STRATIFICATION AND ARITHMETIC DYNAMICS ON CHARACTER VARIETIES

by

Cigole Thomas
A Dissertation
Submitted to the
Graduate Faculty
of
George Mason University
In Partial fulfillment of
The Requirements for the Degree
of
Doctor of Philosophy
Mathematics

Committee:

______________________ Dr. Sean Lawton, Dissertation Director

______________________ Dr. Neil Epstein, Committee Member

______________________ Dr. Rebecca Goldin, Committee Member

______________________ Dr. Robert Oerter , Committee Member

______________________ Dr. Maria Emelianenko, Department Chair

______________________ Dr. Donna Fox, Associate Dean for Student Affairs, College of Science

______________________ Dr. Fernando R. Miralles-Wilhelm, Dean, College of Science

Date: ______________________ Spring Semester 2022
George Mason University
Fairfax, VA

Stratification and Arithmetic Dynamics on Character Varieties

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at George Mason University

By

Cigole Thomas
Master of Science
George Mason University, Fairfax, 2018
Integrated BS - MS
Indian Institute of Science Education and Research Mohali, India, 2015

Director: Dr. Sean Lawton, Professor
Department of Mathematical Sciences

Spring Semester 2022
George Mason University
Fairfax, VA

Dedication

I dedicate this thesis to my parents, Thomas Elias and Shobha Thomas - my first teachers and silent partners in my dreams.

Acknowledgments

First and foremost, I would like to thank my advisor, Sean Lawton. I am very fortunate to have an outstanding teacher who is extremely patient, understanding, encouraging, and supportive. I have greatly benefited from his insightful guidance, contagious enthusiasm for mathematics, and vast knowledge and broad interest in the subject area. In addition to being a great advisor, he is a friend and a good mentor who played a significant role in my growth as a researcher, teacher, and academic.

I want to thank my dissertation committee members, Rebecca Goldin, Neil Epstein, and Robert Oerter, for their valuable suggestions, time, and encouragement. A special thanks to Maria Emelianenko for always finding time to give advice and inspiration. I would like to thank Robert Sachs for teaching me how to be a better teacher. I am grateful to the faculty and staff, especially Christine Amaya, in the mathematics department at George Mason University, for always providing support and help whenever needed.

Two other people I am fortunate to have crossed paths with and thankful for are Jòzef Przytycki, for his kindness and warmth, and Krishnendu Gongopadhyay, who first taught me about geometry and set me on this research path.

I want to especially thank my friends from near and far, friends from GMU who were home away from home, friends from church for their prayers, my lovely family at Norman who don't let me miss home, friends from IISER who are forever family, and school friends who kept the childhood memories alive when I needed it the most. I thank each of them for being lovely people to do life with.

My heartfelt gratitude for my family, who always gave me love and care from afar. My parents, who taught me about God, math, and how to strive to be a better person, my sister Daida Thomas for her unwavering love and support through thick and thin, and my little sister Loria Thomas for her constant supply of love and innocence. I remember my grandmother, whom I lost two years ago. I am thankful for her stories, songs, love, and our fights.

Above all, I am forever grateful to God for giving me all that I have and making me who I am, Jesus for his never-ending love and being an everlasting presence in my life.

Table of Contents

List of Tables

List of Figures

Notation

$\mathbb{C}$	Set of complex numbers	
$\mathbb{R}$	Set of real numbers	
$\mathbb{Z}$	Set of integers	
$\mathbb{Z}_p$	Cyclic group with p elements for prime p	26
$\mathbb{F}_q$	Finite field of order $q = p^k$ where p is a prime and $k \geq 1$	41
$\overline{\mathbb{F}}_q$	Algebraic closure of $\mathbb{F}_q$	41
$\mathrm{Aut}(\Gamma)$	Group of automorphisms of the group Γ	1
$\mathrm{Out}(\Gamma)$	Group of outer automorphisms of the group Γ	1
$\mathrm{M_n(\mathbb{F}_q)}$	Set of all matrices with entries from $\mathbb{F}_q$	5
$\mathrm{GL}_n(\mathbb{F}_q)$	Subgroup of $\mathrm{M}_n(\mathbb{F}_q)$ with matrices of non-zero determinant	5
$\mathrm{SL_n(\mathbb{F}_q)}$	Subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ with matrices of determinant one	5
$\mathrm{Hom}(\Gamma, G)$	G-Representation variety of Γ	6
$\mathrm{Hom}(\Gamma, G)^*$	Non-trivial points in $\mathrm{Hom}(\Gamma, G)$	25
$\mathfrak{X}_\Gamma(G)$	G-Character Variety of Γ	6
$X(\mathbb{F}_q)$	Finite field points of a variety X defined over $\mathbb{Z}$	41
$\mathcal{S}_\Gamma(G, r)$	The set, $\{(A_1, \ldots, A_r) \in G^r \mid R_i((A_1, \ldots, A_r)) = 1\}$	13
$\mathcal{D}(G)$	Set of diagonal matrices in a matrix group G	48
$\mathrm{char}(A)$	Characteristic polynomial of A	55
$Z(G)$	Center of the group G	76

Abstract

STRATIFICATION AND ARITHMETIC DYNAMICS ON CHARACTER VARIETIES

Cigole Thomas, PhD

George Mason University, 2022

Dissertation Director: Dr. Sean Lawton

If G is a reductive algebraic group over $\mathbb{Z}$, the G-character variety of a finitely presented group Γ parameterizes the set of closed conjugation orbits in $\mathrm{Hom}(\Gamma, G)$. The group of automorphisms, $\mathrm{Aut}(\Gamma)$, acts on the representation variety, $\mathrm{Hom}(\Gamma, G)$, which leads to a natural action of the group of outer automorphisms, $\mathrm{Out}(\Gamma)$, on the character variety. In this thesis, we study the dynamics of the action of $\mathrm{Out}(\Gamma)$ on the finite field points of the character variety $\mathfrak{X}_\Gamma(G)$. We provide a criterion in terms of subgroups of G for the action to be non-transitive on the non-trivial points of the representation variety and the character variety. We define *free-type groups* to be groups with elementary automorphisms similar to the Nielsen transformations of a free group. We then proceed to prove that the $\mathrm{Aut}(\Gamma)$ action is transitive on the set of epimorphisms from Γ to G when Γ is free-type. Additionally, we provide a characterization of free-type groups. Finally, we introduce the idea of *asymptotic ratio* as the ratio of the number of points in a maximal orbit to that in the variety as the order of the finite field goes to ∞. If the asymptotic ratio equals one, we say that the action is *asymptotically transitive*. We provide an upper bound for the asymptotic ratio in these cases and thus prove that the action is not asymptotically transitive on the SL_n- character varieties of $\mathbb{Z}^r$ for $n = 2, 3$.

Along the way, we give a new proof for the E-polynomial of these free abelian character varieties.

Chapter 1: Introduction

The objective of this thesis is to understand certain properties of the dynamics of outer automorphism groups acting on character varieties over finite fields. Specifically, properties of the action such as transitivity and the existence of a large orbit are explored. Additionally, a new property called asymptotic transitivity is introduced and investigated for specific groups G and Γ.

