} = G/N$ the images $\bar{x}$ and $\bar{y}$ have the same order $\neq 1$. Then x and y have the same order.*

Theorem 2.2.2 *If G is a σ-OC group and $N \trianglelefteq G$, then $\bar{G} = G/N$ is also a σ-OC group.*

Lemma 2.3.1 *If G is an OC-group, then G does not have a subgroup N of index two and even order.*

Theorem 2.3.2 *If an OC-group G has a non-trivial subgroup N of index two, then $G \cong S_3$.*

Theorem 2.3.3 *Let G be a σ-OC group. If $C_G(t)$ has a normal Sylow 2-subgroup, then $G \cong C_2$ or S_3.*

Theorem 2.3.4 *The only non-trivial order conjugate groups are C_2 or S_3.*

Let G be a finite group and $x \in G$. consider the order class $OS(x) = \{y \in G : o(y) = o(x)\}$ of x in G. If $|OS(x)|$ divides $|G|$, then G is said to have *perfect order subsets*, or, in short, one says that G is a *POS-group*.

In Chapter 3, we study some properties of POS-groups. Some of the results are given as follows.

Lemma 3.1.2 *If G is a POS-group, then, for every prime divisor p of $|G|$, $(p-1)$ is also a divisor of $|G|$. In particular, every non-trivial POS-group is of even order.*

Given a positive integer n and a prime p, we write $\mathrm{ord}_p\, n$ to denote the largest non-negative integer k such that $p^k \mid n$. $\mathrm{ord}_p\, n$ is called the p-adic order of n.

Proposition 3.1.3 *Let G be a POS-group. Then the odd prime factors (if any) of $|G|$ are of the form $1 + 2^k t$, where $k \leq \mathrm{ord}_2\, |G|$ and t is odd, with the smallest one being a Fermat's prime i.e. a prime of the form $2^{2^n} + 1$, $n \geq 0$.*

Proposition 3.1.4 *Let G be a non-trivial POS-group with $\mathrm{ord}_2\, |G| = \alpha$. If $x \in G$, then the number of distinct odd prime factors in $o(x)$ is at most α. In fact, the bound gets reduces by $(k-1)$ if $\mathrm{ord}_2\, o(x) = k \geq 1$.*

Proposition 3.2.1 *Let G be a finite group. If $|G| = 2k$ where k is an odd positive integer having at least three distinct prime factors, and if all the Sylow subgroups of G are cyclic, then G is not a POS-group.*

Proposition 3.2.2 *Let G be a finite group. If $|G| = 42 \times 43^r$, $r \geq 1$, then G is not a POS-group.*

Theorem 3.2.3 *Let G be a finite non-abelian group and p be a prime divisor of $|G|$. Suppose that $|C_G(x)| = p$ for all $x \in G$. If G has more than one conjugacy class of elements of order p, then G does not have perfect order subsets.*

Proposition 3.3.1 *Let G be a finite group with $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ where $\alpha_1, \alpha_2, \dots, \alpha_k$ are positive integers and $2 = p_1 < p_2 < \dots p_k$ are primes such that $p_k - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $k \geq 2$. If G is a POS-group, then the Sylow p_k-subgroup of G is cyclic.*

Proposition 3.3.2 *Let G be a non-trivial POS-group. Then, the following assertions hold :*

(a) *If $\mathrm{ord}_2 |G| = 1$, then either $|G| = 2$, or 3 divides $|G|$.*

(b) *If $\mathrm{ord}_2 |G| = \mathrm{ord}_3 |G| = 1$, then either $|G| = 6$, or 7 divides $|G|$.*

(c) *If $\mathrm{ord}_2 |G| = \mathrm{ord}_3 |G| = \mathrm{ord}_7 |G| = 1$, then either $|G| = 42$, or there exists a prime $p \geq 77659$ such that $43^2 p$ divides $|G|$.*

Theorem 3.4.1 *Let G be a group such that $G \cong S_3 \times (C_2)^t \times M$, where $t \geq 0$ and M is a cyclic group of odd square-free order not divisible by 3. If G is a POS-group, then G is isomorphic to one of the following three groups:*

(a) S_3

(b) $S_3 \times C_2 \times C_7$

(c) $S_3 \times (C_2)^2 \times C_5$

In Chapter 4, we study some results on abelian POS-groups. Some of the important results are as mentioned below.

Lemma 4.2.1 *Let a, b and t be positive integers with $b \leq a$, and let $G \cong (C_{p^a})^t$, where p is a prime. Then the number of elements in G of order p^b is $(p^{b-1})^t(p^t - 1)$.*

Lemma 4.2.2 *Let p be a prime and M be a finite group (not necessarily abelian) such that $\gcd(p, |M|) = 1$. Let G and $\hat{G}$ be two finite groups such that $G \cong (C_{p^a})^t \times M$ and $\hat{G} \cong (C_{p^{a+1}})^t \times M$, where a and t are positive integers. Suppose that d is the order of an element in $\hat{G}$ and that p^{a+1} does not divide d. Then both G and $\hat{G}$ contain the same number of elements of order d.*

The following result helps in generating an infinite family of POS-groups.

Theorem 4.2.3 (Going-up theorem)

Let p be a prime and M be a finite group (not necessarily abelian) such that $\gcd(p, |M|) = 1$. Let G and $\hat{G}$ be two finite groups such that $G \cong (C_{p^a})^t \times M$ and $\hat{G} \cong (C_{p^{a+1}})^t \times M$, where a and t are positive integers. If G has perfect order subsets, then $\hat{G}$ has perfect order subsets.

Proposition 4.2.4 *Let M be the unique non-abelian group of order 21. Then $C_{2^a} \times M$ is a POS-group for each $a \geq 1$.*

Theorem 4.3.2 (Chopping-off theorem)

Let p be a prime and M be a finite group (not necessarily abelian) such that $\gcd(p, |M|) = 1$. Let G and $\hat{G}$ be two finite groups such that $G \cong C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_{s-1}}} \times (C_{p^{a_s}})^t \times M$ and $\hat{G} \cong (C_{p^{a_s}})^t \times M$, where $a_1 \leq a_2 \leq \cdots \leq a_{s-1} < a_s$ are positive integers. If G has perfect order subsets, then $\hat{G}$ also has perfect order subsets.

Theorem 4.3.3 (Going-down theorem)
Let p be a prime and M be a finite group (not necessarily abelian) such that $\gcd(p, |M|) = 1$. *Let G and $\hat{G}$ be two finite groups such that $G \cong (C_{p^a})^t \times M$, $t \geq 0$ and $\hat{G} \cong (C_p)^t \times M$. If G has perfect order subsets, then $\hat{G}$ also has perfect order subsets.*

Suppose that $G \cong (C_2)^t \times M$, where $|M|$ is odd. Then G is called a *minimal POS-group* if G has perfect order subsets and there is no proper subgroup $\hat{M}$ of M such that $(C_2)^t \times \hat{M}$ has perfect order subsets.

Theorem 4.4.4 *Let G be a finite abelian group of even order whose Sylow p-subgroup is a cyclic group of order p for each odd prime p dividing $|G|$. If G is a minimal POS-group, then G is isomorphic to one of the following nine groups:*

(a) C_2

(b) $(C_2)^2 \times C_3$

(c) $(C_2)^3 \times C_3 \times C_7$

(d) $(C_2)^4 \times C_3 \times C_5$

(e) $(C_2)^5 \times C_3 \times C_5 \times C_{31}$

(f) $(C_2)^8 \times C_3 \times C_5 \times C_{17}$

(g) $(C_2)^{16} \times C_3 \times C_5 \times C_{17} \times C_{257}$

(h) $(C_2)^{17} \times C_3 \times C_5 \times C_{17} \times C_{257} \times C_{131071}$

(i) $(C_2)^{32} \times C_3 \times C_5 \times C_{17} \times C_{257} \times C_{65537}$

In Chapter 5, we give some examples and non-examples of POS-groups. Some of the results are given below:

Theorem 5.2.2 *Let p be a Fermat's prime. Let α, β be two positive integers such that $2^\alpha \geq p-1$. Then there exists a homomorphism $\theta : C_{2^\alpha} \to \mathrm{Aut}(C_{p^\beta})$ such that the semidirect product $C_{2^\alpha} \ltimes_\theta C_{p^\beta}$ is a non-abelian POS-group.*

Theorem 5.3.2 *The dihedral group*

$$D_{2n} = \langle x,\, y \,|\, y^n = 1,\, x^2 = 1,\, xy = y^{-1}x \rangle$$

where $n \geq 2$ is a POS-group if and only if $n = 3^l$, for some $l \geq 1$.

Theorem 5.3.3 *The quasi-dihedral group*

$$QD_n = \langle a,\, b \,|\, a^{2^{m-1}} = 1,\, b^2 = 1,\, ba = a^{2^{m-2}+1}b \rangle$$

where $n \geq 2^m$, $m \geq 4$ is not a POS-group.

Theorem 5.3.4 *The semi-dihedral group*

$$SD_n = \langle s,\, t \,|\, s^{2^{m-1}} = 1,\, t^2 = 1,\, ts = s^{2^{m-2}-1}t \rangle$$

where $n = 2^m$, $m \geq 3$ is not a POS-group.

Theorem 5.4.1 *The generalized quaternion group*

$$Q_n = \langle x,\, y \,|\, x^{2^{m-1}} = 1,\, y^2 = x^{2^{m-2}},\, yx = x^{-1}y \rangle$$

where $n = 2^m$, $m \geq 3$ is not a POS-group.

Theorem 5.5.1 *The special linear group $SL(2, q)$ where $q = p^n$ for some prime p and for some positive integer n is a POS-group if and only if*

$$q \in \{2,\, 3,\, 5,\, 7,\, 9,\, 11,\, 17,\, 19,\, 41,\, 49,\, 127,\, 251\}.$$

Proposition 5.5.4 *The projective special linear group $PSL(2, q)$, where $q > 3$ is prime, do not have perfect order subsets.*

Proposition 5.6.1 *For $n \geq 3$, the alternating group A_n is not a POS-group.*

We conclude with the observation that the theory of POS-groups being a relatively new concept have enough scope for future research.

Contents

Preface **i**

List of symbols **xi**

1 Preliminaries **1**

1.1 Some standard groups 1

1.2 Some topics from the theory of groups 3

1.3 Some additional results 5

1.4 Some results from number theory 6

2 Order classes and their relation to conjugacy classes **8**

2.1 Introduction 8

2.2 σ-order conjugate groups 10

2.3 Order conjugate groups 13

3 Groups having perfect order subsets **19**

3.1 Definition and basic properties 19

3.2 Some conditions for non-POS groups 25

3.3 Some more results on POS-groups 26

3.4 A characterization 32

4 Abelian POS-groups **37**

4.1 Fermat numbers 37

4.2 Infinitude of abelian POS-groups 38

4.3 Existence of minimal POS-groups 41

4.4 Some minimal abelian POS-groups 44

5 Some standard POS and non-POS groups **51**

5.1 Cyclic groups 51

5.2 Semidirect product of cyclic groups 54

5.3 Dihedral groups 60

5.4 Quaternion groups 65

5.5 Linear groups 66

5.6 Alternating group 70

Bibliography **71**

Brief Bio-data **75**

List of Symbols

$\mathbb{Z}$	the set of integers
$\mathbb{N}$	the set of natural numbers
$\operatorname{ord}_p n$	the largest non-negative integer k such that $p^k \mid n$ where p is a prime
$\det(A)$	determinant of a square matrix A
$H \leq G$	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
$\lvert G : H \rvert$	index of H in G
G/N	factor group of G by N
HK	$\{hk \mid h \in H,\ k \in K\}$
$H \times K$	the direct product of the groups H and K
$H \ltimes_\theta K$	the semidirect product of H and K with respect to a homomorphism $\theta : H \to \operatorname{Aut}(K)$
aH	$\{ah \mid h \in H\}$, left coset of H
$G \cong H$	G and H are isomorphic groups
$o(g)$	order of g
$\lvert G \rvert$	order of the group G

y^g	gyg^{-1}, conjugate of y
$\mathrm{C}\ell_G(g)$	conjugacy class of g in G
$k(G)$	number of conjugacy classes of G
$\mathrm{Aut}(G)$	automorphism group of G
$Z(G)$	center of the group G
$C_G(x)$	$\{y \in G : xy = yx\}$, centralizer of x in G
$N_G(H)$	normalizer of a subgroup H in G
$\mathrm{Ker}\,\phi$	kernel of the homomorphism ϕ
$\langle a \rangle$	$\{a^n \mid n \in \mathbb{Z}\}$, the cyclic group generated by a
C_n	cyclic group of order n
D_{2n}	dihedral group of order $2n$
Q_n	quaternion group of order $n = 2^m$, $m \geq 3$, dicyclic group
SD_{2n}	Semi-dihedral group of order $n = 2^m$, $m \geq 3$
QD_n	Quasi-dihedral group of order $n = 2^m$, $m \geq 4$
S_n	symmetric group of degree n
A_n	alternating group of degree n
$GL(n, \mathbb{F})$	$\{A \in M_n(\mathbb{F}) \mid \det(A) \neq 0\}$, the general linear group
$SL(n, \mathbb{F})$	$\{A \in M_n(\mathbb{F}) \mid \det(A) = 1\}$, the special linear group

Chapter 1

Preliminaries

In this chapter we recall some of the basic definitions, notations and conventions from the theory of groups and the theory of numbers, which are used in the forth coming chapters.

1.1 Some standard groups

In this section we recall some standard examples of groups. The groups which play perhaps the most crucial role in this dissertation are the cyclic groups. We write C_n to denote a cyclic group of order n.

(A) The permutation groups

The set of all bijective maps on a set X forms a group under the composition of maps. This group is called the *symmetric group* on X and is denoted by $SymX$. In particular, if $X = \{1, 2, \ldots, n\}$, then $SymX$ is also denoted by S_n and is called the symmetric group of degree n. Clearly, $|S_n| = n!$.

The group of even permutations of n symbols is called the *alternating group of degree* n and is denoted by A_n. The alternating groups of degree greater than or equal to 5 form examples of an important class of groups called the simple groups. Clearly $|A_n| = \frac{n!}{2}$.

(B) The dihedral groups

A *dihedral group* D_{2n} of order $2n$, $n \geq 2$, is the group of all symmetries of a regular polygon with n sides. It is presented as

$$D_{2n} = \langle r,\, f | r^n = 1,\, f^2 = 1,\, fr = r^{-1}f \rangle.$$

A *quasi-dihedral group* of order $n = 2^m$, $m \geq 4$, is presented as

$$QD_n = \langle a,\, b\, | a^{2^{m-1}} = 1,\, b^2 = 1,\, ba = a^{2^{m-2}+1}b \rangle.$$

A *semi-dihedral group* of order $n = 2^m,\ m \geq 3$, is presented as

$$SD_n = \langle s,\, t\, | s^{2^{m-1}} = 1,\, t^2 = 1,\, ts = s^{2^{m-2}-1}t \rangle.$$

(C) The quaternion groups

A *quaternion group* of order $n = 2^m,\ m \geq 3$, is presented as

$$Q_n = \langle x, y\, |\, x^{2^{m-1}} = 1,\ y^2 = x^{2^{m-2}},\ yx = x^{-1}y \rangle.$$

In fact, this is a generalization of the well-known group of quaternions

$$Q_8 = \langle i,\, j,\, k\, |\, i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

(D)The linear groups

Let F be a field. The set of all $n \times n$ invertible matrices with entries from F forms a group under matrix multiplication. This group is known as the

general linear group of degree n over the field F and is denoted by $GL_n(F)$ or $GL(n, F)$. For $n \geq 2$, the group $GL(n, F)$ is non-abelian.

Let F be a field. The set of all $n \times n$ matrices of determinant one with the entries from F forms a group under matrix multiplication. This group is called the *special linear group* over the field F and is denoted by $SL_n(F)$ or $SL(n, F)$. In fact, $SL(n, F)$ is a subgroup of $GL(n, F)$.

SL(2, q) is the group of all 2×2 matrices of determinant one with the entries from the finite field $\mathbb{F}_q$ of q elements, where $q = p^n$ for some prime p and for some positive integer n.

Result 1.1.1. *The cardinality of $SL(2, q)$ is $q(q-1)(q+1)$.*

Result 1.1.2. *The exact number of conjugacy classes in $SL(2, q)$ is $q + 4$ when q is odd, and $q + 1$ when q is even.*

The projective special linear group is the quotient of the group of matrices $SL(n, F)$ by its center. It is denoted by $PSL(n, F)$. The cardinality of $PSL(2, q)$ is $(q+1)(q^2-q)$ when $q = 2^n$ and $\frac{1}{2}(q+1)(q^2-q)$ when $q = p^n$, p is an odd prime and $n \geq 0$.

