POWERS IN FINITE GROUPS OF LIE TYPE

A thesis
submitted in partial fulfillment of the requirements
of the degree of

Doctor of Philosophy

by

Rijubrata Kundu
ID: 20163480

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH PUNE

February, 2021

Dedicated to
Maa

Certificate

Certified that the work incorporated in the thesis entitled "*Powers in Finite Groups of Lie Type*", submitted by *Rijubrata Kundu* was carried out by the candidate, under my supervision. The work presented here or any part of it has not been included in any other thesis submitted previously for the award of any degree or diploma from any other university or institution.

Date: February 8, 2021

Dr. Anupam Kumar Singh
Thesis Supervisor

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that violation of the above will be cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Date: February 8, 2021

Rijubrata Kundu
Roll Number: 20163480

Acknowledgements

To my eternal love and my life coach, my late mother, Smt. Pratibha Kundu - I hope I have made you proud.

First and foremost, I would like to express my sincere gratitude to my thesis supervisor Dr. Anupam Singh for the continuous support, for his patience, motivation, enthusiasm and encouragement. He was always ready to discuss with me. He trusted my ability and was patient enough to explain anything to me. I could not have imagined having a better guide for my Ph.D. The questions studied in this thesis are formulated by him.

Besides my supervisor, I would like to thank the rest of my research advisory committee: Prof. Amit Kulshrestha and Dr. Vivek Mohan Mallick for their insightful comments and encouragement. I also take this opportunity to sincerely thank the two reviewers of this thesis whose valuable comments and suggestion helped to improve this exposition. I had the opportunity to talk mathematics with several people. I would like to thank them for their support and encouragement. In particular, I would like to thank Prof. B. Sury, Prof. Amritanshu Prasad and Prof. Amit Kulshrestha.

I owe my understanding of mathematics to many mathematicians at IISER Pune, especially to Dr. Debarghya Banerjee, Dr. Chandrasheel Bhagwat, Dr. Vivek Mohan Mallick, Dr. Supriya Pisolkar, Dr. Manish Mishra and, Dr. Kaneenika Sinha. I am grateful to all of them. I am thankful to NBHM for the financial support in the form of the research fellowship. I would like to acknowledge the support of the institute and its administrative staff members for their cooperation, special thanks are due to Mrs. Suvarna Bharadwaj, Mr. Yogesh, Mr. Tushar Kurulkar and Mrs. Sayalee Damle.

I express my gratitude to the professors of mathematics in IIT Guwahati for their valuable guidance throughout my MSc tenure. Special thanks goes to Prof. Anupam Saikia and Dr. Anjan Chakrabarty for their continuous support and motivation. I am also grateful to the professors of mathematics in my college RKMRC Narendrapur for teaching me the fundamentals of the subject. Especially

to Dr. Nurul Islam, Dr. Nanigopal Mondal, Dr. Parthasarathi Mukhopadhyay, Parthapratim Basu and, Dr. Bijoy Bera. My heartfelt thanks goes to the teachers of my school who have played an important role in my learning process, especially, Ratul Sir due to whom I got interested in mathematics at the first place. A special mention to Kakali ma'am. I thank all of you for having faith in me and guiding me in the right direction.

I thank all my school friends, batchmates in RKMRC Narendrapur, IIT Guwahati and IISER Pune, with whom I shared good times and bad times as well. Many of you will recognize yourselves, and I hope that you will forgive me for not naming you individually. I thank my friends in IIT Guwahati, in particular, Shamik, Shyam, Somenath, Sourav, Sayani, Pranali, Prerona and Shubha. I thank my friends in IISER Pune, especially Kartik, Basudev, Dada, Arijeet, Ramya, Deb, Neha, Dilpreet, Uday, Parul, Sushil da, and others for their help and discussions. A special mention to Dr. Sushil Bhunia, Dr. Dilpreet Kaur and Dr. Parul Gupta. It was fantastic to have the opportunity to discuss mathematics with them. I also thank my dear friends Sumit and Nilanjana, and Arunabha. A special mention goes to my friend Saikat who has been a true friend ever since we met in IISER Pune. I also thank my football team-mates in IISER Pune from the bottom of my heart. Playing with them has given me nothing but happiness.

Finally, I must express my deepest gratitude to my parents, grand parents and sister for providing me with unconditional support and constant encouragement throughout my years of study and through the process of research, writing this thesis and my life in general, without whom this thesis would not have existed. I am also grateful to Rana da and my true school friends Sohan and Nilanjan for all the support. I thank my tiny nieces Aahi and Tuhi. You two have been a source of love and joy ever since you existed. Last but not the least a special mention to Sudipa whose contributions cannot be expressed in words.

Rijubrata Kundu

Contents

Abstract

In this thesis, we study the image of the power map on finite reductive groups. Let G be a connected reductive algebraic group over an algebraically closed field k, of characteristic p. Let G be defined over $\mathbb{F}_q$, where q is a power of p and F be a Steinberg endomorphism of G. Let $M \geq 2$ be an integer. The power map $\omega_M : G(\mathbb{F}_q) \to G(\mathbb{F}_q)$ is defined by $g \mapsto g^M$, where $G(\mathbb{F}_q) = G^F$ is the corresponding finite group of Lie type. Denote the image of this map by $G(\mathbb{F}_q)^M$, which is the set of all M^{th} powers in $G(\mathbb{F}_q)$. We study the asymptotic ($q \to \infty$) of the probability that a randomly chosen element of $G(\mathbb{F}_q)$ is an M^{th} power; that is, we find $\lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|}$. Along the way we consider the related probabilities, $\frac{|G(\mathbb{F}_q)^M_{\mathrm{rg}}|}{|G(\mathbb{F}_q)|}$, $\frac{|G(\mathbb{F}_q)^M_{\mathrm{ss}}|}{|G(\mathbb{F}_q)|}$, $\frac{|G(\mathbb{F}_q)^M_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|}$, which denote the probability that a randomly chosen element from $G(\mathbb{F}_q)$ is an M^{th} power regular, semisimple, and regular semisimple element respectively and show that they are asymptotically the same.

In another direction, we study the image of the power map more explicitly in the case of $\mathrm{GL}(n, q)$, which is the group of $n \times n$ invertible matrices over $\mathbb{F}_q$. We find necessary and sufficient condition for an invertible matrix to be an M^{th} power. In an attempt to enumerate such elements, we get the generating functions for M^{th} power (i) regular and regular semisimple elements (and conjugacy classes) when $(q, M) = 1$, (ii) for semisimple elements and all elements (and conjugacy classes) when M is a prime power and $(q, M) = 1$, and (iii) for all kinds when M is a prime, and q is a power of M.

Notation

k : a field
$k^\times$: $k \setminus \{0\}$
$\bar{k}$: algebraic closure of k
$\mathbb{Z}$: integers
$\mathbb{Q}$: rational numbers
$\mathbb{R}$: real numbers
$\mathbb{C}$: complex numbers
$\mathbb{F}_q$: finite fields with q elements
R : a commutative ring with 1
$R^\times$: units of a ring R
$\cong$: isomorphism
$\deg f$: degree of a polynomial f
Φ : set of all monic irreducible polynomials $f \in \mathbb{F}_q[x]$ except the polynomial x
$N(q,d)$: number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree d
(not including the polynomial x when $d = 1$)
$\mu(r)$: Möbius function on $\mathbb{N}$
$\mathcal{Z}_G(g)$: centralizer of g in G
$\mathfrak{M}(M;q)$: order of M in $(\mathbb{Z}/M\mathbb{Z})^\times$ when $(M,q) = 1$
$Z(G)$: center of G
Aut (V) : set of all automorphisms of V
GL(V) or $GL(n,k)$: general linear group
SL(V) or $SL(n,k)$: special linear group
Sp(n,k) : symplectic group
GO(n,k) : general orthogonal group
GU(n,k) : unitary group
Gal (L/k) : Galois group of a field L over k
det(g) : determinant of a matrix g
S_n : Symmetric group in n symbols
${}^t g$: transpose of a matrix g

${}^t g^{-1}$: transpose inverse of a matrix g
$p(n)$: number of partitions of n
$\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$: diagonal matrix
$\square$: end of a proof

Chapter 1

Introduction

One of the ways to approach problems in finite group theory is to study them statistically. Erdös and Túran initiated this approach to study properties of random permutations, that is, elements of the symmetric group S_n, in a series of papers (see [ET65, ET67a, ET67b, ET68]). The study of these statistics often involves enumeration. The problem of enumeration is often challenging in the sense of obtaining precise formulas, and therefore one seeks alternate ways of counting. One of the most effective ways is to construct a generating function for the enumerative quantity in question, which serves as a vital tool to gain further information on these objects. A classic example is the study of the number of partitions of a natural number n (see for instance [And76]).

A significant part of this thesis attempts to solve the equation $X^M = g$ for any $M \geq 2$, where g is an invertible matrix with entries in the finite field $\mathbb{F}_q$ with q elements. In other words, we attempt to solve the equation $X^M = g$ in the group $\mathrm{GL}(n, q)$. A natural question to ask is how many $g \in \mathrm{GL}(n, q)$ admit a solution to the equation $X^M = g$. This can be re-framed in the language of probability as follows: What is the probability that a randomly chosen element of $\mathrm{GL}(n, q)$ is an M^{th} power or admit an M^{th} root?

The above problem has been studied quite extensively in several papers for the group S_n. For $r \geq 2$, let $S_n^r := \{\pi^r \mid \pi \in S_n\}$ be the set of all permutations π such that the equation $X^r = \pi$ has a solution in S_n. We call π, an r^{th} power in S_n, or an element which admits an r^{th} root in S_n. Thus, the probability that a randomly chosen permutation admits an r^{th} root is $P_r(n) := \frac{|S_n^r|}{n!}$. Blum studied this problem for $r = 2$ in [Blu74] and obtained generating function for $P_2(n)$ as follows:

$$1+\sum_{n=1}^{\infty} P_2(n)u^n = \left(\frac{1+u}{1-u}\right)^{1/2} \prod_{k=1}^{\infty} \cosh\left(\frac{u^{2k}}{2k}\right). \tag{1.1}$$

This generating function is constructed by using the cycle index of the symmetric group S_n, which was originally introduced by G. Pólya (see [PR87]) as follows:

$$Z_n = Z_n(t_1, t_2, \ldots t_n; S_n) = \frac{1}{n!} \sum_{\substack{\pi \in S_n \\ \text{type}(\pi) \\ =(c_1,c_2,\ldots)}} t_1^{c_1} t_2^{c_2} \ldots t_i^{c_i} \ldots \tag{1.2}$$

The polynomial Z_n in the variables $t_1, \ldots, t_n$ is called the cycle index of S_n. Here, $\text{type}(\pi) := (c_1, \ldots, c_n)$ is called the type of the permutation π. Here, c_i denotes the number of i-cycles in π. The type of π determines the conjugacy classes of S_n, for two permutations $\tau, \sigma \in S_n$ are conjugate if and only if $\text{type}(\sigma) = \text{type}(\tau)$. Observe that the type of a permutation in S_n is essentially a partition of n. The product inside the expression for Z_n is a finite product, since there exists $m \in \mathbb{N}$, such that $c_i = 0$ for all $i \geq m$. The coefficient of the monomial $t_1^{a_1} t_2^{a_2} \ldots$, where $\sum_i i a_i = n$ is equal to $\frac{|Cl(\sigma)|}{n!}$, where $\sigma \in S_n$ is such that $\text{type}(\sigma) = (a_1, a_2, \ldots)$ and, $Cl(\sigma)$ denotes the conjugacy class of σ.

Example 1.0.1. The cycle index $Z_3 = Z_3(t_1, t_2, t_3; S_3)$ of S_3 is given by $\frac{1}{6}(t_1^3 + 3t_1t_2 + 2t_3)$.

Thus, for each $n \geq 1$, we have attached a polynomial Z_n to the group S_n, which essentially is the class equation of S_n, where the sizes of the conjugacy classes are coefficients of certain monomials. The cycle index generating function is given by

$$1+\sum_{n=1}^{\infty} Z_n u^n = \prod_{i \geq 1} \exp\left(\frac{t_i u^i}{i}\right). \tag{1.3}$$

Blum (see [Blu74]) showed that $\pi \in S_n$ of type $(a_1, a_2, \ldots, a_n)$ has a square root in S_n if and only if a_{2i} is even for all i such that $2i \leq n$. Blum obtained the generating function for $P_2(n)$ (which is Equation 1.1) by substituting these conditions in the cycle index generating function suitably. He further gave an estimate of $P_2(n)$ by studying the analytic properties of the generating function as follows:

$$P_2(n) \sim K\sqrt{\frac{2}{\pi}} n^{-\frac{1}{2}}, \text{ where, } K = \prod_{k=1}^{\infty} \cosh\left(\frac{1}{2k}\right).$$

This result was further generalized for any $r \geq 2$ by Pouyanne in [Pou02] (once again by using generating functions) to obtain the following:

$$P_r(n) \underset{n\to\infty}{\sim} \frac{\eta_r}{n^{1-\frac{\varphi(r)}{r}}}$$

where φ denotes the Euler's phi function and η_r, an explicit constant.

There are several other results about $P_r(n)$, for example, a partial recursive relation involving $P_r(n)$ was proved in [BMW00]. Further, the authors proved that $P_r(n)$ is a monotonically decreasing sequence and gave a probabilistic proof of the fact that $\lim_{n\to\infty} P_r(n) = 0$. The authors in [BMW00] incorporate bijective methods to prove these results, which gives a different perspective compared to the generating function approach. For more results and estimates on powers in S_n and related ideas, we urge the reader to look at [Ben74], [BG80], [BG89], [BGHP20], [MP76], [Pav82] and, [Tur70]. The set of powers has also been studied for the alternating group A_n in [Pou09] and wreath products in [KM20].

The problem of studying statistical properties of random matrices is nothing new. The probability that a randomly chosen element of $\mathrm{GL}(n,q)$ is regular or, semisimple or, regular semisimple has been investigated in several papers using generating functions. In an effort to give a unified method to construct generating functions for solving enumeration problems in $\mathrm{GL}(n,q)$, Kung [Kun81] developed cycle index for $\mathrm{GL}(n,q)$ very similar to the construction of cycle index of S_n (see Equation 1.2 above). This was further applied by Stong [Sto88] to get several asymptotic results in that direction. We present this briefly in Chapter 5. Fulman [Ful99, Ful02] developed cycle index for other finite classical groups and also provided neat proof of some of the earlier known results for $\mathrm{GL}(n,q)$. We note that Wall [Wal99] independently obtained these results for $\mathrm{GL}(n,q)$. These works were followed up in [FNP05] by Fulman, Neumann and Praeger where they extended the earlier results to all classical groups by obtaining generating functions for the proportion of regular, regular semisimple, and semisimple elements in these groups. Britnell [Bri02, Bri06] studied this for special linear groups and unitary groups. The enumeration of conjugacy classes in the finite classical groups were done by Macdonald and Wall independently in the papers [Mac95, Wal80, Wal63], once again in the sense of generating functions. The enumeration of regular semisimple conjugacy classes in these groups were done in [FG13] using a generating function approach, although some of those results were already proved in [FJK98] without the use of generating functions. These works motivate us to frame and address certain subquestions of the original question of finding the probability that a randomly chosen invertible matrix is an M^{th} power for some fixed integer $M \geq 2$ (see Section 1.2).

From a different point of view, estimating the size of the set of M^{th} powers in a group G can be thought of as estimating the size of the image of the map $\omega_M : G \to G$ defined by $g \mapsto g^M$. The map ω_M is called a power map on the group G. These power maps are particular cases of a more general family of maps on groups called the word maps.

The word maps on finite groups of Lie type and algebraic groups have been studied extensively in the last couple of decades. Larsen, Shalev, Liebeck and Tiep, among others, have successfully addressed the Waring problem for finite simple and quasisimple groups by proving beautiful and essential results in this direction (see the excellent survey article by Shalev [Sha13] and references therein).

Let $\omega = \omega(x_1, \ldots, x_d)$ be an element (that is, a word) of the free group F_d with d generators $x_1, \ldots, x_d$. Let G be a finite group. Thus, ω is of the form $x_{i_1}^{m_1} x_{i_2}^{m_2} \ldots x_{i_r}^{m_r}$ where $i_1, \ldots, i_r \in \{1, 2, \ldots d\}$ and $m_j \in \mathbb{Z}$ for all $1 \leq j \leq r$. The word map induced by ω is,

$$\omega : G^d \to G \qquad\qquad (g_1, g_2, \ldots, g_d) \mapsto \omega(g_1, g_2, \ldots, g_d).$$

For example, consider the word $\omega = x_1^3 x_2^3$ of the free group F_2 with two generators $\{x_1, x_2\}$. This induces the map

$$\omega : G \times G \to G \qquad\qquad (g_1, g_2) \mapsto \omega(g_1, g_2) = g_1^3 g_2^3.$$

The image of the word map ω is denoted by $\omega(G)$. One of the central questions of interest regarding word maps is the following: Which words are surjective on all finite simple groups? This is the Waring problem for finite simple groups. There are several examples of words that have been shown to be surjective on all finite simple groups (and in some cases also for finite quasisimple groups). Notable among those, is the commutator word, which induces the commutator map $\omega : G \times G \to G$ defined by $\omega(g_1, g_2) = g_1 g_2 g_1^{-1} g_2^{-1}$. This was a long-standing conjecture by Ore, which was solved recently (see [LOST10]). The word $x_1^2 x_2^2$ was shown to be surjective on all finite simple groups in [LOST12]. This can be regarded as the non-commutative analogue of the Lagrange Four-Square theorem, which states that any natural number is a sum of at most four squares. More generally, it has been proved that given a non-trivial word ω, there exists $N \in \mathbb{N}$ (depending on ω), such that for all finite simple group G with $|G| \geq N$, we have $\omega(G)^2 = G$ (see [LST11]). Thus, given a word ω, any element of a finite simple group G can be written as a product of two word values if G is large enough.

The study of the word maps naturally has not been restricted only to finding

words which are surjective. For example, the power word x^2 is not surjective on any finite simple group, by virtue of the celebrated Feit-Thompson theorem. In such a case, a natural question to ask is how large is the image $\omega(G)$ with respect to the size of G. One of the most interesting results of this kind is due to Larsen (see [Lar04, Proposition 9]) which states that for any non-trivial word ω and $\epsilon > 0$, there exists r_0 such that if G is a finite simple group of Lie type of rank $> r_0$, then $|\omega(G)| > |G|^{1-\epsilon}$. Better lower bounds were achieved by Larsen and Shalev in [LS09] as follows: For every word ω, there is a number $N(\omega) = N$ such that if G is a finite simple group of Lie type of rank r which is not of type A_r or ${}^2A_r$, and $|G| \geq N$, then, $|\omega(G)| \geq \frac{c}{r}|G|$ for some absolute constant $c > 0$. It is further conjectured in [Sha13], that the above result holds for every finite simple group. This has been settled for the power word $\omega = x^M$ recently, for simple groups of Lie type A_n and ${}^2A_n$ in [GKSV19].

In this thesis, we also study the image of the power word $\omega = x^M$ on any finite group of Lie type. We prove an asymptotic result for the proportion of powers in a finite reductive group. As mentioned earlier, in the rest of the thesis we specialize over the group $\mathrm{GL}(n, q)$ and study the image of the power map, more explicitly using ideas of enumerative combinatorics. This part of the work also solves the question posed by R. Stanley (see Chapter 9) to count all matrices over finite fields which have square roots (see Exercise 180, Chapter 1 of [Sta97]).

1.1 An asymptotic result for the power map

Let G be a connected reductive group over $\bar{\mathbb{F}}_q$, where $\mathbb{F}_q$ is the finite field with q elements. Suppose G is defined over $\mathbb{F}_q$, with Steinberg endomorphism F. The set of fixed points, $G(\mathbb{F}_q) = G^F = \{x \in G \mid F(x) = x\}$ defines a finite group which is known as a finite reductive group or, a finite group of Lie type. Let $M \geq 2$ be a positive integer. We consider the power map $\omega\colon G \to G$ given by $x \mapsto x^M$. Clearly, this map is defined over $\mathbb{F}_q$. We consider the image of the set $G(\mathbb{F}_q)$ under this map, denoted as $G(\mathbb{F}_q)^M$. The elements of $G(\mathbb{F}_q)^M$ are called M-power elements of $G(\mathbb{F}_q)$. Further, we denote the set of M-power regular elements (these are elements of $G(\mathbb{F}_q)$ whose centralizer in G has minimal dimension, see Section 2.7 in Chapter 2) as $G(\mathbb{F}_q)^M_{\mathrm{rg}} = G(\mathbb{F}_q)^M \cap G(\mathbb{F}_q)_{\mathrm{rg}}$, the set of M-power semisimple elements (these are elements which are diagonalizable when G is regarded as embedded in GL, see Section 2.2 in Chapter 2) as $G(\mathbb{F}_q)^M_{\mathrm{ss}} = G(\mathbb{F}_q)^M \cap G(\mathbb{F}_q)_{\mathrm{ss}}$, and M-power regular semisimple elements as $G(\mathbb{F}_q)^M_{\mathrm{rs}} = G(\mathbb{F}_q)^M \cap G(\mathbb{F}_q)_{\mathrm{rs}}$. One of the main result of this thesis determines the asymptotic behaviour as $q \to \infty$ of the following quantities:

$$\frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|}, \frac{|G(\mathbb{F}_q)^M_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|}, \frac{|G(\mathbb{F}_q)^M_{\mathrm{ss}}|}{|G(\mathbb{F}_q)|}, \frac{|G(\mathbb{F}_q)^M_{\mathrm{rg}}|}{|G(\mathbb{F}_q)|}.$$

What we mean here is that we consider the above quantities as a set of real numbers for a fixed G and a fixed M; and study the limit points when $q \to \infty$. The main theorem is as follows:

Theorem A. Let G be a connected reductive group defined over $\mathbb{F}_q$ with Frobenius map F. Let $M \geq 2$ be an integer. Then,

$$\begin{aligned}\lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|} &= \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{\mathrm{ss}}|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{\mathrm{rg}}|}{|G(\mathbb{F}_q)|} \\ &= \sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}\end{aligned}$$

where the sum varies over non-conjugate maximal tori T in $G(\mathbb{F}_q)$, $T = T_{d_1,\ldots,d_s} \cong C_{d_1} \times \cdots \times C_{d_s}$ reflects the cyclic structure of T, the group $W_T = N_{G(\mathbb{F}_q)}(T)/T.$, and (M,d) denotes the g.c.d of M and d.

This theorem is proved in Section 6.1 of Chapter 6. In the subsequent sections of the same chapter, we find out these subsequential limits for the group $\mathrm{GL}(n,q)$ and $\mathrm{GU}(n,q)$, for M being a prime (see Proposition 6.2.3 and Proposition 6.3.2), and provide a series of examples to explain the theorem. The prerequisites to understand the proof of the main result is some basic results in the theory of finite reductive groups which we provide in Chapter 3.

Observe that when $M = 1$ in the above result, it is clear that

$$\lim_{q\to\infty} \frac{|G(\mathbb{F}_q)_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)_{\mathrm{ss}}|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)_{\mathrm{rg}}|}{|G(\mathbb{F}_q)|} = 1.$$

This is well known in the literature (see for example [JKZ13]), which essentially means that the set of regular semisimple elements in a connected reductive group forms a dense subset. Thus, our result can also be viewed as a generalization of the $M = 1$ case.

While the above result gives an asymptotic understanding (as $q \to \infty$), of the proportion of M^{th} powers in a finite reductive group, it is also necessary to understand the image of the power map more explicitly. A central question in this direction is to find sharp bounds for the proportion of M^{th} power in $G(\mathbb{F}_q)$, that is, $\frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|}$, and the related quantities (in terms of the group structure), and if possible to find the exact value as much as possible. We take this up in Chapter 7 and Chapter 8, where we try to develop some tools to answer these questions for

the group GL(n,q).

1.2 A study of the image of power map in GL(n,q)

Let $M \geq 2$ be an integer and $\mathrm{GL}(n,q)^M := \{g^M \mid g \in \mathrm{GL}(n,q)\}$ be the set of elements of GL(n,q) which are M^{th} power or, in other words, possess an M^{th} root in GL(n,q). Then, $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$ is the probability that a randomly chosen element of GL(n,q) is an M^{th} power. Further, suppose, $\frac{|\mathrm{GL}(n,q)^M_{\mathrm{rg}}|}{|\mathrm{GL}(n,q)|}$, $\frac{|\mathrm{GL}(n,q)^M_{\mathrm{ss}}|}{|\mathrm{GL}(n,q)|}$, $\frac{|\mathrm{GL}(n,q)^M_{\mathrm{rs}}|}{|\mathrm{GL}(n,q)|}$ denote the probability that a randomly chosen element of GL(n,q) is an M^{th} power regular, semisimple, or a regular semisimple element respectively. The set of M^{th} powers, GL$(n,q)^M$ of GL(n,q) is closed under conjugation and as such is a union of conjugacy classes. Let $c(n,M), c(n,M)_{\mathrm{rg}}, c(n,M)_{\mathrm{ss}}, c(n,M)_{\mathrm{rs}}$ denote the number of M^{th} power conjugacy classes, M^{th} power regular conjugacy classes, M^{th} power semisimple conjugacy classes, and M^{th} power regular semisimple conjugacy classes respectively. We intend to find out these probabilities and enumerate these classes.

We take a generating function approach to understand the set of powers in GL(n,q). As mentioned earlier a key to construct these generating functions for GL(n,q) (or, in fact for any other finite classical group) is a combinatorial description of the conjugacy classes in these groups, which gives rise to the concept of cycle index. We build these prerequisites in Chapter 4 and Chapter 5 for the group GL(n,q), as these will once again play an important role in this thesis. Before going into the discussion of powers, we quickly mention the generating functions of the regular, semisimple and regular semisimple classes (see [FG13]) and elements in GL(n,q) (see [Ful99], [Ful02], [Wal99]), for this will enable the reader to compare them with the generating functions obtained for the powers mentioned later in this chapter. As mentioned, these will once again be taken up in Chapter 5 in greater detail as a part of the prerequisites.

1.2.1 Generating functions in GL(n,q)

Let Φ be the set of all monic irreducible polynomials of $\mathbb{F}_q[x]$ except the polynomial x. Let $N(q,d)$ denote the number of monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree d. Let $c(n)_{\mathrm{rg}}, c(n)_{\mathrm{ss}}, c(n)_{\mathrm{rs}}$, and $c(n)$ denote the number of regular, semisimple, regular semisimple, and all conjugacy classes in GL(n,q) respectively. Let GL$(n,q)_{\mathrm{rg}}$, GL$(n,q)_{\mathrm{ss}}$, GL$(n,q)_{\mathrm{rs}}$ denote the collection of all regular, semisimple, and regular semisimple elements in GL(n,q) respectively.

The generating function for the number of regular classes and semisimple

classes is given as follows:

$$1+\sum_{n=1}^{\infty} c(n)_{\mathrm{rg}}u^n = 1+\sum_{n=1}^{\infty} c(n)_{ss}u^n = \prod_{d=1}^{\infty}(1-u^d)^{-N(q,d)} = \frac{1-u}{1-qu}. \tag{1.4}$$

In particular, we have $c(n)_{\mathrm{rg}} = c(n)_{ss} = q^n - q^{n-1}$.

The generating function for the number of regular semisimple classes is given by,

$$1+\sum_{n=1}^{\infty} c(n)_{\mathrm{rs}}u^n = \prod_{n=1}^{\infty}(1+u^d)^{N(q,d)} = \frac{1-qu^2}{(1+u)(1-qu)}. \tag{1.5}$$

The generating function for the number of conjugacy classes in GL(n,q) is given as follows:

$$1+\sum_{n=1}^{\infty} c(n)u^n = \prod_{i=1}^{\infty}\frac{1-u^i}{1-qu^i}. \tag{1.6}$$

Now we come to the generating function for the elements. The generating function for the proportion of regular semisimple elements in GL(n,q) is given as follows:

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{rs}}|}{|\mathrm{GL}(n,q)|}u^n = \prod_{d\geq 1}\left(1+\frac{u^d}{q^d-1}\right)^{N(q,d)}. \tag{1.7}$$

Further the generating function for the proportion of regular elements in GL(n,q) is given as follows:

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{rg}}|}{|\mathrm{GL}(n,q)|}u^n = \prod_{d\geq 1}\left(1+\sum_{j=1}^{\infty}\frac{u^{jd}}{q^{(j-1)d}(q^d-1)}\right)^{N(q,d)} \tag{1.8}$$

An alternate version of this generating function only involving infinite products can be given as follows:

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{rg}}|}{|\mathrm{GL}(n,q)|}u^n = \prod_{d\geq 1}\left(1-\frac{u^d}{q^d}\right)^{-N(q,d)}\prod_{d\geq 1}\left(1+\frac{u^d}{q^d(q^d-1)}\right)^{N(q,d)}. \tag{1.9}$$

Finally, the generating function for the proportion of semisimple elements in GL(n,q) is,

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{ss}}|}{|\mathrm{GL}(n,q)|}u^n = \prod_{d\geq 1}\left(1+\sum_{j=1}^{\infty}\frac{u^{jd}}{q^{\frac{j(j-1)}{2}d}\prod_{i=1}^{n}(q^{id}-1)}\right)^{N(q,d)}. \tag{1.10}$$

We divide the problem of studying M^{th} powers in GL(n, q) into two separate cases depending on, if M and q are coprime or not. The Jordan decomposition of elements necessitates this. For an element $g \in \mathrm{GL}(n, q)$ we can write $g = g_s g_u = g_u g_s$ uniquely, where g_s is semisimple part and g_u is unipotent part of g. Thus, $g^M = g_s^M g_u^M$. The semisimple elements are of order coprime to q, and the unipotent elements are of order a power of q. Chapter 7 entirely deals with the case $(M, q) = 1$, while Chapter 8 deals with a special case of $(M, q) \neq 1$.

1.2.2 The $(M, q) = 1$ case:

In this case, factorization of certain composed polynomials plays a pivotal role, which leads us to the definition of *"M-power"* polynomials. We study these polynomials in Section 7.1. These results eventually help us to obtain necessary and sufficient combinatorial conditions for an element to be an M^{th} power in GL(n, q).

The generating functions for regular and regular semisimple classes which are M^{th} power is given by the following:

Theorem B1. Let $M \geq 2$ be an integer and $(q, M) = 1$. For the group GL(n, q), the generating function for regular and regular semisimple classes which are M^{th} power is,

1. $1 + \sum_{n=1}^{\infty} c(n, M)_{\mathrm{rg}} u^n = \prod_{d \geq 1} (1 - u^d)^{-N_M(q,d)}$,
2. $1 + \sum_{n=1}^{\infty} c(n, M)_{\mathrm{rs}} u^n = \prod_{d \geq 1} (1 + u^d)^{N_M(q,d)}$,

where $N_M(q, d)$ is the number of monic irreducible M-power polynomials of degree d.

This is Theorem 7.3.2. We will see later that for $M = 1$, $N_M(q, d)$ is same as $N(q, d)$. Thus, we get back Equation 1.4 and Equation 1.5 by substituting $M = 1$ in (1) and (2) of the above theorem respectively.

The generating function for proportions of M^{th} power regular and regular semisimple elements is given by Theorem 7.3.3 as follows:

Theorem B2. For the group GL(n, q), and $M \geq 2$ with the condition that $(q, M) = 1$,

1. the generating function for the regular semisimple elements which are M^{th} power is

$$1 + \sum_{n=1}^{\infty} \frac{|\mathrm{GL}(n, q)^M_{\mathrm{rs}}|}{|\mathrm{GL}(n, q)|} u^n = \prod_{d \geq 1} \left(1 + \frac{u^d}{q^d - 1}\right)^{N_M(q,d)}.$$

2. The generating function for the regular elements which are M^{th} power is

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)^M_{\mathrm{rg}}|}{|\mathrm{GL}(n,q)|}u^n=\prod_{d\geq 1}\left(1+\sum_{j=1}^{\infty}\frac{u^{jd}}{q^{(j-1)d}(q^d-1)}\right)^{N_M(q,d)}$$
$$=\prod_{d\geq 1}\left(1-\frac{u^d}{q^d}\right)^{-N_M(q,d)}\prod_{d\geq 1}\left(1+\frac{u^d}{q^d(q^d-1)}\right)^{N_M(q,d)}.$$

Once again we see that substituting $M=1$ in the above result, we get back Equation 1.7, Equation 1.8, Equation 1.9 respectively, which is as expected.

To deal with semisimple elements and more general elements, we further assume $M=r^a$, where r is a prime. We get the generating function for semisimple classes and semisimple elements which are M^{th} powers, in Theorem 7.4.2 as follows:

Theorem C. Let $M=r^a$ be a prime power and $(q,M)=1$. Then, we have the following generating functions:

1. $1+\sum_{n=1}^{\infty}c(n,M)_{\mathrm{ss}}u^n=\prod_{i=0}^{a}\prod_{d\geq 1}\left(1-u^{r^id}\right)^{-N^i_M(q,d)}$.

2. $1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)^M_{\mathrm{ss}}|}{|\mathrm{GL}(n,q)|}u^n=\prod_{i=0}^{a}\prod_{d\geq 1}\left(1+\sum_{j=1}^{\infty}\frac{u^{r^ijd}}{q^{\frac{r^ij(r^ij-1)d}{2}}\prod_{t=1}^{r^ij}(q^{td}-1)}\right)^{N^i_M(q,d)}$,

where $N^i_M(q,d)$ is as defined in Section 7.1 of Chapter 7.

It will be observed once again in Section 7.1 of Chapter 7, that if $M=1$, that is, $a=0$, we must have $N^0_M(q,d)=N(q,d)$. Thus, once again putting $M=1$ in (1) and (2) of the above theorem, we get back Equation 1.4 and, Equation 1.10 as desired.

The generating function for the number of M^{th} power conjugacy classes is given in Theorem 7.5.3 as follows:

Theorem D. Let $M=r^a$, where r is a prime, and $(q,M)=1$. Then we have the following generating function,

$$1+\sum_{n=1}^{\infty}c(n,M)u^n=\prod_{j=1}^{\infty}\prod_{i=0}^{a}\prod_{d\geq 1}(1-u^{jr^id})^{-N^i_M(q,d)}.$$

We get back Equation 1.6 in this case when $M=1$.

We finally mention the generating function for $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$ when M is a prime.

Theorem E. Let $M \geq 2$ be a prime and $(M,q)=1$. Then,

$$1+\sum_{n=0}^{\infty}\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}u^n = \prod_{d\geq 1}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jd}}{q^{d\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{N_M(q,d)} \times \prod_{d\geq 1}\left(1+\sum_{n\geq 1}\sum_{\lambda\vdash n}\frac{u^{Mnd}}{q^{Md\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{\widehat{N}(q,d)},$$

where $N_M(q,d)$ denote the number of M-power monic irreducible polynomials of degree d, and $\widehat{N}(q,d)=N(q,d)-N_M(q,d)$, where $N(q,d)$ is the number of monic irreducible polynomials of degree d.

This is Theorem 7.5.5. We study this generating function in further detail in Section 7.6. We obtain the exact value of $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$ when M is prime and n is *"sufficiently small"*. We prove the following:

Theorem F. Let M be a prime and $(M,q)=1$. Let $t=\mathfrak{M}(M;q)$ be the order of q in $(\mathbb{Z}/M\mathbb{Z})^\times$. Then,

$$\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}=\sum_{\substack{\lambda\vdash n\\ \lambda=1^{m_1}2^{m_2}\ldots}}\frac{1}{M^{\pi_t(\lambda)}\prod_{i\geq 1}i^{m_i}m_i!}$$

whenever $n<Mt$ and $\pi_t(\lambda)$ denotes the number of parts of λ divisible by t, that is, $\pi_t(\lambda)=\sum_{t|i}m_i$.

This is Theorem 7.6.1. We further conjecture an upper bound for $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$ in Question 7.6.16 (when $n\geq Mt$).

1.2.3 A particular case of $(M,q)\neq 1$

We deal with the case $(M,q)\neq 1$ in Chapter 8. To make it a little simpler we assume, M is a prime and q is a power of M. We obtain a combinatorial criterion for an invertible matrix to possess an M^{th} root in Theorem 8.1.4. It is then immediately clear from this characterization that any semisimple elements possess a M^{th} root. Further, any regular element is a M^{th} power if and only if it is regular semisimple. We obtain a generating function for the number of M^{th} power conjugacy classes in $\mathrm{GL}(n,q)$ as follows:

Theorem G. Let M be a prime and q be a power of M. The generating function for M^{th} power conjugacy classes in GL(n, q) is,

$$1 + \sum_{n=1}^{\infty} c(n, M)u^n = \prod_{d\geq 1} \left(\prod_{k\geq 1} \frac{1 + u^{d(kM-1)} + \cdots + u^{d(kM-(M-1))}}{1 - u^{dkM}} \right)^{N(q,d)}$$

where $N(q, d)$ is the number of monic irreducible polynomials of degree d.

This is Theorem 8.2.1. We must mention that the $M = 2$ case was already dealt with by Miller in [Mil16]. Our work is a generalization for any prime M.

In Chapter 9, we use the combinatorial characterizations developed in Chapter 7 and Chapter 8, to compute squares and third powers in GL$(2, q)$ and GL$(3, q)$. Finally, to end this thesis, we mention further problems that arise from our investigation of powers in finite reductive groups. This is the subject of Chapter 10. We also mention a character theoretic connection related to powers in finite groups in this chapter.

Although we have already mentioned the theme of each chapter in the discussion above, we once again walk through it for the convenience of the reader.
A Chapter-wise description: A sincere effort has been made to keep this thesis as self-contained as possible. Chapter 2-5 are the basic prerequisites of this thesis which provides the necessary groundwork to understand the results and proofs in this thesis. Almost all the basic notions and results relevant to this thesis have been mentioned in these chapters. Chapter 6-9 deals with the author's research work. Finally, in Chapter 10, we mention some problems in this topic, which will give further motivation to understand this topic completely. This pretty much summarizes the thesis giving glimpses into the main results proved in various chapters.

Chapter 2

Linear Algebraic Groups

This is one of the basic chapters of this thesis, which deals with the notion of linear (or, affine) algebraic groups over an algebraically closed field. We will discuss these groups briefly in this chapter, by defining important concepts and results which are relevant to this thesis. In the next chapter, we will see that these groups can be defined over finite fields, and the results and notions here can be transferred to those groups in a systematic way. We follow the exposition in [MT11] here. We also refer the reader to the classic books [Hum75] and [Spr98] for further details. We will assume here the basic notions of algebraic geometry over an algebraically closed field (see, for example, Chapter 1 of [Har77]). Let k denote an algebraically closed field of arbitrary characteristic, throughout this chapter.

2.1 Linear Algebraic Groups - Definition and Examples

Let X be an affine variety over k, that is, an algebraic set with the induced Zariski topology (of k^n). Let $k[X]$ be the k-algebra of regular (i.e, polynomial) functions on X. If I is the vanishing (radical) ideal of X, that is,

$$I = \{f \in k[X_1, \ldots, X_n] \mid f(x_1, \ldots, x_n) = 0 \text{ for all } (x_1, \ldots, x_n) \in k^n\}$$

then $k[X] = k[X_1, \ldots, X_n]/I$, and is called the coordinate algebra, or the algebra of regular functions on X. With this, we have the following definition,

Definition 2.1.1 (Linear algebraic groups)**.** A *linear (or, affine) algebraic group* G over k is an affine variety over k such that the group operations (multiplication and inversion), that is, $\mu : G \times G \to G$ defined by $\mu(g, h) = gh$, and $i : G \to G$ defined by $i(g) = g^{-1}$ are morphisms of varieties.

Before going to several examples of algebraic groups relevant to this thesis, we define two important concepts which are, connectedness and dimension of algebraic groups.

Let X be an affine variety over k. We call X *irreducible* if X cannot be written as a union of two non-empty closed subsets. It can be proved that X is irreducible if and only if $k[X]$ is an integral domain, that is, the vanishing ideal $I(X)$ is a prime ideal. Observe that if X is irreducible then X is connected but the converse may not be true. A *Noetherian topological* space X (that is, a space X where any decreasing chain of closed subsets stabilize), can be written as a finite union of maximal irreducible closed subsets of X. These are called irreducible components of X. Since an affine variety X is Noetherian with respect to the Zariski topology, X can be written as a finite union of its irreducible components.

Suppose X is an irreducible affine variety. Let $k(X)$ be the field of fractions of $k[X]$. The dimension of X is defined as $\dim(X) := \mathrm{trdeg}_k(k(X))$, the transcendence degree of $k(X)$ over k. Alternatively, it is defined as the maximal length of descending chain of prime ideals in $k[X]$. For an arbitrary affine variety X, $\dim(X) := \max(\dim(X_1), \ldots, \dim(X_r))$, where $X = X_1 \cup \cdots \cup X_r$ is the decomposition of X into its irreducible components. Suppose G is an algebraic group. Let G° denote the irreducible component of G containing the identity 1. It is easy to show that G° is a subgroup of G. Further, the left cosets of G° are precisely the irreducible components of G. Since the cosets are disjoint, these cosets are also connected components of G. Thus, the concept of connectedness and irreducibility coincide in the case of algebraic groups. Since G is a finite union of irreducible components, we conclude that $[G : G^\circ]$ is finite, and G° is a normal subgroup of G. Finally, if H is a closed subgroup of G whose index is finite in G, then H contains G°. Since the dimension of each coset is clearly the same, we have $\dim(G) = \dim(G^\circ)$.

2.1.1 Examples of algebraic groups

We will now see some examples of linear algebraic groups.

Example 2.1.2. The additive group $G = (k, +)$ is clearly an algebraic group, with the coordinate ring $k[G] = k[T]$. This is a connected group of dimension 1. This group G is called the additive group and is denoted by $\mathbb{G}_a$.

Example 2.1.3. The multiplicative group $G = (k^\times, .)$ of k can be identified with the set $\{(x, y) \in k^2 \mid xy = 1\}$, which is an algebraic set of k^2 defined by the ideal $I = (XY - 1)$. Thus, G is an algebraic group with $k[G] = k[X, Y]/(XY - 1) =$

$k[X, X^{-1}]$. Once again G is connected and, of dimension 1. This group G is called the multiplicative group and is denoted by $\mathbb{G}_m$.

Example 2.1.4 (The general linear group over k)**.** The *general linear group over* k denoted by $\mathrm{GL}(n, k)$, is the group of all invertible matrices with entries in k, that is,

$$\mathrm{GL}(n, k) := \{A \in k^{n\times n} \mid \det A \neq 0\}.$$

We can identify $\mathrm{GL}(n, k)$ with the algebraic subset of k^{n^2+1}, given by $\{(A, y) \in k^{n^2} \times k \mid \det A \cdot y = 1\}$. Clearly, multiplication of two matrices and taking inverse of a matrix are both given by polynomials. Thus, $\mathrm{GL}(n, k)$ is an algebraic group. The coordinate ring $k[\mathrm{GL}(n, k)] = k[X_{ij}, Y \mid 1 \leq i, j \leq n]/(\det(X_{ij})Y - 1) \cong k[X_{ij} \mid 1 \leq i, j \leq n]_{\det(X_{ij})}$, where $k[X_{ij} \mid 1 \leq i, j \leq n]_{\det(X_{ij})}$ is the localization of the polynomial ring $k[X_{ij} \mid 1 \leq i, j \leq n]$ at the determinant polynomial $\det(X_{ij})$. The group $\mathrm{GL}(n, k)$ is connected (since, the coordinate ring is an integral domain) of dimension n^2.

Example 2.1.5 (The special linear group)**.** The *special linear group over* k denoted by $\mathrm{SL}(n, k)$ is the group of $n \times n$ matrices of determinant 1, that is,

$$\mathrm{SL}(n, k) = \{A \in k^{n\times n} \mid \det A = 1\}.$$

Clearly, $\mathrm{SL}(n, k)$ is an affine variety, being the vanishing set of the polynomial $\det(X_{ij}) - 1 \in k[X_{ij} \mid 1 \leq i, j \leq n]$. The multiplication and inversion are morphism of varieties, and thus $\mathrm{SL}(n, k)$ is a linear algebraic group, with $k[\mathrm{SL}(n, k)] = k[X_{ij} \mid 1 \leq i, j \leq n]/(\det(X_{ij}) - 1)$. The group $\mathrm{SL}(n, k)$ is connected of dimension $n^2 - 1$.