If G is a complex affine reductive algebraic group and Γ a finitely presented group, then the set of G-representations of Γ form an algebraic set $\mathrm{Hom}(\Gamma, G)$. The group G acts on the set of homomorphisms by conjugation. The *G-character variety* of Γ is the space of equivalence classes of group homomorphisms from Γ to G where two homomorphisms are equivalent if their conjugation orbit closures intersect. The G-character variety of Γ is the categorical quotient in the category of affine varieties denoted by

$$\mathfrak{X}_\Gamma(G) := \mathrm{Hom}(\Gamma, G) /\!/ G.$$

This categorical quotient is constructed using Geometric Invariant Theory (GIT). See the next section for a detailed description of character variety as a GIT quotient. When G is an affine algebraic group defined over the integers, $\mathbb{Z}$, the locus of finite field points of the G-character variety of Γ is well defined. The automorphism group $\mathrm{Aut}(\Gamma)$ acts naturally on the G-representation variety of Γ. This leads to an action of $\mathrm{Out}(\Gamma)$ on the finite field points of $\mathfrak{X}_\Gamma(G)$. In this thesis, the dynamics of this action is explored.

The second chapter explores the property of transitivity and finding a 'large' orbit. We begin by detailing the example of the action of $\mathrm{Out}(\mathbb{Z}^2)$ on the character variety $\mathfrak{X}_{\mathbb{Z}^2}(\mathrm{SL}_2(\mathbb{F}_2))$. A complete description of the orbits along with a visual representation is provided. Motivated by the example, we prove a criterion for the $\mathrm{Aut}(\Gamma)$-action to be non-transitive on the representation variety $\mathrm{Hom}(\Gamma, G)$ for a finitely presented group Γ and any group G. Additionally, when G is an affine algebraic reductive group we deduce a criterion for the $\mathrm{Out}(\Gamma)$-action on the G-character variety of Γ to be non-transitive. We prove that the existence of proper subgroups of G with at least one homomorphism being mapped into the subgroup ensures that the action is non-transitive. As a corollary, we provide a necessary condition for the action to be transitive on the representation variety when Γ is free.

Subsequently, we prove the main result of the thesis. We define free-type groups of n-generators as groups where the automorphism group is similar to that of the free group, F_n. We show that free abelian groups, p-groups, and free nilpotent groups are of free-type. Additionally, we show that free-type groups arise as quotients of free groups by characteristic subgroups. We then proceed to prove that if Γ is of free-type of n-generators, then the set of epimorphisms is a single orbit of the $\mathrm{Aut}(\Gamma)$-action on $\mathrm{Hom}(\Gamma, G)$ when $n \geq 2k$ where k is the minimal size of a generating set of G.

In the final chapter, we explore asymptotic transitivity of the free abelian character variety in the cases when $G = \mathrm{SL}_n(\mathbb{F}_q)$ for $n = 2, 3$. To accomplish this, we stratify the character varieties based on their stabilizer type and count the orbits in each stratum. We then prove that the action is not asymptotically transitive on these character varieties and provide an upper bound for asymptotic ratio, the ratio of the size of the maximal orbit over the size of the variety when the order of the finite field goes to ∞, in each case of $n = 2, 3$. Along the way, we give an alternate proof for the E-polynomial of the free SL_2- and SL_3- character varieties of $\mathbb{Z}^r$.

We now establish some preliminaries required to describe the background and literature on the above results.

1.1 Preliminaries

1.1.1 Definitions

Let $\Bbbk$ be an algebraically closed field and $\mathbb{A}^n(\Bbbk)$ or $\mathbb{A}^n = \{(k_1, \ldots, k_n) \mid k_1, \ldots, k_n \in \Bbbk\}$ denote affine n-space. If S is any collection of polynomials in $\Bbbk[x_1, \ldots, x_n]$, then define $V(S)$ to be the simultaneous zero set of S, i.e.,

$$V(S) = \{p \in \mathbb{A}^n \mid f(p) = 0 \text{ for all } f \in S\}.$$

Definition 1.1.1 (Algebraic Set)**.** A subset $X \subseteq \mathbb{A}^n$ is an *algebraic set* if X is zero set of a collection of polynomials, i.e, $X = V(S)$ for some $S \subseteq \Bbbk[x_1, \ldots, x_n]$.

Definition 1.1.2 ([31])**.** The *Zariski topology* on $\mathbb{A}^n$ is defined by taking the open sets to be the complements of algebraic sets.

Definition 1.1.3 (Affine, Variety, [31])**.** An *affine algebraic variety* (or affine variety) is an irreducible closed subset of $\mathbb{A}^n$. An open subset of an affine variety is a *quasi-affine variety.*

Definition 1.1.4 (Regular functions)**.** Let Y be a quasi-affine variety in $\mathbb{A}^n$. A function $f : Y \to k$ is regular at a point $P \in Y$, if there is an open neighborhood U with $P \in U \subseteq Y$, and polynomials $g, h \in A = \Bbbk[x_1, \ldots, x_n]$, such that h is nowhere zero on U, and $f = g/h$ on U. f is *regular* on Y if it is regular at every point of Y.

Definition 1.1.5 (Morphisms of affine varieties)**.** If X, Y are two affine varieties, a morphism, $\phi : X \to Y$, is a continuous map such that for every open set $V \subseteq Y$, and for every regular function $f : V \to \Bbbk$, the function $f \circ \phi : \phi^{-1}(V) \to k$ is regular.

Definition 1.1.6 (Algebraic Group)**.** An (*affine*) *algebraic group* G over a field $\Bbbk$ is an (affine) algebraic variety over $\Bbbk$ with the structure of a group on its set of points such that multiplication $\mu : G \to G$ and inversion $i : G \to G$ are morphisms of (affine) algebraic varieties.

Remark 1. (Affine) algebraic groups over $\Bbbk$ form a category. Its morphisms are morphisms of (affine) algebraic varieties which induce homomorphisms of the corresponding group structures.

Definition 1.1.7 (Solvable group)**.** A group G is called *solvable* if there exists a sequence of subgroups $1 = H_0 \trianglelefteq \cdots \trianglelefteq H_k$ of G such that for each $i,\ 0 \leq i \leq k-1$,

- H_i is a normal subgroup of H_{i+1} and
- the quotient group H_{i+1}/H_i is abelian.

Definition 1.1.8 (Reductive groups)**.** An affine algebraic group T is an *algebraic torus* if it is isomorphic to $G_m(\Bbbk)^{\times n}$ where $G_m(\Bbbk) = \mathrm{GL}_1(\Bbbk)$ is the one dimensional torus. The radical of an algebraic group is a maximal closed connected solvable normal subgroup. An affine algebraic group G is *reductive* if its radical is an algebraic torus.

Definition 1.1.9 (Mapping Class Group, Chapter 2, [18])**.** A surface S is a two dimensional manifold. Let S be the connected sum of $g \geq 0$ tori (genus g) with $b \geq 0$ disjoint open disks removed (b boundary components) and $n \geq 0$ points removed from the interior (n punctures). Suppose $\mathrm{Homeo}^+(S, \partial S)$ denote the group of orientation-preserving homeomorphisms of S that restrict to the identity on ∂S endowed with compact-open topology. Then the *mapping class group*, denoted by $\mathrm{Mod}(S)$ is the group

$$\mathrm{Mod}(S) = \pi_0(\mathrm{Homeo}^+(S, \partial S))$$

where $\pi_0(X)$ is the zeroth homotopy group of X.

Remark 2. For a surface of genus one with one puncture, $S(1,1)$,

$$\mathrm{Out}(F_2) \approx \mathrm{GL}(2,\mathbb{Z}) \approx \mathrm{Mod}^{\pm}(S_{1,1})$$

where $\mathrm{Mod}^{\pm}(S_{1,1})$ denote the extended mapping class group of $S_{(1,1)}$ (the group of isotopy classes of all homeomorphisms of $S_{(1,1)}$) and F_2 is the free group of rank two, [Theorem 8.1,

[18]]. Therefore, the mapping class group of the one-holed torus is the outer automorphism group $\mathrm{Out}(F_2)$.

