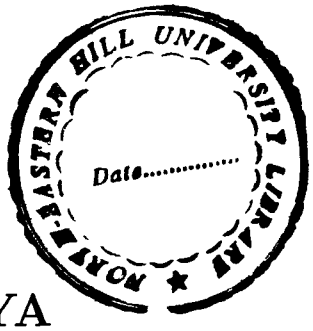
GENERALIZATIONS OF CERTAIN NUMBER THEORETIC CONCEPTS VIA FINITE GROUPS –A SURVEY



ABSTRACT

SEKHAR JYOTI BAISHYA
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
JUNE, 2008

ABSTRACT

Number theory and Group theory are two such branches of mathematics which play a very interesting role in complementing and suplementing each other. Fermat's Little theorem, Quadratic Reciprocity Law and Arithmetic Functions are considered as three jems in number theory. These three topics often play a very crucial role in almost every branch of mathematical sciences. The aim of this disertation is to study the generalizations of these concepts via finite groups. The choice of topics covered in this disertation was motivated primarily by their applicability in classification of finite groups.

One very interesting feature of this disertation is that it can be easily understood with some amount of mathematical knowledge. Ofcourse, there is a chapter on preliminaries in which we recall a few standard facts from Group Theory (including Character Theory), Field Theory and Number Theory. Another important feature is that even though this disertation contains three topics which look independent of one another, one can see that they are actually interlinked through the notion of functions. In other words we can say that this disertation is a chain of three beads.

In October, 1640, a French Mathematician called "Pierre de Fermat" communicated the following theorem to his friend "Frenicle de Bessy".

If p is a prime and a is any integer not divisible by p, then p divides $a^{p-1} - 1$. i,e

$$a^{p-1} \equiv 1 \pmod{p}.$$

This theorem has since been called as " Fermat's Little Theorem (F.L.T.)" or simply " Fermat's Theorem". Almost 100 years later, in 1736 Leonhard Euler gave the first proof of the little theorem. Thereafter many Mathematicians have given sevaral proofs of this theorem, the simplest of them being the one given by the cyclic group of residue classes of integers modulo p, p a prime.

One may ask what happens to the above result when p is not a prime. The answer to this question lies in the following result which is essentially due to C.F.Gauss :

Let a be an arbitrary integer. Then for every positive integer n,

$$\sum_{d|n} \mu(d) a^{n/d} \equiv 0 \pmod{n},$$

where μ is the usual number theoretic Möbius function.

(This also generalizes Euler's Theorem i.e., if $\gcd(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$, $m \geq 1$.) The case when a is a prime was settled by Gauss and his result was published posthumously in 1863. However the general case was settled during the years 1880 to 1883 when four independent proofs was given by Kantor, Weyr, Lucas, and Pellet. Recently 1986, C.J.Smith [1] gave a coloring proof of a more general result. In the year 2006 Pournaki [3] gave a group theoretic generalization of the Gauss's result as follows:

Let G be a finite group of order n and let $\mathbb{C}^*$ be the multiplicative group of non zero complex numbers. If $f : G \longrightarrow \mathbb{C}^*$ is a group homomorphism, then

$$\sum_{g \in G} f(g) a^{n/o(g)} \equiv 0 \pmod{n},$$

for any integer a.

The main objective of Chapter 2 in this dissertation is to study the above mentioned generalization.

In 1796 C. F. Gauss at the age of nineteen proved the first number theoretic reciprocity law, the classical law of Quadratic Reciprocity. It states that if p and q are two distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

where $\left(\frac{\cdot}{q}\right)$ is the Legendre Symbol. This result can be written in a more elegant form using the Kronecker Symbol and the Jacobi Symbol as $\left(\frac{a}{n}\right) = \left(\frac{n^*}{a}\right)$, where n is an odd positive integer, a any integer and $n^* = (-1)^{\frac{n-1}{2}}n$. Using concepts and results known at least hundred years ago, W. Duke and K. Hopkins [26] in 2005 generalized the above result via finite groups as follows:

Let a be a positive integer and G is a finite group of odd order n then

$$\left(\frac{a}{G}\right) = \left(\frac{n^*}{a}\right),$$

where $\left(\frac{a}{G}\right) = o$ if $gcd\,(a,n) \neq 1$ and $\left(\frac{a}{G}\right)$ is the signature of the permutation of the conjugacy classes in G induced by the map $g \longmapsto g^a$ from G to itself, if $gcd\,(a,n) = 1$.

In Chapter 3 we have studied elaborately the above result.

Finaly, in Chapter 4 we consider $\mathcal{G}$ and $\mathcal{X}$ to be the collection of all finite groups and collection of all finite abelian groups (upto isomorphism). Moreover we consider $\mathcal{A}(\mathcal{G})$ and $\mathcal{A}(\mathcal{X})$ which are the collections of all complex-valued functions with domain $\mathcal{G}$ and $\mathcal{X}$ respectively.

In the next section we consider the set (counting multiplicities) $\mathcal{C}(G) = \{H_i/H_{i-1} : i = 1, 2, \ldots, n\}$, where H_i/H_{i-1}'s are composition factors of G. We define convolution of two functions $f, g \in \mathcal{A}(\mathcal{G})$, E-convolution and D-convolution of two functions $f, g \in \mathcal{A}(\mathcal{X})$ and study some properties of these convolutions. Some of the important results in this section are as follows: **Theorem 4.2.5.**, **Theorem 4.2.11.**, **Theorem 4.2.16.**

$\mathcal{A}(\mathcal{G})$ and $\mathcal{A}(\mathcal{X})$ are commutative rings with identity ε under the additive and the multiplicative operations given by ordinary addition and appropriate convolution of funcitons.

We also study the notion of coprimeness and multiplicativity for groups in $\mathcal{G}$ as well as in $\mathcal{X}$. Some of the main results in this regard are as follows:

Theorem 4.4.7. *If $f, g \in \mathcal{A}(\mathcal{G})$ are multiplicative then $(f * g) \circ \rho \in \mathcal{A}(\mathcal{G})$ is also multiplicative.*

Theorem 4.4.8. *If $f, g \in \mathcal{A}(\mathcal{G})$ then $(f * g) \circ \rho = (f \circ \rho) * (g \circ \rho)$.*

Theorem 4.4.10. *If $f \in \mathcal{A}(\mathcal{G})$ with $f(E_0) \neq 0$ then there is a unique $g \in \mathcal{A}(\mathcal{G})$ such that $f * g = g * f = \varepsilon$.*

Corollary 4.4.11. *The set of all functions $f \in \mathcal{A}(\mathcal{G})$ with $f(E_0) \neq 0$ forms an abelian group under the operation given by convolution.*

Theorem 4.4.12. *If $f, g \in \mathcal{A}(\mathcal{G})$ are such that $f \circ \rho$ and $(f * g) \circ \rho$ are multiplicative then $g \circ \rho$ is also multiplicative.*

Corollary 4.4.13. *The set of all multiplicative functions in $\mathcal{A}(\mathcal{G})$ of the form $f \circ \rho$, where $f \in \mathcal{A}(\mathcal{G})$, is an abelian group under the operation given by convolution.*

Where $\rho : \mathcal{G} \longrightarrow \mathcal{G}$ is given by $\rho(G) = \Pi\mathcal{C}(G) \quad , G \in \mathcal{G}$.

In this chapter we have also studied the analogues of the usual number

theoretic Möbius Function and the Liouville's function. Some of the main results in this direction are:

Theorem 4.5.3. *The Möbius Function $\mu \in \mathcal{A}(\mathcal{G})$ is multiplicative.*

Theorem 4.5.6. $\mu * u = u * \mu = \varepsilon$ *i.e.,* $\mu^{-1} = u$ *and* $u^{-1} = \mu$.

Theorem 4.5.10. $\lambda * \mu^2 = \mu^2 * \lambda = \varepsilon$ *i.e.,* $\lambda^{-1} = \mu^2$ *where μ^2 is the ordinary product of μ with itself, and λ is the group theoretic Liouville's function.*

Theorem 4.5.12. *Let $f \in \mathcal{A}(\mathcal{G})$ be a mulptiplicative function such that $f = f \circ \rho$. Then*

f is completely multiplicative if and only if $f * (\mu f) = (\mu f) * f = \varepsilon$.

i.e., $f^{-1} = \mu f$ *where μf is the ordinary product of μ and f.*

As applications of the abelian version of Möbius Function we have:

Theorem 4.6.2. *Let $G_m = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, m-times. Then number of subgroups of G_m of order $p^n (n \leq m)$ is*

$$\frac{(p^m - 1)(p^{m-1} - 1) \ldots (p^{m-n+1} - 1)}{(p-1)(p^2 - 1) \ldots (p^n - 1)}.$$

Theorem 4.6.3. *Let $G_m = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, m-times. Then*

$$\hat{\mu}(G_m) = (-1)^m p^{\frac{1}{2}m(m-1)}.$$

Theorem 4.6.4. *Let $G = \mathbb{Z}_p^{m_1} \times \mathbb{Z}_p^{m_2} \times \cdots \times \mathbb{Z}_p^{m_r}$, m-times, where atleast one $m_i \geq 2$, $i = 1, 2, \ldots, r$. Then*

$$\hat{\mu}(G) = 0.$$

Final part of this chapter is devoted to the study of divisor functions, structure of the normal subgroups of the product of two groups and characterization of groups using divisor functions. Some important results here are:

Theorem 4.8.1. *Let G_1 and G_2 be coprime groups. Then the normal subgroups of the product $G_1 \times G_2$ are exactly the subgroups of the form $N_1 \times N_2$, with $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

Theorem 4.8.2. *Let G_1 and G_2 be any two groups. Then the following conditions are equivalent:*

(i) *Every normal subgroup of the product $G_1 \times G_2$ is of the form $N_1 \times N_2$ with $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

(ii) *For each $H_1 \triangleleft G_1$ and for each $H_2 \triangleleft G_2$, the centres $Z(G_1/H_1)$ and $Z(G_2/H_2)$ of the quotient groups G_1/H_1 and G_2/H_2 have no subgroup in common.*

Theorem 4.9.6. (Abelian Quotient Theorem)

If G is a group with $\sigma(G) \leq 2|G|$ then any abelian quotient of G is cyclic.

Corollary 4.9.7.

(i) *If G is a perfect group then any abelian quotient of G is cyclic.*

(ii) *The perfect abelian groups are precisely the cyclic groups C_n of order n with n perfect.*

We conclude the dissertation by studying and computing some examples of non abelian perfect groups.

Bibliography

[1] C. J. Smyth, *A coloring proof of a Generalization of Fermat's Little Theorem*, Amer. Math. Monthly **93** (6) (1986), 469–471.

[2] J. B. Fraleigh, *A first course in abstract algebra* (Third Edition), Addison-Wesley Publishing Company, Inc., USA, 1982.

[3] M. R. Pournaki, *An extension of a result of Gauss to finite groups: A linear algebraic approach*, Elem. Math. **61** (1) (2006), 24–31.

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

[5] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, (Fifth Edition), John Wiley and Sons, Inc., New York, 2001.

[6] J. Zhang, *Arithmetical conditions on element orders and group structure*, Proc. Amer. Math. Soc. **123** (1) (1995), 39–44.

[7] E. Cohen, *Arithmetical functions of finite abelian groups*, Math. annalen **142** (1961), 165–182.

[8] R. Narasimhan, S. Raghavan, S. S. Rangachari, S. Lal, *Algebraic Number Theory*, Mathematical Pamplets 4, T.I.F.R. 1966.

[9] P. Samuel, *Algebraic Theory of Numbers* (trans. A. J. Silberger) Houghton Mifflin, Boston, 1970.

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

[11] N. Jacobson, *Basic Algebra, vol I* (W. H. Freeman and Company, U.S.A., 1974).

[12] I. M. Isaacs, *"Character Theory of Finite Groups"*, Dover Publications, Inc., New YorK, 1994.

[13] Ya. G. Berkovich, E. M. Zhmud', *Characters of finite groups. Part 1*, (Translations of Mathematical Monographs), Volume 172, American Mathematical Society.

[14] J. B. Dence and T. P. Dence, *Cubic and quartic residues modulo a prime*, Missouri j. math.sci. **7** (1995), 24–31.

[15] M. S. Lucido and M. R. Pournaki, *Elements with square roots in finite groups*, Algebra Colloq. **12** (4) (2005), 677–690.

[16] M. A. Brodie, R. F. Chamberlain and L. C. Kappe, *Finite coverings by normal subgroups*, Proc. Amer. Math. Soc. **104** (3) (1988), 669–674.

[17] A. Mann, *Finite groups containing many involutions*, Proc. Amer. Math. Soc. **122** (2)(1994), 383–385.

[18] P. S. Delsarte, *Fonctions de Möbius sur les groupes abeliens finis*, Annals of Math. **49** (3) (1948), 600–609.

[19] I. M. Isaacs and M. R. Pournaki, *Generalizations of Fermat's Little Theorem via group theory*, Amer. Math. Monthly **112** (8) (2005), 734–740.

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

[21] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer International Student Edition, (Narosa Publishing House, New Delhi, 1993).

[22] E. Zolotarev, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouv. Ann. Math (2), **11** (1872), 354–362.

[23] A. K. Das, *On arithmetic functions of finite groups*, Bull. Austral. Math. Soc. **75** (2007), 45–58.

[24] A. K. Das, *On group elements having square roots*, Bull. Iranian Math. Soc., **31(2)**, (2005), 33–36.

[25] T. Leinster, *Perfect numbers and groups*, arXiv:math.GR/0104012v1 Apr 2001.

[26] W. Duke and K. Hopkins, *Quadratic reciprocity in a finite group*, Amer. Math. Monthly **112** (3) (2005), 251–256.

[27] F. Menegazzo, *The number of generators of a finite group*, Irish Math. Soc. Bulletin. **50** (2003), 117–128.

[28] I. N. Herstein, *Topics in Algebra*, (Second Edition), Wiley Eastern Limited.(2006)

GENERALIZATIONS OF CERTAIN NUMBER THEORETIC CONCEPTS VIA FINITE GROUPS –A SURVEY

BY

SEKHAR JYOTI BAISHYA
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
JUNE, 2008

DS
512.7
BHI

CERTIFICATE

I certify that the dissertation entitled "GENERALIZATIONS OF CERTAIN NUMBER THEORETIC CONCEPTS VIA FINITE GROUPS - A SURVEY" submitted by Mr. Sekhar Jyoti Baishya 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

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

Supervisor

Department of Mathematics

North-Eastern Hill University

Shillong - 793022

Place: Shillong.

30^{th} June, 2008.

NORTH-EASTERN HILL UNIVERSITY

June, 2008

DECLARATION

I, Sekhar Jyoti Baishya, 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.

Sekhar Jyoti Baishya

Signature of the Candidate

Countersigned by:

Signature of the Head

Head
Department of Mathematics
North-Eastern Hill University
Shillong 793022

Signature of the Supervisor

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

ACKNOWLEDGEMENT

This work was carried out under the supervision of Dr. Ashish Kumar Das, Department of Mathematics, North-Eastern Hill University. I express profound indebtedness and gratitude to him for his guidence and invaluable help during the preparation of this dissertation.

My sincere thanks goes to Dr P. K. Saikia, Dr. S. Dutta and Dr. A. M. Buhphang, Department of Mathematics, N.E.H.U., for giving M. Phil courses and also for providing me with lots of help and suggestions.

My sincere thanks goes to Prof. H. K. Mukerjee, and Prof. M. B. Rege, Department of Mathematics, N.E.H.U., for their helpful and valuable suggestions.

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

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

I take this opportunity to thank all my friends and relatives for always encouraging me throughout the duration of this work.

Finally, I am grateful to all my family members, especially my mother and my elder brother Mr. J. J. Baishya, for giving me constant insprriation and support to continue my studies.

Sekhar Jyoti Baishya

PREFACE

Number theory and Group theory are two such branches of mathematics which play a very interesting role in complementing and suplementing each other. Fermat's Little theorem, Quadratic Reciprocity Law and Arithmetic Functions are considered as three jems in number theory. These three topics often play a very crucial role in almost every branch of mathematical sciences. The aim of this disertation is to study the generalizations of these concepts via finite groups. The choice of topics covered in this disertation was motivated primarily by their applicability in classification of finite groups.

One very interesting feature of this disertation is that it can be easily understood with some amount of mathematical knowledge. Ofcourse, there is a chapter on preliminaries in which we recall a few standard facts from Group Theory (including Character Theory), Field Theory and Number Theory. Another important feature is that even though this disertation contains three topics which look independent of one another, one can see that they are actually interlinked through the notion of functions. In other words we can say that this disertation is a chain of three beads.

In October, 1640, a French Mathematician called "Pierre de Fermat" communicated the following theorem to his friend "Frenicle de Bessy".

If p is a prime and a is any integer not divisible by p, then p divides $a^{p-1} - 1$. i,e

$$a^{p-1} \equiv 1 \pmod{p}.$$

This theorem has since been called as " Fermat's Little Theorem (F.L.T.)" or simply " Fermat's Theorem". Almost 100 years later, in 1736 Leonhard Euler gave the first proof of the little theorem. Thereafter many Mathematicians have given sevaral proofs of this theorem, the simplest of them being the one given by the cyclic group of residue classes of integers modulo p, p a prime.

One may ask what happens to the above result when p is not a prime. The answer to this question lies in the following result which is essentially due to C.F.Gauss :

Let a be an arbitrary integer. Then for every positive integer n,

$$\sum_{d|n} \mu(d) a^{n/d} \equiv 0 \pmod{n},$$

where μ is the usual number theoretic Möbius function.

(This also generalizes Euler's Theorem i.e., if $\gcd(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$, $m \geq 1$.) The case when a is a prime was settled by Gauss and his result was published posthumously in 1863. However the general case was settled during the years 1880 to 1883 when four independent proofs was given by Kantor, Weyr, Lucas, and Pellet. Recently 1986, C.J.Smith [1] gave a coloring proof of a more general result. In the year 2006 Pournaki [3] gave a group theoretic generalization of the Gauss's result as follows:

Let G be a finite group of order n and let $\mathbb{C}^*$ be the multiplicative group of non zero complex numbers. If $f : G \longrightarrow \mathbb{C}^*$ is a group homomorphism, then

$$\sum_{g \in G} f(g) a^{n/o(g)} \equiv 0 \pmod{n},$$

for any integer a.

The main objective of Chapter 2 in this dissertation is to study the above mentioned generalization.

In 1796 C. F. Gauss at the age of nineteen proved the first number theoretic reciprocity law, the classical law of Quadratic Reciprocity. It states that if p and q are two distinct odd primes then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

where $\left(\frac{\cdot}{q}\right)$ is the Legendre Symbol. This result can be written in a more elegant form using the Kronecker Symbol and the Jacobi Symbol as $\left(\frac{a}{n}\right) = \left(\frac{n^*}{a}\right)$, where n is an odd positive integer, a any integer and $n^* = (-1)^{\frac{n-1}{2}}n$. Using concepts and results known at least hundred years ago, W. Duke and K. Hopkins [26] in 2005 generalized the above result via finite groups as follows:

Let a be a positive integer and G is a finite group of odd order n then

$$\left(\frac{a}{G}\right) = \left(\frac{n^*}{a}\right),$$

where $\left(\frac{a}{G}\right) = o$ if $gcd\,(a,n) \neq 1$ and $\left(\frac{a}{G}\right)$ is the signature of the permutation of the conjugacy classes in G induced by the map $g \longmapsto g^a$ from G to itself, if $gcd\,(a,n) = 1$.

In Chapter 3 we have studied elaborately the above result.

Finaly, in Chapter 4 we consider $\mathcal{G}$ and $\mathcal{X}$ to be the collection of all finite groups and collection of all finite abelian groups (upto isomorphism). Moreover we consider $\mathcal{A}(\mathcal{G})$ and $\mathcal{A}(\mathcal{X})$ which are the collections of all complex-valued functions with domain $\mathcal{G}$ and $\mathcal{X}$ respectively.

In the next section we consider the set (counting multiplicities) $\mathcal{C}(G) = \{H_i/H_{i-1} : i = 1, 2, \ldots, n\}$, where H_i/H_{i-1}'s are composition factors of G. We define convolution of two functions $f, g \in \mathcal{A}(\mathcal{G})$, E-convolution and D-convolution of two functions $f, g \in \mathcal{A}(\mathcal{X})$ and study some properties of these convolutions. Some of the important results in this section are as follows: **Theorem 4.2.5.**, **Theorem 4.2.11.**, **Theorem 4.2.16.**

$\mathcal{A}(\mathcal{G})$ and $\mathcal{A}(\mathcal{X})$ are commutative rings with identity ε under the additive and the multiplicative operations given by ordinary addition and appropriate convolution of funcitons.

We also study the notion of coprimeness and multiplicativity for groups in $\mathcal{G}$ as well as in $\mathcal{X}$. Some of the main results in this regard are as follows:
Theorem 4.4.7. *If $f, g \in \mathcal{A}(\mathcal{G})$ are multiplicative then $(f * g) \circ \rho \in \mathcal{A}(\mathcal{G})$ is also multiplicative.*
Theorem 4.4.8. *If $f, g \in \mathcal{A}(\mathcal{G})$ then $(f * g) \circ \rho = (f \circ \rho) * (g \circ \rho)$.*
Theorem 4.4.10. *If $f \in \mathcal{A}(\mathcal{G})$ with $f(E_0) \neq 0$ then there is a unique $g \in \mathcal{A}(\mathcal{G})$ such that $f * g = g * f = \varepsilon$.*
Corollary 4.4.11. *The set of all functions $f \in \mathcal{A}(\mathcal{G})$ with $f(E_0) \neq 0$ forms an abelian group under the operation given by convolution.*
Theorem 4.4.12. *If $f, g \in \mathcal{A}(\mathcal{G})$ are such that $f \circ \rho$ and $(f * g) \circ \rho$ are multiplicative then $g \circ \rho$ is also multiplicative.*
Corollary 4.4.13. *The set of all multiplicative functions in $\mathcal{A}(\mathcal{G})$ of the form $f \circ \rho$, where $f \in \mathcal{A}(\mathcal{G})$, is an abelian group under the operation given by convolution.*
Where $\rho : \mathcal{G} \longrightarrow \mathcal{G}$ is given by $\rho(G) = \Pi\mathcal{C}(G)$, $G \in \mathcal{G}$.

In this chapter we have also studied the analogues of the usual number

theoretic Möbius Function and the Liouville's function. Some of the main results in this direction are:

Theorem 4.5.3. *The Möbius Function $\mu \in \mathcal{A}(\mathcal{G})$ is multiplicative.*

Theorem 4.5.6. $\mu * u = u * \mu = \varepsilon$ *i.e.,* $\mu^{-1} = u$ *and* $u^{-1} = \mu$.

Theorem 4.5.10. $\lambda * \mu^2 = \mu^2 * \lambda = \varepsilon$ *i.e.,* $\lambda^{-1} = \mu^2$ *where μ^2 is the ordinary product of μ with itself, and λ is the group theoretic Liouville's function.*

Theorem 4.5.12. *Let $f \in \mathcal{A}(\mathcal{G})$ be a mulptiplicative function such that $f = f \circ \rho$. Then*

f is completely multiplicative if and only if $f * (\mu f) = (\mu f) * f = \varepsilon$.

i.e., $f^{-1} = \mu f$ *where μf is the ordinary product of μ and f.*

As applications of the abelian version of Möbius Function we have:

Theorem 4.6.2. *Let $G_m = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, m-times. Then number of subgroups of G_m of order $p^n (n \leq m)$ is*

$$\frac{(p^m - 1)(p^{m-1} - 1) \ldots (p^{m-n+1} - 1)}{(p - 1)(p^2 - 1) \ldots (p^n - 1)}.$$

Theorem 4.6.3. *Let $G_m = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, m-times. Then*

$$\hat{\mu}(G_m) = (-1)^m p^{\frac{1}{2}m(m-1)}.$$

Theorem 4.6.4. *Let $G = \mathbb{Z}_p^{m_1} \times \mathbb{Z}_p^{m_2} \times \cdots \times \mathbb{Z}_p^{m_r}$, m-times, where atleast one $m_i \geq 2$, $i = 1, 2, \ldots, r$. Then*

$$\hat{\mu}(G) = 0.$$

Final part of this chapter is devoted to the study of divisor functions, structure of the normal subgroups of the product of two groups and characterization of groups using divisor functions. Some important results here are:

Theorem 4.8.1. *Let G_1 and G_2 be coprime groups. Then the normal subgroups of the product $G_1 \times G_2$ are exactly the subgroups of the form $N_1 \times N_2$, with $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

Theorem 4.8.2. *Let G_1 and G_2 be any two groups. Then the following conditions are equivalent:*

(i) *Every normal subgroup of the product $G_1 \times G_2$ is of the form $N_1 \times N_2$ with $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

(ii) *For each $H_1 \triangleleft G_1$ and for each $H_2 \triangleleft G_2$, the centres $Z(G_1/H_1)$ and $Z(G_2/H_2)$ of the quotient groups G_1/H_1 and G_2/H_2 have no subgroup in common.*

Theorem 4.9.6. (Abelian Quotient Theorem)

If G is a group with $\sigma(G) \leq 2|G|$ then any abelian quotient of G is cyclic.

Corollary 4.9.7.

(i) *If G is a perfect group then any abelian quotient of G is cyclic.*

(ii) *The perfect abelian groups are precisely the cyclic groups C_n of order n with n perfect.*

We conclude the dissertation by studying and computing some examples of non abelian perfect groups.

Contents

Chapter 1

Preliminaries

In this chapter we recall some of the basic definitions and results from the theory of groups, the theory of fields and the theory of numbers, which will serve as prerequisites for the forth coming chapters.

1.1 Group Action

Definition 1.1.1. Let G be a group and Ω be a set. Then G is said to *act* on Ω or Ω is said to be a *G-set* if $\forall\, g \in G$ and $\forall\, \alpha \in \Omega$ there exists an elemant $g \cdot \alpha \in \Omega$, determined uniquely by g and α, such that the following conditions hold:

(i) $1 \cdot \alpha = \alpha \;\; \forall\, \alpha \in \Omega$, 1 being the identity element of G,

(ii) $(gh) \cdot \alpha = g \cdot (h \cdot \alpha) \;\; \forall\, \alpha \in \Omega$ and $\forall\, g, h \in G$.

Definition 1.1.2. If Ω is a G-set then for each $\alpha \in \Omega$, the *orbit of* α, denoted

by $\text{orb}(\alpha)$, is defined to be the set

$$\{g \cdot \alpha \in \Omega | g \in G\}.$$

Definition 1.1.3. If Ω is a G-set then for each $\alpha \in \Omega$, the *stabilizer of* α, denoted by $\text{stab}(\alpha)$, is defined to be the subgroup $\{g \in G | g \cdot \alpha = \alpha\}$ of G.

The following result is well-known:

Theorem 1.1.4. *Let Ω be a G-set. Then, for each $x \in \Omega$, the number of elements in the orbit of α equals the index of stabilizer of α, i.e.,*

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

Definition 1.1.5. Let Ω be a G-set and $g \in G$. An element $\alpha \in \Omega$ is said to be g-fixed if $g \cdot \alpha = \alpha$. The set of all elements in Ω which are g-fixed is denoted by $\text{Fix}(g)$. Thus,

$$\text{Fix}(g) = \{\alpha \in \Omega | g \cdot \alpha = \alpha\}.$$

Theorem 1.1.6. (Burnside's theorem)([2], page 160)
Let a group G acts on a finite set Ω. If N is the number of orbits of Ω, then

$$N = \frac{1}{|G|}\sum_{g \in G}\pi(g), \tag{1.1.a}$$

Where

$$\pi(g) = |\,\text{Fix}(g)| = |\,\{\alpha \in \Omega : g \cdot \alpha = \alpha\}\,|\,.$$

The fixed-point counting function π is the *permutation character* associated with the action of G on Ω, and the above theorem says that number N of orbits is exactly the average value of the permutation character over the group G. (We have given the precise defination of *permutation character* in the character theory section of this chapter.)

1.2 Isomorphism Theorems

Theorem 1.2.1. (First isomorphism theorem) ([4], page 22)

Let $\phi : G \longrightarrow H$ be a homomorphism of groups. Then

$$\frac{G}{\operatorname{Ker}\phi} \cong \operatorname{Im}\phi.$$

Hence, in particular, if ϕ is surjective, then

$$\frac{G}{\operatorname{Ker}\phi} \cong H.$$

Theorem 1.2.2. (Second isomorphism theorem) ([4], page 25)

Let H and N be subgroups of G, and $N \lhd G$. Then

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

Theorem 1.2.3. (Third isomorphism theorem) ([4], page 26)

Let H and K be normal subgroups of G and $K \leq H$. Then

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

Theorem 1.2.4. (Correspondance Theorem) ([10], page 98)

Let $\phi : G_1 \longrightarrow G_2$ be a homomorphism of a group G_1 onto a group G_2. Then the following are true:

(i) $H_1 < G_1 \Longrightarrow \phi(H_1) < G_2$,

(ii) $H_2 < G_2 \Longrightarrow \phi^{-1}(H_2) < G_1$,

(iii) $H_1 \lhd G_1 \Longrightarrow \phi(H_1) \lhd G_2$,

(iv) $H_2 \lhd G_2 \Longrightarrow \phi^{-1}(H_2) \lhd G_1$,

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

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

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

Theorem 1.2.6. ([4], page 26)
Let $N \trianglelefteq G$. *Then their is a one to one correspondence between normal subgroups of* G *containing* N *and subgroups of* G/N.

1.3 Direct Products

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

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

Theorem 1.3.2. ([4], page 29)
Let G *be a group with normal subgroups* H *and* K; *if* $H \cap K = \{1\}$ *and* $HK = G$ *then* $G \cong H \times K$, *and in that case we say that* G *is the internal direct product of* H *and* K.

Theorem 1.3.3. *If G_1 and G_2 are groups then $G_1 \times \{e_2\}$ and $\{e_1\} \times G_2$ are normal subgroups of $G_1 \times G_2$ isomorphic to G_1 and G_2 respectively.*

Theorem 1.3.4. *If H and K are two subgroups of a group G such that $G = H \times K$, then H and K are normal subgroups G and $G/H \cong K$ and $G/K \cong H$.*

Theorem 1.3.5. (Cauchy's Theorem) ([2], page 167)
If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.

Theorem 1.3.6. Basis Theorem ([28], page 108)
Every finite abelian group is the internal direct product of its Sylow subgroups.

Theorem 1.3.7. Structure Theorem for Finite abelian group ([28], page 109)
Every finite abelian group is the direct product of cyclic groups.

1.4 Conjugacy Classes

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

Theorem 1.4.1. *The number of conjugates of x in G is $[G : C_G(x)]$. i.e.,*

$$|C\ell(x)| = |G : C_G(x)|.$$

1.5 Normal Series

Definition 1.5.1. A sequence $(G_0, G_1, \cdots, G_r)$ of subgroups of a group G is called a *normal series* of G if

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

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

Definition 1.5.2. A *composition series* of a group G is a normal series $(G_0, G_1, \cdots, G_r)$ without repetition whose factors G_i/G_{i-1} are all simple groups. The factors G_i/G_{i-1} are called composition factors of G.

Note 1.5.3. We often refer to a normal series $(G_0, G_1, \cdots, G_r)$ by saying that

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

is a normal series of G.

Lemma 1.5.4. ([11], page 241)
Every finite group has a composition series.

Theorem 1.5.5. (Jordan-Hölder Theorem) ([11], page 241)
Any two composition series of a finite group are equivalent in the sense that there is a one to one correspondence between their composition factors such that the corresponding factor groups are isomorphic.

Definition 1.5.6. A group G is called *completely reducible* if either G is trivial or G is a direct product of simple groups. Obviously, every simple group is completely reducible.

Definition 1.5.7. A group G is called *decomposible* if it is isomorphic to a direct product of two proper nontrivial subgroups. Otherwise G is called *indecomposible.*

Theorem 1.5.8. ([2], page 91)
Finite indecomposible abelian groups are precisely the cyclic groups having prime power order.

1.6 Character Theory

Definition 1.6.1. Let $\mathbb{F}$ be a field and A be an $\mathbb{F}$-vector space which is also a ring with with 1. Then A is said to be an $\mathbb{F}$-*algebra* if for $c \in \mathbb{F}$ and $x, y \in A$

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

Example 1.6.2. Let G be a finite group and $\mathbb{F}[G]$ be the set of all "formal" sums $\{\sum_{g \in G} a_g g \mid a_g \in \mathbb{F}\}$. Then $\mathbb{F}[G]$ has a $\mathbb{F}$-vector space structure in an obvious way. The elements of $\mathbb{F}[G]$ for which $a_g = 1$ and $a_h = 0$ if $h \neq g$ is identified with g. This identification embedds G into $\mathbb{F}[G]$ and in fact G is a basis for $\mathbb{F}[G]$. To define multiplication on $\mathbb{F}[G]$, we multiply the basis vectors according to their group multiplication and extend linearly to all of $\mathbb{F}[G]$. Then this defines the structure of an $\mathbb{F}$-algebra on $\mathbb{F}[G]$.