Example 2.1.6. Let T_n denote the group of invertible upper triangular matrices over k, that is,

$$\mathrm{T}_n := \{(a_{ij}) \in \mathrm{GL}(n, k) \mid a_{ij} = 0 \text{ for } i > j\}.$$

Let U_n denote the group of unitriangular matrices over k, that is,

$$\mathrm{U}_n := \{(a_{ij}) \in \mathrm{T}_n \mid a_{ii} = 1 \text{ for all } 1 \leq i \leq n\}.$$

Let D_n denote the group of diagonal invertible matrices over k. It is clear that each of these groups are linear algebraic groups. The determination of the coordinate ring of these groups are simple. For example, $k[\mathrm{T}_n] = k[X_{ij} \mid 1 \leq i, j \leq n]/(X_{ij} \mid i > j) \cong k[X_{ij} \mid 1 \leq i \leq j \leq n]$. Thus, T_n is connected. Similarly, U_n and D_n are both connected.

Finally, we move on to a class of examples which are the so-called classical groups. These are groups of isometries of certain non-degenerate bilinear forms on a vector space. For $n \geq 1$, let

$$K_n := \begin{pmatrix} 0 & \cdots & 1 \\ \vdots & \iddots & \vdots \\ 1 & \cdots & 0 \end{pmatrix}.$$

Define $J_{2n} := \begin{pmatrix} 0 & K_n \\ -K_n & 0 \end{pmatrix}$.

Example 2.1.7 (The symplectic group over k)**.** The *symplectic group in dimension* $2n$ *(vector space dimension) over* k is the closed subgroup of $\mathrm{GL}(2n, k)$ defined by

$$\mathrm{Sp}(2n, k) = \{A \in \mathrm{GL}(2n, k) \mid {}^tAJ_{2n}A = J_{2n}\}.$$

Given a non-degenerate alternating bilinear form on a vector space of dimension $2n$, there exists a basis of V such that the matrix of the bilinear form is J_{2n}. Thus, the above group is the group of isometries of an alternating bilinear form (also called skew-symmetric form when $\mathrm{char}(k) \neq 2$). The above symplectic group is generated by transvections (see [Gro02] for details), and thus $\mathrm{Sp}(2n, k) \leq \mathrm{SL}(2n, k)$. In fact, $\mathrm{Sp}(2, k) = \mathrm{SL}(2, k)$ and for $n > 2$, $\mathrm{Sp}(2n, k)$ is a proper subgroup of $\mathrm{SL}(2n, k)$. The group $\mathrm{Sp}(2n, k)$ is connected.

Example 2.1.8 (The odd-dimensional orthogonal groups)**.** First we assume $\mathrm{char}(k) \neq 2$. The *orthogonal group in dimension* $2n + 1$ *over* k is the closed subgroup of $\mathrm{GL}(2n + 1, k)$ defined by

$$\mathrm{GO}(2n + 1, k) = \{A \in \mathrm{GL}(2n + 1, k) \mid {}^tAK_{2n+1}A = K_{2n+1}\}.$$

The above group is the group of isometries of a symmetric bilinear form on a vector space over k of dimension $2n + 1$.

When $\mathrm{char}(k) = 2$, alternating and symmetric bilinear form coincide, thus the above group $\mathrm{GO}(2n + 1, k) \cong \mathrm{Sp}(2n, k)$. Thus, for arbitrary field, the orthogonal groups are defined using the quadratic form $f : k^{2n+1} \to k$ given by,

$$f(x_1, x_2, \ldots, x_{2n+1}) := x_1x_{2n+1} + x_2x_{2n} + \cdots + x_nx_{n+2} + x_{n+1}^2.$$

The group of isometries of the above quadratic form yields the orthogonal group as follows,

$$\mathrm{GO}(2n + 1, k) = \{A \in \mathrm{GL}(2n + 1, k) \mid f(Ax) = f(x) \text{ for all } x \in k^{2n+1}\}.$$

Note that for $\mathrm{char}(k) \neq 2$, this defines the same group as above. These groups are once again defined using polynomials and thus are linear algebraic groups.

Example 2.1.9 (The even dimensional orthogonal groups)**.** For an arbitrary field k and even dimension $2n \geq 2$, the orthogonal group is once again defined using the quadratic form $f : k^{2n} \to k$ defined by,

$$f(x_1, x_2, \ldots, x_{2n}) := x_1x_{2n} + x_2x_{2n-1} + \cdots + x_nx_{n+1}.$$

The orthogonal group is the group of isometries

$$\mathrm{GO}(2n, k) = \{A \in \mathrm{GL}(2n, k) \mid f(Ax) = f(x) \text{ for all } x \in k^{2n}\}.$$

Once again note that when $\mathrm{char}(k) \neq 2$, we have,

$$\mathrm{GO}(2n, k) = \{A \in \mathrm{GL}(2n, k) \mid {}^tAK_{2n}A = K_{2n}\}.$$

These groups are once again defined using polynomials and thus are linear algebraic groups.

Example 2.1.10 (The special orthogonal groups)**.** Suppose $\mathrm{char}(k) \neq 2$. Let $G := \mathrm{GO}(n, k)$ (in this case, it doesn't matter if one takes n to be odd or even). It is clear that if $A \in G$, then $\det(A) = \pm 1$. It can be shown that there exists $A \in G$ such that $\det(A) = -1$. The *special orthogonal group over* k, denoted by $\mathrm{SO}(n, k)$ is defined by $\mathrm{SO}(n, k) := \mathrm{GO}(n, k) \cap \mathrm{SL}(n, k)$. It is clear that $[\mathrm{GO}(n, k) : \mathrm{SO}(n, k)] = 2$. Thus, $\mathrm{GO}(n, k)$ is not connected since $G^\circ \leq \mathrm{SO}(n, q)$. In fact, it can be proved that $G^\circ = \mathrm{SO}(n, k)$. Thus, the special orthogonal group $\mathrm{SO}(n, k)$ is connected algebraic group. Similarly, one can show that $\mathrm{GO}(n, k)$ is not connected in any characteristic by exhibiting an algebraic subgroup of index 2. In characteristic 2, one uses the notion of pseudo-determinant instead of determinant. For more details we urge the reader to see [Gro02].

As a final example, we show that any finite group is also a linear algebraic group.

Example 2.1.11. Let G be a finite group. Then, G can be embedded into $\mathrm{GL}(n, k)$ using the left regular representation. Thus, G can be regarded as an affine variety (since any finite set in an affine variety is an affine variety). Thus, G is a linear algebraic group. It is clear that G is disconnected with each element being a connected component.

We end this section with one of the most important results in the theory of linear algebraic groups. We have already seen that all the examples provided here are closed subgroups of $\mathrm{GL}(n, k)$ for some n. This is true in general.

Theorem 2.1.12. *Let G be a linear algebraic group. Then, there exists $n \in \mathbb{N}$ such that G can be embedded as a closed subgroup of $\mathrm{GL}(n, k)$.*

Due to the above result, one uses the term linear algebraic group instead of affine algebraic group.

2.2 Jordan decomposition in linear algebraic groups

Let V be a finite dimensional vector space over k. Let $\mathrm{End}(V)$ denote the vector space of linear transformations on V. An element $u \in \mathrm{End}(V)$ is called unipotent if $u-1$ is nilpotent. The multiplicative version of Jordan decomposition of invertible linear maps is as follows:

Proposition 2.2.1. *For $g \in \mathrm{GL}(V)$, there exists unique $s, u \in \mathrm{GL}(V)$ such that $g = su = us$, where s is semisimple and u is unipotent.*

We call s the semisimple part and u the unipotent part of g. The above concept of Jordan decomposition can be carried out in any linear algebraic group, which is intuitive from Theorem 2.1.12.

Theorem 2.2.2 (Abstract Jordan decomposition)**.** *Let G be a linear algebraic group.*

1. *For any embedding ρ of G into $\mathrm{GL}(V)$ and for any $g \in G$, there exists $g_s, g_u \in G$ such that $g = g_s g_u = g_u g_s$, where $\rho(g_s)$ is semisimple and $\rho(g_u)$ is unipotent.*

2. *The decomposition $g = g_s g_u = g_u g_s$ is independent of the chosen embedding.*

3. *Let $\phi : G_1 \to G_2$ be a homomorphism of algebraic groups. Then $\phi(g_s) = \phi(g)_s$ and $\phi(g_u) = \phi(g)_u$.*

Definition 2.2.3. Let G be an algebraic group and $g \in G$. The decomposition $g = g_u g_s = g_s g_u$ is called the *Jordan decomposition* of g in G. The element g_s is called the *semisimple* part of g and g_u is called the *unipotent* part of G. If $g = g_u$, g is called an *unipotent* element of G. If $g = g_s$ then, g is called a *semisimple* element of G.

We have,

$$G_u := \{g \in G \mid g \text{ is unipotent}\},$$
$$G_s := \{g \in G \mid g \text{ is semisimple}\}.$$

Let G be an algebraic group consisting entirely of unipotent elements. We call such G, a unipotent group. Examples of unipotent groups are U_n, or any algebraic subgroup of U_n. The next result determines the structure of unipotent groups.

Theorem 2.2.4. *Let $G \leq \mathrm{GL}(n,k)$ be a unipotent group. Then, there exists $g \in \mathrm{GL}(n,k)$ such that $g^{-1}Gg \leq \mathrm{U}_n$.*

Corollary 2.2.5. *A unipotent linear algebraic group is nilpotent, and hence solvable.*

It is clear that $G_u \subseteq G$ is a closed subset. In general, the set $G_s \subseteq G$ consisting of the semisimple elements need not be closed. For example, in $\mathrm{GL}(n,k)$, the set of all semisimple elements is dense. In the next section, we will see that algebraic groups consisting only of semisimple elements play a major role.

2.3 Commutative and solvable algebraic groups

In this section, we mention some results on the structure of commutative algebraic groups. Furthermore, we define the notion of a torus, which plays a central role in studying the structure of algebraic groups. Finally, we state the Lie Kolchin theorem which determines the structure of solvable algebraic groups.

2.3.1 Commutative algebraic groups and tori

The structure of commutative algebraic groups is described by the following result:

Theorem 2.3.1. *Let G be a commutative algebraic group. Then, the sets G_s and G_u are closed subgroups of G and $G \cong G_s \times G_u$. Furthermore, if G is connected, both G_s and G_u are connected.*

Recall that $\mathbb{G}_m$ consists of all semisimple elements, whereas $\mathbb{G}_a$ consists of all unipotent elements, and both have dimension 1. In fact, up to isomorphism, these are the only connected groups of dimension 1. This motivates the following definition.

Definition 2.3.2. A linear algebraic group is called a *torus* if it is isomorphic to a direct product $\mathbb{G}_m \times \cdots \times \mathbb{G}_m$, that is, to D_n (see Example 2.1.6) for some $n \geq 0$.

By definition a torus is abelian, connected, and consists only of semisimple elements. In fact, we have

Proposition 2.3.3. *Let G be a commutative, connected algebraic group consisting*

entirely of semisimple elements. Then, G is a torus.

Let G be an algebraic group. Then $T \leq G$ is called a maximal torus if it is not properly contained in any larger torus of G. We end this section with a very important result on a torus, which is called the rigidity of tori.

Theorem 2.3.4. *Let G be a linear algebraic group and $T \leq G$ be a torus. Then, $N_G(T)^\circ = C_G(T)^\circ$, and $N_G(T)/C_G(T)$ is finite.*

The above result will later allow us to define the notion of a Weyl group which once again plays an important role in determining the structure of linear algebraic groups.

2.3.2 Solvable algebraic groups

We have seen that unipotent algebraic groups can be embedded inside the unitriangular group. Thus, U_n serves as the prototype for unipotent groups, which are nilpotent and hence solvable. This nice characterization is enjoyed by a larger class of groups, which are the connected solvable algebraic groups, where the group of upper triangular matrices, T_n serves as the prototype.

Theorem 2.3.5 (Lie-Kolchin)**.** *Let $G \leq \mathrm{GL}(n, k)$ be a connected solvable linear algebraic group. Then, G is conjugate to a subgroup of T_n.*

The above theorem has strong implications on the structure of G. We have the natural split exact sequence,

$$1 \to \mathrm{U}_n \to \mathrm{T}_n \to \mathrm{D}_n \to 1$$

where $\pi : \mathrm{T}_n \to \mathrm{D}_n$ is defined by,

$$\pi \begin{pmatrix} t_1 & & * \\ & \ddots & \\ 0 & & t_n \end{pmatrix} = \begin{pmatrix} t_1 & & 0 \\ & \ddots & \\ 0 & & t_n \end{pmatrix}.$$

If G is connected solvable, then $G \leq \mathrm{T}_n$ and $G_u = G \cap \mathrm{U}_n$. Thus, G_u is closed normal subgroup of G. Once again we can use the map π above, and let $T := \pi(G)$. Clearly, T is a closed connected subgroup of D_n, and hence by definition, a torus. It follows that $[G, G] \leq G_u$. We have the following structure theorem for connected solvable groups.

Theorem 2.3.6. *Let G be a connected solvable algebraic group. Then, G_u is a closed connected normal subgroup of G, and $[G, G] \leq G_u$. Moreover, all maximal tori are conjugate in G, and if T is a maximal torus of G, then $G = G_u \rtimes T$, and $N_G(T) = C_G(T)$.*

As a corollary of this, we have

Corollary 2.3.7. *Let G be a connected, solvable linear algebraic group. Then, any semisimple element of G is contained in a maximal torus and any unipotent element of G lies in a connected unipotent subgroup of G.*

2.4 G-spaces, quotients and Borel subgroup

This important section deals with quotients of linear algebraic groups. We define the concept of G-spaces for a linear algebraic group G, mention some of its properties. Consequently, we mention one of the most important results that if H is a closed, normal subgroup of G, then G/H is a linear algebraic group. This will allow us to construct more linear algebraic groups. Finally, we define one of the most important subgroups of a linear algebraic group called the Borel subgroups and mention its important properties. These subgroups play a major role in the classification of the connected reductive groups which will be defined in the next section. In this section, we need to consider affine as well as projective varieties.

2.4.1 G-spaces and quotients

In this section, we will consider the action of G on a general variety X, and see some important properties of the related quantities like orbits of the action, set of fixed points under the action, and stabilizers of points. By a variety, we mean both projective and affine variety.

The projective n-space $\mathbb{P}^n$ is defined as the set of one dimensional subspaces of k^{n+1}. Taking common zeros of a collection of homogeneous polynomials of $k[X_0, X_1, \ldots, X_n]$ as closed set defines the Zariski topology on $\mathbb{P}^n$. A projective variety is a closed subset of $\mathbb{P}^n$ carrying the induced Zariski topology.

The k-algebra of regular functions of an affine variety here needs to be replaced by a sheaf of functions as follows: For X an irreducible variety and $x \in X$, let $I(x)$ be the vanishing ideal at the point x and let $\mathcal{O}_x$ be the localization of $k[X]$ with respect to the prime ideal $I(x)$. Define $\mathcal{O}_X(U) = \bigcap_{x \in U} \mathcal{O}_x$, for $U \subseteq X$ open. Thus, $\mathcal{O}_X = \{(U, \mathcal{O}_X(U)) \mid U \subseteq X, \text{open}\}$ defines a *sheaf of functions* on X. One can show that $\mathcal{O}_X(X) = k[X]$. For a more general affine variety $X = X_1 \cup \cdots \cup X_r$, with irreducible components X_i, setting

$$\mathcal{O}_X(U) := \{f : U \to k \mid f|_{U \cap X_i} \in \mathcal{O}_{X_i}(U \cap X_i)\}$$

defines a sheaf on X. The collection of all these sheaves gives the sheaf of functions

on X.

Let $\mathbb{P}^n = \bigcup_{i=0}^{n} U_i$, where U_i consists of points in $\mathbb{P}^n$ with non-zero homogeneous coordinate, that is,

$$U_i = \{\langle (x_0, x_1, \ldots, x_n)\rangle \mid x_i \neq 0\}.$$

Then, U_i can be identified with the affine n-space k^n, via the map,

$$(x_0, \ldots, x_n) \mapsto (\tfrac{x_0}{x_i}, \ldots, \tfrac{x_{i-1}}{x_i}, \tfrac{x_{i+1}}{x_i}, \ldots, \tfrac{x_n}{x_i}).$$

The induced topology on the set U_i coincides with the Zariski topology of k^n. Thus, due to the discussions above, we have the ring $\mathcal{O}_x$ for each $x \in U_i$. Then, for $U \subseteq \mathbb{P}^n$, set $\mathcal{O}(U) := \bigcap_{x \in U} \mathcal{O}_x$. Thus, one gets the sheaf of functions as the set of pairs, $\{(U, \mathcal{O}(U) \mid U \subseteq \mathbb{P}^n\}$. The sheaf of functions for an arbitrary projective variety is defined by the restriction of the sheaves of $\mathbb{P}^n$ on the former variety.

The dimension of an irreducible projective variety is the dimension of any affine open subset. For an arbitrary projective variety one just takes the maximum dimension among the irreducible components. One can define morphism of varieties similarly as in the case of affine varieties, with necessary changes.

Example 2.4.1. Let V be a vector space over k of dimension n. For a strictly increasing sequence of positive integers, $0 < n_1 < n_2 < \cdots < n_d \leq n$, the partial flag variety $\mathcal{F}_{n_1,n_2,\ldots,n_d}$ is defined by,

$$\mathcal{F}_{n_1,n_2,\ldots,n_d} := \left\{ (V_1, V_2, \ldots, V_d) \mid \begin{array}{c} V_i \leq V,\ \dim(V_i) = n_i, \\ \text{and } V_1 \leq V_2 \leq \cdots \leq V_d \end{array} \right\}.$$

The set $\mathcal{F}_{1,2,\ldots,n}$ is called a complete flag variety. It can be proved that any partial flag variety can be embedded as a closed set of a projective variety (see Section 3.3 and Theorem 3.3.7 in [Gec03] for a proof).

We can now define a G-space.

Definition 2.4.2. Let G be a linear algebraic group. A variety X is called a *G-space* if there exists a group action $G \times X \to X$, defined by $(g, x) \mapsto g.x$ for $g \in G, x \in X$, which is also a morphism of varieties.

The following proposition mentions some important properties related to G-spaces.

Proposition 2.4.3. *Let X be a G-space. Then,*

1. *For each $x \in X$, the stabilizer $G_x := \{g \in G \mid g.x = x\}$ is a closed subgroup of G.*

2. The fixed point set $X^G := \{x \in X \mid g.x = x \text{ for all } g \in G\}$ *is closed.*

Furthermore,

Proposition 2.4.4. *Let* X *be a* G*-space. Then, every orbit* $G.x = \{g.x \mid g \in G\}$ *is open in its closure. Further, orbits of minimal dimension are closed.*

Example 2.4.5. Let G be a linear algebraic group. Consider the action of G on G by conjugation. By Proposition 2.4.3, the centralizers of elements (being stabilizers) are closed subgroups. The center $Z(G)$ is also closed.

Suppose G is a linear algebraic group. Consider an algebraic representation of G, that is, a homomorphism of algebraic groups $\rho : G \to \mathrm{GL}(V)$ where V is finite dimensional over k. Then, V is a G-space via the action $g.v = \rho_g(v)$. Furthermore, the projective space $\mathbb{P}(V)$ is also a G-space, via the action $g.\langle v\rangle = \langle \rho_g(v)\rangle$. The following theorem by Chevalley allows one to give a variety structure to G/H, where G is a linear algebraic group and H a closed subgroup of G.

Theorem 2.4.6 (Chevalley)**.** *Let* $H \leq G$ *be a closed subgroup of the linear algebraic group* G*. Then there exists an algebraic representation* $\rho : G \to \mathrm{GL}(V)$ *and a one-dimensional subspace* $W \leq V$ *such that* $H = \{g \in G \mid \rho_g(W) = W\}$*.*

Suppose G is a linear algebraic group G and $H \leq G$ be a closed subgroup. Assuming the setting of the previous theorem where we take $W = \langle v\rangle$, we see that action of G on $\mathbb{P}(V)$ restricted to the orbit of W under G (say X), makes X into a G-space. This induces a natural bijection between G/H and X, which allows us to endow G/H with the structure of a quasi-projective variety, that is, an open subset of a projective variety. We call G/H endowed with this variety structure to be the quotient space of G by H. The following is the main theorem of this subsection.

Theorem 2.4.7. *Let* $H \leq G$ *be a closed normal subgroup of a linear algebraic group* G*. Then* G/H *is an affine variety and* G/H *with the usual group structure is a linear algebraic group.*

This theorem will allow us to construct several more examples of algebraic groups.

Example 2.4.8 (Projective general linear group)**.** Let $G := \mathrm{GL}(n,k)$. $Z(G) = \{\lambda I \mid \lambda \neq 0\}$ is closed normal subgroup. Thus, $\mathrm{PGL}(n,k) := \mathrm{GL}(n,k)/Z(\mathrm{GL}(n,k))$ is a linear algebraic group called the projective general linear group.

Similarly, $\mathrm{PSL}(n,k) := \mathrm{SL}(n,k)/Z(\mathrm{SL}(n,k))$ is also a linear algebraic group. The

same can be applied to the symplectic group and special orthogonal group, which gives their corresponding projective analogues.

2.4.2 Borel subgroups

The structure of a connected solvable group is now well-understood by virtue of the Lie-Kolchin theorem, which says that a connected solvable linear algebraic group G stabilizes a flag $\mathcal{F} : 0 = V_0 \leq V_1 \leq \ldots \leq V_n = k^n$ of subspaces of k^n. For an arbitrary linear algebraic group $G \leq \mathrm{GL}(n, k)$, it is clear that a stabilizer $G_{\mathcal{F}}$ of such a flag is a solvable subgroup, and the quotient $G/G_{\mathcal{F}}$ is a quasi-projective variety. Since under the action of G, the orbits of minimal dimension are closed, one can choose a flag $\mathcal{F}$ such that $G/G_{\mathcal{F}}$ is closed, and so a projective variety. This is what motivates one to define the Borel subgroups.

Definition 2.4.9. Let G be a linear algebraic group. A *Borel subgroup* of G, say B, is a maximal closed connected solvable subgroup of G.

The next theorem is one of the main tools for proving important properties of Borel subgroups.

Theorem 2.4.10 (Borel fixed point theorem)**.** *Let G be a connected solvable algebraic group acting on a non-empty projective G-space of X. Then there exists $x \in X$ such that $g.x = x$ for all $g \in G$.*

The following theorem is the main theorem of this section.

Theorem 2.4.11. *Let G be a linear algebraic group. Then, all Borel subgroups of G are conjugate. Furthermore, if G is connected, then G/B is a projective variety for any Borel subgroup B.*

As a corollary of the above theorem, we write another very important result concerning the maximal tori. We also include a proof of this result.

Corollary 2.4.12. *Let G be a linear algebraic group. Then, all maximal tori of G are conjugate.*

Proof. Let $T \leq G$ be a maximal torus. Then, $T \leq B$ for some Borel subgroup B of G. Let $T_1 \leq B_1 \leq G$ be another maximal torus contained in another Borel B_1 of G. Since B and B_1 are conjugate, there exists $g \in G$, such that $B_1 = gBg^{-1}$. Then $gTg^{-1} \leq B_1$. By Theorem 2.3.6, we conclude that there exists $b \in B_1$, such that $bgTg^{-1}b^{-1} = T_1 \implies (bg)T(bg)^{-1} = T_1$. Thus, T and T_1 are conjugate. □

Definition 2.4.13. For a linear algebraic group G, the *rank* of the group G, is defined to be the dimension of a maximal torus. We denote the rank by $\mathrm{rk}(G)$.

At this point, we define the notion of the Weyl group of a linear algebraic group.

Definition 2.4.14. Let G be a linear algebraic group. The *Weyl group* of G is define to be the group $N_G(T)/C_G(T)$, where T is any maximal torus, $N_G(T)$ and $C_G(T)$ are the normalizer and centralizer of T in G.

Note that the Weyl group is finite by Theorem 2.3.4, and doesn't depend on the maximal torus chosen. We look at some examples of Borel subgroups and maximal tori of certain linear algebraic groups.

Example 2.4.15. Let $G := \mathrm{GL}(n,k)$. Then, T_n is a Borel subgroup of G. The group T_n is a closed connected solvable subgroup. If $H \leq G$ be any closed connected solvable subgroup, then $H \leq g\mathrm{T}_n g^{-1}$ for some $g \in G$. Further, if $\mathrm{T}_n \leq H$, it is clear that $H = \mathrm{T}_n$. For similar reasons, D_n is a maximal torus of G. Any Borel subgroup is conjugate to T_n, and any maximal torus is conjugate to D_n. Since, $\dim(\mathrm{D}_n) = n$, we have $\mathrm{rk}(G) = n$. Finally, we calculate the Weyl group of G. Take $T = \mathrm{D}_n$. Then $N_G(T)$ comes out to be the set of monomial matrices in G, that is, all those matrices which have exactly one non-zero entry in each row and each column. The centralizer $C_G(T) = T$. Therefore, the Weyl group $W = N_G(T)/T \cong S_n$. Thus, the Weyl group of $\mathrm{GL}(n,k)$ is S_n.

Example 2.4.16. When $G := \mathrm{SL}(n,k)$, for similar reasons as above, $\mathrm{T}_n \cap G$, and $\mathrm{D}_n \cap G$ are the Borel subgroup and maximal tori of G, up to conjugacy. The Weyl group of $\mathrm{SL}(n,k)$ is also S_n.

Example 2.4.17. Let $G := \mathrm{Sp}(2n,k)$ (refer to Example 2.1.7 for definition). Define $T := G \cap \mathrm{D}_{2n}$. Using definition,

$$T = \left\{ \begin{pmatrix} t_1 & & & & \\ & \ddots & & & \\ & & t_n & & \\ & & & t_n^{-1} & \\ & & & & \ddots \\ & & & & & t_1^{-1} \end{pmatrix} \mid t_i \in k^\times \right\} \leq G.$$

Clearly T is a torus and $\dim(T) = n$. Thus, $\mathrm{rk}(G) \geq n$. Let $T \leq T_1$, where T_1 is a torus of G. We have $T_1 \leq \mathrm{GL}(2n,k)$. Since T_1 is a torus, T_1 is simultaneously diagonalizable, and thus T_1 is conjugate to a subgroup of $\mathrm{Sp}(2n,k) \cap \mathrm{D}_{2n}$. But, since T is also contained in that conjugate of T_1, we conclude that $T = T_1$. Therefore, T is a maximal torus, and $\mathrm{rk}(G) = n$.

Let $B := G \cap \mathrm{T}_{2n}$. Clearly, B is a connected solvable subgroup of G. Let $B \leq B_1$ where B_1 is a Borel subgroup of G. Now, $B_1 \leq \mathrm{GL}(2n, k)$, thus by Lie-Kolchin theorem, B_1 is simultaneously triangulizable. Thus, B_1 is conjugate to a subgroup of $G \cap \mathrm{T}_{2n}$. But since B is also contained in that conjugate, we conclude that $B = B_1$. Hence, B is a Borel subgroup of G.

Similarly, one can check that $\mathrm{D}_{2n} \cap \mathrm{SO}(2n, k)$, and $\mathrm{D}_{2n+1} \cap \mathrm{SO}(2n+1, k)$ are maximal torus of $\mathrm{SO}(2n, k)$ and $\mathrm{SO}(2n+1, k)$ respectively. Similar result holds for their Borel subgroups.

To finish this section we collect some more important results involving the Borel subgroups and maximal tori.

Proposition 2.4.18. *Let G be a connected linear algebraic group and B be a Borel subgroup. Then, any automorphism of G that fixes B pointwise is identity.*

As a corollary of the above, we have

Corollary 2.4.19. *$Z(G)^\circ \subseteq Z(B) \subseteq C_G(B) \subseteq Z(G)$.*

We have already seen that T_n is a Borel subgroup of $\mathrm{GL}(n, k)$. Since k is algebraically closed, any matrix is conjugate to a upper triangular matrix. Thus, $\mathrm{GL}(n, k) = \bigcup_{g \in \mathrm{GL}(n,k)} g\mathrm{T}_n g^{-1}$. This is true in general.

Theorem 2.4.20. *Let G be a connected algebraic group, and B be a Borel subgroup of G. Then $G = \bigcup_{g \in G} gBg^{-1}$.*

The connectedness in the above theorem is necessary. If G is finite then $G \neq \bigcup_{g \in G} gHg^{-1}$ for any proper subgroup H of G. As a corollary of the above theorem, we have the following,

Corollary 2.4.21. *Let G be a connected algebraic group. Then,*

1. *Every semisimple element of G lies in a maximal torus.*
2. *Every unipotent element of G lies in a closed connected unipotent subgroup.*
3. *The maximal, closed, connected unipotent subgroups are all conjugate and they are of the form B_u for some Borel subgroup B of G.*

2.5 Reductive and semisimple algebraic groups

Finally we are in a position to define reductive and semisimple algebraic groups.

In the later part of this thesis, we will work with reductive algebraic groups over finite fields, also known as the finite groups of Lie type.

Definition 2.5.1. The maximal closed connected solvable normal subgroup of a linear algebraic group G is called the *radical* $R(G)$ of G.

Note that the radical always exists since if $H, H^{'} \leq G$ are two closed connected solvable normal subgroups of G, then so is $HH^{'}$. It is clear from the results of the previous section that $R_u(G) := R(G)_u$, is the maximal closed connected unipotent normal subgroup of G. The subgroup $R_u(G)$ is called the *unipotent radical* of G. We have the relation, $R_u(G) \leq R(G) \leq G^{\circ}$.

Definition 2.5.2. Let G be a connected algebraic group. Then, G is called a *reductive group* if $R_u(G)$ is trivial. The group G is called *semisimple* if $R(G)$ is trivial.

It is easy to see that for a connected algebraic group G, $G/R(G)$ is semisimple and $G/R_u(G)$ is reductive. We give some examples of reductive groups before moving further. First we look at a trivial non-example.

Example 2.5.3. Let G be connected solvable linear algebraic group. Then, $R(G) = G$ and, $R_u(G) = G_u$. Thus, a solvable algebraic group is semisimple if and only if it is trivial, and is reductive if and only if it is a torus.

Example 2.5.4. An abstract construction of a reductive group can be done as follows: let G be a semisimple linear algebraic group and T be a torus. Then $G \times T$ is a linear algebraic group and $R(G \times T) = T$, and hence $G \times T$ is reductive.

Example 2.5.5. Let $G := \mathrm{GL}(n, k)$. Then, clearly $R(G) \leq \mathrm{T}_n$. But since T_n^- is conjugate to T_n, where T_n^- denote the group of invertible lower triangular matrices, we conclude that $R(G) \leq \mathrm{T}_n \cap \mathrm{T}_n^- = \mathrm{D}_n$. Thus, $R_u(G)$ is trivial, and hence G is reductive. In fact it is easy to determine $R(G)$ explicitly here. We have $R(G) = Z(G) = \{\lambda I \mid \lambda \in k^{\times}\} \cong \mathbb{G}_m$. We conclude, $\mathrm{PGL}(n, k)$ is semisimple.

Example 2.5.6. Consider $G := \mathrm{SL}(n, k)$. As above, one can show, $R(G) \leq Z(G) = \{\lambda I \mid \lambda^n = 1\}$. Since $Z(G)$ is finite, we conclude, $R(G) = \{1\}$. Hence G is semisimple.

The radical $R(G)$ can be described using the Borel subgroups as follows,

Proposition 2.5.7. *Let G be a connected linear algebraic group. Then $R(G) = (\bigcap_B B)^{\circ}$, where B runs over all Borel subgroups of G.*

The following proposition describes the radical of a connected reductive group and generalizes the observations made in the above examples.

Proposition 2.5.8. *Let G be connected reductive linear algebraic group. Then,*

1. *$R(G) = Z(G)^\circ$ is a torus.*
2. *$R(G) \cap [G, G]$ is finite.*
3. *$[G, G]$ is semisimple.*

Example 2.5.9. Consider the symplectic group $G := \mathrm{Sp}(2n, k)$. It is easy to show that the center $Z(\mathrm{Sp}(2n, k)) = \{\pm I\}$. Thus, $R(G)$ is trivial, and hence G is semisimple.

Similar computations show that $\mathrm{SO}(2n, k)$ and $\mathrm{SO}(2n + 1, k)$ are also semisimple algebraic groups. We end this section with the definition of simple algebraic group.

Proposition 2.5.10. *Let G be a connected reductive group. Then,*

(a) For a subtorus $S \leq G$, the centralizer $C_G(S)$ is connected and reductive.

(b) If T is a maximal torus of G, then $C_G(T) = T$.

Definition 2.5.11. A connected linear algebraic group is called *simple* if there is no non-trivial connected closed normal subgroup.

Clearly any simple algebraic group is semisimple.

Example 2.5.12. The special linear group $\mathrm{SL}(n, k)$ is a simple algebraic group. The group $\mathrm{SL}(2, k) \times \mathrm{SL}(2, k)$ is semisimple but not simple.

2.6 Classification of reductive algebraic groups

This section deals with the classification of reductive (or, semisimple) algebraic groups over algebraically closed fields. The material in this section is not needed further in the thesis, but we provide it for completeness. Therefore, our account of the classification theorem will be made as brief as possible. We start by introducing the concept of Lie algebra of a linear algebraic group.

2.6.1 Lie algebra of a linear algebraic group

Let A be a k-algebra. A k-linear map $D : A \to A$ is called a derivation if for all $f, g \in A$, we have $D(fg) = fD(g)+gD(f)$. Let $\mathrm{Der}_k(A)$ be the set of all derivation of a k-algebra A. Then, $\mathrm{Der}_k(A)$ is a Lie algebra over k.

Let G be a linear algebraic group. For each $x \in G$, define the map $\lambda_x : k[G] \to k[G]$ defined by $\lambda_x(f)(g) = f(x^{-1}g)$ for all $f \in k[G]$ and $g \in G$. This is a k-algebra homomorphism on $k[G]$.

Definition 2.6.1 (Lie algebra of an algebraic group)**.** The *Lie algebra* of an algebraic group G is the subspace

$$\mathrm{Lie}(G) := \{D \in \mathrm{Der}_k(k[G]) \mid D\lambda_x = \lambda_x D \text{ for all } x \in G\}$$

of left invariant derivation of $k[G]$ is a Lie subalgebra of $\mathrm{Der}_k(k[G])$.

Let X be an affine variety. Then, the tangent space of X at $x \in X$ is defined by

$$T_x(X) := \{\delta : k[X] \to k \text{ linear} \mid \delta(fg) = f\delta(g) + \delta(f)g \text{ for } f, g \in k[X]\}.$$

If G is a linear algebraic group then the tangent space of G at identity which is $T_1(G)$ can be given a Lie algebra structure by the following map

$$\Theta : \mathrm{Lie}(G) \to T_1(G), \qquad \Theta(D)(f) := D(f)(1),$$

which is a isomorphism of linear maps.

Definition 2.6.2 (Differential map)**.** Let $\phi : X \to Y$ be a morphism of affine varieties. The *differential* $d_x(\phi)$ of ϕ at $x \in X$ is the map $d_x(\phi) : T_x(X) \to T_{\phi(x)}(X)$ defined by $d_x(\delta) := \delta \circ \phi^*$ for $\delta \in T_x(X)$.

If $\phi : G \to H$ is a morphism of algebraic groups, then we write $d\phi := d_1\phi : T_1(G) \to T_1(G)$. In fact, $d\phi$ is a homomorphism of Lie algebras on $\mathrm{Lie}(G)$. We also have that $\mathrm{Lie}(G) = \mathrm{Lie}(G^\circ)$ and, $\dim(G) = \dim(G^\circ) = \dim(\mathrm{Lie}(G))$.

Example 2.6.3. Let $G := \mathrm{GL}(n, k)$. Then, $\mathrm{Lie}(G) \cong \mathfrak{gl}(n, k)$ which is the lie algebra of all $n \times n$ matrices over k, with the bracket operation $[A, B] := AB - BA$ for all $A, B \in \mathfrak{gl}(n, k)$.

Example 2.6.4. Let $G := \mathrm{SL}(n, k)$. Then, $\mathrm{Lie}(G) \cong \mathfrak{sl}(n, k)$ which is the lie subalgebra of $\mathfrak{gl}(n, k)$ consisting of all $n \times n$ matrices over k with trace zero.

2.6.2 Adjoint representation of an algebraic group

Let G be an algebraic group. For $x \in G$ define the isomorphism $\mathrm{Int}_x : G \to G$ by $\mathrm{Int}_x(g) = xgx^{-1}$. The differential $d\mathrm{Int}_x : \mathrm{Lie}(G) \to \mathrm{Lie}(G)$ is a Lie algebra automorphism. Let $\mathrm{Ad}\ x := d\mathrm{Int}_x$. This defines a representation

$$\mathrm{Ad} : G \to \mathrm{GL}(\mathrm{Lie}(G)), \qquad x \mapsto \mathrm{Ad}\ x$$

which is called the *adjoint representation* of G.
The above representation is a homomorphism of algebraic groups. Furthermore, the differential of the above adjoint map

$$\mathrm{ad} = d\mathrm{Ad} : \mathrm{Lie}(G) \to \mathfrak{gl}(\mathrm{Lie}(G))$$

is a Lie algebra homomorphism and $(\mathrm{ad}(X))(Y) = [X, Y] = XY - YX$ for $X, Y \in \mathrm{Lie}(G)$. Finally, if G is a connected reductive group then $Ker(\mathrm{Ad}) = Z(G)$.

Example 2.6.5. Let $G := \mathrm{GL}(n, k)$. Then, $\mathrm{Lie}(G) \cong \mathfrak{gl}(n, k)$. Some calculations will show that for $g \in G$, $\mathrm{Ad}(g) : \mathfrak{gl}(n, k) \to \mathfrak{gl}(n, k)$ is given by $X \mapsto gXg^{-1}$ for all $X \in \mathfrak{gl}(n, k)$. Thus,

$$\mathrm{Ad} : \mathrm{GL}(n, k) \to \mathrm{GL}(\mathfrak{gl}(n, k)), \qquad g \mapsto \mathrm{Ad}\ g : \mathfrak{gl}(n, k) \to \mathfrak{gl}(n, k) \text{ given by,}$$
$$\mathrm{Ad}\ g(X) = gXg^{-1}.$$

In fact the same holds for any closed subgroup of $\mathrm{GL}(n, k)$.

2.6.3 Root space decomposition of an algebraic group

We first start with the definition of a character of an algebraic group.

Definition 2.6.6. A *character* of a linear algebraic group G is a morphism of algebraic groups $\chi : G \to \mathbb{G}_m$. The set of characters of g is denoted by $X(G)$.

A character of G can be naturally considered as an element of $k[G]$. The set $X(G)$ is an abelian group with respect to the operation $(\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g)$ for all $\chi_1, \chi_2 \in X(G)$.

Definition 2.6.7. A *cocharacter* of a linear algebraic group G is a morphism of algebraic groups $\gamma : \mathbb{G}_m \to G$. The set of cocharacter of G is denoted by $Y(G)$.

Clearly, $Y(G)$ is also an abelian group with respect to the operation $(\gamma_1 + \gamma_2)(g) = \gamma_1(g)\gamma_2(g)$ for all $\gamma_1, \gamma_2 \in X(G)$.

Example 2.6.8 (Characters and cocharacters of a torus)**.** Let $G = \mathrm{D}_n$, the torus of dimension n. Consider $\chi_i : \mathrm{D}_n \to \mathbb{G}_m$ defined by $\chi_i(\mathrm{diag}(t_1, t_2, \ldots, t_n)) = t_i$. Clearly $\chi_i \in X(\mathrm{D}_n)$. In fact any $\chi \in X(G)$ can be decomposed as $\chi_1^{a_1} \ldots \chi_n^{a_n}$ for $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$. Thus, $X(G) \cong \mathbb{Z}^n$. Similarly, for $a = (a_1, a_2, \ldots a_n) \in \mathbb{Z}^n$, the map $\gamma_a : \mathbb{G}_m \to \mathrm{D}_n$ defined by $\gamma_a(t) = \mathrm{diag}(t^{a_1}, t^{a_2}, \ldots, t^{a_n})$ is a cocharacter. Once again it can be shown that any cocharacter is of this form and hence, $Y(G) \cong \mathbb{Z}^n$.

We now describe the root space decomposition of an algebraic group G. Let G be a linear algebraic group. Let $T \leq G$ be a maximal torus and assume $\dim(T) \geq 1$, which is guaranteed if G is reductive. Let $\mathfrak{g} = \mathrm{Lie}(G)$. Recall the adjoint representation $\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g})$. The image of T under the adjoint representation $\mathrm{Ad}(T) \leq \mathrm{GL}(\mathfrak{g})$ is a set of commuting semisimple elements, so can be simultaneously diagonalized. For $\chi \in X(T)$, let

$$\mathfrak{g}_\chi = \{v \in \mathfrak{g} \mid (\mathrm{Ad}\ t)(v) = \chi(t)v \text{ for all } t \in T\}.$$

This is called the weight space in $\mathfrak{g}$ corresponding to χ. Then, $\mathfrak{g}$ decomposes into certain weight spaces as

$$\mathfrak{g} = \bigoplus_{\chi \in X(T)} \mathfrak{g}_\chi.$$

The above decomposition is called the root space decomposition of G.

Definition 2.6.9. The set of non-zero characters $\chi \in X(T)$ such that $g_\chi \neq 0$ occurring in the above decomposition is called the set of *roots* of G, denoted by $\Phi(G)$ or simply Φ.

It is clear that the size of Φ is finite as $\mathfrak{g}$ is finite dimensional. By the above definition we have,

$$\mathfrak{g} = \mathfrak{g}_0 + \bigoplus_{\chi \in \Phi} \mathfrak{g}_\chi.$$

Let G be a connected reductive group, $T \leq G$ a maximal torus of G, $\mathfrak{g} := \mathrm{Lie}(G)$ and $\Phi = \Phi(G)$. Then,

$$\mathfrak{g} = \mathrm{Lie}(T) + \bigoplus_{\chi \in \Phi} \mathfrak{g}_\chi,$$

with $\dim(\mathfrak{g}_\chi) = 1$ for $\chi \in \Phi$, and $\mathrm{Lie}(T) = \mathfrak{g}_0$. Thus we get, $\dim(G) = \dim(\mathfrak{g}) = |\Phi| + \mathrm{rk}(G)$. For a detailed result on the structure theory of connected reductive group, see Theorem 8.17 in [MT11]. We now give an example of root space decomposition.

Example 2.6.10. Let $G := \mathrm{GL}(n, k)$ with Lie algebra $\mathfrak{g} = \mathfrak{gl}(n, k)$. Let T be the diagonal maximal torus D_n. Then $\mathrm{Lie}(\mathrm{D}_n)$ is the set of all diagonal matrices over k, which is a Lie subalgebra of $\mathfrak{g}$. Let E_{ij} be the matrix whose (i, j) position is 1, all other entries are 0. Now,

$$\mathrm{Ad}(\mathrm{diag}(t_1, t_2, \ldots, t_n)) = t_i t_j^{-1} E_{ij}$$

Thus, the character $\chi_{ij} : T \to \mathbb{G}_m$ defined by $\chi_{ij}(\mathrm{diag}(t_1, t_2, \ldots, t_n)) = t_i t_j^{-1}$ corresponds to a non-zero weight space $\mathfrak{g}_{\chi_{ij}} = \langle E_{ij} \rangle$ for $1 \leq i \neq j \leq n$. Thus, we get the root space decomposition

$$\mathfrak{g} = \mathrm{Lie}(T) + \bigoplus_{1 \leq i \neq j \leq n} \langle E_{ij} \rangle$$

Thus the set of roots $\Phi(G) = \{\chi_{ij} \mid 1 \leq i \neq j \leq n\}$. We have, $|\Phi(G)| = n(n-1)$. As observed earlier all the weight spaces are of dimension 1, and $n^2 = \dim(G) = \dim(\mathrm{Lie}(T)) + |\Phi(G)| = n + n(n-1) = n^2$.

As a consequence of the structure theory of reductive groups we get the following important result,

Proposition 2.6.11. *Let G be a connected reductive group. Then $G = [G, G]R(G) = [G, G]Z(G)^\circ$.*

Since, $[G, G]$ is semisimple, the classification of reductive group boils down to the classification of semisimple algebraic groups.

2.6.4 Classification of semisimple groups

We end this section by discussing the classification of semisimple groups. We describe it very briefly. We have already seen from the root space decomposition of a connected reductive group G with respect to a maximal torus T that, we get a finite set of roots, $\Phi \subseteq X(T) = X$ (corresponding to non-zero weight spaces). Define $E := X \otimes_{\mathbb{Z}} \mathbb{R}$. The group X being a free abelian group, E is therefore a vector-space over $\mathbb{R}$ of the same dimension as the free rank of X. The group X can be naturally identified as a subgroup of E. Thus, we have $\Phi \subseteq X \subseteq E$. The set Φ along with the vector space E fits into a certain combinatorial structure called the root system.