Definition 1.1.10. For $q = p^k$ where p is a prime we define the following groups:

$$\begin{aligned} M_n(\mathbb{F}_q) &:= \{A \mid A = [a_{ij}]_{1\leq i,j\leq n} \text{ where } a_{ij} \in \mathbb{F}_q\} \\ \mathrm{GL}_n(\mathbb{F}_q) &:= \{A \in M_n(\mathbb{F}_q) \mid \det(A) \neq 0 \text{ in } \mathbb{F}_q\} \\ \mathrm{SL}_n(\mathbb{F}_q) &:= \{A \in M_n(\mathbb{F}_q) \mid \det(A) = 1\}. \end{aligned}$$

Group Action

Let G be a group acting on a set S. For $g \in G$ and $s \in S$, we use the notation $g \cdot s$ to denote the image of s under the action of g. Let W denote a subset of S.

Definition 1.1.11 (Orbit)**.** For $s \in S$, *the orbit of* s, $\mathrm{Orb}(s)$, is defined as the set $G \cdot s := \{g \cdot s \mid g \in G\}$.

Definition 1.1.12 (Stabilizer)**.** The *stabilizer of* s is the set $G_s := \{g \in G \mid g \cdot s = s\}$, the set of elements in G that leave s invariant under the action.

Definition 1.1.13 (Transitive Group Action)**.** The action of G on $W \subseteq S$ is called *transitive* if $G \cdot w = W$ for all $w \in W$, i.e, for any $v, w \in W$, there exists $g \in G$ such that $g \cdot v = w$. Equivalently, W contains a single orbit under the action.

Let G be a group acting on a vector space V.

Definition 1.1.14 (Semistable)**.** An orbit $G \cdot v \subset V - \{0\}$ is called *semistable* if its closure does not contain 0.

Definition 1.1.15 (Polystable)**.** An orbit is called *polystable* if it is closed.

1.1.2 Character Variety

Let G be a reductive affine algebraic group over $\mathbb{C}$, and Γ a finitely presented group. Then the G-character variety of Γ is a quotient space of the set of G-conjugation orbits of homomorphisms $\rho : \Gamma \to G$ where two orbits are equivalent if their closures intersect. To construct the character variety explicitly, let $\langle \gamma_1, ..., \gamma_r \mid R_i(\gamma_1, ..., \gamma_r) = 1, i = 1, ..., s\rangle$ be a presentation for Γ where R_i are words in $\gamma^{\pm 1}$. Then the set of homomorphisms, $\mathrm{Hom}(\Gamma, G)$, can be injectively mapped into G^r by the evaluation map defined as:

$$\begin{aligned} \phi : \mathrm{Hom}(\Gamma, G) &\longrightarrow G^r \\ \rho &\longmapsto (\rho(\gamma_1), ..., \rho(\gamma_r)). \end{aligned}$$

Injectivity of the map follows from the fact that the ρ's are homomorphisms. The evaluation map is a bijection when Γ has no relations [see Corollary 2.0.3 for the proof]. Since G is an affine algebraic group over the complex numbers, it is a smooth algebraic variety. The $R_i(\rho(\gamma_i))$'s are polynomial expressions in G, and G^r is a variety as the product of varieties. Therefore, $\mathrm{Hom}(\Gamma, G)$ inherits a subvariety structure from G^r. Note that G acts on $\mathrm{Hom}(\Gamma, G)$ by conjugation, which extends to an action on the coordinate ring $\mathbb{C}[\mathrm{Hom}(\Gamma, G)]$. We consider the invariant subring under this action denoted by $\mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$. This subring is finitely generated by Nagata's theorem [47] and the fact that G is reductive. Then *the G-character variety of* Γ is defined as the Geometric Invariant Theory(GIT) quotient [16] given by

$$\mathfrak{X}_\Gamma(G) := \mathrm{Spec}(\mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G).$$

We are considering the $\mathbb{C}$-points of the scheme with the subspace topology inherited from the Euclidean topology $\mathbb{C}^N$ for some N. This is not the same as the Zariski topology defined on the variety.

Since the GIT quotient identifies the orbits whose closure has a non-empty intersection, the quotient can be parameterized by the unique closed point in each equivalence class, called the *polystable representation* as defined in Definition 1.1.15. When G acts on $\mathrm{Hom}(\Gamma, G)$ by conjugation, $\rho \in \mathrm{Hom}(\Gamma, G)$ is polystable if the orbit $G \cdot \rho = \{g\rho g^{-1} \mid g \in G\}$ is Zariski closed in $\mathrm{Hom}(\Gamma, G)$.

If Γ is the fundamental group of a surface Σ, then $\mathfrak{X}_\Gamma(G)$ is called the G-character variety of Σ.

When $\Bbbk$ is a subfield of $\mathbb{C}$, we can consider the $\Bbbk$-points in $\mathfrak{X}_\Gamma(G)$. This gives some understanding of the topology of $\mathfrak{X}_\Gamma(G)$ as shown in [32].

1.1.3 E-polynomials

We now define the E-polynomials. The following discussion is taken from [11] and [42] . For an affine variety X, we consider the singular cohomology $H^*(X; \Bbbk)$ where $\Bbbk$ is a field of characteristic 0. See [14] and [15] for details. A pure Hodge structure of weight k consists of a finite dimensional complex vector space H with a real structure, and a decomposition

$$H = \bigoplus_{k=p+q} H^{p,q}$$

such that $H^{q,p} = \overline{H^{p,q}}$, where $\overline{H^{p,q}}$ denotes the complex conjugate on H. A Hodge structure of weight k gives rise to a descending *Hodge filtration* ,

$$F^p = \bigoplus_{s \geq p} H^{s,k-s}.$$

A complex variety X admits a mixed *mixed Hodge structure*, which consists of an increasing weight filtration,

$$0 = W_{-1} \subset W_0 \subset \cdots \subset W_{2j} = H^j(X; \mathbb{Q})$$

and a decreasing Hodge filtration

$$H^j(X; \mathbb{C}) = F^0 \supset \cdots \supset F^{m+1} = 0 \text{ such that for all } 0 \leq p \leq l,$$

$$\mathrm{Gr}_l^{W\otimes\mathbb{C}} := W_l \otimes \mathbb{C}/W_{l-1}\otimes\mathbb{C} = F^p(\mathrm{Gr}_l^{W\otimes\mathbb{C}}) \oplus \overline{F^{l-p+1}(\mathrm{Gr}_l^{W\otimes\mathbb{C}})}$$

where

$$F^p(\mathrm{Gr}_l^{W\otimes\mathbb{C}}) = (F_p \cap W_l \otimes \mathbb{C} + W_{l-1}\otimes\mathbb{C})/W_{l-1}\otimes\mathbb{C}.$$