Definition 1.6.3. Let A and B be two $\mathbb{F}$-algebras. Then a mapping $\phi : A \longrightarrow B$ is said to be an *algebra homomorphism* or an $\mathbb{F}$-*homomorphism* if the following satisfies

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

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

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

Definition 1.6.4. Let $M_n(\mathbb{F})$ be the set of all $n \times n$ matrices over $\mathbb{F}$. Let

$$A = \begin{pmatrix} a_{11}\ a_{12} \ldots a_{1n} \\ a_{21}\ a_{22} \ldots a_{2n} \\ \ldots \\ a_{n1}\ a_{n2} \ldots a_{nn} \end{pmatrix}$$

be a matrix in $M_n(\mathbb{F})$. The *determinant* of A is denoted by $\det(A)$ and is defined to be the scalar

$$\det(A) = \sum_{\phi \in S_n} sgn(\phi) a_{1\phi(1)} a_{2\phi(2)} \ldots a_{n\phi(n)}.$$

The *trace* of A is denoted by $\mathrm{tr}(A)$ and is defined to be the scalar

$$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}.$$

Definition 1.6.5. Let A be an $\mathbb{F}$-algebra. A *representation* of A is an algebra homomorphism $\rho : A \longrightarrow M_n(\mathbb{F})$. The integer n is called the *degree* of ρ.

Definition 1.6.6. Two representation ρ and σ of same degree n is said to be *similar* if there exists a non singular $n \times n$ matrix P such that

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

Remark 1.6.7. 'Similarity' is an equivalence relation among representations of same degree.

Definition 1.6.8. Let G be a group and let $\mathbb{F}$ be a field. Then $\mathbb{F}$-representation of G is a homomorphism $\rho : G \longrightarrow \mathrm{GL}(n, \mathbb{F})$ for some positive integer n.

Remark 1.6.9. A representation $\bar{\rho}$ of $\mathbb{F}[G]$ determines an $\mathbb{F}$-representation ρ of G by restriction. Conversely, an $\mathbb{F}$-representation ρ of G determines a representation $\bar{\rho}$ of $\mathbb{F}[\mathbb{G}]$ by linear extension. i.e.,

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

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

Definition 1.6.10. Let A be an $\mathbb{F}$-algebra and let V be a finite dimensional vector space. Suppose for every $v \in V$ and $x \in A$ that a unique $vx \in V$ is defined. Then V is said to be an *A-module* if for all $x, y \in A$, $v, w \in V$, and $c \in \mathbb{F}$ the following satisfies

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

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

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

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

(v) $v1 = v$.

Definition 1.6.11. Let V be an A-module. Then an A-invariant subspace W of V is said to be a *submodule* of V.

Definition 1.6.12. A nonzero A-module V is said to be *irreducible* if its only submodules are 0 and V, otherwise it is called *reducible.*

Fact 1.6.13. Let $\rho : A \longrightarrow M_n(\mathbb{F})$ be a representation of the $\mathbb{F}$-algebra A. Let $V = M_{1\times n}(\mathbb{F})$. Clearly

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

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

Fact 1.6.14. Let M be an A-module. Let $\mathcal{B}$ is an $\mathbb{F}$ basis for M. For all $a \in A$ let $a_M : M \longrightarrow M$ be the map $x \longmapsto xa$, $\forall\ a \in A$. Set $\rho(a) =$ matrix of a_M with respect to the basis $\mathcal{B}$. Then ρ defines a representation of A.

Remark 1.6.15. There is a natural one to one correspondance (as mentioned in Fact 1.6.13 and Fact 1.6.14) between isomorphism classes of A-modules and similarity classes of representations of A.

Definition 1.6.16. A representation $\rho : A \longrightarrow M_n(\mathbb{F})$ is said to be *irreducible* if the corresponding A-module (as per Fact 1.6.13) is irreducible. Otherwise *reducible.*

Definition 1.6.17. Let ρ be an $\mathbb{F}$-representation of G. Then the $\mathbb{F}$-*character* χ of G afforded by ρ is the function given by $\chi(g) = \operatorname{tr}\rho(g)$.

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

Remark 1.6.18. Similar representations of a group G afford equal character and characters are constant on conjugacy classes of a group G.

Definition 1.6.19. Characters afforded by irreducible representations are called *irreducible characters.*

Lemma 1.6.20. ([12], page 16)
The number of similarity classes of irreducible representations of a group G is equal to the number of conjugacy classes of G.

Lemma 1.6.21. ([12], page 16)
Let G be a group and $\mathrm{Irr}(G)$ be the set of all irreducible characters of G. Then $|\mathrm{Irr}(G)|$ equals the number of conjugacy classes of G and

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

Lemma 1.6.22. *Let G be a finite abelian group. Then*

$$\mathrm{Irr}(G) = \mathrm{Hom}(G, \mathbb{C}^*) \cong G.$$

We denote $\mathrm{Hom}(G, \mathbb{C}^*)$ by $\widehat{G}$.

Theorem 1.6.23. (First Orthogonality Relation) ([12], page 20)
The following holds for every finite group G

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

Lemma 1.6.24. ([12], page 20)
Let ρ be a representation of a group G affording the character χ and let $g \in G$. Let $n = o(g)$, the order of g. Then

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

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

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

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

Theorem 1.6.25. (Second Orthogonality Relation) ([12], page 21)
Let G *be a group and* g, $h \in G$. *Then*

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

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

Definition 1.6.26. An *algebraic integer* is a complex number which is a root of a polynomial of the form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

where $a_i \in \mathbb{Z}$ for $0 \leq i \leq n-1$.

Theorem 1.6.27. ([12], page 35)
Sums and products of algebraic integers are algebraic integers.

Theorem 1.6.28. ([13], page 48)
Let G *be a finite group of order* n. *The values of the characters of* G *are algebraic integers in the cyclotomic field* $\mathbb{Q}(\zeta_n)$, *where* ζ_n *is a primitive* n^{th} *root of unity.*

Theorem 1.6.29. ([13], page 50)

Let G be a finite group of order n. The Galois group

$$\mathcal{G} \;=\; G(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \;\cong \mathbb{Z}_n{}^{\star},$$

where $\mathbb{Z}_n{}^{\star}$ is the group of units in the ring $\mathbb{Z}_n$ and ζ_n is a primitive n^{th} root of unity.

Theorem 1.6.30. ([13], page 50)

Let G be a finite group of order n and a is a rational integer prime to n. If $\sigma \in \mathcal{G}$, and $\sigma(\zeta_n) = \zeta_n{}^a$, then

$$\sigma(\chi(g)) \;=\; \chi(g^a)$$

for any character χ and any element g of G.

1.7 Permutation Character

Let G be a finite group acting on $\Omega = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. Consider the map (homomorphism)

$$f : G \longrightarrow GL(k, \mathbb{C}) \;\text{ given by }\; f(g) = [a_{ij}]_{k\times k}\,,$$

where, $a_{ij} = \begin{cases} 1, & \text{if } \; g \cdot \alpha_j = \alpha_i, \\ 0, & \text{otherwise.} \end{cases}$

Then

$$\pi(g) = \mathrm{tr}(f(g)) = |\,\mathrm{Fix}(g)| = |\,\{\alpha \in \Omega : g \cdot \alpha = \alpha\}\,|\,.$$

$\pi(g)$ is called the *permutation character* of the action of G on Ω.

1.8 Theory of numbers

1.9 Elementary Congruences

Definition 1.9.1. If an integer m, not zero, divides the difference $a - b$, we say that a *is congruent to* b *modulo* m and write $a \equiv b \pmod{m}$. If $a - b$ is not divisible by m , we say that a *is not congruent to* b *modulo* m, and in this case we write $a \not\equiv b \pmod{m}$.

Theorem 1.9.2. ([5], page 48)
Let a, b, c, d, x, y *denote integers. Then*

(i) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, $a - b \equiv 0 \pmod{m}$ *are equivalent statements.*

(ii) *If* $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$.

(iii) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $ax + cy \equiv bx + dy \pmod{m}$.

(iv) *If* $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $ac \equiv bd \pmod{m}$.

(v) *If* $a \equiv b \pmod{m}$ *and* $d|m$, $d \geq 0$, *then* $a \equiv b \pmod{d}$.

(vi) *If* $ax \equiv ay \pmod{m}$ *and* $gcd\,(a, m) = 1$, *then* $x \equiv y \pmod{m}$.

1.10 Legendre Symbol, Jacobi Symbol and Kronecker Symbol

Definition 1.10.1. Let p be an odd prime and $a \in \mathbb{N}$ such that $\gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv 0 \pmod{n}$ has a solution, then a is said to be a *quadratic residue mod p*, otherwise a is called a *quadratic non residue mod p*.

Definition 1.10.2. Let p be an odd prime, the *Legendre Symbol* $\left(\frac{\cdot}{p}\right)$ is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a, \\ 1, & \text{if } a \text{ is a q r mod } p, \\ -1, & \text{if } a \text{ is a q n r mod } p. \end{cases}$$

The Legender Symbol has the following properties:-

Theorem 1.10.3. ([5], page 132)
Let p be an odd prime. Then

(i) $a \equiv b \pmod{p}$ *implies that* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(ii) $\left(\frac{a^2}{p}\right) = 1$,

(iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

(iv) $\left(\frac{a_1 a_2 \cdots a_k}{p}\right) = \left(\frac{a_1}{p}\right) \cdots \left(\frac{a_k}{p}\right)$,

(v) $\left(\frac{1}{p}\right) = 1$,

(vi) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

(vii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Definition 1.10.4. Let n be an arbitrary odd positive integer and $n = p_1 p_2 \cdots p_k$ its factorization into primes (not necessarily distinct). Then the *Jacobi Symbol* is defined by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right)$$

where $\left(\frac{a}{p_i}\right)$, $i = 1, 2, \ldots, k$ is the Legendre Symbol.

Convention 1.10.5. $\left(\frac{a}{1}\right) = 1$.

Theorem 1.10.6. ([5], page 139)
If a and n are odd and positive and if $gcd\,(a, n) = 1$, then

$$\left(\frac{a}{n}\right) = (-1)^{\frac{n-1}{2}\frac{a-1}{2}} \left(\frac{n}{a}\right).$$

Definition 1.10.7. A *discriminant* is a non zero integer d such that $d \equiv 0 \pmod 4$ or $d \equiv 1 \pmod 4$.

Definition 1.10.8. For a discriminant d, the *Kronecker Symbol* $\left(\frac{d}{\cdot}\right)$ is defined as

$$\left(\frac{d}{2}\right) = \begin{cases} 0, & \text{if } d \text{ is even,} \\ 1, & \text{if } d \equiv 1 \pmod 8, \\ -1, & \text{if } d \equiv 5 \pmod 8. \end{cases}$$

Convention 1.10.9. $\left(\frac{d}{-1}\right) = sign\ of\ d.$

Convention 1.10.10. $\left(\frac{d}{0}\right) = \begin{cases} 0, & \text{if } d \neq 1, \\ 1, & \text{if } d = 1. \end{cases}$

The value of $\left(\frac{d}{a}\right)$ is then defined for all a by multiplicitavity.

1.11 Algebraic number field

Definition 1.11.1. A subfield K of $\mathbb{C}$ is called an *algebraic number field* if its dimension as a vector space over $\mathbb{Q}$ is finite. The dimension of K over $\mathbb{Q}$ is called the degree of K, and is denoted by $|K : \mathbb{Q}|$.

Definition 1.11.2. A prime p is said to split in the algebraic number field $\mathbb{Q}(\zeta_n)$ if the principal ideal generated by p in the ring of integers of $\mathbb{Q}(\zeta_n)$ factors into $|\mathbb{Q}(\zeta_n) : \mathbb{Q}|$ distinct prime ideals, where $|\mathbb{Q}(\zeta_n) : \mathbb{Q}|$ is the degree of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$.

Definition 1.11.3. Let $\mathbb{F}$ be a finite field of characteristic p. Then the map $\sigma_p : \mathbb{F} \longrightarrow \mathbb{F}$ defined by $\sigma_p(x) = x^p$ for $x \in \mathbb{F}$ is an automorphism, the *frobenius automorphism* of $\mathbb{F}$.

Theorem 1.11.4. ([9], page 91)
p splits in any subfield of $\mathbb{Q}(\zeta_n)$ if and only if σ_p fixes that subfield pointwise.

Corollary 1.11.5. ([9], page 91)
Let d be the discriminant of a finite group G. Then

$$p \text{ splits in } \mathbb{Q}(\sqrt{d}) \text{ if and only if } \sigma_p(\sqrt{d}) = \sqrt{d}.$$

Theorem 1.11.6. ([9], page 77)

Let d be the discriminant of a finite group G. Then

$$p \text{ splits in } \mathbb{Q}(\sqrt{d}) \text{ if and only if } \left(\frac{d}{p}\right) = 1.$$

1.12 Arithmetic Function

A complex valued function defined on the positive integers is called an *arithmetic function.*

Definition 1.12.1. For positive integers n we make the following definitions which are examples of arithmetic functions.

$\tau(n)$ is the number of positive divisors of n i.e., $\tau(n) = \sum_{d|n} 1$.

$\sigma(n)$ is the sum of positive divisors of n i.e., $\sigma(n) = \sum_{d|n} d$.

$\sigma_\alpha(n)$ is the sum of the α^{th} powers of the positive divisors of n i.e., $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$.

Definition 1.12.2. The arithmetical function I given by

$$I(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1 \end{cases}$$

is called the *identity funtion.*

Definition 1.12.3. The arithmetical function u defined by $u(n) = 1$ for all n is called the *unit function.*

Definition 1.12.4. If $n \geq 1$ the *Euler totient* $\varphi(n)$ is defined to be the number of positive integers not exceeding n which are relatively prime to n; thus,

$$\varphi(n) = \sum_{k=1}^{n}{}' 1,$$

where the $'$ indicates that the sum is extended over those k relatively prime to n.

Definition 1.12.5. The *Möbius function* μ is given by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } p^2 \mid n \text{ for some prime p}, \\ (-1)^r, & \text{if } n = p_1 p_2 \dots p_r,\ p_i \text{ distinct primes.} \end{cases}$$

Definition 1.12.6. If f and g are two arithmetical functions then we define their *Dirichlet product (or Dirichlet convolution)* to be the arithmetical function $f * g$ defined by the equation

$$(f * g)(n) = \sum_{d|n} f(d) g(\frac{n}{d}).$$

Theorem 1.12.7. ([21], page 29)

Dirichlet product is commutative and associative. That is, for any arithmetical functions f, g, h we have

$f * g = g * f$ *(commutative law)*

$(f * g) * h = f * (g * h)$ *(associative law).*

Theorem 1.12.8. ([21], page 30)

For all f we have $I * f = f * I = f$.

Theorem 1.12.9. ([21], page 30)
If f is an arithmetical function with $f(1) \neq 0$ then there is a unique arithmetical function g such that

$$f * g = g * f = I.$$

The function g is called the Dirichlet inverse of f and it is denoted by f^{-1}.

Remark 1.12.10. The set of all arithmetical functions f with $f(1) \neq 0$ forms an abelian group under *Dirichlet multiplication.*

Theorem 1.12.11. ([21], page 31)
The functions μ and u are multiplicative inverses, thus $\mu * u = u * \mu = I$, $\mu = u^{-1}$ and $u = \mu^{-1}$.

Definition 1.12.12. An arithmetical function f is called *multiplicative* if f is not identically zero and if

$$f(mn) = f(m)f(n) \text{ whenever } gcd\,(m,n) = 1.$$

Theorem 1.12.13. ([21], page 34)
The Möbius function μ is multiplicative.

Theorem 1.12.14. ([21], page 38)
The function σ is multiplicative.

Definition 1.12.15. An arithmetical function f is called *completely multiplicative* if f is not identically zero and if

$$f(mn) = f(m)f(n) \text{ for all } m, n.$$

Remark 1.12.16. u and I are completely multiplicative functions.

Theorem 1.12.17. ([21], page 34)
If f is multiplicative then $f(1) = 1$.

Theorem 1.12.18. ([21], page 35)
If f and g are multiplicative then $f * g$ is also multiplicative.

Remark 1.12.19. If f and g are completely multiplicative then $f * g$ need not be completely multiplicative.

Theorem 1.12.20. ([21], page 35)
If both g and $f * g$ are multiplicative, then f is also multiplicative.

Theorem 1.12.21. ([21], page 36)
If f is multiplicative, so is f^{-1}, its Dirichlet inverse.

Remark 1.12.22. The set of multiplicative functions is a subgroup of the group of all arithmetical functions f with $f(1) \neq 0$.

An important example of a completely multiplicative function of positive integers is the Liouville's function given by

$$\lambda(n) = (-1)^{\Omega(n)}$$

where n is a positive integer and $\Omega(n)$ is the number of prime factors (counting multiplicity) of n.

1.13 Perfect number

Definition 1.13.1. A positive integer n is said to be a *perfect number* if n is the sum of all its positive divisors other than itself, i.e., if $\sigma(n) = 2n$.

Euclid proved that a number of the form $2^{n-1}(2^n - 1)$ is a perfect number if the factor $(2^n - 1)$ is prime. Leonhard Euler classified the even perfect numbers, but it is a long standing question as to wheather there is any odd perfect number at all. In 1757, Leonhard Euler classified the even perfect numbers as follows:

Theorem 1.13.2. *The even perfect numbers are precisely those numbers* $2^{r-1}(2^r - 1)$ *where* $r \geq 2$ *and* $2^r - 1$ *is prime.*

Proof. Suppose $r \geq 2$ and $2^r - 1$ is prime. Then using Theorem 1.12.14

$$\begin{aligned}
\sigma(2^{r-1}(2^r - 1)) &= \sigma(2^{r-1})\sigma(2^r - 1), \text{ since gcd } (2^{r-1}, 2^r - 1) = 1 \\
&= (1 + 2 + 2^2 + \cdots + 2^{r-1})(1 + (2^r - 1)) \\
&= 2^r(2^r - 1) \\
&= 2(2^{r-1}(2^r - 1))
\end{aligned}$$

Therefore $2^{r-1}(2^r - 1)$ is an even perfect number.

Conversly suppose n is an even perfect number. Write $n = 2^s m$ where $s \geq 1$

and m is odd. Then n being perfect says that

$$\begin{aligned}
& \sigma(2^s m) = 2 \times 2^s m \\
\Longrightarrow\ & \sigma(2^s)\sigma(m) = 2^{s+1} m \\
\Longrightarrow\ & (1 + 2 + 2^2 + \cdots + 2^s)\sigma(m) = 2^{s+1} m \\
\Longrightarrow\ & (2^{s+1} - 1)\sigma(m) = 2^{s+1} m \\
\Longrightarrow\ & (2^{s+1} - 1)(\sigma(m) - m) = m.
\end{aligned}$$

Hence $\sigma(m) - m$ is a proper divisor of m since $2^{s+1} - 1 \geq 1$. But $\sigma(m) - m$ is the sum of the proper divisors of m, so $\sigma(m) - m$ is the unique proper divisor of m. Thus m is prime and $\sigma(m) - m = 1$. Therefore $2^{s+1} - 1 = m$. Now $n = 2^s m = 2^s(2^{s+1} - 1) = 2^{s+1-1}(2^{s+1} - 1)$ with $s + 1 \geq 2$ and $2^{s+1} - 1$ prime. □

Chapter 2

Fermat's Little Theorem via finite groups

2.1 Introduction

In October, 1640, a French Mathematician called "Pierre de Fermat" communicated the following theorem to his friend "Frenicle de Bessy".

If p is a prime and a is any integer not divisible by p, then p divides $a^{p-1} - 1$. i.e.,

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2.1.a}$$

This theorem has since been called as " Fermat's Little Theorem (F.L.T.)" or simply " Fermat's Theorem". Almost 100 years later, in 1736 Leonhard Euler gave the first proof of the little theorem. Thereafter many Mathematicians have given sevaral proofs of this theorem. The shortest among these

proofs is perhaps the following :

Suppose $\mathbb{Z}_p{}^\star$ is the set of all non zero residue classes of integers modulo p . Then $\mathbb{Z}_p{}^\star$ is a group of order $p-1$, whose identity element is $\overline{1}$. Since $p \nmid a$, $\overline{a} \neq \overline{0}$ and so $\overline{a} \in \mathbb{Z}_p{}^\star$. Hence we have

$$\begin{aligned} & \overline{a}^{p-1} = \overline{1} \\ \Longrightarrow \quad & \overline{a^{p-1}} = \overline{1} \\ \Longrightarrow \quad & p|(a^{p-1}-1). \end{aligned}$$

One may ask what happens to (2.1.a) when p is not a prime. The answer to this question lies in the following result which is essentially due to C.F.Gauss :

Let a be an arbitrary integer. Then for every positive integer n,

$$\sum_{d|n} \mu(d) a^{n/d} \equiv 0 \pmod{n}, \tag{2.1.b}$$

where μ is the usual number theoretic Möbius function.

(This also generalizes Euler's Theorem i.e., if $\gcd(a,m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$, $m \geq 1$.) The case when a is a prime was settled by Gauss and his result was published posthumously in 1863. However the general case was settled during the years 1880 to 1883 when four independent proofs was given by Kantor, Weyr, Lucas, and Pellet. Recently 1986, C.J.Smith [1] gave a coloring proof of a more general result.

In this chapter we shall discuss a group theoretic generalization of the Gauss's result (2.1.b), namely,

Let G be a finite group of order n and $f : G \longrightarrow \mathbb{C}^*$, where $\mathbb{C}^*$ is the multiplicative group of non zero complex numbers be a group homomorphism. Then

$$\sum_{g \in G} f(g) a^{n/o(g)} \in \mathbb{Z}$$

and

$$\sum_{g \in G} f(g) a^{n/o(g)} \equiv 0 \pmod{n}, \tag{2.1.c}$$

for any integer a.

This is the Main Theorem of this chapter.

2.2 Induced action

In this section we study some results related to orbit counting. Moreover, given a group element g we define a number $c(g)$ and study some important properties of $c(g)$ which will serve as prerequisites for our Main Theorem.

Let G be a finite group acting on a finite set Ω by left multiplication. Let M be the set of all functions from Ω into some arbitrary finite set A. We can view M as the set of all possible colorings of the points of Ω with colors chosen from the set A. Clearly $|M| = a^{|\Omega|}$, where $a = |A|$. We now define (induced) action of G on M.

Let $f \in M$ and $g \in G$. Define $g \star f : \Omega \longrightarrow A$ given by

$$(g \star f)(\alpha) = f(g^{-1} \cdot \alpha) \text{ for all } \alpha \in \Omega.$$

Clearly $g \star f \in M$, and

(1) $(1 \star f)(\alpha) = f(1 \cdot \alpha) = f(\alpha)$, 1 is the identity of G.

Therefore $1 \star f = f$

(2) $((gh) \star f)(\alpha) = f((gh)^{-1} \cdot \alpha) = f(h^{-1}g^{-1} \cdot \alpha) = f(h^{-1} \cdot (g^{-1} \cdot \alpha)) = (h \star f)(g^{-1} \cdot \alpha) = (g \star (h \star f))(\alpha)$.

Therefore

$$(gh) \star f = g \star (h \star f).$$

Thus, $g \star f$ defines an action of G on M.

Let π be the permutation character associated with the (induced) action of G on M. Then

$$\pi(g) = \mid \{f \in M : g \star f = f\} \mid,\ g \in G. \tag{2.2.a}$$

Lemma 2.2.1. *Let $f \in M$ and $g \in G$. Then*

$$g \star f = f \ \textit{if and only if}\ f(\alpha) = f(g \cdot \alpha),\ \forall\, \alpha\ \in \Omega.$$

Proof. Suppose

$$f(\alpha) = f(g \cdot \alpha),\ \forall\, \alpha\ \in \Omega.$$

We have $g^{-1} \cdot \alpha \in \Omega$.

Now

$$f(g^{-1} \cdot \alpha) = f(g \cdot (g^{-1} \cdot \alpha)) = f((gg^{-1}) \cdot \alpha) = f(1 \cdot \alpha) = f(\alpha)$$

$$\Longrightarrow (g \star f)(\alpha) = f(\alpha) \Longrightarrow g \star f = f.\ \text{i.e., } f \text{ is } g\text{-fixed} \quad (\text{see } 1.1.5).$$

Conversely, suppose

$$g \star f = f.$$

Now, for each $\alpha \in \Omega$, we have

$$f(\alpha) = f((g^{-1}g) \cdot \alpha) = f(g^{-1} \cdot (g \cdot \alpha))$$

$$= (g \star f)(g \cdot \alpha) = f(g \cdot \alpha).$$

□

As an immediate consequence we have the following

Corollary 2.2.2. *f is g-fixed if and only if f is constant on each of the orbits of $< g >$ on Ω.*

Given $g \in G$, let $c(g)$ denote the number of orbits of the cyclic group $< g >$ acting on Ω. Then

$$\begin{aligned}\pi(g) &= \mid \{f \in M : g \star f = f\} \mid . \\ &= \mid \{f \in M : f \text{ is constant on each of the orbits of } < g > \text{ on } \Omega\} \mid . \\ &= a^{c(g)}, \text{ where } a = |A|.\end{aligned}$$

Lemma 2.2.3. *$c(g)$ is the total number of cycles, including trivial "1- cycles", when the permutation of Ω induced by g is written in cyclic notation.*

Proof. Suppose the orbits of $< g >$ on Ω are

$$< g > \alpha_1, < g > \alpha_2, \cdots, < g > \alpha_{c(g)}.$$

Therefore

$$\Omega = \bigsqcup_{i=1}^{c(g)} < g > \alpha_i.$$

Let

$\Omega = \{\alpha_1, g\cdot\alpha_1, g^2\cdot\alpha_1, \cdots, g^{k-1}\cdot\alpha_1, \alpha_2, g\cdot\alpha_2, g^2\cdot\alpha_2, \cdots, g^{k-1}\cdot\alpha_2, \cdots, \alpha_{c(g)}, g\cdot\alpha_{c(g)}, \cdots, g^{k-1}\cdot\alpha_{c(g)}$. Then

$g\cdot\Omega = \{g\cdot\alpha_1, g^2\cdot\alpha_1, \cdots, \alpha_1, g\cdot\alpha_2, g^2\cdot\alpha_2, \cdots, \alpha_2, \cdots, g\cdot\alpha_{c(g)}, g^2\cdot\alpha_{c(g)}, \cdots, \alpha_{c(g)}\}$.

Therefore

$\phi_g = (\alpha_1, g\cdot\alpha_1, g^2\cdot\alpha_1, \cdots, g^{k-1}\cdot\alpha_1)(\alpha_2, g\cdot\alpha_2, g^2\cdot\alpha_2, \cdots, g^{k-1}\cdot\alpha_2)\cdots(\alpha_{c(g)}, g\cdot\alpha_{c(g)}, \cdots, g^{k-1}\cdot\alpha_{c(g)})$

Hence number of cycle is $c(g)$. □

Remark 2.2.4. If $G = S_6$ and $\Omega = \{1,2,3,4,5,6\}$ is the set on which G acts naturally, then for $g = (13)(246) \in G$, we have $c(g) = 3$.

Lemma 2.2.5. *Let G be a finite group of order n acting on itself by left multiplication. Let $g \in G$ such that $o(g) = m$. Then*

$$c(g) = \frac{n}{m},$$

where $c(g)$ is the number of orbits of $\langle g \rangle$ on G.

Proof. Let $H = \langle g \rangle$. Consider the action of H on G given by left multiplication. Let $x \in G$. Then

$$\text{stab}(x) = \{h \in H : h \cdot x = x\} = \{h \in H : h = 1\} = \{1\}.$$

Now

$$|\,\text{orb}(x)| = |H : \text{stab}(x)| = |H : \{1\}| = |H|.$$

Again $G = \bigsqcup_{i=1}^{c(g)} \mathcal{O}_i$, where $\mathcal{O}_i$ is an orbit of G under the action of H such that $|\mathcal{O}_i| = |H|$, for each i.

Hence

$$|G| = c(g)|H|,$$

i.e.,

$$c(g) = \frac{|G|}{|H|} = \frac{n}{m}.$$

□

As an immediate consequence we have the following

Lemma 2.2.6. *Let G be a finite group of order n acting on itself by left multiplication. Let $g \in G$ such that $o(g) = m$. Then*

$$\chi(g) = a^{n/o(g)},$$

where χ is the permutation character associated with the (induced) action of G on M.

Lemma 2.2.7. *Let G act on Ω by left multiplication and $\mathcal{O}$ be a G-orbit of Ω. If $\alpha, \beta \in \mathcal{O}$, then* $\mathrm{stab}(\alpha) \sim \mathrm{stab}(\beta)$. *That is* $\mathrm{stab}(\beta) = g\,\mathrm{stab}(\alpha)g^{-1}$ *for some $g \in G$.*

Proof. Since $\alpha, \beta \in \mathcal{O}$ therefore $\beta = g \cdot \alpha$ for some $g \in G$. Let $g' \in \mathrm{stab}(\alpha)$. Then $g' \cdot \alpha = \alpha$. Now

$$gg'g^{-1} \in g\,\mathrm{stab}(\alpha)g^{-1}. \text{ We show that } gg'g^{-1} \in \mathrm{stab}(\beta).$$

We have

$$\beta = g \cdot \alpha \Longrightarrow g^{-1} \cdot \beta = \alpha$$

Now

$$(gg'g^{-1}) \cdot \beta = (gg') \cdot (g^{-1} \cdot \beta) = (gg') \cdot \alpha = g \cdot (g' \cdot \alpha) = g \cdot \alpha = \beta$$

Therefore

$$gg'g^{-1} \in \mathrm{stab}(\beta) \quad \text{i.e.,} \quad g\,\mathrm{stab}(\alpha)g^{-1} \subseteq \mathrm{stab}(\beta).$$

Again let $h' \in \text{stab}(\beta)$. Then

$$\begin{aligned} & h' \cdot \beta = \beta \\ \Longrightarrow \quad & h' \cdot (g \cdot \alpha) = g \cdot \alpha \\ \Longrightarrow \quad & (h'g) \cdot \alpha = g \cdot \alpha \\ \Longrightarrow \quad & (g^{-1}h'g) \cdot \alpha = \alpha \\ \Longrightarrow \quad & g^{-1}h'g \in \text{stab}(\alpha) \\ \Longrightarrow \quad & h' \in g\,\text{stab}(\alpha)g^{-1} \end{aligned}$$

Therefore

$$\text{stab}(\beta) \subseteq g\,\text{stab}(\alpha)g^{-1}.$$

Hence

$$\text{stab}(\beta) = g\,\text{stab}(\alpha)g^{-1}. \quad \textit{i.e.,} \quad \text{stab}(\alpha) \sim \text{stab}(\beta).$$

□

2.3 Complex polynomial

Definition 2.3.1. For nonnegative integers m, we define

$$\binom{x}{m} = \frac{x(x-1)(x-2)\cdots(x-m+1)}{m!},$$

which is a polynomial of degree m with rational coefficients. For $m = 0$, this is just the constant polynomial 1.

Lemma 2.3.2. *The set*

$$\beta = \left\{ \binom{x}{m} : m \in \mathbb{Z}, m \geq 0 \right\}$$

is a basis for $\mathbb{C}[\mathbb{X}]$.

Proof. We know that $\beta' = \{1, x, x^2, \dots\}$ is a basis for $\mathbb{C}[\mathbb{X}]$. Therefore it is enough to show that β generates β'. We have

$$\begin{aligned}
1 &= \binom{x}{0}, \\
x &= \binom{x}{1}, \\
x^2 &= 2\binom{x}{2} + \binom{x}{1}, \\
x^3 &= 6\binom{x}{3} + 6\binom{x}{2} + \binom{x}{1},
\end{aligned}$$

and so on. Assume that

$$x^{n-1} = c_1\binom{x}{1} + c_2\binom{x}{2} + \cdots + c_{n-1}\binom{x}{n-1}, \quad c_i \in \mathbb{C}.$$

Now

$$\begin{aligned}
\binom{x}{n} &= \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!} \\
\text{or } n!\binom{x}{n} &= x^n + d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + \cdots + d_1x^1, \quad d_i \in \mathbb{C}.
\end{aligned}$$

Hence

$$x^n = n!\binom{x}{n} - d_{n-1}\sum_{i=1}^{n-1} c_{1_i}\binom{x}{i} - d_{n-2}\sum_{i=1}^{n-2} c_{2_i}\binom{x}{i} - \cdots - d_1\binom{x}{i}.$$

Therefore it follows, using induction, that β generates β'. That is β is a basis for $\mathbb{C}[\mathbb{X}]$. □

Lemma 2.3.3. *Let $f(x) \in \mathbb{C}[\mathbb{X}]$ and $f(x) \in \mathbb{Z}$ for all non negative integers x. Then $f(x) \in \mathbb{Z}$ for all integers x.*

Proof. Let $deg f = d$. Then by Lemma 2.3.2,

$$f(x) = \sum_{n=0}^{d} c_n \binom{x}{n}.$$

Since $n!$ divides the product of any n consecutive integers, we have $\binom{x}{n} \in \mathbb{Z}$ $\forall\ x \in \mathbb{Z}$. So it is enough to show that $c_k \in \mathbb{Z}\ \forall\ k = 1, 2, 3, \cdots, d$. By hypothesis

$$f(l) = \sum_{n=0}^{d} c_n \binom{l}{n} \in \mathbb{Z},\ \forall\ l \in \mathbb{Z} \text{ with } l \geq 0.$$

We have $\binom{l}{n} = 0$ if $n > l$ and $\binom{l}{0} = \binom{l}{1} = 1$, therefore

$$c_0 = f(0) \in \mathbb{Z},$$

$$c_0 + c_1 = f(1) \in \mathbb{Z} \Longrightarrow c_1 \in \mathbb{Z},$$

$$c_0 + 2c_1 + c_2 = f(2) \Longrightarrow c_2 = f(2) - c_0 - 2c_1 \in \mathbb{Z}$$

and so on. Since

$$c_k = f(k) - \sum_{i=0}^{k-1} c_i \binom{k}{i} \in \mathbb{Z},$$

it follows, using induction, that $c_k \in \mathbb{Z}\ \forall\ k = 1, 2, 3, \cdots, d$. This completes the proof. □

2.4 λ-good orbit

In this section we shall define λ-good orbit and establish few important results related to permutation character associated to the action of G. We begin with the following definition:

Definition 2.4.1. Let G act on Ω by left multiplication. Let $\lambda : G \longrightarrow \mathbb{C}^*$ be a homomorphism. If $\mathcal{O}$ is a G-orbit on Ω, we say that $\mathcal{O}$ is λ-*good* if the stabilizer in G of every point in $\mathcal{O}$ is contained in Ker λ.