1.2 Some topics from the theory of groups

(A) Isomorphism theorems

The following theorems play crucial roles in the theory of groups.

Result 1.2.1. (First isomorphism theorem) ([19], page 25) *Let G and H be two groups and $\phi : G \to H$ be a homomorphism with* $\operatorname{Ker} \phi = K$ *. Then K is a normal subgroup of G and $G/K \cong \operatorname{Im} \phi$.*

Result 1.2.2. (Second isomorphism theorem) ([19], page 25) *Let G be a group and let H and N be subgroups of G, and $N \trianglelefteq G$. Then*

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

Result 1.2.3. (Third isomorphism theorem) ([19], page 26) *Let G be a group and $K \subset H \subset G$, where both H and K are normal subgroups of G. Then H/K is a normal subgroup of G/K and*

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

(B) Automorphism groups

An isomorphism of a group G onto itself is called an *automorphism*. The set of all automorphisms of a group G, denoted by $\mathrm{Aut}(G)$, forms a group under composition of maps, called the *automorphism group* of G.

Result 1.2.4. (N/C Theorem) ([20], page 50) *Let H be a subgroup of a group G. Then $N_G(H)/C_G(H)$ is isomorphic to a subgroup of* $\mathrm{Aut}(H)$.

(C) Semidirect product of groups

Let X and H be two groups and $\theta : X \to \mathrm{Aut}(H)$ be a homomorphism. Then the cartesian product $X \times H$ forms a group under the binary operation

$$(x_1, h_1)(x_2, h_2) = (x_1x_2, \theta(x_2)(h_1)h_2),$$

where $x_i \in X$, $h_i \in H$, $i = 1, 2$. This group is known as the *semidirect product* of X and H (with respect to θ) and is denoted by $X \ltimes_\theta H$. If θ is the trivial homomorphism, then $X \ltimes_\theta H$ equals the direct product $X \times H$.

The semidirct product of C_2 and C_3 gives S_3. The dihedral group D_{2n} is isomorphic to a semidirect product of C_2 and C_n.

(D) Sylow's theorems

Let G be a group and p be a prime such that $|G| = p^a m$ where a, $m \in \mathbb{N}$ and $p \nmid m$.Then any subgroup of G of order p^a is called a *Sylow p-subgroup* of G.

The set of all Sylow p-subgroups of G is denoted by $Syl_p(G)$.

Result 1.2.5. (Sylow's first theorem) ([11], page 330) *Let G be a finite group such that $|G| = p^a m$ where a, $m \in \mathbb{N}$ and p is a prime with $p \nmid m$. Then there is a subgroup of G of order p^a.*

Result 1.2.6. (Sylow's second theorem) ([11], page 331) *Let G be a finite group and p be a prime such that p divides $|G|$. If P is a p-subgroup of G and $S \in Syl_p(G)$, then there exists $g \in G$ such that $P \subseteq S^g$.*

Result 1.2.7. (Sylow's third theorem) ([11], page 332) *Let G be a finite group and p be a prime such that p divides $|G|$. If n is a positive integer such that $|S_1 : S_1 \cap S_2| \geq p^n \ \forall S_1, S_2 \in Syl_p(G)$ with $S_1 \neq S_2$, then $|Syl_p(G)| \equiv 1(\mathrm{mod} p^n)$. In particular, we have $|Syl_p(G)| \equiv 1(\mathrm{mod} p)$.*

1.3 Some additional results

Result 1.3.1. ([19], page 40) *The number of conjugates of x in G is $|G : C_G(x)|$ i.e., $|\,\mathrm{C}\ell_G(x)| = |G : C_G(x)|$.*

Result 1.3.2. (Frobenius)([12], page 136) *If n is a divisor of the order of a group G, then the number of solutions of $x^n = 1$ in G is a multiple of n.*

Result 1.3.3. ([18], page 290) *If G is a group all of whose Sylow subgroups are cyclic, then G has a presentation*

$$G = \langle a, b \,|a^m = 1 = b^n, b^{-1}ab = a^r \rangle$$

where $r^n \equiv 1 (\mathrm{mod}\, m)$, m is odd, $0 \leq r < m$, and m and $n(r-1)$ are coprime. Conversely, in a group with such a presentation, all Sylow subgroups are cyclic.

1.4 Some results from number theory

The Goldbach's conjecture says that any integer greater than 3 can be written as a sum of two primes. This conjecture remains unsolved till today. However we have the following result due to J. L. Brown [2] and R. E. Dressler [5].

Result 1.4.1. *Every positive integer, except* 1, 2, 4, 6 *and* 9 *can be written as the sum of distinct odd primes.*

Result 1.4.2. *Let a and m be integers such that $1 \leq a < m$. Then, for any divisor d of m, we have that $\gcd(a, m) = d$ if and only if $\gcd(m-a, m) = d$.*

As immediate consequences of the above result, we have

Result 1.4.3. *Let $n \geq 2$ be an integer. Then the exact number of positive integers m such that $m \leq 2^{n-1} - 1$ with $\gcd(2^n - 1, m) = 1$ is $\dfrac{\phi(2^n - 1)}{2}$.*

Result 1.4.4. *Let $n \geq 1$ be an integer. Then the exact number of positive integers m such that $m \leq 2^{n-1}$ with $\gcd(2^n + 1, m) = 1$ is $\dfrac{\phi(2^n + 1)}{2}$.*

Result 1.4.5. *Let $n \geq 1$ be an integer and p be an odd prime. Then the exact number of positive integers m such that $m \leq \dfrac{p^n - 3}{2}$ with $\gcd(p^n - 1,\, m) = 1$ is $\dfrac{\phi(p^n - 1)}{2}$.*

Result 1.4.6. *Let $n \geq 1$ be an integer and p be an odd prime. Then the exact number of positive integers m such that $m \leq \dfrac{p^n - 1}{2}$ with $\gcd(p^n + 1,\, m) = 1$ is $\dfrac{\phi(p^n + 1)}{2}$.*

Result 1.4.7. *Let $m > 1$ be an integer and suppose that d divides m. Then the number of positive integers $k < m$ such that $\gcd(m,\, k) = d$ is $\phi(\frac{m}{d})$.*

Result 1.4.8. *If d divides m and $\phi(m)$ divides $2m$, then $\phi\left(\frac{m}{d}\right)$ divides $2m$.*

Result 1.4.9. *Let $m = \prod_{i=1}^{t} p_i^{a_i}$. Then $\dfrac{2m}{\phi(m)}$ is an integer if and only if exactly one of the following is true:*

(a) *$t = 1$, $p_1 = 2$; so that $m = 2^a$.*

(b) *$t = 1$, $p_1 = 3$; so that $m = 3^b$.*

(c) *$t = 2$, $p_1 = 2$ and $p_2 = 3$; so that $m = 2^a 3^b$.*

(d) *$t = 2$, $p_1 = 2$ and $p_2 = 5$; so that $m = 2^a 5^b$.*

(e) *$t = 3$, $p_1 = 2$, $p_2 = 3$ and $p_3 = 7$; so that $m = 2^a 3^b 7^c$.*

with all exponents positive.

Chapter 2

Order classes and their relation to conjugacy classes

In this chapter, we make an elaborate study on a particular type of maximal subsets of a given finite group, called the order classes, in each of which all the elements are of equal order. We also study some of the properties of the finite groups in which these order classes coincide with the conjugacy classes.

2.1 Introduction

Let G be a finite group and $x \in G$. Then, the set

$$OS_G(x) = \{y \in G : o(y) = o(x)\}$$

is called the *order subset* of G containing x, or, the *order class* of x in G. Most often, when there is no ambiguity, we write $OS(x)$ in place of $OS_G(x)$.

For example, in $S_3 = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$, we have

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

Thus, an order class of G is a maximal subset of G in which all the elements are of the same order.

On the other hand, the set

$$\mathrm{C}\ell_G(x) = \{y \in G : y = gxg^{-1} \text{ for some } g \in G\}$$

is called the *conjugacy class* of x in G. Thus, a conjugacy class is a maximal subset of G in which all the elements are conjugate to each other. Clearly, any two elements of G, which are conjugate to each other, have the same order. Therefore, it follows that each order class of G is a union of certain conjugacy classes of G.

If any two elements of G having the same order are conjugate in G, or, in other words, if each order class of G is a conjugacy class of G, then G is either a trivial group or C_2 or S_3. This is often referred to as Syskin problem, and is mentioned as a well known problem in [17]. This problem remained unsolved for a long period of time. In 1988, J.P. Zhang [27] and in 1989, W. Feit and G. M. Seitz [7] independently settled the problem. Since then several authors have investigated similar problems.

In 1994, C. Li [15] has characterized all finite groups in which any two elements of the same order are conjugate or inverse conjugate (that is, one

is conjugate to the inverse of the other). In other words, Li considered those finite groups G in which $OS(x) = \mathrm{C}\ell_G(x) \cup \mathrm{C}\ell_G(x^{-1})$ for all $x \in G$.

In 2006, X. Du and W. Shi [6] have classified all finite groups in which the number of conjugacy classes exceeds the number of order classes by one. Since each order class of G is a union of certain conjugacy classes of G, there exists a non-negative integer k such that $k(G) = |\pi_e(G)| + k$, where $k(G)$ is the number of conjugacy classes of G, and $\pi_e(G)$ is the set of the orders of the elements of G. Du and Shi called such groups as $co(k)$ groups and characterized all $co(1)$ groups. Clealy, $co(0)$ groups are the ones discussed in the Syskin problem.

In 2007, X. You, G. Qian and W. Shi [26], investigated finite groups in which elements of the same order outside the center are conjugate. They proved that there does not exist a finite non-abelian group with non-trivial center in which elements of the same order outside the center are conjugate.

P. Fitzpatrick [10] has also studied some of properties of the groups in which any two elements of the same order are conjugate. We discuss this in the forthcoming sections.

2.2 σ-order conjugate groups

Let σ be a set of primes. A natural number n is called a *σ-number* if n is a product of primes chosen from the set σ.

A finite group G is said to be a *σ-order conjugate* group, or, simply a *σ-OC* group if, for each σ-number $n \in \pi_e(G)$, all the elements of order n in G are conjugate to each other. Here, as mentioned in Section 2.1, $\pi_e(G)$

denotes the set of the orders of the elements of G.

Given a prime p, an element $x \in G$ is called a *p-element* if $o(x)$ is a power of p. More generally, an element $x \in G$ is called a *σ-element* if $o(x)$ is a σ-number.

Lemma 2.2.1. *Let G be a σ-OC group. Let x and y be p-elements of G where $p \in \sigma$. Assume that $N \trianglelefteq G$ and in the factor group $\bar{G} = G/N$ the images $\bar{x}$ and $\bar{y}$ have the same order $\neq 1$. Then x and y have the same order.*

Proof. Let $o(x) = p^{n+r}$ and $o(y) = p^n$, where $r > 0$. Then

$$\begin{aligned} o(x^{p^r}) &= \frac{o(x)}{\gcd(o(x), p^r)} \\ &= \frac{p^{n+r}}{\gcd(p^{n+r}, p^r)} \\ &= p^n. \end{aligned}$$

Since G is a σ-OC group, we have

$$\begin{aligned} &(x^{p^r})^g = y \text{ for some } g \in G \\ \Rightarrow\ & g^{-1}x^{p^r}g = y \\ \Rightarrow\ & g^{-1}Nx^{p^r}NgN = yN \\ \Rightarrow\ & (\bar{x}^{p^r})^{\bar{g}} = \bar{y}. \end{aligned}$$

But

$$o(\bar{x}^{p^r}) = \frac{o(\bar{x})}{\gcd(o(\bar{x}), p^r)} = \frac{o(\bar{y})}{\gcd(o(\bar{y}), p^r)} < o(\bar{y}).$$

This contradiction shows that $o(x) = o(y)$. □

Theorem 2.2.2. *If G is a σ-OC group and $N \trianglelefteq G$, then $\bar{G} = G/N$ is also a σ-OC group.*

Proof. Let $\bar{x}, \bar{y} \in \bar{G}$ be σ-elements of the same order ${p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}$, where not all the α_i are zero.

Let $o(x) = mn$ where $\gcd(p_i, n) = 1$ for each i and m involves only the primes $p_1, p_2, \dots, p_k$. So there exist integers a and b such that $am + bn = 1$. Hence we have $\bar{x}^{bn} = \bar{x}$. So x^{bn} is a preimage of $\bar{x}$ whose order has the required form.

Let $o(x) = {p_1}^{\beta_1}{p_2}^{\beta_2} \dots {p_k}^{\beta_k}$ and $o(y) = {p_1}^{\gamma_1}{p_2}^{\gamma_2} \dots {p_k}^{\gamma_k}$. We have $\beta_i \geq \alpha_i$ and $\gamma_i \geq \alpha_i$ for all i, since $o(\bar{x})$ divides $o(x)$. Also let $c = {p_2}^{\beta_2}{p_3}^{\beta_3} \dots {p_k}^{\beta_k}$ and $d = {p_2}^{\gamma_2}{p_3}^{\gamma_3} \dots {p_k}^{\gamma_k}$. So

$$\begin{aligned} o(x^c) &= \frac{o(x)}{\gcd(o(x), c)} \\ &= \frac{{p_1}^{\beta_1}{p_2}^{\beta_2} \dots {p_k}^{\beta_k}}{\gcd({p_1}^{\beta_1}{p_2}^{\beta_2} \dots {p_k}^{\beta_k}, {p_2}^{\beta_2}{p_3}^{\beta_3} \dots {p_k}^{\beta_k})} \\ &= {p_1}^{\beta_1}. \end{aligned}$$

Similarly $o(y^d) = {p_1}^{\gamma_1}$. Then

$$\begin{aligned} o(\bar{x^c}) = o(\bar{x}^c) &= \frac{o(\bar{x})}{\gcd(o(\bar{x}, c))} \\ &= \frac{{p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}}{gcd({p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}, {p_2}^{\alpha_2} \dots {p_k}^{\alpha_k})} \\ &= \frac{{p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}}{{p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}} \\ &= {p_1}^{\alpha_1} \end{aligned}$$

Similarly, $o(\bar{y^d}) = o(\bar{y}^d) = {p_1}^{\alpha_1}$. So by lemma 2.2.1, x^c and y^d have the same order. Hence $\beta_1 = \gamma_1$. Hence the theorem follows. □

Lemma 2.2.3. *If G is a σ-OC group and $N \trianglelefteq G$, then N contains all the σ-elements of any order dividing the order of a σ-element of N.*

Proof. Let $a \in N$ be a σ-element and $o(a) = n$. Let x be a σ-element of G and $o(x)$ divides $o(a)$. Suppose that $o(x) = m$. So $n = ms$ for some $s \in \mathbb{N}$. Then $o(a^s) = m$. Hence a^s and x have same order. Since G is σ-OC, we have a^s is conjugate to x. Also $a^s \in N$. Hence $x \in N$. This completes the proof. □

2.3 Order conjugate groups

In the previous section, we have studied some properties of the σ-order conjugate groups, where σ is a set of primes. If, in particular, $\sigma \supseteq \pi(G)$, the set of primes dividing the order of G, then G is called an *order conjugate* group, or, simply an *OC* group. In this section, we study some of the properties of *OC* groups and also some of the particular cases of the famous Syskin problem.

Lemma 2.3.1. *Let G be an OC group. Then G does not have a subgroup N of index two and even order.*

Proof. Suppose that $|G : N| = 2$ and $|N|$ is even. Let $g \in G \setminus N$. Since $|G : N| = 2$, we have

$$g^2 N = N$$
$$\Rightarrow g^2 \in N.$$

Now consider the product $N\langle g\rangle$. We have $N \lneq N\langle g\rangle \leq G$. Since $g \notin N$, $N\langle g\rangle \neq N$. Also $|G : N| = 2$. So we must have

$$N\langle g\rangle = G. \tag{2.3.a}$$

Now since G is a OC group, g is conjugate to its inverse g^{-1}. Hence there exists $u \in G$ such that $ugu^{-1} = g^{-1}$.