Then we define the mixed Hodge number for $H_j(X;\mathbb{C})$ as follows:

$$\begin{aligned} h^{p,q;j}(X) &:= \dim_{\mathbb{C}} \mathrm{Gr}_p^F(\mathrm{Gr}_{p+q}^{W\otimes\mathbb{C}} H^j(X)) \\ &= \dim_{\mathbb{C}} F^p(\mathrm{Gr}_{p+q}^{W\otimes\mathbb{C}}/F^{p+1}(\mathrm{Gr}_{p+q}^{W\otimes\mathbb{C}}) \\ &= \dim_{\mathbb{C}} F^p \cap (W_{p+q}\otimes\mathbb{C}))/(F^{p+1}\cap W_{p+q}\otimes\mathbb{C} + W_{p+q-1}\otimes\mathbb{C}\cap F^p), \end{aligned}$$

using which we define the mixed Hodge polynomial

$$H(X;x,y,t) := \sum h^{p,q;j}(X)x^p y^q t^j.$$

Similarly, the same structure can be obtained by considering cohomology with compact support. This is denoted by $H_c(X;\Bbbk), h_c^{p,q;j}$ and $H_c(X;x,y;t)$. Then the *E-polynomial* is defined to be

$$E(X;x,y) := H_c(X;x,y,-1).$$

1.1.4 Outer Automorphism Group Action on Character Varieties

There is a natural action of $\mathrm{Out}(\Gamma)$, the outer automorphism group of Γ, on $\mathfrak{X}_\Gamma(G)$. Recall that $\mathrm{Out}(\Gamma) := \mathrm{Aut}(\Gamma)/\mathrm{Inn}(\Gamma)$ where $\mathrm{Inn}(\Gamma)$ is the group of inner automorphisms. To define the action, first note that the automorphism group of Γ, $\mathrm{Aut}(\Gamma)$, acts on $\mathrm{Hom}(\Gamma, G)$ as follows:

$$\begin{aligned} \mathrm{Aut}(\Gamma) &\circlearrowleft \mathrm{Hom}(\Gamma, G) \\ \tau\cdot\rho &= \rho\circ\tau^{-1} \end{aligned} \tag{1.1}$$

where $\tau \in \mathrm{Aut}(\Gamma)$ and $\rho \in \mathrm{Hom}(\Gamma, G)$. Since $\mathbb{C}[\mathrm{Hom}(\Gamma, G)]$ is a finitely generated $\mathbb{C}$-algebra, the coordinate ring admits a presentation $\mathbb{C}[x_1, ..., x_n]/I$ where $I \subset \mathbb{C}[x_1, ..., x_n]$ is an ideal. Owing to this presentation, the above defined action extends to an action on the coordinate ring as follows:

$$\sigma \cdot (f + I) = f(\sigma^{-1} \cdot \rho) + I$$

where $\sigma \in \mathrm{Aut}(\Gamma)$ and $f + I \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)]$. Note that $\mathrm{Aut}(\Gamma)$ sends I to I. Then $\mathrm{Inn}(\Gamma)$ acts trivially on the invariant ring. This leads to an action of $\mathrm{Out}(\Gamma)$ on the invariant subring. Finally, each automorphism of the coordinate ring induces a permutation on the set of maximal ideals. Consequently, the action on the coordinate ring extends to an action on the character variety, $\mathfrak{X}_\Gamma(G)$. See Lemma A.0.2 in Appendix for the proof.

1.1.5 Relative Character Variety

Let Σ be a surface with k boundary components say $b_1, ..., b_k$. Then the fundamental group, F, is free. We can stratify the character variety of Σ into relative character varieties by fixing the values of the boundary components. Recall that for defining a character variety we use representations of F to a complex affine algebraic group G. To fix the value of the boundary, we consider conjugacy classes of G and impose that the value of the boundary component lies inside a fixed conjugacy class. In other words, if G_i's are conjugacy classes of G, we are interested in the relative representation variety

$$\mathrm{Hom}_b(F, G) := \{\rho \in \mathrm{Hom}(F, G) \mid \rho(b_i) \in G_i \text{ where } 1 \leq i \leq k\}. \tag{1.2}$$

Then the relative character variety is the GIT quotient

$$\mathrm{Hom}_b(F, G) /\!/ G.$$

In the one-holed torus case with $\pi = F_2$, the free group on two generators, and $G = \mathrm{SL}(2, \mathbb{C})$, the character variety is isomorphic to the affine 3-space, as a consequence of Fricke-Vogt theorem through the following map, [26]:

$$\tau : [\rho] \longmapsto (x, y, z) := (\mathrm{tr}(\rho(X)), \mathrm{tr}(\rho(Y)), \mathrm{tr}(\rho(XY))).$$

Then the relative λ - character variety is obtained by fixing the boundary component which is the trace of the commutator,

$$\mathrm{tr}(XYX^{-1}Y^{-1}) = x^2 + y^2 + z^2 - xyz - 2 = \lambda.$$

See Appendix A for a proof.

1.2 Background

The measure-theoretic dynamics of this action has been explored in specific cases for particular groups and varieties. If G is compact and connected, Goldman [25] and Pickerell-Xia [51] showed that when π is a closed surface group of genus, $g \geq 2$, there is a natural measure class such that the action is ergodic. For complex groups, there have been studies that showed that this action is not ergodic. For a free group of rank 3 or greater, the action of $\mathrm{Out}(F_r)$ on the G-character variety of F_r is ergodic with respect to an invariant measure [27] and [23]. When considering Γ to be the fundamental group of a non-orientable surface and $G = \mathrm{SU}(2)$, there exists a measure class with respect to which the action is ergodic [50]. In [10], Burelle and Lawton proved that for a compact connected Lie group G, $\mathrm{Out}(\Gamma)$-action is ergodic on the connected component of identity of the character variety if Γ is nilpotent and $\mathrm{Aut}(\Gamma)$ has a hyperbolic element.

We are interested in studying the analog of these dynamical systems in an arithmetic setting. When G happens to be a complex reductive group defined over $\mathbb{Z}$, we can look at the $\mathbb{Z}/p\mathbb{Z}$ points. Then we retain the action as defined above, but there is no natural geometric invariant measure necessarily defined on the variety anymore. However, it is still interesting to look at how close the action is to being transitive. In this setting, a comparable problem has been explored by Bourgain, Gamburd and Sarnak in [7], where they studied the $\mathbb{Z}/p\mathbb{Z}$ points of the Markoff equation given by

$$x_1^2 + x_2^2 + x_3^2 - 3x_1x_2x_3 = 0$$

denoted as $\mathbb{X}(\mathbb{Z}/p\mathbb{Z})$, which is related to the SL_2-character variety of the one holed torus. They were interested in the action of the group Γ of affine integral morphisms of the affine 3-space generated by the permutations of the coordinates and Vieta involutions. Their results yield strong approximation property for the Markoff equation for most primes, comparable to asymptotic transitivity.

In [13], Chen shows that for all but finitely many primes p, the group of Markoff automorphisms acts transitively on the nonzero $\mathbb{F}_p$-points of the Markoff equation. This result proves that the action is asymptotically transitive on this variety. Goldman's ergodicity theorem for the compact case extends to relative character varieties when the genus, $g \geq 2$. The results from [13] give reasons to believe that the action on the relative character variety for a one-holed torus when G is $\mathrm{SL}_2(\mathbb{F}_q)$ is also asymptotically transitive.

Cerbu, Gunther, Magee, and Peilen considered a related problem in [12]. A similar problem has also been the subject of a project at Mason Experimental Geometry Lab (MEGL) at GMU and have made some progress in collecting experimental data for smaller values of primes [2].

If we consider the case where the character variety is not relative (that is, without fixing the boundary values) and where G is a compact Lie group, then for a free group of rank $r \geq 3$, the action is ergodic [23]. However, if G is not compact, then the free group action on the character variety is not ergodic [46]. In [28] and [52], the action is shown to be ergodic for certain relative character varieties.

In [24], Gilman shows that the set of epimorphisms forms a transitive orbit under the action of $\mathrm{Out}(\Gamma)$ on $\mathrm{Hom}(\Gamma, G)$ when Γ is free [Theorem 2] and G is a finite group with sufficiently large number of generators. In the second chapter, we generalize this result to groups of free-type. We say that a group is of free-type if its automorphism group includes elementary operations such as permutations, inversion of letters and left multiplication.