Definition 2.6.12 (Root system)**.** A subset Φ of a finite dimensional Eucildean space E is called a *root system* if the following properties are satisfied:

(R1) Φ is finite, $0 \notin \Phi$, $\langle \Phi \rangle = E$,

(R2) if $c \in \mathbb{R}$ is such that $\alpha, c\alpha \in \Phi$, then $c = \pm 1$.

(R3) for each $\alpha \in \Phi$, the reflection $s_\alpha \in \mathrm{GL}(E)$ along α stabilizes Φ.

(R4) for $\alpha, \beta \in \Phi$, $s_\alpha(\beta) - \beta$ is an integral multiple of α.

The group $W := \langle s_\alpha \mid \alpha \in \Phi \rangle \leq \mathrm{GL}(E)$ is called the Weyl group of Φ. The dimension of E is called the rank of the root system.

With this definition the following result holds.

Proposition 2.6.13. *Let G be a connected reductive group and Φ be the set of roots (appearing in the root space decomposition). View Φ as a subset of $E := X \otimes_{\mathbb{Z}} \mathbb{R}$. Then, Φ is a root system in $\langle \Phi \rangle \leq E$. Moreover, if G is semisimple $\langle \Phi \rangle = E$.*

Thus, to a semisimple group of rank n we have attached a combinatorial data which is a root system of rank n.

There is a obvious notion of isomorphism of root systems and therefore one can classify root system of a given rank. This classification is established by attaching a graph with respect to a root system which is called the *Dynkin diagram* of the root system. The graph has restrictive properties which allows one to classify these graphs upto isomorphism. Since two root systems are isomorphic if and only if they have the same Dynkin diagram, it follows that the classification of the Dynkin diagram yields the classification of root systems. In fact, it is enough to classify connected Dynkin diagrams because of the notion of indecomposable root system.

Definition 2.6.14. A root system Φ of the Euclidean space E is called *indecomposable* if Φ cannot be written as a union of mutually orthogonal subsets.

A root system is either indecomposable or can be written as a union of indecomposable root systems (of smaller rank). The Dynkin diagram of a root system is connected if and only if it is indecomposable. Thus, to classify root system it is enough to classify indecomposable root system which in turn is achieved by classifying connected Dynkin diagrams.

It turns out that the root system is not enough to distinguish between two semisimple algebraic groups. For example - The group $\mathrm{SL}(2, k)$ and $\mathrm{PGL}(2, k)$ have the same root system (see Example 9.9, [MT11]). Thus, the cocharacters comes in to the picture, and it is possible to attach a combinatorial data to a reductive algebraic group known as the root datum (see Definition 9.10 in [MT11]). This structure has an underlying root system but have some more information which is enough to distinguish between any semisimple algebraic group (for example $\mathrm{SL}(2)$ and $\mathrm{PGL}(2)$). This is the classification theorem of semisimple groups by Chevalley.

Theorem 2.6.15 (Classification theorem for semisimple groups)**.** *Two semisimple algebraic groups are isomorphic if and only if they have isomorphic root datum. For each root datum there exists a semisimple algebraic group that realizes it. The group is simple if and only if the underlying root system of the root datum is indecomposable.*

2.7 Regular elements in connected reductive group

We finish this chapter by introducing a class of elements in a connected reductive group, known as the regular elements. These elements in some sense constitute most of the group. Let G be a connected reductive group. For $x \in G$, the centralizer $\mathcal{Z}_G(x)$ is a closed subgroup of G.

Definition 2.7.1. An element $x \in G$ is called *regular* if $\dim(\mathcal{Z}_G(x))$ is smallest possible among all the dimensions of centralizers of elements of G.

The next proposition tells how small the dimension of a centralizer can be.

Proposition 2.7.2. *Let G be connected, $x \in G$. Then,* $\dim(\mathcal{Z}_G(x)) \geq \mathrm{rk}(G)$.

The following result is one of the most important result used in this thesis. A finitary analogue of this will appear in Chapter 3, and will play a central role in proving the results in Chapter 6.

Theorem 2.7.3. *Let G be a connected reductive group and s be a semisimple element and $s \in T$, where T is a maximal torus of G. Then s is regular if and only if $\mathcal{Z}_G(s)^\circ = T$. Further, the set of all regular semisimple elements is dense in G.*

We obtain the following two corollaries,

Corollary 2.7.4. *Let G be a connected reductive group. Then, $x \in G$ is regular if and only if* $\dim(\mathcal{Z}_G(x)) = \mathrm{rk}(G)$.

Corollary 2.7.5. *Let G be a connected reductive group. Then, every regular semisimple element of G is contained in a unique maximal torus of G.*

Proof. Let $s \in G$ be regular semisimple. Let $S \in T, T'$, where T and T' are maximal tori of G. Then, by Theorem 2.7.3, $\mathcal{Z}_G(s)^\circ = T = T'$, which yields the result. □

The last corollary will also play a central role in Chapter 8. We also note that for the classical groups defined in Examples 2.1.4 - 2.1.10, the regular elements can be described completely in terms of linear algebra. We will see this for the group $\mathrm{GL}(n, k)$ in Chapter 4.

Chapter 3

Finite Groups of Lie type

This is another basic chapter in the thesis where we briefly discuss the theory (relevant to this thesis) of finite reductive groups or finite groups of Lie type. As mentioned at the beginning of Chapter 2, we will see that the theory of the finite reductive groups can be developed from the theory of linear algebraic groups over algebraically closed fields by using the famous Lang-Steinberg theorem (see Theorem 3.2.1). Let $q = p^a$ be a prime-power, and $k = \bar{\mathbb{F}}_q$ denote the algebraically closed field in characteristic p throughout this chapter. Let G denote a linear algebraic group over k unless specified otherwise. Once again we follow the exposition in Part 3 of [MT11].

3.1 Finite groups of Lie type - Definition and examples

Let $V \subseteq k^n$ be an affine variety over k defined by a set of polynomials $T \subseteq \mathbb{F}_q[T_1, \ldots, T_n]$. We say that V *is defined over* $\mathbb{F}_q$. The map $F_q : k \to k$ defined by $t \mapsto t^q$ is a field automorphism which fixes $\mathbb{F}_q$ pointwise. This is called the *Frobenius automorphism* of k. Since $I \subseteq \mathbb{F}_q[T_1, \ldots, T_n]$, it is clear that we have a well defined morphism,

$$F_q : V \to V, \qquad (v_1, \ldots, v_n) \mapsto (v_1^q, \ldots, v_n^q).$$

This is the induced map F_q on V, induced from the Frobenius automorphism F_q on k. We call this map the Frobenius morphism of V with respect to the $\mathbb{F}_q$-structure given by I. Define,

$$V^{F_q} := V(\mathbb{F}_q) := \{v \in V \mid F_q(v) = v\},$$

for the F_q-fixed points of V. It is clear that F_q is a bijective morphism, although it is not an isomorphism of varieties. Note that V^{F_q} is finite.

Example 3.1.1. Let $G := \mathrm{GL}(n,k)$. The Frobenius morphism $F_q : G \to G$ given by $(a_{ij}) \mapsto (a_{ij}^q)$, is actually a homomorphism of algebraic groups. Then, the set of F_q-fixed points,

$$\mathrm{GL}(n,k)^{F_q} = \{(a_{ij}) \in \mathrm{GL}(n,k) \mid (a_{ij}^q) = (a_{ij})\} = \mathrm{GL}(n,q)$$

is the finite group of $n \times n$ invertible matrices with entries in the field $\mathbb{F}_q$.

Let $G \leq \mathrm{GL}(n,k)$ be any F_q-stable closed subgroup. Then, the Frobenius morphism $F_q : G \to G$ is a homomorphism of algebraic groups. The set of F_q-fixed points $G^{F_q} \leq \mathrm{GL}(n,q)$ is a finite subgroup. These Frobenius maps can be generalized so that a much larger class of groups can be covered.

Definition 3.1.2 (Steinberg endomorphism)**.** An endomorphism $F : G \to G$ is called a *Steinberg endomorphism* if for some $m \geq 1$ the power $F^m : G \to G$ is the Frobenius endomorphism with respect to some $\mathbb{F}_q$-structure of G.

Once again a Steinberg endomorphism is a morphism of varieties which is an automorphism of the abstract group G. We look at another example.

Example 3.1.3 (General unitary group over finite fields)**.** Let $G := \mathrm{GL}(n,k)$. We define the endomorphism,

$$F : G \to G, \qquad (a_{ij}) \mapsto {}^t(a_{ij}^q)^{-1}$$

Then, $F^2 : G \to G$ is given by $(a_{ij}) \mapsto (a_{ij}^{q^2})$, which is the standard Frobenius map F_{q^2} with respect to $\mathbb{F}_{q^2}$. Thus we have,

$$G^F \leq G^{F^2} = \mathrm{GL}(n,q^2).$$

The fixed point group $\mathrm{GU}(n,q) := G^F = \{A \in \mathrm{GL}(n,q^2) \mid {}^t(A^q)A = id\}$ is called the general unitary group over $\mathbb{F}_{q^2}$. The finite group $\mathrm{SU}(n,q) = \mathrm{GU}(n,q) \cap \mathrm{SL}(n,q)$ is called the special unitary group over $\mathbb{F}_{q^2}$. The above definition also shows that $\mathrm{GU}(n,q)$ is the group of isometries of the non-degenerate sesquilinear form on a vector space of dimension n over $\mathbb{F}_{q^2}$. Note that the Steinberg endomorphism F defined above is not a usual Frobenius endomorphism.

Definition 3.1.4. Let G be a connected reductive group over $k = \bar{\mathbb{F}}_q$ for some prime-power q, and F be a Steinberg endomorphism of G. Then, the finite group of fixed points G^F is called a *finite group of Lie type*.

Example 3.1.5 (Symplectic group over finite fields)**.** Let $G := \mathrm{Sp}(2n,k)$ as defined in Example 2.1.7 of the previous chapter. Once again the fixed point set of the usual Frobenius map defined by

$$F_q : G \to G \qquad (a_{ij}) \mapsto (a_{ij}^q)$$

gives, $\mathrm{Sp}(2n,q) = \mathrm{Sp}(2n,k)^{F_q} = \{A \in \mathrm{GL}(n,q) \mid {}^tAJ_{2n}A = J_{2n}\}$, where J_{2n} is as defined in Chapter 2.

Example 3.1.6 (Split and non-split orthogonal groups in even dimension)**.** Suppose $\mathrm{char}(k) \neq 2$. Let $G := \mathrm{GO}(2n,k)$ as defined in Example 2.1.9. It is clear that G is stable under the usual Frobenius map $F_q : \mathrm{GL}(n,q) \to \mathrm{GL}(n,q)$. The fixed point set under F_q gives,

$$\mathrm{GO}^+(2n,q) = \mathrm{GO}(2n,k)^{F_q} = \{A \in \mathrm{GL}(n,q) \mid {}^tAK_{2n}A = K_{2n}\}$$

This is called the *general orthogonal group over* $\mathbb{F}_q$ *of plus-type*, or the *split general orthogonal group over* $\mathbb{F}_q$.

Now, let

$$g := \begin{pmatrix} I_{n-1} & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & I_{n-1} \end{pmatrix}$$

Then $\det(g) = -1$. Thus $g \in \mathrm{GO}(2n,k) \setminus \mathrm{SO}(2n,k)$. The automorphism $F' := gF : \mathrm{GO}(2n,k) \to \mathrm{GO}(2n,k)$ is a Steinberg automorphism and thus, the fixed point set $\mathrm{GO}^-(2n,q) := \mathrm{GO}(2n,k)^{F'}$ is called the *general orthogonal group (over finite field) of minus-type*, or *non-split orthogonal group over finite fields*.

These groups can also be obtained as the isometry group of non-degenerate symmetric bilinear forms (or, equivalently quadratic forms when $\mathrm{char}(k) \neq 2$) over finite fields. There are two non-equivalent bilinear forms on a vector space of dimension n over $\mathbb{F}_q$, one represented by the matrix,

$$B_1 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & d \end{pmatrix}$$

where d is a square in $\mathbb{F}_q^\times$, and another represented by the matrix,

$$B_2 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & d \end{pmatrix}$$

where d is a non-square in $\mathbb{F}_q^\times$. When the dimension is even, the isometry group

with respect to each of these two bilinear forms are non-isomorphic, and thus yields the two groups of plus-type (with respect to B_1) and minus-type (with respect to B_2).

3.2 Lang-Steinberg theorem and its applications

We begin with a theorem which is a crucial tool for transferring the results of an algebraic group G to the group of fixed points G^F for some Steinberg endomorphism F on G.

Theorem 3.2.1 (Lang-Steinberg)**.** *Let G be a connected linear algebraic group G over $\bar{\mathbb{F}}_q$ with Steinberg endomorphism $F : G \to G$. The morphism*

$$L : G \to G, \qquad g \mapsto F(g)g^{-1},$$

is surjective.

Now we turn to some very important results relevant to this thesis. Let G be a connected linear algebraic group with a Steinberg endomorphism F. Suppose V be any non-empty set and G acts transitively on V. Let $F^{'} : V \to V$ be a map. Suppose that the action is $F, F^{'}$-compatible, that is, $F^{'}(g.v) = F(g).F^{'}(v)$ for all $g \in G, v \in V$. Since the action is compatible with $F, F^{'}$, the finite group G^F acts on $V^{F^{'}} := \{v \in V \mid F^{'}(v) = v\}$. Indeed if $v \in V^{F^{'}}$, then for $g \in G^F$, $F^{'}(g.v) = F(g).F^{'}(v) = g.v$. Thus, it is also clear that $V^{F^{'}}$ is finite.

Suppose for some $v \in V$, the stabilizer G_v is closed. Since the action of G on V is transitive, all stabilizers are then closed (being conjugates). Let us take some $v \in V^{F^{'}}$ (assuming $V^{F^{'}}$ is non-empty). Observe that $F(G_v) \subseteq G_v$. Indeed if $x \in G_v$, $F(x).v = F(x).F^{'}(v) = F^{'}(x.v) = F^{'}(v) = v$. Thus, $F(G_v^\circ) \subseteq G_v^\circ$. This gives a induced map $F : G_v/G_v^\circ \to G/G_v^\circ$. In fact, this map is a isomorphism of groups.

Definition 3.2.2. Let H be a (abstract) group and σ be an automorphism of H. We say $h_1, h_2 \in H$ are σ-conjugate if there exists $x \in H$ such that $h_2 = \sigma(x)h_1x^{-1}$. The equivalence classes for this relation are called the *σ-conjugacy classes of H*, or *σ-twisted conjugacy classes of G*.

Note that if σ is the identity map in the above definition then σ-conjugacy classes are nothing but the conjugacy classes of G. The next theorem guarantees that $V^{F^{'}}$ is non-empty and describes the orbits of $V^{F^{'}}$ under the action of G^F.

Theorem 3.2.3. *Let G be a connected linear algebraic group over $k = \bar{\mathbb{F}}_q$, with Steinberg endomorphism F. Let V be a non-empty set with a map $F^{'} : V \to V$.*

Suppose that G acts transitively on V such that the action is F, F' compatible, that is, $F'(g.v) = F(g).F'(v)$ for every $g \in G, v \in V$. Then,

(a) F' has fixed point on V, that is, $V^{F'} \neq \emptyset$.

(b) For any $v \in V^{F'}$, there is a natural one-one correspondence:

$$\{G^F \text{ -orbits on } V^{F'}\} \longleftrightarrow \{F \text{ -conjugacy classes in } G_v/G_v^\circ\}.$$

The correspondence in the above theorem can be given as follows: Let $v \in V^{F'}$. Let $x \in V$. There exists $g \in G$ such that $x = g.v$. With this, we map the orbit of x to the F-conjugacy class of $F(g)g^{-1}G_v^\circ$. This correspondence will be needed later for explicit computations.

Corollary 3.2.4. *Let G be a connected reductive group and $F : G \to G$ be a Steinberg endomorphism. Then, there exists a pair $T \leq B$, consisting of a F-stable maximal torus T contained in an F-stable Borel subgroup B of G. All such pairs (T, B), with $T \leq B$ are G^F-conjugate.*

Definition 3.2.5. A maximal torus of G as in the above corollary is called *maximally split* with respect to F.

Example 3.2.6. Let $G := \mathrm{GL}(n, k)$. Let F_q be the usual Frobenius endomorphism. Consider the pair $(\mathrm{D}_n, \mathrm{T}_n)$, where $\mathrm{D}_n \leq \mathrm{T}_n$ is the diagonal torus contained in the group of upper triangular matrices. Clearly, T_n and D_n are F_q-stable Borel subgroup and maximal tori respectively of G. We have $\mathrm{D}_n^{F_q} \cong \mathbb{F}_q^\times \times \cdots \times \mathbb{F}_q^\times = (\mathbb{F}_q^\times)^n$.

We see in the above example that any maximally split torus is the direct product of n-copies of $\mathbb{F}_q^\times$. This need not be true in the case of an arbitrary Steinberg endomorphism (see Example 21.14 in [MT11]).

3.3 F-stable Tori

We end this chapter with the discussion of F-stable tori of a linear algebraic group G. Let G be a connected reductive group with Steinberg endomorphism F and $V = \{T \leq G \mid T \text{ is a maximal torus}\}$. Define the map $F' : V \to V$, $T \mapsto F(T)$. The group G acts on V by conjugation and this action is transitive by virtue of Corollary 2.4.12 in Chapter 2. The conjugation of G on V is clearly compatible with the map F' on V. Let T be a maximal torus of G. Then the stabilizer of T under the action of G is the normalizer $N_G(T)$, which is closed. The connected

component, $N_G(T)^\circ = C_G(T)^\circ = C_G(T) = T$. Thus, by using Theorem 3.2.3, we conclude that $V^{F'}$ is non-empty, that is, there exists F-stable maximal tori and,

$$\left\{ \begin{array}{c} G^F \text{ -classes of } F \text{ -stable} \\ \text{maximal tori of } G \end{array} \right\} \longleftrightarrow \{F \text{ -conjugacy classes in } W\},$$

where $W = N_G(T)/T$ is the Weyl group of G.

Example 3.3.1. Consider the group $G := \mathrm{GL}(n,k)$ and let F_q be the usual Frobenius endomorphism. Then $G^F = \mathrm{GL}(n,q)$. Let $T = \mathrm{D}_n$ be a F_q-stable maximal torus of G. We have seen in Example 2.4.15 in Chapter 2, that $N_G(T)$ is the subgroup of monomial matrices in G. The group $N_G(T)/T = \{mT \mid m \in N_G(T)\}$, where m are given by the matrices which have exactly one non-zero entry in each row and column, the non-zero entry being always 1. Thus, F_q induces the identity automorphism on $N_G(T)/T \cong S_n$. Thus, by the above discussion,

$$\left\{ \begin{array}{c} \mathrm{GL}(n,q) \text{ -classes of } F_q \text{ -stable} \\ \text{maximal tori of } \mathrm{GL}(n,k) \end{array} \right\} \longleftrightarrow \{\text{Conjugacy classes in } S_n\}.$$

The conjugacy classes in S_n are parametrized by partitions of n, and thus the $\mathrm{GL}(n,q)$ classes of F_q-stable maximal tori of $\mathrm{GL}(n,k)$ are parametrized by the partitions of n. See Example 3.3.7 for more explicit description of maximal tori in $\mathrm{GL}(n,q)$.

Recall that every semisimple element of a connected reductive group G is contained in a maximal torus of G, and a regular semisimple element is contained in a unique such maximal torus (see Corollary 2.4.21, and Corollary 2.7.5 in Chapter 2). In the same light, we have,

Proposition 3.3.2. *Let G be a connected reductive group with Steinberg endomorphism F. Any semisimple element of G^F is contained in a F-stable maximal torus of G. Furthermore, any regular semisimple element of G^F is contained in a unique F-stable maximal torus of G.*

In the light of the above proposition, we define the following,

Definition 3.3.3. Let G be a connected reductive group with Steinberg endomorphism of F. We call a subgroup $H \leq G^F$ a *maximal torus of G^F*, if $H = T^F$ for some *F-stable maximal torus T of G*.

We end this section with the finitary analogue of the density of regular semisimple elements in a connected reductive group G. For an elementary proof of this result see [JKZ13].

Proposition 3.3.4. *Let G be a connected reductive group with Steinberg endomorphism F. Let G^F_{rs} denote the set of all regular semisimple elements in G^F. Then,*

$$\frac{|G^F_{\mathrm{rs}}|}{|G^F|} = 1 + \mathcal{O}(q^{-1}).$$

In other words, $\lim_{q\to\infty} \frac{|G^F_{\mathrm{rs}}|}{|G^F|} = 1$. The following example illustrates the above result.

Example 3.3.5. Consider the finite reductive group $\mathrm{GL}(2,q)$ of invertible 2×2 matrices with entries in $\mathbb{F}_q$. We have, $|\mathrm{GL}(2,q)| = (q^2-q)(q^2-1) = q^4-q^3-q^2+q$. Let $\mathrm{GL}(2,q)_{\mathrm{rs}}$ denote the set of regular semisimple elements in $\mathrm{GL}(2,q)$. We have $|\mathrm{GL}(2,q)_{\mathrm{rs}}| = q^4 - 2q^3 + q$ (see Chapter 9). Thus, $\lim_{q\to\infty} \frac{|\mathrm{GL}(2,q)_{\mathrm{rs}}|}{|\mathrm{GL}(2,q)|} = 1$.

3.3.1 Non-degenerate maximal tori

We begin with a proposition.

Proposition 3.3.6. *Let G be a linear algebraic group with a Steinberg endomorphism $F : G \to G$, and H an F-stable closed connected normal subgroup of G. Then, the natural map $G^F/H^F \to (G/H)^F$ is an isomorphism.*

Let G and V be as defined in this section. Let T be a F-stable maximal torus of G. Recall that the G^F orbits of F-stable maximal tori are in one-one correspondence with the F-conjugacy classes of the Weyl group $W = W(T) = N_G(T)/T$. Due to the discussion at the end of Theorem 3.2.3, this one-one correspondence can be explicitly given as follows: If T' is any F-stable maximal torus of G and $T' = g^{-1}Tg$ for some $g \in G$, then we map the G^F-orbit of T' to the F-conjugacy class of $F(g)g^{-1}W$. Let us now take $w \in W$ with $w = F(g)g^{-1}W$ for some $g \in G$. Call $F(g)g^{-1} = n_w$. Let $T_w = g^{-1}Tg$. Thus we have, $N_G(T_w) = g^{-1}N_G(T)g$.

Applying Proposition 3.3.6, with G equal to $N_G(T_w)$ and H equal to T_w, we have

$$W(T_w)^F = (N_G(T_w)/T_w)^F \cong N_{G^F}(T_w)/T_w^F.$$

Now, for $n \in N_G(T)$,

$$F(g^{-1}ngT_w) = g^{-1}ngT_w \iff gF(g)^{-1}F(n)F(g)g^{-1}(gT_wg^{-1}) = ngT_wg^{-1}$$

$$\iff n_w^{-1}F(n)n_wT = nT.$$

Taking $nT = \bar{n}$ in $N_G(T)/T$, we conclude that,

$$N_{G^F}(T_w)/T_w^F \cong W(T_w)^F \cong C_{W,F}(w) := \{x \in W \mid F(x)wx^{-1} = w\}.$$

For $t \in T$,

$$F(g^{-1}tg) = g^{-1}tg \iff F(t) = n_w^{-1}tn_w.$$

Thus,

$$T_w^F \cong T^{[w]} := \{t \in T \mid F(t) = n_w^{-1}tn_w\}.$$

Example 3.3.7. Let $G := \mathrm{GL}(n,k)$ and F_q be the usual Frobenius map. From Example 3.2.6 and Example 3.3.1, $T = \mathrm{D}_n$ is maximally split and the $\mathrm{GL}(n,q)$-classes of F_q-stable tori are in one-one correspondence with partitions of n. Let $\lambda \vdash n$ be a partition of n, that is, $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r > 0$ for all $1 \leq i \leq r$ and, $\sum \lambda_i = n$. We claim that,

$$T_\lambda^F \cong \mathbb{F}_{q^{\lambda_1}}^\times \times \cdots \times \mathbb{F}_{q^{\lambda_r}}^\times$$

where T_λ is a F-stable maximal torus of G corresponding to the partition $\lambda \vdash n$ of n.

Consider the partition $(n) \vdash n$. Let w_n be the permutation matrix corresponding to the n-cycle $(1, 2, \ldots, n)$. Thus, w_n is obtained from the identity matrix by shifting the first row to second, second to third and so on, that is,

$$w_n = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \end{pmatrix}.$$

By the discussion above, an F-stable maximal tori corresponding to the partition $(n) \vdash n$ is isomophic to

$$D_n^{[w_n]} = \{t \in D_n \mid F_q(t) = w_n^{-1}tw_n\}.$$

Let $t \in D_n$ with diagonal entries $t_1, t_2, \ldots, t_n$. Then $w_n^{-1}tw_n$ has diagonal entries $t_2, t_3, \ldots, t_n, t_1$. Thus, $t \in D_n^{[w_n]}$ if and only if

$$t_1^q = t_2, t_2^q = t_3, \ldots, t_{n-1}^q = t_n, t_n^q = t_1.$$

if and only if

$$t_1^{q^n} = t_1 \text{ and } t_{i+1} = t_1^{q^i} \text{ for } 1 \leq i \leq n-1.$$

This yields,

$$D_n^{[w_n]} = \{\mathrm{diag}(\zeta, \zeta^q, \ldots, \zeta^{q^{n-1}}) \mid \zeta \in \mathbb{F}_{q^n}^\times\} \cong \mathbb{F}_{q^n}^\times.$$

Thus, we see that for the partition $(n) \vdash n$, our claim holds. The general result can be proved using the same argument cycle-by-cycle.

In general, for a F-stable maximal tori of G we must have, $N_{G^F}(T) \subseteq N_{G^F}(T^F)$, but $N_{G^F}(T) \neq N_{G^F}(T^F)$. For example, it might happen when $T \neq \{1\}$, but $T^F = \{1\}$. Taking $q = 2$ in Example 3.2.6, we have $T^F \cong (\mathbb{F}_2^\times)^n = \{1\}$.

Based on the above observation, we now consider the action of G^F on the set of all T^F where T is a F-stable maximal torus of G. We have already seen that the orbits of collection of all F-stable maximal torus under the action of G^F are in one-one correspondence with F-conjugacy classes of the Weyl group W. The same is true for the orbits of $\{T^F \mid T \text{ is a } F\text{ -stable maximal torus of } G\}$ under the action of G, provided q is large enough. We follow the exposition in Chapter 3 of [Car85] from now onwards.

Definition 3.3.8. Let G be a connected reductive group with Steinberg endomorphism F. Let T be a F-stable maximal torus of G. The maximal torus T^F of G^F is called *non-degenerate* if T is the only maximal torus of G containing T^F.

The fact that T is the only maximal torus of G containing T^F is equivalent to saying $T = C_G(T^F)^\circ$. The following proposition sums up the properties enjoyed by non-degenerate maximal tori.

Proposition 3.3.9. *Let $T_1, T_2 \leq G$ be F-stable maximal tori of G and suppose T_1^F, T_2^F are non-degenerate. Then T_1, T_2 are G^F-conjugate maximal tori of G if and only if T_1^F, T_2^F are conjugate subgroups of G^F. Thus, if all the maximal tori of G^F are non-degenerate then there is a one-one correspondence between the conjugacy classes of maximal tori in G^F and the F-conjugacy classes in W. Finally, for a non-degenerate maximal tori T^F of G^F, we must have $N_{G^F}(T) = N_{G^F}(T^F)$.*

Corollary 3.3.10. *Let T be a F-stable maximal torus of G such that T^F is non-degenerate. Then, $N_{G^F}(T^F)/T^F \cong W(T)^F$.*

Finally as indicated before, we have the following theorem.

Theorem 3.3.11. *Let G be a connected reductive group with Steinberg endomorphism F. Then all the maximal tori of G^F are non-degenerate if q is sufficiently large.*

Chapter 4

Conjugacy Classes of $\mathbf{GL}(n, q)$

This chapter deals with the conjugacy classes in the general linear group over finite fields, denoted by $\mathrm{GL}(n, q)$. The conjugacy classes in $\mathrm{GL}(n, q)$ are determined by the well-known theory of rational canonical forms. We discuss this theory briefly in this chapter. We provide a combinatorial way of describing these classes which will play a vital role in establishing the combinatorial background of this thesis. We will also define conjugacy classes of certain special elements in the group, namely semisimple, regular and regular semisimple conjugacy classes. These classes will play a significant role in the problem to be discussed in the subsequent chapters.

4.1 Rational canonical form and conjugacy classes in $\mathbf{GL}(n, q)$

In this section, we will describe the rational canonical form of matrices, which in turn determines the conjugacy classes in $\mathrm{GL}(n, q)$. This theory is well known and can be found in any graduate algebra text (see, for example [DF04]). The rational canonical form for a linear transformation can be described using the structure theory of modules over a principal ideal domain (PID). Let M be a finitely generated module over R, where R is a PID. The following theorem is the fundamental theorem of finitely generated modules over PID (see Chapter 12, [DF04]).

Theorem 4.1.1 (Fundamental Theorem, Invariant Factor Form)**.** *Let R be PID and let M be a finitely generated R-module. Then,*

1. *The module M is isomorphic to the direct sum of finitely many cyclic modules. More precisely,*

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

for some integer $r \geq 0$ and, nonzero elements $a_1, a_2, \ldots, a_m$ of R which are not units in R and which satisfy the divisibility relations, $a_1|a_2|\cdots|a_m$.

2. *The module M is torsion free if and only if M is free.*

3. *In the decomposition in (1),*

$$\mathrm{Tor}(M) \cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m).$$

In particular, M is a torsion module (that is, $\mathrm{Tor}(M) = M$) if and only if $r = 0$ and in this case the annihilator of M is the ideal (a_m).

The integer $r \geq 0$ in the above theorem is called the *free rank* or the *Betti number* of M and the elements $a_1, a_2, \ldots, a_m \in R$ (defined up to multiplication by units in R) are called *invariant factors* of M. An alternate version of this theorem which can be derived as a consequence of the prime decomposition of the elements $a_1, a_2, \ldots, a_m \in R$, is as follows:

Theorem 4.1.2 (Fundamental Theorem, Elementary Divisor Form)**.** *Let R be a PID and let M be a finitely generated R-module. Then, M is the direct sum of finitely many cyclic modules whose annihilators are either (0) or generated by powers of primes in R, i.e,*

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t}),$$

where $r \geq 0$ is an integer and, $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_t^{\alpha_t}$ are positive powers of (not necessarily distinct) primes in R.

The prime powers $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ (defined up to multiplication by units in R) are called the *elementary divisors* of M. In the above theorem if M is torsion (i.e., $r = 0$), and $p_1, p_2, \ldots, p_l \in R$ be the distinct primes occurring in the above decomposition, we can club together all the elementary divisors corresponding to each such prime, which yields

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_l$$

where N_i consists of all elements of M annihilated by some power of the prime p_i. The submodule N_i of M is called the *p_i-primary component* of M. The above decomposition also identifies M up to isomorphism.

Theorem 4.1.3 (Fundamental Theorem, Uniqueness)**.** *Let R be a PID.*

1. *Two finitely generated R-modules M_1 and M_2 are isomorphic if and only if they have the same free rank and the same list of invariant factors.*

2. *Two finitely generated R-modules M_1 and M_2 are isomorphic if and only if they have the same free rank and the same list of elementary divisors.*

Now, with the fundamental theorem at our disposal, we can apply this to linear transformations. Given a linear transformation $T : V \to V$, where V is a vector space of dimension n over $\mathbb{F}_q$, we can define a module V_T over the polynomial ring $\mathbb{F}_q[x]$ where $V_T = V$ and the scalar operation given by $\left(\sum_{i=0}^{n} a_i x^i\right).v = \sum_{i=0}^{n} a_i T^i(v)$ where $T^i = \underbrace{T \circ T \circ \ldots \circ T}_{i \text{ times}}$. In short, the action is defined by saying "x acts on v as T acts on v". We use the notation V_T instead of just V, in order to emphasize that the action is given by T. Since V is finite dimensional vector space over $\mathbb{F}_q$, it is automatically a finitely generated $\mathbb{F}_q[x]$-module. Moreover, it is torsion, since it is finite dimensional. Since $\mathbb{F}_q$ is a field, $\mathbb{F}_q[x]$ is a PID. Thus, by the fundamental theorem (invariant factor form), we get

$$V_T \cong \frac{\mathbb{F}_q[x]}{(a_1(x))} \oplus \frac{\mathbb{F}_q[x]}{(a_2(x))} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{(a_m(x))}$$

as $\mathbb{F}_q[x]$-module, where $a_1(x), a_2(x), \ldots, a_m(x) \in \mathbb{F}_q[x]$ are non-constant monic polynomials satisfying the divisibility criteria $a_1(x)|a_2(x)|\cdots|a_m(x)$. By Theorem 4.1.1(3), we see that the minimal polynomial of T is $a_m(x)$, and the other invariant factors divide this. With such a decomposition, we can now choose a suitable basis for which the matrix of T is quite simple. Given the $\mathbb{F}_q$-vector space $\frac{\mathbb{F}_q[x]}{(a(x))}$, where $a(x) = x^k + b_{k-1}x^{k-1} + \ldots + b_1(x) + b_0$, the set $\{1, \bar{x}, \ldots, \bar{x}^{k-1}\}$ (where $\bar{x} = x (\text{mod } a(x))$ is a basis for it. The linear transformation T acts on this basis as multiplication by x thus giving,

$$T : \begin{array}{c} 1 \mapsto \bar{x} \\ \bar{x} \mapsto \bar{x}^2 \\ \vdots \\ \bar{x} \mapsto \bar{x}^2 \\ \bar{x}^{k-2} \mapsto \bar{x}^{k-1} \\ \bar{x}_{k-1} = \bar{x}^k = -b_0 - b_1\bar{x} - \ldots - b_{k-1}\bar{x}^{k-1} \end{array}$$

Thus, the matrix of T with respect to this basis (on the subspace spanned by the

basis elements) is given by,

$$\begin{pmatrix} 0 & 0 & \cdots & \cdots & \cdots & -b_0 \\ 1 & 0 & \cdots & \cdots & \cdots & -b_1 \\ 0 & 1 & \cdots & \cdots & \cdots & -b_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & 1 & -b_{k-1} \end{pmatrix}.$$

The above matrix is just made up of the coefficients of the polynomial $a(x)$ (along with 0's and 1's), and is called the *companion matrix* of the non-constant monic polynomial $a(x)$. It is easy to see that the characteristic polynomial of $C_{a(x)}$ is the polynomial $a(x)$ itself. We apply the above process for each of the cyclic modules $\frac{\mathbb{F}_q[x]}{a_i(x)}$, and since $V_T = V$ is the direct sum of such modules, we conclude that T can be represented by a block diagonal matrix with the companion matrices $C_{a_i(x)}$ in the block diagonals, i.e,

$$\begin{pmatrix} C_{a_1(x)} & & & \\ & C_{a_2(x)} & & \\ & & \ddots & \\ & & & C_{a_m(x)} \end{pmatrix}.$$

This matrix of T is called the rational canonical form of T. Observe that the characteristic polynomial of T is $a_1(x)a_2(x)\dots a_m(x)$, which is the product of all the invariant factors.

Definition 4.1.4. A matrix is said to be in *rational canonical form* if it is a block diagonal matrix with companion matrices for non-constant monic polynomials $a_1(x), a_2(x), \dots, a_m(x)$ with $a_1(x)|a_2(x)|\dots|a_m(x)$, as the blocks.

It is easy to observe that if two linear transformations T and S are conjugate then the $\mathbb{F}_q[x]$-module V_T is isomorphic to the $\mathbb{F}_q[x]$-module V_S, thus by Theorem 4.1.3, they have the same set of invariant factors and hence the same rational canonical form. Thus, we conclude that rational canonical form determines the similarity classes of matrices over $\mathbb{F}_q$.

Theorem 4.1.5 (Rational Canonical Form)**.** *Let A be a $n \times n$ matrix over $\mathbb{F}_q$. Then, the matrix A is similar to a matrix in rational canonical form (in the sense of Definition 4.1.4). In other words, there exists an invertible matrix P such that PAP^{-1} is in rational canonical form.*

We have discussed the similarity classes with respect to the invariant factor form. The same thing as above can be applied to the elementary divisor form as well. Let T be a linear transformation on V. Then by Theorem 4.1.2,

$$V_T = V \cong \frac{\mathbb{F}_q[x]}{(f_1(x)^{\alpha_1})} \oplus \frac{\mathbb{F}_q[x]}{(f_2(x)^{\alpha_2})} \oplus \cdots \oplus \frac{\mathbb{F}_q[x]}{(f_t(x)^{\alpha_t})}$$

as $\mathbb{F}_q[x]$-module, where f_i's (not necessarily distinct) are monic non-constant irreducible polynomials over $\mathbb{F}_q$. Once again it is possible to choose a basis (similar to above) such that the matrix of T takes a nice block diagonal form $\text{diag}(R_1, R_2, \ldots, R_l)$ where for a fixed $1 \leq i \leq l$, R_i is the block diagonal matrix $\text{diag}(J_{f_i,\lambda_{i_1}}, J_{f_i,\lambda_{i_2}}, \ldots)$ where $\lambda_{i_1}, \lambda_{i_2}, \ldots$ are the various powers occurring in the elementary divisor form corresponding to f_i. The matrix $J_{f_i,\lambda_{i_r}}$ is a block matrix of size λ_{i_r} with each block size $\deg(f_i)$ (here, $\deg(f)$ denotes the degree of the polynomial f) given as follows

$$J_{f_i,\lambda_{i_r}} = \begin{pmatrix} C(f_i) & I & 0 & \cdots & \cdots & 0 \\ & C(f_i) & I & 0 & \cdots & 0 \\ & & \ddots & \ddots & \ddots & \vdots \\ & & & \ddots & \ddots & 0 \\ & & & & C(f_i) & I \\ & & & & & C(f_i) \end{pmatrix}$$

where I denotes the identity matrix. Thus, the matrix $J_{f_i,\lambda_{i_r}}$ is a matrix of size $\deg(f_i)\lambda_{i_r}$. Observe that the matrix $J_{f_i,\lambda_{i_r}}$ has a similar form to a Jordan block (defined over an algebraically closed field). Thus, the above form is an analogue of Jordan canonical form (which exists over algebraically closed fields) where the companion matrices replace the eigen values of transformation. The above matrix is once again a representative of a similarity class of matrices, which is uniquely determined by its elementary divisors. It is this description of the similarity classes using the elementary divisors, which allows us to attach a combinatorial data to a conjugacy class in GL(n,q) (See [Gre55]).

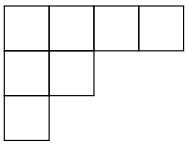
4.1.1 A combinatorial parametrization of the conjugacy classes in GL(n,q)

In order to describe the combinatorial parametrization of a conjugacy class, we need to set a notation. Let $\widetilde{\Phi}$ denote the set of all non-constant, monic, irreducible polynomials $f(x)$ (sometimes we simply write f) with coefficients in $\mathbb{F}_q$. Let $\Phi = \widetilde{\Phi} \backslash \{x\}$. We will use this notation freely from now onwards without further mention. A conjugacy class of GL(n,q) is determined by an associated combinatorial data as follows. Let Λ be the set of all partitions $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ where

$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r > 0$ are integers. The set Λ consists of λ which are all possible partitions of all non-negative integers $|\lambda|$ where $|\lambda|$ is defined to be the sum of its parts. This includes the empty partition of 0. To each $f \in \Phi$, we associate a partition $\lambda_f = (\lambda_{f,1}, \lambda_{f,2}, \ldots)$ of some non-negative integer $|\lambda_f|$. A conjugacy class of GL(n, q) is in one-one correspondence with a function $\Phi \to \Lambda$ satisfying $\sum_{f \in \Phi} |\lambda_f| \deg(f) = n$. The summation constraint implies that the function takes the value empty partition on all but finitely many polynomials in Φ. This one-one correspondence is clear since a conjugacy class is determined by the elementary divisor form, and the associated data reveals the fact that the elementary divisors of a matrix in such a conjugacy class is given by the finite number of polynomials $f_1, f_2, \ldots, f_l$ which takes a non-empty partition as its functional value, and corresponding to each such polynomial f_i, the partition $\lambda_{f_i} = (\lambda_{f_i,1}, \lambda_{f_i,2}, \ldots)$ just denotes the complete set of powers of f_i (taking all $\lambda_{f_i,j} \neq 0$) that occur as elementary divisors. In other words, a representative of such a class is the block diagonal matrix $\text{diag}(R_1, R_2, \ldots, R_l)$ where for a fixed $1 \leq i \leq l$, R_i is the block diagonal matrix $\text{diag}(J_{f_i,\lambda_{f_i,1}}, J_{f_i,\lambda_{f_i,2}}, \ldots)$ where $J_{f_i,\lambda_{f_i,j}}$ is defined as in Page 34. Thus, the conjugacy class of an element $\alpha \in \text{GL}(n, q)$ corresponds to the associated *combinatorial data* Δ_α, which consists of distinct polynomials $f_1, \ldots, f_l$ and associated non-zero partitions $\lambda_{f_i} = (\lambda_{i_1}, \lambda_{i_2}, \ldots)$ for all i. In this notation, we keep only those f_i on which the function on f_i takes value non-empty partition λ_{f_i}. This combinatorial data will prove to be crucial in defining the notion of cycle index of GL(n, q) in the next chapter.

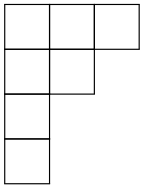
To end this section, we discuss briefly about the centralizer of an element $\alpha \in \text{GL}(n, q)$, which is the set of all elements in GL(n, q) which commute with α. Since the centralizer subgroups of two elements in the same conjugacy class are also conjugate, the size of the centralizer of an element α is only dependent on the associated combinatorial data Δ_α. For our purpose, we will need to know the size of the centralizer of an element. The size of the centralizer of an element in GL(n, q) is well known (see for example Page 181, [Mac95]). We write the formula and give a brief idea about how it can be obtained. We define a notation that will be required to write the formula. Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \vdash n$ be a partition of n. The *Young diagram* corresponding to this partition is an arrangement of square boxes where the first row has λ_1 number of boxes, the second row has λ_2 number of boxes, and so on.

Example 4.1.6. Young diagram corresponding to the partition $(4, 2, 1) \vdash 7$ is,



The *transpose of a partition* $\lambda \vdash n$ of n is the partition of n obtained by transposing the rows and columns of the Young diagram of λ. It is denoted by $\lambda^{'}$.

Example 4.1.7. $\lambda = (4, 2, 1) \vdash 7$, then $\lambda^{'}$ is the partition of 7 whose young diagram is



Thus, $\lambda^{'} = (3, 2, 1, 1) \vdash 7$.