Now by (2.3.a), we have $u = ng^i$ where $n \in N$. So

$$\begin{aligned} & ng^i g(ng^i)^{-1} = g^{-1} \\ \Rightarrow\ & ng^i gg^{-i}n^{-1} = g^{-1} \\ \Rightarrow\ & ngn^{-1} = g^{-1}. \end{aligned}$$

So we have

$$ng = g^{-1}n. \tag{2.3.b}$$

For $t \in \mathbb{N}$,

$$\begin{aligned} (ng)^{2t} &= ((ng)(ng))^t \\ &= (ngg^{-1}n)^t, \qquad \text{by (2.3.}b\text{)} \\ &= n^{2t}. \end{aligned}$$

Hence $(ng)^s = n^s$ for any even number s. Also

$$\begin{aligned} (ng)^{2t+1} &= (ng)^{2t}(ng) \\ &= n^{2t}ng \\ &= n^{2t+1}g. \end{aligned}$$

Again

$$\begin{aligned}(ng)^{2t+1} &= (ng)(ng)^{2t} \\ &= ngn^{2t}.\end{aligned}$$

So

$$ngn^{2t} = n^{2t+1}g. \tag{2.3.c}$$

If $o(ng) = 2r + 1$, then

$$\begin{aligned}&(ng)^{2r+1} = 1 \\ \Rightarrow\ &n^{2r+1} = 1 \\ \Rightarrow\ &g = n^{-(2r+1)} \in N,\end{aligned}$$

which is a contradiction. So $o(ng)$ must be even. Let $o(n) = 2i$ and let $o(ng) = 2j$. Then

$$\begin{aligned}&n^{2i} = 1 \\ \Rightarrow\ &(ng)^{2i} = 1 \\ \Rightarrow\ &2j \leq 2i.\end{aligned}$$

Also

$$\begin{aligned}&(ng)^{2j} = 1 \\ \Rightarrow\ &n^{2j} = 1 \\ \Rightarrow\ &2i \leq 2j.\end{aligned}$$

Hence $o(ng) = 2j = o(n)$. Suppose that $o(n) = 2i + 1$. Then $n^{2i+1} = 1$ and $(ng)^{2i+1} = g$. Now

$$\begin{aligned} & ngn^{-1} = (ng)n^{2i} \\ \Rightarrow\ & ngn^{-1} = g, \quad \text{using } 2.3.c \\ \Rightarrow\ & g^{-1} = g, \qquad \text{using } 2.3.b \\ \Rightarrow\ & o(g) = 2. \end{aligned}$$

Since $g \in G \setminus N$ is a 2 element, by lemma 2.2.3, g has larger order than any 2 element of N. So if m is a 2 element of N, then $o(m) < o(g) = 2$. But $|N|$ is even, so there exists $x \in N$ such that $o(x) = 2$. This is a contradiction. Thus $o(n) = o(ng) = k$ where k is even. Since G is a OC group, n is conjugate to ng and so $ng \in N$, which means that $g \in N$. This is a contradiction. So our assumption was wrong. Hence the lemma follows. □

Fitzpatrick [10] has proved some particular cases of Syskin problem which are as follows:

Theorem 2.3.2. *If an OC group G has a non-trivial subgroup N of index two, then $G \cong S_3$.*

Proof. By the lemma 2.3.1, we have $\mid N \mid$ is odd. Let $t \in G \setminus N$. Then $t^2 \in N$. Suppose that $o(t) = 2r$ where r is odd. If $t \in C_G(x)$ for some $x \in N,\ x \neq 1$, then $|C_G(x)| = 2$. So by theorem 1.2.4, we have

$$\begin{aligned} & \left| \frac{N_G(< x >)}{C_G(x)} \right| = \text{odd} \\ \Rightarrow\ & |\operatorname{Aut} < x > | = \text{odd} \\ \Rightarrow\ & \phi(| < x > |) = \text{odd}, \end{aligned}$$

which is a contradiction. Thus

$$\begin{aligned} & t \notin C_G(x) \ \forall x \in N, \ x \neq 1 \\ \Rightarrow & txt^{-1} \neq x \ \forall x \in N, \ x \neq 1. \end{aligned}$$

But $t\,t^2t^{-1} = t^2 \in N$. So we must have $t^2 = 1$. Hence $o(t) = 2$.

Let $x \in N$. Then

$$\begin{aligned} & tx \in G \setminus N \\ \Rightarrow & (tx)^2 = 1 \\ \Rightarrow & txtx = 1 \\ \Rightarrow & txt = x^{-1} \\ \Rightarrow & txt^{-1} = x^{-1}. \end{aligned}$$

Let x, $y \in N$. Then

$$\begin{aligned} & t(xy)t = (xy)^{-1} \\ \Rightarrow & (txt)(tyt) = y^{-1}x^{-1} \\ \Rightarrow & x^{-1}y^{-1} = y^{-1}x^{-1} \\ \Rightarrow & yx = xy. \end{aligned}$$

Hence N is abelian. Suppose that $|N| \neq 3$. Then there exist x, $y \in N$ such that $x \neq y^{-1}$, $x \neq y$ and $o(x) = o(y)$. So $gxg^{-1} = y$ for some $g \in G$. Since $x \neq y$ and N is abelian we have $g \in G \setminus N$. But then $gxg^{-1} = x^{-1}$. Thus it follows that $y = x^{-1}$ which is again a contradiction. Hence $|N| = 3$ and so $|G| = 6$. Since G is non-abelian, we have $G \cong S_3$. □

Theorem 2.3.3. *Let G be an OC group. If for any involution t in G the centralizer $C_G(t)$ has a normal Sylow 2-subgroup, then $G \cong C_2$ or S_3.*

Proof. Suppose that $t \in Z(S)$ where $S \in Syl_2(G)$. Then $ts = st$ for all $s \in S$. So $s \in C_G(t)$. Hence S is a subgroup of $C_G(t)$ and by hypothesis, $S \trianglerighteq C_G(t)$. By lemma 2.2.1, $\frac{C_G(t)}{S}$ is a $2'$-OC group, of odd order which must be trivial and so $C_G(t) = S$. Now G is a group in which the centralizer of every involution is a 2-group. Suzuki [22] has classified such groups and none of them is OC. Hence $G \cong C_2$ or S_3. □

Theorem 2.3.4. *The only non-trivial order conjugate groups are C_2 or S_3.*

Proof. Let G be an OC group. If G is abelian, then we have $G \cong C_2$. Suppose that G is non-abelian. If G is alternating or of Lie type, then G is not OC by known properties of such groups. If G is sporadic, then from Syskin [23] we have G is not OC. Hence we have $G \cong S_3$. □

R. W. van der Waall and A. Bensaid [24] also have proved the Syskin problem in 1991 by using classification of simple groups. R. W. van der Waal has further classified all finite groups [25] whose subgroups of equal order are conjugate and also all groups whose abelian subgroups of equal order are conjugate.

Chapter 3

Groups having perfect order subsets

In this chapter we study the finite groups whose order is divisible by the size of each of its order classes. This chapter is based on the work of C. E. Finch and L. Jones [9] and A. K. Das [4].

3.1 Definition and basic properties

Let G be a finite group. As mentioned in Chapter 2, the order class of an element $x \in G$ is defined as $OS(x) = \{y \in G : o(y) = o(x)\}$. The group G is said to have *perfect order subsets*, or, G is said to be a *POS-group* if $|OS(x)|$ divides $|G|$ for all $x \in G$.

For example, in $S_3 = \{(1), (1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$, we have the following table.

Element order	Cardinality of order subset
1	1
2	3
3	2

It follows that S_3 is a POS-group.

Again consider $C_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Then we have,

Element order	Cardinality of order subset
1	1
2	1
3	2
6	2

So C_6 has perfect order subsets.

Property of having perfect order subsets is not necessarily passed on to subgroups. For example, A_3 is a subgroup of S_3 and S_3 has perfect order subsets but A_3 has no perfect order subsets.

The finite groups that are not POS-groups are often referred to as non-POS-groups.

Lemma 3.1.1. *For each $x \in G$, $|OS(x)|$ is a multiple of $\phi(o(x))$.*

Proof. Define a relation $\sim$ on G by $a \sim b$ if a and b generate the same cyclic subgroup of G, that is, $< a >=< b >$. Now we show that $\sim$ is an equivalence relation on G.

(a) Reflexivity : Clearly $a \sim a$ for all $a \in G$..

(b) Symmetry : Let a, $b \in G$ be such that $a \sim b$. Then

$$< a > =< b >$$
$$\Rightarrow < b > =< a >$$
$$\Rightarrow \ b \sim a$$

(c) Transitivity : Let $a, b, c \in G$ be such that $a \sim b$ and $b \sim c$. Then $< a >=< b >$ and $< b >=< c >$. So

$$< a > =< c >$$
$$\Rightarrow \ a \sim c$$

Hence $\sim$ is an equivalence relation on G.

Now

$$\begin{aligned}[a] &= \{b \in G : a \sim b\} \\ &= \{b \in G :< a >=< b >\} \\ &= \text{Set of all generators of} < a >\end{aligned}$$

So it follows that $|[a]| = \phi(o(a))$ and for all $y \in [a]$, $o(a) = o(y)$.

Therefore for all $x \in G$ and for all $a \in OS(x)$, we have

$$[a] \subset OS(x)$$

Also we have,

$$OS(x) = \bigsqcup [a] \quad \text{where a is the representative of each equivalence class in } OS(x).$$

$$\begin{aligned} \Rightarrow \mid OS(x) \mid &= \underbrace{\mid [a] \mid + \mid [a] \mid + \cdots \mid [a] \mid}_{k \text{ times}} \\ &= k \mid [a] \mid \\ &= k\phi(o(x)) \end{aligned}$$

Hence the lemma follows. □

Proposition 3.1.2. *If G is a POS-group, then, for every prime divisor p of $|G|$, $(p-1)$ is also a divisor of $|G|$. In particular, every non-trivial POS-group is of even order.*

Proof. Suppose that G is a POS-group and it is non-trivial. Then there exists a prime p dividing $|G|$. Now by Cauchy's theorem, G has an element x of order p. By the proposition 3.1.1, $\phi(o(x))$ divides $|OS(x)|$ which implies $\phi(p) = p - 1$ divides $|OS(x)|$. Since G is a POS-group, $|OS(x)|$ divides $|G|$. So $p - 1$ divides $|G|$.

For the second part note that if $p = 2$, then there is nothing to prove. Let p be odd. Then $p - 1$ is even, i.e. $p - 1 = 2m$ for some $m \in \mathbb{N}$. Now, by the first part, $p - 1$ divides $|G|$. So 2 divides $|G|$. Therefore $|G|$ is even. □

Given a positive integer n and a prime p, we write $\text{ord}_p\, n$ to denote the largest non-negative integer k such that $p^k \mid n$. $\text{ord}_p\, n$ is called the p-adic order of n.

Proposition 3.1.3. *Let G be a POS-group. Then the odd prime factors (if any) of $|G|$ are of the form $1 + 2^k t$, where $k \leq \operatorname{ord}_2 |G|$ and t is odd, with the smallest one being a Fermat's prime.*

Proof. Let p be an odd prime factor of $|G|$. Then $p-1$ is even. Suppose that k is the largest non-negative integer s.t. 2^k divides $p-1$ and n is the largest non-negative integer s.t. 2^n divides $|G|$.

Let $p-1 = 2^k t$ where t is odd. Then $p = 1 + 2^k$. We have by proposition 3.1.2, $(p-1)$ divides $|G|$. So 2^k divides $|G|$. Also 2^n is the highest power of 2 dividing $|G|$. Hence $k \leq n$ and therefore $k = \operatorname{ord}_2(p-1) \leq \operatorname{ord}_2 |G|$. Hence $p = 1 + 2^k t$ where t is odd and $k \leq \operatorname{ord}_2 |G|$. Now if $t = 1$, then $p = 1 + 2^k$. Since p is a prime, k is a power of 2. Hence p is a Fermat's prime. □

Proposition 3.1.4. *Let G be a non-trivial POS-group with $\operatorname{ord}_2 |G| = \alpha$. If $x \in G$, then the number of distinct odd prime factors in $o(x)$ is at most α. In fact, the bound gets reduces by $(k-1)$ if $\operatorname{ord}_2 o(x) = k \geq 1$.*

Proof. Suppose that $o(x) = 2^k n$, $k \geq 0$ and n has r distinct odd prime factors. Let $n = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r}$. Then

$$\begin{aligned}
\phi(n) &= p_1^{t_1} p_2^{t_2} \dots p_r^{t_r} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \\
&= p_1^{t_1} p_2^{t_2} \dots p_r^{t_r} \frac{(p_1 - 1)(p_2 - 1) \dots (p_r - 1)}{p_1 p_2 \dots p_r} \\
&= p_1^{t_1 - 1} p_2^{t_2 - 1} \dots p_r^{t_r - 1} (p_1 - 1)(p_2 - 1) \dots (p_r - 1).
\end{aligned}$$

Now $p_1, p_2, \dots, p_r$ are odd primes. So $(p_1 - 1), (p_2 - 1), \dots, (p_r - 1)$ are even.

Let $(p_1-1)(p_2-1)\dots(p_r-1) = 2^r m$. Then $\phi(n) = p_1^{t_1-1}p_2^{t_2-1}\dots p_r^{t_r-1}$. So

$$\begin{aligned}
&\phi(n) = p_1^{t_1-1}p_2^{t_2-1}\dots p_r^{t_r-1}2^r m \\
\Rightarrow\quad & 2^r \mid \phi(n) \\
\Rightarrow\quad & 2^r \mid \phi(o(x)).
\end{aligned}$$

Since G is a POS-group, by proposition 3.1.2, 2^r divides $|G|$. But $\operatorname{ord}_2 |G| = \alpha$. Hence $r \leq \alpha$. So the number of distinct odd prime factors in $o(x)$ is at most α.

For the second part, suppose that $\operatorname{ord}_2 |G| = k \geq 1$. Then by the first part, $o(x) = 2^k$ where $n = p_1^{t_1}p_2^{t_2}\dots p_r^{t_r}$; $p_1, p_2, \dots, p_r$ are odd primes.

Now

$$\begin{aligned}
\phi(o(x)) &= \phi(2^k n) \\
&= \phi(2^k)\phi(n) \\
&= (2^k - 2^{k-1})(2^r m p_1^{t_1-1}p_2^{t_2-1}\dots p_r^{t_r-1}) \\
&= 2^{r+k-1}(m p_1^{t_1-1}p_2^{t_2-1}\dots p_r^{t_r-1}).
\end{aligned}$$

So 2^{r+k-1} divides $\phi(o(x))$. Hence

$$\begin{aligned}
& r + k - 1 \leq \alpha \\
\Rightarrow\ & r \leq \alpha - (k-1).
\end{aligned}$$

This completes the proof. □

3.2 Some conditions for non-POS groups

In this section we study some conditions under which a finite group cannot have perfect order subsets.

Proposition 3.2.1. *Let G be a finite group. If $|G| = 2k$ where k is an odd positive integer having at least three distinct prime factors, and if all the Sylow subgroups of G are cyclic, then G is not a POS-group.*

Proof. G has the following presentation

$$G =< x, y : x^m = 1 = y^n,\ xyx^{-1} = y^r >$$

Where $0 \leq r < m$, $r^n \equiv 1 (\mathrm{mod}\, m)$, m is odd, $\gcd(m, n(r-1)) = 1$ and $mn = 2k$. Clearly at least one of m and n is divisible by two distinct odd primes. So, $o(x)$ and $o(y)$ is divisible by at least two distinct odd primes. So by proposition 3.1.4, G is not a POS-group. □

Proposition 3.2.2. *Let G be a finite group. If $|G| = 42 \times 43^r,\ r \geq 1$, then G is not a POS-group.*

Proof. Suppose that G is a POS-group. Given that $|G| = 2 \times 3 \times 7 \times 43^r,\ r \geq 1$. Since G is a POS-group, by proposition 3.3.1, the Sylow 43-subgroup of G is cyclic. We have all Sylow subgroups of G are Cyclic. Also $|G|$ is a product of three distinct odd prime factors. By proposition 3.2.1, G is not a POS-group. This is a contradiction. Hence G is not a POS-group. □

The following theorem due to C. E. Finch and L. Jones [9] gives us a criterion to eliminate some more non-abelian groups which do not have perfect order subsets.

Theorem 3.2.3. *Let G be a finite non-abelian group and let p be a prime divisor of $|G|$. Suppose that $|C_G(x)| = |\{y \in G : xy = yx\}| = p$ for all $x \in G$. If G has more than one conjugacy class of elements of order p, then G does not have perfect order subsets.*

Proof. Let N be the number of conjugacy classes of elements in G of order p. Since $|C_G(x)| = p$, for every element x in G of order p, we have

$$Cl(x) = \frac{|G|}{|C_G(x)|} = \frac{|G|}{p}.$$

Thus the total number of elements of order p in G is $\frac{N|G|}{p}$. If G has perfect order subsets, then, for some $k \in \mathbb{N}$, we have

$$\begin{aligned} \frac{N|G|}{p}k &= |G| \\ \Rightarrow \quad Nk &= p \\ \Rightarrow \quad N &= p, \end{aligned}$$

which is impossible as $N \geq 2$. So G does not have perfect order subsets. □

3.3 Some more results on POS-groups

In this section we study some more results on finite groups having perfect order subsets.