In the third chapter, we explore the asymptotic transitivity of the outer automorphism group action of $\mathbb{Z}^r$ on $\mathrm{SL}_n(\mathbb{F}_q)$-character varieties of $\mathbb{Z}^r$ for $n = 2, 3$. Along the way, we compute the E-polynomial, also known as the Hodge-Deligne polynomial or Serre polynomial, of these character varieties. Hausel and Rodriguez-Villegas introduced arithmetic methods inspired by the Weil conjectures to compute the E-polynomials of G-character varieties when $G = \mathrm{GL}_n(\mathbb{C}), \mathrm{SL}_n(\mathbb{C})$ and $\mathrm{PGL}_n(\mathbb{C})$. In [32], they use a theorem of N. Katz [Appendix, [32]] that allows the calculation of E-polynomials by counting the finite field points of these varieties and obtain the E-polynomials for $G = \mathrm{GL}_n(\mathbb{C})$ as a generating function. In [45], Mereb use similar methods to calculate the E-polynomial when $G = \mathrm{SL}_2(\mathbb{C})$ and a generating function for the $\mathrm{SL}_n(\mathbb{C})$ case. The Hodge polynomials of $\mathrm{SL}_2(\mathbb{C})$ character varieties for curves of small genus were computed in [42] by stratifying the space of representations and using fibrations. The E-polynomial of $\mathfrak{X}_{\mathbb{Z}^r}(\mathrm{SL}_2(\mathbb{C}))$ has been calculated in [11] using arithmetic methods. We provide a shorter version of the proof. In [40], the E-polynomials of $\mathfrak{X}_{\mathbb{Z}^r}(\mathrm{SL}_n(\mathbb{C}))$ are calculated for $n = 2, 3$ using complex geometry methods. We give an arithmetic proof for the case when $n = 3$ using a method that counts the number of possible characteristic polynomials for matrices over finite fields. Additionally, this method gives a count of orbits in each stratum when $n = 2, 3$. In [20], Florentino, Nozad and Zamora gave explicit expressions for the E-polynomial of the GL_n-character varieties combining combinatorics of partitions with arithmetic methods. The authors extend the stratification by polystable type to SL_n-character varieties in [21] and compute the E-polynomial of each stratum for the free abelian case.

Chapter 2: Transitivity

We first prove an introductory result that concerns the set of representations from a finitely presented group Γ to any group G, which will be useful in the subsequent discussion. We show that the set is in bijective correspondence with the set of tuples that satisfy the relations of the group, Γ. First, we state the following well known fact from group theory.

Theorem 2.0.1. *Let $G = \langle g_i \mid R_i \rangle$ and H be finitely generated groups. If f is a function that maps g_i to an element of H, then f extends to a homomorphism $F : G \to H$ if and only if $f(R_i) = e_H$, the identity element in H, for all i.*

This theorem ensures that any map from a generating set of Γ to G that satisfies the relations of Γ can be uniquely extended to a homomorphism from Γ to G.

Lemma 2.0.2. *Let Γ be a finitely presented group with r generators and G be a group. Suppose $\langle \gamma_1, \dots, \gamma_r \mid R_i,\ 1 \le i \le s \rangle$ is a given presentation of Γ. Then $\mathrm{Hom}(\Gamma, G)$ is in bijective correspondence with the set of r-tuples in G that satisfies the relations of Γ,*

$$\mathcal{S}_\Gamma(G, r) := \{(A_1, \dots, A_r) \in G^r \mid R_i((A_1, \dots, A_r)) = 1\}.$$

Proof. We define a map

$$\begin{aligned} \Psi : \mathrm{Hom}(\Gamma, G) &\longrightarrow \mathcal{S}_\Gamma(G, r) \\ \Psi(\rho) &= (\rho(\gamma_1), \dots, \rho(\gamma_r)). \end{aligned}$$

Since ρ is a homomorphism, by definition, $R_i((\rho(\gamma_1), \dots, \rho(\gamma_r))) = 1$. Therefore, the map is well defined. Suppose $\Psi(\rho_1) = \Psi(\rho_2)$ for $\rho_1, \rho_2 \in \mathrm{Hom}(\Gamma, G)$. Then $(\rho_1(\gamma_1), \dots, \rho_1(\gamma_r)) =$

$(\rho_2(\gamma_1), \ldots, \rho_2(\gamma_r))$. Since homomorphisms are uniquely determined by the images of generators, it follows that the map is injective. Let $A = (A_1, \ldots, A_r) \in G^r$ such that $R_i(A_1, \ldots, A_r) = 1$. Then, define a map $\phi_A : \Gamma \to \Gamma$ such that $\phi(\gamma_i) = A_i$. Since $R_i(A_1, \ldots, A_r) = 1$, this mapping can be uniquely extended to a homomorphism from Γ to G. Thus, Ψ is surjective and this concludes the proof. □

Corollary 2.0.3. *If Γ is free,* $\mathrm{Hom}(\Gamma, G)$ *is in bijection with the set G^r.*

2.1 Dynamics of $\mathrm{Out}(\mathbb{Z}^r)$-action on $\mathrm{SL}_2(\mathbb{F}_q)$-character varieties of $\mathbb{Z}^r$

Let Γ be the free abelian group generated by the set $\langle \gamma_1, \ldots, \gamma_r \rangle$. Then Γ is isomorphic to the Cartesian product, $\mathbb{Z}^r$. Throughout this section, without loss of generality we assume that $\Gamma = \mathbb{Z}^r$. In this section, we look at the dynamics of the action of $\mathrm{Out}(\Gamma)$ on the abelian $\mathrm{SL}_2(\mathbb{F}_q)$-character variety of Γ. We first consider the action of $\mathrm{Out}(\mathbb{Z}^r)$ on the set of representations $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_2(\mathbb{F}_q))$.

Corollary 2.1.1. *The set* $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_2(\mathbb{F}_q))$ *is in bijective correspondence with the pairwise commuting r-tuples,* $\{(A_1, \ldots, A_r) \in \mathrm{SL}_2(\mathbb{F}_q)^r \mid A_iA_j = A_jA_i \ 1 \leq i, j \leq r\}$.

Proof. Observe that $\mathbb{Z}^r = \{(x_1, \ldots, x_r) \mid x_ix_j = x_jx_i, 1 \leq i, j \leq r\}$. Then the result follows by Lemma 2.0.2. □

2.1.1 Outer Automorphism Group of $\mathbb{Z}^r$

Since $\mathbb{Z}^r$ is abelian, the group of inner automorphisms is trivial. Therefore, the outer automorphism group, $\mathrm{Out}(\mathbb{Z}^r) \cong \mathrm{Aut}(\mathbb{Z}^r)$. We first compute $\mathrm{Out}(\mathbb{Z}^r)$, a known result.

Lemma 2.1.2. *The outer automorphism group of $\mathbb{Z}^r$,* $\mathrm{Out}(\mathbb{Z}^r)$*, is* $\mathrm{GL}_r(\mathbb{Z})$.

Proof. Let $x = (x_1, x_2, \ldots, x_r) \in \mathbb{Z}^r$. Define z_i to be the column vector with 1 as the single non-zero entry in the i^{th} row. Then any $x \in \mathbb{Z}^r$ can be written as a linear combination of the z_i's as follows.

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} = x_1 \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + x_2 \cdot \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + x_r \cdot \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Therefore, any endomorphism $\phi : \mathbb{Z}^r \longmapsto \mathbb{Z}^r$ is completely determined by the image of z_i's, $\phi(z_i)$ for $i = 1, \ldots, r$. Let $\phi(z_i) = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ri} \end{pmatrix}$. Then, ϕ can be regarded as multiplication by the matrix, $A_\phi := \begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & \cdots & \vdots \\ a_{r1} & \cdots & a_{rr} \end{pmatrix}$. If ϕ is an automorphism, then there exists an inverse automorphism ϕ^{-1} of $\mathbb{Z}^r$. Now consider the matrix $A_{\phi^{-1}}$ that corresponds to ϕ^{-1}. Since $\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = 1$, it follows that $A_\phi A_{\phi^{-1}} = A_\phi A_\phi^{-1} = I$, the identity matrix. Therefore, A_ϕ is invertible i.e., $A_\phi \in \mathrm{GL}_r(\mathbb{Z})$.