By the above lemma we see that the stabilizers in G of various poins in $\mathcal{O}$ are congugate in G and so if any one of them is contained in the normal subgroup Ker λ, then $\mathcal{O}$ will be λ-good.

If λ is the trivial homomorphism which maps every element of G to the complex number 1, then every G-orbit is λ-good.

Lemma 2.4.2. *Let $\lambda : G \longrightarrow \mathbb{C}^*$ be a non trivial homomorphism, where G is a finite group. Then*

$$\sum_{g \in G} \lambda(g) = 0.$$

Proof. Let $h \in G$ such that $\lambda(h) \neq 0$.

Now

$$\lambda(h) \sum_{g \in G} \lambda(g) = \sum_{g \in G} \lambda(h)\lambda(g) = \sum_{g \in G} \lambda(gh) = \sum_{g \in G} \lambda(g).$$

Therefore

$$\sum_{g \in G} \lambda(g) = 0, \text{ since} \lambda(h) \neq 0.$$

□

Note that in the above lemma, λ can be replaced by an arbitrary multiplicative function.

Lemma 2.4.3. *The permutation character π associated to the action of G on Ω is the sum of the permutation characters associated to the action of G on the orbits of G on Ω.*

Proof. Let $\theta_1, \theta_2, \cdots, \theta_n$ be the orbits of G on Ω. Then

$$\Omega = \theta_1 \sqcup \theta_2 \sqcup \cdots \sqcup \theta_n.$$

Let σ_{θ_i} be the permutation character associated with the action of G on θ_i. Now

$$\begin{aligned} & \sigma_{\theta_i}(g) = \mid \{\alpha \in \theta_i : g \cdot \alpha = \alpha\} \mid \\ \Longrightarrow \quad & \sum_{i=1}^{n} \sigma_{\theta_i}(g) = \sum_{i=1}^{n} \mid \{\alpha \in \theta_i : g \cdot \alpha = \alpha\} \mid \\ \Longrightarrow \quad & \sum_{i=1}^{n} \sigma_{\theta_i}(g) = \mid \{\alpha \in \Omega : g \cdot \alpha = \alpha\} \mid = \pi(g). \end{aligned}$$

□

Lemma 2.4.4. *Let θ be an orbit of G on Ω and let σ_θ be the permutation character associated with the action of G on θ. Then*

$$\sum_{g \in G} \lambda(g)\sigma_\theta(g) = \mid G \mid \delta_\theta, \quad \textit{where } \delta_\theta = \begin{cases} 1, & \textit{if } \theta \textit{ is } \lambda\textit{-good,} \\ 0, & \textit{otherwise.} \end{cases}$$

Proof.

$$\begin{aligned} S &= \sum_{g \in G} \lambda(g)\sigma_\theta(g) \\ &= \sum_{g \in G} \lambda(g) \mid \{\beta \in \theta : g \cdot \beta = \beta\} \mid \\ &= \sum_{g \in G} \lambda(g) \mid \mathrm{Fix}_\theta(g) \mid \\ &= \sum_{g \in G} \lambda(g) \sum_{\beta \in \mathrm{Fix}_\theta(g)} 1 \end{aligned}$$

$$= \sum_{g \in G} \sum_{\beta \in \mathrm{Fix}_\theta(g)} \lambda(g)$$

$$= \sum_{g \in G} \sum_{\beta \in \theta} \delta_{\beta,g} \lambda(g), \text{ where, } \delta_{\beta,g} = \begin{cases} 1, & \text{if } g \cdot \beta = \beta \\ 0, & \text{otherwise} \end{cases}$$

$$= \sum_{\beta \in \theta} \sum_{g \in G} \delta_{\beta,g} \lambda(g)$$

$$= \sum_{\beta \in \theta} \sum_{g \in \mathrm{stab}(\beta)} \lambda(g).$$

Now $\lambda \mid_{\mathrm{stab}(\beta)}$ is a homomorphism from $\mathrm{stab}(\beta)$ to $\mathbb{C}^*$. If $\mathrm{stab}(\beta) \subseteq \mathrm{Ker}\,\lambda$, then by Lemma 2.2.7 $\lambda \mid_{\mathrm{stab}(\beta)}$ is trivial for all β. In this case θ is λ-good and

$$S = \mid \theta \mid\mid \mathrm{stab}(\beta) \mid = \mid G \mid .$$

If $\mathrm{stab}(\beta) \nsubseteq \mathrm{Ker}\,\lambda$, then $\lambda \mid_{\mathrm{stab}(\beta)}$ is non trivial.
Therefore by Lemma 2.4.2

$$\sum_{g \in \mathrm{stab}(\beta)} \lambda(g) = 0 \text{ and so } S = 0.$$

□

Lemma 2.4.5. *Let $\lambda : G \longrightarrow \mathbb{C}^*$ be a homomorphism where G is a finite group. Suppose G acts on some finite set Ω by left multiplication and let X be the number of λ-good orbits for this action. Then*

$$X = \frac{1}{|G|} \sum_{g \in G} \lambda(g) \pi(g),$$

where π is the permutation character associated with this action.

Proof. We have by Lemma 2.4.4,

$$\sum_{g\in G}\lambda(g)\sigma_\theta(g) =\mid G \mid \delta_\theta, \text{ where } \delta_\theta = \begin{cases} 1, & \text{if } \theta \text{ is } \lambda\text{-good} \\ 0, & \text{otherwise} \end{cases}$$

$$\Longrightarrow \sum_{\theta}\sum_{g\in G}\lambda(g)\sigma_\theta(g) = \sum_{\theta} \mid G \mid \delta_\theta$$

$$\Longrightarrow \sum_{g\in G}\lambda(g)\sum_{\theta}\sigma_\theta(g) =\mid G \mid X$$

$$\Longrightarrow \sum_{g\in G}\lambda(g)\pi(g) =\mid G \mid X, \text{ by Lemma 2.4.3.}$$

$$\Longrightarrow X = \frac{1}{\mid G \mid}\sum_{g\in G}\lambda(g)\pi(g).$$

□

2.5 The Main Theorem

We are now in a position to prove our Main Theorem. In this section we shall give two different proofs of the Main Theorem. Further we shall also include some results related to primitive n^{th} roots of unity and with the help of these results we shall show that our Main Theorem is actually a ganaralization of Fermat's Little Theorem/ Gauss' Theorem.

Let G acts on some finite set Ω by left multiplication. As before let M be the set of all mappings from Ω into some finite set A with $|A| = a$. Consider the induced action of G on M. We saw that the associated permutation character π is given by the formula $\pi(g) = a^{c(g)}$.

If we apply Lemma 2.4.5 in this situation we get the following

Theorem 2.5.1. *Let G be a finite group acting on a finite set Ω by left multiplication and let $f : G \longrightarrow \mathbb{C}^*$ be a homomorphism. Then for each integer a,*

$$\sum_{g\in G} f(g)a^{c(g)} \in \mathbb{Z}$$

and

$$\sum_{g\in G} f(g)a^{c(g)} \equiv 0 \pmod{n},$$

where $c(g)$ is the number of orbits of $< g >$ on Ω.

Proof. From the above Lemma, considering the induced action of G on Ω, we have

$$\frac{1}{|G|}\sum_{g\in G} f(g)\pi(g) \in \mathbb{Z}$$

$$\Longrightarrow \quad \frac{1}{|G|}\sum_{g\in G} f(g)a^{c(g)} \in \mathbb{Z}, \qquad \text{for each positive integer } a.$$

$$\Longrightarrow \quad \frac{1}{n}\sum_{g\in G} f(g)a^{c(g)} \in \mathbb{Z}, \qquad \text{for any integer } a, \text{ by Lemma 2.3.3.}$$

$$\Longrightarrow \quad \sum_{g\in G} f(g)a^{c(g)} \in \mathbb{Z}, \qquad \text{for any integer } a.$$

and

$$\sum_{g\in G} f(g)a^{c(g)} \equiv 0 \pmod{n}, \qquad \text{for any integer } a.$$

□

In particular if G acts on itself by left multiplication, we saw in Lemma 2.2.6 that the associative permutation character $\chi(g) = a^{n/o(g)}$. In this case we get the Main Theorem directly. But still we give a different proof of the Main Theorem.

Theorem 2.5.2. (The Main Theorem)

Let G be a finite group of order n and $f : G \longrightarrow \mathbb{C}^*$ be a group homomorphism. Then

$$\sum_{g\in G} f(g)a^{n/o(g)} \in \mathbb{Z}$$

and

$$\sum_{g\in G} f(g)a^{n/o(g)} \equiv 0 \pmod{n}, \tag{2.5.a}$$

for any integer a.

Proof. The permutation character χ is actually a character of G and f is also a character of G. We have

$[f, \chi] \in \mathbb{Z}$ [12], page 21

$\Longrightarrow \frac{1}{n}\sum_{g\in G} f(g)\chi(g) \in \mathbb{Z}$

$\Longrightarrow \frac{1}{n}\sum_{g\in G} f(g)a^{n/o(g)} \in \mathbb{Z}$, for all nonnegative integer a, by Lemma 2.2.6.

$\Longrightarrow \frac{1}{n}\sum_{g\in G} f(g)a^{n/o(g)} \in \mathbb{Z}$, for all integer a, by Lemma 2.3.3.

$\Longrightarrow \sum_{g\in G} f(g)a^{n/o(g)} \in \mathbb{Z}$, for all integer a.

and

$$\sum_{g\in G} f(g)a^{n/o(g)} \equiv 0 \pmod{n}, \quad \text{for all integer } a.$$

□

Pournaki [3] has also gave a Linear algebraic approach to prove the above Theorem.

Lemma 2.5.3. *Any n^{th} root of unity is a primitive d^{th} root of unity for some $d|n$, also such a d is uniquely determined by n. In other words $G = \bigsqcup_{d|n} G_d$, where G is the set of all n^{th} roots of unity and G_d is the set of all primitive d^{th} roots of unity.*

Proof. Note that G is a cyclic group of order n. Let $y \in G$. Then $o(y) = d$ for some $d|n$. That is $y^d = 1$ but $y^k \neq 1$ if $k < d$. That is y is a primitive d^{th} root of unity.
Uniqueness is clear, because order of any element of a group is unique. □

Lemma 2.5.4. *Let $G(n)$ be the sum of all n^{th} roots of unity. Then*

$$G(n) = 0, \quad if\ n > 1$$

Proof. Let x be a primitive n^{th} root of unity. Then

$$\begin{aligned} & x^n = 1 \\ \implies & (x^n - 1) = 0 \\ \implies & (x-1)(x^{n-1} + x^{n-2} + \cdots + 1) = 0 \\ \implies & (x^{n-1} + x^{n-2} + \cdots + 1) = 0, \text{ since } x \neq 1 \\ \implies & G(n) = 0. \end{aligned}$$

Since if x is a primitive n^{th} root of unity, then $1, x, x^2, \cdots x^{n-1}$ are the n^{th} roots of unity. □

Lemma 2.5.5. *Let n be a positive integer. Then the sum of all the primitive n^{th} roots of unity in $\mathbb{C}$ is $\mu(n)$, where μ is the usual number theoretic Möbius function.*

Proof. Let G be the set of all n^{th} roots of unity and G_d be the set of all primitive d^{th} roots of unity. Let

$F(n)$ = sum of all the primitive n^{th} roots of unity.

$G(n)$ = sum of all the n^{th} roots of unity.

Then, by Lemma 2.5.3, we have

$$\begin{aligned} G(n) &= \sum_{x \in G} x \\ &= \sum_{d|n} \sum_{x \in G_d} x = \sum_{d|n} F(d). \end{aligned}$$

By Möbius inverson formula

$$F(n) = \sum_{d|n} \mu(d) G(\frac{n}{d}).$$

Therefore, by Lemma 2.5.4, we have

$$F(n) = \mu(n).$$

□

The following theorem shows that Theorem 2.5.2 is indeed a generalization of congruence (2.1.b).

Theorem 2.5.6. *Let a be an arbitrary integer. Then for every positive integer n,*

$$\sum_{d|n} \mu(d) a^{n/d} \equiv 0 \pmod{n}$$

where μ is the usual number theoretic Möbius function.

Proof. Let G be the (cyclic) group of order n consisting of all the n^{th} roots of unity in $\mathbb{C}$, and let $f : G \hookrightarrow \mathbb{C}^*$ be the inclussion map. Now for any integer a, we have (Theorem 2.5.2) already proved that

$$\begin{aligned}
&\sum_{g\in G} f(g)a^{n/o(g)} \equiv 0 \pmod{n} \\
\implies &\sum_{g\in G} g a^{n/o(g)} \equiv 0 \pmod{n} \\
\implies &\sum_{d|n} \left(\sum_{g\in G_d} g \right) a^{n/d} \equiv 0 \pmod{n} \\
\implies &\sum_{d|n} \mu(d) a^{n/d} \equiv 0 \pmod{n}, \quad \text{by Lemma 2.5.5.}
\end{aligned}$$

□

We can also obtain some generalizations of Fermat's Little Theorem by reducing the congruence (2.5.a) to special cases. For example-

Considering $f : G \longrightarrow \mathbb{C}^*$ to be the trivial homomorphism, we get the following corollary of the above Theorem:

Corollary 2.5.7. *Let G be a finite group of order n. Then*

$$\sum_{g\in G} a^{n/o(g)} \equiv 0 \pmod{n} \tag{2.5.b}$$

for any integer a.

In the special case where G is cyclic of prime order p, G contains one element of order 1 and $p-1$ elements of order p, and so the congruence (2.5.b) gives

$$a^p \equiv a \pmod{p},$$

for all integers a, which is Fermat's Little Theorem.

Applying congruence (2.5.b) to the case where G is cyclic of order n, we obtain the following corollary which generalizes Fermat's Little Theorem.

Corollary 2.5.8. *Let a be an arbitrary integer. Then for every positive integer n,*

$$\sum_{d|n} \varphi(d) a^{n/d} \equiv 0 \pmod{n},$$

where φ is the Euler totient function.

Proof. Since G is a cyclic group of order n, for each divisor d of n there exists a unique subgroup of order d. Therefore for each divisor d of n there exists exactly $\varphi(d)$ elements of order d in G. Then by Corollary 2.5.7, we have

$$\sum_{d|n} \varphi(d) a^{n/d} \equiv 0 \pmod{n},$$

for all $a \in \mathbb{Z}$. □

Chapter 3

Quadratic Reciprocity Law in finite groups

The Quadratic Reciprocity Law has a very special place in the theory of numbers ever since Gauss, at the age of ninteen, proved it in 1796. Since then many proofs have been given. In this chapter, we present a recently developed group-theoretic generalization of the law.

3.1 An elegant form of Quadratic Reciprocity Law

The classical quadratic reciprocity law states that for any two distinct odd primes p and q,

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right). \tag{3.1.a}$$

Using the notion of Legendre Symbol, Jacobi Symbol and Kronecker Symbol as mentioned in Section 1.10, this law can be restated as follows:

Theorem 3.1.1. *Let n be an odd positive integer and a any integer. then*

$$\left(\frac{a}{n}\right) = \left(\frac{n^*}{a}\right),$$

where $n^* = (-1)^{\frac{n-1}{2}} n$.

To prove this theorem, we need the following lemma:

Lemma 3.1.2. *Let n be an odd positive integer. Then*

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

is a discriminant.

Proof of the Lemma:

$$n \text{ is odd} \Longrightarrow n \equiv 1 \pmod 4 \text{ or } n \equiv -1 \pmod 4.$$

Now

$$\begin{aligned} n \equiv 1 \pmod 4 &\Longrightarrow n = 1 + 4t, \ t \in \mathbb{Z} \\ &\Longrightarrow \frac{n-1}{2} = 2t \\ &\Longrightarrow n^* = n \equiv 1 \pmod 4 \\ &\Longrightarrow n^* \text{ is a discriminant.} \end{aligned}$$

Again

$$\begin{aligned} n \equiv -1 \pmod 4 &\Longrightarrow n = -1 + 4t, \ t \in \mathbb{Z} \\ &\Longrightarrow n - 1 + 2 = 4t \end{aligned}$$

$$\Longrightarrow \quad \frac{n-1+2}{2} = 2t$$
$$\Longrightarrow \quad \frac{n-1}{2} + 1 = 2t$$
$$\Longrightarrow \quad \frac{n-1}{2} = 2t - 1$$
$$\Longrightarrow \quad n^* = -n \equiv 1 \pmod 4$$
$$\Longrightarrow \quad n^* \text{ is a discriminant.}$$

Proof of the Theorem:

Without any loss we can assume that $a > 0$ and gcd $(a, n) = 1$, since

$$\left(\frac{a}{n}\right) = 0 = \left(\frac{n^*}{a}\right), \text{ if gcd } (a, n) \neq 1.$$

and

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \text{sign of } n^* = \left(\frac{n^*}{-1}\right).$$

Let $a = 2^k b$, where b is an odd integer and $k \in \mathbb{N} \cup \{0\}$. Then

$$\left(\frac{a}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{b}{n}\right) = (-1)^{\frac{n^2-1}{8}k}(-1)^{\frac{b-1}{2}\frac{n-1}{2}} \left(\frac{n}{b}\right). \tag{3.1.b}$$

Now,

$$\begin{aligned}\left(\frac{n^*}{a}\right) = \left(\frac{n^*}{2}\right)^k \left(\frac{n^*}{b}\right) = \left(\frac{n^*}{2}\right)^k \left(\frac{(-1)^{\frac{n-1}{2}} n}{b}\right) \\ &= (-1)^{\frac{n^2-1}{8}k} \left(\frac{-1}{b}\right)^{\frac{n-1}{2}} \left(\frac{n}{b}\right) \\ &= (-1)^{\frac{n^2-1}{8}k}(-1)^{\frac{b-1}{2}\frac{n-1}{2}} \left(\frac{n}{b}\right) \\ &= \left(\frac{a}{n}\right), \text{ by } (3.1.b).\end{aligned}$$

3.2 Legendre symbol in terms of Dirichlet Character

A character f of the group $\mathbb{Z}_n{}^\star$, the group of units in $\mathbb{Z}_n$ where n is a positive integer, gives rise to a Dirichlet character modulo n. In this section we shall show that if we take n to be an odd prime p, then $\mathbb{Z}_p{}^\star$ has a unique character of order 2 and its associated Dirichlet character is the usual Legendre symbol.

Definition 3.2.1. Consider $\mathbb{Z}_n$ as a ring, where n is a positive integer. Let $G = \mathbb{Z}_n{}^\star$ be the group of units in $\mathbb{Z}_n$. Corresponding to each character f of G, we define an arithmetical function $\chi_f : \mathbb{N} \longrightarrow \mathbb{C}$ given by

$$\chi_f(a) = \begin{cases} f(\overline{a}), & \text{if gcd } (a,n) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

The function χ_f is called a *Dirichlet character modulo n.*

Consider the group $\mathbb{Z}_p{}^\star$, p an odd prime. Then $\mathbb{Z}_p{}^\star$ is a cyclic group of (even) order $p-1$. Therefore $\mathrm{Hom}(\mathbb{Z}_p{}^\star, \mathbb{C}^\star)$ is a cyclic group of order $p-1$ and has a unique element of order 2 say f. Then

Lemma 3.2.2. *χ_f is the usual Legendre Symbol.*

Proof. We have

$$\chi_f(a) = \begin{cases} f(\overline{a}), & \text{if gcd } (a,p) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Define

$$\overline{f} : \mathbb{Z}_p{}^\star \longrightarrow \mathbb{C}^\star \text{ given by } \bar{f}(\overline{a}) = \left(\frac{a}{p}\right).$$

Clearly it is well defined. Now for $\overline{x}, \overline{y} \in \mathbb{Z}_p^{\star}$,

$$\overline{f}(\overline{x}\,\overline{y}) = \overline{f}(\overline{xy}) = \left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \overline{f}(\overline{x})\overline{f}(\overline{y}).$$

Therefore $\overline{f}$ is a homomorphism of $\mathbb{Z}_p^{\star}$ of order 2 and so $\overline{f} = f$.

Therefore

$$\chi_f(a) = \begin{cases} \overline{f}(\overline{a}), & \text{if gcd } (a,p) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

$$= \begin{cases} \left(\frac{a}{p}\right), & \text{if gcd } (a,p) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Thus χ_f is the usual Legendre Symbol. □

3.3 Legendre symbol: Zolotarev's observation.

In 1872, Egor Ivanovich Zolotarev, a Russian mathematician gave another interpretation of Legendre Symbol. In this section we shall study this ovservation elaborately.

Let $G = \mathbb{Z}_p$, the group of residue classes modulo p under addition. Let a be an integer such that gcd $(a,p) = 1$.

Consider

$$\phi_{\overline{a}} : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \text{ given by } \overline{x} \longmapsto \overline{ax}.$$

Now

$$\overline{x} = \overline{y} \implies \overline{ax} = \overline{ay} \implies \phi_{\overline{a}}(\overline{x}) = \phi_{\overline{a}}(\overline{y}).$$

Therefore $\phi_{\overline{a}}$ is well defined. Again

$$\overline{ax} = \overline{ay} \implies ax \equiv ay \pmod{p} \implies x \equiv y \pmod{p} \implies \overline{x} = \overline{y}.$$

That is $\phi_{\overline{a}}$ is one one. Therefore $\phi_{\overline{a}}$ is a permutation on $\mathbb{Z}_p$.

Note 3.3.1. We have

$$\phi_{\overline{a}} : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p, \ \phi_{\overline{b}} : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p \implies \phi_{\overline{a}} \circ \phi_{\overline{b}} : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p.$$

Now

$$(\phi_{\overline{a}} \circ \phi_{\overline{b}})(\overline{x}) = \phi_{\overline{a}}(\phi_{\overline{b}}(\overline{x})) = \phi_{\overline{a}}(\overline{bx}) = \overline{abx} = \phi_{\overline{ab}}(\overline{x}).$$

Therefore

$$\phi_{\overline{a}} \circ \phi_{\overline{b}} = \phi_{\overline{ab}}.$$

Lemma 3.3.2. *Define*

$$F : \mathbb{Z}_p{}^{\star} \longrightarrow \mathbb{C}^{\star} \text{ given by } F(\overline{a}) = sgn\ \phi_{\overline{a}}.$$

Then F is a homomorphism.

Proof. For $\overline{a}, \overline{b} \in \mathbb{Z}_p{}^{\star}$,

$$\begin{aligned} F(\overline{a}\,\overline{b}) = F(\overline{ab}) = sgn\ \phi_{\overline{ab}} &= sgn\ (\phi_{\overline{a}} \circ \phi_{\overline{b}}) \\ &= sgn\ \phi_{\overline{a}}\ sgn\ \phi_{\overline{b}} = F(\overline{a})F(\overline{b}). \end{aligned}$$

(noting that signature of the product is the product of the signature.)

Therefore F is a homomorphism on $\mathbb{Z}_p{}^{\star}$ i.e., F is a character of $\mathbb{Z}_p{}^{\star}$. □

Now let $\overline{x}$ be a generator of $\mathbb{Z}_p{}^{\star}$. Then $\phi_{\overline{x}}$ is a $(p-1)$ cycle. That is $\phi_{\overline{x}}$ is odd. Thus F is non trivial. Also F has order 2. Hence

$$F = f = \left(\frac{\cdot}{p}\right),$$

since in $\mathbb{Z}_p^{\star}$ order 2 homomorphism is unique.

3.4 The Quadratic symbol for a finite group

In this section we define the Quadratic symbol for a finite group G and study some properties and implications of this symbol.

Let G be a finite group of order n with conjugacy classes $C_1 = \{1\}, C_2, \ldots, C_m$. Let a be an integer relatively prime to n.

Lemma 3.4.1. *Consider the map $f : G \longrightarrow G$ given by $f(g) = g^a$. Then f is a permutation of G.*

Proof. Suppose $g_1^a = g_2^a$.
Now

$$g_1 = g_1^1 = g_1^{ax+ny} = g_1^{ax} g_1^{ny} = g_1^{ax} = g_2^{ax} = g_2^{ax+ny} = g_2.$$

Therefore f is an injective map from G onto itself. That is f is a permutation of G. □

This f induces a permutation on the conjugacy classes of G also sending $C \longmapsto C^a$. Let this permutation be ϕ_a.

We now define Quadratic symbol for a finite group as follows:

Definition 3.4.2. Define $F : \mathbb{N} \longrightarrow \mathbb{C}$ given by

$$F(a) = \begin{cases} sgn\ \phi_a, & \text{if } \gcd(a, n) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

$F(a)$ is called the *Quadratic symbol* of G at a and is denoted by $\left(\frac{a}{G}\right)$.

In view of Zolotarev's observation we can see that the Quadratic symbol for $G = \mathbb{Z}_p$, where p is an odd prime is the Legendre symbol:

$$\left(\frac{a}{G}\right) = \left(\frac{a}{|G|}\right). \tag{3.4.a}$$

The following lemma tells us a very interesting property of F, which says

Lemma 3.4.3. *F defines a real Dirichlet character modulo n.*

Proof. Let G be a finite group of order n, and a be an integer relatively prime to n. Define

$$f : \mathbb{Z}_n{}^\star \longrightarrow \mathbb{C}^\star \text{ given by } f(\overline{a}) = sgn\ \phi_a,$$

Where ϕ_a is the permutation on the conjugacy classes of G given by $C_j \longmapsto C_j{}^a$. Now

$$\overline{a} = \overline{b} \implies a = b + nt \implies sgn\ \phi_a = sgn\ \phi_b,$$

(noting that $C^{b+nt} = C^b$ and therefore $\phi_{b+nt} = \phi_b$). So f is well defined. Also

$$(\phi_a \circ \phi_b)(C) = \phi_a(\phi_b(C)) = \phi_a(C^b) = C^{ab} = \phi_{ab}(C).$$

That is $\phi_a \circ \phi_b = \phi_{ab}$. So,

$$f(\overline{a}\overline{b}) = f(\overline{ab}) = sgn\ \phi_{ab} = sgn\ (\phi_a \circ \phi_b) = f(\overline{a})f(\overline{b}).$$

Therefore f is a character on $\mathbb{Z}_n{}^\star$.

Now,

$$F(a) = \begin{cases} sgn\ \phi_a, & \text{if } \gcd(a,n) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

$$= \begin{cases} f(\overline{a}), & \text{if } \gcd(a,n) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Thus F is a real Dirichlet character modulo n. □

Definition 3.4.4. Let G be any group (finite or infinite). Consider the map $f : G \longrightarrow G$ given by $g \longmapsto g^{-1}$.

A conjugacy class C in G is said to be *real* if $C^{-1} = C$ otherwise it is said to be *complex*. Here C^{-1} denotes $f(C)$.

Remark 3.4.5. The complex conjugacy classes occurs in pairs C and C^{-1} with $|C| = |C^{-1}|$. We order the conjugacy classes so that the first r_1 classes are real. Thus $m = r_1 + 2r_2$, where r_2 is half the number of complex conjugacy classes. We then set

$$\begin{aligned} d = d(G) =& (-1)^{r_2}|G|^{r_1}\prod_{j=1}^{r_1}|C_j|^{-1} \\ =& (-1)^{r_2}\frac{|G|}{|C_1|}\frac{|G|}{|C_2|}\cdots\frac{|G|}{|C_{r_1}|} \\ =& (-1)^{r_2}n\frac{|G|}{|C_2|}\cdots\frac{|G|}{|C_{r_1}|}. \end{aligned}$$

Since for any conjugacy class C, $\dfrac{|G|}{|C|}$ is a nonzero integer therefore it follows d is a non zero integer. Clearly, given a prime p we have $p \mid n$ if and only if $p \mid d$. Thus d has the same prime divior as n. We call d the *discriminant* of G, a name that is justified by the fact that $d \equiv o$ or $1 \pmod 4$, as we shall see later.

3.5 Matrix of character table

In this section we shall consider the Matrix of a character table and then establish a very crucial relation between the determinant of the Matrix of a character table and d, the discriminant of G.

Let G be a finite group with conjugacy classes $C_1 = \{1\}, C_2, \ldots, C_m$ and $g_j \in C_j$ be a representative element for all j. The matrix

$$M = [\chi_i(g_j)]_{m \times m}$$

where χ_i, $i = 1, 2, \ldots, m$ are the irreducible characters of G is called the *Matrix of the character table* of G.