Proposition 3.3.1. *Let G be a finite group with $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ where $\alpha_1, \alpha_2, \dots \alpha_k$ are positive integers and $2 = p_1 < p_2 < \dots p_k$ are primes such that $p_k - 1 = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, $k \geq 2$. If G is a POS-group, then the Sylow p_k-subgroup of G is cyclic.*

Proof. By Sylow's first theorem, G has a Sylow p_k-subgroup. By Sylow's third theorem, the number of Sylow p_k-subgroups are $1 + tp_k$ where $t \in \mathbb{N} \cup \{0\}$. Now

$$\begin{aligned}
&(1 + tp_k) \mid |G| \\
\Rightarrow &(1 + tp_k) \mid p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \\
\Rightarrow &(1 + tp_k) \mid p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{k-1}^{\alpha_{k-1}}, \quad \text{since } \gcd(1 + tp_k, p_k) = 1 \\
\Rightarrow &(1 + tp_k) \mid (p_k - 1) \\
\Rightarrow &(1 + tp_k) \leq (p_k - 1) \\
\Rightarrow &0 < 2 \leq (1 - t)p_k \\
\Rightarrow &(1 - t) > 0, \qquad \text{since } p_k > 0 \\
\Rightarrow &1 > t \\
\Rightarrow &t = 0.
\end{aligned}$$

So G has a unique Sylow p_k-subgroup, say P. Hence every element of G, of order a power of p_k, lies in P.

Let $m_i = |\{x \in G : o(x) = p_k^i,\ 1 \leq i \leq \alpha_k\}|$. Then by lemma 3.1.1, $\phi(p_k^i)$ divides m_i. Hence, for some integer $x_i \geq 0$, we have

$$\begin{aligned}
m_i &= \phi(p_k^i) x_i \\
&= p_k^{i-1}(p_k - 1) x_i
\end{aligned}$$

Since G is a POS-group, we have

$$\begin{aligned}
& m_i \mid |G| \\
\Rightarrow\ & p_k^{i-1}(p_k-1)x_i \mid p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{k-1}^{\alpha_{k-1}}p_k^{\alpha_k} \\
\Rightarrow\ & p_k^{i-1}(p_k-1)x_i r = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_{k-1}^{\alpha_{k-1}}p_k^{\alpha_k} \qquad \text{for some } r \in \mathbb{N} \\
\Rightarrow\ & p_k^{i-1}(p_k-1)x_i r = (p_k-1)p_k^{\alpha_k} \\
\Rightarrow\ & p_k^{i-1}x_i r = p_k^{\alpha_k} \\
\Rightarrow\ & x_i r = p_k^{\alpha_k-i+1}.
\end{aligned}$$

So

$$x_i \mid p_k^{\alpha_k-i+1} \tag{3.3.a}$$

whenever $x_i \neq 0,\ 1 \leq i \leq k$. Now

$$\begin{aligned}
& \sum_{i=1}^{\alpha_k} m_i = |P| - 1 \\
\Rightarrow\ & \sum_{i=1}^{\alpha_k} p_k^{i-1}(p_k-1)x_i = p_k^{\alpha_k} - 1 \\
\Rightarrow\ & \sum_{i=1}^{\alpha_k} p_k^{i-1}x_i = \frac{p_k^{\alpha_k}-1}{p_k-1} \\
\Rightarrow\ & \sum_{i=1}^{\alpha_k} p_k^{i-1}x_i = \sum_{i=1}^{\alpha_k} p_k^{i-1}.
\end{aligned}$$

So we have

$$\sum_{i=1}^{\alpha_k} p_k^{i-1}(x_i-1) = 0. \tag{3.3.b}$$

From the above equation, we get

$$\begin{aligned}
& p_k \mid (x_1 - 1) \\
\Rightarrow\ & x_1 \equiv 1 (\mathrm{mod} p_k).
\end{aligned}$$

So by (3.3.a), we have $x_1 = 1$. Then from (3.3.b) we get

$$\sum_{i=2}^{\alpha_k} p_k^{i-1}(x_i - 1) = 0.$$

Repeating the above process inductively, we get

$$\begin{aligned} & x_1 = x_2 = \cdots = x_{\alpha_k} = 1 \\ \Rightarrow \quad & m_{\alpha_k} = p_k^{\alpha_k - 1}(p_k - 1) \neq 0. \end{aligned}$$

Hence P is cyclic. □

Proposition 3.3.2. *Let G be a non-trivial POS-group. Then, the following assertions hold :*

(a) *If* $\operatorname{ord}_2 |G| = 1$, *then either* $|G| = 2$, *or* 3 *divides* $|G|$.

(b) *If* $\operatorname{ord}_2 |G| = \operatorname{ord}_3 |G| = 1$, *then either* $|G| = 6$, *or* 7 *divides* $|G|$.

(c) *If* $\operatorname{ord}_2 |G| = \operatorname{ord}_3 |G| = \operatorname{ord}_7 |G| = 1$, *then either* $|G| = 42$, *or there exists a prime* $p \geq 77659$ *such that* $43^2 p$ *divides* $|G|$.

Proof. Since G is a non-trivial POS-group, by proposition 3.1.2, $|G|$ is even. So let $|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ where $k \geq 1,\ 2 = p_1 < p_2 < \ldots < p_k$ are primes, and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers.

Now for all $i = 1, 2, \ldots, k$ we have $\gcd(p_i, p_i - 1) = 1$. Also by proposition 3.1.2, we have, $(p_i - 1)$ divides $|G|$, $\ i = 1, 2, \ldots, k$.

(a) If $k = 1$, then $|G| = p_1^{\alpha_1} = 2$, since $\alpha_1 = 1$.

Now suppose that $k \geq 2$. We have $|G| = 2\, p_2^{\alpha_2}\, p_3^{\alpha_3} \ \ldots\ p_k^{\alpha_k}$, since $\alpha_1 = 1$.

Also

$$\begin{aligned}
&(p_2 - 1) \mid |G| \\
\Rightarrow\ &(p_2 - 1) \mid 2\, p_2^{\alpha_2}\, p_3^{\alpha_3}\, \ldots\, p_k^{\alpha_k} \\
\Rightarrow\ &(p_2 - 1) \mid 2, \quad \text{since } p_3, \ldots p_k \text{ are odd primes and } (p_2 - 1) \text{ is even} \\
\Rightarrow\ &p_2 - 1 = 2, \quad \text{since } p_2 > p_1 = 2 \\
\Rightarrow\ &p_2 = 3.
\end{aligned}$$

Hence 3 divides $|G|$.

(b) If $k = 2$, then we have

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} = 2 \times 3 = 6, \quad \text{since } \alpha_1 = \alpha_2 = 1.$$

Now suppose that $k \geq 3$. We have $|G| = 6 p_3^{\alpha_3} \ldots p_k^{\alpha_k}$. Also

$$\begin{aligned}
&(p_3 - 1) \mid |G| \\
\Rightarrow\ &(p_3 - 1) \mid 6\, p_3^{\alpha_3} \ldots p_k^{\alpha_k} \\
\Rightarrow\ &(p_3 - 1) \mid 6, \quad \text{since } (p_3 - 1) \text{ is even} \\
\Rightarrow\ &p_3 - 1 = 6 \\
\Rightarrow\ &p_3 = 7.
\end{aligned}$$

Hence 7 divides $|G|$.

(c) If $k = 3$, then

$$|G| = p_1^{\alpha_1}\, p_2^{\alpha_2}\, p_3^{\alpha_3} = 2 \times 3 \times 7 = 42$$

Now suppose that $k \geq 4$. We have

$$|G| = 42\, p_4^{\alpha_4}\, \ldots\, p_k^{\alpha_k}$$

Also

$$\begin{aligned} & (p_4 - 1) \mid |G| \\ \Rightarrow & (p_4 - 1) \mid 42 \\ \Rightarrow & p_4 = 43. \end{aligned}$$

If $k \geq 5$, then, for $\alpha_4 = 1$, we have

$$|G| = 2 \times 3 \times 7 \times 43 \times p_5^{\alpha_5} \dots p_k^{\alpha_k} = 1806 \times p_5^{\alpha_5} \dots p_k^{\alpha_k},$$

since $\alpha_1 = \alpha_2 = \alpha_3 = 1$. Therefore $p_5 - 1$ divides 1806, which is not possible for any prime $p_5 > 43$. Hence we must have $\alpha_4 > 1$. Also by proposition 3.2.2, there exists a prime $p_5 > 43$ which divides $|G|$. Since $p = 77659 = 2 \times 3 \times 7 \times 43^2 + 1$ is the smallest prime greater than 43 such that $(p-1)$ divides $2 \times 3 \times 7 \times 43^r,\ r > 1$, it follows that $p_5 \geq 77659$. This completes the proof. □

Remark 3.3.3. Using proposition 3.2.1 and the celebrated theorem of Frobenius (see Result 1.3.2), one can show that if $|G| = 42 \times 43^r \times 77659$, $r \leq 3$, then G is not a POS-group. The proof involves counting of group elements of order powers of 43.

We have enough evidence in support of the following conjecture; however, a concrete proof is still eluding.

Conjecture 3.3.4. *If G is a POS-group such that* $\mathrm{ord}_2 |G| = ord_3|G| = ord_7|G| = 1$, *then* $|G| = 42$.

3.4 A characterization

In this section we have the following result.

Theorem 3.4.1. *Let G be a group such that $G \cong S_3 \times (C_2)^t \times M$, where $t \geq 0$ and M is a cyclic group of odd square-free order not divisible by 3. If G is a POS-group, then G is isomorphic to one of the following three groups:*

(a) S_3

(b) $S_3 \times C_2 \times C_7$

(c) $S_3 \times (C_2)^2 \times C_5$

Proof. First suppose that $t = 0$. Then $G \cong S_3 \times M$.

Since $|M|$ is odd and $3 \nmid |M|$, there are no elements of order 2 and 3 in M. Since, in S_3, the number of elements of order 2 is 3 and the number of elements of order 3 is 2, G has three elements of order 2 and two elements of order 3. Let p be the smallest prime dividing $|M|$. Then the number of elements of order p is $(p-1)$. Since G is a POS-group, by proposition 3.1.2, $(p-1)$ divides $|G|$. Now $p \neq 2, 3$ since $2 \nmid |M|$, $3 \nmid |M|$. Suppose that $p = 5$. Then the number of elements of order 5 is 4 and 4 divides $|G|$. Hence 4 divides $|S_3||M|$ which implies 2 divides $3|M|$. This is not possible as $|M|$ is odd. Hence $p = 5$ is not possible. So 7 is the smallest prime dividing $|M|$.

Now S_3 has three elements of order 2 and M has six elements of order 7. Thus if $(x, y) \in G$ such that $o(x, y) = 14$, then $o(x) = 2$ and $o(y) = 7$ since $\gcd(o(x), o(y)) = 1$. We have three choices for the first position and six choices for the second position. Hence the total number of elements of

order 14 in G is 18 and $18 \nmid |G|$, since $|G|$ is square free. So M is trivial and $G \cong S_3$, which is indeed a POS-group.

Next suppose that $t \geq 1$. Then $G \cong S_3 \times (C_2)^t \times M$. Now we count the number of elements of order 2. Suppose that $(s, z_1, z_2, \ldots z_t, m) \in S_3 \times (C_2)^t \times M$ s.t. $o(s, z_1, z_2, \ldots z_t) = 2$. Then $o(m) = 1$ as $2 \nmid |M|$.

Since S_3 has three elements of order 2, the number of choices for the first position in $(s, z_1, z_2, \ldots z_t, m)$ is 3. Now each of $z_i, 1 \leq i \leq t$, has two choices. Hence the total number of choices for the next t positions is $\underbrace{2 \times 2 \times \cdots \times 2}_{\text{t times}} = 2^t$. Again if we take the first position as identity, then number of choices $= 2^t - 1$. Hence the number of elements of order 2 is

$$3.2^t + 2^t - 1 \ = \ 2^{t+2} - 1.$$

Now we count the number of elements of order 6. Suppose that the order of the element $(s, z_1, z_2, \ldots z_t, m)$ is 6. Since S_3 has two elements of order 3, the number of choices for the first position is 2. The number of choices for the next positions is $2^t - 1$. Hence the total number of elements of order 6 is $2(2^t - 1)$. Thus the total number of elements of order 6 is $2(2^t - 1)$. Since G is a POS-group, $2(2^t - 1)$ divides $6.2^t|M|$. Since $2^t - 1$ does not divide 2^t, we have $2^t - 1$ divides $3|M|$. Also $2^{t+2} - 1$ divides $6.2^t|M|$ which implies that $2^{t+2} - 1$ divides $3|M|$. So $3|M|$ is divisible by both $2^t - 1$ and $2^{t+2} - 1$. If p is an odd prime dividing $t + 2$, then $t + 2 = pk$ for some k. Now

$$2^{t+2} - 1 = 2^{pk} - 1 = (2^p - 1)((2^p)^{k-1} + (2^p)^{k-2} + \ldots + 1).$$

So $(2^p - 1)$ divides $(2^{t+2} - 1)$. Then $2^p - 1$ divides $|G|$ which implies $2^p - 1$ divides $2^{t+1}.3|M|$. Since p is an odd prime, we have $p \geq 3$, and so $2^p - 1 \geq 7$.

Thus $2^p - 1 \nmid 3$. Also $2^p - 1 \nmid 2^{t+1}$. So $2^p - 1$ divides $|M|$. Since $|M|$ is square free, $2^p - 1$ is square free. Suppose that q is a prime divisor of $2^p - 1$. Then

$$2^p \equiv 1 (\mathrm{mod}\, q)$$

Hence the order of 2 modulo q is p, i.e. in the multiplicative group C_q^*, $o([2]) = p$. Hence p divides $|C_q^*| = q - 1$. So if q_1 and q_2 are distinct primes dividing $2^p - 1$, then p divides $q_1 - 1$ and $q_2 - 1$ and consequently p^2 divides $(q_1 - 1)(q_2 - 1)$, which is the number of elements of order $q_1 q_2$ in G.
So p^2 divides $6.2^t|M|$ i.e. p^2 divides $3|M|$. This is not possible as $|M|$ is square free. So $2^p - 1$ must be prime.

Suppose that p_1 and p_2 are two distinct odd primes dividing $t + 2$. Then from above

$$2^{p_1} - 1 \equiv 1 (\mathrm{mod} 3)$$

$$2^{p_2} - 1 \equiv 1 (\mathrm{mod} 3)$$

Hence 3 divides $2^{p_1} - 2$ and $2^{p_2} - 2$. So 9 divides $(2^{p_1} - 2)(2^{p_2} - 2)$, the number of elements of order $(2^{p_1} - 1)(2^{p_2} - 1)$. So 9 divides $|G|$ i.e. 3 divides $|M|$, which is a contradiction. So at most one odd prime divides $t + 2$.

Suppose that $2p$ divides $t + 2$, where p is an odd prime. Then $2^p - 1$ is prime. So 3 divides $2^p - 2$. Now $t + 2 = 2pk$ for some k. So,

$$\begin{aligned} 2^{t+2} - 1 &= 4^{pk} - 1 \\ &= (1 + 3)^{pk} - 1 \\ &= 3 \left[\binom{pk}{1} + \binom{pk}{2} .3 + \ldots + 3^{p\,k-1} \right] \end{aligned}$$

Thus, 3 divides $2^{t+2}-1$, and hence 9 divides $(2^{t+2}-1)(2^p-2)$. Now, the total number of elements of order 2 is $2^{t+2}-1$ and the number of elements of order 2^p-1 is 2^p-2. Hence the total number of elements of order $2(2^p-1)$ in G is $(2^{t+2}-1)(2^p-2)$. Therefore 9 divides $|G| = |S_3 \times M|$. This is not possible as $|S_3 \times M|$ is square free. Hence $t+2$ is necessarily a power of a single prime. Suppose that $t+2 = p^b$ for some odd prime p. If $b = 1$, then from above, 2^p-1 divides $2^{t+2}-1$. Suppose $b \geq 1$. Then $2^{t+2}-1$ is not prime. Also 2^{t+2} is square free. So there exists a prime $q \neq 2^p-1$ such that q divides $2^{t+2}-1$. Thus p^2 divides $(q-1)(2^p-2)$, the number of elements of order $q(2^p-1)$ in $|G|$, which is a contradiction since $|S_3 \times M|$ is square free. Thus $b = 1$ and $t+2$ is prime.