Now define the following map:

$$\begin{aligned} \Psi : \mathrm{Aut}(\mathbb{Z}^r) &\longrightarrow \mathrm{GL}_r(\mathbb{Z}) \\ \Psi(\phi) &= A_\phi. \end{aligned}$$

The map Ψ is well defined by the above argument. By definition, $\phi(z_i)$ uniquely determines ϕ. Therefore, if $\Psi(\phi_1) = \Psi(\phi_2)$ then $A_{\phi_1} = A_{\phi_2}$. Consequently, $\phi_1 = \phi_2$, by the construction of A_{ϕ_i}. Thus, Ψ is injective.

To prove surjectivity, suppose $A \in \mathrm{GL}_r(\mathbb{Z})$. Define a map $\phi_A : \mathbb{Z}^r \mapsto \mathbb{Z}^r$ such that $\phi(z_i) = a_i$, the i^{th} column of A. This map can be uniquely extended to an endomorphism of $\mathbb{Z}^r$. Since A is invertible, $\phi_A \circ \phi_{A^{-1}} = \phi_{A^{-1}} \circ \phi_A$ is the identity map. Therefore ϕ is an automorphism and Ψ is surjective. This concludes the proof. $\square$

Remark 3. If $A \in \mathrm{GL}_r(\mathbb{Z})$, then $\det(A)$ is invertible in $\mathbb{Z}$. Therefore, $\det(A) = \pm 1$.

2.1.2 Action of $\mathrm{Out}(\mathbb{Z}^r)$ on the Character Variety

The automorphism group of $\mathbb{Z}^r$ acts on the set of homomorphisms $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_2(\mathbb{F}_q))$. Let $\gamma \in \mathrm{Aut}(\mathbb{Z}^r)$ and $A = \begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & a_{rr} \end{pmatrix} \in \mathrm{GL}_r(\mathbb{Z})$ corresponds to the automorphism, γ^{-1} of $\mathbb{Z}^r$ (as defined in the proof of Lemma 2.1.2). For $(x_1, \ldots, x_r) \in \mathbb{Z}^r$ and $\rho \in \mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_2(\mathbb{F}_q))$, let $\rho(x_i) = Y_i \in \mathrm{SL}_2(\mathbb{F}_q)$. Then the action of Γ on ρ is defined as follows:

$$
\begin{aligned}
\gamma \cdot \rho &= \rho(\gamma^{-1}(x_1, \ldots, x_r)) \\
&= \rho\left(\begin{pmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \cdots & a_{rr} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix} \right) \\
&= \rho\left(\begin{pmatrix} a_{11}x_1 + \cdots + a_{1r}x_r \\ \vdots \\ a_{r1}x_1 + \cdots + a_{rr}x_r \end{pmatrix} \right)
\end{aligned} \tag{2.1}
$$

$$= \begin{pmatrix} a_{11}\rho(x_1) + \cdots + a_{1r}\rho(x_r) \\ \vdots \\ a_{r1}\rho(x_1) + \cdots + a_{rr}\rho(x_r) \end{pmatrix}$$

$$= \begin{pmatrix} Y_1^{a_{11}} \cdots Y_r^{a_{1r}} \\ \vdots \\ Y_1^{a_{r1}} \cdots Y_r^{a_{rr}} \end{pmatrix}.$$

Example 2.1.1 ($q = 2$)**.** In this example, we explore in detail and exhaustively compute the orbits of the action. The goal is to understand the action in detail for a small prime before proceeding to the general case. The calculations in this example, including the visualization, are done using *Mathematica*, [34].

The first step is to compute the group, $\mathrm{SL}_2(\mathbb{F}_2)$. It is a straightforward calculation to show that the set $\mathrm{SL}_2(\mathbb{F}_2) = \{I, X_1, X_2, X_3, X_4, X_5\}$ where the matrices X_i's are defined as follows:

$$X_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; X_2 := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \; X_3 := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \; X_4 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \; X_5 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and I denotes the identity matrix of rank 2. We now compute the group structure. Simple calculations give the Cayley Table of $\mathrm{SL}_2(\mathbb{F}_2)$.

Table 2.1: Cayley table of $\mathrm{SL}_2(\mathbb{F}_2)$

$\times$	I	X_1	X_2	X_3	X_4	X_5
I	I	X_1	X_2	X_3	X_4	X_5
X_1	X_1	I	X_5	X_4	X_3	X_2
X_2	X_2	X_4	X_3	I	X_5	X_1
X_3	X_3	X_5	I	X_2	X_1	X_4
X_4	X_4	X_2	X_1	X_5	I	X_3
X_5	X_5	X_3	X_4	X_1	X_2	I

By comparing the Cayley tables, it is clear that $\mathrm{SL}_2(\mathbb{F}_2)$ is isomorphic to the symmetric group on three letters, S_3. In particular, $\mathrm{SL}_2(\mathbb{F}_2)$ satisfies the following relations.

$$X_1^2 = X_4^2 = X_5^2 = I = X_2^3 = X_3^3$$

$$X_2X_1X_2^{-2}X_1 = X_2X_1X_2X_1 = I$$

Remark 4. Using the above relations, we can deduce the following presentation for $\mathrm{SL}_2(\mathbb{F}_2)$:

$$\mathrm{SL}_2(\mathbb{F}_2) = \langle X_1, X_2 \mid X_1^2 = X_2^3 = I, X_2X_1X_2^{-2}X_1 = I\rangle.$$

Lemma 2.1.3. *Let* $(X_{i_1}, \ldots, X_{i_r}) \in \mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_2(\mathbb{F}_2))$. *Then* $(X_{i_1}, \ldots, X_{i_r})$ *are of the following three types:*

1. $(X_{i_1}, \ldots, X_{i_r})$ *where* $X_{i_j} \in \{X_i, I\}$ *for all* $1 \leq j \leq r$ *and for a fixed* i *such that* $1 \leq i \leq 5$ *.*

2. $(X_{i_1}, \ldots, X_{i_r})$ *such that* $X_{i_k} = X_j$ *for a fixed* j *with* $1 \leq j \leq 5$*.*

3. $(X_{i_1}, \ldots, X_{i_r})$ *where* $X_{i_j} \in \{I, X_2, X_3\}$ *for all* $1 \leq j \leq r$*.*

Proof. Let $\rho \in \mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_2(\mathbb{F}_q))$. Then, by Corollary 2.1.1, ρ can be represented by a commuting r-tuple in $\mathrm{SL}_2(\mathbb{F}_2)$. Therefore, it suffices to classify the types of pairwise commuting tuples in $\mathrm{SL}_2(\mathbb{F}_2)$. By the relations from Table 2.1, the only pairs of matrices that commute are the following:

1. $\{(X_i, X_i) \mid 1 \leq i \leq 5\} \cup \{(I, I)\}$

2. $\{(I, X_i) \mid 1 \leq i \leq 5\}$ and $\{(X_i, I) \mid 1 \leq i \leq 5\}$

3. $\{(X_2, X_3), (X_3, X_2)\}$

Let $(Y_1, \dots, Y_r) \in \mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_2(\mathbb{F}_2))$ and suppose $Y_j = X_i$ for $1 \leq j \leq 5$. Then (Y_j, Y_k) has to be one of the pairs of tuples above. This proves the result. $\square$

Visualization of the orbits

We use the following set of generators of $\mathrm{GL}_2(\mathbb{Z}) \cong \mathrm{Aut}(\mathbb{Z}^2)$ to look at the action of $\mathrm{Aut}(\mathbb{Z}^2)$ on $\mathrm{Hom}(\mathbb{Z}^2, \mathrm{SL}_2(\mathbb{F}_2))$ and $\mathrm{Hom}(\mathbb{Z}^2, \mathrm{SL}_2(\mathbb{F}_3))$ as defined in Section 1.1.4.

$$S = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

A visual representation of the orbits for the case when $r = 2$ is given in Figure 2.1. All the visualizations in this section are generated using the *Mathematica* software.
We now prove that these are all the orbits under the action of the full group of $\mathrm{Aut}(\mathbb{Z}^2)$ on $\mathrm{Hom}(\mathbb{Z}^2, \mathrm{SL}_2(\mathbb{F}_2))$.