Lemma 3.5.1. *Let G be a finite group of order n with conjugacy clases $C_1 = \{1\}, C_2, \ldots, C_m$. M be the matrix of character table of G. Then*

$$(\det M)^2 = l^2 d,$$

where

$$d = (-1)^{r_2} |G|^{r_1} \prod_{j=1}^{r_1} |C_j|^{-1}, \quad l \in \mathbb{N}$$

Proof. Let $\chi_1, \chi_2, \ldots, \chi_m$ be the irreducible characters of G. $g_i \in C_i$ be a representative element of C_i, $i = 1, 2, \ldots, m$. Now

$$M = \begin{pmatrix} \chi_1(g_1)\ \chi_1(g_2) & \cdots & \chi_1(g_m) \\ \chi_2(g_1)\ \chi_2(g_2) & \cdots & \chi_2(g_m) \\ & \cdots & \\ \chi_m(g_1)\ \chi_m(g_2) & \cdots & \chi_m(g_m) \end{pmatrix}$$

$$M^* = (\overline{M})' = \begin{pmatrix} \overline{\chi_1(g_1)}\ \overline{\chi_2(g_1)} & \cdots & \overline{\chi_m(g_1)} \\ \overline{\chi_1(g_2)}\ \overline{\chi_2(g_2)} & \cdots & \overline{\chi_m(g_2)} \\ & \cdots & \\ \overline{\chi_1(g_m)}\ \overline{\chi_2(g_m)} & \cdots & \overline{\chi_m(g_m)} \end{pmatrix}$$

Again

$$M^*M = \begin{pmatrix} \overline{\chi_1(g_1)}\ \overline{\chi_2(g_1)} & \cdots & \overline{\chi_m(g_1)} \\ \overline{\chi_1(g_2)}\ \overline{\chi_2(g_2)} & \cdots & \overline{\chi_m(g_2)} \\ & \cdots & \\ \overline{\chi_1(g_m)}\ \overline{\chi_2(g_m)} & \cdots & \overline{\chi_m(g_m)} \end{pmatrix} \begin{pmatrix} \chi_1(g_1)\ \chi_1(g_2) & \cdots & \chi_1(g_m) \\ \chi_2(g_1)\ \chi_2(g_2) & \cdots & \chi_2(g_m) \\ & \cdots & \\ \chi_m(g_1)\ \chi_m(g_2) & \cdots & \chi_m(g_m) \end{pmatrix}$$

$$= \begin{pmatrix} \sum_{i=1}^{m} \overline{\chi_i(g_1)}\chi_i(g_1) & \sum_{i=1}^{m} \overline{\chi_i(g_1)}\chi_i(g_2) & \cdots & \sum_{i=1}^{m} \overline{\chi_i(g_1)}\chi_i(g_m) \\ \sum_{i=1}^{m} \overline{\chi_i(g_2)}\chi_i(g_1) & \sum_{i=1}^{m} \overline{\chi_i(g_2)}\chi_i(g_2) & \cdots & \sum_{i=1}^{m} \overline{\chi_i(g_2)}\chi_i(g_m) \\ & & \cdots & \\ \sum_{i=1}^{m} \overline{\chi_i(g_m)}\chi_i(g_1) & \sum_{i=1}^{m} \overline{\chi_i(g_m)}\chi_i(g_2) & \cdots & \sum_{i=1}^{m} \overline{\chi_i(g_m)}\chi_i(g_m) \end{pmatrix}$$

$$= \begin{pmatrix} |C_G(g_1)| & \dots & 0 \\ & \dots & \\ 0 & \dots & |C_G(g_m)| \end{pmatrix}, \text{ by } \textit{Theorem } 1.6.25$$

$$= \begin{pmatrix} |G||C_1|^{-}1 & \dots & 0 \\ & \dots & \\ 0 & \dots & |G||C_m|^{-}1 \end{pmatrix} \tag{3.5.a}$$

Now,

$$\det \overline{M} = \begin{vmatrix} \overline{\chi_1(g_1)} & \overline{\chi_1(g_2)} & \dots & \overline{\chi_1(g_m)} \\ \overline{\chi_2(g_1)} & \overline{\chi_2(g_2)} & \dots & \overline{\chi_2(g_m)} \\ & \dots & & \\ \overline{\chi_m(g_1)} & \overline{\chi_m(g_2)} & \dots & \overline{\chi_m(g_m)} \end{vmatrix}$$

$$= \begin{vmatrix} \chi_1(g_1^{-1}) & \chi_1(g_2^{-1}) & \dots & \chi_1(g_m^{-1}) \\ \chi_2(g_1^{-1}) & \chi_2(g_2^{-1}) & \dots & \chi_2(g_m^{-1}) \\ & \dots & & \\ \chi_m(g_1^{-1}) & \chi_m(g_2^{-1}) & \dots & \chi_m(g_m^{-1}) \end{vmatrix}, \textit{ by } \textit{Lemma } 1.6.24.$$

$$= \begin{vmatrix} \chi_1(g_1) & \chi_1(g_2) & \dots & \chi_1(g_{r_1}) & \chi_1(g_{r_1+1}^{-1}) & \dots & \chi_1(g_{r_1+2r_2}^{-1}) \\ \chi_2(g_1) & \chi_2(g_2) & \dots & \chi_2(g_{r_1}) & \chi_2(g_{r_1+1}^{-1}) & \dots & \chi_2(g_{r_1+2r_2}^{-1}) \\ & & & \dots & & & \\ \chi_m(g_1) & \chi_m(g_2) & \dots & \chi_m(g_{r_1}) & \chi_m(g_{r_1+1}^{-1}) & \dots & \chi_m(g_{r_1+2r_2}^{-1}) \end{vmatrix}$$

Suppose,

$$\chi_s(g_{r_1+i}^{-1}) = \chi_s(g_{r_1+j}), \text{ where } i, j \in \{1, 2, \dots, 2r_2\};\ \ i \neq j;\ s \in \{1, 2, \dots, m\}.$$

Then

$$\begin{aligned} & \overline{\chi_s(g_{r_1+i})} = \chi_s(g_{r_1+j}) \\ \iff & \overline{\overline{\chi_s(g_{r_1+i})}} = \overline{\chi_s(g_{r_1+j})} \\ \iff & \chi_s(g_{r_1+i}) = \chi_s(g_{r_1+j}^{-1}). \end{aligned}$$

Therefore

$$\det \overline{M} = \begin{vmatrix} \chi_1(g_1)\ \chi_1(g_2)\ \cdots\ \chi_1(g_{r_1})\ \chi_1(g_{\phi(r_1+1)})\ \cdots\ \chi_1(g_{\phi(r_1+2r_2)}) \\ \chi_2(g_1)\ \chi_2(g_2)\ \cdots\ \chi_2(g_{r_1})\ \chi_2(g_{\phi(r_1+1)})\ \cdots\ \chi_2(g_{\phi(r_1+2r_2)}) \\ \cdots \\ \chi_m(g_1)\ \chi_m(g_2)\ \cdots\ \chi_m(g_{r_1})\ \chi_m(g_{\phi(r_1+1)})\ \cdots\ \chi_m(g_{\phi(r_1+2r_2)}) \end{vmatrix}.$$

where, $\phi \in SymX$, $X = \{r_1+1, r_1+2, \ldots, r_1+2r_2\}$ such that ϕ is a product of transpositions of total length $2r_2$. Therefore

$$\det \overline{M} = sgn(\phi) \cdot \det M = (-1)^{r_2} \det M. \tag{3.5.b}$$

Again by equation (3.5.a), we have

$$\begin{aligned} & \det(M^*M) = |G|^{r_1} \prod_{j=1}^{r_1} |C_j|^{-1} |G|^{2r_2} \prod_{i=1}^{2r_2} |C_{r_1+i}|^{-1} \\ \implies & \det(M^*)det(M) = |G|^{r_1} \prod_{j=1}^{r_1} |C_j|^{-1} \left(|G|^{r_2} \prod_{i=1}^{r_2} |C_{r_1+i}|^{-1} \right)^2, \text{ by Remark 3.4.5.} \\ \implies & (-1)^{r_2} (\det M)^2 = |G|^{r_1} \prod_{j=1}^{r_1} |C_j|^{-1} l^2, \text{ by equation (3.5.}b\text{).} \\ \implies & (\det M)^2 = (-1)^{r_2} |G|^{r_1} \prod_{j=1}^{r_1} |C_j|^{-1} l^2 \\ \implies & (\det M)^2 = l^2 d, \quad l \in \mathbb{N}. \end{aligned}$$

This completes the proof. □

Remark 3.5.2. We have

$$\det(M) = \sum_{\phi \in S_m} sgn(\phi)\chi_1(g_{\phi(1)})\chi_2(g_{\phi(2)}) \cdots \chi_m(g_{\phi(m)}).$$

Let

$$A = \sum_{\phi \in S_m,\ \phi \text{ even}} \chi_1(g_{\phi(1)})\chi_2(g_{\phi(2)}) \cdots \chi_m(g_{\phi(m)}).$$

$$B = \sum_{\phi \in S_m,\ \phi \text{ odd}} \chi_1(g_{\phi(1)})\chi_2(g_{\phi(2)}) \cdots \chi_m(g_{\phi(m)}).$$

Clearly $\det M = A - B$.

In view of Theorem 1.6.28, we have A and B are algebraic integers and therefore $A + B$ and AB are algebraic integers. We shall in fact prove that $A + B$ and AB are rational integers. The following lemma is important to prove this result.

Lemma 3.5.3. *Let G be a finite group of order n with conjugacy classes $C_1 = \{1\}, C_2, \ldots, C_m$ and $g_i \in C_i$ be a representative element for all i. If gcd $(a, n) = 1$, then*

$$\{g_1, g_2, \ldots, g_m\} = \{g_1^a, g_2^a, \ldots, g_m^a\}.$$

Proof. It is enough to show that g_i^a is not conjugate to g_j^a for any $i, j = 1, 2, \ldots, m$; $i \neq j$. Suppose, $g_i^a \sim g_j^a$ for $i, j = 1, 2, \ldots, m$; $i \neq j$. Then

$$\begin{aligned} & g_j^a = g g_i^a g^{-1}, \text{ for some } g \in G \\ \Longrightarrow \quad & g_j^a = (g g_i g^{-1})^a \\ \Longrightarrow \quad & g_j = g g_i g^{-1}, \text{ by Lemma 3.4.1} \\ \Longrightarrow \quad & g_i \sim g_j, \end{aligned}$$

a contradiction. Therefore g_i^a is not conjugate to g_j^a. □

Following is a corollary of the above lemma:

Corollary 3.5.4. *Let G be a finite group of order n with conjugacy classes $C_1 = \{1\}, C_2, \ldots, C_m$ and $g_i \in C_i$ be a representative element for all i. If gcd $(a, n) = 1$, then there exist $\psi \in S_m$ such that $g_i^a = g_{\psi(i)}$.*

Theorem 3.5.5. *$A+B$ and AB are invariant under the Galois group. That is, if G is a finite group of order n and a is a rational integer prime to n and if $\sigma \in \mathcal{G}$, and $\sigma(\zeta_n) = \zeta_n{}^a$, then*

$$\sigma(A + B) = A + B \text{ and } \sigma(AB) = AB.$$

Hence in particular $A + B$ and AB are rational integers.

Proof. In this proof $\phi \in S_m$.

$$\begin{aligned}
\sigma(A+B) &= \sigma\left(\sum_{\phi}\chi_1(g_{\phi(1)})\chi_2(g_{\phi(2)})\cdots\chi_m(g_{\phi(m)})\right) \\
&= \sum_{\phi}\sigma\left(\chi_1(g_{\phi(1)})\chi_2(g_{\phi(2)})\cdots\chi_m(g_{\phi(m)})\right) \\
&= \sum_{\phi}\sigma\left(\chi_1(g_{\phi(1)})\right)\sigma\left(\chi_2(g_{\phi(2)})\right)\cdots\sigma\left(\chi_m(g_{\phi(m)})\right) \\
&= \sum_{\phi}\chi_1(g^a_{\phi(1)})\chi_2(g^a_{\phi(2)})\cdots\chi_m(g^a_{\phi(m)}), \quad \text{by Theorem 1.6.30} \\
&= \sum_{\phi}\chi_1(g_{\psi(\phi(1))})\chi_2(g_{\psi(\phi(2))})\cdots\chi_m(g_{\psi(\phi(m))}), \quad \text{by Corollary 3.5.4} \\
&= \sum_{\phi}\chi_1(g_{\phi(1)})\chi_2(g_{\phi(2)})\cdots\chi_m(g_{\phi(m)}) \\
&= A + B.
\end{aligned}$$

Again

$$
\begin{aligned}
&\sigma(AB) \\
&= \sigma\left(\left(\sum_{\phi\ even}\chi_1(g_{\phi(1)})\cdots\chi_m(g_{\phi(m)})\right)\left(\sum_{\phi\ odd}\chi_1(g_{\phi(1)})\cdots\chi_m(g_{\phi(m)})\right)\right) \\
&= \sigma\left(\sum_{\phi\ even}\chi_1(g_{\phi(1)})\cdots\chi_m(g_{\phi(m)})\right)\sigma\left(\sum_{\phi\ odd}\chi_1(g_{\phi(1)})\cdots\chi_m(g_{\phi(m)})\right) \\
&= \left(\sum_{\phi\ even}\chi_1(g^a_{\phi(1)})\cdots\chi_m(g^a_{\phi(m)}\right)\left(\sum_{\phi\ odd}\chi_1(g^a_{\phi(1)})\cdots\chi_m(g^a_{\phi(m)}\right) \\
&= \left(\sum_{\phi\ even}\chi_1(g_{\psi(\phi(1))})\cdots\chi_m(g_{\psi(\phi(m))})\right)\left(\sum_{\phi\ odd}\chi_1(g_{\psi(\phi(1))})\cdots\chi_m(g_{\psi(\phi(m))})\right) \\
&= \left(\sum_{\phi\ even}\chi_1(g_{\phi(1)})\cdots\chi_m(g_{\phi(m)})\right)\left(\sum_{\phi\ odd}\chi_1(g_{\phi(1)})\cdots\chi_m(g_{\phi(m)})\right) \\
&= AB.
\end{aligned}
$$

□

3.6 Generalized Q. R. L.

We are now in a position to prove the Generalized Quadratic Reciprocity Law for finite groups.

Theorem 3.6.1. Generalized Q. R. L.
Let G be a finite group of order n with discriminant $d = (-1)^{r_2} n \frac{|G|}{|C_2|}\cdots\frac{|G|}{|C_{r_1}|}$. Then

(i) $d \equiv 0$ *or* $1 \pmod 4$.

(ii) *For any integer* a, $\left(\frac{a}{G}\right) = \left(\frac{d}{a}\right)$.

(iii) *For any integer* a, $\left(\frac{a}{G}\right)$ *is trivial if and only if* d *is a square.*

Proof. Proof of Part (i)

We have

$$l^2 d = (detM)^2 = (A-B)^2 = (A+B)^2 - 4AB.$$

Again

$$\begin{aligned} & (A+B)^2 - 4AB \equiv (A+B)^2 \pmod 4 \\ \Longrightarrow \quad & (A+B)^2 - 4AB \equiv 0 \text{ or } 1 \pmod 4 \\ \Longrightarrow \quad & l^2 d \equiv 0 \text{ or } 1 \pmod 4. \end{aligned} \tag{3.6.a}$$

Now, if G is odd, then l is odd and d is odd. Therefore

$$l^2 d \equiv 1 \pmod 4 \text{ and } l^2 \equiv 1 \pmod 4.$$

Which implies $d \equiv 1 \pmod 4$.

Again if G is even, then since

$$|G| = 1 + |C_2| + \cdots + |C_{r_1}| + |C_{r_1+1}| + \cdots + |C_{r_1+2r_2}|,$$

we have C_i is odd for some $i = 2, 3, \ldots, r_1$, (noting that complex conjugacy classes occurs in pairs). It follows $d \equiv 0 \pmod 4$. □

The prove of part (ii) is a direct consequence of the following propositions:

Proposition 3.6.2. *Let* $\sigma \in \mathcal{G}$ *be such that* $\sigma(\zeta_n) = \zeta_n{}^a$, *where* ζ_n *is a primitive* n^{th} *root of unity and gcd* $(a, n) = 1$. *Then*

$$\sigma(\sqrt{d}) = \left(\frac{a}{G}\right)\sqrt{d}.$$

Proof. We have

$$detM = \begin{vmatrix} \chi_1(g_1)\ \chi_1(g_2) & \cdots & \chi_1(g_m) \\ \chi_2(g_1)\ \chi_2(g_2) & \cdots & \chi_2(g_m) \\ & \cdots & \\ \chi_m(g_1)\ \chi_m(g_2) & \cdots & \chi_m(g_m) \end{vmatrix}$$

Using Theorem 1.6.30, we get

$$\begin{aligned} \sigma(detM) &= \begin{vmatrix} \chi_1(g_1^a)\ \chi_1(g_2^a) & \cdots & \chi_1(g_m^a) \\ \chi_2(g_1^a)\ \chi_2(g_2^a) & \cdots & \chi_2(g_m^a) \\ & \cdots & \\ \chi_m(g_1^a)\ \chi_m(g_2^a) & \cdots & \chi_m(g_m^a) \end{vmatrix} \\ &= \left(\frac{a}{G}\right) detM. \end{aligned}$$

It follows from Theorem 3.5.1 that

$$\sigma(\pm l\sqrt{d}) = \left(\frac{a}{G}\right)(\pm l\sqrt{d}).$$

Which implies that

$$\sigma(\sqrt{d}) = \left(\frac{a}{G}\right)\sqrt{d}.$$

□

Proposition 3.6.3. *Let G be a finite group of order n with discriminant d. Then for any prime p, $p \nmid n$*

$$\left(\frac{p}{G}\right) = \left(\frac{d}{p}\right).$$

Proof. We know that d and p has the same prime divisors. Therefore $p \nmid n \implies p \nmid d$ and so $\left(\frac{d}{p}\right) = \pm 1$.

Suppose $\left(\frac{d}{p}\right) = 1$. Then applying Theorem 1.11.6 and Corollary 1.11.5, we get

$$\begin{aligned} p \text{ splits in } \mathbb{Q}(\sqrt{d}) \ \ i.e., \ \sigma_p(\sqrt{d}) &= \sqrt{d} \\ i.e., \ \left(\frac{p}{G}\right)\sqrt{d} &= \sqrt{d} \\ i.e., \ \left(\frac{p}{G}\right) &= 1 = \left(\frac{d}{p}\right). \end{aligned}$$

Next Suppose $\left(\frac{d}{p}\right) = -1$. Then also applying Theorem 1.11.6 and Corollary 1.11.5, we get

$$\begin{aligned} p \text{ doesnot split in } \mathbb{Q}(\sqrt{d}) \ \ i.e., \ \ \sigma_p(\sqrt{d}) &\neq \sqrt{d} \\ i.e., \ \ \sigma_p(\sqrt{d}) &= -\sqrt{d} \\ i.e., \ \ \left(\frac{p}{G}\right)\sqrt{d} &= -\sqrt{d} \\ i.e., \ \ \left(\frac{p}{G}\right) &= -1 = \left(\frac{d}{p}\right). \end{aligned}$$

Therefore we can conclude that

$$\left(\frac{p}{G}\right) = \left(\frac{d}{p}\right) \text{ if } p \nmid n.$$

□

Proposition 3.6.4. *Let G be a finite group of order n with discriminant d. Then*

$$\left(\frac{-1}{G}\right) = \left(\frac{d}{-1}\right).$$

Proof. Let $C_1 = \{1\}, C_2, \ldots, C_m$ be the conjugacy classes of G. r_1 the number of real conjugacy classes and r_2 half the number of complex conjugacy

classes.

We have

$$\left(\frac{d}{-1}\right) = sign\ d = (-1)^{r_2},\ \text{By Remark 3.4.5.}$$

Again

$$\left(\frac{-1}{G}\right) = sgn\ \phi_{-1},$$

where ϕ_{-1} is the permutation on the conjugacy classes of G given by $C \longmapsto C^{-1}$. Now

$$\phi_{-1} = \begin{pmatrix} C_1 & C_2 & \dots & C_{r_1} & C_{r_1+1} & \dots & C_m \\ C_1 & C_2 & \dots & C_{r_1} & C_{\phi(r_1+1)} & \dots & C_{\phi(m)} \end{pmatrix}$$

where $\phi \in SymX$, $X = \{r_1+1, r_1+2, \dots, r_1+2r_2\}$ such that ϕ is a product of transpositions of total length $2r_2$.

Therefore

$$\left(\frac{-1}{G}\right) = sgn\ \phi_{-1} = (-1)^{r_2} = \left(\frac{d}{-1}\right).$$

□

Since $\left(\frac{a}{G}\right)$ is a character modulo n therefore $\left(\frac{a}{G}\right)$ is totally multiplicative. Therefore Part (ii) of our main result follows from The above propositions by multiplicativity.

Proof of Part (iii)

We have by Lemma 3.6.2

$$\sigma(\sqrt{d}) = \left(\frac{a}{G}\right)\sqrt{d},\ \sigma \in \mathcal{G},\ a \text{ any integer prime to } n.$$

If $\left(\frac{a}{G}\right) = 1$, then

$$\sigma(\sqrt{d}) = \sqrt{d} \Longrightarrow \sqrt{d} \in \mathbb{Q} \Longrightarrow d \text{ is a square.}$$

Again if d is a square then

$$\sqrt{d} \in \mathbb{Q} \Longrightarrow \sqrt{d} = \sigma(\sqrt{d}) = \left(\frac{a}{G}\right)\sqrt{d} \Longrightarrow \left(\frac{a}{G}\right) = 1.$$

The following lemma is very important to prove the direct generalization of classical quadratic reciprocity law.

Lemma 3.6.5. *Let G be a finite group of odd order n. Then G has only one real conjygacy class namely $\{1\}$.*

Proof. Suppose C is any real conjugacy class of G and $g \in C$. Now

$$C \text{ is real} \Longrightarrow C = C^{-1} \Longrightarrow g \in C^{-1}.$$

Again $g \in C \Rightarrow g^{-1} \in C^{-1}$. Therefore $g \sim g^{-1}$. Now

$$\begin{aligned} g \sim g^{-1} &\Longrightarrow g^{-1} = hgh^{-1}, \text{for some } h \in G \\ &\Longrightarrow g = hg^{-1}h^{-1} = hhgh^{-1}h^{-1} = h^2gh^{-2} \\ &\Longrightarrow gh^2 = h^2g \\ &\Longrightarrow h^2 \in C_G(g). \end{aligned}$$

Moreover since n is odd, therefore $o(h)$ is odd, say $o(h) = 2l+1$ for some positive integer l. Now

$$h = h^{2l+1}h = h^{2l+2} = (h^2)^{l+1}.$$

Again

$$h^2 \in C_G(g) \Longrightarrow (h^2)^{l+1} \in C_G(g) \Longrightarrow h \in C_G(g) \Longrightarrow hg = gh.$$

Now

$$g^{-1} = hgh^{-1} = ghh^{-1} = g.$$

But $o(g)$ is odd. Therefore $g = 1$. i.e., $C = \{1\}$. □

In the special case if we take G to be a group of odd order, we get the following corollary of the Main Theorem, which is a direct generalization of classical quadratic reciprocity law (Theorem 3.1.1).

Corollary 3.6.6. *Let G be a finite group of odd order n. Then $d = n^*$ and for any integer a*

(i) $\left(\frac{a}{G}\right) = \left(\frac{n^*}{a}\right)$.

(ii) $\left(\frac{a}{G}\right)$ *is trivial if and only if n is a square.*

Proof. Proof of Part(i)
Let $C_1 = \{1\}, C_2, \ldots, C_m$ be the conjugacy classes of G. Then $C_1 = \{1\}$ is the only real conjugacy class of G and $d = (-1)^{\frac{m-1}{2}} n$. Now

$$n \text{ is odd} \Longrightarrow d \text{ is odd} \Longrightarrow d \equiv 1 \pmod 4 \Longrightarrow (-1)^{\frac{m-1}{2}} n \equiv 1 \pmod m. \tag{3.6.b}$$

Again we have

$$\begin{aligned} n \text{ is odd} &\Longrightarrow n^* \text{ is a discriminant} \Longrightarrow n^* \equiv 1 \pmod 4 \\ &\Longrightarrow (-1)^{\frac{n-1}{2}} n \equiv 1 \pmod 4. \end{aligned} \tag{3.6.c}$$

From equations (3.6.b) and (3.6.c) we get

$$\begin{aligned} & (-1)^{\frac{m-1}{2}} n \equiv (-1)^{\frac{n-1}{2}} n \pmod 4 \\ \Longrightarrow \quad & (-1)^{\frac{m-1}{2}} \equiv (-1)^{\frac{n-1}{2}} \pmod 4, \quad \text{since gcd } (n, 4) = 1. \\ \Longrightarrow \quad & (-1)^{\frac{m-1}{2}} = (-1)^{\frac{n-1}{2}} \\ \Longrightarrow \quad & d = n^*. \end{aligned}$$

and for any integer a,

$$\left(\frac{a}{G}\right) = \left(\frac{n^*}{a}\right).$$

□

To prove Part (ii) we need the following:

Lemma 3.6.7. *Let n be an odd positive integer. Then*

n^* is a square if and only if n is a square.

Proof.

$$n \text{ is odd } \Longrightarrow n \equiv \pm 1 \pmod 4.$$

Suppose n is a square. Then $n \not\equiv -1 \pmod 4$ and so

$$n \equiv 1 \pmod 4. \text{ So, } n = 1 + 4t, \text{ for some } t \in \mathbb{Z}.$$

Therefore

$$n^* = (-1)^{\frac{n-1}{2}} n = (-1)^{\frac{4t+1-1}{2}} n = (-1)^{2t} n = n, \text{ which is a square.}$$

Conversly, Suppose that n^* is a square. Now

$$n^* = (-1)^{\frac{n-1}{2}} n = \pm n.$$

Since n is positive,

$$n^* \neq -n. \text{ So } n = n^*, \text{ which is a square.}$$

□

The proof of Part (ii) follows immediately in view of our main theorem namely Theorem 3.6.1 and Lemma 3.6.7.

Finally we see from Theorem 3.6.6 and (3.1.a) that Zolotarev's result (3.4.a) holds for any group G of odd order.

Chapter 4

Arithmetic Functions of Finite Groups

One of the major portions in the theory of numbers is occupied by the arithmetic functions. These are complex valued functions defined on the set of positive integers. This chapter deals with the complex valued functions defined on the collection of all finite groups (abelian as well as non abelian).

4.1 Introduction

Let $\mathcal{G}$ be the collection of all finite groups (upto isomorphism). Then $\mathcal{G}$ can be regarded as a monoid with respect to the direct product of groups (treating the isomorphic groups as the identical ones). The identity element of $\mathcal{G}$ is given by the trivial group E_0, the group of order 1.

Let $\mathcal{X}$ be the collection of all finite abelian groups (upto isomorphism)

and let J be the collection of all completely reducible groups of $\mathcal{X}$. Then $\mathcal{X}$ and J are submonoids of $\mathcal{G}$.

Again let N^* be the monoid of the positive integers. Then $N^* \cong J$ under the correspondence $n \longmapsto G$, where n is a positive integer and G the unique completely reducible group of order n.

Let $\mathcal{A}(\mathcal{G})$ denote the collection of all complex-valued functions with domain $\mathcal{G}$ and $\mathcal{A}(\mathcal{X})$ denote the collection of all complex-valued functions with domain $\mathcal{X}$. Then $|\ |$, u and ε are three well known members of $\mathcal{A}(\mathcal{G})$

where for a given $G \in \mathcal{G}$ we define

$$|G| = \text{ the order of } G, \quad u(G) = 1, \quad \text{and} \quad \varepsilon(G) = \begin{cases} 1, & \text{if } G = E_0, \\ 0, & \text{otherwise.} \end{cases}$$

Similarly if we take $G \in \mathcal{X}$, then $|\ |$, u and ε defined as above are also members of $\mathcal{A}(\mathcal{X})$.

Moreover the functions A and τ'defined by $A(G) =$ the grade of $G =$ number of groups in $\mathcal{X}$ of order $\leq |G|$ and $\tau'(G) =$ number of direct factors of G are also members of $\mathcal{A}(\mathcal{X})$.

4.2 Convolutions of functions

In this section we study convolution of any two functions $f, g \in \mathcal{A}(\mathcal{G})$. We also study convolution of any two functions $f, g \in \mathcal{A}(\mathcal{X})$ defined in two different ways and some properties of these convolutions.

4.2.1 Convolution of functions in $\mathcal{A}(\mathcal{G})$

Let $G \in \mathcal{G}$. Then G has a composition series given by

$$E_0 = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = G.$$

The *Jordan-Hölder Theorem* states that any two composition series for a group have the same set-with-multiplicities of composition factors, upto isomorphism of factors. We denote this set with-multiplicities as $\mathcal{C}(G)$. Thus, for the above composition series

$$\mathcal{C}(G) = \{H_i/H_{i-1} : i = 1, 2, \ldots, n\}$$

and it is uniquely determined by G upto isomorphism of factors. By convention $\mathcal{C}(E_0) = \phi$.

Theorem 4.2.1. *For all $K \trianglelefteq G$ the set $\mathcal{C}(G)$ is the disjoint union (i.e., union counting multiplicities) of the sets $\mathcal{C}(G/K)$ and $\mathcal{C}(K)$.*

Proof. Let

$$(\{K\} =) H_0/K \lhd H_1/K \lhd H_2/K \lhd \cdots \lhd H_n (= G)/K$$

be a composition series of G/K. Since $\{K\} = H_0/K$, therefore $H_0 = K$. Moreover each H_i is a subgroup of G containing K. Also by (Third Isomorphism) Theorem 1.2.3,

$$\frac{H_{i+1}/K}{H_i/K} \cong \frac{H_{i+1}}{H_i}(simple), \quad i = 0, 1, 2, \ldots, n. \tag{4.2.a}$$

Now let

$$E_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_{m-1} \lhd K$$

be a composition series of K. Then

$$E_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_{m-1} \lhd K \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_{n-1} \lhd H_n = G$$

is a composition series of G. And

$$\begin{aligned} \mathcal{C}(G) &= \{N_1/E_0, N_2/N_1, \ldots, K/N_{m-1}, H_1/K, H_2/H_1, \ldots, G/H_{n-1}\} \\ &= \mathcal{C}(K) \sqcup C\,(G/K)\,. \end{aligned}$$

□

Following is a direct corollary of the above theorem.

Corollary 4.2.2. *For any $G_1, G_2 \in \mathcal{G}$, $\mathcal{C}(G_1 \times G_2)$ is the disjoint union (i.e., union counting multiplicities) of $\mathcal{C}(G_1)$ and $\mathcal{C}(G_2)$.*

Proof. In view of Theorems 1.3.3 and 1.3.4, we have $G_1 \trianglelefteq (G_1 \times G_2)$, and $(G_1 \times G_2)/G_1 \cong G_2$. Therefore by above theorem

$$\mathcal{C}(G_1 \times G_2) = \mathcal{C}(G_1) \sqcup \mathcal{C}((G_1 \times G_2)/G_1) = \mathcal{C}(G_1) \sqcup \mathcal{C}(G_2).$$

□

Given $G \in \mathcal{G}$, let $\Pi\mathcal{C}(G)$ denote the direct product of all members (counting multiplicities) of the set-with-multiplicities $\mathcal{C}(G)$. Clearly for any $G \in \mathcal{G}$, $\Pi\mathcal{C}(G)$ is completely reducible. As a convention we take $\Pi\mathcal{C}(E_0) = E_0$.

Definition 4.2.3. If f and g are any two functions in $\mathcal{A}(\mathcal{G})$ then their *convolution* is defined to be the function $f * g \in \mathcal{A}(\mathcal{G})$ given by

$$(f * g)(G) \;=\; \sum f(H)g(K),$$

where $G \in \mathcal{G}$, and the summation is over all ordered pairs $(H, K) \in \mathcal{G} \times \mathcal{G}$ which satisfy one of the following conditions:

(i) One of H and K is G, and the other is E_0,

(ii) $H \times K = \Pi\mathcal{C}(G)$, and none of H and K is E_0.

i.e.,

$$(f * g)(G) = f(G)g(E_0) + f(E_0)g(G) + \sum_{\substack{(H,K)\in\mathcal{G}\times\mathcal{G} \\ H\times K=\Pi\mathcal{C}(G) \\ H\neq E_0, K\neq E_0}} f(H)g(K),$$

where $G \in \mathcal{G}$.

Remark 4.2.4. If $f, g \in \mathcal{A}(\mathcal{G})$ then one can also define their *ordinary product* $fg \in \mathcal{A}(\mathcal{G})$ given by

$$fg(G) = f(G)g(G), \ \forall\, G \in \mathcal{G}.$$

However, the convolution defined above turns out to be more fruitful.

Theorem 4.2.5. *$\mathcal{A}(\mathcal{G})$ is a commutative ring with identity ϵ under the additive and the multiplicative operations given respectively by ordinary addition and convolution of funcitons.*

Proof. The proof of the theorem is a direct consequence of the following lemmas. □

Lemma 4.2.6. *If $f, g, h \in \mathcal{A}(\mathcal{G})$ then $((f * g) * h) = (f * (g * h))$.*

Proof. In this proof the sumation is taken over all ordered pairs (H, K), $(H', K'), (H'', K'') \in \mathcal{G} \times \mathcal{G}$ such that none of H, K, H', K', H'', K'' is E_0.

Now for $G \in \mathcal{G}$

$$
\begin{aligned}
&((f * g) * h)(G) \\
&= (f * g)(G)h(E_0) + (f * g)(E_0)h(G) + \sum_{H \times K = \Pi C(G)} (f * g)(H)h(K) \\
&= f(G)g(E_0)h(E_0) + f(E_0)g(G)h(E_0) + \sum_{H' \times K' = \Pi C(G)} f(H')g(K')h(E_0) \\
&+ f(E_0)g(E_0)h(G) + \sum_{H \times K = \Pi C(G)} (f(H)g(E_0)h(K) + f(E_0)g(H)h(K) \\
&+ \sum_{H'' \times K'' = \Pi C(H) = H} f(H'')g(K'')h(K)) \\
&= f(G)g(E_0)h(E_0) + f(E_0)g(G)h(E_0) + \sum_{H' \times K' = \Pi C(G)} f(H')g(K')h(E_0) \\
&+ f(E_0)g(E_0)h(G) + \sum_{H \times K = \Pi C(G)} f(H)g(E_0)h(K) + f(E_0)g(H)h(K) \\
&+ \sum_{\substack{H'' \times K'' \times K = \Pi C(G) \\ (H'', K'', K) \in \mathcal{G} \times \mathcal{G} \times \mathcal{G} \\ H'' \neq E_0, K'' \neq E_0, K \neq E_0}} f(H'')g(K'')h(K) \\
&= \sum_{(L, M, N) \in \mathcal{G} \times \mathcal{G} \times \mathcal{G}} f(L)g(M)h(N),
\end{aligned}
$$

such that

(*i*) One of L, M and N is G, and the other two are E_0, *or*

(*ii*) $L \times M \times N = \Pi C(G)$, and no two of L, M, N are E_0.

Similarly we can show that

$$(f * (g * h))(G) = \sum_{(L, M, N) \in \mathcal{G} \times \mathcal{G} \times \mathcal{G}} f(L)g(M)h(N),$$

such that the above two conditions hold.

□

Lemma 4.2.7. *If $f, g, h \in \mathcal{A}(\mathcal{G})$ then*

$$f * (g + h) = (f * g) + (f * h).$$

Proof. In this proof the sumation is taken over the ordered pairs (H, K), $(H', K') \in \mathcal{G} \times \mathcal{G}$ such that none of H, K, H', K' is E_0.

Now for $G \in \mathcal{G}$

$$\begin{aligned}
&(f * (g + h))(G) \\
&= f(G)(g + h)(E_0) + f(E_0)(g + h)(G) + \sum_{H \times K = \Pi C(G)} f(H)(g + h)(K) \\
&= f(G)g(E_0) + f(G)h(E_0) + f(E_0)g(G) + f(E_0)h(G) \\
&+ \sum_{H \times K = \Pi C(G)} f(H)g(K) + f(H)h(K).
\end{aligned}$$

Again

$$\begin{aligned}
&((f * g) + (f * h))(G) \\
&= (f * g)(G) + (f * h)(G) \\
&= f(G)g(E_0) + f(E_0)g(G) + \sum_{H \times K = \Pi C(G)} f(H)g(K) \\
&+ f(G)h(E_0) + f(E_0)h(G) + \sum_{H' \times K' = \Pi C(G)} f(H')g(K') \\
&= f(G)g(E_0) + f(E_0)g(G) + f(G)h(E_0) + f(E_0)h(G) \\
&+ \sum_{H \times K = \Pi C(G)} \{f(H)g(K) + f(H)h(K)\}.
\end{aligned}$$

Hence

$$f * (g + h) = (f * g) + (f * h).$$

□

4.2.2 Convolutions of functions in $\mathcal{A}(\mathcal{X})$

Here we give the definition of E-convolution of two functions in $\mathcal{A}(\mathcal{X})$ and study some properties of this convolution.