Similar argument shows that either $t = 1$, t is a power of 2 or t is an odd prime. Since, t and $t+2$ have the same parity, there are three possibilities.

Case I $t = 1$.

In this case $t+2 = 3$. So, the number of elements of order 2 is $2^3-1 = 7$. Since G is a POS-group, 7 divides $|G|$. Hence

$$G \cong S_3 \times C_2 \times C_7 \times \tilde{M}$$

But then the number of elements of order 42 is 12. Hence $\tilde{M}$ is trivial. For, if there is an odd prime p dividing $|\ \tilde{M}\ |$, then the number of elements of order $42p$ is $12(p-1)$, a multiple of 8, and so we have a contradiction since 8 does not divide $|G|$. Thus

$$G \cong S_3 \times C_2 \times C_7,$$

which is a POS-group.

Case II Both t and $t+2$ are odd primes.

In this case both $2^t - 1$ and $2^{t+2} - 1$ are primes and they divide $|G|$. So 9 divides $(2^t - 2)(2^{t+2} - 2)$, the number of elements of order $(2^t - 1)(2^{t+2} - 1)$ in G. Therefore we do not get any new POS-group from this case.

Case III $t = 2^a$ and $t + 2 = 2^b$ for some positive integers a and b.

In this case $2^{b-1} - 2^{a-1} = 1$. So we have $a = 1$ and $b = 2$. Now, the number of elements of order 2 is $2^4 - 1 = 15$ and since 15 divides $|\ G\ |$, we have

$$G \cong S_3 \times (C_2)^2 \times C_5 \times \tilde{M}$$

But then the number of elements of order 30 is 24. Therefore, as in Case I (noting that 16 does not divide $|G|$), it follows that $\tilde{M}$ must be trivial. Hence

$$G \cong S_3 \times (C_2)^2 \times C_5,$$

which is a POS-group. □

Chapter 4

Abelian POS-groups

In this chapter, we discuss in detail some properties of abelian POS-groups. This chapter is based primarily on the work of C. E. Finch and L. Jones [8].

4.1 Fermat numbers

A Fermat number, named after Pierre de Fermat who first studied them, is a positive integer of the form $F_n = 2^{2^n} + 1$ where n is a non-negative integer. If F_n happens to be prime, F_n is called a Fermat prime. Fermat numbers and Fermat primes were first studied by Pierre de Fermat, who showed that F_n is prime for each $n \leq 4$, and conjectured that all Fermat numbers are prime. This conjecture was disproved by Leonhard Eular in 1732 when he showed that $F_5 = 4294967297$ is divisible by 641. It is now known that F_n is composite for many values of n but till now, no new value of n has been found for which F_n is prime.

Lemma 4.1.1. *The Fermat number F_5 is composite and is divisible by* 641.

Proof. Putting $a = 2^7$ and $b = 5$ in $1 + ab$, we have, $1 + ab = 1 + 2^7.5 = 641$. Now,

$$1 + ab - b^4 = 1 + (a - b)b^3 = 1 + (128 - 125)5 = 2^4.$$

So, we have

$$\begin{aligned} F_5 &= 2^{2^5} + 1 \\ &= 2^4a^4 + 1 \\ &= (1 + ab - b^4)a^4 + 1 \\ &= (1 + ab)a^4 + (1 - a^4b^4) \\ &= 641[a^4 + (1 - ab)(1 + a^2b^2)]. \end{aligned}$$

Thus, 641 divides F_5. □

4.2 Infinitude of abelian POS-groups

In this section, we study how one can exhibit an infinite family of abelian POS-groups.

Lemma 4.2.1. *Let a, b and t be positive integers with $b \leq a$, and let $G \cong (C_{p^a})^t$, where p is a prime. Then the number of elements in G of order p^b is $(p^{b-1})^t(p^t - 1)$.*

Proof. The number of elements of order p^b in C_{p^a} is the number of generators of the unique cyclic subgroup of C_{p^a} of order p^b. This number is $\phi(p^b) = p^b - p^{b-1}$, where ϕ is the Euler's phi function.

Now the number of elements in C_{p^a} which does not have order p^b is

$$\begin{aligned} & p^b - \phi(p^b) \\ =& p^b - p^b + p^{b-1} \\ =& p^{b-1}. \end{aligned}$$

Hence the number of elements in G of order p^b is

$$\begin{aligned} & (p^b)^t - (p^{b-1})^t \\ =& (p^{b-1})^t p^t - (p^{b-1})^t \\ =& (p^{b-1})^t (p^t - 1). \end{aligned}$$

This completes the proof. □

Lemma 4.2.2. *Let p be a prime and M be a finite group (not necessarily abelian) such that $\gcd(p, |M|) = 1$. Let G and $\hat{G}$ be two finite groups such that $G \cong (C_{p^a})^t \times M$ and $\hat{G} \cong (C_{p^{a+1}})^t \times M$ where a and t are positive integers. Suppose that d is the order of an element in $\hat{G}$ and that p^{a+1} does not divide d. Then both G and $\hat{G}$ contain the same number of elements of order d.*

Proof. Suppose that $(x, y) \in \hat{G}$ where $x \in (C_{p^{a+1}})^t$, $y \in M$ and $o(x, y) = d$. d can be factored as $p^r n$ where $r \leq a$, $n \mid |M|$ and $p \nmid n$, since $p^{a+1} \nmid d$. Now the number of elements of order p^r in $(C_{p^a})^t$ is same as the number of elements of order p^r in $(C_{p^{a+1}})^t$. Hence the number of elements of order d in G is same as the number of elements of order d in $\hat{G}$. □

We now have the main result of this section.

Theorem 4.2.3. (Going-up theorem)

Let p be a prime and M be a finite group (not necessarily abelian) such that $\gcd(p, |M|) = 1$. *Let G and $\hat{G}$ be two finite groups such that $G \cong (C_{p^a})^t \times M$ and $\hat{G} \cong (C_{p^{a+1}})^t \times M$ where a and t are positive integers. If G has perfect order subsets, then $\hat{G}$ has perfect order subsets.*

Proof. Let $(x, y) \in \hat{G}$ where $x \in (C_{p^{a+1}})^t$, $y \in M$. Suppose that $o(x, y) = d$. First assume that $p^{a+1} \nmid d$. Then by lemma 4.2.2, $|OS_G(x, y)| = |OS_{\hat{G}}(x, y)|$. So $|OS_{\hat{G}}(x, y)|$ divides $|\hat{G}|$.

Next assume that $p^{a+1} \mid d$. So we can write $d = p^{a+1} n$ where $n \mid |M|$. Number of elements of order p^{a+1} is

$$(p^{a+1} - 1)^t (p^t - 1) = (p^a)^t (p^t - 1).$$

Now the number of elements in G having order $p^a n$ is $(p^{a-1})^t (p^t - 1)k$ where k is the number of elements in M of order $o(y)$. Since G is a POS-group, we have

$$\begin{aligned} & (p^{a-1})^t (p^t - 1)k \mid |G| \\ \Rightarrow\ & (p^{a-1})^t (p^t - 1)k \mid (p^a)^t |M| \\ \Rightarrow\ & (p^t - 1)k \mid |M|, \quad \text{since } p \nmid |M| \\ \Rightarrow\ & (p^a)^t \, (p^t - 1) \, k \mid |\hat{G}|. \end{aligned}$$

So $\hat{G}$ has perfect order subsets. □

As a consequence, we have the following result due to Das [4].

Corollary 4.2.4. *Let M be the unique non-abelian group of order* 21. *Then $C_{2^a} \times M$ is a POS-group for each $a \geq 1$.*

Proof. M has one identity element, six elements of order 7 and 14 elements of order 3. Therefore, for $C_2 \times M$ we have the following table:

Orders of group elements	Cardinalities of corresponding order subsets
1	1
2	1
3	14
6	14
7	6
14	6

It follows that $C_2 \times M$ is a POS-group. Since M need not be abelian, by using going-up theorem, we have $C_{2^a} \times M$ is a POS-group for each $a \geq 1$. □

Example 4.2.5. $(C_2)^4 \times C_3 \times C_5$ has perfect order subsets. Using going-up theorem, we have $(C_{3^2}) \times (C_2)^4 \times C_5$ i.e. $C_9 \times (C_2)^4 \times C_5$ has perfect order subsets. Also $C_{25} \times (C_2)^4 \times C_3$ has perfect order subsets. Applying the going-up theorem successively yields groups such as $(C_{16})^4 \times C_9 \times C_{125}$ with perfect order subsets.

From the above observations, it follows that starting with a group having perfect order subsets we can generate new ones using going-up theorem. In fact, this method enables us to exhibit an infinite family of such groups.

4.3 Existence of minimal POS-groups

We can also find a smaller POS-group starting from a bigger POS-group. Chopping-off theorem and going-down theorem give us techniques for finding

such groups.

Suppose that $G \cong (C_2)^t \times M$, where $|M|$ is odd. We call G a *minimal POS-group* if G has perfect order subsets and there is no proper subgroup $\hat{M}$ of M such that $(C_2)^t \times \hat{M}$ has perfect order subsets.

Example 4.3.1. $(C_2)^2 \times C_3$ is a minimal POS-group.

Theorem 4.3.2. (Chopping-off theorem)
Let p be a prime and M be a finite group (not necessarily abelian) such that $\gcd(p, |M|) = 1$. Let G and $\hat{G}$ be two finite groups such that $G \cong C_{p^{a_1}} \times C_{p^{a_2}} \times \cdots \times C_{p^{a_{s-1}}} \times (C_{p^{a_s}})^t \times M$ and $\hat{G} \cong (C_{p^{a_s}})^t \times M$ where $a_1 \leq a_2 \leq \cdots \leq a_{s-1} < a_s$ are positive integers. If G is a POS-group, then $\hat{G}$ is also a POS-group.

Proof. Let $(x, y) \in \hat{G}$ where $x \in (C_{p^{a_s}})^t$, $y \in M$. Then $o(x, y) = p^b\, m$, $b \leq a_s$, $o(x) = p^b, o(y) = m$. Suppose that $p^c\, k$ is the number of elements of order m in M where $p \nmid k$. Then by lemma 4.2.1 the number of elements of order $p^{a_s}\, m$ in G is $(p^{b-1})^t(p^t - 1)p^c\, k$.

Now the number of elements of order $p^{a_s}\, m$ in G is

$$p^{a_1}\, p^{a_2}\, \ldots\, p^{a_{s-1}}(p^{a_s-1})^t(p_t - 1)\, p^c\, k = p^{\sum_{i=1}^{s-1} a_i}\, (p^{a_s-1})^t(p^t - 1)\, p^c\, k.$$

Since G is a POS-group, we have

$$
\begin{aligned}
& p^{\sum_{i=1}^{s-1} a_i}\,(p^{a_s-1})^t(p^t-1)\,p^c\,k \mid |G| \\
\Rightarrow\ & p^{a_1+a_2+\cdots+a_{s-1}+(a_s-1)\,t+c}(p_t-1)\,k \mid p^{a_1+a_2+\cdots+a_{s-1}+a_s\,t}\,|M| \\
\Rightarrow\ & p^{a_1+a_2+\cdots+a_{s-1}+a_s\,t}\,|M| = p^{a_1+a_2+\cdots+a_{s-1}+(a_s-1)\,t+c}(p_t-1)\,k\,z \quad \text{for some } z\in\mathbb{Z} \\
\Rightarrow\ & p^t\,|M| = p^c\,(p^t-1)\,k\,z \\
\Rightarrow\ & (p^t-1)\,k \mid |M|, \quad \text{since } \gcd(p,\,(p^t-1)\,k)=1
\end{aligned}
$$

and $t \geq c$, since $p \nmid |M|$.

Now

$$
\begin{aligned}
& (p^t-1)\,k \mid |M| \\
\Rightarrow\ & (p^b)^t(p^t-1)\,k \mid p^{a_s\,t}\,|M|, && \text{since } b \leq a_s \\
\Rightarrow\ & p^{bt-(t-c)}(p^t-1)\,k \mid p^{a_s\,t}\,|M|, && \text{since } c \leq t \\
\Rightarrow\ & (p^{b-1})^t\,(p^t-1)\,p^c\,k \mid |\hat{G}|.
\end{aligned}
$$

Now $(p^{b-1})^t p^c\,k$ is the number of elements of order $p^b\,m$ in G. Hence $\hat{G}$ has perfect order subsets. □

Theorem 4.3.3. (Going-down theorem)

Let p be a prime and M be a finite group (not necessarily abelian) such that $\gcd(p, |M|) = 1$. Let G and $\hat{G}$ be two finite groups such that $G \cong (C_{p^a})^t \times M$ and $\hat{G} \cong (C_p)^t \times M$ where a and t are positive integers. If G is a POS-group, then $\hat{G}$ is also a POS-group.

Proof. Let $(x,\, y) \in \hat{G}$ where $x \in (C_p)^t$, $y \in M$. Suppose that $o(x,\, y) = d$. So d can be factored as pm where $o(y) = m$. Hence the number of elements

of order d in $\hat{G}$ is $(p^{1-1})^t(p^t - 1)\,k = (p^t - 1)\,k$ where k is the number of elements in M of order m.

Now the number of elements of order $p^a\,m$ in G is $(p^{a-1})^t(p^t - 1)\,k$ which divides $|G|$.

Hence

$$\begin{aligned} & |G| = (p^{a-1})^t\,(p^t - 1)\,k \\ \Rightarrow\ & p^{a\,t}\,|M| = p^{a\,t-t}\,(p^t - 1)\,k\,r \\ \Rightarrow\ & p^t\,|M| = (p^t - 1)\,k\,r \\ \Rightarrow\ & |\hat{G}| = (p^t - 1)\,k\,r \\ \Rightarrow\ & (p^t - 1)\,k \mid |\hat{G}|. \end{aligned}$$

So $\hat{G}$ has perfect order subsets. □

Since we are dealing with finite groups, it follows immediately that the repeated application of the above two theorems will always end up with a minimal POS-group.

4.4 Some minimal abelian POS-groups

Lemma 4.4.1. *Let p be a prime, let a be a positive integer and let q be a prime divisor of $2^{p^a} - 1$. Then p divides $q - 1$.*

Proof. Since $2^{p^a} \equiv 1 \pmod{q}$, 2^{p^a} is the identity element in $(C_q)^*$ where $(C_q)^*$ is the multiplicative group of nonzero elements of C_q. Since $2^{p^a} \equiv 1\,(mod\ q)$, $o(2)$ divides p^a. So p divides $o(2)$. By Langrange's theorem, $o(2)$ divides $|(C_q)^*|$ which implies p divides $q - 1$. □

Lemma 4.4.2. *If $G \cong (C_2)^t \times M$ is a minimal abelian POS-group where $|M|$ is odd and square-free, then $t = p^a$ where p is a prime and $a \geq 0$.*

Proof. Without any loss, we may assume that t is not a power of 2. Since $G \cong (C_2)^t \times M$ and $|M|$ is odd, number of elements of order 2 in G is $2^t - 1$. Since G has perfect order subsets,

$$\begin{aligned} & (2^t - 1) \mid |G| \\ \Rightarrow\ & (2^t - 1) \mid 2^t\,|M| \\ \Rightarrow\ & (2^t - 1) \mid |M|. \end{aligned}$$

So $2^t - 1$ is square-free. Let p be an odd prime dividing t. So $t = p\,m$ for some m. Now

$$2^t - 1 = 2^{pm} - 1 = (2^p - 1)[(2^p)^{m-1} + (2^p)^{m-2} + \ldots + 1].$$

So $(2^p - 1)$ divides $(2^t - 1)$, and thus $(2^p - 1)$ is square-free. Suppose that q_1 and q_2 are distinct primes dividing $2^p - 1$. Then by lemma 4.4.1, p^2 divides $(q_1 - 1)(q_2 - 1)$ which is the number of elements of order $q_1\,q_2$ in G. So p^2 divides $|M|$ which is not possible. Hence $2^p - 1$ must be prime.

Since p is odd, we have $2^p \equiv 2 \pmod 3$ which implies that 3 divides $2^p - 2$. Suppose that p_1 and p_2 are disinct odd primes dividing t. So 9 divides $(2^{p_1} - 2)(2^{p_2} - 2)$ which is the number of elements of order $(2^{p_1} - 1)(2^{p_2} - 1)$ in G. Since $(2^{p_1} - 2)(2^{p_2} - 2)$ divides $2^t\,|M|$, it follows that 9 divides $|M|$. This is a contradiction since $|M|$ is square-free. Hence at most one odd prime p divides t.