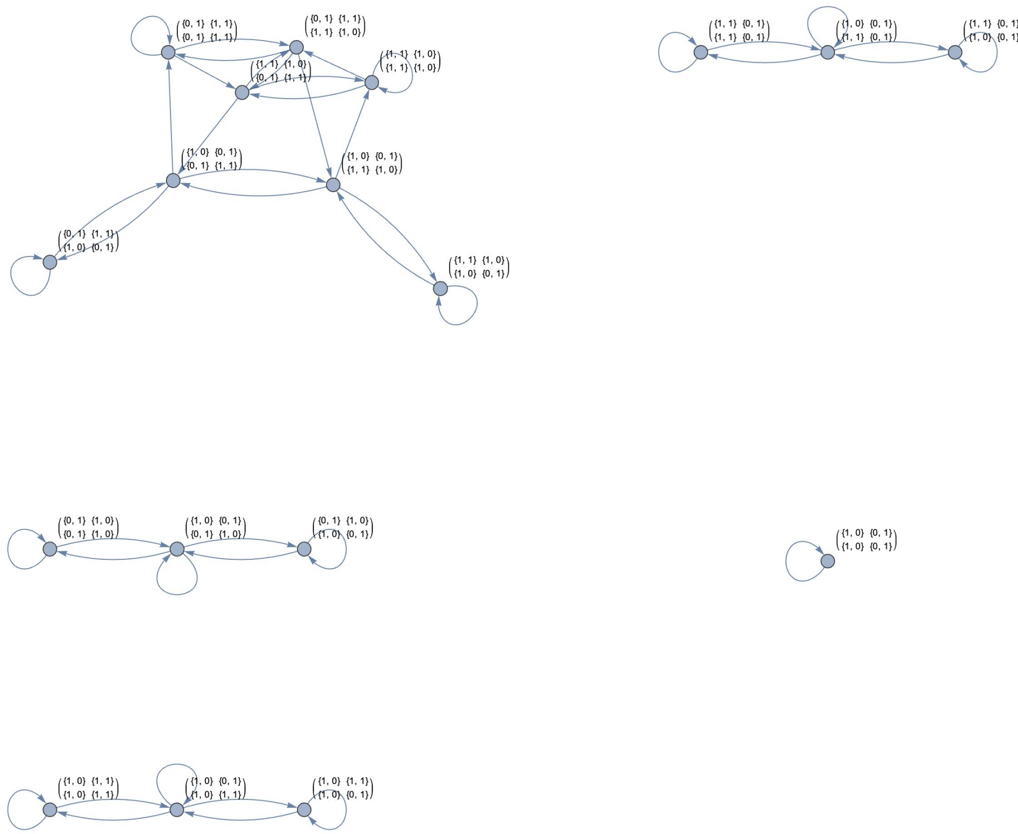

Figure 2.1: Orbits under the action of generators of $\mathrm{Aut}(\mathbb{Z}^2)$ on $\mathrm{Hom}(\mathbb{Z}^2, \mathrm{SL}_2(\mathbb{F}_2))$

Lemma 2.1.4. *There are exactly five orbits under the action of* $\mathrm{Aut}(\mathbb{Z}^2)$ *on* $\mathrm{Hom}(\mathbb{Z}^2, \mathrm{SL}_2(\mathbb{F}_2))$.

1. $\{(I, I)\}$
2. $\{(X_1, X_1), (X_1, I), (I, X_1)\}$
3. $\{(X_4, X_4), (X_4, I), (I, X_4)\}$
4. $\{(X_5, X_5), (X_5, I), (I, X_5)\}$
5. $\{(X_i, X_j) \mid X_i, X_j \in \{I, X_2, X_3\}\} \setminus \{(I, I)\}$

Proof. By Figure 2.1, it is clear that there are at most five orbits. We will show that it is not possible to go from one orbit to another through the action of an element in $\mathrm{Aut}(\mathbb{Z}^2)$. Recall that, when $r = 2$, by Corollary 2.1.1, $\mathrm{Hom}(\mathbb{Z}^2, \mathrm{SL}_2(\mathbb{F}_q))$ is in bijective correspondence with the set

$$\mathcal{S}_{\mathbb{Z}^2}(\mathrm{SL}_2(\mathbb{F}_q)) := \{(A, B) \in \mathrm{SL}_2(\mathbb{F}_q) \mid AB = BA\}.$$

Suppose $\gamma^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ so that $\gamma = \pm \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Then $\gamma^{-1}(x, y) = (ax + by, cx + dy)$.

Let $\rho(x) = A$ and $\rho(y) = B$. Then the action of γ on ρ as defined in Equation 2.1 reduces to the following:

$$\rho(\gamma^{-1}(x, y)) = \rho\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\right) = (A^a B^b, A^c B^d). \tag{2.2}$$

Therefore, if $(\rho(x), \rho(y))$ is denoted by (A, B), then:

$$\begin{aligned} \mathrm{Orb}(A, B) &= \left\{ (A^a B^b, A^c B^d) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \right\} \\ &= \left\{ (A^a B^b, A^c B^d) \mid ad - bc = \pm 1 \right\}. \end{aligned}$$

Clearly, $\mathrm{Orb}((I, I)) = \{(I, I)\}$ since $I^k = I$ for all values of k. For $i \in \{1, 4, 5\}$, consider the element (X_i, X_i). Then $(X_i^a X_i^b, X_i^c X_i^d) = (X_i^{a+b}, X_i^{c+d})$. Since $X_i^2 = I$, it follows that $\mathrm{Orb}((X_i, X_i))$ can only have tuples with entries X_i or I. This proves the first four parts of the lemma.

The visual representation shows that the rest of the elements form an orbit. Another way to prove this is as follows. We fix $(X_2, I) \in \mathcal{S}_{\mathbb{Z}^2}(\mathrm{SL}_2(\mathbb{F}_2))$ which is not an element in any of the other orbits, as a reference point. Let (X_i, X_j) be such that $X_i, X_j \in \{I, X_2, X_3\}$ and not equal to (I, I). By Equation (2.2), $(X_i, X_j) \in \mathrm{Orb}((X_2, I))$ iff there exists $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in$ $\mathrm{GL}_2(\mathbb{Z}^2)$ such that $(X_2^a, X_2^c) = (X_i, X_j)$. Since $X_3 = X_2^2 = X^{-1}$ and $I = X_2^3 = X^0$, let $a, c \in \{-1, 0, 1, 2, 3\}$. For fixed values of a and c, we want to check if there exists an integer solution to the equation

$$ad - bc = 1.$$

To compute this, we use the following well-known result from number theory, the proof of which uses Bézout's identity. See [1] for a proof.

Lemma 2.1.5. *Let $ax + by = c$ be a linear Diophantine equation in two variables, x and y. Then the equation has a solution in $\mathbb{Z}^2$ if and only if $\gcd(a, b)$ divides c.*

Using this result, to get a desired pair of elements (X_i, X_j), it suffices to find a pair a, c that are co-prime such that $X_2^a = X_i$ and $X_2^c = X_j$. Notice that for any combination of pairs, $a, c \in \{1, 2, 3\}$, $\gcd(a, c) = 1$ except when $a, c = 2$ and $a, c = 3$. Since $a = 2$ and $c = 2$ is the same as choosing $a = 2$ and $c = -1$ which are coprime integers, it follows that this pair is admissible.