Definition 4.2.8. If f and g are any two functions $\mathcal{A}(\mathcal{X})$, then the *E-convolution* is defined to be the function $f \cdot g \in \mathcal{A}(\mathcal{X})$ given by

$$(f \cdot g)(G) = \sum_{\substack{D \times E = G \\ (D,E) \in \mathcal{G} \times \mathcal{G}}} f(D)g(E)$$

Remark 4.2.9. When G is restricted to $J(\cong N^*)$ then the E-convolution reduces to the usual number theoretic convolution which is multiplicative.

Remark 4.2.10. $\tau' = u \cdot u$.

Proof. We have

$$(u \cdot u)(G) = \sum_{\substack{D \times E = G \\ (D,E) \in \mathcal{G} \times \mathcal{G}}} u(D)u(E) = \tau'(G).$$

□

The following theorem is immediate from the above definition.

Theorem 4.2.11. *$\mathcal{A}(\mathcal{X})$ is a commutative ring with identity ε under the additive and the multiplicative operations given respectively by ordinary function addition and E-convolution of funcitons.*

Proof. If $f, g, h \in \mathcal{A}(\mathcal{X})$, then

$$(f \cdot (g \cdot h))(G) = ((f \cdot g) \cdot h)(G) = \sum_{L \times M \times N = G} f(L)g(M)h(N),$$

where the summation is over all ordered triples $(L, M, N) \in \mathcal{G} \times \mathcal{G} \times \mathcal{G}$ such that $L \times M \times N = G$. The associative law for multiplication is thus established. The other ring properties can be easily verified. □

Now we give the definition of *D-convolution* of two functions in $\mathcal{A}(\mathcal{X})$ and study some properties of this convolution.

Definition 4.2.12. If f and g are any two functions in $\mathcal{A}(\mathcal{X})$ the *D-convolution* of f, g is defined to be the function $f \odot g \in \mathcal{A}(\mathcal{X})$ given by

$$(f \odot g)(G) = \sum_{H \leq G} f(H)g(G/H).$$

Lemma 4.2.13. *Suppose* $f, g \in \mathcal{A}(\mathcal{X})$. *Then* $f \odot g = g \odot f$, *i.e., D-convolution of functions is commutative.*

The following proposition is important to prove the lemma.

Proposition 4.2.14. *Let* H *be a subgroup of a finite abelian group* G *and* $H^{\perp} = \{\chi \in \widehat{G} \mid \chi(H) = \{1\}\}$, *where* $\widehat{G} = \mathrm{Hom}(G, \mathbb{C}^*)$. *Then*

(i) $\widehat{G/H} \cong H^{\perp}$,

(ii) $\widehat{G}/H^{\perp} \cong \widehat{H}$.

Proof.

$$\text{Define } \phi : \widehat{G/H} \longrightarrow H^{\perp} \text{ given by } \phi(f) = \chi, \text{ where}$$

$$\chi : G \longrightarrow C^* \text{ given by } \chi(g) = f(gH) \ \forall\, g \in G.$$

Clearly ϕ is well defined. Again let $\chi_1, \chi_2 \in H^\perp$. Then $\chi_1(g) = f_1(gH)$ and $\chi_2(g) = f_2(gH)$ for some $f_1, f_2 \in \widehat{G/H}$. Now

$$\begin{aligned} & \chi_1 = \chi_2 \\ \Longrightarrow \quad & \chi_1(g) = \chi_2(g) \quad \forall\, g \in G \\ \Longrightarrow \quad & f_1(gH) = f_2(gH) \quad \forall\, gH \in G/H \\ \Longrightarrow \quad & f_1 = f_2. \end{aligned}$$

Therefore ϕ is one one. Moreover given any $\chi \in H^\perp$ we can define a function $f \in \widehat{G/H}$ given by $f(gH) = \chi(g) \quad \forall\, gH \in G/H$. Thus ϕ is onto. Again let $f_1, f_2 \in \widehat{G/H}$. Then $f_1(gH) = \chi_1(g)$ and $f_2(gH) = \chi_2(g)$ for some $\chi_1, \chi_2 \in \widehat{G}$. Therefore $(f_1 f_2)(gH) = (\chi_1\chi_2)(g)$. Which implies $\phi(f_1 f_2) = \chi_1\chi_2 = \phi(f_1)\phi(f_2)$, i.e., ϕ is a homomorphism. This proves part (i).

For part (ii), consider $\lambda : \widehat{G} \longrightarrow \widehat{H}$ given by $\lambda(\chi) = \chi_{|H}$. Clearly this map is onto. Moreover $\lambda(\chi_1\chi_2) = (\chi_1\chi_2)_{|H} = \chi_{1|H}\chi_{2|H} = \lambda(\chi_1)\lambda(\chi_2)$. Again if I_H is the identity element of $\widehat{H}$ then $\mathrm{Ker}(\lambda) = \{\chi \in \widehat{G} : \lambda(\chi) = I_H\} = \{\chi \in \widehat{G} : \chi_{|H} = I_H\} = H^\perp$. Therefore by First isomorphism Theorem 1.2.1, we have $\widehat{G}/H^\perp \cong \widehat{H}$.

□

Proof of the lemma :

For $f, g \in \mathcal{A}(\mathcal{X})$ and $G \in \mathcal{X}$, we have

$$(f \odot g)(G) = \sum_{H \leq G} f(H) g(G/H)$$

$$= \sum_{H \leq G} f(\widehat{G}/H^{\perp}) g(H^{\perp})$$
$$= \sum_{H^{\perp} \leq \widehat{G}} g(H^{\perp}) f(\widehat{G}/H^{\perp})$$
$$= (g \odot f)(\widehat{G}) = (g \odot f)(G),$$

noting that for any finite abelian group G, $\widehat{G} \cong G$ (Lemma 1.6.22) and H can be replaced by $H^{\perp}$ because $\perp$ is a one to one correspondence between the set of subgroups of G and the set of subgroups of $\widehat{G}$ ([12], page 30).

Lemma 4.2.15. *Suppose $f, g, h \in \mathcal{A}(\mathcal{X})$. Then $f \odot (g \odot h) = (f \odot g) \odot h$, i.e., D-convolution of functions is associative.*

Proof. For $f, g, h \in \mathcal{A}(\mathcal{X})$ and $G \in \mathcal{X}$, we have

$$\begin{aligned}
(f \odot (g \odot h))(G) &= \sum_{H \leq G} f(H)(g \odot h)(G/H) \\
&= \sum_{H \leq G} f(H) \left(\sum_{K' \leq G/H} g(K') h\left(\frac{G/H}{K'}\right) \right) \\
&= \sum_{H \leq G} f(H) \left(\sum_{K/H \leq G/H} g(K/H) h\left(\frac{G/H}{K/H}\right) \right) \\
&= \sum_{H \leq G} f(H) \left(\sum_{H \leq K \leq G} g(K/H) h\left(G/K\right) \right) \\
&= \sum_{K \leq G} \left(\sum_{H \leq K} f(H) g(K/H) \right) h(G/K) \\
&= \sum_{K \leq G} (f \odot g)(K) h(G/K) \\
&= ((f \odot g) \odot h)(G).
\end{aligned}$$

Hence

$$f \odot (g \odot h) = (f \odot g) \odot h.$$

□

As a consecuence of the above results we can make the following theorem.

Theorem 4.2.16. *$\mathcal{A}(\mathcal{X})$ is a commutative ring with identity ϵ under the additive and the multiplicative operations given respectively by ordinary function addition and D-convolution of funcitons.*

4.3 Coprime groups and multiplicative functions

Definition 4.3.1. The groups $G_1, G_2 \in \mathcal{G}$ are said to be *coprime* or *relatively prime* if $\mathcal{C}(G_1)$ and $\mathcal{C}(G_2)$ have no member (i.e., composition factor) in common. For example the *alternating groups* A_5 and A_6 are coprime.

Definition 4.3.2. The groups $G_1, G_2 \in \mathcal{G}$ are said to be *almost coprime* if $\mathcal{C}(G_1)$ and $\mathcal{C}(G_2)$ have no abelian member (i.e., composition factor) in common.

In view of the above definition we get the following:

Theorem 4.3.3. *If the groups G_1 and G_2 have coprime orders, then they will be coprime.*

Proof. Let the groups G_1 and G_2 have coprime orders. Suppose $X(\neq E_0) \in \mathcal{C}(G_1) \cap \mathcal{C}(G_2)$. Then $X \in \mathcal{C}(G_1)$ and $X \in \mathcal{C}(G_2)$. Which implies $|X| \mid |G_1|$

and $|X| \mid |G_2|$. Which is a contradiction to our hypothesis that orders of G_1 and G_2 are coprime. Therefore the groups G_1 and G_2 are coprime. □

The converse of the above proposition is not true. For example the *alternating groups* A_5 and A_6 are coprime but they do not have coprime orders. But if the groups G_1 and G_2 are abelian and coprime, then the converse of the above proposition is true.

Theorem 4.3.4. *If the groups G_1 and G_2 are abelian and coprime, then they have coprime orders.*

Proof. Suppose gcd $(|G_1|, |G_2|) \neq 1$. Then there exists some prime p such that $p \mid |G_1|$ and $p \mid |G_2|$.
By Cauchy's Theorem 1.3.5,

there exists $g_1 \in G_1$ and $g_2 \in G_2$ such that $o(g_1) = o(g_2) = p$.

Now consider the subgroups $< g_1 >$ and $< g_2 >$ of G_1 and G_2 respectively. Then $< g_1 > \lhd G_1$ and $< g_2 > \lhd G_2$, since G is abelian, and $|< g_1 >| = |< g_2 >| = p$.

Now by Theorem 4.2.1

$$\mathcal{C}(G_1) = \mathcal{C}(G_1/ < g_1 >) \sqcup \mathcal{C}(< g_1 >).$$

and

$$\mathcal{C}(G_2) = \mathcal{C}(G_2/ < g_2 >) \sqcup \mathcal{C}(< g_2 >).$$

But $< g_1 > \cong < g_2 >$, being cyclic group of same order. Therefore

$$\mathcal{C}(< g_1 >) = \mathcal{C}(< g_2 >) \ \ i.e., \ \ \mathcal{C}(G_1) \cap \mathcal{C}(G_2) \neq \phi,$$

a contradiction, since G_1 and G_2 are coprime. Hence G_1 and G_2 have coprime orders. □

Definition 4.3.5. A function $f \in \mathcal{A}(\mathcal{G})$ which is not identically zero will be called *multiplicative* if we have

$$f(G_1 \times G_2) = f(G_1)f(G_2)$$

whenever $G_1, G_2 \in \mathcal{G}$ are coprime.

Definition 4.3.6. A function $f \in \mathcal{A}(\mathcal{G})$ which is not identically zero will be called *completely multiplicative* if we have

$$f(G_1 \times G_2) = f(G_1)f(G_2)$$

for all $G_1, G_2 \in \mathcal{G}$.

Definition 4.3.7. A function $f \in \mathcal{A}(\mathcal{G})$ which is not identically zero will be called *almost completely multiplicative* if we have

$$f(G_1 \times G_2) = f(G_1)f(G_2)$$

whenever $G_1, G_2 \in \mathcal{G}$ are almost coprime.

Remark 4.3.8. We have

(i) $f(E_0) = 1$ if f satisfies any of the multiplicativity conditions.

(ii) $|\ |$, u and ε are all completely multiplicative functions.

Returning back to abelian groups we have the following definitions.

Definition 4.3.9. The *greatest common direct factor* gcd (G_1, G_2) of two groups $G_1, G_2 \in \mathcal{X}$ is defined to be the group of maximal order in $\mathcal{X}$ which is a direct factor of both G_1 and G_2.

Definition 4.3.10. The groups $G_1, G_2 \in \mathcal{X}$ are said to be *E-coprime* if gcd $(G_1, G_2) = E_0$.

Definition 4.3.11. Let $f \in \mathcal{A}(\mathcal{X})$ be such that $f(E_0) = 1$. Then f will be called *E-multiplicative* if we have

$$f(G_1 \times G_2) = f(G_1)f(G_2)$$

for all $G_1, G_2 \in \mathcal{X}$ such that gcd $(G_1, G_2) = E_0$.

Definition 4.3.12. Let $f \in \mathcal{A}(\mathcal{X})$ be such that $f(E_0) = 1$. Then f will be called *totally E-multiplicative* if we have

$$f(G_1 \times G_2) = f(G_1)f(G_2)$$

for all $G_1, G_2 \in \mathcal{X}$.

Remark 4.3.13. If $f(G)$ is *E-multiplicative* , then it is completely determined by the values for $G = P^k$, where $k = 1, 2, \ldots$ and P ranges over indecomposable groups of $\mathcal{X}$.

Remark 4.3.14. If G is restricted to J, then since $N^* \cong J$, the above defination becomes equivalent to the usual usual number theoretic defination of a *multiplicative* function.

Remark 4.3.15. The functions $|\ |$ and ε are both *totally E-multiplicative* and hence *E-multiplicative.*

As a consequence of Theorem 4.2.11, we have the following corollary.

Corollary 4.3.16. *The set of E-multiplicative functions is a sub-semigroup with identity ε of the E-multiplicative semigroup of $\mathcal{A}(\mathcal{X})$.*

Proof. Let S be the collection of all E-multiplicative functions in $\mathcal{A}(\mathcal{X})$. To prove the result it is enough to show that if $f_1 \in S$, $f_2 \in S$, then $f = f_1 \cdot f_2 \in S$. Certainly, $f_1(E_0) = f_2(E_0) = 1$ implies that $f(E_0) = 1$. Suppose now that $G = G_1 \times G_2$, gcd $(G_1, G_2) = E_0$. If D, E is any pair of groups in $\mathcal{X}$ such that $D \times E = G$ then by the Basis Theorem 1.3.6, D and E have unique decompositions, $D = D_1 \times D_2$, $E = E_1 \times E_2$ such that $D_1 \times E_1 = G_1$, $D_2 \times E_2 = G_2$. Hence gcd $(D_1, D_2) =$ gcd $(E_1, E_2) = E_0$. Therefore noting that $f_1, f_2 \in S$, we get

$$\begin{aligned}
f(G_1 \times G_2) &= \sum_{\substack{D_1 \times E_1 = G_1 \\ D_2 \times E_2 = G_2}} f_1(D_1 \times D_2) f_2(E_1 \times E_2) \\
&= \sum_{\substack{D_1 \times E_1 = G_1 \\ D_2 \times E_2 = G_2}} f_1(D_1) f_1(D_2) f_2(E_1) f_2(E_2) \\
&= \sum_{D_1 \times E_1 = G_1} f_1(D_1) f_2(E_1) \sum_{D_2 \times E_2 = G_2} f_1(D_2) f_2(E_2) \\
&= (f_1 \cdot f_2)(G_1)(f_1 \cdot f_2)(G_2) \\
&= f(G_1) f(G_2).
\end{aligned}$$

Therefore $f \in S$. Again ε is the identity in S. □

Definition 4.3.17. The groups $G_1, G_2 \in \mathcal{X}$ are said to be *D-coprime* if their orders are coprime i.e., if gcd $(|G_1|, |G_2|) = 1$.

Definition 4.3.18. Let $f \in \mathcal{A}(\mathcal{X})$ be such that $f(E_0) = 1$. Then f will be called *D-multiplicative* if we have

$$f(G_1 \times G_2) = f(G_1)f(G_2)$$

whenever $G_1, G_2 \in \mathcal{X}$ are D-coprime.

Note 4.3.19. The functions $|\ |$, u and ε are D-multiplicative.

4.4 Some results on arithmetic functions of $\mathcal{A}(\mathcal{G})$

Consider the factorization map $\rho : \mathcal{G} \longrightarrow \mathcal{G}$ given by $\rho(G) = \Pi\mathcal{C}(G)$ where $G \in \mathcal{G}$. By Jordan-Hölder Theorem, ρ is well-defined.

Theorem 4.4.1. *ρ is a monoid homomorphism.*

Proof. Let $G_1, G_2 \in \mathcal{G}$. Now in view of Corollary 4.2.2, we have

$\rho(G_1 \times G_2) = \Pi\mathcal{C}(G_1 \times G_2) = \Pi(\mathcal{C}(G_1) \sqcup \mathcal{C}(G_2)) = (\Pi\mathcal{C}(G_1)) \times (\Pi\mathcal{C}(G_2))$
$= \rho(G_1) \times \rho(G_2)$. □

Theorem 4.4.2. *$\rho(G) = G$ if and only if G is completely reducible in $\mathcal{G}$.*

Proof. Suppose $\rho(G) = G$. Then G is completely reducible as $\rho(G) = \Pi\mathcal{C}(G)$ is completely reducible.
Conversly suppose G is completely reducible. Then

$$G = E_0 \text{ or } G = G_1 \times G_2 \times G_3 \times \cdots \times G_n,$$

where G_i's are simple (not necessarily distinct).

Now

$$\begin{aligned}\rho(G) &= \rho(G_1 \times G_2 \times G_3 \times \cdots \times G_n) \\ &= \rho(G_1) \times \rho(G_2) \times \rho(G_3) \times \cdots \times \rho(G_n) \\ &= G_1 \times G_2 \times G_3 \times \cdots \times G_n = G.\end{aligned}$$

□

Note 4.4.3. On the completely reducible groups the convolution '$*$' coincides with the *E-convolution* which is multiplicative.

Theorem 4.4.4. *If G_1 and G_2 are coprime, then $\rho(G_1)$ and $\rho(G_2)$ are also coprime.*

Proof. Suppose there exists some $K \in \mathcal{G}$ such that

$$\begin{aligned} & K \in C(\rho(G_1)) \cap C(\rho(G_2)) \\ \Longrightarrow\ & K \in C(\rho(G_1)) \ \&\ K \in C(\rho(G)) \\ \Longrightarrow\ & K \text{ is a direct factor of } \rho(\rho(G_1)) = \rho(G_1) \\ & \ \&\ K \text{ is a direct factor of } \rho(\rho(G_2)) = \rho(G_2) \\ \Longrightarrow\ & K \in C(G_1) \cap C(G_2), \end{aligned}$$

a contradiction. Hence $\rho(G_1)$ and $\rho(G_2)$ are coprime. □

In general, the convolution of two multiplicative functions in $\mathcal{A}(\mathcal{G})$ is not multiplicative. But using the fact that if G_1, G_2 are completely reducible then $G_1 \times G_2$ is also completely reducible, we make the following:

Lemma 4.4.5. *If the groups $G_1, G_2 \in \mathcal{G}$ are coprime as well as completely reducible, then*

$$(f * g)(G_1 \times G_2) = (f * g)(G_1)(f * g)(G_2);$$

when f and g are multiplicative.

Here we mention some important relations between an arithmetic function and the factorization map ρ.

Theorem 4.4.6. *If $f \in \mathcal{A}(\mathcal{G})$ is multiplicative then $f \circ \rho \in \mathcal{A}(\mathcal{G})$ is also multiplicative.*

Proof. Let $G_1, G_2 \in \mathcal{G}$ be coprime. Then by Theorem 4.4.4, $\rho(G_1)$ and $\rho(G_2)$ are also coprime. Now
$(f \circ \rho)(G_1 \times G_2) = f(\rho(G_1 \times G_2)) = f(\rho(G_1) \times \rho(G_2)) = f(\rho(G_1))f(\rho(G_2))$
$= (f \circ \rho)(G_1)(f \circ \rho)(G_2)$. □

Theorem 4.4.7. *If $f, g \in \mathcal{A}(\mathcal{G})$ are multiplicative then $(f * g) \circ \rho \in \mathcal{A}(\mathcal{G})$ is also multiplicative.*

Proof. Let $G_1, G_2 \in \mathcal{G}$ be coprime.
Now

$$\begin{aligned}((f * g) \circ \rho)(G_1 \times G_2) &= (f * g)(\rho(G_1 \times G_2)) \\ &= (f * g)(\rho(G_1) \times \rho(G_2)) \\ &= (f * g)(\rho(G_1))(f * g)(\rho(G_2)) \\ &= ((f * g) \circ \rho)(G_1)((f * g) \circ \rho)(G_2);\end{aligned}$$

noting that $\rho(G_1), \rho(G_2)$ are coprime as well as completely reducible. Thus $f * g$ is multiplicative. □

Theorem 4.4.8. *If $f, g \in \mathcal{A}(\mathcal{G})$ then $(f * g) \circ \rho = (f \circ \rho) * (g \circ \rho)$.*

Proof. We have

$$((f * g) \circ \rho)(G)$$
$$= (f * g)(\rho(G))$$
$$= f(\rho(G))g(E_0) + f(E_0)g(\rho(G)) + \sum_{\substack{(H,K)\in\mathcal{G}\times\mathcal{G} \\ H\times K=\rho(\rho(G))=\rho(G)}} f(H)g(K).$$

Again

$$((f \circ \rho) * (g \circ \rho))(G)$$
$$= (f\circ\rho)(G)(g\circ\rho)(E_0)+(f\circ\rho)(E_0)(g\circ\rho)(G)+\sum_{\substack{(H\prime,K\prime)\in\mathcal{G}\times\mathcal{G} \\ H\prime\times K\prime=\rho(G)}}(f\circ\rho)(H\prime)(g\circ\rho)(K\prime)$$
$$= f(\rho(G))g(E_0) + f(E_0)g(\rho(G)) + \sum_{\substack{(\rho(H\prime),\rho(K\prime)\in\mathcal{G}\times\mathcal{G} \\ \rho(H\prime)\times\rho(K\prime)=\rho(G)}} f(\rho(H\prime))g(\rho(K\prime))$$
$$= f(\rho(G))g(E_0) + f(E_0)g(\rho(G)) + \sum_{\substack{(H,K)\in\mathcal{G}\times\mathcal{G} \\ H\times K=\rho(G)}} f(H)g(K). \qquad \square$$

Corollary 4.4.9. *ρ induces a unitary ring homomorphism of $\mathcal{A}(\mathcal{G})$ into itself given by $f \longmapsto f \circ \rho$ where $f \in \mathcal{A}(\mathcal{G})$.*

Proof. Let $h : \mathcal{A}(\mathcal{G}) \longrightarrow \mathcal{A}(\mathcal{G})$ be given by $f \longmapsto f \circ \rho$.

Clearly h is well defined. Now,

$$h(f * g) = (f * g) \circ \rho = (f \circ \rho) * (g \circ \rho) = h(f) * h(g).$$

$\square$

Theorem 4.4.10. *If $f \in \mathcal{A}(\mathcal{G})$ with $f(E_0) \neq 0$ then there is a unique $g \in \mathcal{A}(\mathcal{G})$ such that $f * g = g * f = \varepsilon$.*

Proof. Given $G \in \mathcal{G}$. Suppose $|G| = 1$ i.e., $G = E_0$. We can calculate $g(G)$ from

$$1 = \varepsilon(G) = (f * g)(G) = f(E_0)g(E_0).$$

Next suppose $|G| = 2$. We can calculate $g(G)$ from

$$0 = \varepsilon(G) = (f * g)(G) = f(G)g(E_0) + f(E_0)g(G).$$

Continuing by mathematical induction we see that if $g(G)$ has been evaluated for groups of orders $j = 1, 2, \ldots, n-1$, then $g(G)$ is determined by

$$0 = \varepsilon(G) = (f * g)(G) = f(G)g(E_0) + f(E_0)g(G) + \sum_{\substack{(H,K)\in\mathcal{G}\times\mathcal{G} \\ H\times K=\Pi C(G)}} f(H)g(K);$$

noting that this equation contains $g(G)$ only in the term $f(E_0)g(G)$, and so can be solved to give a unique value for $g(G)$. □

As an immediate consequence of the avove theorem we have the following:

Corollary 4.4.11. *The set of all functions $f \in \mathcal{A}(\mathcal{G})$ with $f(E_0) \neq 0$ forms an abelian group under the operation given by convolution.*

Proof. Let $\mathcal{A}'(\mathcal{G}) = \{f \in \mathcal{A}(\mathcal{G}) : f(E_0) \neq 0\}$. Suppose $f, g \in \mathcal{A}'(\mathcal{G})$. Now

$$(f * g)(E_0) = f(E_0)g(E_0) \neq 0$$

and so $(f * g) \in \mathcal{A}'(\mathcal{G})$. Again we have by the above theorem if $f \in \mathcal{A}'(\mathcal{G})$ then $f^{-1} \in \mathcal{A}(\mathcal{G})$. Suppose $f^{-1}(E_0) = 0$. Then

$$(f * f^{-1})(E_0) = f(E_0)f^{-1}(E_0) = 0$$

i.e., $\varepsilon(E_0) = 0$, contradiction. Therefore $f^{-1}(E_0) \neq 0$. i.e., $f^{-1} \in \mathcal{A}'(\mathcal{G})$. We know that $(\mathcal{A}(\mathcal{G}), +, *)$ is a commutative ring with identity ε. Therefore $*$ is 'associative' and 'commutative' in $\mathcal{A}'(\mathcal{G})$. Hence $(\mathcal{A}'(\mathcal{G}), *)$ is an abelian group. □

Theorem 4.4.12. *If $f, g \in \mathcal{A}(\mathcal{G})$ are such that $f \circ \rho$ and $(f * g) \circ \rho$ are multiplicative then $g \circ \rho$ is also multiplicative.*

Proof. Let $G_1, G_2 \in \mathcal{G}$ be any two coprime groups. We shall use induction on the direct factors of $\rho(G_1)$ and $\rho(G_2)$ to prove that

$$(g \circ \rho)(G_1 \times G_2) = (g \circ \rho)(G_1)(g \circ \rho)(G_2).$$

We have E_0 is a direct factor of both $\rho(G_1)$ and $\rho(G_2)$. Now

$$\begin{aligned}
(g \circ \rho)(E_0 \times E_0) &= (g \circ \rho)(E_0) \\
&= ((\varepsilon * g) \circ \rho)(E_0) \\
&= (\varepsilon \circ \rho)(E_0) * (g \circ \rho)(E_0), \quad \text{by Theorem 4.4.8} \\
&= \varepsilon(\rho(E_0)) * (g \circ \rho)(E_0) \\
&= \varepsilon(E_0) * (g \circ \rho)(E_0) \\
&= (f \circ \rho)(E_0) * (g \circ \rho)(E_0) \\
&= ((f * g) \circ \rho)(E_0) \\
&= 1,
\end{aligned}$$

and so, as the induction hypothesis, we assume that for each direct factor K_1 of $\rho(G_1) = \Pi(G_1)$ and for each direct factor K_2 of $\rho(G_2) = \Pi(G_2)$ with

$K_1 \times K_2 \neq \rho(G_1) \times \rho(G_2)$ we have

$$(g \circ \rho)(K_1 \times K_2) = (g \circ \rho)(K_1)(g \circ \rho)(K_2)$$

$$i.e., \quad g(\rho(K_1 \times K_2)) = g(\rho(K_1))g(\rho(K_2))$$

$$i.e., \quad g(K_1 \times K_2) = g(K_1)g(K_2).$$

Then, since $(f * g) \circ \rho$ is multiplicative, we have

$$((f * g) \circ \rho)(G_1 \times G_2) = ((f * g) \circ \rho)(G_1)\ ((f * g) \circ \rho)(G_2)$$

$$\Longrightarrow \quad (f * g)(\rho(G_1) \times \rho(G_2)) \ = \ (f * g)(\rho(G_1))\ (f * g)(\rho(G_2))$$

$$\Longrightarrow \quad \sum_{\substack{(H,K)\in\mathcal{G}\times\mathcal{G} \\ H\times K=\rho(G_1)\times\rho(G_2)}} f(H)g(K)$$

$$= \left(\sum_{\substack{(H_1,K_1)\in\mathcal{G}\times\mathcal{G} \\ H_1\times K_1=\rho(G_1)}} f(H_1)g(K_1) \right) \left(\sum_{\substack{(H_2,K_2)\in\mathcal{G}\times\mathcal{G} \\ H_2\times K_2=\rho(G_2)}} f(H_2)g(K_2) \right)$$

$$\Longrightarrow \quad \sum_{\substack{(H_1\times H_2,K_1\times K_2)\in\mathcal{G}\times\mathcal{G} \\ H_1\times H_2\times K_1\times K_2=\rho(G_1)\times\rho(G_2)}} f(H_1 \times H_2)g(K_1 \times K_2)$$

$$= \sum_{\substack{(H_1,K_1),(H_2,K_2)\in\mathcal{G}\times\mathcal{G} \\ H_1\times K_1=\rho(G_1),\ H_2\times K_2=\rho(G_2)}} f(H_1 \times H_2)g(K_1)g(K_2),$$

Therefore, using induction hypothesis, we have

$$g(\rho(G_1) \times \rho(G_2)) = g(\rho(G_1))g(\rho(G_2)).$$

This completes the proof. □

We can now make the following important corollary of the above theorem.

Corollary 4.4.13. *The set of all multiplicative functions in $\mathcal{A}(\mathcal{G})$ of the form $f \circ \rho$, where $f \in \mathcal{A}(\mathcal{G})$, is an abelian group under the operation given by convolution.*

Proof. Suppose
$A :=$ The set of all functions $f \in \mathcal{A}(\mathcal{G})$ with $f(E_0) \neq 0$. Then $(A, *)$ is an abelian group by Corollary 4.4.11. Again suppose
$A' :=$ The set of all multiplicative functions in $\mathcal{A}(\mathcal{G})$ of the form $f \circ \rho$ where $f \in \mathcal{A}(\mathcal{G})$. Clearly $A' \subseteq A$. We shall show that $A' \leq A$. Let $f \circ \rho$, $g \circ \rho \in A'$. Now

$$(f \circ \rho) * (g \circ \rho) = (f * g) \circ \rho,$$

which is multiplicative by Theorem 4.4.7. Therefore $(f \circ \rho) * (g \circ \rho) \in A'$. Again using Theorem 4.4.8 we have

$$(f \circ \rho) * (f^{-1} \circ \rho) = (f * f^{-1}) \circ \rho = \varepsilon \circ \rho = \varepsilon,$$

which is multiplicative. Therefore $(f \circ \rho)^{-1} = (f^{-1} \circ \rho)$, which is multiplicative by the above Theorem 4.4.12. Since $f^{-1} \in \mathcal{A}(\mathcal{G})$, therefore $(f^{-1} \circ \rho) \in A'$, i.e., $(f \circ \rho)^{-1} \in A'$. Hence $A' \leq A$. □

4.5 The Möbius Function

The *Möbius function*, which is one of the most useful examples of arithmetic functions of positive integers, is given by

$$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{if } \omega(n) = \Omega(n) \\ 0, & \text{otherwise} \end{cases}$$

where n is a positive integer, $\omega(n)$ is the number of distinct prime factors of n, and $\Omega(n)$ is the number of prime factors (counting multiplicity) of n.

4.5.1 Möbius function for finite groups (abelian and non abelian)

The group-theoretic analogues of ω, Ω and the Möbius function μ is defined as

$\omega(G)$ = number of distinct (i.e., non-isomorphic) factors in $\mathcal{C}(G)$,

$\Omega(G)$ = number of factors (counting multiplicity) in $\mathcal{C}(G)$, and

$$\mu(G) = \begin{cases} (-1)^{\omega(G)}, & \text{if } \omega(G) = \Omega(G) \\ 0, & \text{otherwise} \end{cases}$$

where $G \in \mathcal{G}$.

Clearly $\omega(E_0) = 0 = \Omega(E_0)$ and so $\mu(E_0) = 1$.

Remark 4.5.1. Taking $G = C_n$, we have

$$\omega(C_n) = \omega(n), \quad \Omega(C_n) = \Omega(n) \quad \text{and,} \quad \mu(C_n) = \mu(n)$$

because $C_n = C_{p_1{}^{r_1}} \times \cdots \times C_{p_k{}^{r_k}}$, where $p_1{}^{r_1}, \ldots, p_k{}^{r_k}$ is the standard prime factorization of n, and so $\mathcal{C}(C_n)$ consists of the simple groups C_{p_i}, each having multiplicity r_i, $1 \leq i \leq k$.

Theorem 4.5.2. *$\Omega(G_1 \times G_2) = \Omega(G_1) + \Omega(G_2)$ for all $G_1, G_2 \in \mathcal{G}$, and $\omega(G_1 \times G_2) = \omega(G_1) + \omega(G_2)$ if G_1 and G_2 are coprime.*

Proof. In view of Corollary 4.2.2, given $G_1, G_2 \in \mathcal{G}$, we know that $\mathcal{C}(G_1 \times G_2) = \mathcal{C}(G_1) \sqcup \mathcal{C}(G_2)$. Now

$$\begin{aligned}
\Omega(G_1 \times G_2) &= \text{number of factors in } \mathcal{C}(G_1 \times G_2) \\
&= \text{number of factors in } \mathcal{C}(G_1) \sqcup \mathcal{C}(G_2) \\
&= \text{number of factors in } \mathcal{C}(G_1) + \text{number of factors in } \mathcal{C}(G_2) \\
&= \Omega(G_1) + \Omega(G_2).
\end{aligned}$$

Again suppose G_1, G_2 are coprime, then $\mathcal{C}(G_1) \cap \mathcal{C}(G_2) = \phi$. Now,

$$\begin{aligned}
\omega(G_1 \times G_2) &= \text{number of distinct factors in } \mathcal{C}(G_1 \times G_2) \\
&= \text{number of distinct factors in } \mathcal{C}(G_1) \sqcup \mathcal{C}(G_2) \\
&= \text{number of distinct factors in } \mathcal{C}(G_1) \\
&\quad + \text{number of distinct factors in } \mathcal{C}(G_2) \\
&= \omega(G_1) + \omega(G_2).
\end{aligned}$$

□

Theorem 4.5.3. *The Möbius Function $\mu \in \mathcal{A}(\mathcal{G})$ is multiplicative.*

Proof. Let $G_1, G_2 \in \mathcal{G}$ be coprime.