Suppose that $2p$ divides t, where p is an odd prime. Then $t = 2pk$ for

some k. Now

$$\begin{aligned} 2^t - 1 &= 2^{2\,p\,k} - 1 \\ &= (1+\ 3)^{p\,k} - 1 \\ &= 3\ \left[\binom{pk}{1} + \binom{pk}{2}.3 + \cdots + 3^{pk-1}\right]. \end{aligned}$$

Hence 3 divides $2^t - 1$ and so 9 divides $(2^t - 1)(2^p - 2)$. Since, in G, the number of elements of order 2 is $2^t - 1$ and the number of elements of order $2^p - 1$ is $2^p - 2$, it follows that the total number of elements of order $2(2^p - 1)$ in G is $(2^t - 1)(2^p - 2)$. Hence 9 divides $|M|$ which is a contradiction. Therefore t must be a power of a prime. □

Lemma 4.4.3. *If $G \cong (C_2)^t \times M$ is a minimal abelian POS-group, where $|M|$ is odd and square-free, then $t = p^a$ with $a \leq 1$ when p is an odd prime and $a \leq 5$ when p is even.*

Proof. By lemma 4.4.2, $t = p^a$. Suppose that $t = p^a$ where p is an odd prime and $a \geq 2$. Now $2^p - 1$ is a prime divisor of $2^{p^a} - 1$. Since $2^{p^a} - 1$ square-free, there is some prime $q \neq 2^p - 1$ q divides $2^{p^a} - 1$. Then by lemma 4.4.1, p divides $q - 1$. Also we have,

$$\begin{aligned} & p \mid 2^p - 2 \\ \Rightarrow \quad & p^2 \mid (q-1)(2^{p-2}) \end{aligned}$$

which is the number of elements of order $q(2^p - 1)$ in G. Then p^2 divides $|M|$. This is a contradicton. Hence $t = p^a$ with $a \leq 1$.

Next we consider the case $t = 2^a$, $a \geq 1$. Then $2^t - 1 = 2^{2^a} - 1$, $a \geq 1$.

Note that

$$2^{2^a} - 1 = \prod_{n=0}^{a-1}(2^{2^n} + 1) = \prod_{n=0}^{a-1} F_n.$$

Let us assume that $a \geq 6$. Then F_5 divides $2^{2^a} - 1$. Also $F_0 = 3$ divides $2^{2^a} - 1$. But $F_5 = 4294967297 = 641 \times 6700417$, and so, 6700417 is a prime factor of F_5. Also 3 divides 6700416. So 9 divides $(2^{2^a} - 1)(6700416)$, the number of elements of order 2×6700417 in G. Thus, 9 divides $2^t|M|$, and so, 9 divides $|M|$. This is impossible since $|M|$ is square-free. So $a \leq 5$. □

Theorem 4.4.4. *Let G be a finite abelian group of even order whose Sylow p-subgroup is a cyclic group of order p for each odd prime p dividing $|G|$. If G is a minimal POS-group, then G is isomorphic to one of the following nine groups:*

(a) C_2

(b) $(C_2)^2 \times C_3$

(c) $(C_2)^3 \times C_3 \times C_7$

(d) $(C_2)^4 \times C_3 \times C_5$

(e) $(C_2)^5 \times C_3 \times C_5 \times C_{31}$

(f) $(C_2)^8 \times C_3 \times C_5 \times C_{17}$

(g) $(C_2)^{16} \times C_3 \times C_5 \times C_{17} \times C_{257}$

(h) $(C_2)^{17} \times C_3 \times C_5 \times C_{17} \times C_{257} \times C_{131071}$

(i) $(C_2)^{32} \times C_3 \times C_5 \times C_{17} \times C_{257} \times C_{65537}$

Proof. Suppose that $G \cong (C_2)^t \times M$ is a minimal POS-group where $|M|$ is odd. Then by lemma 4.4.2, $t = p^a$ where p is a prime. By lemma 4.4.3, if p is odd, then $a \leq 1$ and if p is even, then $a \leq 5$. Thus, $t = 1$ or p if p is odd.

Since $2(2^{p-1} - 1)$, the number of elements of order $2^p - 1$, divides $\mid G \mid$, it follows that if we take $t = p - 1$, then $p - 1$ is even and since t is a power of a prime, $p - 1$ must be a power of 2. Hence

$$p - 1 = 2^k \quad \text{for some } k$$
$$\Rightarrow p = 2^k + 1.$$

So p is a Fermat prime. Hence $p = 3, 5, 17, 257, 65537$. So if $t = p$, then $t = 3, 5, 17, 257, 65537$.

Now if p is even, then $a \leq 5$. So

$$t = 2, 2^2, 2^3, 2^4, 2^5$$
$$= 2, 4, 8, 16, 32.$$

Hence t is a member of $\{1, 2, 3, 4, 5, 8, 16, 17, 32\}$.

If $t = 1$, then $G \cong C_2$.

if $t = 2$, then since G is a POS-group, we have $2^2 - 1$ divides $|G|$. So 3 divides $|M|$.

Since $|M|$ is odd, $M \cong C_3$. Hence $G \cong (C_2)^2 \times C_3$.

If $t = 3$, then $2^3 - 1 = 7$ and 7 divides $|G| = 8|M|$. Hence 7 divides $|M|$. But $7 - 1 = 6$ should also divide $|G|$. So

$$M \cong C_3 \times C_7.$$

Hence

$$G \cong (C_2)^4 \times C_3 \times C_7.$$

If $t = 4$, then $2^4 - 1 = 15$ and 15 divides $|G| = 2^4|M|$. So 3×5 divides $|M|$. Hence

$$M \cong C_3 \times C_5.$$

So

$$G \cong (C_2)^4 \times C_3 \times C_5.$$

If $t = 5$, then $2^5 - 1 = 31$ and 31 divides $2^5\,|M|$. Also 31 is prime. So $31 - 1 = 30$ divides $|G| = 2^5\,|M|$. 30 can be factored as $2 \times 3 \times 5$. So

$$M \cong C_3 \times C_5 \times C_{31}$$

Hence

$$G \cong (C_2)^5 \times C_3 \times C_5 \times C_{31}$$

If $t = 8$, then $2^8 - 1 = 255$ and 255 divides $2^8|M|$. So $255 = 3 \times 5 \times 17$ divides $|M|$. Therefore

$$M \cong C_3 \times C_5 \times C_{17}.$$

Hence

$$G \cong (C_2)^8 \times C_3 \times C_5 \times C_{17}.$$

If $t = 16$, then $2^{16} - 1 = 65535$ and 65535 divides $2^{16}|M|$. So $65535 = 3 \times 5 \times 17 \times 257$ divides $|M|$. So

$$M \cong C_3 \times C_5 \times C_{17} \times C_{257}.$$

Hence

$$G \cong (C_2)^{16} \times C_3 \times C_5 \times C_{17} \times C_{257}.$$

If $t = 17$, then $2^{17} - 1 = 131071$ and 131071 divides $2^{17}|M|$. 131071 is a prime number. Also $131071 - 1 = 131070$ divides $|G| = 2^{17}|M|$. So $2 \times 3 \times 5 \times 17 \times 257$ divides $2^{17}|M|$, *i.e.*, $3 \times 5 \times 17 \times 257$ divides $|M|$.

So

$$M \cong C_3 \times C_5 \times C_{17} \times C_{257} \times C_{131071}.$$

Hence

$$G \cong (C_2)^{32} \times C_3 \times C_5 \times C_{17} \times C_{257} \times C_{131071}.$$

If $t = 32$, then $2^{32} - 1 = 4294967295$ which divides $|G| = 2^{32}|M|$. So 65535×65537 divides $|M|$, *i.e.*, $3.5 \times 17 \times 257 \times 65537$ divides $|M|$. So

$$M \cong C_3 \times C_5 \times C_{17} \times C_{257} \times C_{65537}$$

and hence

$$G \cong (C_2)^{32} \times C_3 \times C_5 \times C_{17} \times C_{257} \times C_{65537}.$$

This completes the proof. □

Chapter 5

Some standard POS and non-POS groups

In this chapter we consider several standard examples of finite groups and study whether they have perfect order subsets or not. This chapter is based on the work of S. Libera and P. Tlucek [16], A. K. Das [4] and C. E. Finch and L. Jones [9].

5.1 Cyclic groups

Lemma 5.1.1. *Let n be a positive integer. Then $\phi(n)$ divides n if and only if $n = 1$ or $n = 2^k\, 3^l$ with where $k \geq 1$ and $l \geq 0$.*

Proof. Suppose that $n > 1$ and $\phi(n)$ divides n. Let $n = p_1^{r_1}\, p_2^{r_2}\, \ldots\, p_t^{r_t}$, where $t \geq 1$ and $p_1 < p_2 < \ldots < p_t$ are primes. Also, $r_i \geq 1$ for $1 \leq i \leq t$. Then

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}), \ldots (1 - \frac{1}{p_t}). \qquad (5.1.a)$$

So

$$\begin{aligned}\phi(n) &= p_1^{r_1} p_2^{r_2} \ldots p_t^{r_t} \, \frac{(p_1 - 1)(p_2 - 1) \ldots (p_t - 1)}{p_1 \, p_2 \cdots p_t} \\ &= p_1^{r_1 - 1} p_2^{r_2 - 1} \ldots p_t^{r_t - 1} (p_1 - 1)(p_2 - 1) \ldots (p_t - 1).\end{aligned}$$

Since $\phi(n)$ divides n, $n = \phi(n)\, k$ for some $k \in \mathbb{Z}$. Using $(5.1.a)$, we have

$$\begin{aligned}\phi(n) &= \phi(n)\, k \, \frac{(p_1 - 1)(p_2 - 1) \ldots (p_t - 1)}{p_1 \, p_2 \ldots p_t} \\ \Rightarrow \; p_1 \, p_2 \ldots p_t &= k \, (p_1 - 1)(p_2 - 1) \ldots (p_t - 1).\end{aligned}$$

So

$$(p_1 - 1)(p_2 - 1) \ldots (p_t - 1) \mid p_1 \, p_2 \ldots p_t. \qquad (5.1.b)$$

Similarly, if $(p_1 - 1)(p_2 - 1) \ldots (p_t - 1)$ divides $p_1 \, p_2 \ldots p_t$, then $\phi(n) \mid n$. Thus we see that $\phi(n)$ divides n if and only if $(p_1 - 1)(p_2 - 1) \ldots (p_t - 1)$ divides $p_1 \, p_2 \ldots p_t$.

Suppose that $p_1 > 2$. Then $(p_1 - 1)$ is even. So from $(5.1.b)$, we have, $p_1 \, p_2 \ldots p_t$ is even. So atleast one of $p_1, p_2, \ldots, p_t$ is even, which is impossible as p_1 is the smallest prime among them. Hence $p_1 = 2$. Thus, if $t = 1$, then we are through.

Next we assume that $t > 2$. Then $(p_2 - 1)$, $(p_3 - 1)$, $\ldots$, $(p_t - 1)$ are even. Hence $(p_2 - 1)(p_3 - 1) \ldots (p_k - 1) = 2^{t-1} \, s$ for some $s \in \mathbb{N}$. By $(5.1.b)$, 2^t divides $p_1 \, p_2 \ldots p_t$. Note that $2^{t-1} \geq 4$. So 4 divides $p_1 \, p_2 \ldots p_t$ which implies 2 divides $p_1 \, p_2 \ldots p_t$. This is a contradiction since $p_1, p_2, \ldots, p_t$ are odd primes. Hence $t \leq 2$.

If $t = 2$, then from $(5.1.b)$, we have $(p_1 - 1)(p_2 - 1)$ divides $p_1 p_2$. So $(p_2 - 1)$ divides $2 \, p_2$. Since $\gcd((p_2 - 1), p_2) = 1$, we have $(p_2 - 1) \nmid p_2$. Hence $(p_2 - 1)$ divides 2 and so $p_2 = 3$.

Putting all these together we see that if $n > 1$ and n divides $\phi(n)$, then n is of the form $2^k 3^l$ with $k \geq 1$, $l \geq 0$.

Conversely, suppose that $n = 2^k 3^l$, $k \geq 1$, $l \geq 0$. If $l = 0$, then $n = 2^k$. So $\phi(n) = \phi(2^k) = 2^{k-1}$. Thus, $\phi(n)$ divides n. on the other hand, if $l \geq 1$, then

$$\begin{aligned}\phi(n) &= n\,(1 - \frac{1}{2})\,(1 - \frac{1}{3}) \\ &= \frac{n}{3} \\ &= 2^k\,3^{l-1}.\end{aligned}$$

So $2^k\,3^{l-1}$ divides $2^k\,3^l = n$. Hence the lemma follows. □

Proposition 5.1.2. *C_n is a POS-group if and only if $n = 1$ or $n = 2^\alpha\,3^\beta$ where $\alpha \geq 1$, $\beta \geq 0$.*

Proof. Suppose that d is a positive divisor of n. For each positive divisor d of n, C_n has exactly $\phi(d)$ elements of order d, where ϕ is Euler's phi function. So C_n is a POS-group if and only if $\phi(d)$ divides n for each positive divisor d of n i.e. if and only if $\phi(n)$ divides n. By the above lemma, we have $n = 2^\alpha\,3^\beta$ where $\alpha \geq 1$, $\beta \geq 0$. □

Proposition 5.1.3. *A 2-group is a POS-group if and only if it is cyclic.*

Proof. Let G be a POS-group with $|G| = 2^m$, $m \geq 0$. For $0 \leq n \leq m$, let $X_n = \{g \in G : g^{2^n} = 1\}$. Let $g \in X_{n-1}$. Then

$$\begin{aligned}g^{2^{n-1}} &= 1 \\ \Rightarrow g^{2^n} &= 1.\end{aligned}$$

So $g \in X_n$ and hence $X_{n-1} \subseteq X_n$. We use induction to show that $|X_n| = 2^n$ for all n with $0 \leq n \leq m$. This is equivalent to saying that G is cyclic.

Now, $|X_0| = 1 = 2^0$. So let us assume that $n \geq 1$. We show that

$$X_n - X_{n-1} = \{g \in G : o(g) = 2^n\}.$$

Let $g \in X_n - X_{n-1}$. Then $g^{2^n} = 1$ and $g^{2^{n-1}} \neq 1$. Suppose that $o(g) = 2^k$. Since $g^{2^n} = 1$ we should have $k \leq n$. But if $k < n$ then $k \leq n - 1$ and then $g^{2^k} = 1$ which implies $g^{2^{n-1}} = 1$ which is not possible. So $k = n$ and so $o(g) = 2^n$.

Conversely, let $o(g) = 2^n$. Then $g^{2^n} = 1$. Also since $2^{n-1} < 2^n$, $g^{2^{n-1}} \neq 1$. Hence

$$X_n - X_{n-1} = \{g \in G : o(g) = 2^n\}.$$

Using lemma 3.1.1, we have

$$|X_n| - |X_{n-1}| = |X_n - X_{n-1}| = 0 \text{ or } 2^t \qquad (5.1.c)$$

for some t with $n - 1 \leq t \leq m$, since $|G| = 2^m$. By induction hypothesis, $|X_{n-1}| = 2^{n-1}$, and by Result 1.3.2, 2^n divides $|X_n|$. So $|X_n| = 2^n$. Hence by proposition 5.1.2, G is a POS-group. □

5.2 Semidirect product of cyclic groups

Recall that if X and H are any two groups and $\theta : X \to \text{Aut}(H)$ is a homomorphism, then the cartesian product $X \times H$ forms a group under the binary operation

$$(x_1, h_1)(x_2, h_2) = (x_1x_2, \theta(x_2)(h_1)h_2),$$

where $x_i \in X$, $h_i \in H$, $i = 1, 2$. This group is known as the *(external) semidirect product* X with H (with respect to θ) and is denoted by $X \ltimes_\theta H$.