Let $\mathcal{Z}(\alpha)$ denote the centralizer of an element $\alpha \in \mathrm{GL}(n, q)$. The $\mathbb{F}_q[x]$ module V_α via α has the decomposition

$$V_\alpha = N_1 \oplus N_2 \oplus \ldots \oplus N_l$$

where,

$$N_i = \frac{\mathbb{F}_q[x]}{f_i(x)^{\lambda_{i_1}}} \oplus \frac{\mathbb{F}_q[x]}{f_i(x)^{\lambda_{i_2}}} \oplus \ldots \oplus \frac{\mathbb{F}_q[x]}{f_i(x)^{\lambda_{i_r}}}$$

is the f_i-primary component of V_α. Here, $\lambda_{f_i} = (\lambda_{i_1}, \lambda_{i_2}, \ldots, \lambda_{i_r}) \vdash |\lambda_{f_i}|$. It is clear that an element $g \in \mathcal{Z}(\alpha)$ is just an automorphism of the $\mathbb{F}_q[x]$-module V_α, since $g(x.v) = g(\alpha(v)) = \alpha(g(v)) = x.g(v)$ for all $v \in V$. We conclude that the elements that commute with α are automorphism of the $\mathbb{F}_q[x]$-module V_α. Therefore, to count the number of elements in $\mathcal{Z}(\alpha)$ we need to count the number of the automorphism of the module V_α. Now,

$$\mathrm{Aut}(V_\alpha) = Aut(N_1) \times \mathrm{Aut}(N_2) \times \ldots \times \mathrm{Aut}(N_l).$$

Since, N_i is a finite $\mathbb{F}_q[x]$-module (annihilated by some power of f_i), it can be proved (see Page 181, 1.6, [Mac95]) that,

$$|\mathrm{Aut}(N_i)| = q^{\deg(f_i)\sum_j (\lambda^{'}_{i_j})^2} \prod_{t \geq 1} \left(\frac{1}{q^{\deg(f_i)}} \right)_{m_t(\lambda_{f_i})}$$

where $\left(\frac{u}{q}\right)_i = (1 - \frac{u}{q})(1 - \frac{u}{q^2}) \cdots (1 - \frac{u}{q^i})$. Thus, we get,

$$|\mathcal{Z}(\alpha)| = \prod_{i=1}^{l} \left[q^{\deg(f_i)\sum_j (\lambda'_{i_j})^2} \prod_{t\geq 1} \left(\frac{1}{q^{\deg(f_i)}} \right)_{m_t(\lambda_{f_i})} \right]. \tag{4.1}$$

4.2 Regular, Semisimple, and Regular Semisimple classes

Regular, semisimple, and regular semisimple elements were defined in Chapter 1, for any linear algebraic group. In $\mathrm{GL}(n,q)$, these elements have simple linear algebra characterizations, involving the elementary divisors. A semisimple element in $\mathrm{GL}(n,q)$ is an element which is diagonalizable over $\bar{\mathbb{F}}_q$. In terms of modules, if $\alpha \in \mathrm{GL}(n,q)$ is semisimple, it means that for each f-primary component N of the $\mathbb{F}_q[x]$-module V_α, where f is a non-constant monic irreducible polynomial, the highest power of f that annihilates the submodule N is f itself. Thus,

$$V_\alpha = \frac{\mathbb{F}_q[x]}{(f_1(x))} \oplus \ldots \oplus \frac{\mathbb{F}_q[x]}{(f_1(x))} \oplus \frac{\mathbb{F}_q[x]}{(f_2(x))} \oplus \ldots \oplus \frac{\mathbb{F}_q[x]}{(f_2(x))} \oplus \ldots \oplus \frac{\mathbb{F}_q[x]}{(f_t(x))} \oplus \ldots \oplus \frac{\mathbb{F}_q[x]}{(f_t(x))}$$

where $f_1, f_2, \ldots, f_t(x)$ are monic non-constant irreducible polynomials over $\mathbb{F}_q$. The collection of all semisimple elements is a union of conjugacy classes. Thus a *semisimple class* is a conjugacy class consisting of semisimple elements. A regular element in $\mathrm{GL}(n,q)$ is an element whose minimal polynomial is the same as the characteristic polynomial. Once again, in terms of modules, if $\alpha \in \mathrm{GL}(n,q)$ is regular, then it is clear that each f-primary component N in the elementary divisor form of the $\mathbb{F}_q[x]$-module V_α is isomorphic to $\frac{\mathbb{F}_q[x]}{(f(x))^\alpha}$ for some $\alpha > 0$. Thus, each f-primary component is a cyclic module. This is why regular matrices are referred to as *cyclic matrices* in the literature. It is once again clear that the set of all regular elements is a union of conjugacy classes. Thus, a conjugacy class consisting of regular elements is called a *regular conjugacy class*.

Finally, a regular semisimple matrix in $\mathrm{GL}(n,q)$ is the one that is both regular and semisimple. Thus, if $\alpha \in \mathrm{GL}(n,q)$ is regular semisimple, then each f-primary component N in the elementary divisor form of the $\mathbb{F}_q[x]$-module V_α is isomorphic to $\frac{\mathbb{F}_q[x]}{(f(x))}$. Since the characteristic polynomial of the matrix α is the product of all the elementary divisors, we see that it can be written as $f_1 f_2 \cdots f_k$, where f_i are non-constant monic irreducible polynomials. This means that the characteristic polynomial of α is separable, that is, no irreducible factor occurs more than once. Thus, these matrices are sometimes referred to as *separable matrices*. A conjugacy class consisting only of regular semisimple elements is called a *regular semisimple conjugacy class*. We will see that the three types of matrices defined above will

play a key role in the subsequent chapters.

Chapter 5

Cycle index of $\mathbf{GL}(n, q)$

This chapter deals with one of the most important tools in this thesis, known as, generating functions. In the subject of enumerative combinatorics, generating functions play a vital role, in varied counting problems. In this chapter, we briefly introduce the notion of generating functions and give examples of various generating functions that occur in the context of counting the number of conjugacy classes in $\mathrm{GL}(n, q)$. Finally, we introduce the very important notion of cycle index for $\mathrm{GL}(n, q)$ (see equation 1.2, chapter 1 for cycle index of S_n), and give some important applications relevant to our work. All of these are quite well known in literature.

5.1 Generating function

Let $(a_n)_{n\geq 0}$ be a sequence of real numbers.

Definition 5.1.1 (Generating function)**.** The *ordinary generating function* of the sequence $(a_n)_{n\geq 0}$ is defined as the formal power series $\sum_{n=0}^{\infty} a_n x^n$.

Therefore, the ordinary generating function corresponding to the sequence $(a_n)_{n\geq 0}$ is an element of the ring of formal power series with coefficients in $\mathbb{R}$, denoted by $\mathbb{R}[[x]]$. From now onwards, we will write generating function in place of ordinary generating function. We give several examples of generating functions.

Example 5.1.2 (Addition and multiplication of two generating functions)**.** Let $\sum_{n=0}^{\infty} a_n x^n$ and $\sum_{n=0}^{\infty} b_n x^n$ be the generating function for the sequence (a_n) and (b_n) respctively. Then, the sum of these two generating function, defined similar to

sum of two polynomials, is

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n$$

gives the generating function for the sequence $(a_n + b_n)$. Similarly, the product of these two generating functions, is given by the Cauchy product which is,

$$\left(\sum_{n=0}^{\infty} a_n x^n\right) \times \left(\sum_{n=0}^{\infty} b_n x^n\right) = \sum_{n=0}^{\infty} c_n x^n$$

where, $c_n = \sum_{k=0}^{n} a_k b_{n-k}$. Thus, the product of the generating function for the sequence (a_n) and (b_n) yields the generating function of the sequence (c_n), given by the Cauchy product.

Example 5.1.3. Consider the sequence $(a_n)_{n\geq 0}$ with $a_n = 1$ for every $n \geq 0$. The generating function for this sequence is

$$1 + x + x^2 + x^3 + \cdots = \frac{1}{1-x}.$$

We say, $\frac{1}{1-x}$ is a closed form for the generating function of the sequence $(a_n) = (1, 1, 1, 1, \ldots)$. Note here, that the above equality is just equality in the ring of formal power series. We don't take into account the analytic notions of a power series, like the radius of convergence and so on.

Example 5.1.4. Consider the sequence (a_n), where $a_n = \frac{1}{n!}$. The generating function for this sequence is given by,

$$1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \exp(x).$$

Example 5.1.5 (Fibonacci Numbers)**.** The Fibonacci sequence is quite well known in mathematics and has a variety of applications. The first few terms of the sequence are given by $(0, 1, 1, 2, 3, 5, 8, 13, \ldots)$. This can be defined recursively. Let (a_n) be the sequence of Fibonacci numbers. Then, the sequence is defined as,

$$a_n = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ a_{n-2} + a_{n-1} & \text{if } n \geq 2 \end{cases}.$$

We intend to find a closed form for the generating function of the Fibonacci se-

quence. The generating function for (a_n) is,

$$s(x) = x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + 13x^7 + \cdots .$$

Due to the recursive relation above, we get,

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

$$\implies s(x) = x + xs(x) + x^2 s(x) \implies s(x) = \frac{x}{1 - x - x^2}.$$

Therefore, we can say that the n^{th} Fibonacci number can be read off from the coefficient of x^n in the formal power series expansion of $\frac{x}{1-x-x^2}$.

We now turn to a more important example. The next example gives the generating function for the number of partitions of n.

Example 5.1.6 (Partitions of natural numbers)**.** Let $p(n)$ be the number of partitions of n. For simplicity, we take, $p(0) = 1$. Simple computations show, $p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 5, p(5) = 7, p(6) = 11, p(7) = 15$ and so on. Thus,

$$1 + \sum_{n=1}^{\infty} p(n) x^n = 1 + x + 2x^2 + 3x^3 + 5x^4 + 7x^5 + 11x^6 + \cdots .$$

Although, a closed form for the above generating function similar to the one for Fibonacci numbers can't be given, still one can write the above generating functions in the form of an infinite product. We will later see that this kind of representation of generating function can be suitable in specific situations. The following proposition is well-known. We give a proof for completeness.

Proposition 5.1.7.

$$1 + \sum_{n=1}^{\infty} p(n) x^n = \prod_{i=1}^{\infty} \frac{1}{1 - x^i}.$$

Proof. Given a partition $\lambda \vdash n$, we have already seen that in frequency (or, power) notation, $\lambda = \langle 1^{m_1}, 2^{m_2}, \cdots \rangle$, where m_i denotes the number of times i occur in λ. Consider the following infinite product,
$(1 + x + x^2 + \cdots)(1 + x^2 + x^4 + \cdots)(1 + x^3 + x^6 + \cdots) \cdots (1 + x^i + x^{2i} + \cdots) \cdots$.
By interpreting $x^{it} = (x^i)^t$ in the product $(1 + x^i + x^{2i} + \cdots)$, as corresponding to the partition $\underbrace{(i, i, \ldots, i)}_{t \text{ times}}$ of it, it is easy to see that $p(n)$ is given by the coefficient

of x^n in the above infinite product. Since,

$$1 + x^i + x^{2i} + \cdots = \frac{1}{1 - x^i},$$

we get the desired result. □

Generating functions in enumerative combinatorics, as mentioned before, can be useful in counting different mathematical quantities. This can range from getting closed formulas in some cases, to getting recursive formula in others, and many other properties. It is very intriguing that to date there is no closed formula for $p(n)$, although several properties of $p(n)$ can be derived from the generating function in Proposition 5.1.7. We end this section, with two well-known results on $p(n)$, which can be proved solely by using generating functions. These two results will highlight the importance of generating functions in enumeration. We start with a lemma which is well known. We state it without proof.

Lemma 5.1.8 (Euler's Pentagonal number theorem)**.**

$$\prod_{i=1}^{\infty}(1 - x^i) = 1 + \sum_{k=1}^{\infty}(-1)^k(x^{k(3k+1)/2} + x^{k(3k-1)/2}).$$

The numbers $g_k = \frac{1}{2}k(3k-1)$ for $k = \pm 1, \pm 2, \ldots$, are called Pentagonal numbers. The following recursive formula for $p(n)$, is a direct consequence of its generating function in Proposition 5.1.7 and Lemma 5.1.8. For convenience let us assume $p(n) = 0$ for $n < 0$, and $p(0) = 1$.

Proposition 5.1.9. *For $n \geq 2$,*

$$p(n) = \sum_{k \in \mathbb{Z}}(-1)^{k-1}p(n - g_k),$$

where g_k are the Pentagonal numbers.

Proof. Observe that,

$$\left(\prod_{i=1}^{n}\frac{1}{1 - x^i}\right)\left(\prod_{i=1}^{n}(1 - x^i)\right) = 1.$$

Now, the proof follows from Proposition 5.1.7 and Lemma 5.1.8. □

Example 5.1.10. From the above proposition, $p(8) = p(7) + p(6) - p(3) - p(1) = 15 + 11 - 3 - 1 = 22$.

We end this section with another well-known identity of partitions, again due to Euler. Suppose $\lambda \vdash n$, be a partition of n. We say λ is an odd partition of n, if each part in λ is odd. In other words, $m_i(\lambda) = 0$ when i is even. We say λ is distinct partition of n, if each part is distinct. In other words, $m_i(\lambda)$ is atmost 1 for all $i \geq 1$.

Proposition 5.1.11. *The number of odd partitions of n is equal to the number of distinct partitions of n.*

Proof. Let $d(n)$ denote the number of distinct partitions of n, and $o(n)$ denote the number of odd partitions of n. From the proof of Proposition 5.1.7, it can be easily seen, that, $d(n)$ is the coefficient of x^n, in the product $(1+x)(1+x^2)(1+x^3)\cdots(1+x^i)\cdots$. Thus, we have

$$1 + \sum_{n=1}^{\infty} d(n)x^n = \prod_{i=1}^{\infty}(1+x^i).$$

On the other hand, it is clear that $o(n)$ is the coefficient of x^n in the infinite product,

$$(1+x+x^2+\cdots)(1+x^3+x^6+\cdots)(1+x^5+x^{10}+\cdots)\cdots(1+x^{2i-1}+x^{2(2i-1)}+\cdots)$$

$$\cdots = \prod_{i=1}^{\infty}\frac{1}{1-x^{2i-1}} = \prod_{i=1}^{\infty}\frac{1-x^{2i}}{1-x^i} = \prod_{i=1}^{\infty}(1+x^i).$$

The penultimate equality is obtained by multiplying $\prod_{i=1}^{\infty}(1-x^{2i})$, to both the numerator and denominator. Thus, we have

$$1 + \sum_{n=1}^{\infty} o(n)u^n = \prod_{i=1}^{\infty}(1+x^i).$$

Since, the generating function for $d(n)$ and $o(n)$ are same, we conclude that $d(n) = o(n)$, thus completing the proof. □

5.2 Generating functions for the number of conjugacy classes in GL(n,q)

In this section we will obtain the generating function for the number of conjugacy classes in GL(n,q), as well as, for some other related quantities, relevant for our purpose. These generating functions are quite well known (see [Mac81], [FG13]). Let $c(n)$ denote the number of conjugacy classes in GL(n,q). Let

$c(n)_{\mathrm{rg}}, c(n)_{\mathrm{rs}}, c(n)_{\mathrm{ss}}$ denote the number of regular, regular semisimple, semsimple conjugacy classes in GL(n, q) (see chapter 4 for the definitions). Recall that $\Phi = \widetilde{\Phi} \setminus \{x\}$, where $\widetilde{\Phi}$ denotes the set of all monic irreducible polynomials over $\mathbb{F}_q$. Let $\widetilde{N}(q, d)$ denote the number of polynomials of degree d in $\widetilde{\Phi}$. In other words, $\widetilde{N}(q, d)$ is the number of *monic irreducible polynomials of degree d*. Let $N(q, d)$ denote the number of polynomials of degree d in Φ. It is easy to see that $\widetilde{N}(q, d)$ and $N(q, d)$ are related as, $N(q, d) = \widetilde{N}(q, d) - 1$, when $d = 1$, and $N(q, d) = \widetilde{N}(q, d)$ otherwise. The formula for $\widetilde{N}(q, d)$ is well-known, which we state without proof.

$$\widetilde{N}(q, d) = \frac{1}{d} \sum_{r|d} \mu(r) q^{\frac{d}{r}} \tag{5.1}$$

where μ is the well known Möbius function defined on the set of natural numbers as follows:

$$\mu(r) = \begin{cases} 1 & \text{when } r = 1, \\ (-1)^t & \text{when } r \text{ is square free, and } r = p_1 p_2 \dots p_t, \\ & \text{where } p_i \text{ are primes for all } 1 \leq i \leq t, \\ 0 & \text{when } r \text{ has square factor.} \end{cases}$$

An elementary conceptual proof of Equation 5.1 can be found in [CM11]. Thus, we have

$$N(q, d) = \frac{1}{d} \sum_{r|d} \mu(r)(q^{\frac{d}{r}} - 1) \tag{5.2}$$

since, $\sum_{r|d} \mu(r)$ is equal to 1 when $r = 1$ and 0 otherwise.
We must also mention here that $N(q, d)$ is also the number of Lyndon words in q alphabets of length d. Thus $N(q, d)$ arises in combinatorics even when q is not a prime (see [Lot02] for more about Lyndon words).

We begin with an identity (see [Ful99]) that will play a very important role later.

Lemma 5.2.1. $\prod_{d=1}^{\infty} (1 - u^d)^{-\widetilde{N}(q,d)} = \frac{1}{1-qu}$.

Proof. Consider the infinite product

$$\prod_{f \in \widetilde{\Phi}} (1 - u^{\deg f})^{-1} = \prod_{f \in \widetilde{\Phi}} (1 + u^{\deg f} + u^{2\deg f} + \cdots).$$

Due to the unique factorization of polynomials over $\mathbb{F}_q$, the coefficient of u^n in the above product is clearly the number of monic polynomials of degree n. The number

of monic polynomials of degree n over $\mathbb{F}_q$ is q^n, which in fact is the coefficient of u^n in $\frac{1}{1-qu}$. Thus, we get

$$\prod_{f\in\widetilde{\Phi}}(1-u^{\deg f})^{-1}=\frac{1}{1-qu}.$$

Clubbing together all the degree d polynomials in $\widetilde{\Phi}$ in the product on the left hand side of the above equality, proves the lemma. □

5.2.1 Number of regular, regular semisimple, and semisimple classes

In Chapter 4, we have seen that the regular elements in GL(n,q) are in one-one correspondence with monic polynomials of degree n with non-zero constant term. The number of such polynomials is $q^{n-1}(q-1)=q^n-q^{n-1}$. Similarly, the semisimple elements in GL(n,q) are in one-one correspondence with monic polynomials of degree n with non-zero constant terms. Thus, we have

$$c(n)_{\mathrm{rg}}=c(n)_{\mathrm{ss}}=q^n-q^{n-1}.$$

The following proposition gives the generating function (with closed form) for $c(n)_{\mathrm{rg}}$ and $c(n)_{\mathrm{ss}}$.

Proposition 5.2.2.

$$1+\sum_{n=1}^{\infty}c(n)_{\mathrm{rg}}u^n=1+\sum_{n=1}^{\infty}c(n)_{\mathrm{ss}}u^n=\prod_{d=1}^{\infty}(1-u^d)^{-N(q,d)}=\frac{1-u}{1-qu}.$$

Proof. The coefficient of u^n in $\frac{1-u}{1-qu}$ is q^n-q^{n-1}, which is also the number of regular (and, semisimple) classes in GL(n,q). The final equality holds by Lemma 5.2.1. □

In chapter 4, we have seen that the regular semisimple classes in GL(n,q) are in one-one correspondence with separable polynomials of degree n, that is, polynomials of degree n, which are square-free. The following proposition gives the generating function for $c(n)_{\mathrm{rs}}$ (see [FG13]).

Proposition 5.2.3.

$$1+\sum_{n=1}^{\infty}c(n)_{\mathrm{rs}}u^n=\prod_{n=1}^{\infty}(1+u^d)^{N(q,d)}=\frac{1-qu^2}{(1+u)(1-qu)}.$$

Proof. As a consequence of unique factorization, the coefficient of u^n in the product

$$\prod_{f \in \Phi} (1 + u^{\deg f})$$

is equal to the number of monic separable polynomials of degree n. This is because allowing only $u^{\deg f}$ ensures that f can occur at most once in any unique factorization. Clubbing together the degree d polynomials in Φ in the above product, we get the first equality. The second equality follows form Lemma 5.1 since,

$$\prod_{n=1}^{\infty} (1 + u^d)^{N(q,d)} = \frac{\prod_{d=1}^{\infty} (1 - u^d)^{-N(q,d)}}{\prod_{d=1}^{\infty} (1 - u^{2d})^{-N(q,d)}}.$$

□

From the above generating function, it is easy to get a closed formula for $c(n)_{\text{rs}}$ (see [FG13, Theorem 2.2]). We just mention this formula without proof.

$$c(n)_{rs} = \frac{q^{n+1} - q^n + (-1)^{n+1}(q-1)}{q+1}.$$

See [FJK98] for alternative proofs of these results and [FG13, FJK98] for results on other finite classical groups.

5.2.2 Number of conjugacy classes in GL(n, q)

Recall that $c(n)$ denote the number of conjugacy classes in GL(n, q). The generating function for $c(n)$ is well-known and can be found in [Mac81, **?**]. We briefly outline the idea of obtaining this generating function (see [Mac81] for more details). In Chapter 4, given a matrix $\alpha \in \text{GL}(n, q)$, we associated a combinatorial data Δ_α which consists of some finitely many monic irreducible polynomials (except the polynomial x) $f_1, f_2, \ldots, f_k$ and partitions $\lambda_{f_i} \vdash |\lambda_{f_i}|$ for all $1 \leq i \leq k$, such that $\sum_i |\lambda_{f_i}| \deg f_i = n$. We now provide a modified version of this data which will help us in obtaining the required generating function. Define polynomials u_j as follows:

$$u_j = \prod_i f_i^{m_j(\lambda_{f_i})}.$$

Observe that u_j is a monic polynomial with a non-zero constant term, and satisfies, $\sum_j j \deg(u_j) = n$. It is clear from the above discussion that we obtain only finitely many non-constant monic polynomials u_i. Thus, to any elements $\alpha \in \text{GL}(n, q)$,

we have attached certain finite number of non-constant monic polynomials, say $u_1, u_2, \ldots, u_l$ satisfying the relation $\sum_j j\deg(u_j) = n$. This data determines α up to conjugacy. Thus we now have a modified combinatorial data corresponding to each conjugacy class of GL(n, q).

Suppose $\nu \vdash n$ be a partition of n, where $\nu = \langle 1^{n_1}, 2^{n_2}, \cdots \rangle$. A conjugacy class C of GL(n, q) is called a type-ν conjugacy class if $\deg(u_j) = n_j$ for all $j \geq 1$, where u_i are the polynomials that occur in the combinatorial data of C. Therefore, we have grouped the conjugacy classes by a certain rule, which corresponds to a partition of n. For example - consider the partition $\nu = \langle 1^n \rangle \vdash n$. Then a conjugacy class will be of type-ν if there is only one polynomial u_1 of degree n. By definition of u_j's, it is clear that such a conjugacy is a semisimple conjugacy class. Conversely a semisimple conjugacy class will be of type-ν, where $\nu = \langle 1^n \rangle \vdash n$. Thus, corresponding to the partition $\langle 1^n \rangle \vdash n$ we have grouped all semisimple conjugacy classes.

Given a partition $\nu = \langle 1^{n_1}, 2^{n_2}, \cdots \rangle$, let c_ν denote the number of type-ν conjugacy classes. To count the number of such classes, for each $j \geq 1$ such that $n_j > 0$, we have to count the number of ways we can choose non-constant monic polynomials u_j with non-zero constant term of degree n_j, which is equal to $q^{n_j} - q^{n_j - 1}$. Thus,

$$c_\nu = \prod_{n_i > 0} (q^{n_i} - q^{n_i - 1}).$$

Therefore, the number of conjugacy classes $c(n)$ is given by,

$$c(n) = \sum_{\nu \vdash n} c_\nu = \sum_{\substack{\nu \vdash n \\ \nu = \langle 1^{n_1}, 2^{n_2}, \cdots \rangle}} \left(\prod_{n_i > 0} (q^{n_i} - q^{n_i - 1}) \right). \tag{5.3}$$

We now have all we need to write the generating function for $c(n)$.

Lemma 5.2.4. *Let* $f(u) = 1 + \sum_{n=1}^{\infty} a_n u^n$. *Suppose* $\nu = \langle 1^{n_1}, 2^{n_2}, \cdots \rangle$ *is a partition of* n. *Define* $b_n = \sum_{\nu \vdash n} \left(\prod_{n_i > 0} a_{n_i} \right)$. *Then,*

$$1 + \sum_{n=1}^{\infty} b_n u^n = \prod_{t=1}^{\infty} f(u^t).$$

Proof. The Lemma follows simply by computing the coefficients of u^n on both

sides. □

Proposition 5.2.5. $1 + \sum_{n=1}^{\infty} c(n)u^n = \prod_{i=1}^{\infty} \frac{1-u^i}{1-qu^i}$.

Proof. The proof follows by putting $a_n = q^n - q^{n-1}$ in the above Lemma and using Equation 5.3. □

Some elementary properties can be derived from the above generating function of $c(n)$. We collect some of these, whose proof can be found in [Mac81].

Proposition 5.2.6. *The number $c(n)$ has the following properties:*

1. *$c(n)$ is a monic polynomial in q of degree n. Moreover, $c_n(q) = q^n - (q^a + q^{a-1} + \ldots + q^{b+1} + q^b) + \ldots$, where $a = \lfloor \frac{1}{2}(n-1) \rfloor, b = \lfloor \frac{1}{3}n \rfloor$.*
2. *The constant term in $c(n)$ is $(-1)^k$, whenever $n = \frac{1}{2}k(3k+1)$, for some $k \in \mathbb{Z}$. Otherwise, the constant term is 0.*
3. *$q - 1 \mid c(n)$.*

5.3 Cycle index of GL(n, q) and its applications

Polýa (see [PR87]) introduced the notion of cycle index in the symmetric group S_n, to study conjugacy class functions, that is, properties which are invariant under conjugation. Let $\pi \in S_n$, and for $i \geq 1$, $m_i(\pi)$ denote the number of i-cycles in π. It is clear that $\sum_i i m_i(\pi) = n$. Thus, $m_i(\pi) = 0$ for $i > n$. It is well known that two permutations $\pi, \tau \in S_n$ are conjugate in S_n, if and only if $m_i(\pi) = m_i(\tau)$ for all $i \geq 1$. It can be seen that $\langle 1^{m_1(\pi)}, 2^{m_2(\pi)}, \cdots \rangle \vdash n$. Therefore, partitions of n determine the conjugacy classes in S_n. Define,

$$Z_n = Z_n(t_1, t_2, \ldots t_n) = \frac{1}{n!} \sum_{\pi \in S_n} t_1^{m_1(\pi)} t_2^{m_2(\pi)} \ldots t_n^{m_n(\pi)}.$$

The above polynomial in the variables $t_1, t_2, \ldots, t_n$ is called the *cycle index* of S_n, or the *cycle polynomial* of S_n. The coefficient of a monomial of the form $t_1^{c_1} t_2^{c_2} \ldots t_n^{c_n}$ is equal to the number of elements in the conjugacy class parametrized by the partition $\langle 1^{c_1}, 2^{c_2}, \cdots \rangle \vdash n$ divided by $n!$, which is further equal to one divided by the centralizer of an element in such a class. Since the size of the centralizer is given by $\prod_i i^{c_i} c_i!$, we get

Proposition 5.3.1. $1 + \sum_{n=1}^{\infty} Z_n u^n = \prod_{i \geq 1} \exp\left(\frac{t_i u^i}{i}\right)$.

The above generating function is called the *cycle index generating function* of S_n. This generating function enabled the study of several properties of random permutations which were only dependent on the cycle structure of permutations (for context see Chapter 1 and references therein).

The Cycle index of $\mathrm{GL}(n,q)$ was developed along the same lines as done by Pólya for S_n by J. Kung in [Kun81]. R. Stong in [Sto88] studied properties of linear transformations acting on sets, for example, the proportions of semisimple elements in $\mathrm{GL}(n,q)$, using the cycle index. Later, J. Fulman provided a neater version of the cycle index (see [Ful99]) and, used it to write the generating functions for the proportions of regular, regular semisimple, and semisimple matrices in $\mathrm{GL}(n,q)$, and studied the asymptotic behaviour of these proportions (see also [Wal99]). He further developed the cycle index of some other classical groups like $\mathrm{Sp}(2n,q), \mathrm{GU}(n,q)$, and others, using the description of conjugacy classes in these groups obtained by G.E.Wall in [Wal80, Wal63].

Given $\alpha \in \mathrm{GL}(n,q)$, we have attached a combinatorial data Δ_α which consists of all monic irreducible polynomials over $\mathbb{F}_q$ and associated to each such polynomial $f \in \Phi$, is a partition $\lambda_f \vdash |\lambda_f|$, where $|\lambda_f| \geq 0$, and satisfies $\sum_{f\in\Phi} |\lambda_f|\deg(f) = n$. We have already seen that such a data determines α uniquely up to conjugacy in $\mathrm{GL}(n,q)$. Let $x_{f,\lambda}$ be a variable associated to a pair (f,λ) where f is a monic irreducible polynomial and λ a partition. The *cycle index* is defined to be

$$Z_{\mathrm{GL}(n,q)} = \frac{1}{|\mathrm{GL}(n,q)|} \sum_{\alpha\in\mathrm{GL}(n,q)} \prod_{\substack{f\in\Phi \\ |\lambda_f(\alpha)|>0}} x_{f,\lambda_f(\alpha)}.$$

The significance of this expression is that the coefficient of a monomial represents the probability that an element α of $\mathrm{GL}(n,q)$ belongs to its conjugacy class, which is, one over the order of its centralizer (or that of any representative of its conjugacy class). We have already seen that the size of the centralizer of an element α in $\mathrm{GL}(n,q)$ (which depends only on its combinatorial data Δ_α), is given by

$$\prod_{f\in\Delta_\alpha} \left(q^{\deg(\mathrm{f})\cdot\sum_i (\lambda'_{f,i})^2} \prod_{i\geq 1} \left(\frac{1}{q^{\deg(f)}}\right)_{m_i(\lambda_f)} \right)$$

where the notation $\left(\frac{u}{q}\right)_i$ denotes $(1-\frac{u}{q})(1-\frac{u}{q^2})\cdots(1-\frac{u}{q^i})$. The following proposition gives the cycle index generating function in a neat form (see Section 2.1, [Ful02]), which will be useful for our purpose. This is the analogous version of Proposition 5.3.1, which gives the cycle index generating function for S_n.

Proposition 5.3.2.

$$1+\sum_{n=1}^{\infty} Z_{\mathrm{GL}(n,q)}u^n = \prod_{f\in\Phi}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j} x_{f,\lambda}\frac{u^{j.\deg(f)}}{q^{\deg(f).\sum_i(\lambda_i')^2}\prod_{t\geq 1}\left(\frac{1}{q^{\deg(f)}}\right)_{m_t(\lambda)}}\right).$$

We will now apply the cycle index to obtain generating functions for the proportions of regular, regular semisimple, and semisimple matrices in GL(n,q) (see once again [Ful99], and [Ful02]). Let $\alpha\in\mathrm{GL}(n,q)$ be regular. We have seen that this means the combinatorial data Δ_α of α consists of polynomials $f_1,f_2,\ldots,f_k$, with associated partition $\lambda_{f_i}=(|\lambda_{f_i}|)\vdash|\lambda_{f_i}|>0$, for each $1\leq i\leq k$. Therefore, to obtain the generating function for $\frac{|\mathrm{GL}(n,q)_{\mathrm{rg}}|}{|\mathrm{GL}(n,q)|}$, which is the probability that a randomly chosen matrix in GL(n,q) is regular, we must replace $x_{f,\lambda}$ by,

$$x_{f,\lambda}=\begin{cases}1 & ;\text{when } \lambda=(j)\vdash j\\ 0 & ;\text{otherwise}\end{cases}$$

for each $f\in\Phi, j\geq 1$ and $\lambda\vdash j$, in the cycle index generating function in Proposition 5.3.2. Grouping together all polynomials of degree d in Φ, we have the generating function for proportions of regular elements in an infinite product form as follows:

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{rg}}|}{|\mathrm{GL}(n,q)|}u^n=\prod_{d\geq 1}\left(1+\sum_{j=1}^{\infty}\frac{u^{jd}}{q^{(j-1)d}(q^d-1)}\right)^{N(q,d)}. \tag{5.4}$$

The above generating function gives an alternate form (see [Wal99]) as follows:

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{rg}}|}{|\mathrm{GL}(n,q)|}u^n=\prod_{d\geq 1}\left(1-\frac{u^d}{q^d}\right)^{-N(q,d)}\prod_{d\geq 1}\left(1+\frac{u^d}{q^d(q^d-1)}\right)^{N(q,d)}. \tag{5.5}$$

Let $\alpha\in\mathrm{GL}(n,q)$ be semisimple. Once again from chapter 4, this means that the combinatorial data Δ_α of α consists of polynomials $f_1,f_2,\ldots,f_k$, with associated partition $\lambda_{f_i}=(1,1,\ldots,1)\vdash|\lambda_{f_i}|>0$, for each $1\leq i\leq k$. Therefore, to obtain the generating function for $\frac{|\mathrm{GL}(n,q)_{\mathrm{ss}}|}{|\mathrm{GL}(n,q)|}$, which is the probability that a randomly chosen matrix in GL(n,q) is semisimple, we must replace $x_{f,\lambda}$ by,

$$x_{f,\lambda}=\begin{cases}1 & ;\text{when } \lambda=(1,1,\ldots,1)\vdash j\\ 0 & ;\text{otherwise}\end{cases}$$

for each $f \in \Phi, j \geq 1$ and $\lambda \vdash j$, in the cycle index generating function. Thus we get,

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{ss}}|}{|\mathrm{GL}(n,q)|}u^n=\prod_{d\geq 1}\left(1+\sum_{j=1}^{\infty}\frac{u^{jd}}{q^{\frac{j(j-1)}{2}d}\prod\limits_{i=1}^{n}(q^{id}-1)}\right)^{N(q,d)}. \tag{5.6}$$

Finally, let $\alpha \in \mathrm{GL}(n,q)$ is regular semisimple. This means that $\lambda_{f_i} = (1) \vdash |\lambda_{f_i}| = 1$ for $1 \leq i \leq k$, where $f_i \in \Delta_\alpha$ for $1 \leq i \leq k$ with $|\lambda_{f_i}| > 0$. Thus, to obtain the generating function for $\frac{|\mathrm{GL}(n,q)_{\mathrm{rs}}|}{|\mathrm{GL}(n,q)|}$, which is the probability that a randomly chosen matrix in GL(n,q) is regular semisimple, we must replace $x_{f,\lambda}$ by,

$$x_{f,\lambda}=\begin{cases}1 & ;\text{when } \lambda=(1)\vdash j=1\\ 0 & ;\text{otherwise}\end{cases}$$

for each $f \in \Phi, j \geq 1$ and $\lambda \vdash j$, in the cycle index generating function. Thus we get the generating function as follows,

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{rs}}|}{|\mathrm{GL}(n,q)|}u^n=\prod_{d\geq 1}\left(1+\frac{u^d}{q^d-1}\right)^{N(q,d)}. \tag{5.7}$$

The above three generating functions as we will see in Chapter 7, will be constructed in the more general context of powers where these will turn up as particular cases. We will use the cycle index to construct these generating functions.

Chapter 6

Asymptotics of powers in finite groups of Lie type

This chapter deals with the author's work in [KKS20]. We work in the setting of Chapter 3. Let $k = \bar{\mathbb{F}}_q$ and G be a connected reductive group over k. Let F be a Steinberg endomorphism on G giving rise to a finite group of Lie type $G(\mathbb{F}_q) = G^F$. Let $M \geq 2$ be a positive integer. We consider the power map $\omega\colon G \to G$ given by $x \mapsto x^M$. Clearly, this map is defined over $\mathbb{F}_q$. We consider the image of the set $G(\mathbb{F}_q)$ under this map, denoted as $G(\mathbb{F}_q)^M$. Let $G(\mathbb{F}_q)_{\mathrm{rg}}, G(\mathbb{F}_q)_{\mathrm{ss}}, G(\mathbb{F}_q)_{\mathrm{rs}}$ denote the set of regular elements, semisimple elements and, regular semisimple elements in $G(\mathbb{F}_q)$ respectively (see Chapter 3). Further, we denote the set of M-power regular semisimple elements as $G(\mathbb{F}_q)^M_{\mathrm{rs}} = G(\mathbb{F}_q)^M \cap G(\mathbb{F}_q)_{\mathrm{rs}}$ the set of M-power semisimple elements as $G(\mathbb{F}_q)^M_{\mathrm{ss}} = G(\mathbb{F}_q)^M \cap G(\mathbb{F}_q)_{\mathrm{ss}}$, and M-power regular elements as $G(\mathbb{F}_q)^M_{\mathrm{rg}} = G(\mathbb{F}_q)^M \cap G(\mathbb{F}_q)_{\mathrm{rg}}$. In this chapter we are interested in studying the asymptotic values of the following as $q \to \infty$:

$$\frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|}, \frac{|G(\mathbb{F}_q)^M_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|}, \frac{|G(\mathbb{F}_q)^M_{\mathrm{ss}}|}{|G(\mathbb{F}_q)|}, \frac{|G(\mathbb{F}_q)^M_{\mathrm{rg}}|}{|G(\mathbb{F}_q)|}.$$

What we mean here is that we consider the above quantities as a set of real numbers for a fixed G (thus the rank is fixed) and a fixed M; and study the limit points when $q \to \infty$.

The main theorem of this chapter (see Theorem 6.1.1) finds the $q \to \infty$ limits of the aforementioned quantities. We apply this theorem to $\mathrm{GL}(n, q)$ and $\mathrm{GU}(n, q)$ to find more explicit answers to these limiting values in Section 6.2 and 6.3 respectively, by assuming M to be a prime. The values are given in a sum-product form and are combinatorial in nature. Thus we use our knowledge of generating functions as developed in Chapter 5 to provide generating functions for these val-

ues. We will get a verification of these results in the case of $\mathrm{GL}(n,q)$ in Chapter 9, where we explicitly compute squares and cubes in the group $\mathrm{GL}(n,q)$ in some small ranks. We once again clarify the fact that we will be using the notation $G(\mathbb{F}_q)$ to mean G^F for a connected reductive group G and a Steinberg endomorphism F so that we don't have to write both F and M in the power.

6.1 The main theorem and its proof

As seen in Chapter 3, for a reductive group G over k, with Steinberg endomorphism F, a maximal torus of $G(\mathbb{F}_q)$ is the group of F-fixed points $T(\mathbb{F}_q)(=T^F)$ of a F-stable maximal torus of G. Since $T(\mathbb{F}_q) \leq G(\mathbb{F}_q)$ is a finite abelian group, it can be written as a product of cyclic groups (see [BG07], [Zav19] for the explicit cyclic structure of maximal tori in classical groups). The limiting values of the powers in $G(\mathbb{F}_q)$ as $q \to \infty$ is given in terms of the cyclic structure of maximal tori of $G(\mathbb{F}_q)$. The main theorem is as follows:

Theorem 6.1.1. *Let G be a connected reductive group defined over $\mathbb{F}_q$ with Frobenius map F. Let $M \geq 2$ be an integer. Then,*

$$\begin{aligned}\lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|} &= \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{\mathrm{ss}}|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{\mathrm{rg}}|}{|G(\mathbb{F}_q)|} \\ &= \sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}\end{aligned}$$

where the sum varies over non-conjugate maximal tori T in $G(\mathbb{F}_q)$, $T = T_{d_1,\cdots,d_s} \cong C_{d_1} \times \cdots \times C_{d_s}$ reflects the cyclic structure of T, and the group $W_T = N_{G(\mathbb{F}_q)}(T)/T$.

The rest of this section is devoted to the proof of this result. We begin with some preparatory lemma.

Lemma 6.1.2. *Let H be a finite Abelian group written as a product of cyclic groups $H = C_{d_1} \times \cdots \times C_{d_s}$. Then,*

$$\frac{|H^M|}{|H|} = \frac{1}{(M,d_1)\cdots(M,d_s)}.$$

Proof. We begin with a cyclic group, i.e, $s = 1$ case. Let $H = C_d$ be a finite cyclic group of order d. We need to show, $\frac{|C_d^M|}{|C_d|} = \frac{1}{(M,d)}$ where (M,d) denotes the gcd of M and d. Consider the map $\omega\colon C_d \to C_d$ defined by $g \mapsto g^M$. It is a group homomorphism with kernel $ker(\omega) = \{g \in C_d \mid g^M = 1\}$. Clearly, elements of the kernel are precisely given by $g^{(M,d)} = 1$. Thus, $\frac{|C_d^M|}{|C_d|} = \frac{1}{ker(\omega)} = \frac{1}{(M,d)}$.

Now, for an Abelian group H, the power map is a group homomorphism. Thus, when $H = C_{d_1} \times \cdots \times C_{d_s}$, the map $\omega\colon C_{d_1} \times \cdots \times C_{d_s} \to C_{d_1} \times \cdots \times C_{d_s}$ is $(g_1, \ldots, g_s) \mapsto (g_1^M, \ldots, g_s^M)$. Thus, kernel is given by $(g_1, \ldots, g_s)$ where $g_i^{(M,d_i)} = 1$ for all i. This gives the required result. □

Recall that, a regular semisimple element in $G(\mathbb{F}_q)$ is contained in a unique F-stable maximal torus of G (see Proposition 3.3.2, chapter 3) .

Lemma 6.1.3. *Let $\alpha \in G(\mathbb{F}_q)_{\mathrm{rs}}$. Suppose α belongs to the F-stable maximal torus $\bar{T}$. Then, $X^M = \alpha$ has a solution in $G(\mathbb{F}_q)$ if and only if $Y^M = \alpha$ has a solution in $\bar{T}(\mathbb{F}_q)$.*

Proof. Let $A \in G(\mathbb{F}_q)$ such that $A^M = \alpha$. Write Jordan decomposition $A = A_s A_u$, which implies $A_s^M = \alpha$. Now, every semisimple element belongs to some F-stable torus, say $A_s \in \bar{T}'(\mathbb{F}_q)$. Then, $\alpha \in \bar{T}'(\mathbb{F}_q)$. But, α being regular semisimple, it belongs to a unique maximal torus. Thus, $\bar{T}'(\mathbb{F}_q) = \bar{T}(\mathbb{F}_q)$, hence the solution $A_s \in \bar{T}(\mathbb{F}_q)$. □

For a reductive group G, recall that $\mathrm{rk}(G)$ denotes the rank of G. In short, we write r to denote the rank. From Chapter 2 we also know that for such a G, there is a root datum Φ, and we denote $|\Phi^+| = N$, where Φ^+ is the set of positive roots. Then, it is known that $\dim(G) = 2N + r$ and $|G(\mathbb{F}_q)| = \mathcal{O}(q^{2N+r})$. The final piece needed for the proof of the main theorem is the density result of the regular semisimple elements in $G(\mathbb{F}_q)$ which is Proposition 3.3.4. The key ingredient from this proposition is the following estimate:

$$|\{x \in T \mid x \text{ is not regular}\}| = \mathcal{O}(q^{r-1}).$$

We will use this several times. Here, T is a maximal torus of $G(\mathbb{F}_q)$.
Now we are ready to get an estimate for M^{th} power regular semisimple elements.

Theorem 6.1.4. *Let G be a reductive group defined over $\mathbb{F}_q$ with Steingberg endomorphism F. Assume that all maximal torus of $G(\mathbb{F}_q)$ are non-degenerate. Then, the proportion of M^{th} power regular semisimple elements in $G(\mathbb{F}_q)$ is,*

$$\frac{|G(\mathbb{F}_q)_{\mathrm{rs}}^M|}{|G(\mathbb{F}_q)|} = \sum_{T = T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)} + \mathcal{O}(q^{-1})$$

where the sum varies over non-conjugate maximal tori T in $G(\mathbb{F}_q)$, $T = T_{d_1,\cdots,d_s} \cong C_{d_1} \times \cdots \times C_{d_s}$ reflects the cyclic structure, and the group $W_T = N_{G(\mathbb{F}_q)}(T)/T$.

Proof. Since a regular semisimple element of $G(\mathbb{F}_q)$ belongs to a unique F-stable maximal torus, we have,

$$G(\mathbb{F}_q)^M_{\mathrm{rs}} = G(\mathbb{F}_q)_{\mathrm{rs}} \cap G(\mathbb{F}_q)^M = \bigcup_{\bar{T}\in\tau} \left(\bar{T}(\mathbb{F}_q)_{\mathrm{rs}} \cap G(\mathbb{F}_q)^M\right)$$

where τ is the set of all F-stable maximal tori of G. Now, let $\bar{T}$ be a F-stable maximal torus of G and $T = \bar{T}(\mathbb{F}_q)$. Then, from Lemma 6.1.3 we have,

$$\bar{T}(\mathbb{F}_q)_{\mathrm{rs}} \cap G(\mathbb{F}_q)^M = T_{\mathrm{rs}} \cap G(\mathbb{F}_q)^M = T^M \cap G(\mathbb{F}_q)_{\mathrm{rs}}.$$

Suppose the cyclic structure of $T = C_{d_1} \times \cdots \times C_{d_s}$. Thus, using the argument in [JKZ13, Lemma 4.5] to prove $T \cap G(\mathbb{F}_q)_{\mathrm{rs}} = q^r + \mathcal{O}(q^{r-1})$ where it is shown that the non regular elements in T are $\mathcal{O}(q^{r-1})$, we get,

$$|T^M \cap G(\mathbb{F}_q)_{\mathrm{rs}}| = |T^M| + \mathcal{O}(q^{r-1}) = \frac{1}{(M,d_1)\cdots(M,d_s)}|T| + \mathcal{O}(q^{r-1})$$

where r is the dimension of T and the second equality follows from Lemma 6.1.2. Hence,

$$\begin{aligned}\frac{|G(\mathbb{F}_q)^M_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|} &= \frac{1}{|G(\mathbb{F}_q)|}\sum_{\bar{T}\in\tau, T=\bar{T}(\mathbb{F}_q)} \left(\frac{1}{(M,d_1)\cdots(M,d_s)}|T| + \mathcal{O}(q^{r-1})\right) \\ &= \left(\sum_{T=T_{d_1,\ldots,d_s}} \frac{1}{(M,d_1)\cdots(M,d_s)}\frac{1}{|W_T|}\right) + \frac{1}{|W_T||T|}\mathcal{O}(q^{r-1})\end{aligned}$$

where we take $T = T_{d_1,\ldots,d_s}$ up to conjugacy. We note that for a fixed T, the number of conjugates is $\frac{|G(\mathbb{F}_q)|}{|W_T||T|}$ (see Proposition 3.3.9 and Corollary 3.3.10 in Chapter 3). Now, since for any H we have $(q-1)^{\dim(H)} \leq |H(\mathbb{F}_q)| \leq (q+1)^{\dim(H)}$ where $\dim(H) = 2N + r$ and r is rank of H, applying this to T, we get

$$\frac{|G(\mathbb{F}_q)^M_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|} = \sum_{T=T_{d_1,\ldots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)} + \mathcal{O}(q^{-1}).$$

This completes the proof. □

We remark that the quantity $\displaystyle\sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}$ is intrinsic to the structure of G with given M, even though it seem to involve q.