Suppose $\omega(G_1) = \Omega(G_1)$ and $\omega(G_2) = \Omega(G_2)$. Then

$$\begin{aligned} & \omega(G_1) + \omega(G_2) = \Omega(G_1) + \Omega(G_2) \\ \Longrightarrow \quad & \omega(G_1 \times G_2) = \Omega(G_1 \times G_2). \end{aligned}$$

Now

$$\begin{aligned} \mu(G_1 \times G_2) = (-1)^{\omega(G_1 \times G_2)} = (-1)^{\omega(G_1)+\omega((G_2)} &= (-1)^{\omega(G_1)}(-1)^{\omega(G_2)} \\ &= \mu(G_1)\mu(G_2). \end{aligned}$$

Again suppose $\omega(G_1) \neq \Omega(G_1)$ or $\omega(G_2) \neq \Omega(G_2)$. Then

$$\begin{aligned} & \omega(G_1) + \omega(G_2) \neq \Omega(G_1) + \Omega(G_2) \\ \Longrightarrow \quad & \omega(G_1 \times G_2) \neq \Omega(G_1 \times G_2). \end{aligned}$$

Now

$$\mu(G_1 \times G_2) = 0 = \mu(G_1)\mu(G_2).$$

Thus μ is multiplicative. □

Proposition 4.5.4. *$\mu(P^k) = 0$ if P is simple and $k > 1$.*

Proof. If P is simple and $k > 1$, we have $\Omega(P^k) = k$. But since the groups P, P are not coprime therefore $\omega(P^k) \neq k$. Which follows the result. □

Theorem 4.5.5. *$\mu \circ \rho = \mu$ and $u \circ \rho = u$, where ρ is the factorization map.*

Proof. To show $\mu \circ \rho = \mu$. Suppose $C(G) = \{K_1, K_2, \ldots, K_n\}$. Each K_i is simple and so $C(K_i) = K_i$, $i = 1, 2, \ldots, n$. Now $\rho(G) = K_1 \times K_2 \times \cdots \times K_n$.

Case I: Each K_i is distinct. In this case we have

$$\begin{aligned}(\mu \circ \rho)(G) = \mu(\rho(G)) &= \mu(K_1 \times K_2 \times \cdots \times K_n) \\ &= \mu(K_1)\mu(K_2)\ldots\mu(K_n) \\ &= (-1)^n = (-1)^{\omega(G)} = \mu(G).\end{aligned}$$

Case II: Each K_i is not distinct. In this case we have $\omega(G) \neq \Omega(G)$. Now

$$(\mu \circ \rho)(G) = \mu(\rho(G)) = 0 = \mu(G).$$

Noting that $\mu(P^k) = 0$ if P is simple and $k > 1$ a positive integer. Therefore $\mu \circ \rho = \mu$ in each case.

For the second part

$$(u \circ \rho)(G) = u(\rho(G)) = 1 = u(G). \text{ i.e., } u \circ \rho = u.$$

□

Theorem 4.5.6. *$\mu * u = u * \mu = \varepsilon$ i.e., $\mu^{-1} = u$ and $u^{-1} = \mu$.*

Proof. We have $\mu \circ \rho = \mu$ and $u \circ \rho = u$. Now μ is mulptiplicative and u is mulptiplicative. Therefore

$$\begin{aligned} & (\mu * u) \circ \rho \text{ is mulptiplicative, by Theorem 4.4.7} \\ \Longrightarrow\ & (\mu \circ \rho) * (u \circ \rho) \text{ is mulptiplicative, by Theorem 4.4.8} \\ \Longrightarrow\ & \mu * u \text{ is mulptiplicative.}\end{aligned}$$

Again for any $G \in \mathcal{G}$

$$(\mu * u)(G) = ((\mu * u) \circ \rho)(G) = (\mu * u)(\rho(G)) = (\mu * u)(\Pi C(G)).$$

Now, for $G \neq E_0$, $\Pi C(G)$ is a product of powers of distinct simple groups in $\mathcal{G}$. And for each simple group $P \in \mathcal{G}$, for each positive integer k,

$$\begin{aligned}(\mu * u)(P^k) &= \sum_{\substack{(H,L)\in\mathcal{G}\times\mathcal{G} \\ H\times L=P^k}} \mu(H)u(L) \\ &= \mu(E_0)u(P^k) + \mu(P)u(P^{k-1}) + \dots \\ &+ \mu(P^{k-1})u(P) + \mu(P^k)u(E_0) \\ &= \mu(E_0) + \mu(P) + \cdots + \mu(P^k) \\ &= 1 - 1 + 0 + \cdots + 0 = 0.\end{aligned}$$

By mulptiplicativity of $\mu * u$ it follows that

$$(\mu * u)(G) = (\mu * u)(\Pi C(G)) = 0 = \varepsilon(G),\ \forall G \in \mathcal{G}.$$

Therefore

$$\mu * u = u * \mu = \varepsilon \ \ i.e.,\ \ u^{-1} = \mu.$$

□

As an immediate consequence, we have the following analogue of the Möbius inversion formula.

Theorem 4.5.7. *For $f, g \in \mathcal{A}(\mathcal{G})$, $f = g * u \Longleftrightarrow g = f * \mu$.*

Proof. We have to simply 'multiply' the first equation on the right by μ to get the second, and the second equation on the right by u to get the first. □

An important example of a completely multiplicative function of positive integers is the *Liouville's* function given by

$$\lambda(n) = (-1)^{\Omega(n)}$$

where n is a positive integer. We define the group-theoretic analogues of λ as

$$\lambda(G) = (-1)^{\Omega(G)}$$

where $G \in \mathcal{G}$.

Theorem 4.5.8. *The Liouville's function $\lambda \in \mathcal{A}(\mathcal{G})$ is completely multiplicative.*

Proof. For any $G_1, G_2 \in \mathcal{G}$, we have

$$\begin{aligned}
\lambda(G_1 \times G_2) &= (-1)^{\Omega(G_1 \times G_2)} \\
&= (-1)^{\Omega(G_1)+\Omega(G_2)}, \text{ by Theorem 4.5.2} \\
&= (-1)^{\Omega(G_1}(-1)^{\Omega(G_2)} \\
&= \lambda(G_1)\lambda(G_2).
\end{aligned}$$

□

Theorem 4.5.9. *$\lambda \circ \rho = \lambda$ and $\mu^2 \circ \rho = \mu^2$ where ρ is the factorization map.*

Proof. To show $\lambda \circ \rho = \lambda$. Suppose $C(G) = \{K_1, K_2, \ldots, K_n\}$. Each K_i is simple and so $C(K_i) = K_i$, $i = 1, 2, \ldots, n$ and $\rho(G) = K_1 \times K_2 \times \cdots \times K_n$. Now

$$\begin{aligned}
(\lambda \circ \rho)(G) &= \lambda(\rho(G)) \\
&= \lambda(K_1 \times K_2 \times \cdots \times K_n) \\
&= \lambda(K_1)\lambda(K_2)\ldots\lambda(K_n) \\
&= (-1)^n = (-1)^{\Omega(G)} = \lambda(G).
\end{aligned}$$

i.e., $\lambda \circ \rho = \lambda$.

For the second part

$$\begin{aligned}(\mu^2 \circ \rho)(G) = \mu^2(\rho(G)) &= \mu(\rho(G))\mu(\rho(G)) \\ &= (\mu \circ \rho)(G)(\mu \circ \rho)(G) \\ &= \mu(G)\mu(G) = \mu^2(G), \quad \text{by Theorem 4.5.5.}\end{aligned}$$

i.e., $\mu^2 \circ \rho = \mu^2$. □

Theorem 4.5.10. $\lambda * \mu^2 = \mu^2 * \lambda = \varepsilon$ *i.e.,* $\lambda^{-1} = \mu^2$ *where* μ^2 *is the ordinary product of* μ *with itself.*

Proof. We have $\lambda \circ \rho = \lambda$ and $\mu^2 \circ \rho = \mu^2$. Now λ is mulptiplicative and μ^2 is mulptiplicative. Therefore

$$\begin{aligned} & (\lambda * \mu^2) \circ \rho \text{ is mulptiplicative} \\ \Longrightarrow\ & (\lambda \circ \rho) * (\mu^2 \circ \rho) \text{ is mulptiplicative, by Theorem 4.4.8} \\ \Longrightarrow\ & \lambda * \mu^2 \text{ is mulptiplicative.}\end{aligned}$$

Again for any $G \in \mathcal{G}$

$$\begin{aligned}(\lambda * \mu^2)(G) &= ((\lambda * \mu^2) \circ \rho)(G) \\ &= (\lambda * \mu^2)(\rho(G)) \\ &= (\lambda * \mu^2)(\Pi C(G)).\end{aligned}$$

Now, for $G \neq E_0$, $\Pi C(G)$ is a product of powers of distinct simple groups in

$\mathcal{G}$. And for each simple group $P \in \mathcal{G}$, for each positive integer k,

$$\begin{aligned}(\lambda * \mu^2)(P^k) &= \sum_{\substack{(H,L)\in\mathcal{G}\times\mathcal{G} \\ H\times L = P^k}} \lambda(H)\mu^2(K) \\ &= \lambda(E_0)\mu^2(P^k) + \lambda(P)\mu^2(P^{k-1}) + \dots \\ &+ \lambda(P^{k-1})\mu^2(P) + \lambda(P^k)\mu^2(E_0) \\ &= \lambda(P^k) + \lambda(P^{k-1}) \\ &= (-1)^k + (-1)^{k-1} \\ &= 0.\end{aligned}$$

By mulptiplicativity of $\lambda * \mu^2$ it follows that

$$(\lambda * \mu^2)(G) = (\lambda * \mu^2)(\Pi C(G)) = 0 = \varepsilon(G),\ \forall G \in \mathcal{G}.$$

Therefore

$$\lambda * \mu^2 = \mu^2 * \lambda = \varepsilon \quad i.e., \quad \lambda^{-1} = \mu^2.$$

□

Theorem 4.5.11. *For each $G \in \mathcal{G}$,*

$$(\lambda * u)(G) = (u * \lambda)(G) = \begin{cases} 1, & \text{if } \rho(G) = \rho(H \times H) \text{ for some } H \in \mathcal{G}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. We have

$$\begin{aligned}(\lambda * u)(P^k) &= \lambda(E_0) + \lambda(P) + \lambda(P^2) + \cdots + \lambda(P^k) \\ &= 1 - 1 + 1 - \cdots + (-1)^k = \begin{cases} 0, & \text{if } k \text{ is odd} \\ 1, & \text{if } k \text{ is even} \end{cases}\end{aligned}$$

for each simple group $P \in \mathcal{G}$, and for each positive integer k. Hence, it follows that if $G \in \mathcal{G}$ then $(\lambda * u)(G) = 0$ or 1 depending on whether there exists or does not exist a factor in $\mathcal{C}(G)$ having odd multiplicity. □

Theorem 4.5.12. *Let $f \in \mathcal{A}(\mathcal{G})$ be a mulptiplicative function such that $f = f \circ \rho$. Then f is completely multiplicative if and only if $f * (\mu f) = (\mu f) * f = \varepsilon$. i.e., $f^{-1} = \mu f$ where μf is the ordinary product of μ and f.*

Proof. In this proof $(H, K) \in \mathcal{G} \times \mathcal{G}$ such that none of H and K is E_0. Suppose f is completely multiplicative. Now for each $G \in \mathcal{G}$, we have

$$\begin{aligned}
(f * (\mu f))(G) &= f(G)(\mu f)(E_0) + f(E_0)(\mu f)(G) + \sum_{H \times K = \Pi C(G)} f(H)(\mu f)(K) \\
&= f(G) + \mu(G) f(G) + \sum_{H \times K = \Pi C(G)} f(H \times K)\mu(K) \\
&= f(G) + \mu(G) f(G) + \sum f(\Pi C(G))\mu(K) \\
&= f(G) + \mu(G) f(G) + \sum (f \circ \rho)(G)\mu(K) \\
&= f(G) + \mu(G) f(G) + f(G) \sum \mu(K) \\
&= f(G) + \mu(G) f(G) + f(G)\left((u * \mu)(G) - \mu(E_0) - \mu(G)\right) \\
&= f(G)(u * \mu)(G) \\
&= \varepsilon(G).
\end{aligned}$$

By Theorem 4.5.6; noting that $(f \circ \rho)(G) = f(G)$, $f(E_0) = 1$ and $\varepsilon(G) = 0$ for $G \neq E_0$.

Conversely, since f is mulptiplicative it is enough to show that $f(P^k) =$

$f(P)^k$ for each simple group P in $\mathcal{G}$ and for each positive integer k. Now,

$$\begin{aligned}(\mu f) * f = \varepsilon &\Longrightarrow ((\mu f) * f)(P^k) = 0 \\ &\Longrightarrow \mu(E_0)f(E_0)f(P^k) + \mu(P)f(P)f(P^{k-1}) = 0 \\ &\Longrightarrow f(P^k) = f(P)f(P^{k-1})\end{aligned}$$

and so, by iteration, $f(P^k) = f(P)^k$. This completes the proof. □

4.5.2 Möbius functions for finite abelian groups

In this subsection we shall study E-Möbius function and D-Möbius function for any group $G \in \mathcal{X}$ and some related results. We begin with the following theorem:

Theorem 4.5.13. *There exists a unique function $\tilde{\mu}(G)$ satisfying the relation*

$$\sum_{D \times E = G} \tilde{\mu}(D) = \varepsilon(G). \tag{4.5.a}$$

This function is E-multiplicative and determined by

$$\tilde{\mu}(E_0) = 1, \quad \tilde{\mu}(P^k) = \begin{cases} -1, & \text{if } k = 1 \\ 0, & \text{if } k > 1, \end{cases}$$

where P is an indecomposible group in $\mathcal{X}$.

Proof. If there exists such a function, it must be unique, because

$$\begin{aligned}(\tilde{\mu} \cdot u)(G) &= \sum_{D \times E = G} \tilde{\mu}(D)u(E) = \varepsilon(G) \\ \Longrightarrow \quad \tilde{\mu} \cdot u &= \varepsilon\end{aligned}$$

i.e., $\tilde{\mu}$ is the multiplicative inverse of u in the ring $\mathcal{A}(\mathcal{X})$ and hence unique.

We now show that a function is actually determined by (4.5.a). If there exists such a function, then

$$(\tilde{\mu} \cdot u)(E_0) = \sum_{D \times E = E_0} \tilde{\mu}(D)u(E) = \varepsilon(E_0)$$

$$\Longrightarrow \quad \tilde{\mu}(E_0) = 1.$$

If P is indecomposible, then P is a cyclic group with order a power of a prime. Now

$$(\tilde{\mu} \cdot u)(P) = \sum_{D \times E = P} \tilde{\mu}(D)u(E) = \varepsilon(P)$$

$$\Longrightarrow \quad \tilde{\mu}(P) = -1.$$

Again,

$$(\tilde{\mu} \cdot u)(P^2) = \sum_{D \times E = P^2} \tilde{\mu}(D)u(E) = \varepsilon(P^2)$$

$$\Longrightarrow \quad -1 + 1 + \tilde{\mu}(P^2) = 0$$

$$\Longrightarrow \quad \tilde{\mu}(P^2) = o,$$

and hence by induction

$$\tilde{\mu}(P^k) = 0 \text{ for all } k \geq 2.$$

Thus if $G = E_o$ or the power of an indecomposible group P, then (4.5.a) is satisfied, provided

$$\tilde{\mu}(E_0) = 1, \quad \tilde{\mu}(P^k) = \begin{cases} -1, & \text{if } k = 1, \\ 0, & \text{if } k > 1. \end{cases} \tag{4.5.b}$$

The conditions (4.5.b) determine a unique E-multiplicative function $\tilde{\mu}(G)$, by Remark 4.3.13. This function (i.e., $\tilde{\mu}$) satisfies (4.5.a) for all $G \in \mathcal{X}$; because, if we put

$$T(G) = \sum_{D \times E = G} \tilde{\mu}(D), \quad G \in \mathcal{X}, \tag{4.5.c}$$

then $T = \tilde{\mu} \cdot u$, which is E-multiplicative by Cor 4.3.16. But ε is also E-multiplicative, and therefore, since the relation

$$T(G) = \varepsilon(G),$$

holds for groups of the form $G = P^k$, by Remark 4.3.13 it must be valid for all $G \in \mathcal{X}$. □

As an immediate consequence, we have the following analogue of the Möbius inversion formula.

Theorem 4.5.14. *For functions $f_1(G), f_2(G)$ of $\mathcal{A}(\mathcal{X})$*

$$f_1(G) = \sum_{D \times E = G} f_2(D) \text{ if and only if } f_2(G) = \sum_{D \times E = G} \tilde{\mu}(D) f_1(E).$$

Proof. In the commutative ring $\mathcal{A}(\mathcal{G})$, by (4.5.a), we have

$$\tilde{\mu} \cdot u = \varepsilon.$$

Now

$$f_1 = f_2 \cdot u \implies \tilde{\mu} \cdot f_1 = \tilde{\mu} \cdot (f_2 \cdot u) = f_2 \cdot (\tilde{\mu} \cdot u) = f_2 \cdot \varepsilon = f_2. \tag{4.5.d}$$

Again

$$f_2 = \tilde{\mu} \cdot f_1 \implies f_2 \cdot u = (\tilde{\mu} \cdot f_1) \cdot u = f_1 \cdot (\tilde{\mu} \cdot u) = f_1 \cdot \varepsilon = f_1. \tag{4.5.e}$$

Equations (4.5.d) and (4.5.e) gives the result. □

The following corollary is immediate.

Corollary 4.5.15. *If $f_1(G)$ is an arbitrary function of $\mathcal{A}(\mathcal{X})$, then there exists a uniquely determined function $f_2(G)$ such that*

$$f_1(G) = \sum_{D \times E = G} f_2(D).$$

Theorem 4.5.13 has the following corollaries.

Corollary 4.5.16. *If $G = {P_1}^{e_1} \times {P_2}^{e_2} \times \cdots \times {P_r}^{e_r}$, where $P_1, P_2, \ldots, P_r$ are distinct and indecomposible, then the function $\tilde{\mu}(G)$ defined by the theorem has the following evaluation:*

$$\tilde{\mu}(G) = \begin{cases} (-1)^r, & \text{if } G = P_1 \times P_2 \times \cdots \times P_r, \\ 0, & \text{otherwise.} \end{cases}$$

Corollary 4.5.17. *In case $G \in J(\cong N^*)$, the collection of all completely reducible groups of $\mathcal{X}$, then G is of the type*

$$G = {\mathbb{Z}_{p_1}}^{n_1} \times {\mathbb{Z}_{p_2}}^{n_2} \times \cdots \times {\mathbb{Z}_{p_k}}^{n_k},$$

where $p_1, p_2, \ldots, p_r$ are distinct primes. In this case

$$\tilde{\mu}(G) = \begin{cases} (-1)^k, & \text{if } n_1 = n_2 = \cdots = n_k = 1, \\ 0, & \text{otherwise.} \end{cases}$$

i.e., If $G \in J$, then $\tilde{\mu}(G)$ reduces to the ordinary Möbius function.

Let $U = \mathcal{X}_s$ be a semigroup of $\mathcal{X}$ containing E_0 and generated by a set s of indecomposible groups of $\mathcal{X}$. If s is the set of all indecomposible groups of $\mathcal{X}$, then $U = \mathcal{X}_s = \mathcal{X}$. Again if s is the set of all irreducible groups of $\mathcal{X}$, then $U = \mathcal{X}_s = J$, where J is the set of all completely reducible groups.

Definition 4.5.18. The *enumerative totient* $\varphi(G)$ is defined to be the number of groups $H \in \mathcal{X}$ such that H is of order $\leq |G|$ and E-coprime to G.

Definition 4.5.19. The generalized *totient* $\varphi_U(G)$ is defined to be the number of groups in U of order $\leq |G|$ and E-coprime to G. Clearly

$$\varphi_{\mathcal{X}}(G) = \varphi(G).$$

If $G \in J$ then $\varphi_J(G)$ reduces to the ordinary Euler φ-function (since $J \cong N^*$).

Definition 4.5.20. The U-grade of G, $A_U(G)$ is defined to be the total number of groups in U of order $\leq |G|$.

Remark 4.5.21. It follows from the above definition that

(i) $A_{\mathcal{X}}(G) = A(G)$.

(ii) $A_J(G) = |G|$, since $J \cong N^*$.

Remark 4.5.22. Since U is generated by indecomposible groups, it follows that $G_1 \times G_2 \in U \iff G_1, G_2 \in U$.

Theorem 4.5.23. $\varphi_U(G) = \sum_{D \times E = G} \mu_U^*(D) A_U(E)$, *where*

$$\mu_U^*(G) = \begin{cases} \tilde{\mu}(G), & \text{if } G \in U, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let $H, D, K \in \mathcal{G}$ and $H \in U$. We have by the defination of $\varphi_U(G)$ and $\varepsilon(G)$

$$\begin{aligned}
\varphi_U(G) &= \sum_{\substack{|H|\leq|G| \\ H\in U}} \varepsilon(\gcd(G,H)) \\
&= \sum_{\substack{|H|\leq|G| \\ H\in U}} \sum_{D\times K=(G,H)} \tilde{\mu}(D), \text{ by Theorem 4.5.13} \\
&= \sum_{\substack{|H|\leq|G| \\ H\in U}} \sum_{D\times H_1=H} \sum_{D\times E=G} \tilde{\mu}(D) \\
&= \sum_{D\times E=G} \tilde{\mu}(D) \sum_{\substack{D\times H_1=H \\ |H|\leq|G| \\ H\in U}} 1 \\
&= \sum_{\substack{D\times E=G \\ D\in U}} \tilde{\mu}(D) \sum_{\substack{|D\times H_1|\leq|G| \\ H_1\in U}} 1, \text{ by Remark 4.5.22.} \\
&= \sum_{\substack{D\times E=G \\ D\in U}} \tilde{\mu}(D) \sum_{\substack{|D||H_1|\leq|G| \\ H_1\in U}} 1 \\
&= \sum_{D\times E=G} \mu_U^*(D) \sum_{\substack{|H_1|\leq|E| \\ H_1\in U}} 1, \text{ by definition of } \mu_U^*(D). \\
&= \sum_{D\times E=G} \mu_U^*(D) A_U(E).
\end{aligned}$$

□

In view of Remark 4.5.21, we now have the following corolaries:

Corollary 4.5.24. *If $U = \mathcal{X}$, then $\varphi_{\mathcal{X}}(G) = \varphi(G) = \sum_{D\times E=G} \tilde{\mu}(D)A(E)$.*

Corollary 4.5.25. *If $U = J$, then $\varphi_J(G) = \sum_{D\times E=G} \mu_J^*(D)|E|$.*

Corollary 4.5.26. $\sum_{D\times E=G} \varphi(D) = A(G)$.

Proof. We have form Corollary 4.5.24

$$\varphi(G) = \sum_{D\times E=G} \tilde{\mu}(D)A(E)$$

Therefore by Theorem 4.5.14,

$$\sum_{D\times E=G} \varphi(G) = A(G).$$

□

Theorem 4.5.27. *The function φ_J is E-multiplicative.*

Proof. We know that the function $|\ |$ is E-multiplicative. Again by Theorem 4.5.13 μ_J^* is E-multiplicative. Therefore in view of Theorem 4.3.16, $\varphi_J = \mu_J{}^* \cdot |\ |$ is E-multiplicative. □

4.5.3 Partition function

In this section we study Partition function defined on positive integers and Zeta function of $\mathcal{X}$ and some results related to them.

Definition 4.5.28. For positive integer r, define

$P(r)$:= number of (unrestricted) partitions of r.

$E(r)$:= number of partitions of r into an even number of distinct parts.

$U(r)$:= number of partitions of r into an odd number of distinct parts.

As a convention we take $P(0) = E(0) = 1$ and $U(0) = 0$. Let $n > 0$ have the canonical factorization $n = \Pi p^r$ into powers of distinct primes p.

Define the functions a and ν given by $a(n) = \sum_{|G|=n} u(G)$ and $\nu(n) = \sum_{|G|=n} \tilde{\mu}(G)$. Then we have the following:

Theorem 4.5.29. *The functions a and ν are E-multiplicative.*

Proof. We have

$$a(n) = \sum_{|G|=n} 1. \tag{4.5.f}$$

Let $n = n_1 n_2$, gcd $(n_1, n_2) = 1$. By the Basis Theorem 1.3.6, each G in (4.5.f) has a unique factorization, $G = G_1 \times G_2$ such that $|G_1| = n_1$, $|G_2| = n_2$. Hence gcd $(G_1, G_2) = E_0$. Now

$$\begin{aligned} a(n = n_1 n_2) = \sum_{|G_1 \times G_2|=n} 1 &= \sum_{|G_1|=n_1, |G_2|=n_2} 1 \\ &= \sum_{|G_1|=n_1} 1 \sum_{|G_2|=n_2} 1 \\ &= a(n_1)a(n_2). \end{aligned}$$

i.e., a is E-multiplicative. Again

$$\begin{aligned} \nu(n = n_1 n_2) = \sum_{|G_1 \times G_2|=n} \tilde{\mu}(G) &= \sum_{|G_1|=n_1, |G_2|=n_2} \tilde{\mu}(G_1 \times G_2) \\ &= \sum_{|G_1|=n_1} \tilde{\mu}(G_1) \sum_{|G_2|=n_2} \tilde{\mu}(G_2) \\ &= \nu(n_1)\nu(n_2). \end{aligned}$$

i.e., ν is E-multiplicative. □

Theorem 4.5.30. *We have* $\nu(p^r) = P'(r)$, *where* $P'(r) = E(r) - U(r)$.

Proof. Let

$$\mathcal{X}' = \{G \in \mathcal{X} : |G| = p^r\}.$$

$$\mathcal{X}_1 = \{G \in \mathcal{X}' : G \text{ is a product of even number of distinct groups}\}.$$

$$\mathcal{X}_2 = \{G \in \mathcal{X}' : G \text{ is a product of odd number of distinct groups}\}.$$

Then $|\mathcal{X}_1| = E(r)$ and $|\mathcal{X}_2| = U(r)$. Now

$$\begin{aligned}
\nu(p^r) &= \sum_{|G|=p^r} \tilde{\mu}(G) \\
&= \sum_{G\in\mathcal{G}_1} \tilde{\mu}(G) + \sum_{G\in\mathcal{G}_2} \tilde{\mu}(G) \\
&= |\mathcal{X}_1| - |\mathcal{X}_2|, \quad \text{by Corollary 4.5.16.} \\
&= E(r) - U(r) \\
&= P'(r).
\end{aligned}$$

□

Theorem 4.5.31. $a(n) = \prod_{p^r|n} P(r)$, $\nu(n) = \prod_{p^r|n} P'(r)$, *where* $P'(r) = E(r) - U(r)$.

Proof. We know that the number of non isomorphic abelian group of order p^r is $P(r)$. Therefore $a(p^r) = P(r)$. Now,

$$\begin{aligned}
a(n) &= a({p_1}^{r_1}{p_2}^{r_2}\dots{p_k}^{r_k}) \\
&= a({p_1}^{r_1})a({p_2}^{r_2})\dots a({p_k}^{r_k}) \\
&= P(r_1)P(r_2)\dots P(r_k) \\
&= \prod_{p^r|n} P(r).
\end{aligned}$$

Again

$$\begin{aligned}\nu(n) &= \nu({p_1}^{r_1}{p_2}^{r_2}\dots{p_k}^{r_k}) \\ &= \nu({p_1}^{r_1})\nu({p_2}^{r_2})\dots\nu({p_k}^{r_k}) \\ &= P'(r_1)P'(r_2)\dots P'(r_k), \text{ by Theroem 4.5.30.} \\ &= \prod_{p^r|n} P'(r).\end{aligned}$$

□

Following lemma is a consequence of Theorem 4.5.13.

Lemma 4.5.32. $\sum_{de=n} a(d)\nu(e) = \varepsilon(n) \equiv \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases}$

Proof. From Theorem 4.5.13, we have

$$\begin{aligned} & \sum_{D\times E=G} \tilde{\mu}(D) = \varepsilon(G) \\ \Longrightarrow & \sum_{|G|=n} \sum_{D\times E=G} \tilde{\mu}(D) = \sum_{|G|=n} \varepsilon(G) \\ \Longrightarrow & \sum_{|D|\,|E|=n} \tilde{\mu}(D) = \varepsilon(n) \\ \Longrightarrow & \sum_{de=n} \sum_{|D|=d,\,|E|=e} \tilde{\mu}(D) = \varepsilon(n) \\ \Longrightarrow & \sum_{de=n} \sum_{|D|=d} \tilde{\mu}(D) \sum_{|E|=e} 1 = \varepsilon(n) \\ \Longrightarrow & \sum_{de=n} \nu(d)a(e) = \varepsilon(n). \end{aligned}$$

□

Lastly we study "zeta function" of $\mathcal{X}$ and establish a very interesting result.

Definition 4.5.33. The "zeta-function" of $\mathcal{X}$ is defined for real values of $s > 1$ by

$$Z(s) = \sum_{G \in \mathcal{X}} \frac{1}{|G|^s} = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}.$$

Theorem 4.5.34. $\sum_{G \in \mathcal{X}} \frac{\tilde{\mu}(G)}{|G|^s} = \sum_{n=1}^{\infty} \frac{\nu(n)}{n^s} = \frac{1}{Z(s)}$.

Proof. We have

$$\begin{aligned} \sum_{G \in \mathcal{X}} \frac{\tilde{\mu}(G)}{|G|^s} &= \sum_{n=1}^{\infty} \sum_{G \in \mathcal{X},\, |G|=n} \frac{\tilde{\mu}(G)}{n^s} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} \nu(n) \\ &= \sum_{n=1}^{\infty} \frac{\nu(n)}{n^s}. \end{aligned} \tag{4.5.g}$$

Again

$$\begin{aligned} \left(\sum_{n=1}^{\infty} \frac{a(n)}{n^s} \right) \left(\sum_{m=1}^{\infty} \frac{\nu(m)}{m^s} \right) &= \sum_{m,\, n} \frac{a(n)\nu(m)}{n^s m^s} \\ &= \sum_{k=1}^{\infty} \frac{1}{k^s} \sum_{mn=k} a(n)\nu(m) \\ &= \sum_{k=1}^{\infty} \frac{\varepsilon(k)}{k^s} = 1. \end{aligned}$$

Therefore

$$\left(\sum_{m=1}^{\infty} \frac{\nu(m)}{m^s} \right) = \frac{1}{\left(\sum_{n=1}^{\infty} \frac{a(n)}{n^s} \right)} = \frac{1}{Z(s)}. \tag{4.5.h}$$

Combining equations (4.5.g) and (4.5.h) we get the required result. □

Definition 4.5.35. The D-Möbius Function $\hat{\mu}$ is defined by the formula

$$\hat{\mu} \odot u = \varepsilon.$$

Lemma 4.5.36. $\hat{\mu}(E_0) = 1$.

Proof. We have

$$\begin{aligned} & (\hat{\mu} \odot u)(E_0) = \varepsilon(E_0) \\ \Longrightarrow \quad & \hat{\mu}(E_0)u(E_0) = 1 \\ \Longrightarrow \quad & \hat{\mu}(E_0) = 1. \end{aligned}$$

□

Proposition 4.5.37. *For each $G \in \mathcal{X}$, the equation $(\hat{\mu} \odot u)(G) = \varepsilon(G)$ has a unique solution for $\hat{\mu}(G)$.*

Proof. We use induction on the order of G. Suppose $|G| = 1$ i.e., $G = E_0$, then $\hat{\mu}(G) = 1$. Next suppose $|G| = 2$. Then

$$\begin{aligned} & (\hat{\mu} \odot u)(G) = \varepsilon(G) \\ \Longrightarrow \quad & \hat{\mu}(E_0)u(G) + \hat{\mu}(G)u(E_0) = 0 \\ \Longrightarrow \quad & \hat{\mu}(G) = -1 \end{aligned}$$

Suppose for all $H \in \mathcal{X}$ whose order is less than order of G, $\hat{\mu}(H)$ is uniquely determined. Now,

$$\begin{aligned} & (\hat{\mu} \odot u)(G) = \varepsilon(G) \\ \Longrightarrow \quad & \sum_{H \leq G} \hat{\mu}(H)u(\frac{G}{H}) = 0 \\ \Longrightarrow \quad & \sum_{H \leq G} \hat{\mu}(H) = 0 \end{aligned}$$

$$\implies \sum_{H<G} \hat{\mu}(H) + \hat{\mu}(G) = 0$$

$$\implies \hat{\mu}(G) = -\sum_{H<G} \hat{\mu}(H). \tag{4.5.i}$$

i.e., $\hat{\mu}(G)$ is uniquely determined. □

Considering G to be $C_2 \times C_2$ and C_4, one can see that the Möbius Functions $\mu(G)$, $\tilde{\mu}(G)$ and $\hat{\mu}(G)$ and are all distinct.