Proposition 5.2.1. *Let G be a POS-group with $|G| = 2^\alpha p^\beta$ where α and β are positive integers, and p is a Fermat's prime. If $2^\alpha < (p-1)^3$ then G is isomorphic to a semidirect product of a group of order 2^α with the cyclic group C_{p^β}.*

Proof. Since p is a Fermat's prime, $p = 2^{2^k} + 1$ where $k \geq 0$. Hence we have

$$2^{2^k} \equiv -1 (\mathrm{mod}\, p)$$
$$\Rightarrow 2^{2^{k+1}} \equiv 1 (\mathrm{mod}\, p).$$

Thus order of 2 modulo p is $2^{2^{k+1}}$. Let $X_n = \{g \in G \mid g^{p^n} = 1\}$. Then using the same argument as in the proof of the proposition 5.1.3, we get $|X_n| = p^n$ for all n with $0 \leq n \leq \beta$. So G has a unique Sylow p-subgroup and it is cyclic. Hence the proposition follows. □

Theorem 5.2.2. *Let p be a Fermat's prime. Let α, β be two positive integers such that $2^\alpha \geq p-1$. Then there exists a homomorphism $\theta : C_{2^\alpha} \to \mathrm{Aut}(C_{p^\beta})$ such that the semidirect product $C_{2^\alpha} \ltimes_\theta C_{p^\beta}$ is a non-abelian POS-group.*

Proof. Since p is a Fermat's prime, we have $p = 2^{2^k} + 1$ where $k \geq 0$. Now the group $U(C_{p^\beta})$ of units in the ring C_{p^β} is cyclic since p^β has a primitive root. Also

$$\begin{aligned} |U(C_{p^\beta})| &= \phi(p^\beta) \\ &= p^\beta \left(1 - \frac{1}{p}\right) \\ &= p^{\beta-1} 2^{2^k}. \end{aligned}$$

So we have, $x^{p^{\beta-1}2^{2^k}} \equiv 1(\mathrm{mod}\, p^\beta)$ for some $x \in U(C_{p^\beta})$. Also

$$\begin{aligned}
&(x^{p^{\beta-1}2^{2^k-1}})^2 \equiv 1(\mathrm{mod}\, p^\beta) \\
\Rightarrow\ & p^\beta \mid (x^{p^{\beta-1}2^{2^k-1}})^2 - 1 \\
\Rightarrow\ & p^\beta \mid (x^{p^{\beta-1}2^{2^k-1}} + 1)(x^{p^{\beta-1}2^{2^k-1}} - 1).
\end{aligned}$$

Hence $x^{p^{\beta-1}2^{2^k-1}} \equiv -1(\mathrm{mod} p^\beta)$. Thus if we take $z = x^{p^{\beta-1}}$, we have

$$z^{2^{2^k}} \equiv 1(\mathrm{mod} p^\beta)$$

and

$$z^{2^{2^k-1}} \equiv -1(\mathrm{mod}\, p^\beta).$$

Moreover, we may choose z in such a way that

$$z^{2^{2^k}} \not\equiv 1(\mathrm{mod}\, p^{\beta+1}).$$

Define a mapping $f : C_{p^\beta} \to C_{p^\beta}$ by $f(b) = b^z$ where $\gcd(z, p) = 1$. Since $\gcd(z, p^\beta) = 1$, there exist two integers m and n such that $mz + np^\beta = 1$. Suppose that $c \in C_{p^\beta}$. Then $c = b^i$ for some integer i. Now $b = b^{mz+np^\beta} = (b^m)^z$. Hence $b^i = (b^{im})^z = b^{mi}$. So f is onto and hence one-one. Also f is a homomorphism. Hence $f \in \mathrm{Aut}(C_{p^\beta})$.

Now consider the mapping $\theta : C_{2^\alpha} \to \mathrm{Aut}(C_{p^\beta})$ defined by $\theta(a) = f$. Then θ is a homomorphism. Also

$$\begin{aligned}
\theta(a^x)(b^y) &= f^x(b^y) \\
&= (f(b^y))^x \\
&= b^{yz^x}.
\end{aligned}$$

Hence

$$\theta(a^x)(b^y) = b^{yz^x}. \tag{5.2.a}$$

Now

$$\begin{aligned}(a^x, b^y)^2 &= (a^x, b^y)(a^x, b^y)\\ &= (a^{2x}, b^{yz^x}b^y)\\ &= (a^{2x}, b^{y(z^x+1)})\end{aligned}$$

$$\begin{aligned}(a^x, b^y)^3 &= \left(a^{3x}, \theta(a^{2x})(b^y)b^{y(z^x+1)}\right)\\ &= \left(a^{3x}, b^{y(z^x+z^{2x}+1)}\right)\\ &= \left(a^{3x}, b^{y\left(\frac{z^{3x}-1}{z^x-1}\right)}\right).\end{aligned}$$

Similarly

$$(a^x, b^y)^4 = \left(a^{3x}, b^{y\left(\frac{z^{4x}-1}{z^x-1}\right)}\right).$$

So, in $C_{2^\alpha} \ltimes_\theta C_{p^\beta}$, repeating this process, we have,

$$(a^x, b^y)^{2^{\alpha-r}} = (1, b^\gamma) \tag{5.2.b}$$

where

$$\begin{aligned}\gamma &= y \times \frac{z^{2^{\alpha-r}x} - 1}{z^x - 1}\\ &= y \times \frac{z^{2^\alpha m} - 1}{z^{2^r m} - 1}.\end{aligned}$$

Put $c = \mathrm{ord}_p\, m$. Then $m = p^c u$ for some positive integer u such that $p \nmid u$. Therefore we have for all $r \geq 2^k$,

$$z^{2^r m} = \left(z^{2^{2^k}}\right)^{2^{r-2^k}p^{cu}} \equiv 1 (\mathrm{mod} p^{\beta+c})$$

but

$$z^{2^r m} \not\equiv 1 (\mathrm{mod} p^{\beta+c+1}).$$

Since z has order 2^{2^k} modulo p, we have

$$2^{2^k} \mid 2^r m \Longrightarrow 2^k \leq r.$$

So if $r < 2^k$ then

$$z^{2^r m} \not\equiv 1 (\mathrm{mod}\, p).$$

Thus we have

$$\gamma = \begin{cases} p^{\beta+c+s}, & \text{if } r < 2^k, \\ p^s w, & \text{if } r \geq 2^k, \end{cases}$$

where u and w are two positive integers both coprime to p. Hence we have,

$$o\left((a^x, b^y)^{2^{\alpha-r}}\right) = \begin{cases} 1, & \text{if } r < 2^k, \\ p^{\beta-s} & \text{if } r \geq 2^k. \end{cases} \tag{5.2.c}$$

Suppose that $o(a^x, b^y) = t$. Then we have,

$$\begin{aligned} & (a^x, b^y)^t = (1,1) \\ \Rightarrow \quad & a^{tx} = 1 \\ \Rightarrow \quad & 2^\alpha \mid 2^r tm \\ \Rightarrow \quad & 2^{\alpha-r} \mid t, \end{aligned}$$

since $2^{\alpha-r} \nmid m$ as m is odd. So from (5.2.c), we have

$$o(a^x, b^y) = \begin{cases} 2^{\alpha-r}, & \text{if } r < 2^k, \\ 2^{\alpha-r} p^{\beta-s} & \text{if } r \geq 2^k. \end{cases} \tag{5.2.d}$$

Hence we can count the number of elements of $C_{2^\alpha} \ltimes_\theta C_{p^\beta}$ having a given order, and construct the following table:

Orders of group elements	Cardinalities of corresponding order subsets
1	1
$2^{\alpha-r}$, $(0 \leq r < 2^k)$	$2^{\alpha-r-1}p^\beta$
$2^{\alpha-r}$, $(2^k \leq r < \alpha)$	$2^{\alpha-r-1}$
$p^{\beta-s}$, $(0 \leq s < \beta)$	$p^{\beta-s-1}(p-1)$
$2^{\alpha-r}p^{\beta-s}$, $(2^k \leq r < \alpha,\, 0 \leq s < \beta)$	$2^{\alpha-r-1}p^{\beta-s-1}(p-1)$

From this table, we get that $C_{2^\alpha} \ltimes_\theta C_{p^\beta}$ is a non-abelian POS-group. □

Remark 5.2.3. For $p = 5$, taking $z = -1$ in the proof of the above theorem, we get another class of non-abelian POS-groups, namely, $C_{2^\alpha} \ltimes_\theta C_{5^\beta}$ where $\alpha \geq 2$ and $\beta \geq 1$. We have the following table:

Orders of group elements	Cardinalities of corresponding order subsets
1	1
2^α	$2^{\alpha-1}5^\beta$
$2^{\alpha-r}$, $(1 \leq r < \alpha)$	$2^{\alpha-r-1}$
$5^{\beta-s}$, $(0 \leq s < \beta)$	$2^2 5^{\beta-s-1}$
$2^{\alpha-r}5^{\beta-s}$, $(1 \leq r < \alpha,\, 0 \leq s < \beta)$	$2^{\alpha-r+1}5^{\beta-s-1}$

Remark 5.2.4. Consider the semidirect product $C_6 \ltimes_\theta C_7$. Using the same argument in the above theorem, we get that $C_6 \ltimes_\theta C_7$ is a non-abelian POS-group. In this case we consider the homomorphism $\theta : C_6 \to \mathrm{Aut}(C_7)$ given

by $\theta(a)(b) = b^2$ where a and b are generators of C_6 and C_7 respectively. We have the following table:

Orders of group elements	Cardinalities of corresponding order subsets
1	1
2	1
3	14
6	14
7	6
14	6

5.3 Dihedral groups

Lemma 5.3.1. *Consider the dihedral group*

$$D_{2n} = \langle x,\, y \,|\, y^n = 1,\, x^2 = 1,\, xy = y^{-1}x \rangle$$

of order $2n$, $n \geq 2$. *Let* $x \in D_{2n}$ *be such that* $o(x) = i$, $i \neq 2$. *Then* $|OS(x)| = \phi(i)$.

Proof. $|OS(x)| = |\{y \in D_{2n} | o(y) = i\}|$ consists of rotation of order i. Now $\langle r \rangle$ is the subgroup of rotation of D_{2n} of order n. So if $y \in OS(x)$, then $y = r^m$ for some m and

$$o(y) = o(r^m) = \frac{n}{\gcd(m, n)} = i.$$

Hence the elements in $OS(x)$ are all rotations of the form r^s such that $o < s < n$ and $\gcd(s, n) = \dfrac{n}{i}$.

Let $\frac{n}{i} = d$, then $r^s \in OS(x)$ if and only if $\gcd(\frac{s}{d}, \frac{n}{d}) = 1$ and $0 < s < n$. The number of such s is $\phi(\frac{n}{d}) = \phi(i)$, where ϕ is Euler's phi function. Thus we have, $|OS(x)| = \phi(i)$.

□

Theorem 5.3.2. *The dihedral group*

$$D_{2n} = \langle x, y \,|\, y^n = 1, x^2 = 1, xy = y^{-1}x \rangle$$

is a POS-group if and only if $n = 3^l$, *for some* $l \geq 1$.

Proof. Suppose that $n = 3^l$. Let $x \in D_{2n}$ be such that $o(x) = 2$. Since n is odd, only the reflections have order 2. So $|OS(x)| = n$ which clearly divides $|D_{2n}|$.

If $|o(x)| \neq 2$ divides n, then we must have $o(x) = 3^q$ for some $o \leq q \leq l$. When $q > 0$, we have

$$\phi(o(x)) = \phi(3^q) = 3^q(1 - \frac{1}{3}) = 2.3^{q-1}$$

which divides $2n$. When $q = 0$, then $o(x) = 1$ and $|OS(x)| = 1$. So D_{2n} is a POS-group when $n = 3^l$.

Conversely, suppose that D_{2n} is a POS-group. D_{2n} is the group of symmetries of a regular n gon, the dihedral group splits into n rotations and n reflections. Suppose that n is even. Then the only rotation of order 2 is the rotation by 180°. Also each reflection has order 2. Hence if $x \in D_{2n}$ such that $o(x) = 2$, then $|OS(x)| = n + 1$. Since $n + 1$ is odd and $n + 1 > n$, this is not possible. Hence D_{2n} is not a POS-group when n is even.

Now assume that n is odd. We have assumed that D_{2n} is a POS-group. So if $x \in D_{2n}$ such that $o(x) = n$, then $|OS(x)|$ must divide $|D_{2n}| = 2n$. Now

$\phi(n)$ divides $2n$. Also $\gcd(2, n) = 1$ and $\phi(2) = 1$. So $\phi(n) = \phi(n)\phi(2) = \phi(2n)$.

From lemma 5.1.1, $\phi(n)$ divides $2n$ if and only if $2n = 2^k 3^l$ with $k \geq 1$. Since n is odd, we must have $n = 3^l$ for some $l \geq 1$. □

We have the following result for the quasi-dihedral group.

Theorem 5.3.3. *The quasi-dihedral group*

$$QD_n = \langle a, b \,|\, a^{2^{m-1}} = 1, b^2 = 1, ba = a^{2^{m-2}+1}b \rangle$$

where $n = 2^m$, $m \geq 4$ is not a POS-group.

Proof. Suppose that QD_n is a POS-group. Let $r \in QD_n$ be such that $o(r) = 2$. We shall show that QD_n is not a POS-group by showing that $|OS(r)|$ does not divide n. To begin, we shall show that for $0 < i < \frac{n}{2}$ there is only one element of the form a^i with order 2.

If $o(a^i) = 2$, then since $o(a) = \frac{n}{2}$, we have

$$\begin{aligned} 2i &\equiv 0 (\text{mod } \frac{n}{2}) \\ \Rightarrow\ i &\equiv 0 (\text{mod } \frac{n}{4}). \end{aligned}$$

Since $0 < i < \frac{n}{2}$, we must have $i = \frac{n}{4}$. Let $a^j b \in QD_n$ be such that $o(a^j b) = 2$ where $0 \leq j < \frac{n}{2}$. Now

$$\begin{aligned} ba &= a^{2^{m-2}+1}b \\ \Rightarrow\ a &= b^{-1}(a^{\frac{n}{4}} + 1)b \\ \Rightarrow\ a^j &= b^{-1}a^{(\frac{n}{4}+1)j}b \\ \Rightarrow\ ba^j &= a^{(\frac{n}{4}+1)j}b. \end{aligned}$$

So we have $a^j ba^j b = a^j a^{(\frac{n}{4}+1)j} bb = a^{(\frac{n}{4}+2)j}$. Since $o(a^j b) = 2$, we have

$$\begin{aligned}
(\frac{n}{4}+2)j &\equiv 0(\text{mod } \frac{n}{2}) \\
\Rightarrow\ (2^{m-2}+2)j &\equiv 0(\text{mod } 2^{m-1}) \\
\Rightarrow\ 2j(2^{m-2}+2) &\equiv 0(\text{mod } 2^{m-1}) \\
\Rightarrow\ j(2^{m-3}+1) &\equiv 0(\text{mod } 2^{m-1}).
\end{aligned}$$

When $m > 3,\ \gcd(1+2^{m-3}, 2^{m-2}) = 1$. So $j \equiv 0(\text{mod}2^{m-2})$. Hence j must be a multiple of 2^{m-2} i.e. $\frac{n}{4}$. Thus the number of elements of the form $a^j b$ with order 2 is 2. Therefore, if $t \in QD_{2n}$ such that $o(t) = 2$, then $|OS(t)| = 3$ and 3 does not divide n since $n = 2^m$. This is a contadiction. So QD_n is not a POS-group. □

Theorem 5.3.4. *The semi-dihedral group*

$$SD_n = \langle s,\, t \,|\, s^{2^{m-1}} = 1,\, t^2 = 1,\, ts = s^{2^{m-2}-1}t \rangle$$

where $n = 2^m$, $m \geq 3$ is not a POS-group.

Proof. Supose SD_n is a POS-group. We shall show that there are $\frac{n}{2}$ elements of the form $s^i t$, where $0 \leq i < \frac{n}{2}$. Furthermore, half of these elements have i even, and half have i odd. Thus, there are $\frac{n}{4}$ elements of the form $s^i t$ when i is even and $\frac{n}{4}$ elements of the form $s^i t$ when i is odd. We claim that $o(s^i t) = 2$ if and only if i is even.

We have

$$\begin{aligned} ts &= s^{2^{m-2}-1}t \\ \Rightarrow s &= t^{-1}s^{(\frac{n}{4}-1)}t \\ \Rightarrow s^i &= t^{-1}s^{(\frac{n}{4}-1)i}t \\ \Rightarrow ts^i &= s^{(\frac{n}{4}-1)i}t. \end{aligned}$$

Now

$$\begin{aligned} s^its^it &= s^is^{(\frac{n}{4}-1)i}tt \\ &= s^{i+\frac{n}{4}i-i}t^2 \\ &= s^{\frac{in}{4}}. \end{aligned}$$

Since $o(s) = \frac{n}{2}$, we have $s^{\frac{in}{4}} = 1$ if and only if $\frac{in}{4} \equiv o(\mathrm{mod}\frac{n}{2})$, *i.e.*, if and only if $i \equiv 0(\mathrm{mod}2)$.