Corollary 6.1.5. *With the notation as above we have,*

$$\frac{1}{M^{rk(G)}} \leq \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|} = \sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)} \leq 1.$$

Proof. The upper end is achieved when M is coprime to the order of all maximal tori (for example, if $M \mid q$), and the lower end is achieved when M divides order of each cyclic factors in all maximal tori. Thus we have,

$$\frac{1}{M^{\mathrm{rk}(G)}} \leq \sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|M^s} \leq \sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}$$
$$\leq \sum_T \frac{1}{|W_T|} = 1.$$

□

Note that for a fixed G, the limit above depends on varying M. See Section 6.2 for explicit limiting values.

Lemma 6.1.6. *Let G be a reductive group defined over $\mathbb{F}_q$ with Steinberg endomorphism F and $M \geq 2$, an integer. Then, we have*

1. $\dfrac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|} = \dfrac{|G(\mathbb{F}_q)^M_{\mathrm{rs}}|}{|G(\mathbb{F}_q)|} + \mathcal{O}(q^{-1})$.

2. $\dfrac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|} = \dfrac{|G(\mathbb{F}_q)^M_{\mathrm{ss}}|}{|G(\mathbb{F}_q)|} + \mathcal{O}(q^{-1})$.

3. $\dfrac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|} = \dfrac{|G(\mathbb{F}_q)^M_{\mathrm{rg}}|}{|G(\mathbb{F}_q)|} + \mathcal{O}(q^{-1})$.

Proof. To prove (1) we show that $|G(\mathbb{F}_q)^M| = |G(\mathbb{F}_q)^M_{\mathrm{rs}}| + \mathcal{O}(q^{2N+r-1})$. Now,

$$|G(\mathbb{F}_q)^M| = |G(\mathbb{F}_q)^M_{\mathrm{rs}}| + |G(\mathbb{F}_q)^M_{\mathrm{nrs}}|$$

where "nrs" refers to non regular semisimple elements, and

$$|G(\mathbb{F}_q)^M_{\mathrm{nrs}}| \leq |G(\mathbb{F}_q)_{\mathrm{nrs}}| = \mathcal{O}(q^{2N+r-1})$$

gives us,

$$|G(\mathbb{F}_q)^M| = |G(\mathbb{F}_q)^M_{\mathrm{rs}}| + \mathcal{O}(q^{2N+r-1}).$$

Since $|G(\mathbb{F}_q)| = \mathcal{O}(q^{2N+r})$ we get the required result.

Now, since

$$|G(\mathbb{F}_q)^M| + \mathcal{O}(q^{2N+r-1}) = |G(\mathbb{F}_q)^M_{\mathrm{rs}}| \leq |G(\mathbb{F}_q)^M_{\mathrm{ss}}| \leq |G(\mathbb{F}_q)^M|$$

we get, $|G(\mathbb{F}_q)^M_{\mathrm{ss}}| = |G(\mathbb{F}_q)^M| + \mathcal{O}(q^{2N+r-1})$. A similar argument proves the result for regular elements. □

Proof of Theorem 6.1.1. The proof follows from Lemma 6.1.6 and Theorem 6.1.4 and Theorem 3.3.11 in Chapter 3. □

6.2 Asymptotics of powers in GL(n,q)

In this section we want to explore Theorem 6.1.1 for the group GL(n,q). We ask further question as follows: Determine all possible limiting values for a given M, that is, what are the possible values of $\sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}$ for GL(n,q). Recall, from Chapter 3 that GL(n,q) is the group of F_q-fixed points of GL(n,k) where F_q is the usual Frobenius map. Recall further that maximal tori of GL(n,q) are parametrized by partitions of n. If $(\lambda_1,\lambda_2,\ldots,\lambda_r) \vdash n$ is a partition of n, and T is a maximal tori of GL(n,q) corresponding to the partition λ, we have

$$T \cong \mathbb{F}^{\times}_{q^{\lambda_1}} \times \cdots \times \mathbb{F}^{\times}_{q^{\lambda_r}}.$$

Thus, in terms of cyclic structure, $T \cong C_{q^{\lambda_1}-1} \times \ldots \times C_{q^{\lambda_r}-1}$ (see Example 3.3.1, and 3.3.7 in Chapter 3 for detailed computations). Furthermore, $W(T)$ is $\mathcal{Z}_{S_n}(\sigma_\lambda)$, which is the centralizer of an element $\sigma_\lambda \in S_n$ where σ_λ corresponds to the partition λ (see discussion in Page 42, Chapter 3). The above discussion yields the following proposition.

Proposition 6.2.1. *The proportion of M^{th} powers in* GL(n,q) *is as follows,*

$$\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|} = \sum_{\substack{\lambda \vdash n \\ \lambda = \langle 1^{m_1}, 2^{m_2}, \cdots \rangle}} \frac{1}{\prod_i (M, q^i-1)^{m_i}} \frac{1}{|\mathcal{Z}_{S_n}(\sigma_\lambda)|} + \mathcal{O}(q^{-1})$$

where $|\mathcal{Z}_{S_n}(\sigma_\lambda)| = \prod_i m_i! i^{m_i}$.

For fixed n, M, let $\mathfrak{P}_{\mathrm{GL}}(n,q,M) := \frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$. We now assume M to be a prime and determine the possible subsequential limits of the set $\mathfrak{P}_{\mathrm{GL}}(n,q,M)$. When $M \nmid q$, denote by $o(q)$ the order of q in $(\mathbb{Z}/M\mathbb{Z})^{\times}$. Given b a positive

integer, let us define

$$\pi_b(\lambda) = \begin{cases} \sum_{b|i} m_i & \text{if } 1 \leq b \leq n, \\ 0 & \text{otherwise} \end{cases}$$

for $\lambda = \langle 1^{m_1}, 2^{m_2}, \cdots \rangle$ a partition of n. Thus, $\pi_b(\lambda)$ is the number of parts (counted with multiplicity) of λ divisible by b. It is quite easy to determine the surjectivity of the power maps for $GL(n,q)$.

Proposition 6.2.2. *Let $M \geq 2$ be a prime and $\omega\colon \mathrm{GL}(n,q) \to \mathrm{GL}(n,q)$ be the power map $x \mapsto x^M$. Then, ω is surjective if and only if $(M,q) = 1$ and $o(q) > n$ where $o(q)$ is order of q in $(\mathbb{Z}/M\mathbb{Z})^\times$.*

Proof. For any finite group G, and M a prime, ω is surjective if and only if $(M, |G|) = 1$. Now we know that $|GL(n,q)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^{n}(q^i - 1)$. Hence, the result follows. □

Proposition 6.2.3. *Let M be a prime. Then,*

1. *if $M \mid q$ then, $\lim_{q\to\infty} \mathfrak{P}_{\mathrm{GL}}(n,q,M) = 1$.*
2. *If $(M,q) = 1$ then,*

$$\lim_{q\to\infty} \mathfrak{P}_{\mathrm{GL}}(n,q,M) = \sum_{\lambda\vdash n} \frac{1}{M^{\pi_{o(q)}(\lambda)}} \frac{1}{|\mathcal{Z}_{S_n}(\sigma_\lambda)|}.$$

Thus, there are at most $1 + \nu(M-1)$ subsequential limits of $\mathfrak{P}_{\mathrm{GL}}(n,q,M)$ as $q \to \infty$, where $\nu(M-1) = |\{a \mid 1 \leq a \leq n \text{ and } a \mid (M-1)\}|$.

Proof. If $M \mid q$, all semisimple elements of GL(n,q) (being of order coprime to q) remain in GL$(n,q)^M$. Thus, we get

$$\lim_{q\to\infty} \mathfrak{P}_{\mathrm{GL}}(n,q,M) = \lim_{q\to\infty} \frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|} = 1.$$

Now we may assume $(M,q) = 1$. If $o(q) > n$ then the limit is 1 which is already obtained. Thus, we consider $o(q) \leq n$. In view of Proposition 6.2.1, all we need to find out is when $(M, q^i - 1) = M$. We claim that, $(M, q^i - 1) = M$ if and only if $o(q) \mid i$. For if, $M \mid (q^i - 1)$, then we have $q^i \equiv 1 \pmod{M}$. Thus, $o(q) \mid i$. This gives the formula.

Now, $o(q)$ is something which divides $M - 1$ and λ can have at most n parts, we note that $\pi_{o(q)}(\lambda)$ can take at most $\nu(M-1)$ values.

However, for being a limit point of a set it remains to show that there are infinitely many values of q giving rise to the same value. For this, we need to prove that given a there are infinitely many q which are of order a in $(\mathbb{Z}/M\mathbb{Z})^\times$. Since $(q, M) = 1$, it follows from Dirichlet's theorem on primes in an arithmetic progression that there are infinitely many primes of the form $q + xM$. Notice that the order of each such prime is the same as a in $(\mathbb{Z}/M\mathbb{Z})^\times$. This completes the proof. □

We remark that for the case $M \mid q$, the same formula works where we may take $\pi_a(\lambda) = 0$ for all λ.

Corollary 6.2.4. *For $M = 2$, these values are*

$$1 \text{ and } \sum_{\lambda \vdash n} \frac{1}{2^{\pi(\lambda)} |\mathcal{Z}_{S_n}(\sigma_\lambda)|}$$

where $\pi(\lambda)$ denotes the number of parts of λ.

Example 6.2.5. Consider $G := \mathrm{GL}(2, q)$. When $M = 2$, the limit points are 1 and, $\frac{1}{2^2.2!} + \frac{1}{2.2} = \frac{1}{8} + \frac{1}{4} = \frac{3}{8}$.

When $M = 3$, then one of the limit points is 1. To find the other two limit points we first observe that $(\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$. Thus there are two possible value of $o(q)$ which are 1 and 2. When $o(q) = 1$, the limit point is given by,

$$\sum_{\lambda \vdash 2} \frac{1}{3^{\pi_1(\lambda)}.|\mathcal{Z}_{S_n}(\sigma_\lambda)|} = \frac{1}{3^2.2!} + \frac{1}{3.2} = \frac{1}{18} + \frac{1}{6} = \frac{2}{9}.$$

When $o(q) = 2$, the limit point is given by,

$$\sum_{\lambda \vdash 2} \frac{1}{3^{\pi_2(\lambda)}.|\mathcal{Z}_{S_n}(\sigma_\lambda)|} = \frac{1}{2!} + \frac{1}{3.2} = \frac{1}{2} + \frac{1}{6} = \frac{2}{3}.$$

Thus, the possible subsequential limits of $\mathfrak{P}_{\mathrm{GL}}(2, q, 3)$ as q varies is given by $\{1, \frac{2}{9}, \frac{2}{3}\}$.

Example 6.2.6. Consider $G := \mathrm{GL}(3, q)$. When $M = 2$, the limit points are given by 1 and,

$$\sum_{\lambda \vdash 3} \frac{1}{2^{\pi(\lambda)} |\mathcal{Z}_{S_n}(\sigma_\lambda)|} = \frac{1}{2^3.3!} + \frac{1}{2^2.2} + \frac{1}{2.3} = \frac{1}{48} + \frac{1}{8} + \frac{1}{6} = \frac{5}{16}.$$

When $M = 3$, once again we observe that $o(q) = 1$ or, 2 or q is a power of 3, in which case the limiting value is 1. When $o(q) = 1$, the limiting value is given

by,

$$\sum_{\lambda\vdash 3}\frac{1}{3^{\pi_1(\lambda)}|\mathcal{Z}_{S_n}(\sigma_\lambda)|}=\frac{1}{3^3.3!}+\frac{1}{3^2.2}+\frac{1}{3.3}=\frac{1}{162}+\frac{1}{18}+\frac{1}{9}=\frac{14}{81}.$$

When $o(q)=2$, the limiting value is,

$$\sum_{\lambda\vdash 3}\frac{1}{3^{\pi_2(\lambda)}|\mathcal{Z}_{S_n}(\sigma_\lambda)|}=\frac{1}{3!}+\frac{1}{3.2}+\frac{1}{3}=\frac{1}{6}+\frac{1}{6}+\frac{1}{3}=\frac{2}{3}.$$

Thus the possible subsequential limits of $\mathfrak{P}_{\mathrm{GL}}(3,q,3)$ as q varies is given by $\{1,\frac{14}{81},\frac{2}{3}\}$.

We look at another example involving $\mathrm{SL}(n,q)$. In $\mathrm{SL}(n,q)$ the non-conjugate maximal tori are parametrized by the partitions of n, once again. The cyclic structure of maximal tori of this group is determined by Theorem 1 in [Zav19]. We just compute the limiting values for $\mathrm{SL}(2,q)$, although we mention that, once again for M prime, the possible subsequential limits for $\frac{|\mathrm{SL}(n,q)^M|}{|\mathrm{SL}(n,q)|}$ as $q\to\infty$ can be found explicitly as has been done in the $\mathrm{GL}(n,q)$ case.

Example 6.2.7. For the group $\mathrm{SL}(2,q)$, we have

$$\lim_{q\to\infty}\frac{|\mathrm{SL}(2,q)^M|}{|\mathrm{SL}(2,q)|}=\frac{1}{2(M,q-1)}+\frac{1}{2(M,q+1)}.$$

since corresponding to the partition $(1,1)\vdash 2$, the maximal torus is isomorphic to $\mathbb{F}_q^\times$, whereas for the partition $(2)\vdash 2$, the maximal torus is isomorphic to $\mathbb{F}_q^1=\{\alpha\in(\mathbb{F}_{q^2})^\times\mid \alpha^{1+q}=1\}$. When q is odd and M is a prime this takes the values

$$\begin{cases}\frac{1}{2} & \text{if } M=2\\ \frac{M+1}{2M} & \text{if } M \text{ coprime to } q, \text{ and divides order of SL(2,q)}\\ 1 & \text{otherwise.}\end{cases}$$

This explains the limits obtained in [KS20a, Theorem 5.1].

6.2.1 Generating function for the limit points of powers in GL(n,q)

For a prime $M\geq 2$, from Proposition 6.2.3, we have the finitely many limit points for $\mathrm{GL}(n,q)$ (except the limit point 1) of the form

$$P(n,t,M):=\sum_{\lambda=\langle 1^{m_1},2^{m_2},\ldots\rangle\vdash n}\frac{1}{M^{\pi_t(\lambda)}}\frac{1}{\prod_{i\geq 1}i^{m_i}m_i!}$$

where, $t(\leq n)$ is a divisor of $M-1$ and $\pi_t(\lambda)$ denotes the number of parts in λ divisible by t. Note that if $t > n$, $P(n,t,M) = 1$ (this is the surjective case, see Proposition 6.2.2) and when $t \leq n$, $P(n,t,M) < 1$. We will write the generating function for $P(n,t,M)$ for fixed $t \leq n$ and M. We begin with a lemma.

Lemma 6.2.8.

$$\prod_{i=1}^{\infty} \exp\left(\frac{u^i}{i}\right) = \frac{1}{1-u}.$$

Proof. The coefficient of u^n in $\prod_{i=1}^{\infty} \exp\left(\frac{u^i}{i}\right)$ is $\sum_{\lambda \vdash n} \frac{1}{\prod_{i\geq 1} i^{m_i} m_i!} = 1$, which is because of the class equation of S_n. □

Proposition 6.2.9. *The generating function is as follows*

$$1 + \sum_{n=1}^{\infty} P(n,t,M)u^n = \frac{(1-u^t)^{\frac{M-1}{Mt}}}{(1-u)}.$$

Proof. By comparing coefficients we can write,

$$\begin{aligned}
1 + \sum_{n=1}^{\infty} P(n,t,M)u^n &= \left(\prod_{i\geq 1, t\nmid i} \exp\left(\frac{u^i}{i}\right)\right) \times \left(\prod_{i\geq 1, t\mid i} \exp\left(\frac{u^i}{Mi}\right)\right) \\
&= \left(\prod_{i\geq 1} \exp\left(\frac{u^i}{i}\right)\right) \times \left(\prod_{i\geq 1, t\mid i} \exp\left(\frac{u^i}{Mi}\right)\right) \times \left(\prod_{i\geq 1, t\mid i} \exp\left(\frac{u^i}{i}\right)\right)^{-1} \\
&= \left(\frac{1}{1-u}\right) \times \left(\prod_{i\geq 1} \exp\left(\frac{u^{ti}}{Mit}\right)\right) \times \left(\prod_{i\geq 1} \exp\left(\frac{u^{ti}}{ti}\right)\right)^{-1} \\
&= \left(\frac{1}{1-u}\right) \times \left(\prod_{i\geq 1} \exp\left(\frac{u^{ti}}{i}\right)\right)^{1/Mt} \times \left(\prod_{i\geq 1} \exp\left(\frac{u^{ti}}{i}\right)\right)^{-1/t}
\end{aligned}$$

Replacing u by u^t in Lemma 6.2.8 and substituting above we get,

$$1 + \sum_{n=1}^{\infty} P(n,t,M)u^n = \left(\frac{1}{1-u}\right) \times \left(\frac{1}{1-u^t}\right)^{1/Mt} \times \left(\frac{1}{1-u^t}\right)^{-1/t} = \frac{(1-u^t)^{\frac{M-1}{Mt}}}{1-u}.$$

This proves the proposition. □

We explain this through an example here.

Example 6.2.10. Consider $M = 3$. The, the divisors of $M-1$ are 1 and 2.

t	G.F. of $P(n,t,3)$	Small order terms
1	$(1-u)^{-\frac{1}{3}}$	$1+\frac{1}{3}u+\frac{2}{9}u^2+\frac{14}{81}u^3+\frac{35}{243}u^4+\frac{91}{729}u^5+\frac{728}{6561}u^6+\mathcal{O}(u^7)$
2	$\frac{(1-u^2)^{1/3}}{1-u}$	$1+u+\frac{2}{3}u^2+\frac{2}{3}u^3+\frac{5}{9}u^4+\frac{5}{9}u^5+\frac{40}{81}u^6+\mathcal{O}(u^7)$

Table 6.1: Small values of $P(n,t,3)$.

Therefore, when $n=1$, the set of limit points are $\{1,\frac{1}{3}\}$. For $n=2$, the set of limit points are $\{1,\frac{2}{9},\frac{2}{3}\}$ and for $n=3$, the set of limit points are $\{1,\frac{14}{81},\frac{2}{3}\}$.

To end this section, we explore some further properties of $P(n,t,M)$ using its generating function.

Lemma 6.2.11. *Let $r\geq 2$ be any integer. Suppose $\omega\neq 1$ be an r^{th} root of unity. Suppose $f(x)$ is a function such that $f(x)=f(\omega x)$. Let $g(x)=(1+x+x^2+\ldots+x^{r-1})f(x)$. If $g(x)=\sum_{n=0}^{\infty}a_nx^n$ then we must have, $a_{kr}=a_{kr+1}=\cdots=a_{kr+k-1}$ for every $k\geq 0$.*

Using this we prove the following property of $P(n,t,M)$.

Proposition 6.2.12. *$P(kt,t,M)=P(kt+1,t,M)=\ldots=P(kt+k-1,t,M)$ for all $k\geq 0$, where we set $P(0,t,M)=1$.*

Proof. From Proposition 6.2.9 we have, $1+\sum_{n=1}^{\infty}P(n,t,M)u^n=\frac{(1-u^t)^{\frac{M-1}{Mt}}}{1-u}$. Let $f(u)=(1-u^t)^{\frac{M(1-t)-1}{Mt}}$. Then, $\frac{(1-u^t)^{\frac{M-1}{Mt}}}{1-u}=(1+u+\ldots+u^{t-1})f(u)$ and $f(u)=f(\omega u)$, where $\omega\neq 1$, is a t^{th} root of unity. Thus, the result holds by Lemma 6.2.11. □

6.3 Asymptotics of powers in GU(n,q)

Similar to Section 6.2, we want to get the estimates in Theorem 6.1.1, for the unitary group GU(n,q). Recall that GU(n,q) is obtained from GL$(n,\bar{\mathbb{F}}_q)$ with the Frobenius map $F\colon (a_{ij})\mapsto {}^t(a_{ij}^q)^{-1}$. Thus, GU$(n,q)\leq$ GL(n,q^2). Once again, the question is to determine the limit $\sum_{T=T_{d_1,\cdots,d_s}}\frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}$ more explicitly. The maximal tori for this group is well known and can be, for example, found in [GKSV19, Section 2]. We recall the same along with its cyclic structure which we require for our purpose.

Similar to the case of GL(n,q), the conjugacy classes of maximal tori in GU(n,q) are in one-one correspondence with the conjugacy classes of S_n. Hence,

the non-conjugate maximal tori are parameterized by the partitions of n. For a maximal torus T of $\mathrm{GU}(n,q)$, there exists a partition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ of n such that

$$T \cong \mathbb{M}_{\lambda_1} \times \cdots \times \mathbb{M}_{\lambda_r}$$

where $\mathbb{M}_s = \{x \in \bar{\mathbb{F}}_q \mid x^{q^s-(-1)^s} = 1\}$. Thus, the cyclic structure is $T \cong C_{q^{\lambda_1}-(-1)^{\lambda_1}} \times \ldots \times C_{q^{\lambda_r}-(-1)^{\lambda_r}}$. Note that when s is even $\mathbb{M}_s \cong \mathbb{F}_{q^s}^*$, and when s is odd, $\mathbb{M}_s = \{x \in \mathbb{F}_{q^{2s}} \mid x^{q^s+1} = 1\}$. Corresponding to a partition λ of n, let σ_λ denote the standard element of the conjugacy class of S_n with cycle-type λ. Let T be a maximal torus of $\mathrm{GU}(n,q)$ parametrized by the partition λ of n. Then, $W_T \cong \mathcal{Z}_{S_n}(\sigma_\lambda)$. For a fixed n, M, let $\mathfrak{P}_{\mathrm{GU}}(n,q,M) := \frac{|\mathrm{GU}(n,q)^M|}{|\mathrm{GU}(n,q)|}$.

Proposition 6.3.1. *The proportion of M^{th} powers in $\mathrm{GU}(n,q)$ is,*

$$\frac{|\mathrm{GU}(n,q)^M|}{|\mathrm{GU}(n,q)|} = \sum_{\substack{\lambda \vdash n \\ \lambda = \langle 1^{m_1}, 2^{m_2}, \ldots \rangle}} \prod_i \frac{1}{(M, q^i - (-1)^i)^{m_i}} \frac{1}{|\mathcal{Z}_{S_n}(\sigma_\lambda)|} + \mathcal{O}(q^{-1}).$$

Further, the set of limits $\lim_{q\to\infty} \mathfrak{P}_{\mathrm{GU}}(n,q,M)$ and $\lim_{q\to\infty} \mathfrak{P}_{\mathrm{GL}}(n,q,M)$ are same, in fact, in bijection under $q \mapsto -q$.

Proof. This is clear from the discussion above, and the Theorem 6.1.1. □

The bijection $q \mapsto -q$ reminds us of the *Ennola duality*. Ennola observed that the character table of $\mathrm{GU}(n,q)$ can be obtained from that of $\mathrm{GL}(n,q)$ by replacing q with $-q$ (see [Enn63]). This phenomena is known as the *Ennola duality*, and can also be defined in the more general setting of finite reductive groups.

Let M be a prime. Now, we determine the possible subsequential limits of the set $\mathfrak{P}_{\mathrm{GU}}(n,q,M)$ explicitly and write the generating function. For a partition $\lambda = (n_1, n_2, \ldots, n_s) \vdash n$, let us denote by $\pi'_b(\lambda)$ as follows: $\pi'_b(\lambda) = 0$ if $b > n$, else it is the number of n_i such that if n_i is even $b \mid n_i$; and if n_i is odd, b is even and $b \mid 2n_i$. Recall when $(M,q) = 1$ we denote by $o(q)$ the order of q in $(\mathbb{Z}/M\mathbb{Z})^\times$.

Proposition 6.3.2. *Let M be a prime. Then,*

1. *When $M \mid q$, we have*

$$\lim_{q\to\infty} \mathfrak{P}_{\mathrm{GU}}(n,q,M) = \lim_{q\to\infty} \frac{|\mathrm{GU}(n,q)^M|}{|\mathrm{GU}(n,q)|} = 1.$$

2. *Let $M>2$ be a prime and $(M,q)=1$. Then,*

$$\lim_{q\to\infty}\mathfrak{P}_{\mathrm{GU}}(n,q,M)=\sum_{\lambda\vdash n}\frac{1}{M^{\pi'_{o(q)}(\lambda)}|\mathcal{Z}_{S_n}(\sigma_\lambda)|}=\lim_{q\to\infty}\mathfrak{P}_{\mathrm{GL}}(n,-q,M).$$

3. *When $M=2$, and q odd,*

$$\lim_{q\to\infty}\mathfrak{P}_{\mathrm{GU}}(n,q,2)=\sum_{\lambda\vdash n}\frac{1}{2^{\pi(\lambda)}|\mathcal{Z}_{S_n}(\sigma_\lambda)|}=\lim_{q\to\infty}\mathfrak{P}_{\mathrm{GL}}(n,q,2)$$

where $\pi(\lambda)$ denotes the number of parts of λ.

Proof. If $M\mid q$, all semisimple elements of $\mathrm{GU}(n,q)$ (being of order coprime to q) remain in $\mathrm{GU}(n,q)^M$. Thus, we get

$$\lim_{q\to\infty}\mathfrak{P}_{\mathrm{GU}}(n,q,M)=\lim_{q\to\infty}\frac{|\mathrm{GU}(n,q)^M|}{|\mathrm{GU}(n,q)|}=1.$$

Now, we can assume $M\nmid q$. In view of Proposition 6.3.1, all we need to find out is when $(M,q^i-(-1)^i)=M$. We claim that, $(M,q^i-(-1)^i)=M$ if and only if when i is even $o(q)\mid i$, and when i is odd $o(q)$ is even and $o(q)\mid 2i$. For if i is even, $M\mid(q^i-1)$ if and only if $o(q)\mid i$. If i is odd, $M\mid(q^i+1)$ if and only if $o(q)$ is even and $o(q)\mid 2i$. This gives the formula. The last part is so because when q is odd, $2\mid(q^i-(-1)^i)$ for all i. □

6.3.1 Generating functions for the limit points of powers in $\mathrm{GU}(n,q)$

For a prime M and t a divisor of $M-1$, we denote

$$\tilde{P}(n,t,M)=\sum_{\lambda=\langle 1^{m_1},2^{m_2},\cdots\rangle\vdash n}\frac{1}{M^{\pi'_t(\lambda)}\prod_{i\geq 1}i^{m_i}m_i!}.$$

The generating function for $\tilde{P}(n,t,M)$ is as follows:

Proposition 6.3.3. *For M a prime, we have,*

1. *When t is odd,*

$$1+\sum_{n=1}^{\infty}\tilde{P}(n,t,M)u^n=\frac{(1-u^{2t})^{\frac{M-1}{2Mt}}}{1-u}.$$

2. *When t is even and $t/2$ is even,*

$$1 + \sum_{n=1}^{\infty} \tilde{P}(n, t, M)u^n = \frac{(1 - u^t)^{\frac{M-1}{Mt}}}{1 - u}.$$

3. *When t is even and $t/2$ is odd,*

$$1 + \sum_{n=1}^{\infty} \tilde{P}(n, t, M)u^n = \frac{(1 - u^{t/2})^{\frac{2(M-1)}{Mt}}}{1 - u}.$$

Proof. Let $o(q) = t$. Suppose t is odd. Then $o(-q) = 2t$. Now suppose t is even. Further assume that $t/2$ is even. Then $o(-q) = t$. Finally, if t is even such that $t/2$ is odd, then it is clear that $o(-q) = t/2$. The result then follows from Proposition 6.3.2 and Proposition 6.2.9. □

Example 6.3.4. Consider $M = 3$. We have the following table for all the divisors of $M - 1 = 2$.

t	G.F. of $\tilde{P}(n, t, M)$	Small order terms
1	$\frac{(1-u^2)^{1/3}}{1-u}$	$1 + u + \frac{2}{3}u^2 + \frac{2}{3}u^3 + \frac{5}{9}u^4 + \frac{5}{9}u^5 + \frac{40}{81}u^6 + \mathcal{O}(u^7)$
2	$(1 - u)^{-\frac{1}{3}}$	$1 + \frac{1}{3}u + \frac{2}{9}u^2 + \frac{14}{81}u^3 + \frac{35}{243}u^4 + \frac{91}{729}u^5 + \frac{728}{6561}u^6 + \mathcal{O}(u^7)$

Table 6.2: Small values of $\tilde{P}(n, t, 3)$.

Once again we see when $n = 1$, the set of limit points are $\{1, \frac{1}{3}\}$. For $n = 2$, the set of limit points are $\{1, \frac{2}{9}, \frac{2}{3}\}$ and for $n = 3$, the set of limit points are $\{1, \frac{14}{81}, \frac{2}{3}\}$. Thus the sets are clearly same as in the case of GL(n, q).

Chapter 7

M^{th} powers in $\mathbf{GL}(n,q)$ when $(M,q)=1$

This chapter deals with the author's work in [KS20b]. In the previous chapter, we have dealt with the asymptotic of powers in a general finite reductive group. In this chapter, we specialize over the general linear group $\mathrm{GL}(n,q)$ of all $n\times n$ invertible matrices with entries in $\mathbb{F}_q$, and determine explicitly the set of all matrices that are some M^{th} power.

We quickly recall some notations that we will use in this chapter (see Chapter 1). Let $M\geq 2$ be an integer. The *power map* $\omega_M : \mathrm{GL}(n,q)\to\mathrm{GL}(n,q)$ is defined by $g\mapsto g^M$. The image of ω_M denoted by $\mathrm{GL}(n,q)^M=\{g^M \mid g\in\mathrm{GL}(n,q)\}$, is the set of all invertible matrices which are M^{th} powers, or in other words, possess M^{th} root. It is easy to see that the image $\mathrm{GL}(n,q)^M$ is closed under conjugation and hence is a union of conjugacy classes of $\mathrm{GL}(n,q)$. Let C be a conjugacy class of $\mathrm{GL}(n,q)$ which is contained in $\mathrm{GL}(n,q)^M$. We call C a M^{th} *power conjugacy class.*

In this chapter, one of the main questions we will address is which invertible matrices are M^{th} powers. As a consequence of the Jordan decomposition of invertible matrices, it is necessary that the determination of M^{th} powers must be divided into two separate cases, depending on the gcd of M and q. The first case is when $(M,q)=1$ which is dealt with in this chapter. In the next chapter we deal with the case of $(M,q)\neq 1$. The question of enumeration of M^{th} powers is approached in the sense of generating function. We will use the theory of cycle index to deduce the generating function for the proportion of M^{th} powers in $\mathrm{GL}(n,q)$, which is $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$. We also deduce the generating function for the number of conjugacy classes which are M^{th} powers, denoted by $c(n,M)$.

In addition to this we deal with certain kind of elements. Let $\mathrm{GL}(n,q)^M_{\mathrm{rg}}$,

$\mathrm{GL}(n,q)^M_{\mathrm{ss}}$, $\mathrm{GL}(n,q)^M_{\mathrm{rs}}$ denote those regular, semisimple and, regular semisimple invertible matrices which are in the set $\mathrm{GL}(n,q)^M$ of M^{th} power invertible matrices. In short, these denote the set of M^{th} power regular, M^{th} power semisimple, and M^{th} power regular semisimple elements in $\mathrm{GL}(n,q)$. These sets are also characterized and generating function for the proportion of such elements are given. It is noteworthy that proportions of M^{th} power regular, semisimple and regular semisimple elements are generalization of proportion of regular, semisimple and regular semisimple elements in $\mathrm{GL}(n,q)$, by taking $M = 1$, and as such the generating functions obtained for the former proportions are generalization of the generating functions obtained for the latter proportions (see Section 5.3, Chapter 5). We also obtain generating functions for $c(n,M)_{\mathrm{rg}}$, $c(n,M)_{\mathrm{ss}}$ and, $c(n,M)_{\mathrm{rs}}$ which are the M^{th} power regular, M^{th} power semisimple and, M^{th} power regular semisimple conjugacy classes of $\mathrm{GL}(n,q)$ respectively.

To characterize a matrix which is a M^{th} power, certain kinds of polynomials, which we call M-power polynomials, play a crucial role. We start this chapter with a detailed investigation of such polynomials.

7.1 M-power polynomials

Recall from Chapter 4 that the set of all monic, irreducible polynomials of degree ≥ 1 over the field $\mathbb{F}_q$, except x, is denoted as Φ. Counting of this set is done using $N(q,d)$ (see Equation 5.2, Chapter 5). Let $M \geq 2$ be an integer. For a polynomial $f(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0 \in \mathbb{F}_q[x]$ we denote the composed polynomial,

$$f(x^M) = x^{Md} + a_{d-1}x^{M(d-1)} + \ldots + a_1x^M + a_0,$$

where we substitute x^M in place of x in the expression of $f(x)$. Now we define,

Definition 7.1.1 (M-power polynomial)**.** A non-constant, irreducible, monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree d is said to be an *M-power polynomial* if $f(x^M)$ has an irreducible factor of degree d. In general, a non-constant, monic polynomial f is said to be an *M-power polynomial* if each irreducible factor of f is an M-power polynomial.

Example 7.1.2. The polynomial $x - a \in \mathbb{F}_q[x]$ is M-power if and only if $a \in \mathbb{F}_q^M = \{a^M \mid a \in \mathbb{F}_q\}$.

We denote the set of monic, irreducible polynomials which are M-power by $\tilde{\Phi}^M$ and denote $\Phi^M = \tilde{\Phi}^M \setminus \{x\}$. Let $\tilde{N}_M(q,d)$ be the number of polynomials of degree

d in $\tilde{\Phi}^M$ and $N_M(q,d)$ be that of Φ^M. We have a simple relation $N_M(q,d) = \tilde{N}_M(q,d)$ except for $d=1$ and $N_M(q,1) = \tilde{N}_M(q,1) - 1 = \frac{q-1}{(M,q-1)}$.

Example 7.1.3. Let us compute $N_2(q,2)$, i.e., the number of 2-power polynomials of degree 2 over $\mathbb{F}_q$. An irreducible polynomial f of degree 2 can be factored over $\mathbb{F}_{q^2}$ as $f(x) = (x-\alpha)(x-\sigma(\alpha))$ where σ is the Frobenius automorphism. Now, $f(x^2) = (x^2-\alpha)(x^2-\sigma(\alpha))$ has a factor of degree 2 over $\mathbb{F}_q$ if and only if α has a square root. Thus, for $N_2(q,2)$ we need to count elements α which are in $(\mathbb{F}_{q^2}^*)^2$ but not in $\mathbb{F}_q$. We get, $N_2(q,2) = \frac{1}{2}\left(\frac{q^2-1}{(2,q^2-1)} - (q-1)\right)$.

More generally we have the following (thanks to Prof. Will Sawin),

Proposition 7.1.4. *For $d > 1$ we have,*

$$N_M(q,d) = \frac{1}{d}\sum_{r|d}\mu(r)\frac{\left(M(q^{d/r}-1),(q^d-1)\right)}{(M,q^d-1)}.$$

Proof. Our proof is generalisation of the proof for $N(q,d)$ in [CM11]. Let f be an irreducible M-power polynomial of degree $d>1$. That is, $f(x^M)$ has an irreducible factor of degree d. The irreducible polynomial f is characterised with its root in $\mathbb{F}_{q^d}$. Consider the field extension $\mathbb{F}_{q^d}$ of $\mathbb{F}_q$ and the power map $\theta\colon \mathbb{F}_{q^d}^* \to \mathbb{F}_{q^d}^*$ defined by $\theta(x) = x^M$. Thus, M-power polynomial f is characterised by an element in the image of θ which is primitive. Now, consider the set

$$T = \{\alpha \in \mathbb{F}_{q^d}^* \mid \alpha \in \mathbb{F}_{q^d}^M, \alpha \notin \text{ any proper subfield of } \mathbb{F}_{q^d}\}.$$

Then, we get $N_M(q,d) = \frac{1}{d}|T|$. Now we count the set T. To do this, we count $T(d,e) = \{\alpha^M \in \mathbb{F}_{q^e} \mid \alpha \in \mathbb{F}_{q^d}\}$ and apply the inclusion-exclusion principle. The number of pre-images of each element in $Im(\theta)$ is $|Ker(\theta)|$, which is (M, q^d-1). Now, suppose $\alpha \in \mathbb{F}_{q^d}^*$, such that $\alpha^M \in \mathbb{F}_{q^e}$. Then $\left(\alpha^M\right)^{q^e} = \alpha^M$. Thus, the number of $\alpha \in \mathbb{F}_{q^d}^*$, which are solution of the equation $\alpha^{M(q^e-1)} = 1$, is $(M(q^e-1), q^d-1)$. Hence we get $|T(d,e)| = \frac{(M(q^e-1),q^d-1)}{(M,q^d-1)}$. The result follows. □

For some small values of M and d we write $N_M(q,d)$ in tables below.

q	$N_2(q,2)$	$N_2(q,3)$	$N_2(q,4)$
odd	$\frac{1}{4}(q-1)^2$	$\frac{1}{6}(q^3-q)$	$\frac{1}{8}(q^2-1)^2$
even	$\frac{1}{2}(q^2-q)$	$\frac{1}{3}(q^3-q)$	$\frac{1}{4}(q^4-q^2)$

Table 7.1: Values of $N_2(q,2)$, $N_2(q,3)$, and $N_2(q,4)$

$q \pmod 3$	$N_3(q,2)$	$N_3(q,3)$	$N_3(q,4)$
0	$\frac{1}{2}(q^2-q)$	$\frac{1}{3}(q^3-q)$	$\frac{1}{4}(q^4-q^2)$
1	$\frac{1}{6}(q^2-q)$	$\frac{1}{9}(q^3-3q+2)$	$\frac{1}{12}(q^4-q^2)$
2	$\frac{1}{6}(q-1)(q-2)$	$\frac{1}{3}(q^3-q)$	$\frac{1}{12}(q^4-q^2)$.

Table 7.2: Values of $N_3(q,2)$, $N_3(q,3)$, and $N_3(q,4)$

Now, we move on to the problem of determining the degrees of irreducible polynomials occurring in the unique factorization of the composed polynomial $f(x^M)$, corresponding to an irreducible polynomial f. This determination of degrees will play a crucial role in determining the M^{th} powers in $\mathrm{GL}(n,q)$. Since we are trying to determine the M^{th} powers in $\mathrm{GL}(n,q)$ when $(M,q)=1$ in this chapter, we will now study M-power polynomials when $(M,q)=1$.

7.1.1 M-power polynomials when $(M,q)=1$

There is an extensive literature to determine the factors of polynomial $f(x^M)$ (more generally for composition of two polynomials) and their degrees. For $(s,q)=1$, the notation $\mathfrak{M}(s;q)$ is the order of q in $(\mathbb{Z}/s\mathbb{Z})^\times$, that is $\mathfrak{M}(s;q)$ is the smallest integer such that $q^{\mathfrak{M}(s;q)} \equiv 1 \pmod s$. For an irreducible polynomial $f(x)$, which is not x, exponent of f is the order of a root (which is same for all roots) of $f(x)$ in the multiplicative group $\bar{\mathbb{F}_q}^*$ (see [LN83, Chapter 3, Section 1]). We mention the following result due to Butler (see [But55, Theorem in Section 3]) which we need in sequel.

Proposition 7.1.5 (Butler)**.** *Let $f(x)$ be an irreducible polynomial of degree d over $\mathbb{F}_q$ and $(q,M)=1$. Let t be the exponent of $f(x)$. Write $M=M_1M_2$ in such a way that $(M_1,t)=1$ and each prime factor of M_2 is a divisor of t. Then,*

1. *$f(x^M)$ has no repeated roots.*
2. *The multiplicative order of each root of $f(x^M)$ in $\bar{\mathbb{F}_q}^*$ is M_2tb, for some b that $b \mid M_1$.*
3. *Further, for a fixed $b \mid M_1$, the number of irreducible factors of $f(x^M)$ of which roots have the above order is*

$$\frac{M_2 d\phi(b)}{\mathfrak{M}(M_2tb;q)}$$

and each of the factors is of degree $\mathfrak{M}(M_2tb;q)$, where ϕ is Euler's totient function.

We use this to obtain some further information regarding M-power polynomials when M is a prime power.

Lemma 7.1.6. *Let $M = r^a$ where r is a prime and $(q, M) = 1$. Suppose $f(x)$ is an irreducible polynomial of degree d over $\mathbb{F}_q$ of exponent t. Then we have the following:*

1. *If $r \nmid t$, the polynomial $f(x^M)$ has an irreducible factor of degree d, that is, f is an M-power polynomial.*

2. *If $r \mid t$, the polynomial $f(x^M)$ factors as a product of r^{a-i} irreducible polynomials each of degree dr^i for some $1 \leq i \leq a$.*

Proof. Let α be a root of $f(x)$ and t be its multiplicative order. Then, $\mathbb{F}_q[\alpha] \cong \mathbb{F}_{q^d}$, hence $t \mid (q^d - 1)$ (also gives $(t, q) = 1$). In fact, because $\mathbb{F}_{q^d}$ is splitting field of f, the number d is smallest with the property that $t \mid (q^d - 1)$ (see [LN83, Theorem 3.3, 3.5]), hence $\mathfrak{M}(t; q) = d$.

First, let $r \nmid t$, then $M_1 = M$ and $M_2 = 1$. Thus, by taking $b = 1$ in part 3 of Proposition 7.1.5, $f(x^M)$ has an irreducible factor of degree $\mathfrak{M}(t; q) = d$. This shows that f is an M-power polynomial.

Now, let us consider the case when $r \mid t$, then $M_1 = 1$ and $M_2 = M = r^a$. Once again applying Proposition 7.1.5, all of the irreducible factors of $f(x^M)$ are of same degree, which is $\mathfrak{M}(r^a t; q) = s$(say). That is s is obtained from the equation $q^s \equiv 1 \pmod{r^a t}$. We claim that $d \mid s$ and $s \mid r^a d$ thus s would have required form. Since $r^a t \mid (q^s - 1)$ hence $t \mid (q^s - 1)$. This combined with the fact that the order of q modulo t is d, we get that $d \mid s$. Now, for the second one we show $q^{r^a d} \equiv 1 \pmod{r^a t}$ (which would give $s \mid r^a d$). We can write

$$(q^{r^a d} - 1) = (q^{dr^{a-1}} - 1)(q^{dr^{a-1}(r-1)} + \cdots + q^d + 1).$$

Going modulo r the second term on right becomes 0 as $q^d \equiv 1 \pmod{r}$ (as $r \mid t$). Thus this term is a multiple of r. By further reducing $a - 1$, inductively, we get $(q^{r^a d} - 1) = (q^d - 1)r^a.h$ for some h. Notice that t divides the first term. Hence the result. □

Corollary 7.1.7. *With notation as in the Lemma, let f(x) be an irreducible polynomial of degree d. Then, $\mathfrak{M}(r; q) \nmid d$ implies f is an M-power polynomial.*

Proof. We claim that if $\mathfrak{M}(r; q) \nmid d$ then $r \nmid t$. Suppose $r \mid t$, then $r \mid (q^d - 1)$. This gives $\mathfrak{M}(r; q) \mid d$, as $\mathfrak{M}(r; q)$ is the smallest with the property that $r \mid (q^{\mathfrak{M}(r;q)} - 1)$. Now, the result follows by Lemma 7.1.6. □

When M is a prime we can get an easier way to decide if $f(x)$ is an M-power using $\mathfrak{M}(M;q)$ instead of the exponent which, in general, is difficult to compute.