Following is a analogue of Möbius inverson formula.

Proposition 4.5.38. *For $f, g \in \mathcal{A}(\mathcal{X})$, we have $f \odot u = F \iff f = F \odot \hat{\mu}$.*

Proof.

$$f \odot u = F \Rightarrow (f \odot u) \odot \hat{\mu} = F \odot \hat{\mu} \Rightarrow f \odot (u \odot \hat{\mu}) = F \odot \hat{\mu}$$
$$\Rightarrow f \odot \varepsilon = F \odot \hat{\mu} \Rightarrow f = F \odot \hat{\mu}.$$

Conversly,

$$f = F \odot \hat{\mu} \Rightarrow f \odot u = (F \odot \hat{\mu}) \odot u \Rightarrow f \odot u = F \odot (\hat{\mu} \odot u)$$
$$\Rightarrow f \odot u = F \odot \varepsilon \Rightarrow f \odot u = F.$$

□

Proposition 4.5.39. *The D-Möbius Function $\hat{\mu}$ is D-multiplicative.*

Proof. Let $G_1, G_2 \in \mathcal{X}$ be such that gcd $(|G_1|, |G_2|) = 1$. If $|G_1 \times G_2| = 1$ then $G_1 = E_0, G_2 = E_0$, and so

$$\hat{\mu}(G_1 \times G_2) = \hat{\mu}(E_0) = \hat{\mu}(G_1)\hat{\mu}(G_2).$$

Hence the result is trivial. Now suppose the result is true for all subgroups of $G_1 \times G_2$ which has order $< |G_1 \times G_2|$. By (4.5.i) we have,

$$\begin{aligned}
\hat{\mu}(G_1 \times G_2) &= - \sum_{\substack{H_1 \leq G_1, H_2 \leq G_2 \\ H_1 \times H_2 \neq G_1 \times G_2}} \hat{\mu}(H_1 \times H_2) \\
&= - \sum_{\substack{H_1 \leq G_1, H_2 \leq G_2 \\ H_1 \times H_2 \neq G_1 \times G_2}} \hat{\mu}(H_1)\hat{\mu}(H_2) \\
&= - \sum_{H_1 \leq G_1, H_2 \leq G_2} \hat{\mu}(H_1)\hat{\mu}(H_2) + \hat{\mu}(G_1)\hat{\mu}(G_2) \\
&= \hat{\mu}(G_1)\hat{\mu}(G_2).
\end{aligned}$$

Hence $\hat{\mu}$ is D-multiplicative. □

Let $\mathcal{M}$ be the collection of all complex valued functions defined on $\mathcal{X} \times \mathcal{X}$. We now prove the following theorem, by means of which we shall give a different proof of the above proposition.

Theorem 4.5.40. *If $F \in \mathcal{M}$, then there exists a unique $f \in \mathcal{M}$ such that for $(G_1, G_2) \in \mathcal{X} \times \mathcal{X}$,*

$$F((G_1, G_2)) = \sum_{H \leq G_1, K \leq G_2} f((H, K)).$$

Proof. If such a function exists then it is unique. Consider the function $\phi \in \mathcal{M}$ given by

$$\begin{aligned}
\phi((G_1, G_2)) &= \sum_{K \leq G_2} f((G_1, K)) \\
i,e \ \ \phi((G_1, -)) &= f((G_1, -)) \odot u \\
i,e \ \ f((G_1, -)) &= \phi((G_1, -)) \odot \hat{\mu}, \quad \text{by Proposition 4.5.38.}
\end{aligned}$$

Therefore

$$f((G_1, G_2)) = \sum_{K \leq G_2} \phi((G_1, K))\hat{\mu}\left(\frac{G_2}{K}\right). \tag{4.5.j}$$

Again

$$\begin{aligned} F(-, G_2)(G_1) &= F((G_1, G_2)) \\ &= \sum_{H \leq G_1} (f(H, -) \odot u)(G_2) \\ &= \sum_{H \leq G_1} \phi(H, -)(G_2) \end{aligned}$$

$$\begin{aligned} &= \sum_{H \leq G_1} \phi(H, G_2) \\ &= (\phi(-, G_2) \odot u)(G_1). \end{aligned}$$

i.e.,

$$\phi(-, G_2) = F(-, G_2) \odot \hat{\mu}, \text{ by Proposition 4.5.38.}$$

Therefore

$$\phi((G_1, G_2)) = \sum_{H \leq G_1} F((H, G_2))\hat{\mu}\left(\frac{G_1}{H}\right). \tag{4.5.k}$$

From equations (4.5.j) and (4.5.k), we see that f depends only on F and $\hat{\mu}$. Hence f is unique. Now we show that such a function f exists. Consider the functions $f, \phi \in \mathcal{M}$ given by (4.5.j) and (4.5.k) respectively. Now given $G_1 \in \mathcal{X}$, consider the functions

$$\theta_{G_1}(G_2) = \phi((G_1, G_2)) \text{ and } f_{G_1}(G_2) = f((G_1, G_2))$$

defined on $\mathcal{X}$. Similarly, given $G_2 \in \mathcal{X}$, consider the functions

$$\psi_{G_2}(G_1) = \phi((G_1, G_2)) \text{ and } F_{G_2}(G_1) = F((G_1, G_2))$$

defined on $\mathcal{X}$. Then from (4.5.j), we get

$$f_{G_1}(G_2) = \sum_{K \leq G_2} \theta_{G_1}(K)\hat{\mu}\left(\frac{G_2}{K}\right), \text{ i.e., } f_{G_1} = \theta_{G_1} \odot \hat{\mu} \text{ i.e., } \theta_{G_1} = f_{G_1} \odot u.$$

Similarly, from (4.5.k), we get

$$\psi_{G_2} = F_{G_2} \odot \hat{\mu} \text{ i.e., } F_{G_2} = \psi_{G_2} \odot u.$$

Now

$$\begin{aligned}
\sum_{H \leq G_1, K \leq G_2} f((H,K)) &= \sum_{H \leq G_1} \sum_{K \leq G_2} f_H(K) \\
&= \sum_{H \leq G_1} (f_H \odot u)(G_2) \\
&= \sum_{H \leq G_1} \theta_H(G_2) \\
&= \sum_{H \leq G_1} \phi((H, G_2)) \\
&= \sum_{H \leq G_1} \psi_{G_2}(H) \\
&= (\psi_{G_2} \odot u)(G_1) \\
&= F_{G_2}(G_1) \\
&= F((G_1, G_2)).
\end{aligned}$$

□

We now give another proof of the Proposition 4.5.39.

Proof: Let $F \in \mathcal{M}$ be given by

$$F((G_1, G_2)) = \varepsilon(G_1)\varepsilon(G_2).$$

Consider, $g \in \mathcal{M}$ given by

$$g((G_1, G_2)) = \hat{\mu}(G_1)\hat{\mu}(G_2).$$

Now,

$$\begin{aligned}
\sum_{H_1 \leq G_1, H_2 \leq G_2} g((H_1, H_2)) &= \sum_{H_1 \leq G_1, H_2 \leq G_2} \hat{\mu}(H_1)\hat{\mu}(H_2) \\
&= \left(\sum_{H_1 \leq G_1} \hat{\mu}(H_1) \right) \left(\sum_{H_2 \leq G_2} \hat{\mu}(H_2) \right) \\
&= \varepsilon(G_1)\varepsilon(G_2) \\
&= F((G_1, G_2)). \qquad (4.5.1)
\end{aligned}$$

Again consider, $h \in \mathcal{M}$ given by

$$h((G_1, G_2)) = \hat{\mu}(G_1 \times G_2).$$

Now,

$$\begin{aligned}
\sum_{H_1 \leq G_1, H_2 \leq G_2} g((H_1, H_2)) &= \sum_{H_1 \leq G_1, H_2 \leq G_2} \hat{\mu}(H_1 \times H_2) \\
&= \sum_{H_1 \times H_2 \leq G_1 \times G_2} \hat{\mu}(H_1 \times H_2) \\
&= \varepsilon(G_1 \times G_2) \\
&= \varepsilon(G_1)\varepsilon(G_2)
\end{aligned}$$

$$= F((G_1, G_2)). \tag{4.5.m}$$

Hence g and h are two solutions of the equation

$$F((G_1, G_2)) = \sum_{H_1 \leq G_1, H_2 \leq G_2} f((H_1, H_2)).$$

It follows from the Theorem 4.5.40 that, $g = h$. i.e.,

$$\hat{\mu}(G_1 \times G_2) = \hat{\mu}(G_1)\hat{\mu}(G_2). \ \textit{i.e.,} \ \ \hat{\mu} \text{ is D-multiplicative.}$$

4.6 Computation of $\hat{\mu}(G)$ for any $G \in \mathcal{X}$

Suppose $G_m = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ m-times. Every element of G_m is of order 1 or p. So every subgroup of G_m of order p^n $(n \leq m)$ is of the form $G_n = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, n-times (upto isomorphism). We look for n elements in G_m say $v_1, v_2, \ldots, v_n$ such that $v_i \notin < v_1, v_2, \ldots, \widehat{v_i}, \ldots, v_n >$. Clearly $< v_1, v_2, \ldots, v_n >$ is a subgroup of G_m of order p^n.

Lemma 4.6.1. *Let $\mathcal{S}$ be the collection of all ordered sets $\{v_1, v_2, \ldots, v_n\}$ taking from G_m such that $v_i \notin < v_1, v_2, \ldots, \widehat{v_i}, \ldots, v_n >$ for each i. Then*

$$|\mathcal{S}| = (p^m - 1)(p^m - p) \ldots (p^m - p^{n-1}).$$

Proof. Total number of elements in G_m is p^m. But we can't take 0 in our choice of v_i's. Therefore v_1 can be choosen in $(p^m - 1)$ ways. For the choice of v_2 we have to avoid the multiples of v_1. There are p multiples of v_1. Therefore v_2 can be choosen in $(p^m - p)$ ways. Continuing in this way we see that v_n can be choosen in $(p^m - p^{n-1})$ ways. Therefore $|\mathcal{S}| = (p^m - 1)(p^m - p) \ldots (p^m - p^{n-1})$. □

Theorem 4.6.2. *Let $G_m = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, m-times. Then number of subgroups of G_m of order $p^n (n \leq m)$ is*

$$\frac{(p^m - 1)(p^{m-1} - 1)\dots(p^{m-n+1} - 1)}{(p-1)(p^2-1)\dots(p^n-1)}.$$

Proof. Let $\mathcal{S}$ be defined above and $\mathcal{H}$ be the set of all subgroups of G_m of order $p^n (n \leq m)$. Define

$$f : \mathcal{S} \longrightarrow \mathcal{H} \text{ given by } \{v_1, v_2, \dots, v_n\} \longmapsto < v_1, v_2, \dots, v_n > .$$

Clearly this map is onto, since each $H \in \mathcal{H}$ has an ordered basis.

Note that each $H \in \mathcal{H}$ has $(p^n - 1)(p^n - p)\dots(p^n - p^{n-1})$ many basis sets. Therefore

$$|f^{-1}(H)| = (p^n - 1)(p^n - p)\dots(p^n - p^{n-1}) = k \text{ (say)}.$$

Now $\mathcal{S} = \bigsqcup_{H \in \mathcal{H}} f^{-1}(H)$, i.e., $|\mathcal{S}| = \sum_{H \in \mathcal{H}} |f^{-1}(H)| = k \sum_{H \in \mathcal{H}} 1 = k|\mathcal{H}|$. Therefore

$$\begin{aligned} |\mathcal{H}| = \frac{|\mathcal{S}|}{k} &= \frac{(p^m - 1)(p^m - p)\dots(p^m - p^{n-1})}{(p^n - 1)(p^n - p)\dots(p^n - p^{n-1})} \\ &= \frac{(p^m - 1)(p^{m-1} - 1)\dots(p^{m-n+1} - 1)}{(p-1)(p^2-1)\dots(p^n-1)}. \end{aligned}$$

□

Theorem 4.6.3. *Let $G_m = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, m-times. Then*

$$\hat{\mu}(G_m) = (-1)^m p^{\frac{1}{2}m(m-1)}.$$

Proof. We use induction on m. If $m = 1$ then

$$\hat{\mu}(G_1) = \hat{\mu}(\mathbb{Z}_p) = -1 = (-1)^m p^{\frac{1}{2}m(m-1)}.$$

Suppose the result is true for all groups G_r, $r \leq m$. If we denote the number of subgroups of G_{m+1} of order $p^r (r \leq m+1)$ by $\begin{bmatrix} m+1 \\ r \end{bmatrix}_p$, then from the definition of $\hat{\mu}$, we have $\sum_{r=0}^{m+1} \begin{bmatrix} m+1 \\ r \end{bmatrix}_p \hat{\mu}_r = 0$. That is

$$
\begin{aligned}
-\hat{\mu}(G_{m+1}) - 1 &= \sum_{r=1}^{m} \begin{bmatrix} m+1 \\ r \end{bmatrix}_p \hat{\mu}_r \\
&= \sum_{r=1}^{m} \begin{bmatrix} m+1 \\ r \end{bmatrix}_p (-1)^r p^{\frac{1}{2}r(r-1)} \\
&= \sum_{r=1}^{m} \left(p^r \begin{bmatrix} m \\ r \end{bmatrix}_p + \begin{bmatrix} m \\ r-1 \end{bmatrix}_p \right) (-1)^r p^{\frac{1}{2}r(r-1)}, \text{ ([11], page 465)} \\
&= \sum_{r=1}^{m} \begin{bmatrix} m \\ r \end{bmatrix}_p (-1)^r p^{\frac{1}{2}(r+1)(r+1-1)} + \sum_{r=1}^{m} \begin{bmatrix} m \\ r-1 \end{bmatrix}_p (-1)^r p^{\frac{1}{2}r(r-1)}
\end{aligned}
$$

or,

$$
\begin{aligned}
-\hat{\mu}(G_{m+1}) &= \sum_{r=1}^{m+1} \begin{bmatrix} m \\ r-1 \end{bmatrix}_p (-1)^{r-1} p^{\frac{1}{2}r(r-1)} + \sum_{r=1}^{m} \begin{bmatrix} m \\ r-1 \end{bmatrix}_p (-1)^r p^{\frac{1}{2}r(r-1)} \\
&= (-1)^m p^{\frac{1}{2}(m+1)(m+1-1)} + \sum_{r=1}^{m} \begin{bmatrix} m \\ r-1 \end{bmatrix}_p p^{\frac{1}{2}r(r-1)} ((-1)^{r-1} + (-1)^r)
\end{aligned}
$$

i.e., $\hat{\mu}(G_{m+1}) = (-1)^{m+1} p^{\frac{1}{2}(m+1)(m+1-1)}$. and hence by induction the result follows. □

Let G be a finite abelian group. $|G| = n = {p_1}^{e_1} {p_2}^{e_2} \ldots {p_k}^{e_k}$. Then $G \cong G_1 \times G_2 \times \cdots \times G_K$, where G_i is a subgroup of order ${p_i}^{e_i}$. Again $G_i =$

$\mathbb{Z}_{p_i^{n_1}} \times \mathbb{Z}_{p_i^{n_2}} \times \cdots \times \mathbb{Z}_{p_i^{n_t}}$, where $n_1 + n_2 + \ldots n_t = e_i$. Since $\hat{\mu}$ is multiplicative therefore to find $\hat{\mu}(G)$ it is enough to look at the groups of the type $H = \mathbb{Z}_{p^{n_1}} \times \mathbb{Z}_{p^{n_2}} \times \cdots \times \mathbb{Z}_{p^{n_t}}$.

Theorem 4.6.4. *Let $G = \mathbb{Z}_p^{m_1} \times \mathbb{Z}_p^{m_2} \times \cdots \times \mathbb{Z}_p^{m_r}$, r-times, where atleast one $m_i \geq 2$, $i = 1, 2, \ldots, r$. Then*

$$\hat{\mu}(G) = 0.$$

Proof. We use induction on the order of G. Suppose the result is true for all groups of the type G and order less than that of G. Now,

$$\hat{\mu}(G) = -\sum_{H<G} \hat{\mu}(H) = -\left(\sum_{H \leq G_r} \hat{\mu}(H) + \sum_{H<G}{}' \hat{\mu}(H) \right),$$

where $G_r = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, r-times and the $'$ indicates that the summation is extended over all subgroups of G in which atleast one element has order grater than p. Therefore it follows, using induction that $\hat{\mu}(G) = 0$. □

4.7 Divisor functions

Some well-known examples of divisor functions which form an integral part of arithmetic functions of positive integers are given by

$$\tau(n) = \sum_{d|n} 1, \quad \sigma(n) = \sum_{d|n} d, \quad \text{and} \quad \sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

where n is a positive integer and α is any complex number.

The group-theoretic anlogues of these functions are defined as

$$\tau(G) = \sum_{N \trianglelefteq G} 1, \quad \sigma(G) = \sum_{N \trianglelefteq G} |N|, \quad \text{and} \quad \sigma_\alpha(G) = \sum_{N \trianglelefteq G} |N|^\alpha$$

where $G \in \mathcal{G}$. Thus,

$\tau(G)$ is the number of normal subgroups of G,

$\sigma(G)$ is the sum of the orders of normal subgroups of G, *and*

$\sigma_\alpha(G)$ the sum of the α^{th} powers of the orders of normal subgroups of G.

Clearly, $\sigma_0(G) = \tau(G)$ and $\sigma_1(G) = \sigma(G)$. Also, in particular, if we take $G = C_n$ then $\sigma_\alpha(C_n) = \sigma_\alpha(n)$; noting that there is an one to one correspondence between the normal subgroups of C_n and the divisors of n given by $N \longmapsto |N|$, where $N \trianglelefteq C_n$.

Theorem 4.7.1. *Since every proper non-trivial normal subgroup N of a finite group G satisfies $2 \leq |N| \leq \frac{|G|}{2}$, we have*

$$2\tau(G) + |G| - 3 \leq \sigma(G) \leq 1 + \tau(G)\frac{|G|}{2}.$$

Proof. Let $E_0 \neq N \lhd G$. Then $2 \leq |N| \leq \dfrac{|G|}{2}$.
Suppose $N_1, N_2, \ldots, N_n$ are the proper non-trivial normal subgroups of G. Then

$$\begin{aligned}
& 2 \leq |N_1| \leq \frac{|G|}{2}, \quad 2 \leq |N_2| \leq \frac{|G|}{2}, \ldots, 2 \leq |N_n| \leq \frac{|G|}{2}. \\
\Longrightarrow \quad & 2n \leq \sum_{N \lhd G} |N| \leq n\frac{|G|}{2}. \\
\Longrightarrow \quad & 2\sum_{N \lhd G} 1 \leq \sigma(G) - 1 - |G| \leq \left(\sum_{N \lhd G} 1\right)\frac{|G|}{2}. \\
\Longrightarrow \quad & 2(\tau(G) - 2) \leq \sigma(G) - 1 - |G| \leq (\tau(G) - 2)\frac{|G|}{2}. \\
\Longrightarrow \quad & 2\tau(G) - 4 \leq \sigma(G) - 1 - |G| \leq \tau(G)\frac{|G|}{2} - |G|. \\
\Longrightarrow \quad & 2\tau(G) + |G| - 3 \leq \sigma(G) \leq \tau(G)\frac{|G|}{2} + 1.
\end{aligned}$$

□

Theorem 4.7.2. *If $G \in \mathcal{G}$, then*

$$\sigma(G) = \sum_{g \in G} \tau(G/N_g),$$

where N_g is the smallest normal subgroup of G containing g.

Proof. We know that, $\forall g \in G$, the normal subgroups of G/N_g are in one to one correspondence with the set $\{N : N_g \trianglelefteq N \trianglelefteq G\} = \{N : g \in N \trianglelefteq G\}$, and so $\tau(G/N_g) = |\{N : g \in N \trianglelefteq G\}|$. Therefore,

$$\begin{aligned}
\sigma(G) &= \sum_{N \trianglelefteq G} |N| = \sum_{N \trianglelefteq G} \sum_{g \in N} 1 \\
&= \sum_{N \trianglelefteq G} \sum_{g \in G} \delta_{g,N}, \text{ where } \delta_{g,N} = \begin{cases} 1, & \text{if } g \in N, \\ 0, & \text{otherwise.} \end{cases} \\
&= \sum_{g \in G} \sum_{N \trianglelefteq G} \delta_{g,N} \\
&= \sum_{g \in G} \sum_{g \in N \trianglelefteq G} 1 = \sum_{g \in G} |\{N : g \in N \trianglelefteq G\}| = \sum_{g \in G} \tau(G/N_g).
\end{aligned}$$

□

We know that For each element $a \in G$, the set $H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G. Moreover this is the smallest subgroup of G containing a. Because if H' be another subgroup of G containing a, then by closure property of H' all of $a^2, a^3, \ldots a^n, \cdots \in H'$, and thus $H \subseteq H'$.

As a corollary of Theorem 4.7.2 we have the following number theoretic identity.

Corollary 4.7.3. *For any positive integer n, $\sigma(n) = \sum_{k=0}^{n-1} \tau(\gcd(n,k))$.*

Proof. Putting $G = C_n$, in Theorem 4.7.2, we have

$$\begin{aligned}
&\sigma(n) = \sigma(C_n) \\
&= \sum_{k=0}^{n-1} \tau\left(\frac{C_n}{< k >}\right), \quad < k > \text{ is the subgroup of } C_n \text{ generated by } k \\
&= \sum_{k=0}^{n-1} \tau\left(\frac{C_n}{C_{k'}}\right), \quad \text{where } k' = \frac{n}{\gcd(n,k)} \\
&= \sum_{k=0}^{n-1} \tau(C_{\gcd(n,k)}) = \sum_{k=0}^{n-1} \tau(\gcd(n,k)).
\end{aligned}$$

□

4.8 Normal subgroups of the product $G_1 \times G_2$

In this section we study the structure of the normal subgroups of the product of two groups.

Theorem 4.8.1. *Let G_1 and G_2 be coprime groups. Then the normal subgroups of the product $G_1 \times G_2$ are exactly the subgroups of the form $N_1 \times N_2$, with $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

Proof. Let $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$. Suppose $(n_1, n_2), (n_1', n_2') \in N_1 \times N_2$; $n_1, n_1' \in N_1; n_2, n_2' \in N_2$. Now $(n_1, n_2)(n_1', n_2') = (n_1 n_1', n_2, n_2') \in N_1 \times N_2$. i.e., $N_1 \times N_2 \leq G_1 \times G_2$. Again let $(g_1, g_2) \in G_1 \times G_2$ and $(n_1, n_2) \in N_1 \times N_2$. Then $(g_1, g_2)(n_1, n_2)(g_1^{-1}, g_2^{-1}) = (g_1 n_1 g_1^{-1}, g_2 n_2 g_2^{-1}) \in N_1 \times N_2$. Therefore $N_1 \times N_2 \trianglelefteq G_1 \times G_2$.

Conversely, suppose $N \trianglelefteq G_1 \times G_2$. Let $\pi_i : G_1 \times G_2 \longrightarrow G_i$, $(i = 1, 2)$ be the projection map. For $(g_1, g_2), (g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$,

$\pi_1((g_1, g_2)(g_1^{-1}, g_2^{-1})) = \pi_1(g_1 g_1^{-1}, g_2 g_2^{-1}) = g_1 g_1^{-1} = \pi_1((g_1, g_2))\pi_1((g_1^{-1}, g_2^{-1}))$.

i.e., π_1 is a homomorphism from $G_1 \times G_2$ to G_1. Similarly π_2 is a homomorphism from $G_1 \times G_2$ to G_2. And therefore π_i is a homomorphism from N to G_i also. By (*First Isomorphism*) Theorem 1.2.1

$$\pi_1(N) \cong \frac{N}{\mathrm{Ker}(\pi_1|N)} = \frac{N}{\mathrm{Ker}(\pi_1) \cap N} = \frac{N}{(\{e_1\} \times G_2) \cap N} = \frac{N}{G_2 \cap N}. \tag{4.8.a}$$

Again by Theorem 4.2.1

$$C(N) = C\left(\frac{N}{G_2 \cap N}\right) \sqcup C(G_2 \cap N) = C(\pi_1(N)) \sqcup C(G_2 \cap N). \tag{4.8.b}$$

Similarly

$$\pi_2(N) \cong \frac{N}{\mathrm{Ker}(\pi_2|N)} = \frac{N}{\mathrm{Ker}(\pi_2) \cap N} = \frac{N}{(G_1 \times \{e_2\}) \cap N} = \frac{N}{G_1 \cap N}, \tag{4.8.c}$$

and

$$C(N) = C(\pi_2(N)) \sqcup C(G_1 \cap N). \tag{4.8.d}$$

from equations (4.8.b) and (4.8.d)

$$C(\pi_1(N)) \sqcup C(G_2 \cap N) = C(\pi_2(N)) \sqcup C(G_1 \cap N). \tag{4.8.e}$$

But $C(\pi_i(N)) \subseteq C(G_i)$ and G_1, G_2 are coprime. Therefore by Defination 4.3.1

$$C(\pi_1(N)) \cap C(\pi_2(N)) = \phi \tag{4.8.f}$$

Again $G_1 \cap N = (G_1 \times \{e_2\}) \cap N \subseteq G_1 \times \{e_2\} = G_1$. Similarly $G_2 \cap N = (\{e_1\} \times G_2) \cap N \subseteq \{e_1\} \times G_2 = G_2$. Therefore $C(G_1 \cap N) \subseteq C(G_1)$ and

$C(G_2 \cap N) \subseteq C(G_2)$ and so

$$C(G_1 \cap N) \cap C(G_2 \cap N) = \phi \tag{4.8.g}$$

Hence

$$C(\pi_i(N)) = C(G_i \cap N) \Longrightarrow |\pi(C(\pi_i(N)))| = |\pi(C(G_i \cap N))|$$

$$\Longrightarrow |\pi_i(N)| = |G_i \cap N|. \tag{4.8.h}$$

Again any element of $G_1 \cap N = G_1 \times \{e_2\} \cap N$ is of the form (n_1, e_2), for some $(n_1, n_2) \in N$, and clearly $(n_1, e_2) \in \pi_1(N) \times \{e_2\} = \pi_1(N)$ for any $(n_1, e_2) \in G_1 \cap N$. Thus $G_1 \cap N \subseteq \pi_1(N)$. Similarly $G_2 \cap N \subseteq \pi_2(N)$. By (4.8.h) we have $G_i \cap N = \pi_i(N)$. Therefore

$$\pi_1(N) \times \pi_2(N) = (G_1 \cap N) \times (G_2 \cap N) \tag{4.8.i}$$

Now we have

(i) $(G_1 \cap N) \trianglelefteq N$, $(G_2 \cap N) \trianglelefteq N$.

(ii) $(G_1 \cap N) \cap (G_2 \cap N) = \{(e_1, e_2)\}$.

(iii) $N = (G_1 \cap N)(G_2 \cap N)$.

Therefore by Theorem 1.3.2 we have

$$N = (G_1 \cap N) \times (G_2 \cap N) = \pi_1(N) \times \pi_2(N),$$

with $\pi_i(N) \trianglelefteq G_i$. □

Given any two groups G_1 and G_2 (finite or infinite, abelian or non-abelian), we now develop a condition which is equivalent to saying that every normal subgroup of the product $G_1 \times G_2$ is of the form $N_1 \times N_2$ with $N_i \trianglelefteq G_i$, $i = 1, 2$.

Definition 4.8.2. We shall say that the groups G_1 and G_2 have a *subgroup in common* if there exist non-trivial subgroups H_1 of G_1, and H_2 of G_2 such that $H_1 \cong H_2$.

Theorem 4.8.3. *Let G_1 and G_2 be any two groups. Then the following conditions are equivalent:*

(i) *Every normal subgroup of the product $G_1 \times G_2$ is of the form $N_1 \times N_2$ with $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

(ii) *For each $H_1 \lhd G_1$ and for each $H_2 \lhd G_2$, the centres $Z(G_1/H_1)$ and $Z(G_2/H_2)$ of the quotient groups G_1/H_1 and G_2/H_2 have no subgroup in common.*

Proof. Suppose that G_1 and G_2 satisfy the second condition. Let $N \trianglelefteq G_1 \times G_2$. Set $H_1 = \pi_1((G_1 \times \{e_2\}) \cap N)$ and $H_2 = \pi_2((\{e_1\} \times G_2) \cap N)$ where e_i are identities of G_i and $\pi_i : G_1 \times G_2 \longrightarrow G_i$ are projections, $i = 1, 2$. Then $H_1 \times \{e_2\}, \{e_1\} \times H_2 \subset N \subset \pi_1(N) \times \pi_2(N)$ and so

$$H_1 \times H_2 = (H_1 \times \{e_2\})(\{e_1\} \times H_2) \subset \pi_1(N) \times \pi_2(N) \tag{4.8.j}$$

It may be noted here that $H_i \trianglelefteq G_i$ and $H_i \trianglelefteq \pi_i(N)$, $i = 1, 2$. Now, suppose $a_1 \in \pi_1(N)$. Then $(a_1, a_2) \in N$ for some $a_2 \in G_2$; in fact $a_2 \in \pi_2(N)$. Therefore, $\forall g_1 \in G_1$, we have

$$\begin{aligned}
&(g_1 a_1 {g_1}^{-1}, a_2) = (g_1, e_2)(a_1, a_2)({g_1}^{-1}, e_2) \in N \\
\Longrightarrow\ &(g_1 a_1 {g_1}^{-1} {a_1}^{-1}, e_2) \in N \\
\Longrightarrow\ &g_1 a_1 {g_1}^{-1} {a_1}^{-1} \in H_1 \\
\Longrightarrow\ &g_1 H_1 a_1 H_1 = a_1 H_1 g_1 H_1 \in G_1/H_1.
\end{aligned}$$

Thus, $a_1H_1 \in Z(G_1/H_1)$. So, we have $\pi_1(N)/H_1 \subset Z(G_1/H_1)$. Similarly, $\pi_2(N)/H_2 \subset Z(G_2/H_2)$. Note that if $a_1, b_1 \in \pi_1(N)$ then $(a_1, a_2), (b_1, b_2) \in N$ for some $a_2, b_2 \in \pi_2(N)$, and so $(a_1{b_1}^{-1}, a_2{b_2}^{-1})$, $(a_1b_1, a_2b_2) \in N$. Therefore,

$$a_1H_1 = b_1H_1 \iff a_1{b_1}^{-1} \in H_1 \iff (a_1{b_1}^{-1}, e_2) \in N$$
$$\iff (e_1, a_2{b_2}^{-1}) \in N \iff a_2{b_2}^{-1} \in H_2 \iff a_2H_2 = b_2H_2.$$

This means that we have a well-defined injective map $f : \pi_1(N)/H_1 \longrightarrow \pi_2(N)/H_2$ given by $f(a_1H_1) = a_2H_2$ where $(a_1, a_2) \in N$. Also, $f(a_1H_1b_1H_1) = f(a_1b_1H_1) = a_2b_2H_2 = a_2H_2b_2H_2 = f(a_1H_1)f(b_1H_1)$, showing that f is a homomorphism. Finally, if $b \in \pi_2(N)$ then $(a, b) \in N$ for some $a \in \pi_1(N)$ and so $f(aH_1) = bH_2$, which implies that f is surjective. Thus f is an isomorphism. Hence it follows from the hypothesis that $\pi_i(N)/H_i$ are trivial subgroups of $Z(G_i/H_i)$, $i = 1, 2$. Therefore, $H_i = \pi_i(N)$, $i = 1, 2$, and so $N = H_1 \times H_2$, by (4.8.j).