Let $o < j < \frac{n}{2}$. We claim that $o(s^j) = 2$ if and only if $j = \frac{n}{4}$. Suppose that $j = \frac{n}{4}$. Then $(s^j)^2 = s^{\frac{n}{2}} = 1$. Conversely supppose $o(s^j) = 2$ for some $0 < j < \frac{n}{2}$. Since $s^{2j} = 1$, $\frac{n}{2}$ divides $2j$, and so, we have

$$j \equiv 0(\mathrm{mod}\frac{n}{4}).$$

Since $0 < j < \frac{n}{2}$, there is exactly one value for j, namely $j = \frac{n}{4}$, which satisfies this condition.

Now let $r \in SD_n$ such that $o(r) = 2$. Then $|OS(r)| = \frac{n}{4}+1$. Since we have assumed that SD_n is a POS-group, $|OS(r)|$ must divide $|SD_n| = n = 2^m$. The divisors of n larger than $\frac{n}{4}$ are only $\frac{n}{2}$ and n itself. Now if $\frac{n}{4} + 1 = \frac{n}{2}$, then this equation does not have an integer solution and if $\frac{n}{4} + 1 = \frac{n}{2}$ then

we have $n = 4$. But $n \geq 8$, by assumption. So we have a contradiction. Therefore $|OS(r)|$ does not divide n and SD_n is not a POS-group. □

5.4 Quaternion groups

Theorem 5.4.1. *The generalized quaternion group*

$$Q_n = \langle x,\, y \,|\, x^{2^{m-1}} = 1,\, y^2 = x^{2^{m-2}},\, yx = x^{-1}y \rangle$$

where $n = 2^m$, $m \geq 3$ is not a POS-group.

Proof. Let $x \in Q_n$ such that $o(x) = 4$. We shall show that Q_n is not a POS-group by showing that $|OS(x)|$ does not divide n. There are $\frac{n}{2}$ elements of the form $x^i y$ where $0 \leq i < \frac{n}{2}$. We claim that $|x^i y| = 4 \; \forall \, 0 \leq i < \frac{n}{2}$. Now $x = y^{-1}x^{-1}y$, and so, $x^i = y^{-1}x^{-i}y$. Therefore,

$$x^i y x^i y = x^i y (y^{-1}x^{-i}y)y = y^2 = x^{2^{m-2}}.$$

Hence $o(x^i y) \neq 2$. Clearly $o(x^i y) \neq 3$ since 3 does not divide n. Now

$$(x^i y x^i y)^2 = (x^{2^{m-2}})^2 = x^{2m-1} = 1.$$

So $o(x^i y) = 4$ and we have at least $\frac{n}{2}$ elements of order 4. Now let $j \in \mathbb{N}$ and $0 \leq j < \frac{n}{2}$. Since $o(x^{\frac{n}{2}}) = 4$, so there is at least one element of the form x^j with order 4. Let $k \in \mathbb{N}$ be the number of elements of the form x^j that have order 4. Hence the total number of elements of order 4 is $\frac{n}{2} + k$. For Q_n to be a POS-group, $\frac{n}{2} + k$ should divide $|\, Q_n \,| = n$. So $k = 0$ or $\frac{n}{2}$. But $k \neq 0$ since $|OS(x)| = |\{y \in G | o(y) = 4\}|$ is non-empty. So $k = \frac{n}{2}$, but there are only $\frac{n}{2} - 1$ elements of the form x^j with $o < j < \frac{n}{2}$ which is a contradiction. So Q_n is not a POS-group. □

5.5 Linear groups

$SL(2,q)$ is the group of all 2×2 matrices of determinant one with the entries from the finite field $\mathbb{F}_q$ of q elements, where $q = p^n$ for some prime p. We shall show that $SL(2,q)$ is a POS-group if it satisfies certain conditions.

Theorem 5.5.1. *$SL(2,q)$ has perfect order subsets if and only if*

$$q \in \{2,\ 3,\ 5,\ 7,\ 9,\ 11,\ 17,\ 19,\ 41,\ 49,\ 127,\ 251\}.$$

Proof. The exact number of conjugacy classes in $SL(2,q)$ is $q+4$ when q is odd and $q+1$ when q is even. We construct the table 5.5.2 for the structure of conjugacy classes when q is odd and table 5.5.3 when q is even.

Conjugacy class Representative	Order of the Representative	Cardinality of the class
1	1	1
z	2	1
c	p	$\frac{q^2-1}{2}$
d	p	$\frac{q^2-1}{2}$
zc	$2p$	$\frac{q^2-1}{2}$
zd	$2p$	$\frac{q^2-1}{2}$
$a^l,\quad 1 \le l \le \frac{q-3}{2}$	$\frac{q-1}{\gcd(l,q-1)}$	$q(q+1)$
$b^m,\quad 1 \le m \le \frac{q-1}{2}$	$\frac{q+1}{\gcd(m,q+1)}$	$q(q-1)$

Table 5.5.2: q is odd

Conjugacy class Representative	Order of the Representative	Cardinality of the class
1	1	1
c	2	q^2-1
$a^l, \quad 1 \leq l \leq \frac{q-2}{2}$	$\frac{q-1}{\gcd(l,q-1)}$	$q(q+1)$
$b^m, \quad 1 \leq m \leq \frac{q}{2}$	$\frac{q+1}{\gcd(m,q+1)}$	$q(q-1)$

Table 5.5.3: q is even

From table 5.5.2 we see that the number of elements of each of the orders 1, 2, p and $2p$ divides the order of $SL(2,q)$ for any value of q. So the restrictions on q are imposed by the order subsets determined by the elements a^l and b^m. The same is true when q is even, as can seen from Table 5.5.3.

Let d be a divisor of $q-1$ with d not equal to $\frac{q-1}{2}$ or $q-1$. By lemma 1.4.7 the number of positive integers $l \leq q-1$ such that $\gcd(l,q-1)=d$ is $\phi\left(\frac{q-1}{d}\right)$. By lemma 1.4.2 the number of such integers $l < \frac{q-1}{2}$ is $\frac{\phi(\frac{q-1}{d})}{2}$. Hence the total number of elements in $SL(2,q)$ of order $\frac{q-1}{d}$ is $\frac{\phi(\frac{q-1}{d})}{q}(q+1)$. From lemma 1.4.8 it is clear that we have to consider only the case when $d=1$. A similar argument holds for b^m. Using corollaries 1.4.5 and 1.4.6 we get that the total number of elements in $SL(2,q)$ of order $q-1$ is $\frac{\phi(q-1)}{q}(q+1)$ and the total number of elements in $SL(2,q)$ of order $q+1$ is $\frac{\phi(q+1)}{q}(q+1)$. Summarizing all these, we have $SL(2,q)$ is a POS-group if and only if $\frac{2(q-1)}{\phi(q-1)}$ and $\frac{2(q+1)}{\phi(q+1)}$ are both integers. We use theorem 1.4.9 for finding the values of

q. Here $m = q \pm 1$. We get the following twelve equations:

$$3^b - 3^a = 2$$
$$2^{c-1} - 2^{a-1}5^b = 1$$
$$2^{b-1} - 2^{a-1} = 1$$
$$2^{b-1}3^c - 2^{a-1} = 1$$
$$2^{c-1} - 2^{a-1}3^b = 1$$
$$2^{c-1}5^d - 2^{a-1}3^b = 1$$
$$2^{c-1}3^d - 2^{a-1}5^b = 1$$
$$2^{b-1}5^c - 2^{a-1} = 1$$
$$2^{b-1}3^c7^d - 2^{a-1} = 1$$
$$2^{d-1} - 2^{a-1}3^b7^c = 1$$
$$2^{c-1}3^d7^e - 2^{a-1}5^b = 1$$
$$2^{d-1}5^e - 2^{a-1}3^b7^e = 1$$

Solving these equations by using a combination of divisibility, congruence and Pell equation arguments, we get the following table:

Equation	$q-1$	$q+1$	Solutions	Corresponding q
$3^b - 3^a = 2$	3^a	3^b	$(0,1)$	2
$2^{c-1} - 2^{a-1}5^b = 1$	2^a5^b	2^c	none	none
$2^{b-1} - 2^{a-1} = 1$	2^a	2^b	$(1,2)$	3
$2^{b-1}3^c - 2^{a-1} = 1$	2^a	2^b3^c	$(2,1,1)$	5
			$(4,1,2)$	17
$2^{c-1} - 2^{a-1}3^b = 1$	2^a3^b	2^c	$(1,1,3)$	7
$2^{c-1}5^d - 2^{a-1}3^b = 1$	2^a3^b	2^c5^d	$(1,2,2,1)$	19
			$(4,1,1,2)$	49
$2^{c-1}3^d - 2^{a-1}5^b = 1$	2^a5^b	2^c3^d	$(1,1,2,1)$	11
			$(5,1,1,4)$	$161 = 7 \times 23$
$2^{b-1}5^c - 2^{a-1} = 1$	2^a	2^b5^c	$(3,1,1)$	9
$2^{b-1}3^c7^d - 2^{a-1} = 1$	2^a	$2^b3^c7^d$	none	none
$2^{d-1} - 2^{a-1}3^b7^c = 1$	$2^a3^b7^c$	2^d	$(1,2,1,7)$	127
$2^{c-1}3^d7^e - 2^{a-1}5^b = 1$	2^a5^b	$2^c3^d7^e$	$(3,1,1,1,1)$	41
			$(1,3,2,2,1)$	251
$2^{d-1}5^e - 2^{a-1}3^b7^e = 1$	$2^a3^b7^e$	2^d5^e	none	none

The theorem now follows from the above table. □

Proposition 5.5.4. *The projective special linear group $PSL(2,q)$, where $q > 3$ is prime, do not have perfect order subsets.*

Proof. Let S be a Sylow q-subgroup of $PSL(2,q)$. Since $|PSL(2,q)| = \frac{q(q-1)(q+1)}{2}$, we have $|S| = q$ and $C_G(S) = S$. Assume that G contains exacly one conjugacy class of elements of order q. We count the number N of elements of order q in two ways. First, we see that $N = \frac{|G|}{|S|} = \frac{(q-1)(q+1)}{2}$. Let

k be the number of Sylow $q-$subgroups of G. Then $N = k(q-1)$ and so $k = \frac{q+1}{2}$. But this is impossible as $k \equiv 1 (\mathrm{mod}\, q)$. □

PROBLEM : To determine whether or not $GL(n, F)$ is a POS-group.

5.6 Alternating group

In [9], Finch and Jones have proved that if $n \geq 4$ is a positive integer such that n or $n-1$ is a prime, then the alternating group A_n is not a POS-group. They conjectured that A_n is a not a POS-group for all $n \geq 4$. A. K. Das [4] has settled this conjecture as follows.

Proposition 5.6.1. *For $n \geq 3$, the alternating group A_n is not a POS-group.*

Proof. Consider a positive integer $n \geq 3$. Then, in view of Result 1.4.1, either n or $n-1$ can be written as the sum of distinct odd primes $p_1, p_2, \ldots, p_k$ where $k \geq 1$). If $x \in A_n$ is such that $o(x) = p_1 p_2 \ldots p_k$, then $|OS(x)| = |\{y \in A_n : o(y) = p_1 p_2 \ldots p_k\}| = \frac{n!}{p_1 p_2 \ldots p_k}$ which does not divide $|A_n| = \frac{n!}{2}$. Hence A_n is not a POS-group. □

PROBLEM : To determine whether or not S_n is a POS-group.

We conclude this chapter and also the dissertation by observing that the notion of POS-groups provides us with yet another interesting bridge between the theory of finite groups and the theory of numbers. Also, being a relatively new concept have enough scope for future research. It will also be an interesting work to classify all finite POS-groups.

Bibliography

[1] P. B. Bhattacharya, S. K. Jain, S. R. Nagpal *"Basic abstract algebra"*, second edition, Cambridge University Press, Cambridge, 1997.

[2] J. L. Brown, Jr., *Generalization of Richert's Theorem*, Amer. Math. Monthly, **83**(2) (1976), 631–634.

[3] D. Burton, *Elementary number theory*, (Second Edition), Wm. C. Brown Publishers, Dubuque, Iowa, 1989.

[4] A. K. Das, *On finite groups having perfect order subsets*, International Journal of Algebra, Vol. 3, **29**, (2009), 629–637.

[5] R. E. Dressler, *A Stronger Bertrand's Postulate with an Application to Partitions*, Proc. Amer. Math. Soc. **33** No. 2, (1972), 226–228.

[6] X. Du and W. Shi, *Finite groups with conjugacy classes number one greater than its same order classes number*, Communications in Algebra, **34** (2006), 1345–1359.

[7] W. Feit and G.M. Seitz, *On finite rational groups and related topics*, Illinois J. Math **33** (1989), 103–131.

[8] C. E. Finch and L. Jones *A curious connection between Fermat numbers and finite groups*, Amer. Math Monthly **109** (2002), 517–524.

[9] C. E. Finch and L. Jones *Nonabellian groups with perfect order subsets*, JP J. Algebra Number Theory Appl. **3** No. 1, (2003), 13–26. See also: Corrigendum to: *"Nonabelian groups with perfect order subsets" [JP J. Algebra Number Theory Appl.* **3** *No. 1, (2003), 13–26]*, JP J. Algebra Number Theory Appl. **4** No. 2, (2004), 413–416.

[10] P. Fitzpatrick, *Order conjugacy in finite groups*, Proc. R. Ir. Acad., **85A** No. 1, (1985), 53–58.

[11] J. A. Gallian, *"Contemporary Abstract Algebra "*, 2nd edition D. C. Heath, 1990

[12] M. Hall, *Theory of groups*, Macmillan, New York, 1959.

[13] N. Jacobson, *"Basic Algebra I"*, W. H. Freeman and Co., San Francisco, 1974.

[14] H. Kurzweil, B. Stellmacher, *The Theory of Finite Groups, An Introduction*, "Springer", UTX, New York, 2004.

[15] C. Li, *Finite groups in which every pair of elements of the same order is either conjugate or inverse conjugate*, Communications in Algebra, **22** No.8, (1994), 2807–2816.

[16] S. Libera and P. Tlucek, *Some perfect order subset groups*, Pi Mu Epsilon Journal, **11** (2003), 495–498.

[17] V. D. Mazurov, *The Kourovka Notebook. Unsolved problems in group theory*, Amer. Math. Soc. Trans. Ser. 2, Vol. 121. Providence, RI.

[18] D. J. S. Robinson, *A course in the theory of groups* (Second Edition), Graduate Text in Mathematics **80**, Springer, New York, 1996.

[19] J. J. Rotman, *An Introduction to the Theory of Groups*, 3rd edition, Allyn and Bacon, Inc, 1984.

[20] W. R. Scott, *"Group Theory"*, Dover Publications, Inc., New YorK, 1987.

[21] S. Sezer and Robert W. Van der Waall, *Finite groups all of whose abelian subgroups of equal order are conjugate*, Turk. J. Math, **30** (2006), 139–175.

[22] M. Suzuki, *Finite groups with nilpotent centralisers*, Trans. Am. math. Soc., **99** (1961), 425–470.

[23] S. A. Syskin, *Abstract properties of the simple sporadic groups*, Russ. Math. Surveys, **35** (1980), 209–246.

[24] Robert W. Van der Waall and Adaouia Bensaid, *On finite groups whose elements of equal order are conjugate*, Simon Stevin, **65** No. 3-4 (1991), 361–374.

[25] Robert W. Van der Waall, *Finite groups whose subgroups of equal order are conjugate*, Indagationes Math, **4** (1993), 239–254.

[26] X. You, G. Qian and W. Shi, *Finite groups in which elements of the same order outside the center are conjugate*, Science in China Series A: Mathematics, October **50** No. 10, (2007), 1493–1500.

[27] J. P. Zhang, *About Syskin problem of finite groups*, Sci. in China **18** No. 2, (1988), 124–128.

[28] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.4.12; 2008, (`http://www.gap-system.org`).

Brief Bio-data

1. Name:	SARBANI KONWAR
2. Sex:	Female
3. Date of birth:	27^{th} June, 1983.
4. Father's Name:	Shri Ratneswar Konwar
5. Nationality:	Indian
6. Permanent Address:	East Milannagar, P.O. - C. R. Building Dist. - Dibrugarh, Assam, Pin - 786 003.
7. Academic Qualification:	M. Sc. in Mathematics, Gauhati University.

8. Workshop/Conference attended:
UGC-SAP workshop on *Algebra, Algebraic Topology and related topics*, held at North-Eastern Hill University, Meghalaya, organized by Dept. of Mathematics, NEHU, Meghalaya, from March 15 to 20, 2010.