Lemma 7.1.8. *Let M be a prime and $(q,M)=1$. Let $f(x)$ be an irreducible polynomial of degree d over $\mathbb{F}_q$. Then we have the following:*

1. *If $\mathfrak{M}(M;q) \nmid d$, then $f(x^M)$ factors as a product of an irreducible polynomial of degree d, and $\frac{d(M-1)}{lcm(\mathfrak{M}(M;q),d)}$ irreducible polynomials of degree $lcm(\mathfrak{M}(M;q),d)$. Thus, f is an M-power polynomial.*

2. *If $\mathfrak{M}(M;q) \mid d$, then $f(x^M)$ is either irreducible or has a factor of degree d. Thus, if $f(x^M)$ is reducible it is M-power.*

Proof. Let us write $s=\mathfrak{M}(M;q)$. Let us begin with the case when $s \nmid d$. We must have $(M,t)=1$ and thus $M_1=M, M_2=1$. For if $(M,t)\neq 1$, i.e., $M \mid t$, combined with $t \mid (q^d-1)$ we get $M \mid (q^d-1)$. This gives, $s \mid d$ as t is smallest with this property which is contrary to our assumption. Thus by Proposition 7.1.5, $f(x^M)$ has factors corresponding to $b=1$ and $b=M$. For the case $b=1$ we get a factor of degree d as in the previous Lemma. It also has $\frac{d\phi(M)}{\mathfrak{M}(Mt;q)}$ factors of degree $\mathfrak{M}(Mt;q)$. We claim that $\mathfrak{M}(Mt;q)=lcm(\mathfrak{M}(M;q),d)$. But, this is clear because $(\mathbb{Z}/Mt\mathbb{Z})^\times \cong (\mathbb{Z}/M\mathbb{Z})^\times \times (\mathbb{Z}/t\mathbb{Z})^\times$ because $(M,t)=1$. This completes the proof of first part.

Now, to prove the second part we have $s \mid d$. First we take $M \nmid t$. We have $M_1=M$ and $M_2=1$. Thus $f(x^M)$ has factors $\frac{d}{\mathfrak{M}(s;q)}=1$ irreducible polynomial of degree $\mathfrak{M}(s;q)=d$ and $\frac{d(M-1)}{\mathfrak{M}(tM;q)}$ irreducible polynomials each of degree $\mathfrak{M}(tM;q)=lcm(\mathfrak{M}(M;q),d)$. Now take the case $M \mid t$. We have $M_1=1$ and $M_2=M$. Thus $f(x^M)$ is a product of $\frac{Md}{\mathfrak{M}(tM;q)}$ irreducible polynomials each of degree $\mathfrak{M}(tM;q)$ which is either d or Md (from second part of Lemma 7.1.6). When $\mathfrak{M}(tM;q)=d$ we have f an M-power, else $f(x^M)$ is irreducible. □

When $M=r^a$, we set some notation and do further counting of polynomials appearing in the Lemma 7.1.6 above. For $1 \leq i \leq a$, denote the set of all polynomials $f \in \Phi$ such that $f(x^M)$ has r^{a-i} irreducible factors each of degree $r^i \deg(f)$, by $\Phi_{M,i}$. Then by Lemma 7.1.6 we have

$$\Phi = \Phi^M \bigcup \bigcup_{i=1}^{a} \Phi_{M,i} = \bigcup_{i=0}^{a} \Phi_{M,i}$$

where, for convenience, we denote $\Phi^M = \Phi_{M,0}$. Note that the above union is disjoint. Denote $\widehat{N}(q,d) = N(q,d) - N_M(q,d)$. For $1 \leq i \leq a$, we denote the

number of irreducible polynomials $f(x)$ in $\Phi_{M,i}$ of degree d by $N_M^i(q,d)$. Thus,

$$N(q,d) = N_M(q,d) + \widehat{N}(q,d) = \sum_{i=0}^{a} N_M^i(q,d)$$

where, for notational convenience, we denote $N_M(q,d)$ as $N_M^0(q,d)$. We have the following formula for $N_M^i(q,d)$.

Proposition 7.1.9. *Let $M = r^a$ where r is a prime. For natural numbers d and e, let $\widetilde{T}(d,e)$ denote the number of field generators of $\mathbb{F}_{q^e}$, that has a M^{th} root in the field $\mathbb{F}_{q^d}$. Then, for $1 \leq i \leq a$ we have,*

$$N_M^i(q,d) = \frac{1}{d}\left(|\tilde{T}(dr^i,d)| - |\tilde{T}(dr^{i-1},d)|\right).$$

Proof. The proof is similar to that of Proposition 7.1.4. Since $\widetilde{T}(d,e)$ denotes the number of field generators of $\mathbb{F}_{q^e}$, that has a M^{th} root in the field $\mathbb{F}_{q^d}$ we have,

$$|\tilde{T}(d,e)| = \sum_{r|e} \mu(r) \frac{\left(M(q^{e/r}-1), q^d-1\right)}{(M, q^d-1)}$$

where μ is the Mobius function. Comparing with the proof of Proposition 7.1.4, we note that $\frac{1}{d}|\tilde{T}(d,d)| = N_M(q,d)$.

To compute $N_M^i(q,d)$, we need to find the number of field generators of $\mathbb{F}_{q^d}$ which possess M^{th} root in the field $\mathbb{F}_{q^{dr^i}}$ but not in any smaller subfield between $\mathbb{F}_{q^{dr^i}}$ and $\mathbb{F}_{q^d}$. The set $\widetilde{T}(dr^i,d)$ gives the total number of field generators of $\mathbb{F}_{q^d}$, which posses M^{th} root in the field $\mathbb{F}_{q^{dr^i}}$. Thus, to get $N_M^i(q,d)$ we need to subtract $|\widetilde{T}(dr^{i-1},d)|$. Finally we also note that we d such elements correspond to a polynomial thus we divide by that to get the result. □

We look at an example here.

Example 7.1.10. Let us take $M = 2^2$ and $d = 1$. We have already seen $N_4^0(q,1) = N_4(q,1) = \frac{q-1}{(4,q-1)}$. Now, $N_4^1(q,1)$ counts the number of polynomials $x - \lambda$, such that $x^4 - \lambda$ factors as a product of two irreducible degree 2 polynomials. Thus we have, $N_4^1(q,1) = \left(\frac{(q-1)(4,q+1)}{(4,q^2-1)} - \frac{q-1}{(4,q^2-1)}\right) = \frac{q-1}{(4,q^2-1)}\left((4,q+1)-1\right)$. Finally, $N_4^2(q,1)$ counts the number of polynomials $x - \lambda$ such that $x^4 - \lambda$ is irreducible. Thus,

$$N_4^2(q,1) = \frac{(4(q^2-1), q^4-1)}{(4,q^4-1)} - \frac{(4(q-1), q^4-1)}{(4,q^4-1)} - \frac{(4(q-1), q^2-1)}{(4,q^2-1)}$$

$$= (q-1)\left(\frac{(q+1)(4,q^2+1)}{(4,q^4-1)} - \frac{(4,q^3+q^2+q+1)}{(4,q^4-1)} - \frac{(4,q+1)}{(4,q^2-1)}\right).$$

7.2 M^{th} powers in GL(n,q)

We consider the power map $\omega\colon \mathrm{GL}(n,q) \to \mathrm{GL}(n,q)$ given by $x \mapsto x^M$. We further assume that $(q,M)=1$. Let $\alpha \in \mathrm{GL}(n,q)$ with combinatorial data Δ_α which determines α up to conjugacy. We have introduced this in Section 4.1.1, Chapter 4. Conversely, to such a data we have an associated representative matrix of the conjugacy class which we make use of in the sequel for further computations.

Lemma 7.2.1. *Let $\gamma \in \mathbb{F}_q^*$ and $J_{\gamma,n} = \begin{pmatrix} \gamma & 1 & 0 & 0 & \cdots \\ & \gamma & 1 & 0 & \cdots \\ & & \ddots & \ddots & \vdots \\ & & & \gamma & 1 \\ & & & & \gamma \end{pmatrix}$ be the Jordan matrix of size n. Then, $(J_{\gamma,n})^M$ is conjugate to $J_{\gamma^M,n}$.*

Proof. We write $J_{\gamma,n} = \gamma I_n + N$ and notice that N is a nilpotent matrix satisfying $N^n = 0$ and $N^k \neq 0$ for all $k < n$. Thus,

$$(J_{\gamma,n})^M = (\gamma I_n + N)^M = \gamma^M I_n + \binom{M}{1}\gamma^{M-1} I_n N + \cdots + N^M.$$

Hence, $(J_{\gamma,n})^M$ has all diagonal entries γ^M, and all entries above the diagonal $M\gamma^{M-1}$. Since $(q,M)=1$, the result follows. □

Let $f \in \Phi$ be a polynomial of degree $k \geq 1$. Then, f splits over $\mathbb{F}_{q^k}$. The Galois automorphisms of this field is obtained by taking powers of the Frobenius automorphism denoted as σ_k. Let $f_M \in \mathbb{F}_q[x]$ be the minimal polynomial of M^{th} power of one of the roots of f. If η is a root of f then other roots of f are $\sigma_k^i(\eta)$ for $0 \leq i \leq k-1$, and f_M is the minimal polynomial of η^k. Note that f_M is uniquely associated to f, say it is of degree d. Then, $d \mid k$ and $\mathbb{F}_{q^d}$ is the splitting field of f_M which is a subfield of $\mathbb{F}_{q^k}$. We have the following,

Lemma 7.2.2. *Let $f \in \Phi$ be of degree $k \geq 1$, and f_M be minimal polynomial of M^{th} power of a root of f of degree d. Then, exactly $\frac{k}{d}$ roots of $f(x)$ raised to the power M give a root of $f_M(x)$. Further, $f(x)$ is an irreducible factor of the polynomial $f_M(x^M)$.*

Proof. Let $\eta \in \mathbb{F}_{q^k}$ be a root of $f(x)$, and $\eta^M = \zeta \in \mathbb{F}_{q^d}$ with minimal polynomial $f_M(x)$. Then, the set of roots of f is $\mathcal{S} = \{\sigma_k^i(\eta) \mid 0 \leq i \leq k-1\} \subset \mathbb{F}_{q^k}$ and under the M^{th} power map this goes inside the set $\tilde{\mathcal{S}} = \{\sigma_d^i(\zeta) \mid 0 \leq i \leq d-1\} \subset \mathbb{F}_{q^d}$

which are roots of f_M. Thus the first statement follows.

We note that η is a root of $f_M(x^M)$ as $(x^M-\zeta)=(x^M-\eta^M)$ is a factor. Thus, the minimal polynomial of η, which is f, divides $f_M(x^M)$. □

Now, we consider slightly more general case of $\alpha \in \mathrm{GL}(n,q)$ with combinatorial data Δ_α and determine the data Δ_{α^M} for α^M.

Proposition 7.2.3. *Suppose $\alpha \in \mathrm{GL}(n,q)$ with Δ_α consisting of a single irreducible polynomial f of degree k and $\lambda_f = (\lambda_1,\ldots,\lambda_l)$ where $|\lambda_f| = \frac{n}{k}$. Let f_M be the minimal polynomial of a M^{th} power of a root of f, say of degree d. Then, Δ_{α^M} consists of a single polynomial f_M and $|\lambda_{f_M}| = \frac{n}{d}$ with*

$$\lambda_{f_M} = (\underbrace{\lambda_1,\ldots,\lambda_1}_{s},\ldots,\underbrace{\lambda_l,\ldots,\lambda_l}_{s})$$

where $s = \frac{k}{d}$.

Proof. Recall from Section 5.3.2, the associated representative of conjugacy class corresponding to α is the matrix $A_\alpha = \mathrm{diag}(J_{f,\lambda_1},\ldots,J_{f,\lambda_l})$ where J_{f,λ_i} is a block matrix of size $\lambda_i.k$ with each block size k and diagonals $C(f)$. Thus to compute A_α^M we first look at a single block J_{f,λ_i}. Note that $J_{f,\lambda_i} = D+N$ where $D = \mathrm{diag}(C(f),\ldots,C(f))$ and $N = \begin{pmatrix} 0 & I & & \\ & 0 & I & \\ & & \ddots & \ddots \\ & & & 0 \end{pmatrix}$ and $DN = ND$. Thus,

$$J_{f,\lambda_i}^M = (D+N)^M = D^M + MD^{M-1}N + \cdots$$

where $D^M = \mathrm{diag}(C(f)^M,\ldots,C(f)^M)$. Since $(q,M)=1$, the data Δ_{α^M} will depend only on how $C(f)^M$ splits up. Over $\mathbb{F}_{q^k}$, the companion matrix $C(f)$ is conjugate to the diagonal matrix $\mathrm{diag}(\eta,\sigma(\eta),\ldots,\sigma^{k-1}(\eta))$ where $Gal(\mathbb{F}_{q^k}/\mathbb{F}_q) =< \sigma >$. Thus, J_{f,λ_i} is conjugate to the matrix $\mathrm{diag}(J_{\eta,\lambda_i}, J_{\sigma(\eta),\lambda_i},\ldots,J_{\sigma^{k-1}(\eta),\lambda_i})$. Now, using Lemma 7.2.1, we get J_{f,λ_i}^M is conjugate to $\mathrm{diag}(J_{\eta^M,\lambda_i}, J_{\sigma(\eta)^M,\lambda_i},\ldots,J_{\sigma^{k-1}(\eta)^M,\lambda_i})$ over $\mathbb{F}_{q^k}$. Thus, by grouping together the blocks where the conjugates of $\zeta=\eta^M$ appear, we get J_{f,λ_i}^M is conjugate to

$$\mathrm{diag}\left(\underbrace{J_{\zeta,\lambda_i}, J_{\sigma_d(\zeta),\lambda_i},\ldots,J_{\sigma_d^{d-1}(\zeta),\lambda_i}}_{1},\ldots,\underbrace{J_{\zeta,\lambda_i}, J_{\sigma_d(\zeta),\lambda_i},\ldots,J_{\sigma_d^{d-1}(\zeta),\lambda_i}}_{s}\right)$$

with s many grouped blocks, because of Lemma 7.2.2. Further, notice that

$$\text{diag}(J_{\zeta,\lambda_i}, J_{\sigma_d(\zeta),\lambda_i}, \ldots, J_{\sigma_d^{d-1}(\zeta),\lambda_i})$$

where $Gal(\mathbb{F}_{q^d}/\mathbb{F}_q) =< \sigma_d >$, is conjugate to J_{f_M,λ_i}; which is a block matrix of size $\lambda_i.d$ with block size d. Thus, J_{f,λ_i}^M is conjugate to $\text{diag}(\underbrace{J_{f_M,\lambda_i}, \ldots, J_{f_M,\lambda_i}}_{s})$. This gives us the required result. □

In this proposition, the partition λ_{f_M} can be easily visualized in the power notation of partitions where the multiplicity of each part gets multiplied by s. We can generalize the above result to a more general setup where Δ_α has more than one polynomials but the minimal polynomial of M^{th} power of a root of each one of them is a single polynomial.

Proposition 7.2.4. *Suppose $\alpha \in$ GL(n,q) with associated data Δ_α consisting of polynomials $f_i \in \Phi$ of degree d_i and partitions $\lambda_{f_i} = (\lambda_{i_1}, \lambda_{i_2}, \ldots)$, $1 \le i \le l$. Let $h(x)$ be a polynomial of degree d which is the minimal polynomial of M^{th} power of a root of each f_i for all i (that is, $(f_i)_M = h, \forall i$). Then, Δ_{α^M} consists of the single polynomial $h(x)$ and partition*

$$\lambda_{h(x)} = \left(\underbrace{\lambda_{1_1}^{\frac{d_1}{d}}, \lambda_{1_2}^{\frac{d_1}{d}}, \ldots}, \ldots, \underbrace{\lambda_{i_1}^{\frac{d_i}{d}}, \lambda_{i_2}^{\frac{d_i}{d}}, \ldots}, \ldots, \underbrace{\lambda_{l_1}^{\frac{d_l}{d}}, \lambda_{l_2}^{\frac{d_l}{d}}, \ldots}\right)$$

with $|\lambda_{h(x)}| = \frac{n}{d}$.

The proof of this follows from the earlier proposition. A more general version of this Proposition can be written where we have $h_1(x), \ldots, h_m(x)$ which are the minimal polynomials of M^{th} powers of a subset of f_i's. We also note that in this proposition the partition obtained need not be ordered. However, there is no loss here if we make it ordered.

Now, we apply the results obtained so far to get certain classes that are M^{th} power.

Proposition 7.2.5. *Let $\alpha \in$ GL(n,q) with combinatorial data Δ_α. Suppose, each partition λ_{f_i} in Δ_α has all its parts distinct. Then, $X^M = \alpha$ has a solution in* GL(n,q) *if and only if f_i is M-power for all i (that is, $f_i(x^M)$ has an irreducible factor of degree $deg(f_i)$ for all i).*

Proof. It suffices to prove this for a single polynomial $i = 1$ case. Thus we may assume, $\alpha \in$ GL(n,q) with Δ_α consisting of a single polynomial $h(x) \in \Phi$ of degree d and partition $\lambda_{h(x)}$ of $\frac{n}{d}$ has all of its parts distinct. Now, we need to prove $X^M = \alpha$ has a solution in GL(n,q) if and only if the polynomial $h(x^M)$ has

an irreducible factor of degree d.

First, let us assume that there exists an $A \in \mathrm{GL}(n,q)$ such that $A^M = \alpha$. Suppose, the combinatorial data Δ_A consists of polynomials f_i of degree d_i and partitions λ_{f_i}. Then, M^{th} power of roots of f_i, for all i, are roots of $h(x)$, i.e., $(f_i)_M = h(x)$ for all i. Therefore, by Proposition 7.2.4, the associated partition $\lambda_{h(x)}$ will have each λ_{i_j} repeating $\frac{d_i}{d}$ many times. But, we are given that parts of $\lambda_{h(x)}$ are all distinct. Hence, $d_i = d$ for all i. Thus, by fixing f as one of the f_i and by using Lemma 7.2.2, we have $s = 1$ and $h(x^M)$ has an irreducible factor of degree d, as required.

Now for converse, since $h(x^M)$ has an irreducible factor of degree d, call it $g(x)$. Then M^{th} power of each root of $g(x)$ is a root of $h(x)$. Now, take A to be the standard representative of the conjugacy class with combinatorial data Δ_A consisting of the polynomial $g(x)$ with $\lambda_{g(x)} = \lambda_{h(x)}$. From Proposition 7.2.3, we see that $\Delta_{A^M} = \Delta_\alpha$. This proves the required result. □

To obtain neat results for arbitrary α in GL(n,q) we put some restrictions on M (for example a prime power). Recall (last paragraph of Section 7.1) that for $1 \le i \le a$, we denote the set of all polynomials $f \in \Phi$ such that $f(x^M)$ has r^{a-i} irreducible factors each of degree $r^i \deg(f)$, by $\Phi_{M,i}$. Also, for convenience we denote the set of M-power polynomials $\Phi^M = \Phi_{M,0}$ and we have, $\Phi = \bigcup_{b=0}^{a} \Phi_{M,b}$.

Proposition 7.2.6. *Let $M = r^a$ where r is a prime. Let $\alpha \in \mathrm{GL}(n,q)$ with combinatorial data Δ_α consisting of polynomials $f_i \in \Phi$ of degree d_i and partitions $\lambda_{f_i} = \langle 1^{m_1(\lambda_{f_i})}, 2^{m_2(\lambda_{f_i})}, \cdots \rangle$ written in power notation, $1 \le i \le l$. Then, $X^M = \alpha$ has a solution in* GL(n,q) *if and only if for each $1 \le i \le l$, one of the following holds:*

1. $f_i \in \Phi^M$.
2. $f_i \in \Phi_{M,b}$ *for some* b, $1 \le b \le a$ *and* $r^b \mid m_j(\lambda_{f_i})$ *for all* j.

Proof. Let us first assume $X^M = \alpha$ has a solution B in GL(n,q). It is enough to prove this result when Δ_α consists of a single irreducible polynomial f with associated partition λ_f. Let the degree of f be d and hence $|\lambda_f| = \frac{n}{d}$. Since, M is a prime power, from Lemma 7.1.6 either $f(x^M)$ is an M-power polynomial or it splits into r^{a-b} irreducible polynomials each of degree dr^b for some $b \ge 1$. That is, either $f \in \Phi^M$ or $f \in \Phi_{M,b}$. We show that if (2) does not hold then f must be an M-power polynomial. Thus, let us assume that there exists i_0, such that $m_{i_0}(\lambda_f)$, the number of times i_0 appears in the partition λ_f, is not divisible by r^b. Now, we need to show that $f(x^M)$ has a factor of degree d. Let Δ_B consists of irreducible

polynomials $g_1, g_2, \ldots$ with associated partitions $\lambda_{g_1}, \lambda_{g_2}, \ldots$. Since, $B^M = \alpha$ the M^{th} power of roots of g_j are roots of f for all j. Then, from Proposition 7.2.4, we conclude that Δ_{B^M} consists of the polynomial f with the partition where each part of λ_{g_j} repeats $\frac{s_j}{d}$ times, where $deg(g_j) = s_j$. Thus, $d \mid s_j$ for all j. Notice that a particular part in λ_f can come from more than one λ_{g_j}, i.e, $m_{i_0}(f)$ is of the form $\sum_j \frac{s_j}{d}$. Now, from Lemma 7.2.2 we see that g_j are the factors of $f(x^M)$. Invoking Lemma 7.1.6, each irreducible factor of $f(x^M)$ (which are g_j in our case) has degree dr^b. Thus, $s_j = dr^b$. Since, $r^b \nmid m_{i_0}(f)$ there exists j_0 such that $r^b \nmid s_{j_0}$. Hence, $s_{j_0} = d$. This implies f is an M-power polynomial.

To prove the converse, we can work with the blocks of either kind. First, let $f \in \Phi^M$, i.e., $f(x^M)$ has an irreducible factor of degree d. Then, following the proof for converse of Proposition 7.2.5, we get a solution for $X^M = \alpha$. The main case we need to deal with is the second kind. Let α has associated data Δ_α consisting of polynomial f and partition $\lambda_f = 1^{m_1} \ldots i^{m_i} \ldots$ with the property that $f \in \Phi_{M,b}$ for some $b \geq 1$, i.e, $f(x^M)$ is a product of r^{a-b} irreducible polynomials each of degree dr^b, and $r^b \mid m_i$ for all i. Let g be one of the factors of $f(x^M)$ and $\lambda_g = 1^{\frac{m_1}{r^b}} \ldots \lambda_i^{\frac{m_i}{r^b}} \ldots$. Let B be a matrix associated with data g and λ_g. Then from Proposition 7.2.3, B^M is conjugate to α. This completes the proof. □

Now, we write a corollary of this when M is a prime.

Corollary 7.2.7. *Let M be a prime with $(q, M) = 1$. Denote $t = \mathfrak{M}(M; q)$. Let $\alpha \in$ GL(n,q) with combinatorial data Δ_α consisting of polynomials $f_i \in \Phi$ of degree d_i and partitions $\lambda_{f_i} = (\lambda_{i_1}, \lambda_{i_2}, \ldots)$, $1 \leq i \leq l$. Then, $X^M = \alpha$ has a solution in* GL(n,q) *if and only if for each $1 \leq i \leq l$ one of the following holds,*

1. *$t \nmid d_i$.*
2. *$f_i \in \Phi^M$ (in this case, it is equivalent to saying that $f_i(x^M)$ is reducible).*
3. *$M \mid m_j(\lambda_{f_i})$ for every j.*

This follows from Lemma 7.1.8.

7.3 M^{th} power regular semisimple and regular classes in GL(n,q)

In this section, we look at the regular and regular semisimple classes in GL(n,q) which are M^{th} powers and get generating function for the same.

Proposition 7.3.1. *Let $\alpha \in \mathrm{GL}(n,q)$ with associated data Δ_α. Let α be a regular element with the polynomials $f_1,\ldots,f_l$ in Δ_α. Then, $X^M = \alpha$ has a solution in $\mathrm{GL}(n,q)$ if and only if f_i is M-power polynomial, for all i.*

Proof. Since, α is regular the associated partition λ_{f_i} has single part, for all i. The result follows from Proposition 7.2.5. □

We note that if α is a regular semisimple element, we can apply this proposition as well. The generating functions are as follows.

Theorem 7.3.2. *Let $M \geq 2$ be an integer and $(q,M)=1$. For the group $\mathrm{GL}(n,q)$, the generating function for regular and regular semisimple classes which are M^{th} power is,*

1. $1+\sum_{n=1}^{\infty} c(n,M)_{\mathrm{rg}}u^n = \prod_{d\geq 1}(1-u^d)^{-N_M(q,d)}$.
2. $1+\sum_{n=1}^{\infty} c(n,M)_{\mathrm{rs}}u^n = \prod_{d\geq 1}(1+u^d)^{N_M(q,d)}$.

Proof. From Proposition 7.3.1, it follows that a regular class $\alpha \in \mathrm{GL}(n,q)$ is a M^{th} power in $\mathrm{GL}(n,q)$ if and only if each irreducible factor $f(x)$ of its characteristic polynomial $\chi_\alpha(x)$ is M-power polynomial. In other words, the regular conjugacy classes which are M^{th} power, are in one-one correspondence with the set of M-power polynomials with non-zero constant term. Therefore,

$$1+\sum_{n=1}^{\infty} c(n,M)_{\mathrm{rg}}u^n = \prod_{f\in\Phi^M}(1-u^{deg(f)})^{-1} = \prod_{d\geq 1}(1-u^d)^{-N_M(q,d)}.$$

This proves the first part.

The regular semisimple M^{th} power conjugacy classes in $\mathrm{GL}(n,q)$ are characterized by separable M-power polynomials with non-zero constant term, and hence,

$$1+\sum_{n=1}^{\infty} c(n,M)_{\mathrm{rs}}u^n = \prod_{f\in\Phi^M}(1+u^{deg(f)}) = \prod_{d\geq 1}(1+u^d)^{N_M(q,d)}.$$

This proves the required result. □

We get back the generating functions of regular classes in Proposition 5.2.2 and regular semisimple classes in Proposition 5.2.3 by putting $M=1$ in the above theorem.

Now, we can use this to get the generating function for the M^{th} power regular and regular semisimple elements.

Theorem 7.3.3. *For the group* $\mathrm{GL}(n,q)$*, and* $M \geq 2$ *with the condition that* $(q,M)=1$*,*

1. *the generating function for the regular semisimple elements which are* M^{th} *power is*

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)^M_{\mathrm{rs}}|}{|\mathrm{GL}(n,q)|}u^n=\prod_{d\geq 1}\left(1+\frac{u^d}{q^d-1}\right)^{N_M(q,d)}.$$

2. *The generating function for the regular elements which are* M^{th} *power is*

$$\begin{aligned}1+\sum_{n=1}^{\infty}\frac{|GL(n,q)^M_{\mathrm{rg}}|}{|GL(n,q)|}u^n&=\prod_{d\geq 1}\left(1+\sum_{j=1}^{\infty}\frac{u^{jd}}{q^{(j-1)d}(q^d-1)}\right)^{N_M(q,d)}\\&=\prod_{d\geq 1}\left(1-\frac{u^d}{q^d}\right)^{-N_M(q,d)}\prod_{d\geq 1}\left(1+\frac{u^d}{q^d(q^d-1)}\right)^{N_M(q,d)}.\end{aligned}$$

Proof. We use Proposition 7.2.5 here. To get (1), in the Equation 5.3.2 of cycle index generating function, we take $n=1$ on the right side (and hence the second sum runs over partitions of 1 which is (1)) and the outer product runs over all $f\in\Phi^M$. Thus, to get the desired generating function we put $x_{f,\lambda}=1$, when $f\in\Phi^M$ and 0 otherwise. We get,

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)^M_{\mathrm{rs}}|}{|\mathrm{GL}(n,q)|}u^n=\prod_{f\in\Phi^M}\left(1+\frac{u^{deg(f)}}{q^{deg(f)}-1}\right)=\prod_{d\geq 1}\left(1+\frac{u^d}{q^d-1}\right)^{N_M(q,d)}.$$

Here we used the following: for the partition $(1)=1^1$ and $q^{deg(f).\sum_i(\lambda'_i)^2}\left(\frac{1}{q^{deg(f)}}\right)_1=q^{deg(f)}\left(1-\frac{1}{q^{deg(f)}}\right)=q^{deg(f)}-1$.

The generating function for regular elements is obtained in similar fashion. Here we take the partition $(n)\vdash n$ on the right in the cycle index generating function. The transpose of this partition is $(n)'=(1,1,\ldots,1)=1^n$ and hence $q^{deg(f).\sum_i(\lambda'_i)^2}\left(\frac{1}{q^{deg(f)}}\right)_1=q^{n.deg(f)}\left(1-\frac{1}{q^{deg(f)}}\right)=q^{(n-1).deg(f)}(q^{deg(f)}-1)$. Therefore,

$$\begin{aligned}1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)^M_{\mathrm{rg}}|}{|\mathrm{GL}(n,q)|}u^n&=\prod_{f\in\Phi^M}\left(1+\sum_{j=1}^{\infty}\frac{u^{j.deg(f)}}{q^{(j-1)deg(f)}(q^{deg(f)}-1)}\right)\\&=\prod_{d\geq 1}\left(1+\sum_{j=1}^{\infty}\frac{u^{jd}}{q^{(j-1)d}(q^d-1)}\right)^{N_M(q,d)}.\end{aligned}$$

To deduce the alternate formula, we note that,

$$1+\sum_{j=1}^{\infty}\frac{u^{jd}}{q^{(j-1)d}(q^d-1)}=\left(1-\frac{u^d}{q^d}\right)^{-1}\left(1+\frac{u^d}{q^d(q^d-1)}\right)$$

which can be verified by computing coefficients on both sides. □

Once again these generating functions are generalization ($M=1$ case) of the ones obtained in Equation 5.4, 5.5 and, 5.7.

7.4 M^{th} power semisimple classes in $\mathbf{GL}(n,q)$ when M is a prime power

In this section, we deal with semisimple elements which are M^{th} power. We assume $M=r^a$ for some prime r and $(q,M)=1$.

Proposition 7.4.1. *Let $M=r^a$ be a prime power and $(q,M)=1$. Let $\alpha\in\mathrm{GL}(n,q)$ be semisimple with the corresponding combinatorial data Δ_α consisting of polynomials f_i and partitions λ_{f_i}. Then, $X^M=\alpha$ has a solution in $\mathrm{GL}(n,q)$ if and only if for each i, one of the following holds,*

1. *$f_i\in\Phi^M$.*
2. *$f_i\in\Phi_{M,b}$, for some $1\le b\le a$, and $r^b\mid|\lambda_{f_i}|$.*

Proof. We recall that when α is semisimple all partitions in Δ_α are of the form $1^{|\lambda_{f_i}|}$. Thus, the second condition in Proposition 7.2.6 becomes the required one here. □

Now recall the notation $N_M^i(q,d)$ preceding the Proposition 7.1.9. We have,

Theorem 7.4.2. *Let $M=r^a$ be a prime power and $(q,M)=1$. Then, we have the following generating functions:*

1. $$1+\sum_{n=1}^{\infty}c(n,M)_{\mathrm{ss}}u^n=\prod_{i=0}^{a}\prod_{d\ge1}\left(1-u^{r^id}\right)^{-N_M^i(q,d)}.$$
2. $$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{ss}}^M|}{|\mathrm{GL}(n,q)|}u^n=\prod_{i=0}^{a}\prod_{d\ge1}\left(1+\sum_{j=1}^{\infty}\frac{u^{r^ijd}}{q^{\frac{r^ij(r^ij-1)d}{2}}\prod_{t=1}^{r^ij}(q^{td}-1)}\right)^{N_M^i(q,d)}.$$

Proof. Recall the notation $\Phi_{M,i}$ defined at the end of Section 7.1 when $M=r^a$. By Proposition 7.2.6, it is clear that a semisimple conjugacy class which is M^{th}

power, corresponds to (in fact, one-one correspondence) a monic polynomial g of degree n over $\mathbb{F}_q$ with the property that the multiplicity of each of its irreducible factors which belong to $\Phi_{M,i}$ for some i, must be a multiple of r^i. Therefore, we get,

$$\begin{aligned}1+\sum_{n=1}^{\infty} c(n,M)_{\mathrm{ss}}u^n &= \prod_{i=0}^{a}\prod_{f\in\Phi_{M,i}}\left(1+u^{r^i deg(f)}+u^{2r^i deg(f)}+\cdots\right)\\ &= \prod_{i=0}^{a}\prod_{f\in\Phi_{M,i}}\left(1-u^{r^i deg(f)}\right)^{-1} = \prod_{i=0}^{a}\prod_{d\geq 1}\left(1-u^{r^i d}\right)^{-N_M^i(q,d)}.\end{aligned}$$

This proves the first part.

For the proof of second part, we use the cycle index generating function once again. In the Equation 5.3.2, on the right hand side, we put $x_{f,\lambda}=1$ when $\lambda=(1,1,\ldots,1)\vdash r^i j$, and $f\in\Phi_{M,i}$ for each $j\geq 1$, else we put $x_{f,\lambda}=0$. We also note that when $\lambda=(1,1,\ldots,1)\vdash n$ and $f\in\Phi$, we have,

$$\begin{aligned}q^{deg(f).\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^{deg(f)}}\right)_{m_i(\lambda)} &= q^{n^2 deg(f)}\left(1-\frac{1}{q^{deg(f)}}\right)\cdots\left(1-\frac{1}{q^{n.deg(f)}}\right)\\ &= q^{n^2.deg(f)}\frac{(q^{deg(f)}-1)\cdots(q^{n.deg(f)}-1)}{q^{\frac{n(n+1)}{2}deg(f)}}\\ &= q^{\frac{n(n-1)}{2}deg(f)}\prod_{i=1}^{n}(q^{i.deg(f)}-1).\end{aligned}$$

Therefore, we have,

$$1+\sum_{n=1}^{\infty}\frac{|\mathrm{GL}(n,q)_{\mathrm{ss}}^M|}{|\mathrm{GL}(n,q)|}u^n=\prod_{i=0}^{a}\left(\prod_{f\in\Phi_{M,i}}\left(1+\sum_{j=1}^{\infty}\frac{u^{r^i j.deg(f)}}{q^{\frac{r^i j(r^i j-1).deg(f)}{2}}\prod_{t=1}^{r^i j}(q^{t.deg(f)}-1)}\right)\right).$$

This gives the desired generating function. □

Putting $M=1$ in part (2) of the above result gives Equation 5.6 which is the generatin function for the proportion of semisimple elements.

In the case,when $M=r$ is a prime, the formula gets further simplified as i runs from 0 to 1 in the formula above.

Corollary 7.4.3. *Let M be a prime and $(q,M)=1$. Let $\alpha\in\mathrm{GL}(n,q)$ be semisimple with the corresponding combinatorial data Δ_α consisting of polynomials f_i and partitions λ_{f_i}. Then, $X^M=\alpha$ has a solution in $\mathrm{GL}(n,q)$ if and only if for each i, one of the following holds,*

1. *$f_i\in\Phi^M$.*

2. $M \mid |\lambda_{f_i}|$.

Proof. This follows from Proposition above and Corollary 7.2.7 . □

Corollary 7.4.4. *Let M be a prime with $(q,M)=1$. Then,*

$$1+\sum_{n=1}^{\infty} c(n,M)_{\mathrm{ss}}u^n = \left(\frac{1-u^M}{1-qu^M}\right)\prod_{d\geq 1}\left(1+u^d+u^{2d}+\cdots+u^{d(M-1)}\right)^{N_M(q,d)}.$$

Proof. Recall that here we have $N(q,d) = N_M^0(q,d) + N_M^1 q,d = N_M(q,d) + N_M^1(q,d)$. By taking $a=1$ (and thus $r=M$) in Theorem 7.4.2, we have,

$$\begin{aligned}
1+\sum_{n=1}^{\infty} c(n,M)_{\mathrm{ss}}u^n &= \prod_{d\geq 1}(1-u^d)^{-N_M(q,d)}\prod_{d\geq 1}(1-u^{Md})^{-N_M^1(q,d)}\\
&= \prod_{d\geq 1}(1-u^d)^{-N_M(q,d)}\prod_{d\geq 1}(1-u^{Md})^{N_M(q,d)-N(q,d)}\\
&= \prod_{d\geq 1}\left(\frac{1-u^{Md}}{1-u^d}\right)^{N_M(q,d)}\prod_{d\geq 1}(1-u^{Md})^{-N(q,d)}\\
&= \prod_{d\geq 1}\left(\frac{1-u^{Md}}{1-u^d}\right)^{N_M(q,d)}\cdot\left(\frac{1-u^M}{1-qu^M}\right).
\end{aligned}$$

The last equality follows from the generating function formula for $N(q,d)$ (see the Proposition 5.2.2, Chapter 5) by taking u^M for u. Putting $M=1$ in the above result, we get the generating function for semisimple classes (see Proposition 5.2.2) as expected. □

7.5 M^{th} power conjugacy classes in $\mathrm{GL}(n,q)$ when M is a prime power

In this section, we work with general elements and assume $M = r^a$, for some prime r, and $(q,M)=1$. Now, we proceed to construct generating functions for $c(n,M)$ and $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$. Recall from Chapter 5, Section 5.2.2, Macdonald's parametrization of conjugacy classes in $\mathrm{GL}(n,q)$, which led to the notion of type-ν conjugacy classes of $\mathrm{GL}(n,q)$. Now, we determine the number of conjugacy classes that are M^{th} powers by counting the number of type-ν conjugacy classes that are M^{th} powers. Recall the notation: $\Phi_{M,i}$ is the set of all polynomials $f\in\Phi$ with the property that all irreducible factors of $f(x^M)$ are of degree $r^i\deg(f)$. We also have $\Phi = \bigcup_{i=0}^{a}\Phi_{M,i}$ where $\Phi_{M,0}$ the set of M-power polynomials. The Proposition 7.2.6

can be rephrased in terms Macdonald's notation as follows.

Proposition 7.5.1. *Let $M = r^a$ where r is a prime and $(q, M) = 1$. Let $\alpha \in \mathrm{GL}(n,q)$, with associated Macdonald's data $(u_1, u_2, \ldots)$. Write $u_i(x) = \prod_j f_{ij}^{a_{ij}}$ as a product of irreducible polynomials $f_{ij} \in \Phi$. Then, $X^M = \alpha$ has a solution in $\mathrm{GL}(n,q)$ if and only if, for all f_{ij}, $f_{ij} \in \Phi_{M,b}$, for some $0 \leq b \leq a$, implies $r^b \mid a_{ij}$.*

Proof. We write each $u_i(x) = \prod_j f_{ij}^{a_{ij}}$ as a product of irreducibles. Then the set f_{ij} and the corresponding powers $m_i(\lambda_{f_{ij}}) = a_{ij}$ give back the combinatorial data Δ_α. The result follows from Proposition 7.2.6. □

Note the subtle difference between this proposition and the semisimple case (Proposition 7.4.1). In the present case, we require that r^b divides the multiplicity of each part appearing in the partitions. In general, it is not true that $X^M = \alpha$ has a solution in $\mathrm{GL}(n,q)$ if and only if $Y^M = \alpha_s$ has a solution where α_s is the semisimple part of α.

Example 7.5.2. Take $\alpha = \begin{pmatrix} \lambda_1 & 1 & \\ & \lambda_1 & \\ & & \lambda_2 \end{pmatrix} \in \mathrm{GL}(3,q)$ and $M = 2$. Then, $X^M = \alpha$ has a solution in $\mathrm{GL}(3,q)$ if and only if $\lambda_1, \lambda_2 \in \mathbb{F}_q^{*2}$. However, $Y^2 = \alpha_s = \begin{pmatrix} \lambda_1 & & \\ & \lambda_1 & \\ & & \lambda_2 \end{pmatrix}$ has solution if and only if $\lambda_2 \in \mathbb{F}_q^{*2}$, because $\begin{pmatrix} \lambda_1 & 1 \\ & \lambda_1 \end{pmatrix}^2 = \begin{pmatrix} \lambda_1 & \\ & \lambda_1 \end{pmatrix}$.

Now, we write the generating function for $c(n, M)$. We have the following,

Theorem 7.5.3. *Let $M = r^a$, where r is a prime, and $(q, M) = 1$. Then we have the following generating function,*

$$1 + \sum_{n=1}^{\infty} c(n,M)u^n = \prod_{j=1}^{\infty} \prod_{i=0}^{a} \prod_{d \geq 1} (1 - u^{jr^i d})^{-N_M^i(q,d)}.$$

Proof. Let $c_{\nu,M}$ denote the number of type-ν conjugacy classes that are M^{th}-powers. For a partition $\nu = \langle 1^{n_1}, 2^{n_2}, \cdots \rangle$ of n, from Proposition 7.5.1 we have

$$c_{\nu,M} = \prod_{n_i > 0} c(n_i, M)_{\mathrm{ss}}$$

where n_i represent $\deg(u_i)$. Now,

$$c(n,M) = \sum_{\nu \vdash n} c_{\nu,M} = \sum_{\nu \vdash n} \left(\prod_{n_i > 0} c(n_i, M)_{\mathrm{ss}} \right).$$

We apply Lemma 5.2.4, taking $a_n = c(n,M)_{\mathrm{ss}}$, thus $f(u) = \prod_{i=0}^{a} \prod_{d \geq 1} (1 -$

$u^{r^i d})^{-N_M^i(q,d)}$ is the generating function for M-power semisimple classes (by Theorem 7.4.2). Thus, $b_n = c(n,M)$ and we get,

$$1 + \sum_{n=1}^{\infty} c(n,M)u^n = \prod_{t=1}^{\infty} f(u^t)$$

which gives the required result. □

Corollary 7.5.4. *Let M be a prime and $(q,M)=1$. Then we have,*

$$1 + \sum_{n=1}^{\infty} c(n,M)u^n = \prod_{j=1}^{\infty} \left(\left(\frac{1-u^{Mj}}{1-qu^{Mj}} \right) \prod_{d\geq 1} \left(\frac{1-u^{Mjd}}{1-u^{jd}} \right)^{-N_M(q,d)} \right).$$

When $M=1$ in the above result, we point out that we get back Propostion 5.2.5, as expected.

To end this chapter we write the generating function for $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$. To make it simple we assume M is prime. Recall that $\widehat{N}(q,d) = N(q,d) - N_M(q,d)$ is the set of all polynomials $f \in \Phi$ such that $f(x^M)$ is irreducible. We have the following,

Theorem 7.5.5. *Let $M \geq 2$ be a prime and $(M,q)=1$. Then,*

$$\begin{aligned} 1 + \sum_{n=0}^{\infty} \frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|} u^n &= \prod_{d\geq 1} \left(1 + \sum_{j\geq 1} \sum_{\lambda \vdash j} \frac{u^{jd}}{q^{d\sum_i (\lambda_i')^2} \prod_{i\geq 1} \left(\frac{1}{q^d}\right)_{m_i(\lambda)}} \right)^{N_M(q,d)} \\ &\quad \times \prod_{d\geq 1} \left(1 + \sum_{n\geq 1} \sum_{\lambda \vdash n} \frac{u^{Mnd}}{q^{M^2 d\sum_i (\lambda_i')^2} \prod_{i\geq 1} \left(\frac{1}{q^d}\right)_{m_i(\lambda)}} \right)^{\widehat{N}(q,d)} \end{aligned}$$

Proof. By Corollary 7.2.7, we know that $\alpha \in \mathrm{GL}(n,q)$ is M^{th} power if and only if for each $f \in \Delta_\alpha$, either f is M-power or else, $M \mid m_j(\lambda_f)$ for all $j \geq 1$. Thus, in the cycle index generating function (see Equation 5.3.2), we put, for each $f \in \Phi, \lambda \in \Lambda$,

$$x_{f,\lambda} = \begin{cases} 1 & ; \text{if } f \in \Phi^M \\ 1 & ; \text{if } f \in \Phi \setminus \Phi^M \text{ and, } M \mid m_j(\lambda) \text{ for all } j \geq 1 \\ 0 & ; \text{otherwise} \end{cases}$$

Substituting these values, we get the generating function. □

7.6 An application of the generating function for powers

Till now we have developed several generating functions involving the proportion of M^{th} powers in $\mathrm{GL}(n,q)$. These generating functions look complex in form. In this final section of the chapter, we mention some methods to make these generating functions much more simpler and accessible when M is prime. As an application, the explicit value of the probability $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$ is determined for some values of n. For the rest of this section we assume M is prime and $(M,q)=1$. We start by stating the main result of this section.

Theorem 7.6.1. *Let M be a prime and $(M,q)=1$. Let $t=\mathfrak{M}(M;q)$. Then,*

$$\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}=\sum_{\substack{\lambda\vdash n\\ \lambda=\langle 1^{m_1},2^{m_2},\cdots\rangle}}\frac{1}{M^{\pi_t(\lambda)}\prod_{i\geq 1}i^{m_i}m_i!}$$

whenever $n<Mt$ and $\pi_t(\lambda)$ denote the number of parts of λ divisible by t. In power notation, $\pi_t(\lambda)=\sum_{t|i}m_i$.

We quickly give some examples.

Example 7.6.2. Let $M=2$. We have $t=1$. Thus, we get $\frac{|(\mathbb{F}_q^\times)^2|}{|\mathbb{F}_q^\times|}=\frac{1}{2}$, which is well known.