Conversely, suppose G_1 and G_2 do not satisfy the second condition. So, there exist $H_i \lhd G_i$, $i = 1, 2$, such that $Z(G_1/H_1)$ and $Z(G_2/H_2)$ have a subgroup in common. Let K_i/H_i be non-trivial subgroups of $Z(G_i/H_i)$, $i = 1, 2$, such that there is an isomorphism $F : K_1/H_1 \longrightarrow K_2/H_2$. Put $N = \{(a_1, a_2) \in K_1 \times K_2 : F(a_1H_1) = a_2H_2\}$. Let $(a_1, a_2), (b_1, b_2) \in N$ then $F(a_1H_1) = a_2H_2$ and $F(b_1H_1) = b_2H_2$. So, $F(a_1{b_1}^{-1}H_1) = a_2{b_2}^{-1}H_2$. Thus $(a_1, a_2)(b_1, b_2)^{-1} = (a_1{b_1}^{-1}, a_2{b_2}^{-1}) \in N$, showing that N is a subgroup of $G_1 \times G_2$. Again let $(a_1, a_2) \in N$ and $(g_1, g_2) \in G_1 \times G_2$. Then, $(g_1, g_2)(a_1, a_2)(g_1, g_2)^{-1} = (g_1a_1{g_1}^{-1}, g_2a_2{g_2}^{-1}) \in K_1 \times K_2$, since $K_i \trianglelefteq G_i$, $i = 1, 2$. Also, since $a_iH_i \in K_i/H_i \subset Z(G_i/H_i)$, $i = 1, 2$, we have

$$F(g_1 a_1 {g_1}^{-1} H_1) = F(a_1 H_1) = a_2 H_2 = g_2 a_2 {g_2}^{-1} H_2.$$

Thus $(g_1, g_2)(a_1, a_2)(g_1, g_2)^{-1} \in N$, and so $N \trianglelefteq G_1 \times G_2$. On the other hand, suppose N is of standard form $N_1 \times N_2$ where $N_i \trianglelefteq G_i$, $i = 1, 2$. Then, $\pi_i(N) = N_i$, $i = 1, 2$. But since F is bijective, we have $\pi_i(N) = K_i$, $i = 1, 2$. Therefore, $N = K_1 \times K_2$. Since K_1/H_1 is non-trivial, there is some $a_1 \in K_1$ such that $a_1 H_1 \neq H_1$. But $(a_1, e_2) \in K_1 \times K_2 = N$. So, $F(a_1 H_1) = e_2 H_2 = H_2$, the zero element of K_2/H_2. Therefore, since F is injective, we have $a_1 H_1 = H_1$, the zero element of K_1/H_1. This contradiction shows that N is not of the form mentioned in the first condition. □

The following corollary generalizes Theorem 4.8.1.

Corollary 4.8.4. *If $G_1, G_2 \in \mathcal{G}$ are almost coprime, then every normal subgroup of the product $G_1 \times G_2$ is of the form $N_1 \times N_2$ with $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$.*

Proof. Let $H_1 \triangleleft G_1$ and $H_2 \triangleleft G_2$ be such that the centres $Z(G_1/H_1)$ and $Z(G_2/H_2)$ have a subgroup in common. So, there are non-trivial subgroups K_i/H_i of $Z(G_i/H_i)$, $i = 1, 2$, such that

$$K_1/H_1 \cong K_2/H_2.$$

Then $\mathcal{C}(K_1/H_1) = \mathcal{C}(K_2/H_2)$. Since $H_i \triangleleft K_i \trianglelefteq G_i$, we have

$$\mathcal{C}(K_i/H_i) \subseteq \mathcal{C}(K_i) \subseteq \mathcal{C}(G_i),\ i = 1, 2.$$

Thus, $\mathcal{C}(G_1)$ and $\mathcal{C}(G_2)$ have an abelian member in common. A contradiction since $G_1, G_2 \in \mathcal{G}$ are almost coprime. By Theorem 4.8.3 we get the required result. □

The converse of the above corollary may not be true. For example Consider the Symmetric group S_4 and C_3 in $\mathcal{G}$.

$$\{e\} \lhd V \lhd A_4 \lhd S_4$$

is the composition series of S_4, where

$$V = \{e, (12)(34), (13)(24), (14)(23)\}$$

is the normal subgroup of S_4. Thus $C(S_4) = \{V, A_4/V, S_4/A_4\}$. Again $C(C_3) = \{C_3\}$. Therefore $C(S_4)$ and $C(C_3)$ have an abelian member in common, namely $C_3 = A_4/V$. i.e., S_4 and C_3 are not almost coprime.

But for each $H_1 \lhd S_4$ and for each $H_2 \lhd C_3$, the centres $Z(S_4/H_1)$ and $Z(C_3/H_2)$ of the quotient groups S_4/H_1 and C_3/H_2 have no subgroup in common. Therefore every normal subgroup of the product $S_4 \times C_3$ is of the form $N_1 \times N_2$ with $N_1 \trianglelefteq S_4$ and $N_2 \trianglelefteq C_3$.

Proposition 4.8.5. *If $f \in \mathcal{A}(\mathcal{G})$ is multiplicative (or, almost completely multiplicative) then the function $F \in \mathcal{A}(\mathcal{G})$ given by*

$$F(G) = \sum_{N \trianglelefteq G} f(N)$$

is also multiplicative (or, almost completely multiplicative).

Proof. Let $G_1, G_2 \in \mathcal{G}$ be a pair of coprime (or, almost coprime) groups. Clearly, if $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$ then N_1 and N_2 are also coprime (or, almost coprime) (since $C(N_1) \subseteq C(G_1)$ etc). So, we have

$$\begin{aligned} F(G_1 \times G_2) &= \sum_{N \trianglelefteq (G_1 \times G_2)} f(N) = \sum_{N_1 \trianglelefteq G_1, N_2 \trianglelefteq G_2} f(N_1 \times N_2) \\ &= \sum_{N_1 \trianglelefteq G_1} \sum_{N_2 \trianglelefteq G_2} f(N_1) f(N_2) = F(G_1) F(G_2). \end{aligned}$$

□

Lemma 4.8.6. *The map $f : \mathcal{G} \longmapsto \mathbb{C}$ defined by $f(G) = |G|^\alpha$, where $\alpha \in \mathbb{C}$, is completely multiplicative.*

Proof. For $G_1, G_2 \in \mathcal{G}$,
$f(G_1 \times G_2) = |G_1 \times G_2|^\alpha = (|G_1| \cdot |G_2|)^\alpha = |G_1|^\alpha \cdot |G_2|^\alpha = f(G_1)f(G_2)$
Thus f is a completely multiplicative function in $\mathcal{A}(\mathcal{G})$. □

Corollary 4.8.7. *σ_α is almost completely multiplicative.*

Proof. Let $G_1, G_2 \in \mathcal{G}$ be almost coprime. Now

$$\begin{aligned}
\sigma_\alpha(G_1 \times G_2) &= \sum_{N \trianglelefteq G_1 \times G_2} |N|^\alpha \\
&= \sum_{N_1 \trianglelefteq G_1, N_2 \trianglelefteq G_2)} |N_1 \times N_2|^\alpha \\
&= \sum_{N_1 \trianglelefteq G_1} \sum_{N_2 \trianglelefteq G_2} |N_1|^\alpha |N_2|^\alpha \\
&= \sum_{N_1 \trianglelefteq G_1} |N_1|^\alpha \sum_{N_2 \trianglelefteq G_2} |N_2|^\alpha \\
&= \sigma_\alpha(G_1)\sigma_\alpha(G_2).
\end{aligned}$$

Therefore σ_α is almost completely multiplicative. □

4.9 Characterization of groups using divisor functions

In this section we try to charactrize finite groups using the notion of divisor functions studied in earlier sections.

Definition 4.9.1. A finite group G is called *perfect* if $\sigma(G) = 2|G|$. It may be mentioned here that this notion of perfect group, has aparently no relation with the more conventional counterpart available in the literature, namely the groups which are equal to their commutator subgroups.

For example C_6, the cyclic group of order 6 is a perfect group. (In the last section of this chpter we shall discuss "Perfect groups" elaborately).

Definition 4.9.2. An *abelian quotient* of a group G is a quotient group of G which is abelian.

Lemma 4.9.3. *For any group G,*

$$\sigma(G) = \sum_{g \in G} |\{N : N \trianglelefteq G, g \in N\}| = \sum_{g \in G} |\{\textit{normal subgroups of } G \textit{ containing } g\}|.$$

Proof. We have

$$\begin{aligned} \sigma(G) &= \sum_{N \trianglelefteq G} |N| \\ &= |\{(N, g) : N \trianglelefteq G, g \in N\}| \\ &= \sum_{g \in G} |\{N : N \trianglelefteq G, g \in N\}|. \end{aligned}$$

□

Definition 4.9.4. An element h of G is called a *normal generator* of G if the only normal subgroup of G containing h is G itself.

Proposition 4.9.5. *Let G be a group.*

(i) *If $\sigma(G) \leq 2|G|$ then G has a normal generator.*

(ii) *If G has a normal generator then any abelian quotient of G is cyclic.*

Proof. (i) Suppose $\nu(g) := |\{\text{normal subgroups of } G \text{ containing } g\}|$. By Lemma 4.9.3
$\sigma(G) \leq 2|G| \iff \sum_{g\in G} \nu(g) \leq 2|G| \iff \frac{1}{|G|}\sum_{g\in G} \nu(g) \leq 2 \iff$ the mean over all $g \in G$ *of* $\nu(g) \leq 2$.

Case I:

If G is not simple or not trivial then $\nu(e) \geq 3$, e the identity element of G. So for the mean to be ≤ 2, there must be some $h \in G$ for which $\nu(h) = 1$ and this says exactly that h is a normal generator of G.

Case II:

If G is simple then any non identity element of G is a normal generator.

Case III:

If G=$\{e\}$ then e is a normal generator.

(ii) Let A be an abelian quotient of G, with $\pi : G \longrightarrow A$ a surjective homomorphism, and let h be a normal generator of G. Suppose $K \trianglelefteq A$ and $\pi(h) \in K$. Then $\pi^{-1}(K) \trianglelefteq G$ such that $h \in \pi^{-1}(K)$. Therefore $\pi^{-1}(K) = G$ (since the only normal subgroup containing h is G). i.e., $\pi(G) = K = A$ (π is surjective). Therefore the only normal subgroup of A containing $\pi(h)$ is A. i.e., $\pi(h)$ is a normal generator of A. Now $\pi(h) \in <\pi(h)> \trianglelefteq A$. Therefore $A = <\pi(h)>$, cyclic. Hence the result. □

Theorem 4.9.6. (Abelian Quotient Theorem)

If G is a group with $\sigma(G) \leq 2|G|$ then any abelian quotient of G is cyclic.

Proof. Follows from the above proposition. □

The above theorem has the following corolaries, the second of which says that abelian perfect groups 'are' just perfect numbers:

Corollary 4.9.7.

(i) *If G is a perfect group then any abelian quotient of G is cyclic.*

(ii) *The perfect abelian groups are precisely the cyclic groups C_n of order n with n perfect.*

Proof. Part (i) is immediate. For (ii) let A be perfect abelian. Now $A/\{e\}$ is an abelian quotient of the perfect group A. Hence $A/\{e\}$ i.e., A is cyclic. But we have already seen that the perfect cyclic groups correspond exactly to the perfect numbers. □

Most trivial characterrization of groups using divisor functions is perhaps the following:

$$\sigma_\alpha(G) = |G|^\alpha + 1 \Longleftrightarrow G \text{ is a simple group}$$

where $G \in \mathcal{G}$, and α is a complex number. Also, we know that any finite abelian group G has a (normal) subgroup of order d for every divisor d of $|G|$, and G has exactly one such subgroup for every divisor d if and only if G is cyclic. Therefore, for any abelian group $G \in \mathcal{G}$, we have $\sigma_\alpha(G) \geq \sigma_\alpha(|G|)$, and the equality holds if and only if G is cyclic.

Definition 4.9.8. A group G is said to be *covered by a collection of subgroups* if each element of the group belongs to atleast one subgroup in the collection.

In our context:

Let $G \in \mathcal{G}$. If $G = \bigcup_{H_i \leq G} H_i$, then G is said to be covered by H_i's. $\{H_i : H_i \leq G\}$ is called a *covering* of G. If $G = \bigcup_{H_i < G} H_i$, then $\{H_i : H_i < G\}$ is called *non trivial covering*, otherwise *trivial.*

Theorem 4.9.9. [16] *A group has a finite non trivial covering by subgroups iff it has a finite non cyclic quotient. i.e., for finite G*

$$G = \bigcup_{H<G} H \text{ if and only if } G \text{ has a finite non cyclic quotient.}$$

Fact 4.9.10. From the above theorem we can say that if $G \neq \bigcup_{H<G} H$ then every quotient of G is cyclic.

Fact 4.9.11. In particular if $G \in \mathcal{G}$ such that $G \neq \bigcup_{N \lhd G} N$ then every abelian quotient of G is cyclic.

Lemma 4.9.12. *Let $G \in \mathcal{G}$ be such that $G = \bigcup_{N \lhd G} N$. Then $\tau(G) \geq 5$.*

Proof. Since $|N| \leq \frac{|G|}{2} \quad \forall N \lhd G$, and since the identity element of G is a common member of all normal subgroups of G, it follows that any two proper normal subgroups of G can contain at the most $|G| - 1$ distinct elements. Hence G must have atleast three proper nontrivial normal subgroups, which in turn implies that $\tau(G) \geq 5$. □

Proposition 4.9.13. *Let $G \in \mathcal{G}$. If $\sigma(G) \leq 2|G| + 2$ then $G \neq \bigcup_{N \lhd G} N$.*

Proof. Let us assume that $G = \bigcup_{N \lhd G} N$. Then, for each $g \in G$, the smallest normal subgroup N_g of G containing g is a proper normal subgroup of G, and so $G/N_g \neq \{e\}$ which means $\tau(G/N_g) \geq 2$. Therefore, by Theorem 4.7.2, we have

$$\begin{aligned}\sigma(G) =& \sum_{g \in G} \tau(G/N_g) \\ =& \tau(G/\{e\}) + \sum_{g \in G, g \neq e} \tau(G/N_g) \\ \geq& \tau(G) + 2(|G| - 1),\end{aligned}$$

since there are $|G| - 1$ numbers of non identity elements and for each of them $\tau(G/N_g) \geq 2$. Again (given)

$$\begin{aligned} & \sigma(G) \leq 2|G| + 2 \\ \Longrightarrow \quad & \tau(G) + 2(|G| - 1) \leq 2|G| + 2 \\ \Longrightarrow \quad & \tau(G) + 2|G| - 2 \leq 2|G| + 2 \\ \Longrightarrow \quad & \tau(G) \leq 4,\end{aligned}$$

a contradiction. Hence $G \neq \bigcup_{N \lhd G} N$. □

We have the following corollary to the above proposition, which is also an improvement to the *abelian quotient theorem.*

Corollary 4.9.14. *If G is a finite group with $\sigma(G) \leq 2|G| + 2$ then every abelian quotient of G is cyclic.*

Proof. In view of Fact 4.9.11, the proof is immediate. □

Remark 4.9.15. If $q : G \longrightarrow G'$ is a homomorphism of groups $G, G' \in \mathcal{G}$ then $\tau(q(G)) \leq \tau(G)$, since $q^{-1}(M) \trianglelefteq G \quad \forall\ M \trianglelefteq q(G)$. In particular, we have $\tau(G/N) \leq \tau(G) \quad \forall\ G \in \mathcal{G}$ and $\forall\ N \trianglelefteq G$; moreover, the inequality is strict if N is nontrivial.

Theorem 4.9.16. [16]. *A group has a nontrivial finite covering by normal subgroups if and only if it has a quotient isomorphic to an elementary abelian p-group of rank two for some prime p.*

Proposition 4.9.17. *Let $G \in \mathcal{G}$ be such that $\tau(G) = 5$ and $G = \bigcup_{N \lhd G} N$. Then $G = C_2 \times C_2$.*

Proof. By the above Theorem, there is a normal subgroup of G such that $G/N = C_p \times C_p$ for some prime p. So,

$$\begin{aligned} \tau(G/N) &= \tau(C_p \times C_p) = p + 3 \\ \Longrightarrow \tau(G) &\geq p + 3, \text{ since } \tau(G) \geq \tau(G/N), \\ \Longrightarrow p = 2 &\Longrightarrow N = \{e\}, \end{aligned}$$

otherwise $5 = \tau(G) > \tau(G/N) = p + 3 = 5$ which is absurd. Hence the proposition follows. □

The Proposition tells us that if $G \neq C_2 \times C_2$ then the hypothesis of the above Corollary can be further improved to $\sigma(G) \leq 2|G| + 3$.

4.10 Examples of Perfect Groups

In this section we study some examples of perfect groups among some of the well-known families of finite groups. As mentioned earlier a finite group G is

said to be *perfect* if $\sigma(G) = 2|G|$.

For example let C_n be the *cyclic group* of order n. Then C_n has exactly one normal subgroup of order d for each divisor d of n, so $\sigma(C_n) = \sigma(n)$, and C_n is perfect just when n is perfect. Thus perfect groups provide a generalization of the concept of perfect numbers, and C_6, C_{28}, C_{496} are all perfect groups.

Remark 4.10.1. None of the *symmetric groups* S_n or *alternating groups* A_n is perfect. If $n \geq 5$ then A_n is simple and the only normal subgroups of S_n are $1, A_n$ and S_n. So $\sigma(A_n) \neq 2|A_n|$ and $\sigma(S_n) \neq 2|S_n|$. For $n \leq 4$, we have

$$\begin{aligned} \sigma(A_1) &= 1, & \sigma(S_1) &= 1, \\ \sigma(A_2) &= 1, & \sigma(S_2) &= 1+2 = 3, \\ \sigma(A_3) &= 1+3 = 4, & \sigma(S_3) &= 1+3+6 = 10, \\ \sigma(A_4) &= 1+4+12 = 17, & \sigma(S_4) &= 1+4+12+24 = 41. \end{aligned}$$

Remark 4.10.2. A (finite) *p-group* is a group of order p^r, where p is prime and $r \geq 0$. Lagrange's Theorem says that the order of any subgroup of a group divides the order of the group, so if G is a p-group then $\sigma(G) \equiv 1 \pmod{p}$. Hence no p-group is perfect.

Remark 4.10.3. The perfect *dihedral* groups are in one-to-one correspondence with the odd perfect numbers [25]. So it is an open question whether there are any perfect *dihedral* groups at all.

The following Theorem is a corollary of the Theorem 4.8.1, and is a direct analogue of Theorem 1.12.14.

Theorem 4.10.4. *σ is multiplicative.*

Proof. If G_1 and G_2 are coprime, then

$$\begin{aligned}\sigma(G_1 \times G_2) &= \sum_{N_1 \trianglelefteq G_1, N_2 \trianglelefteq G_2} |N_1 \times N_2| \\ &= \sum_{N_1 \trianglelefteq G_1} \sum_{N_2 \trianglelefteq G_2} |N_1||N_2| \\ &= \sum_{N_1 \trianglelefteq G_1} |N_1| \sum_{N_2 \trianglelefteq G_2} |N_2| \\ &= \sigma(G_1)\sigma(G_2).\end{aligned}$$

□

4.10.1 Some examples of non-abelian perfect groups (Even Order)

Example 4.10.5. $S_3 \times C_5$. The group $S_3 \times C_5$ of order 30 is perfect. For S_3 and C_5 have coprime orders (6 and 5), so are coprime. Now

$$\sigma(S_3 \times C_5) = \sigma(S_3)\sigma(C_5) = (1+3+6)(1+5) = 60 = 2|S_3 \times C_5|.$$

We present the next two examples along with the method by which they were found.

Example 4.10.6. $A_5 \times C_{15128}$. The group $A_5 \times C_{15128}$ of order 907680 is perfect. Firstly A_5 is simple of order $5!/2 = 60$ and $\sigma(A_5) = 1 + 60 = 61$. Let us try to find a perfect group G of the form $G = A_5 \times G_1$, where G_1 is

some group prime to A_5. Now $A_5 \times G_1$ is perfect. Therefore,

$$\sigma(A_5 \times G_1) = 2|A_5 \times G_1|$$
$$\Longrightarrow \sigma(A_5)\sigma(G_1) = 2|A_5||G_1|$$
$$\Longrightarrow \frac{\sigma(G_1)}{|G_1|} = \frac{2|A_5|}{\sigma(A_5)} = \frac{120}{61}. \tag{4.10.a}$$

Therefore our G_1 should be such that it satisfies (4.10.a). Let us look for such a group G_1 amongst those of the form $G_1 = C_{61} \times G_2$, where G_2 is prime to C_{61} and A_5. Now $A_5 \times C_{61} \times G_2$ is perfect. Therefore

$$\sigma(A_5)\sigma(C_{61})\sigma(G_2) = 2|A_5||C_{61}||G_2|$$
$$\Longrightarrow \frac{\sigma(G_2)}{|G_2|} = \frac{2|A_5||C_{61}|}{\sigma(A_5)\sigma(C_{61})} = \frac{2 \cdot 60 \cdot 61}{61 \cdot 62} = \frac{60}{31}. \tag{4.10.b}$$

Therefore our G_2 should be such that it satisfies (4.10.b). Similarly let us look for such a group G_2 amongst those of the form $G_2 = C_{31} \times G_3$, where G_3 is prime to C_{31}, C_{61} and A_5. Again $A_5 \times C_{61} \times C_{31} \times G_3$ is perfect. Therefore

$$\sigma(A_5)\sigma(C_{61})\sigma(C_{31})\sigma(G_3) = 2|A_5||C_{61}||C_{31}||G_3|$$
$$\Longrightarrow \frac{\sigma(G_3)}{|G_3|} = \frac{2|A_5||C_{61}||C_{31}|}{\sigma(A_5)\sigma(C_{61})\sigma(C_{31})} = \frac{2 \cdot 60 \cdot 61 \cdot 31}{61 \cdot 62 \cdot 32} = \frac{15}{8}. \tag{4.10.c}$$

Therefore our G_3 should be such that it satisfies (4.10.c). Such G_3 is C_8, and the groups A_5, C_{61}, C_{31} and C_8 are pairwise coprime. Thus if

$$G = A_5 \times C_{61} \times C_{31} \times C_8 = A_5 \times C_{61 \times 31 \times 8} = A_5 \times C_{15128},$$

then G is perfect.

Example 4.10.7. $A_6 \times C_{366776}$. The group $A_6 \times C_{366776}$ of order 132039360 is perfect. This time, we start with the simple group A_6 of order $6!/2 = 360$. We have $\sigma(A_6) = 1 + 360 = 361$. Let us try to find a perfect group G of the form $G = A_6 \times G_1$ where G_1 is some group prime to A_6. Now $A_6 \times G_1$ is perfect. Therefore,

$$\begin{aligned} \sigma(A_6)\sigma(G_1) &= 2|A_6||G_1| \\ \implies \frac{\sigma(G_1)}{|G_1|} &= \frac{2|A_6|}{\sigma(A_6)} = \frac{720}{361}. \end{aligned} \tag{4.10.d}$$

Therefore our G_1 should be such that it satisfies (4.10.d). Let us look for such a group G_1 amongst those of the form $G_1 = C_{361} \times G_2$, where G_2 is prime to C_{361} and A_6. Now $A_6 \times C_{361} \times G_2$ is perfect. Therefore

$$\begin{aligned} \sigma(A_6)\sigma(C_{361})\sigma(G_2) &= 2|A_6||C_{361}||G_2| \\ \implies \frac{\sigma(G_2)}{|G_2|} &= \frac{2|A_6||C_{361}|}{\sigma(A_6)\sigma(C_{361})} = \frac{2 \cdot 360 \cdot 361}{361 \cdot (1 + 19 + 361)} = \frac{240}{127}. \end{aligned} \tag{4.10.e}$$

(note that $361 = 19^2$ and 127 is prime.) Therefore our G_2 should be such that it satisfies (4.10.e). Similarly let us look for such a group G_2 amongst those of the form $G_2 = C_{127} \times G_3$, where G_3 is prime to C_{127}, C_{361} and A_6. Again $A_6 \times C_{361} \times C_{127} \times G_3$ is perfect. Therefore

$$\begin{aligned} \sigma(A_6)\sigma(C_{361})\sigma(C_{127})\sigma(G_3) &= 2|A_6||C_{361}||C_{127}||G_3| \\ \implies \frac{\sigma(G_3)}{|G_3|} &= \frac{2|A_6||C_{361}||C_{127}|}{\sigma(A_6)\sigma(C_{361})\sigma(C_{127})} = \frac{2 \cdot 360 \cdot 361 \cdot 127}{361 \cdot 381 \cdot 128} = \frac{15}{8}. \end{aligned} \tag{4.10.f}$$

Therefore our G_3 should be such that it satisfies (4.10.f). Such G_3 is C_8, and the groups A_6, C_{361}, C_{127} and C_8 are pairwise coprime. Thus if

$$G = A_6 \times C_{361} \times C_{127} \times C_8 = A_6 \times C_{361 \times 127 \times 8} = A_6 \times C_{366776},$$

then G is perfect.

Few more examples of nonabelian perfect groups:

Consider the generalized quaternion group $\mathbb{Q}_{4m}$ of order $4m, m \geq 2$, given by

$$\mathbb{Q}_{4m} =< a, b \mid a^{2m} = 1, b^2 = a^m, bab^{-1} = a^{-1} > .$$

Theorem 4.10.8. *If m is odd then the proper normal subgroups of $\mathbb{Q}_{4m}$ are precisely the subgroups of the cyclic group generated by a.*

Proof.

$$\mathbb{Q}_{4m} = \{1, a, a^2, \ldots, a^{2m-1}, b, ab, a^2b, \ldots, a^{2m-1}b\}.$$

We have

$$bab^{-1} = a^{-1} \Longrightarrow ba = a^{-1}b \Longrightarrow aba^{-1} = ba^{-2} \tag{4.10.g}$$

Also

$$bab^{-1} = a^{-1} \Longrightarrow ba^ib^{-1} = a^{-i} \Longrightarrow ba^i = a^{-i}b \Longrightarrow a^iba^i = b \ \forall\, i \in \mathbb{Z}. \tag{4.10.h}$$

Let $N \trianglelefteq < a >$ and $a^kb^l, k = 0, 1, \ldots, 2m-1;\ l = 0, 1$ be any element of $\mathbb{Q}_{4m}$.

If $l = 0$, then clearly $a^ka^ja^{-k} \in N,\ \forall\, a^j \in N\ ;\ j = 0, 1, \ldots, 2m-1$.

If $l = 1$, then by (4.10.h), $a^kba^jb^{-1}a^{-k} = a^ka^{-j}a^{-k} = a^{-j} \in N\ ,\ \forall\, a^j \in N$.

Therefore $N \lhd \mathbb{Q}_{4m}$.

Next let N be a normal subgroup of $\mathbb{Q}_{4m}$ such that $a^ib \in N$ for some $i \geq 0$. Then by (4.10.h)

$$a^m = b^2 = a^iba^ib = (a^ib)(a^ib) \in N.$$

Again

$$a^{2i+m} = (a^ib)(ba^i) = (a^ib)b(a^ib)b^{-1} \in N.$$

It follows $a^{2i} \in N$. Let $d = \gcd(2i, m)$. Then $d = 2ix + my$ for some $x, y \in \mathbb{Z}$. So

$$a^d = a^{2ix+my} = (a^{2i})^x (a^m)^y \in N.$$

Note that, since m is odd, d is also odd. Therefore $d|i$ and hence $a^i \in N$ forcing $b \in N$ and so $aba^{-1} \in N$. Now by (4.10.g)

$$aba^{-1} \in N \Longrightarrow ba^{-2} \in N \Longrightarrow a^2b^{-1} \in N \Longrightarrow a^2 \in N.$$

Since d is odd therefore gcd $(d, 2) = 1$ and so $a \in N$. Hence $N = \mathbb{Q}_{4m}$. □

The following is a direct corollary of the above theorem.

Corollary 4.10.9. $\sigma(\mathbb{Q}_{4m}) = 4m + \sigma(2m)$ *if m is odd.*

Using multiplicativity of σ one can see that the non abelian groups $\mathbb{Q}_{12}, \mathbb{Q}_{20} \times C_{19}, \mathbb{Q}_{28} \times C_{13}, \mathbb{Q}_{244} \times A_5 \times C_{43} \times C_{11}$ and $\mathbb{Q}_{220} \times C_{109}$ are all perfect groups.

We conclude the dissertation with the following unsolved problems:

Problem 1 : To develop a group theoretic analogue of Wilson's theorem, namely, if p is a prime then $(p-1)! \equiv -1 \pmod{p}$.

Problem 2 : Is there any H with $|H| = a$ such that $\left(\frac{a}{G}\right) = \left(\frac{n^*}{H}\right)$ where $n^* = (-1)^{\frac{n-1}{2}} n$, n odd integer ?

Problem 3 : Suppose a, n are positive integers such that gcd $(a, n) = 1$ and G, H are finite groups of order n and a respectively. Is there any relation between $\left(\frac{a}{G}\right)$ and $\left(\frac{n}{H}\right)$?

Problem 4 : Given two finite groups G and H, which positive integers a satisfy $\left(\frac{a}{G}\right) = \left(\frac{a}{H}\right)$?

Problem 5 : If G is a finite group then for which positive integers n we have

(i) $\left(\frac{n}{G}\right) = \left(\frac{n+1}{G}\right)$,

(ii) $\left(\frac{n-1}{G}\right) = \left(\frac{n}{G}\right) = \left(\frac{n+1}{G}\right)$.

Problem 6 : To study all groups G for a given value of $\tau(G)$.

Problem 7 : To study in detail under what condition a finite group has a normal generator.

Problem 8 : To study the decomposibility of any non abelian group using various multiplicative functions.

Bibliography

[1] C. J. Smyth, *A coloring proof of a Generalization of Fermat's Little Theorem*, Amer. Math. Monthly **93** (6) (1986), 469–471.

[2] J. B. Fraleigh, *A first course in abstract algebra* (Third Edition), Addison-Wesley Publishing Company, Inc., USA, 1982.

[3] M. R. Pournaki, *An extension of a result of Gauss to finite groups: A linear algebraic approach*, Elem. Math. **61** (1) (2006), 24–31.

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

[5] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, (Fifth Edition), John Wiley and Sons, Inc., New York, 2001.

[6] J. Zhang, *Arithmetical conditions on element orders and group structure*, Proc. Amer. Math. Soc. **123** (1) (1995), 39–44.

[7] E. Cohen, *Arithmetical functions of finite abelian groups*, Math. annalen **142** (1961), 165–182.

[8] R. Narasimhan, S. Raghavan, S. S. Rangachari, S. Lal, *Algebraic Number Theory*, Mathematical Pamplets 4, T.I.F.R. 1966.

[9] P. Samuel, *Algebraic Theory of Numbers* (trans. A. J. Silberger) Houghton Mifflin, Boston, 1970.

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

[11] N. Jacobson, *Basic Algebra, vol I* (W. H. Freeman and Company, U.S.A., 1974).

[12] I. M. Isaacs, *"Character Theory of Finite Groups"*, Dover Publications, Inc., New YorK, 1994.

[13] Ya. G. Berkovich, E. M. Zhmud', *Characters of finite groups. Part 1*, (Translations of Mathematical Monographs), Volume 172, American Mathematical Society.

[14] J. B. Dence and T. P. Dence, *Cubic and quartic residues modulo a prime*, Missouri j. math.sci. **7** (1995), 24–31.

[15] M. S. Lucido and M. R. Pournaki, *Elements with square roots in finite groups*, Algebra Colloq. **12** (4) (2005), 677–690.

[16] M. A. Brodie, R. F. Chamberlain and L. C. Kappe, *Finite coverings by normal subgroups*, Proc. Amer. Math. Soc. **104** (3) (1988), 669–674.

[17] A. Mann, *Finite groups containing many involutions*, Proc. Amer. Math. Soc. **122** (2)(1994), 383–385.

[18] P. S. Delsarte, *Fonctions de Möbius sur les groupes abeliens finis*, Annals of Math. **49** (3) (1948), 600–609.

[19] I. M. Isaacs and M. R. Pournaki, *Generalizations of Fermat's Little Theorem via group theory*, Amer. Math. Monthly **112** (8) (2005), 734–740.

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

[21] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer International Student Edition, (Narosa Publishing House, New Delhi, 1993).

[22] E. Zolotarev, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouv. Ann. Math (2), **11** (1872), 354–362.

[23] A. K. Das, *On arithmetic functions of finite groups*, Bull. Austral. Math. Soc. **75** (2007), 45–58.

[24] A. K. Das, *On group elements having square roots*, Bull. Iranian Math. Soc., **31(2)**, (2005), 33–36.

[25] T. Leinster, *Perfect numbers and groups*, arXiv:math.GR/0104012v1 Apr 2001.

[26] W. Duke and K. Hopkins, *Quadratic reciprocity in a finite group*, Amer. Math. Monthly **112** (3) (2005), 251–256.

[27] F. Menegazzo, *The number of generators of a finite group*, Irish Math. Soc. Bulletin. **50** (2003), 117–128.

[28] I. N. Herstein, *Topics in Algebra*, (Second Edition), Wiley Eastern Limited.(2006)

BRIEF BIO-DATA

1. Name:	SEKHAR JYOTI BAISHYA
2. Sex:	Male
3. Date of birth:	1^{st} January, 1978.
4. Father's Name:	Late. Umesh Chandra Baishya
5. Nationality:	Indian
6. Permanent Address:	Vill - Birubari, P.O. - Gopinath Nagar Dist. - Kamrup, Assam, Pin - 781 016.
7. Academic Qualification:	M. Sc. in Mathematics, Gauhati University.

8. Seminar/Workshop attended:

(i) Symposium on *Some recent advances in Mathematics*, organised by the Department of Mathematics, NEHU Shillong, from 4^{th} to 5^{th} April, 2007.

(ii) North East School on *Computational geometry*, jointly organised by ISI Kolkata, and St. Anthony's College, Shillong, from 1^{st} to 3^{rd} November, 2007.

(iii) Advanced Instructiional School on *Algebraic and analytic number theory*, organised by HRI Allahabad, from 3^{rd} to 28^{th} December, 2007.

(iv) *CMFT Workshop 2008*, organised by IASST Guwahati, from 3^{rd} to 10^{th} January, 2008.

(v) International Workshop and Conference on *Surface mapping class groups and related topics*, organised by the Department of Mathematics, NEHU Shillong, from 16^{th} to 28^{th} June, 2008.