Example 7.6.3. Let $M=3$. Then possible values for t are 1 and 2. When $t=1$, that is, $q\equiv 1(\mathrm{mod}\ 3)$ we have, $Mt=3$. Thus, by the above theorem,

$$\frac{|\mathrm{GL}(1,q)^3|}{|\mathrm{GL}(1,q)|}=\frac{|(\mathbb{F}_q^\times)^3|}{|\mathbb{F}_q^\times|}=\frac{1}{3}\text{ and, }\frac{|\mathrm{GL}(2,q)^3|}{|\mathrm{GL}(2,q)|}=\frac{1}{3^2.2!}+\frac{1}{3.2}=\frac{2}{9}.$$

The above results can be verified from Table 9.5 of Chapter 9.

When $t=2$, that is, $q\equiv 2(\mathrm{mod}\ 3)$ we have $Mt=6$. We write the values in the following table:

n	1	2	3	4	5
$\frac{\lvert\mathrm{GL}(n,q)^3\rvert}{\lvert\mathrm{GL}(n,q)\rvert}$	1	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{5}{9}$	$\frac{5}{9}$

Table 7.3: Values of $\frac{|\mathrm{GL}(n,q)^3|}{|\mathrm{GL}(n,q)|}$ when $q\equiv(\mathrm{mod}\ 3)$ and $n<6$.

Once again the result for $n=2,3$ can be verified from Table 9.5 and Table 9.11.

Recall from Section 6.2 of Chapter 6, that

$$P(n,t,M) = \sum_{\substack{\lambda \vdash n \\ \lambda = 1^{m_1} 2^{m_2} \dots}} \frac{1}{M^{\pi_t(\lambda)} \prod_{i \geq 1} i^{m_i} m_i!}$$

gives the subsequential limits (except possibly 1) of $\mathfrak{P}_{\mathrm{GL}}(n,q,M) := \frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$ (for fixed n, M and varying q). Theorem 7.6.1 states that $\mathfrak{P}_{\mathrm{GL}}(n,q,M) = P(n,t,M)$ when $n < Mt$, where t is the order of q in $(\mathbb{Z}/M\mathbb{Z})^\times$.

Remark 7.6.4. The power map on $\mathrm{GL}(n,q)$ is surjective if and only if $(M,q) = 1$ and $n < \mathfrak{M}(M;q) = t$ (see Proposition 6.2.2). This is reflected in the above theorem since $P(n,t,M) = 1$ if and only if $n < t$.

The rest of the section is devoted to the proof of Theorem 7.6.1. As we go along, we will see simplification of some of the generating function that has been already obtained in this chapter.

7.6.1 A relation between $N_M(q,d)$, and $N(q,d)$, and related identities

We have already seen that $N_M(q,d)$ plays a pivotal role in obtaining the generating functions related to powers. We derive a simple recursive formulation of $N_M(q,d)$ in terms of $N(q,d)$, which will play a major role in the simplification process of the related generating functions.

Proposition 7.6.5. *Let $M \geq 2$ be a prime. Suppose $\mathfrak{M}(M;q) = t$. Let $t \mid d$ and, $d = M^k.t.y$ with $k \geq 0$ and, $M \nmid y$. Then,*

$$\widehat{N}(q,d) = N(q,d) - N_M(q,d) = \frac{M-1}{M^{k+1}t} N(q^{M^k t}, y)$$

Proof. From Proposition 7.1.4, we have,

$$N_M(q,d) = \frac{1}{d(M, q^d-1)} \sum_{r \mid d} \mu(r) \left(M(q^{d/r}-1), (q^d-1) \right)$$

$$= \frac{1}{Md} \sum_{r \mid d} \mu(r)(q^{d/r}-1)(M, \frac{q^d-1}{q^{d/r}-1})$$

The second equality follows from the fact that $(M, q^d-1) = M$ as $t \mid d$. Therefore,

$$\begin{aligned}\widehat{N}(q,d) &= \left(\frac{1}{d}\sum_{r|d}\mu(r)(q^{d/r}-1)\right) - \left(\frac{1}{Md}\sum_{r|d}\mu(r)(q^{d/r}-1)(M,\frac{q^d-1}{q^{d/r}-1})\right) \\ &= \frac{1}{d}\sum_{r|d}\left(\mu(r)(q^{d/r}-1)\left[1-\frac{(M,\frac{q^d-1}{q^{d/r}-1})}{M}\right]\right).\end{aligned} \tag{7.1}$$

Now, we claim that,

$$\sum_{r|d}\left(\mu(r)(q^{d/r}-1)\left[1-\frac{(M,\frac{q^d-1}{q^{d/r}-1})}{M}\right]\right) = \frac{M-1}{M}\sum_{r|y}\mu(r)(q^{d/r}-1) \tag{7.2}$$

where, $d = M^k.t.y$, with $(M,y)=1$.

To prove the claim, we observe that if $r \mid d$ such that $r \mid M^k$, then $r \nmid y$ (assuming $k \geq 1$, or else, this case is redundant). Now, if $r = M^a$, where $a \geq 2$, then $\mu(r) = 0$. If, $r = M$, then observe that,

$$(M,\frac{q^d-1}{q^{d/r}-1}) = M \implies 1-\frac{(M,\frac{q^d-1}{q^{d/r}-1})}{M} = 0.$$

This is because, if $r = M$, $\frac{q^d-1}{q^{d/M}-1} = q^{\frac{d}{M}(M-1)}+\ldots+q^{\frac{d}{M}}+1$. Now, since, $t \mid \frac{d}{M}$ we can conclude that, $q^{\frac{d}{M}(M-1)}+\ldots+q^{\frac{d}{M}}+1 \equiv \underbrace{1+1+\ldots+1}_{M \text{ times}} (\text{mod } M) \equiv 0 (\text{mod } M)$. Therefore, we have proved that if $r \mid d$ such that $r \mid M^k$, then

$$\mu(r)(q^{d/r}-1)\left[1-\frac{(M,\frac{q^d-1}{q^{d/r}-1})}{M}\right] = 0.$$

Now, suppose that $r \mid d$, and $(r,M)=1$. We have $d = M^k.t.y$, and along with that let us assume that $(t,y)=s$. Thus, $t = s.a$, and $(y,a)=1$. Suppose, further $r \mid a$. Then, $r \nmid y$. In this case also, observe that,

$$(M,\frac{q^d-1}{q^{d/r}-1}) = M \implies 1-\frac{(M,\frac{q^d-1}{q^{d/r}-1})}{M} = 0$$

This is because, clearly $M \mid \left(\frac{q^d-1}{q^{d/r}-1}\right)$, as $M \mid q^d-1$, but $M \nmid q^{d/r}-1$. Suppose that $r \mid d$ such that $r \mid s.b$, where $(b,s) \neq 1$, and $r > s$. In this case $\mu(r) = 0$ as r

is not square free. Finally to establish the claim, we see that if $r \mid y$,

$$(M, \frac{q^d-1}{q^{d/r}-1}) = 1 \implies 1 - \frac{(M, \frac{q^d-1}{q^{d/r}-1})}{M} = 1 - \frac{1}{M}.$$

Therefore, we have established the claim made in equation 7.2. Now, from equation 7.1, we get,

$$\widehat{N}(q,d) = \frac{M-1}{Md}\sum_{r|y}\mu(r)(q^{d/r}-1) = \left(\frac{M-1}{M^{k+1}.t}\right)\left(\frac{1}{y}\sum_{r|y}\mu(r)((q^{M^k t})^{y/r}-1)\right)$$

$$= \frac{M-1}{M^{k+1}.t}N(q^{M^k t}, y).$$

This completes the proof. □

Corollary 7.6.6. *Suppose $M \geq 2$ is a prime with $(M,q) = 1$. Let $t = \mathfrak{M}(M;q)$. We have,*

$$\widehat{N}(q,d) = \begin{cases} 0 & \text{when } t \nmid d \\ \frac{M-1}{M^{k+1}.t}N(q^{M^k t}, y) & \text{when } d = M^k.t.y \text{ for some } k \geq 0. \end{cases}$$

Proof. The proof follows from the previous proposition and Corollary 7.1.7. □

Example 7.6.7. Take $M = 2$. Then $t = 1$ is the only choice. We have calculated $N_2(q,2), N_2(q,3), N_2(q,4)$ in Table 7.1.

$$N_2(q,5) = N(q,5) - \tfrac{1}{2}N(q,5) = \tfrac{1}{10}(q^5 - q)$$

since $k = 0$ in the above case.

$$N_2(q,6) = N(q,6) - \tfrac{1}{4}N(q^2,3) = N(q,6) - \tfrac{1}{12}(q^6 - q^2)$$

since $k = 1$ in the above case. Thus, $N(q,6) = \frac{1}{6}(q^6 - q^2 - q^3 + q)$ gives,

$$N_2(q,6) = \frac{1}{12}(q^6 - q^2 - 2q^3 + 2q).$$

Example 7.6.8. Let $M \geq 2$ be a prime and $(M,q) = 1$. Then, Let $M = 3$. The possible values of t are 1 and 2. Let us first take $t = 1$, that is, $q \equiv 1 (\text{mod } 3)$. We have recorded the expressions for $N_3(q,2), N_3(q,3), N_3(q,4)$ in Table 7.2. We calculate $N_3(q,5)$.

$$N_3(q,5) = N(q,5) - \frac{1}{3}N(q,5) = \frac{2}{15}(q^5 - q).$$

$$N_3(q,6) = N(q,6) - \frac{1}{9}N(q^3,2) = N(q,6) - \frac{1}{18}(q^6 - q^2)$$

since $k = 1$ here. Thus, we have,

$$N_3(q,6) = \frac{1}{18}(2q^6 - 3q^3 - 2q^2 + 3q).$$

Let us now take $t = 2$, that is, $q \equiv 2 (\mathrm{mod}\ 3)$. In this case when $d = 5$, observe that $t \nmid d$, and therefore,

$$N_3(q,5) = N(q,5) = \frac{1}{5}(q^5 - q).$$

When $d = 6$, we have $k = 1$, and thus,

$$N_3(q,6) = N(q,6) - \frac{1}{18}N(q^6,1) = N(q,6) - \frac{1}{18}(q^6 - 1).$$

Thus,

$$N_3(q,6) = \frac{1}{18}(2q^6 - 3q^3 - 3q^2 + 3q + 1).$$

Then next lemma will prove to be useful.

Lemma 7.6.9. *Suppose $k \geq 1$. Suppose $M \nmid d$. Then,*

$$N(q^{M^k}, d) = M^k N(q, M^k d) + N(q^{M^{k-1}}, d).$$

Proof. We have,

$$\begin{aligned}
N(q^{M^k}, d) &= \frac{1}{d}\sum_{r|d}\mu(r)((q^{M^k})^{d/r} - 1) \\
&= \frac{1}{d}\left(\sum_{r|M^k d}\mu(r)(q^{\frac{M^k d}{r}} - 1) - \sum_{\substack{Mr|M^k d \\ (r,M)=1}}\mu(Mr)(q^{\frac{M^k d}{Mr}} - 1)\right) \\
&= \frac{1}{d}\left(\sum_{r|M^k d}\mu(r)(q^{\frac{M^k d}{r}} - 1) + \sum_{r|d}\mu(r)((q^{M^{k-1}})^{d/r} - 1)\right) \\
&= M^k\left(\frac{1}{M^k d}\sum_{r|M^k d}\mu(r)(q^{\frac{M^k d}{r}} - 1)\right) + \left(\frac{1}{d}\sum_{r|d}\mu(r)((q^{M^{k-1}})^{d/r} - 1)\right) \\
&= M^k N(q, M^k d) + N(q^{M^{k-1}}, d)
\end{aligned}$$

This completes the proof. □

We can now prove a very important identity. Recall from Proposition 5.2.2 in

Chapter 5, the following identity,

$$c(q,u)=\prod_{d=1}^{\infty}(1-u^d)^{-N(q,d)}=\frac{1-u}{1-qu}.$$

Proposition 7.6.10. *Let $M\geq 2$ be a prime with $(M,q)=1$. Suppose $t=\mathfrak{M}(M;q)$. Then,*

$$\prod_{d\geq 1}(1-u^d)^{\widehat{N}(q,d)}=\prod_{k=0}^{\infty}\left(\frac{1-u^{M^kt}}{1-q^tu^{M^kt}}\right)^{\frac{1-M}{M^{k+1}t}}=\prod_{k=0}^{\infty}c(q^t,u^{M^kt})^{\frac{1-M}{M^{k+1}t}}.$$

Proof. Using Corollary 7.6.6, we have,

$$\begin{aligned}
\prod_{d\geq 1}(1-u^d)^{\widehat{N}(q,d)} &= \prod_{k=0}^{\infty}\prod_{M\nmid d}(1-u^{M^k.t.d})^{\widehat{N}(q,M^k.t.d)}\\
&= \prod_{k=0}^{\infty}\prod_{M\nmid d}(1-u^{M^k.t.d})^{\frac{M-1}{M^{k+1}t}N(q^{M^k.t.d},d)}=\left[\prod_{k=0}^{\infty}\prod_{M\nmid d}(1-u^{M^k.t.d})^{\frac{N(q^{M^k.t.d},d)}{M^k}}\right]^{\frac{M-1}{Mt}}\\
&= \left[\prod_{M\nmid d}(1-u^{td})^{N(q^t,d)}\right]^{\frac{M-1}{Mt}}\left[\prod_{k=1}^{\infty}\prod_{M\nmid d}(1-u^{M^k.t.d})^{\frac{N(q^{M^k.t.d},d)}{M^k}}\right]^{\frac{M-1}{Mt}}\\
&= \left[\prod_{M\nmid d}(1-u^{td})^{N(q^t,d)}\right]^{\frac{M-1}{Mt}}\left[\prod_{k=1}^{\infty}\prod_{M\nmid d}(1-u^{M^k.t.d})^{N(q^t,M^k.t.d)+\frac{N(q^{M^{k-1}.t},d)}{M^k}}\right]^{\frac{M-1}{Mt}}.
\end{aligned}$$

The last equality follows from Lemma 7.6.9, where we replace q by q^t. Therefore, we get,

$$\prod_{d\geq 1}(1-u^d)^{\widehat{N}(q,d)}=$$

$$\begin{aligned}
&\left[\prod_{k=0}^{\infty}(1-u^{M^k.t.d})^{-N(q^t,M^k.t.d)}\right]^{\frac{1-M}{Mt}}\left[\prod_{k=1}^{\infty}\prod_{M\nmid d}(1-u^{M^k.t.d})^{\frac{N(q^{M^{k-1}.t},d)}{M^k}}\right]^{\frac{M-1}{Mt}}\\
&= \left(\prod_{d\geq 1}(1-u^{td})^{-N(q^t,td)}\right)^{\frac{1-M}{Mt}}\left[\prod_{k=1}^{\infty}\prod_{M\nmid d}(1-u^{M^k.t.d})^{\frac{N(q^{M^{k-1}.t},d)}{M^{k-1}}}\right]^{\frac{M-1}{M^2t}}\\
&= \left(\frac{1-u^t}{1-q^tu^t}\right)^{\frac{1-M}{Mt}}\left[\prod_{k=1}^{\infty}\prod_{M\nmid d}(1-u^{M^k.t.d})^{\frac{N(q^{M^{k-1}.t},d)}{M^{k-1}}}\right]^{\frac{M-1}{M^2t}}.
\end{aligned}$$

Again one can apply Lemma 7.6.9, and do the steps performed above to conclude,

that,

$$\prod_{d\geq 1}(1-u^d)^{\widehat{N}(q,d)} =$$

$$\left(\frac{1-u^t}{1-q^tu^t}\right)^{\frac{1-M}{Mt}}\left(\frac{1-u^{Mt}}{1-q^tu^{Mt}}\right)^{\frac{1-M}{M^2t}}\left[\prod_{k=2}^{\infty}\prod_{M\nmid d}(1-u^{M^k.t.d})^{\frac{N(q^{M^{k-2}.t},d)}{M^{k-2}}}\right]^{\frac{M-1}{M^3t}}.$$

Inductively, we conclude,

$$\prod_{d\geq 1}(1-u^d)^{\widehat{N}(q,d)} = \prod_{k=0}^{\infty}\left(\frac{1-u^{M^kt}}{1-q^tu^{M^kt}}\right)^{\frac{1-M}{M^{k+1}t}} = \prod_{k=0}^{\infty}c(q^t,u^{M^kt})^{\frac{1-M}{M^{k+1}t}}.$$

□

7.6.2 Reformulating the generating functions for M^{th} power regular and regular semisimple classes

As a quick application of Proposition 7.6.10 in the previous section, we now show that the generating functions of M^{th} power regular semisimple and regular conjugacy classes that were obtained in Theorem 7.3.2 can be reformulated to look much simpler. Before stating the theorem we recall from Proposition 5.2.3, the generating function of the number of regular semisimple classes.

$$s(q,u) = 1+\sum_{n=1}^{\infty}c(n)_{\mathrm{rs}}u^n = \prod_{n=1}^{\infty}(1+u^d)^{N(q,d)} = \frac{1-qu^2}{(1+u)(1-qu)}.$$

Theorem 7.6.11. *Let $M\geq 2$ be a prime and $(M,q)=1$. Suppose $\mathfrak{M}(M;q)=t$. Then,*

1. $1+\sum_{n=1}^{\infty}c(n,M)_{\mathrm{rg}}u^n = c(q,u)\prod_{k=0}^{\infty}c(q^t,u^{M^kt})^{\frac{1-M}{M^{k+1}t}}$.
2. $1+\sum_{n=1}^{\infty}c(n,M)_{\mathrm{rs}}u^n = s(q,u)\prod_{k=0}^{\infty}s(q^t,u^{M^kt})^{\frac{1-M}{M^{k+1}t}}$.

Proof. Using Theorem 7.3.2 and Proposition 7.6.10, we have,

$$1+\sum_{n=1}^{\infty}c(n,M)_{\mathrm{rg}}u^n = \prod_{d\geq 1}(1-u^d)^{-N_M(q,d)}$$

$$= \prod_{d\geq 1}(1-u^d)^{-N(q,d)}\prod_{d\geq 1}(1-u^d)^{\widehat{N}(q,d)} = c(q,u)\prod_{\substack{d\geq 1\\ t\nmid d}}(1-u^d)^{\widehat{N}(q,d)}$$

$$= c(q,u)\prod_{d\geq 1}(1-u^{td})^{\widehat{N}(q,td)} = c(q,u)\prod_{k=0}^{\infty}c(q^t,u^{M^kt})^{\frac{1-M}{M^{k+1}t}}.$$

We also have,

$$1+\sum_{n=1}^{\infty} c(n,M)_{\mathrm{rs}}u^n = \prod_{d\geq 1}(1+u^d)^{N_M(q,d)}$$

$$= \prod_{d\geq 1}(1+u^d)^{N(q,d)}\prod_{d\geq 1}(1+u^d)^{-\widehat{N}(q,d)} = s(q,u)\frac{\prod\limits_{\substack{d\geq 1\\ t|d}}(1-u^{2d})^{-\widehat{N}(q,d)}}{\prod\limits_{\substack{d\geq 1\\ t|d}}(1-u^{d})^{-\widehat{N}(q,d)}}$$

$$= s(q,u)\prod_{k=0}^{\infty} s(q^t,u^{M^k t})^{\frac{1-M}{M^{k+1}t}}.$$

□

Example 7.6.12. Let $M=3$, and q is such that such that $\mathfrak{M}(3,q)=t=2$. We have,

$$1+\sum_{n=1}^{\infty} c(n,3)_{\mathrm{rg}}u^n = c(q,u)\prod_{k=0}^{\infty} c(q^2,u^{2.3^k})^{-\frac{1}{3^{k+1}}}$$

$$= \left(\frac{1-u}{1-qu}\right)\left(\frac{1-u^2}{1-q^2u^2}\right)^{-\frac{1}{3}}\left(\frac{1-u^6}{1-q^2u^6}\right)^{-\frac{1}{9}}\prod_{k=2}^{\infty} c(q^2,u^{2.3^k})^{-\frac{1}{3^{k+1}}}.$$

Similarly,

$$1+\sum_{n=1}^{\infty} c(n,3)_{\mathrm{rs}}u^n = s(q,u)\prod_{k=0}^{\infty} s(q^2,u^{2.3^k})^{-\frac{1}{3^{k+1}}} = \left(\frac{1-qu^2}{(1+u)(1-qu)}\right)$$
$$\left(\frac{1-q^2u^4}{(1+u^2)(1-q^2u^2)}\right)^{-\frac{1}{3}}\left(\frac{1-q^2u^{12}}{(1+u^6)(1-q^2u^6)}\right)^{-\frac{1}{9}}\prod_{k=2}^{\infty} s(q^2,u^{2.3^k})^{-\frac{1}{3^{k+1}}}.$$

We make table to compute these classes for some small value of n. We know, $c(n)_{\mathrm{rg}} = q^n - q^{n-1}$.

n	Number of regular classes	Number of M^{th} power regular classes
1	$q-1$	$q-1$
2	q^2-q	$\frac{2}{3}q^2-q+\frac{1}{3}$
3	q^3-q^2	$\frac{2}{3}q^3-\frac{2}{3}q^2+\frac{1}{3}q-\frac{1}{3}$
4	q^4-q^3	$\frac{5}{9}q^4-\frac{2}{3}q^3+\frac{2}{9}q^2-\frac{1}{3}q+\frac{2}{9}$
5	q^5-q^4	$\frac{5}{9}q^5-\frac{5}{9}q^4+\frac{2}{9}q^3-\frac{2}{9}q^2+\frac{2}{9}q-\frac{2}{9}$
6	q^6-q^5	$\frac{40}{81}q^6-\frac{5}{9}q^5+\frac{5}{27}q^4-\frac{2}{9}q^3+\frac{1}{27}q^2-\frac{2}{9}q+\frac{23}{81}$

Table 7.4: Table for $c(n,3)_{\mathrm{rg}}$ for $q\equiv 2(\mathrm{mod}\ 3)$.

We can also make similar simplification to the generating functions for the proportion of regular semisimple elements and regular elements that are M^{th} powers.

Theorem 7.6.13. *Let $M \geq 2$ be a prime and $(M, q) = 1$. Suppose $\mathfrak{M}(M; q) = t$. Then,*

1. $1 + \sum_{n=1}^{\infty} \frac{|\mathrm{GL}(n,q)^M_{\mathrm{rg}}|}{|\mathrm{GL}(n,q)|} u^n = C(q,u) \prod_{k=0}^{\infty} C(q^t, u^{M^k t})^{\frac{1-M}{M^{k+1}t}}$.

2. $1 + \sum_{n=1}^{\infty} \frac{|\mathrm{GL}(n,q)^M_{\mathrm{rs}}|}{|\mathrm{GL}(n,q)|} u^n = S(q,u) \prod_{k=0}^{\infty} S(q^t, u^{M^k t})^{\frac{1-M}{M^{k+1}t}}$.

where $C(q,u)$ and $S(q,u)$ denote the generating functions for the proportion of regular elements in $\mathrm{GL}(n,q)$ and the proportion of regular semisimple elements in $\mathrm{GL}(n,q)$ respectively (see Equation 5.4 and Equation 5.7 respectively).

Proof. The proof is similar to Theorem 7.6.11. □

7.6.3 Proof of Theorem 7.6.1

The proof is based on the simplification of the generating function for the proportion of M^{th} powers given in Theorem 7.5.5 which can be done in a way exactly similar to the ones we have done in the previous subsection. We begin with a simple lemma.

Lemma 7.6.14.

$$\prod_{d\geq 1} \left(1 + \sum_{n\geq 1} \sum_{\lambda \vdash n} \frac{u^{nd}}{q^{d\sum_i (\lambda_i')^2} \prod_{i\geq 1} \left(\frac{1}{q^d}\right)_{m_i(\lambda)}} \right)^{N(q,d)} = \frac{1}{1-u}.$$

Proof. The left hand side can be obtained by putting $x_{f,\lambda} = 1$ for every $f \in \Phi$ and every partition λ in Proposition 5.3.2. Therefore, the coefficient of u^n in the formal power series written in the left hand side is $\frac{1}{|\mathrm{GL}(n,q)|} \sum_{\alpha \in \mathrm{GL}(n,q)} 1 = 1$. Thus,

$$\prod_{d\geq 1} \left(1 + \sum_{n\geq 1} \sum_{\lambda \vdash n} \frac{u^{nd}}{q^{d\sum_i (\lambda_i')^2} \prod_{i\geq 1} \left(\frac{1}{q^d}\right)_{m_i(\lambda)}} \right)^{N(q,d)} = 1 + u + u^2 + \cdots = \frac{1}{1-u}.$$

□

Proof of Theorem 7.6.1. Let us denote

$$P_1 = \prod_{d\geq 1}\left(1+\sum_{n\geq 1}\sum_{\lambda\vdash n}\frac{u^{Mnd}}{q^{M^2d\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{\widehat{N}(q,d)}$$

and,

$$P_2 = \prod_{d\geq 1}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jd}}{q^{d\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{N_M(q,d)}.$$

Thus from Theorem 7.5.5, we have,

$$1+\sum_{n=0}^{\infty}\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}u^n = P_2P_1.$$

Now, we analyze P_2 separately. We have,

$$\begin{aligned} P_2 &= \frac{1}{1-u}\prod_{d\geq 1}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jd}}{q^{d\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{-\widehat{N}(q,d)} \\ &= \frac{P_3}{1-u} \end{aligned}$$

where,

$$\begin{aligned} P_3 &= \prod_{d\geq 1}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jd}}{q^{d\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{-\widehat{N}(q,d)} \\ &= \prod_{t|d}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jd}}{q^{d\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{-\widehat{N}(q,d)} \end{aligned}$$

$$= \prod_{k=0}^{\infty}\prod_{M\nmid d}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jM^k td}}{q^{td\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^{td}}\right)_{m_i(\lambda)}}\right)^{-\widehat{N}(q,M^k.t.d)}$$

$$= \prod_{k=0}^{\infty}\prod_{M\nmid d}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jM^k td}}{q^{td\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^{td}}\right)_{m_i(\lambda)}}\right)^{\frac{1-M}{M^{k+1}.t}N(q^{M^k t},d)}.$$

Using Lemma 7.6.9,

$$P_3 = \prod_{M\nmid d}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{tjd}}{q^{td\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^{td}}\right)_{m_i(\lambda)}}\right)^{N(q^t,d)} \times$$

$$\prod_{k=1}^{\infty}\prod_{M\nmid d}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jM^k td}}{q^{td\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^{td}}\right)_{m_i(\lambda)}}\right)^{\left(N(q^t,M^k.d)+\frac{N(q^{M^{k-1}t},d)}{M^k}\right)\frac{1-M}{Mt}}$$

$$= \prod_{d\geq 1}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{tjd}}{q^{td\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^{td}}\right)_{m_i(\lambda)}}\right)^{N(q^t,d).\frac{1-M}{Mt}} \times$$

$$\prod_{k=1}^{\infty}\prod_{M\nmid d}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jM^k td}}{q^{td\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^{td}}\right)_{m_i(\lambda)}}\right)^{N(q^{M^{k-1}t},d)\frac{1-M}{M^{k+1}t}}$$

$$= \left(\frac{1}{1-u^t}\right)^{\frac{1-M}{Mt}}\prod_{k=1}^{\infty}\prod_{M\nmid d}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jM^k td}}{q^{td\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^{td}}\right)_{m_i(\lambda)}}\right)^{\frac{N(q^{M^{k-1}t},d)}{M^{k-1}}\frac{1-M}{M^2 t}}.$$

Inductively, we get,

$$P_3 = \prod_{k=0}^{\infty}(1-u^{M^k t})^{\frac{M-1}{M^{k+1}t}}.$$

Thus,

$$1+\sum_{n=0}^{\infty}\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}u^n = P_2P_1 = \frac{P_3}{1-u}P_1 = \frac{\prod_{k=0}^{\infty}(1-u^{M^kt})^{\frac{M-1}{M^{k+1}t}}}{1-u}P_1$$
$$= P_1\frac{(1-u^t)^{\frac{M-1}{Mt}}}{1-u}\prod_{k=1}^{\infty}(1-u^{M^kt})^{\frac{M-1}{M^{k+1}t}}.$$

Finally observe that when $n < Mt$, the coefficient of the generating function in the right-hand side is contributed by the coefficient of $\frac{(1-u^t)^{\frac{M-1}{Mt}}}{1-u}$ which is precisely $P(n,t,M)$. This proves the result. □

As a corollary of the above proof, we have found a simpler version of the generating function in Theorem 7.5.5.

Corollary 7.6.15.

$$1+\sum_{n=0}^{\infty}\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}u^n = \frac{P_1}{1-u}\prod_{k=0}^{\infty}(1-u^{M^kt})^{\frac{M-1}{M^{k+1}t}},$$

where $P_1 = \prod_{d\geq 1}\left(1+\sum_{n\geq 1}\sum_{\lambda\vdash n}\frac{u^{Mnd}}{q^{M^2d\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{\widehat{N}(q,d)}$.

We end this section by asking whether the following result is true.

Question 7.6.16. *Is the following result true: Let M be a prime. Assume $(M,q)=1$, and let $\mathfrak{M}(M;q)=t$ denote the order of q in $(\mathbb{Z}/M\mathbb{Z})^\times$. Then,*

$$\mathfrak{P}(n,M,q) := \frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|} \leq \sum_{\substack{\lambda\vdash n\\ \lambda=\langle 1^{m_1},2^{m_2},\cdots\rangle}} \frac{1}{M^{\pi_t(\lambda)}}\prod_i\frac{1}{m_i!i^{m_i}}$$

where $\pi_t(\lambda)$ denotes the number of parts of $\lambda\vdash n$ divisible by t, and, equality holds if and only if $n<Mt$.

The above result (if true) determines an upper bound for the proportion of M^{th} powers in $\mathrm{GL}(n,q)$. For a more general question over a finite reductive group, see Chapter 10.

We mention another interesting observation. If the above theorem holds, then

we must have $\lim_{n\to\infty} \frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|} = 0$ for a fixed q, M. This is clear by applying the Sandwich theorem along with the fact that $\lim_{n\to\infty} P(n,t,M) = 0$.

Chapter 8

M^{th} powers in $\mathbf{GL}(n,q)$ when M is a prime and $(M,q) \neq 1$

In the previous chapter, we dealt with the case when M is coprime to q. Recall that we are interested in determining the image of the power map $\omega\colon \mathrm{GL}(n,q) \to \mathrm{GL}(n,q)$ given by $x \mapsto x^M$. From the point of view of Jordan decomposition of elements, when $(q,M)=1$, all unipotent elements survive as they are of order, a power of q. Now, we want to focus on the case when M and q are not coprime. For simplicity of computations, we take the case M is a prime and q is a power of M. In this case, all semisimple elements survive in the image. Miller (see [Mil16]) enumerated squares in $\mathrm{GL}(n,2^a)$; thus dealt with a particular case, $M=2$, of our situation. The material of this chapter is once again taken from the author's work in [KS20b] and follows closely to that of Miller.

We fix M a prime and q, a power of M. We determine the conjugacy classes that are M^{th} powers in $\mathrm{GL}(n,q)$. We begin with a Lemma (analogous to our earlier Lemma 7.2.1) which is [Mil16, Lemma 2]. Recall the notation that $J_{\gamma,n}$ denotes a Jordan block matrix of size n with diagonal γ.

8.1 M^{th} powers in $\mathbf{GL}(n,q)$, where M is prime and q is a power of M

Lemma 8.1.1 (Miller). *Let $J_{0,n}$ be the Jordan block corresponding to scalar 0. Then, $J_{0,n}^M$ is conjugate to*

$$\underbrace{J_{0,\lceil \frac{n}{M} \rceil} \oplus \cdots \oplus J_{0,\lceil \frac{n}{M} \rceil}}_{\bar{n}} \oplus \underbrace{J_{0,\lfloor \frac{n}{M} \rfloor} \oplus \cdots \oplus J_{0,\lfloor \frac{n}{M} \rfloor}}_{(M-\bar{n})}$$

where $0 \leq \bar{n} \leq M-1$ *is* $n \pmod M$ *and* $\lceil \frac{n}{M} \rceil$, $\lfloor \frac{n}{M} \rfloor$ *are the ceiling and floor functions respectively.*

8.1.1 A map on partitions

In the view of Lemma above, we define the following map Θ_M on the set of partitions Λ. Let $\Lambda(n)$ denote the set of all partitions of n; thus $\Lambda = \bigcup_{n\geq 0} \Lambda(n)$. We define the map $\Theta_M \colon \Lambda(n) \to \Lambda(n)$ as follows: Let $\lambda = \langle 1^{m_1(\lambda)}, 2^{m_2(\lambda)}, \cdots \rangle$ be a partition of n then $\Theta_M(\lambda) = \langle 1^{m_1(\Theta_M(\lambda))}, 2^{m_2(\Theta_M(\lambda))}, \cdots \rangle$ where

$$m_i(\Theta_M(\lambda)) = M.m_{(iM)}(\lambda) + \sum_{j=1}^{M-1} (M-j)\left(m_{(iM-j)}(\lambda) + m_{(iM+j)}(\lambda)\right).$$

If we take $M = 2$, we get the function defined in [Mil16, Proposition 3]. Since, this map is quite important for us, we elaborate this alternatively using the other notation for a partition. Given a partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ of n, we have

$$\Theta_M(\lambda) = \left(\underbrace{\left\lceil \frac{\lambda_1}{M} \right\rceil, \ldots, \left\lceil \frac{\lambda_1}{M} \right\rceil}_{\bar{\lambda}_1}, \underbrace{\left\lfloor \frac{\lambda_1}{M} \right\rfloor, \ldots, \left\lfloor \frac{\lambda_1}{M} \right\rfloor}_{M-\bar{\lambda}_1}, \ldots, \underbrace{\left\lceil \frac{\lambda_k}{M} \right\rceil, \ldots, \left\lceil \frac{\lambda_k}{M} \right\rceil}_{\bar{\lambda}_k}, \underbrace{\left\lfloor \frac{\lambda_k}{M} \right\rfloor, \ldots, \left\lfloor \frac{\lambda_k}{M} \right\rfloor}_{M-\bar{\lambda}_k} \right)$$

suitably rearranged in non-increasing order, where $0 \leq \bar{\lambda}_i \leq (M-1)$ is $\lambda_i \pmod M$. It is easy to see that both of the above definitions are the same. We give some examples to illustrate this map.

$\lambda \vdash 4$	$\Theta_2(\lambda)$	$\lambda \vdash 4$	$\Theta_2(\lambda)$
$(3,1)$	$(2,1,1)$	$(2,2)$	$(1,1,1,1)$
$(1,1,1,1)$	$(1,1,1,1)$	(4)	$(2,2)$
$(2,1,1)$	$(1,1,1,1)$		

Table 8.1: The map Θ_2 on partitions of 4.

Thus, we see that $\Theta_2(\Lambda(4)) = \{(1,1,1,1),(2,1,1),(2,2)\} \subset \Lambda(4)$ and similarly $\Theta_3(\Lambda(5)) = \{(1,1,1,1,1),(2,1,1,1),(2,2,1)\} \subset \Lambda(5)$. We make a table to illustrate the size of image for some small values.

n	$\lvert\Lambda(n)$	$\lvert\Theta_2(\Lambda(n))\rvert$	$\lvert\Theta_3(\Lambda(n))\rvert$	$\lvert\Theta_5(\Lambda(n))\rvert$
1	1	1	1	1
2	2	1	1	1
3	3	2	1	1

n	$\lvert\Lambda(n)$	$\lvert\Theta_2(\Lambda(n))\rvert$	$\lvert\Theta_3(\Lambda(n))\rvert$	$\lvert\Theta_5(\Lambda(n))\rvert$
4	5	3	2	1
5	7	4	3	1
6	11	5	4	2
7	15	7	5	3
8	22	10	6	4
9	30	13	7	5
10	42	16	9	6
11	56	21	12	7
12	77	28	16	8
13	101	35	20	9
14	135	43	24	10
15	176	55	28	11

Table 8.2: Values of $|\Theta_M(\Lambda(n))|$ for $M = 2, 3, 5$.

We would like to count the image of Θ_M. The following Lemma is a generalization of [Mil16, Proposition 3].

Lemma 8.1.2. *Let $\Theta_M \colon \Lambda(n) \to \Lambda(n)$ be the map described above. Then, a partition μ of n is in the image of Θ_M if and only if $\sum_{j=1}^{M-1} m_{(iM-j)}(\mu') \leq 1$, for each $i \geq 1$, where μ' is the conjugate transpose partition of μ.*

Proof. The proof is along the same lines as in [Mil16]. □

Now we can write the generating function for this quantity. This generalizes the result mentioned in [Mil16] (just before Proposition 3) for $M = 2$.

Proposition 8.1.3. *With the notation as above,*

$$1 + \sum_{n=1}^{\infty} |\Theta_M(\Lambda(n))| u^n = \prod_{k=1}^{\infty} \frac{1 + u^{kM-1} + u^{kM-2} + \cdots + u^{kM-(M-1)}}{1 - u^{kM}}.$$

Proof. By the previous Lemma, we see that the k^{th} term $|\Theta_M(\Lambda(k))|$ is equal to the number of partitions $\lambda \vdash k$ satisfying $\sum_{j=1}^{M-1} m_{(iM-j)}(\lambda') \leq 1$. This means that for each $i \geq 1$, at most one of $m_{iM-j}(\lambda') = 1$, and all other terms are 0 in the sum. For counting sake, we can think of λ instead of λ'. Thus, $|\Theta_M(\Lambda(k))|$ is the coefficient if u^k in the following product:

$$\left((1+u+u^2+\cdots+u^{M-1})\left(\sum_{t=0}^{\infty}u^{tM}\right)\right)\times$$
$$\left((1+u^{M+1}+u^{M+2}+\cdots+u^{2M-1})\left(\sum_{t=0}^{\infty}u^{2tM}\right)\right)\times\cdots$$
$$\cdots\times\left((1+u^{iM+1}+u^{iM+2}+\cdots+u^{iM+(M-1)})\left(\sum_{t=0}^{\infty}u^{itM}\right)\right)\times\cdots$$
$$=\prod_{i=1}^{\infty}\left(1+u^{(i-1)M+1}+u^{(i-1)M+2}+\cdots+u^{(i-1)M+(M-1)}\right)\left(\frac{1}{1-u^{iM}}\right)$$
$$=\prod_{i=1}^{\infty}\frac{1+u^{iM-1}+u^{iM-2}+\cdots+u^{iM-(M-1)}}{1-u^{iM}}.$$

This completes the proof. □

Now, we are ready to describe the result which generalises [Mil16, Theorem 1], and determines M^{th} powers in GL(n,q) in this case.

Theorem 8.1.4. *Let M be a prime and q be a power of M. Let $\alpha \in GL(n,q)$ and Δ_α be its associated combinatorial data consisting of f_i and λ_{f_i}. Then, $X^M = \alpha$ has a solution in $GL(n,q)$ if and only if the partitions λ_{f_i} are in $\Theta_M(\Lambda(|\lambda_{f_i}|))$, for all i.*

Proof. Let $A \in \mathrm{GL}(n,q)$ be a solution of $X^M = \alpha$. It suffices to prove the statement when A has a single Jordan block. Thus we may assume, A corresponds to the polynomial g and partition $\mu_g = (\mu_1,\ldots,\mu_k)$. If $g(x) = (x-a_1)\cdots(x-a_d)$ then define $g^{(M)}(x) = (x-a_1^M)\cdots(x-a_d^M)$. Clearly, $g^{(M)}$ is defined over $\mathbb{F}_q$ if g is so. Now, we claim that the associated combinatorial data to A^M is $g^{(M)}$ and the partition $\Theta_M(\mu)$. Since, raising power M is a bijection on $\mathbb{F}_q^*$, we can easily find g such that $g^{(M)} = f$ (for example, by factorising it as a product of linear polynomials). Thus, this gives the required condition that λ_f must be $\Theta_M(\mu)$.

For the converse, we have α with its combinatorial data satisfying $\lambda_{f_i} \in \Theta_M(\Lambda(|\lambda_{f_i}|))$, for all i. Without loss of generality, we may assume it has a single Jordan block, say α is conjugate to $J_{f,k}$. Rest of the proof is similar to the [Mil16, Corollary 3 and Corollary 4], thus we mention it briefly. By factorising f over $\bar{\mathbb{F}}_q$, we can reduce it to constructing the solution A for the Jordan matrix $J_{\beta,m}$ where β is a root of f. We take $A = J_{\gamma,m}$ and get $A^M = \gamma^M I + J_{0,m}^M$ (since q is an M power). By Lemma 8.1.1, the combinatorial data Δ_{A^M} consists of polyno-

mial $(x-\gamma^M)$ and the partition $\mu = \left(\underbrace{\left\lceil \frac{m}{M} \right\rceil, \ldots, \left\lceil \frac{m}{M} \right\rceil}_{\bar{m}}, \underbrace{\left\lfloor \frac{m}{M} \right\rfloor, \ldots, \left\lfloor \frac{m}{M} \right\rfloor}_{M-\bar{m}}\right)$. Thus, we choose γ so that $\gamma^M = \beta$. Combined with the fact that $\mu \in \Theta_M(\Lambda(m))$, and putting together the Galois conjugate blocks, we get the proof. □

Since, order of a semisimple element α is coprime to M, the equation $X^M = \alpha$ always has a solution in $\mathrm{GL}(n,q)$. Further,

Corollary 8.1.5. *With notation as above, let $\alpha \in GL(n,q)$ be a regular element. Then, $X^M = \alpha$ has a solution in $GL(n,q)$ if and only if α is semisimple.*

Proof. Since α is regular, the combinatorial data Δ_α consists of f_i and λ_{f_i} with exactly one part $|\lambda_{f_i}|$. Then by Theorem 8.1.4, $X^M = \alpha$ has a solution if and only if, for each i, the partition $\lambda_f = (|\lambda_{f_i}|)$ is in $\Theta_M(|\lambda_{f_i}|)$. Now, from definition of Θ_M, this is possible only if $|\lambda_{f_i}| = 1$ for all i. This proves that $X^M = \alpha$ has a solution if and only if α is semisimple. □

We summarise this as follows:

Proposition 8.1.6. *Let M be a prime and q be a power of M. Then,*

1. *the M^{th} power semisimple classes in $GL(n,q)$ are $c(n,M)_{\mathrm{ss}} = c(n)_{\mathrm{ss}}$. The generating function for semisimple classes (respectively semisimple elements) which are M^{th} power is same as that of all semisimple classes (respectively semisimple elements).*

2. *The M^{th} power regular and regular semisimple classes in $GL(n,q)$ are $c(n,M)_{\mathrm{rg}} = c(n,M)_{\mathrm{rs}} = c(n)_{\mathrm{rs}}$. The generating function for regular and regular semisimple classes (respectively elements) which are M^{th} power is same as that of all regular semisimple classes (respectively elements).*

8.2 Generating function for the M^{th} power conjugacy classes

The following result generalizes [Mil16, Theorem 2].

Theorem 8.2.1. *Let M be a prime and q be a power of M. The generating*

function for M^{th} power conjugacy classes in $GL(n,q)$ is,

$$1+\sum_{n=1}^{\infty} c(n,M)u^n = \prod_{d\geq 1}\left(\prod_{k\geq 1}\frac{1+u^{d(kM-1)}+\cdots+u^{d(kM-(M-1))}}{1-u^{dkM}}\right)^{N(q,d)}.$$

Proof. By Theorem 8.1.4 we have (the first equality below),

$$\begin{aligned}1+\sum_{n=1}^{\infty} c(n,M)u^n &= \sum_{\lambda_f\in\Theta_M(|\lambda_f|)} u^{\sum_{f\in\phi}|\lambda_f|.deg(f)} = \prod_{f\in\Phi}\sum_{\lambda_f\in\Theta_M(|\lambda_f|)} u^{|\lambda_f|.deg(f)}\\ &= \prod_{f\in\Phi}\prod_{k\geq 1}\frac{1+u^{deg(f).(kM-1)}+ux^{deg(f).(kM-2)}+\cdots+u^{deg(f).(kM-(M-1))}}{1-u^{deg(f).kM}}\\ &= \prod_{d\geq 1}\left(\prod_{k\geq 1}\frac{1+u^{d(kM-1)}+\cdots+u^{d(kM-(M-1))}}{1-u^{dkM}}\right)^{N(q,d)}.\end{aligned}$$

The third equality follows from Proposition 8.1.3 by taking u as $u^{deg(f)}$. □

We note that for $M=2$, we get [Mil16, Theorem 2] by substituting $q=2$ in the following.

Corollary 8.2.2. *For $M=2$ we have,*

$$1+\sum_{n=1}^{\infty} c(n,2)u^n = \prod_{n\geq 1}\frac{(1-u^{2n})(1-qu^{2n})}{(1+u^{2n-1})(1-qu^n)(1-qu^{4n})}.$$

Proof. From previous Theorem we have,

$$1+\sum_{n=1}^{\infty} c(n,2)u^n = \prod_{d\geq 1}\prod_{k\geq 1}\left(\frac{1+u^{d(2k-1)}}{1-u^{2dk}}\right)^{N(q,d)}.$$

Since $\prod_{k\geq 1}\frac{1+u^{2k-1}}{1-u^{2k}} = \prod_{k\geq 1}\frac{1-u^{2k}}{(1-u^k)(1-u^{4k})}$ (obtained by multiplying with $(1-u^{2k-1})$ in the numerator and denominator) we get

$$1+\sum_{n=1}^{\infty} c(n,2)u^n = \prod_{d\geq 1}\prod_{k\geq 1}\left(\frac{1-u^{2dk}}{(1-u^{dk})(1-u^{4dk})}\right)^{N(q,d)}.$$

Now, we use $\prod_{d\geq 1}(1-u^d)^{-N(q,d)} = \frac{1-y}{1-qy}$ to get the required result. □

We can obtain the formula for general elements as follows:

Proposition 8.2.3. *With the notation as above,*

$$1+\sum_{n=1}^{\infty}\frac{|GL(n,q)^M|}{|GL(n,q)|}u^n=\prod_{f\in\Phi}\left(1+\sum_{n\geq 1}\sum_{\substack{\lambda\vdash n\\ \lambda\in\Theta_M(\Lambda(n))}}\frac{u^{n.deg(f)}}{q^{deg(f).\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^{deg(f)}}\right)_{m_i(\lambda_f)}}\right).$$

Proof. This follows from Theorem 8.1.4 and the cycle index generating function Equation 5.3.2. □

Chapter 9

Computing squares and third powers in $\mathbf{GL}(2,q)$ and $\mathbf{GL}(3,q)$

In this chapter we compute squares and third powers in the groups $\mathrm{GL}(2,q)$, and $\mathrm{GL}(3,q)$, using the necessary and sufficient conditions for powers we have developed in Chapter 7 and Chapter 8. Since $M = 2,3$ here, when $(M,q) = 1$ we use here Corollary 7.2.7 from Chapter 7. When q is a power of M, we use Theorem 8.1.4 from Chapter 8. We state these results once again here for convenience. These computations also verify the asymptotic results ($q \to \infty$) we obtained for $\mathrm{GL}(n,q)$ in Chapter 6. We use the notations of Chapter 7 and Chapter 8 freely here.

Proposition 9.0.1. *Let M be a prime with $(q,M) = 1$. Let $t = \mathfrak{M}(M;q)$ be the order of M in $(\mathbb{Z}/M\mathbb{Z})^\times$. Let $\alpha \in GL(n,q)$ with combinatorial data Δ_α consisting of polynomials $f_i \in \Phi$ of degree d_i and partitions $\lambda_{f_i} = (\lambda_{i_1}, \lambda_{i_2}, \ldots)$, $1 \leq i \leq l$. Then, $X^M = \alpha$ has a solution in $GL(n,q)$ if and only if for each $1 \leq i \leq l$ one of the following holds,*

1. *$t \nmid d_i$.*
2. *$f_i \in \Phi^M$ (in this case, it is equivalent to saying that $f_i(x^M)$ is reducible).*
3. *$M \mid m_j(\lambda_{f_i})$ for every j.*

Proposition 9.0.2. *Let M be a prime and q be a power of M. Let $\alpha \in GL(n,q)$ and Δ_α be its associated combinatorial data consisting of f_i and λ_{f_i}. Then, $X^M = \alpha$ has a solution in $GL(n,q)$ if and only if the partitions λ_{f_i} are in $\Theta_M(\Lambda(|\lambda_{f_i}|))$, for all i.*

9.1 Computing squares and third powers in GL$(2,q)$

We first need complete information of the conjugacy classes of GL$(2,q)$. We make a table containing the pieces of information we need. The classification is based on the different types of combinatorial data possible.

Combinatorial data of conjugacy classes	Number of elements in the conjugacy class	Number of such class
$f_1 = x-\mu_1, f_2 = x-\mu_2$ $\lvert\lambda_{f_1}\rvert = 1, \lvert\lambda_{f_2}\rvert = 1$	$q(q+1)$	$\frac{1}{2}(q-1)(q-2)$
$f = x-\mu$ $\lvert\lambda_f\rvert = 2, 1+1 \vdash 2$	1	$q-1$
$f = x-\mu$ $\lvert\lambda_f\rvert = 2, 2 \vdash 2$	q^2-1	$q-1$
$f = x^2+ax+b$ f is irreducible,$\lvert\lambda_f\rvert = 1$	q^2-q	$N(q,2) = \frac{1}{2}(q^2-q)$

Table 9.1: Conjugacy classes in GL$(2,q)$

Since, we are calculating, squares and third powers in GL$(2,q)$, we need the values of $N_2(q,2), N_3(q,2)$. We had already recorded this in Chapter 7 (see table 7.1).

q	$N_2(q,2)$
odd	$\frac{1}{4}(q-1)^2$
even	$\frac{1}{2}(q^2-q)$

$q \pmod 3$	$N_3(q,2)$
0	$\frac{1}{2}(q^2-q)$
1	$\frac{1}{6}(q^2-q)$
2	$\frac{1}{6}(q-1)(q-2)$

Table 9.2: Values of $N_2(q,2)$ and $N_3(q,2)$.

9.1.1 Computing squares in GL$(2,q)$

Theorem 9.1.1. *There are q^2-1 conjugacy classes in* GL$(2,q)$*, and* $\lvert\text{GL}(2,q)\rvert = (q^2-1)(q^2-q)$*. The following table gives the number of conjugacy classes and elements that are squares.*

q	$c(2,2)$	$\lvert\mathrm{GL}(2,q)^2\rvert$
odd	$\frac{1}{8}(3q^2+4q-7)$	$\frac{3}{8}q^4-\frac{5}{8}q^3+\frac{1}{8}q^2+\frac{5}{8}q-\frac{1}{2}$
even	q^2-q	q^4-2q^3+2q-1

Table 9.3: Squares in GL$(2,q)$.

Proof. When q is odd, we use Proposition 9.0.1. We enumerate the number of classes of each type as given in Table 9.1, which are squares.

1. The first type of conjugacy classes are squares if and only if μ_1 and μ_2 both are squares in $\mathbb{F}_q^\times$. The number of such classes are $\frac{1}{2}\left(\frac{q-1}{2}\right)\left(\frac{q-1}{2}-1\right) = \frac{1}{8}(q-1)(q-3)$.

2. All conjugacy classes of type 2 are squares (since, $2 \mid |\lambda_f| = 2$). Thus there are $q-1$ of them.

3. A conjugacy class of type 3 is a square if and only if $x-\mu$ is 2-power polynomial, that is, μ is a square in $\mathbb{F}_q^\times$ (since, $2 \nmid m_2(\lambda_f)$). Thus there are $\frac{q-1}{2}$ such classes.

4. A conjugacy class of type 4 is square if and only if f is 2-power polynomial. The number of such polynomials is given by $N_2(q,2)$, which is thus the number of square conjugacy classes of this type.

Adding all these gives $c(2,2)$ when q is odd as required. Thus, $\lvert\mathrm{GL}(2,q)^2\rvert$ is then readily obtained with the help of the information in Table 9.1.

When q is even we use Proposition 9.0.2, where we put $M=2$ and $n=2$. Observe that, $\Theta_2(\lambda) = (1,1)$ where λ is any partition of 2. With this observe that all classes of type 1,2,4 in Table 9.1 are squares while type 3 classes are non-squares. The result for $c(2,2)$ and $\lvert\mathrm{GL}(2,q)^2\rvert$ is then readily read-off from Table 9.1.

□

Corollary 9.1.2. *The following table gives the sizes of* $\mathrm{GL}(2,q)^2_{\mathrm{rg}}, \mathrm{GL}(2,q)^2_{\mathrm{ss}}$, $\mathrm{GL}(2,q)^2_{\mathrm{rs}}$.

9.1.2 Computing third powers in GL$(2,q)$

Theorem 9.1.3. *The following table gives the number of conjugacy classes and elements that are third powers.*

q	$\lvert\mathrm{GL}(2,q)^2_{\mathrm{rg}}\rvert$	$\lvert\mathrm{GL}(2,q)^2_{\mathrm{ss}}\rvert$	$\lvert\mathrm{GL}(2,q)^2_{\mathrm{rs}}\rvert$
odd	$\frac{3}{8}q^4-\frac{5}{8}q^3+\frac{1}{8}q^2$ $-\frac{3}{8}q-\frac{1}{2}$	$\frac{3}{8}q^4-\frac{9}{8}q^3+\frac{5}{8}q^2+\frac{9}{8}q-1$	$\frac{3}{8}q^4-\frac{9}{8}q^3+\frac{5}{8}q^2+\frac{1}{8}q$
even	q^4-2q^3+q	q^4-2q^3+2q-1	q^4-2q^3+q

Table 9.4: Values of $\lvert\mathrm{GL}(2,q)^2_{\mathrm{rg}}\rvert$, $\lvert\mathrm{GL}(2,q)^2_{\mathrm{ss}}\rvert$ and, $\lvert\mathrm{GL}(2,q)^2_{\mathrm{rs}}\rvert$.

$q(\mathrm{mod}\ 3)$	$c(2,3)$	$\lvert\mathrm{GL}(2,q)^3\rvert$
0	q^2-q	q^4-2q^3+2q-1
1	$\frac{2}{9}(q^2-1)$	$\frac{2}{9}(q^4-q^3-q^2+q)$
2	$\frac{2}{3}(q^2-1)$	$\frac{2}{3}(q^4-q^3-q^2+q)$

Table 9.5: Third powers in GL$(2,q)$

Proof. The proof is similar to Theorem 9.1.1. □

Corollary 9.1.4. *The following table gives the sizes of* $\mathrm{GL}(2,q)^3_{\mathrm{rg}}, \mathrm{GL}(2,q)^3_{\mathrm{ss}}$, $\mathrm{GL}(2,q)^3_{\mathrm{rs}}$.

$q(\mathrm{mod}\ 3)$	$\lvert\mathrm{GL}(2,q)^3_{\mathrm{rg}}\rvert$	$\lvert\mathrm{GL}(2,q)^3_{\mathrm{ss}}\rvert$	$\lvert\mathrm{GL}(2,q)^3_{\mathrm{rs}}\rvert$
0	q^4-2q^3+q	q^4-2q^3+2q-1	q^4-2q^3+q
1	$\frac{2}{9}q^4-\frac{2}{9}q^3-\frac{2}{9}q^2$ $-\frac{1}{9}q+\frac{1}{3}$	$\frac{2}{9}q^4-\frac{5}{9}q^3+\frac{1}{9}q^2$ $+\frac{5}{9}q-\frac{1}{3}$	$\frac{2}{9}q^4-\frac{5}{9}q^3+\frac{1}{9}q^2+\frac{2}{9}$
2	$\frac{2}{3}q^4-\frac{2}{3}q^3-\frac{2}{3}q^2$ $-\frac{1}{3}q+1$	$\frac{2}{3}q^4-\frac{5}{3}q^3+\frac{1}{3}q^2$ $+\frac{5}{3}q-1$	$\frac{2}{3}q^4-\frac{5}{3}q^3+\frac{1}{3}q^2+\frac{2}{3}q$

Table 9.6: Values of $\lvert\mathrm{GL}(2,q)^3_{\mathrm{rg}}\rvert$, $\lvert\mathrm{GL}(2,q)^3_{\mathrm{ss}}\rvert$ and, $\lvert\mathrm{GL}(2,q)^3_{\mathrm{rs}}\rvert$

Remark 9.1.5. The information in Tables 9.3, 9.4, 9.5, 9.6 verifies the asymptotic results we have obtained for $M=2,3$ for the group GL$(2,q)$ in Example 6.2.5.

9.2 Computing squares and third powers in GL$(3,q)$

We will follow the same outline, as in the previous section.

Combinatorial data of conjugacy classes	Number of elements in the conjugacy class	Number of such classes
$f_1=x-\mu_1, \lvert\lambda_{f_1}\rvert=1$		

$f_2 = x-\mu_2, \lvert\lambda_{f_2}\rvert = 1$ $f_3 = x-\mu_3, \lvert\lambda_{f_3}\rvert = 1$	$q^3(q+1)(q^2+q+1)$	$\frac{1}{6}(q-1)(q-2)(q-3)$
$f_1 = x-\mu_1, f_2 = x-\mu_2$ $\lvert\lambda_{f_1}\rvert = 2, 1+1 \vdash 2$ $\lvert\lambda_{f_2}\rvert = 1$	$q^2(q^2+q+1)$	$(q-1)(q-2)$
$f_1 = x-\mu_1, f_2 = x-\mu_2$ $\lvert\lambda_{f_1}\rvert = 2, 2 \vdash 2$ $\lvert\lambda_{f_2}\rvert = 1$	$q^2(q+1)(q^3-1)$	$(q-1)(q-2)$
$f = x-\mu$ $\lvert\lambda_f\rvert = 3, 1+1+1 \vdash 3$	1	$q-1$
$f = x-\mu$ $\lvert\lambda_f\rvert = 3, 3 \vdash 3$	$q(q^2-1)(q^3-1)$	$q-1$
$f = x-\mu$ $\lvert\lambda_f\rvert = 3, 2+1 \vdash 3$	$(q+1)(q^3-1)$	$q-1$
$f_1 = x-\mu$ $f_2 = x^2+ax+b$ $\lvert\lambda_{f_1}\rvert = 1, \lvert\lambda_{f_2}\rvert = 1$	q^6-q^3	$\frac{1}{2}q(q-1)^2$
$f = x^3+ax^2+bx+c$ f is irreducible,$\lvert\lambda_f\rvert = 1$	$(q^3-q)(q^3-q^2)$	$N(q,3) = \frac{1}{3}(q^3-q)$

Table 9.7: Conjugacy classes in GL$(3,q)$

Since, we are calculating, squares and third powers in GL$(3,q)$, in addition to the values of $N_2(q,3), N_3(q,3)$. We will also need $N_2(q,2)$ and, $N_3(q,2)$ which we already in Table 9.2.

q	$N_2(q,3)$
odd	$\frac{1}{6}(q^3-q)$
even	$\frac{1}{3}(q^3-q)$

$q \pmod 3$	$N_3(q,3)$
0	$\frac{1}{3}(q^3-q)$
1	$\frac{1}{9}(q^3-3q+2)$
2	$\frac{1}{3}(q^3-q)$

Table 9.8: Values of $N_2(q,3)$ and $N_3(q,3)$.

9.2.1 Computing squares in GL$(3,q)$

Theorem 9.2.1. *There are q^3-q conjugacy classes in* GL$(3,q)$*, and* $|\mathrm{GL}(3,q)| = (q^3-1)(q^3-q)(q^3-q^2)$*. The following table gives the number of conjugacy classes and elements that are squares in* GL$(3,q)$*.*

q	$c(3,2)$	$\lvert\mathrm{GL}(3,q)^2\rvert$
odd	$\frac{1}{16}(5q^3+3q^2-5q-3)$	$\frac{1}{16}(5q^9-7q^8-q^7+2q^6+3q^5+q^4$ $-7q^3+4q^2)$
even	$(q-1)(q^2+1)$	$q^9-2q^8+2q^6+q^5-q^4-3q^3+q^2+q$

Table 9.9: Squares in GL$(3, q)$.

Proof. Assume that q is odd. Let us write down the number of conjugacy classes of each type which are squares.

1. Any class of type 1 is a square class if and only if each f_i $(1 \leq i \leq 3)$ is 2-power, that is, μ_1, μ_2, μ_3 are squares in $F^\times$. The number of such classes is $\binom{(q-1)/2}{3} = \frac{1}{48}(q-1)(q-3)(q-5)$.

2. A class of type 2 is a square class if and only if $x - \mu_2$ is a 2-power polynomial, that is, μ_2 is a square in $\mathbb{F}_q^\times$. Number of such classes is given by $\left(\frac{q-1}{2}\right)\left(\frac{q-1}{2}\right) + \left(\frac{q-1}{2}\right)\left(\frac{q-1}{2}-1\right) = \frac{1}{2}(q-1)(q-2)$.

3. A class of type 3 is a square class if and only if both μ_1, μ_2 are squares in $\mathbb{F}_q^\times$. There are $\frac{1}{4}(q-1)(q-3)$ such classes.

4. A class of type 4 is a square if and only ifμ is a square in $\mathbb{F}_q^\times$ (since $2 \nmid m_1(\lambda_f) = 3$). Thus there are $\frac{q-1}{2}$ such classes.

5. A class of type 5 is a square if and only if μ is a square in $\mathbb{F}_q^\times$. Thus there are $\frac{q-1}{2}$ such classes.

6. A class of type 6 is a square if and only if μ is a square in $\mathbb{F}_q^\times$. Thus there are $\frac{q-1}{2}$ such classes.

7. A class of type 7 is a square class if and only if both f_1 and f_2 are 2-power polynomials. The number of such classes is given by $\frac{q-1}{2}.N_2(q,2) = \frac{1}{8}(q-1)^3$ (see Table 9.2).

8. A class of type 8 is a square if and only if f is 2-power polynomial. The number of such classes is given by $N_2(q,3) = \frac{1}{6}(q^3-q)$ (see Table 9.8).

Thus adding all these up we get $c(3,2)$ when q is odd. The expression for $\lvert\mathrm{GL}(3,q)^2\rvert$ can be found out using Table 9.7.

When q is even, we apply Proposition 9.0.2 with $n = 3, M = 2$. We have,

$$\Theta_2(\lambda) = \begin{cases} (1,1,1) & \text{when } \lambda = (1,1,1) \vdash 3 \text{ or, } \lambda = (2,1) \vdash 3 \\ (2,1) & \text{when } \lambda = (3) \vdash 3 \end{cases}.$$

It is clear then that classes of type 1,2,4,6,7,8 are square classes, while classes of type 3 and 5 are non-squares. With this the expressions for $c(3,2)$ and $|\mathrm{GL}(3,q)^2|$ are easily calculated using Table 9.7. □

Corollary 9.2.2. *The following table gives the sizes of* $\mathrm{GL}(3,q)^2_{\mathrm{rg}}, \mathrm{GL}(3,q)^2_{\mathrm{ss}}$, $\mathrm{GL}(3,q)^2_{\mathrm{rs}}$.

q	$\lvert\mathrm{GL}(3,q)_{\mathrm{rg}}\rvert$	$\lvert\mathrm{GL}(3,q)^2_{\mathrm{ss}}\rvert$	$\lvert\mathrm{GL}(3,q)^2_{\mathrm{rs}}\rvert$
odd	$\frac{5}{16}q^9 - \frac{7}{16}q^8 - \frac{1}{16}q^7$ $-\frac{3}{8}q^6 + \frac{11}{16}q^5 + \frac{1}{16}q^4$ $+\frac{9}{16}q^3 - \frac{1}{4}q^2 - \frac{1}{2}q$	$\frac{5}{16}q^9 - \frac{11}{16}q^8 + \frac{3}{16}q^7$ $+\frac{7}{8}q^6 - \frac{5}{16}q^5 - \frac{11}{16}q^4$ $-\frac{11}{16}q^3 + q^2 + \frac{1}{2}q - \frac{1}{2}$	$\frac{5}{16}q^9 - \frac{11}{16}q^8 + \frac{3}{16}q^7$ $+\frac{3}{8}q^6 + \frac{11}{16}q^5$ $-\frac{11}{16}q^4 - \frac{3}{16}q^3$
even	$q^9 - 2q^8 + q^6 + 2q^5$ $-q^4 - q^3$	$q^9 - 2q^8 + 2q^6 - q^4$ $-2q^3 + 2q^2 + q - 1$	$q^9 - 2q^8 + q^6 + 2q^5$ $-q^4 - q^3$

Table 9.10: Values of $|\mathrm{GL}(3,q)^2_{\mathrm{rg}}|, |\mathrm{GL}(3,q)^2_{\mathrm{ss}}|$ and, $|\mathrm{GL}(3,q)^2_{\mathrm{rs}}|$.

9.2.2 Computing third powers in $\mathbf{GL}(3,q)$

Theorem 9.2.3. *The following table gives the number of conjugacy classes and elements that are third powers in* $\mathrm{GL}(3,q)$.

$q \pmod 3$	$c(3,3)$	$\lvert\mathrm{GL}(3,q)^3\rvert$
0	$q^2(q-1)$	$q^9 - 2q^8 + 2q^6 - q^4$ $-2q^3 + 2q^2 + q - 1$
1	$\frac{1}{81}(14q^3 + 3q^2 + 42q - 59)$	$\frac{1}{81}(14q^9 - 14q^8 - 32q^7 + 36q^6$ $+14q^5 - 22q^4 + 4q^3 + 54q - 54)$
2	$\frac{1}{3}(2q^3 + q^2 - 2q - 1)$	$\frac{2}{3}(q^9 - q^8 - q^7 + q^5 + q^4 - q^3)$

Table 9.11: Third powers in $\mathrm{GL}(3,q)$.

Proof. The proof is similar to Theorem 9.2.1. □

Corollary 9.2.4. *The following table gives the sizes of* $\mathrm{GL}(3,q)^3_{\mathrm{rg}}, \mathrm{GL}(3,q)^3_{\mathrm{ss}}$, $\mathrm{GL}(3,q)^3_{\mathrm{rs}}$.

$q \pmod 3$	$\lvert\mathrm{GL}(3,q)_{\mathrm{rg}}\rvert$	$\lvert\mathrm{GL}(3,q)^3_{\mathrm{ss}}\rvert$	$\lvert\mathrm{GL}(3,q)^3_{\mathrm{rs}}\rvert$
0	$q^9-2q^8+q^6$ $+2q^5-q^4-q^3$	$q^9-2q^8+2q^6-q^4$ $-2q^3+2q^2+q-1$	$q^9-2q^8+q^6$ $+2q^5-q^4-q^3$
1	$\frac{14}{81}q^9-\frac{14}{81}q^8-\frac{32}{81}q^7$ $+\frac{1}{3}q^6+\frac{23}{81}q^5-\frac{22}{81}q^4$ $+\frac{40}{81}q^3-\frac{1}{9}q^2-\frac{1}{3}q$	$\frac{14}{81}q^9-\frac{23}{81}q^8-\frac{23}{81}q^7$ $+\frac{8}{9}q^6-\frac{13}{81}q^5-\frac{58}{81}q^4$ $-\frac{5}{81}q^3+\frac{4}{9}q^2+q-1$	$\frac{14}{81}q^9-\frac{23}{81}q^8-\frac{23}{81}q^7$ $+\frac{7}{9}q^6+\frac{23}{81}q^5$ $-\frac{58}{81}q^4+\frac{4}{81}q^3$
2	$\frac{2}{3}q^9-\frac{2}{3}q^8-\frac{2}{3}q^7$ $-q^6+\frac{5}{3}q^5+\frac{2}{3}q^4$ $+\frac{4}{3}q^3-q^2-q$	$\frac{2}{3}q^9-\frac{5}{3}q^8+\frac{1}{3}q^7$ $+2q^6-\frac{1}{3}q^5-\frac{4}{3}q^4$ $-\frac{5}{3}q^3+2q^2+q-1$	$\frac{2}{3}q^9-\frac{5}{3}q^8+\frac{1}{3}q^7$ $+q^6+\frac{5}{3}q^5-\frac{4}{3}q^4$ $-\frac{2}{3}q^3$

Table 9.12: Values of $\lvert\mathrm{GL}(3,q)^3_{\mathrm{rg}}\rvert$, $\lvert\mathrm{GL}(3,q)^3_{\mathrm{ss}}\rvert$ and, $\lvert\mathrm{GL}(3,q)^3_{\mathrm{rs}}\rvert$.

Remark 9.2.5. The information in Tables 9.9, 9.10, 9.11, 9.12 verifies asymptotic results we have obtained for $M = 2, 3$ for the group $\mathrm{GL}(2,q)$ in Example 6.2.5.

9.3 A solution to a problem by R. Stanley

In [Sta97], the author Richard Stanley had asked to count the number of matrices over the finite field $\mathbb{F}_q$ which have a square root (see Exercise 180 of Chapter 1). V. Miller in [Mil16] characterized invertible matrices with square roots in characteristic 2. This led to the generating function for the number of conjugacy classes of all invertible matrices with square roots which is Corollary 8.2.2 (see Chapter 8). On the other hand, when the characteristic is not 2, the invertible matrices having square roots are characterized by Corollary 7.2.7 by putting $M = 2$. This leads to the generating functions for the number of conjugacy classes of invertible matrices possessing square roots and the proportion of matrices with square roots obtained by putting $M = 2$ in Corollary 7.5.4 and Theorem 7.5.5 respectively (see Chapter 7). We collect these generating functions so obtained in the following theorem,

Theorem 9.3.1. *We have the following:*

1. *Suppose q is a power of 2. The generating function for $c(n,2)$ which is the number of conjugacy classes of invertible matrices which have square roots is given by*

$$1+\sum_{n=1}^{\infty} c(n,2)u^n = \prod_{n\geq 1} \frac{(1-u^{2n})(1-qu^{2n})}{(1+u^{2n-1})(1-qu^n)(1-qu^{4n})}.$$

2. Suppose q is not a power of 2. Then,

$$1+\sum_{n=1}^{\infty} c(n,2)u^n = \prod_{j=1}^{\infty}\left(\left(\frac{1-u^{2j}}{1-qu^{2j}}\right)\prod_{d\geq 1}(1+u^{jd})^{-N_2(q,d)}\right).$$

3. Suppose q is not a power of 2. Then,

$$\begin{aligned}1+\sum_{n=0}^{\infty}\frac{|\mathrm{GL}(n,q)^2|}{|\mathrm{GL}(n,q)|}u^n &= \prod_{d\geq 1}\left(1+\sum_{j\geq 1}\sum_{\lambda\vdash j}\frac{u^{jd}}{q^{d\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{N_2(q,d)}\\ &\quad\times\prod_{d\geq 1}\left(1+\sum_{n\geq 1}\sum_{\lambda\vdash n}\frac{u^{2nd}}{q^{4d\sum_i(\lambda_i')^2}\prod_{i\geq 1}\left(\frac{1}{q^d}\right)_{m_i(\lambda)}}\right)^{\widehat{N}(q,d)},\end{aligned}$$

where $\widehat{N}(q,d) = N(q,d) - N_2(q,d)$.

Here, $N_2(q,d)$ denotes the number of 2-power polynomials.

The above results answer the question posed by Stanley in the sense of generating functions. We expect that further concrete results about these (like some form of recursive relation on n or, sharp bounds or, even closed formula) can be deduced from the generating functions so-obtained or, otherwise.

Chapter 10

Future Plans

This thesis revolves around the study of the image of the power map in finite reductive groups. We have attempted to study the image of the power map $\omega_M : G^F \to G^F$ given by $g \mapsto g^M$ where $M \geq 2$ is an integer and G is connected reductive group over $\bar{\mathbb{F}}_q$ with Steinberg endomorphism F. There are lots of questions that still remain to be answered to get a more explicit understanding of this map on these infinite families of finite groups. In this final chapter, we mention some of the interesting questions in this direction.

10.1 Further Questions

The most general question on this topic is to study the image of the power map on a finite reductive group G, that is, to understand whether there exists a solution of the equation $X^M = g$ (for $g \in G$) in G. Since this map is mostly non-surjective it is natural to ask how *"big"* or *"small"* is the image compared to the size of the group which in turn naturally leads to the idea of enumerating the M^{th} powers in G. This thesis has addressed two kinds of problems in this direction. In Chapter 6, we have solved the problem of asymptotic as $q \to \infty$ for the proportion of M^{th} powers in a finite reductive group G. In the second part, to understand the image more explicitly, we have specialized over the group $\mathrm{GL}(n, q)$, and derived generating functions for the proportion of powers, which is often the tool for questions related to enumeration. This explicit study perfectly makes sense over any finite classical group. This leads us to the first question.

Problem 10.1.1. *Derive generating functions for the proportion of regular, regular semisimple, semisimple and all elements that are M^{th} powers in the classical groups like* $\mathrm{SL}(n, q)$, $\mathrm{Sp}(2n, q)$, $\mathrm{GU}(n, q)$, $\mathrm{GO}(2n + 1, q)$, $\mathrm{GO}^+(2n, q)$, $\mathrm{GO}^-(2n, q)$

etc., (see Chapter 3 for definitions). Derive the generating functions for the number of conjugacy classes of regular, regular semisimple, semisimple and all elements that are M^{th} powers in these classical groups.

We have generating functions for the M^{th} power invertible matrices and we used these generating functions to determine the exact value of $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$ for some values of n. We had further guessed an upper bound for the proportion of M^{th} powers in $\mathrm{GL}(n,q)$ (see Question 7.6.16 in Chapter 7).

Problem 10.1.2. *Check the validity of the statement in Question 7.6.16.*

A positive proof of the above problem will also determine the limiting value of these proportions in $\mathrm{GL}(n,q)$ as $n \to \infty$ (with M, q fixed, and in the case $(M,q) = 1$) (see [Ful99] for the limiting values of proportion of semisimple, regular and, regular semisimple elements in $\mathrm{GL}(n,q)$ as $n \to \infty$).

Problem 10.1.3. *Determine* $\lim_{n\to\infty} \frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$ *when M is a prime and q is a power of M (see Chapter 8).*

Problem 10.1.4. *Determine sharp bounds (both upper and lower) for* $\frac{|\mathrm{GL}(n,q)^M|}{|\mathrm{GL}(n,q)|}$, *and more generally in case of all the other finite classical groups.*

We have already conjectured that the asymptotic values (that is, subsequential limits) as $q \to \infty$ are also upper bound for the proportion of powers in $\mathrm{GL}(n,q)$. This leads us to conjecture a more general result for any $M \geq 2$, and not just primes as follows:

Problem 10.1.5. *Is the following true: Let $M \geq 2$ be any integer and G be a connected reductive group with Steinberg endomorphism F. Let $G(\mathbb{F}_q)$ denote the finite group of fixed points of G under F. Then,*

$$\frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|} \leq \sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}$$

where the sum varies over non-conjugate maximal tori T in $G(\mathbb{F}_q)$, $T = T_{d_1,\cdots,d_s} \cong C_{d_1} \times \cdots \times C_{d_s}$ reflects the cyclic structure of T and the group $W_T = N_{G(\mathbb{F}_q)}(T)/T$.

Problem 10.1.6. *Given a reductive group G with Steinberg endomorphism F,*

determine the explicit value of the expression,

$$\sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}.$$

We have already answered this for $\mathrm{GL}(n,q)$ *and* $\mathrm{GU}(n,q)$ *by assuming* M *to be prime in Chapter 6.*

We believe answers to these questions will serve as a wealth of information on the image of power maps on finite reductive groups.

So far we have concentrated on the image of the power map ω_M. It is equally interesting and important to understand the pre-image of this map. More precisely, what information can we have on the fiber of each element under the power map? In other words,

Problem 10.1.7. *Let* G *be a finite reductive group. Fix* $g \in G$*, and suppose* $X^M = g$ *has a solution in* G *for a fixed* $M \geq 2$*. Study the set* $F_g^M := \{\alpha \in G \mid \alpha^M = g\} \subseteq G$*, which is the set of all solutions of the equation* $X^M = g$ *in* G*.*

All the questions that have been posed for the image set make perfect sense for the fiber F_g^M of $g \in G$. It is worthwhile to mention a character theoretic connection here.

Let G be a finite group and $Irr(G)$ denote the set of all *irreducible characters* of G. Let ω be an element of the free group F_d on d generators. Consider the corresponding word map $\omega : G^d \to G$. For $g \in G$, the fiber F_g^ω is defined by,

$$F_g^\omega = \{(g_1, g_2, \ldots, g_d) \in G^d \mid \omega(g_1, \ldots, g_d) = g\}.$$

Let $N_g^\omega = |F_g^\omega|$. We define the map,

$$N_G^\omega : G \to \mathbb{C} \text{ by,} \qquad\qquad N_G^\omega(g) = N_g^\omega.$$

The function N_G^ω is a class-function and thus $N_g^\omega = \sum_{\chi \in Irr(G)} a_{\omega,\chi}\chi$ is a $\mathbb{C}$-linear combination of the irreducible characters of χ. This is not always a character of G. The coefficients $a_{\omega,\chi}$ are called *Fourier coefficients* of G with respect to the word ω. For the commutator word ω, a classical result of Frobenius says that $a_{\omega,\chi} = \frac{|G|}{\chi(1)}$ for all $\chi \in Irr(G)$. Thus for the commutator word ω, N_G^ω is indeed a character of G. In general, the Fourier coefficients can be found out using the

inverse Fourier transform.

$$a_{\omega,\chi} = \frac{1}{|G|} \sum_{(g_1,\ldots,g_d)\in G^d} \chi(\omega(g_1,\ldots,g_d)^{-1}),$$

although this is not always easy to use in practice.

For the power word $\omega = x^2$, the coefficient $a_{\omega,\chi}$ can only be $+1, 0, -1$. This coefficient attached to χ is called the *Frobenius-Schur indicator* of χ. For a general power word $\omega = x^M$ for an integer $M \geq 2$,

$$a_{\omega,\chi} = \frac{1}{|G|} \sum_{g\in G} \chi(g^M).$$

These coefficients are called the *generalized Frobenius-Schur indicators*. In our setting, it will also be interesting to determine these in the case of finite reductive groups more explicitly. For more literature on these Fourier coefficients, we refer the reader to the survey article by Shalev (see Section 4 and Section 7, [Sha13]), and references therein).

Bibliography

[And76] George E. Andrews, *The theory of partitions*, Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976, Encyclopedia of Mathematics and its Applications, Vol. 2. MR 0557013

[Ben74] Edward A. Bender, *Asymptotic methods in enumeration*, SIAM Rev. **16** (1974), 485–515. MR 376369

[BG80] Ethan D. Bolker and Andrew M. Gleason, *Counting permutations*, J. Combin. Theory Ser. A **29** (1980), no. 2, 236–242. MR 583962

[BG89] Edward A. Bertram and Basil Gordon, *Counting special permutations*, European J. Combin. **10** (1989), no. 3, 221–226. MR 1029166

[BG07] A. A. Buturlakin and M. A. Grechkoseeva, *The cyclic structure of maximal tori in finite classical groups*, Algebra Logika **46** (2007), no. 2, 129–156. MR 2356522

[BGHP20] John Bamberg, S. P. Glasby, Scott Harper, and Cheryl E. Praeger, *Permutations with orders coprime to a given integer*, Electron. J. Combin. **27** (2020), no. 1, Paper No. 1.6, 14. MR 4057178

[Blu74] Joseph Blum, *Enumeration of the square permutations in S_n*, J. Combinatorial Theory Ser. A **17** (1974), 156–161. MR 345833

[BMW00] Miklós Bóna, Andrew McLennan, and Dennis White, *Permutations with roots*, Random Structures Algorithms **17** (2000), no. 2, 157–167. MR 1774748

[Bri02] John R. Britnell, *Cyclic, separable and semisimple matrices in the special linear groups over a finite field*, J. London Math. Soc. (2) **66** (2002), no. 3, 605–622. MR 1934295

[Bri06] ———, *Cyclic, separable and semisimple transformations in the special unitary groups over a finite field*, J. Group Theory **9** (2006), no. 4, 547–569. MR 2243246

[But55] M. C. R. Butler, *The irreducible factors of $f(x^m)$ over a finite field*, J. London Math. Soc. **30** (1955), 480–482. MR 71463

[Car85] Roger W. Carter, *Finite groups of Lie type*, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1985, Conjugacy classes and complex characters, A Wiley-Interscience Publication. MR 794307

[CM11] Sunil Chebolu and Jan Minac, *Counting irreducible polynomials over finite fields using the inclusion-exclusion principle*, Math. Mag. (2011), 369–371.

[DF04] David S. Dummit and Richard M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR 2286236

[Enn63] Veikko Ennola, *On the characters of the finite unitary groups*, Ann. Acad. Sci. Fenn. Ser. A I No. **323** (1963), 35. MR 0156900

[ET65] P. Erdős and P. Turán, *On some problems of a statistical group-theory. I*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **4** (1965), 175–186 (1965). MR 184994

[ET67a] ———, *On some problems of a statistical group-theory. II*, Acta math. Acad. Sci. Hungar. **18** (1967), 151–163. MR 0207810

[ET67b] ———, *On some problems of a statistical group-theory. III*, Acta Math. Acad. Sci. Hungar. **18** (1967), 309–320. MR 215908

[ET68] ———, *On some problems of a statistical group-theory. IV*, Acta Math. Acad. Sci. Hungar. **19** (1968), 413–435. MR 232833

[FG13] Jason Fulman and Robert Guralnick, *The number of regular semisimple conjugacy classes in the finite classical groups*, Linear Algebra Appl. **439** (2013), no. 2, 488–503. MR 3089699

[FJK98] P. Fleischmann, I. Janiszczak, and R. Knörr, *The number of regular semisimple classes of special linear and unitary groups*, Linear Algebra Appl. **274** (1998), 17–26. MR 1611977

[FNP05] Jason Fulman, Peter M. Neumann, and Cheryl E. Praeger, *A generating function approach to the enumeration of matrices in classical groups over finite fields*, Mem. Amer. Math. Soc. **176** (2005), no. 830, vi+90. MR 2145026

[Ful99] Jason Fulman, *Cycle indices for the finite classical groups*, J. Group Theory **2** (1999), no. 3, 251–289. MR 1696313

[Ful02] ———, *Random matrix theory over finite fields*, Bull. Amer. Math. Soc. (N.S.) **39** (2002), no. 1, 51–85. MR 1864086

[Gec03] Meinolf Geck, *An introduction to algebraic geometry and algebraic groups*, Oxford Graduate Texts in Mathematics, vol. 10, Oxford University Press, Oxford, 2003. MR 2032320

[GKSV19] Alexey Galt, Amit Kulshrestha, Anupam Singh, and Evgeny Vdovin, *On Shalev's conjecture for type A_n and ${}^2A_n$*, J. Group Theory **22** (2019), no. 4, 713–728. MR 3975688

[Gre55] J. A. Green, *The characters of the finite general linear groups*, Trans. Amer. Math. Soc. **80** (1955), 402–447. MR 72878

[Gro02] Larry C. Grove, *Classical groups and geometric algebra*, Graduate Studies in Mathematics, vol. 39, American Mathematical Society, Providence, RI, 2002. MR 1859189

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157

[Hum75] James E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York-Heidelberg, 1975, Graduate Texts in Mathematics, No. 21. MR 0396773

[JKZ13] F. Jouve, E. Kowalski, and D. Zywina, *Splitting fields of characteristic polynomials of random elements in arithmetic groups*, Israel J. Math. **193** (2013), no. 1, 263–307. MR 3038553

[KKS20] Amit Kulshrestha, Rijubrata Kundu, and Anupam Singh, *Asymptotics of the powers in finite reductive groups*, arXiv:2004.12616 (2020).

[KM20] Rijubrata Kundu and Sudipa Mondal, *Powers in the wreath product of G with S_n*, arXiv:2010.04954 (2020).

[KS20a] Amit Kulshrestha and Anupam Singh, *Computing n-th roots in* SL_2 *and Fibonacci polynomials*, Proc. Indian Acad. Sci. Math. Sci. **130** (2020), no. 1, Paper No. 31, 20. MR 4092502

[KS20b] Rijubrata Kundu and Anupam Singh, *Generating functions for the powers in* $GL(n, q)$., arXiv:2003.14057 (2020).

[Kun81] Joseph P. S. Kung, *The cycle structure of a linear transformation over a finite field*, Linear Algebra Appl. **36** (1981), 141–155. MR 604337

[Lar04] Michael Larsen, *Word maps have large image*, Israel J. Math. **139** (2004), 149–156. MR 2041227

[LN83] Rudolf Lidl and Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983, With a foreword by P. M. Cohn. MR 746963

[LOST10] Martin W. Liebeck, E. A. O'Brien, Aner Shalev, and Pham Huu Tiep, *The Ore conjecture*, J. Eur. Math. Soc. (JEMS) **12** (2010), no. 4, 939–1008. MR 2654085

[LOST12] ———, *Products of squares in finite simple groups*, Proc. Amer. Math. Soc. **140** (2012), no. 1, 21–33. MR 2833514

[Lot02] M. Lothaire, *Algebraic combinatorics on words*, Encyclopedia of Mathematics and its Applications, vol. 90, Cambridge University Press, Cambridge, 2002, A collective work by Jean Berstel, Dominique Perrin, Patrice Seebold, Julien Cassaigne, Aldo De Luca, Steffano Varricchio, Alain Lascoux, Bernard Leclerc, Jean-Yves Thibon, Veronique Bruyere, Christiane Frougny, Filippo Mignosi, Antonio Restivo, Christophe Reutenauer, Dominique Foata, Guo-Niu Han, Jacques Desarmenien, Volker Diekert, Tero Harju, Juhani Karhumaki and Wojciech Plandowski, With a preface by Berstel and Perrin. MR 1905123

[LS09] Michael Larsen and Aner Shalev, *Word maps and Waring type problems*, J. Amer. Math. Soc. **22** (2009), no. 2, 437–466. MR 2476780

[LST11] Michael Larsen, Aner Shalev, and Pham Huu Tiep, *The Waring problem for finite simple groups*, Ann. of Math. (2) **174** (2011), no. 3, 1885–1950. MR 2846493

[Mac81] I. G. Macdonald, *Numbers of conjugacy classes in some finite classical groups*, Bull. Austral. Math. Soc. **23** (1981), no. 1, 23–48. MR 615131

[Mac95] ———, *Symmetric functions and Hall polynomials*, second ed., Oxford Mathematical Monographs, The Clarendon Press, Oxford University Press, New York, 1995, With contributions by A. Zelevinsky, Oxford Science Publications. MR 1354144

[Mil16] Victor S. Miller, *Counting matrices that are squares*, arXiv:1606.09299 (2016).

[MP76] Mikhail Petrovich Mineev and Alexander Ivanovich Pavlov, *On the number of permutations of special form*, Mathematics of the USSR-Sbornik 28, no. 3 (1976).

[MT11] Gunter Malle and Donna Testerman, *Linear algebraic groups and finite groups of Lie type*, Cambridge Studies in Advanced Mathematics, vol. 133, Cambridge University Press, Cambridge, 2011. MR 2850737

[Pav82] Alexander Ivanovich Pavlov, *On the limit distribution of the number of cycles and the logarithm of the order of a class of permutations*, Mathematics of the USSR-Sbornik 42, no. 4 (1982).

[Pou02] Nicolas Pouyanne, *On the number of permutations admitting an m-th root*, Electron. J. Combin. **9** (2002), no. 1, Research Paper 3, 12. MR 1887084

[Pou09] M. R. Pournaki, *On the number of even permutations with roots*, Australas. J. Combin. **45** (2009), 37–42.

[PR87] G. Pólya and R. C. Read, *Combinatorial enumeration of groups, graphs, and chemical compounds*, Springer-Verlag, New York, 1987, Pólya's contribution translated from the German by Dorothee Aeppli. MR 884155

[Sha13] Aner Shalev, *Some results and problems in the theory of word maps*, Erdös centennial, Bolyai Soc. Math. Stud., vol. 25, János Bolyai Math. Soc., Budapest, 2013, pp. 611–649. MR 3203613

[Spr98] T. A. Springer, *Linear algebraic groups*, second ed., Progress in Mathematics, vol. 9, Birkhäuser Boston, Inc., Boston, MA, 1998. MR 1642713

[Sta97] Richard P. Stanley, *Enumerative combinatorics. Vol. 1*, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 1997, With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original. MR 1442260

[Sto88] Richard Stong, *Some asymptotic results on finite vector spaces*, Adv. in Appl. Math. **9** (1988), no. 2, 167–199. MR 937520

[Tur70] P. Turán, *On some connections between combinatorics and group theory*, Combinatorial theory and its applications, III (Proc. Colloq., Balatonfüred, 1969), 1970, pp. 1055–1082. MR 0306107

[Wal63] G. E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Austral. Math. Soc. **3** (1963), 1–62. MR 0150210

[Wal80] ———, *Conjugacy classes in projective and special linear groups*, Bull. Austral. Math. Soc. **22** (1980), no. 3, 339–364. MR 601642

[Wal99] ———, *Counting cyclic and separable matrices over a finite field*, Bull. Austral. Math. Soc. **60** (1999), no. 2, 253–284. MR 1711918

[Zav19] Andrei V. Zavarnitsine, *On the maximal tori in finite linear and unitary groups*, Sib. Èlektron. Mat. Izv. **16** (2019), 1069–1078. MR 3995166