When $a = c = 3$, the equation $3d - 3b = 1$ has no integer solution. Therefore the pair $(3, 3)$ is not admissible and hence $(X^3, X^3) = (I, I)$ is not in the orbit. $\square$

Additionally, we looked at the action of generators of $\mathrm{Aut}(\mathbb{Z}^2)$ on $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_2(\mathbb{F}_3))$. The orbits thus obtained are shown in Figure 2.2. The figure indicates that the action might not be transitive. In the next section, we prove that this is indeed the case for a more general class of groups Γ and G.

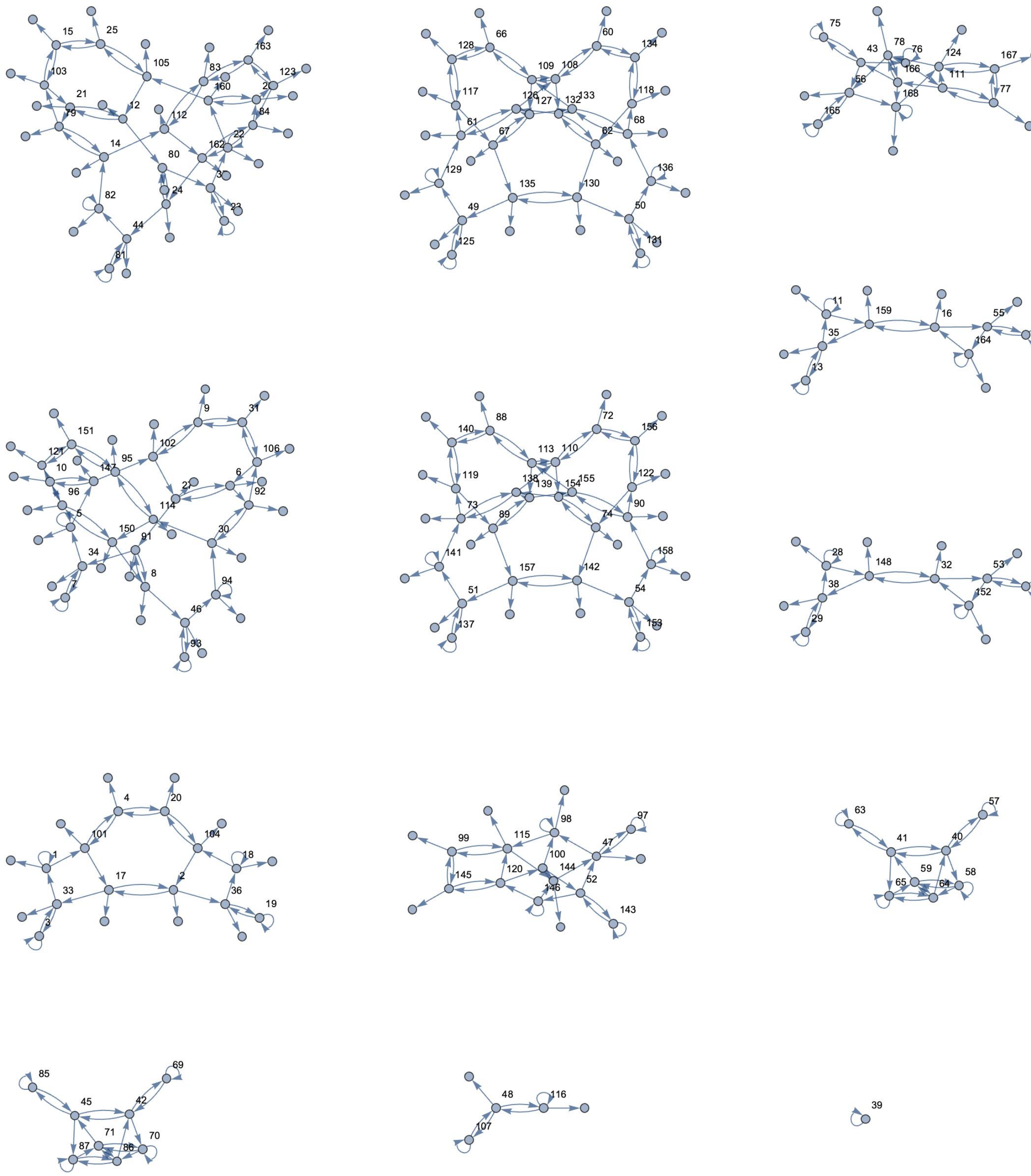

Figure 2.2: Orbits under the action of generators of $\mathrm{Aut}(\mathbb{Z}^2)$ on $\mathrm{Hom}(\mathbb{Z}^2, \mathrm{SL}_2(\mathbb{F}_3))$

2.2 Non-Transitivity Theorem

2.2.1 Action of $\mathrm{Aut}(\Gamma)$ on $\mathrm{Hom}(\Gamma, G)$

Observations from the previous section motivated us to generalize these results to outer automorphism group actions on $\mathrm{Hom}(\Gamma, G)$ for G an affine algebraic group. We first define the action for the general case of Γ and G.

Lemma 2.2.1. *Let $\Gamma = \langle \gamma_1, ..., \gamma_r \mid R_i,\ i = 1, \ldots, s\rangle$ be a finitely presented group and G a group. Then $\mathrm{Aut}(\Gamma)$ acts on $\mathrm{Hom}(\Gamma, G)$ as follows:*

$$\alpha \cdot \rho = \rho \circ \alpha^{-1},\ \textit{for } \alpha \in \mathrm{Aut}(\Gamma) \textit{ and } \rho \in \mathrm{Hom}(\Gamma, G).$$

Proof. Suppose $\rho \in \mathrm{Hom}(\Gamma, G)$. Let $\alpha \in \mathrm{Aut}(\Gamma)$. Then, $\alpha \cdot \rho = \rho(\sigma^{-1}(\gamma_1, \ldots, \gamma_r))$. The action is well defined since $\alpha^{-1} \in \mathrm{Aut}(\Gamma)$ and $\rho \circ \alpha^{-1} \in \mathrm{Hom}(\Gamma, G)$. Clearly, $e \cdot \rho = \rho \circ e^{-1} = \rho \circ e = \rho$ where e is the identity element of $\mathrm{Aut}(\Gamma)$. Finally, note that

$$\begin{aligned}
(\sigma_1 \circ \sigma_2) \cdot \rho &= \rho \circ (\sigma_1 \circ \sigma_2)^{-1} = \rho \circ (\sigma_2^{-1} \circ \sigma_1^{-1}) \\
&= (\rho \circ \sigma_2^{-1}) \circ \sigma_1^{-1} = \sigma_1 \cdot (\rho \circ \sigma_2^{-1}) \\
&= \sigma_1 \cdot (\sigma_2 \cdot \rho).
\end{aligned}$$

This completes the proof. $\square$

Lemma 2.2.2 (Subgroup Lemma)**.** *Let $\Gamma = \langle \gamma_1, ..., \gamma_r \mid R_i,\ i = 1, \ldots, s\rangle$ be a finitely presented group and G a group. If H is a subgroup of G and $\rho \in \mathrm{Hom}(\Gamma, G)$ is such that $(\rho(\gamma_1), \ldots, \rho(\gamma_r)) \in H^r$, then $\mathrm{Orb}(\rho) \subseteq H^r$.*

Proof. Let $(\rho(\gamma_1), \ldots, \rho(\gamma_r) = (H_1, \ldots, H_r) \in H^r$ and $\alpha \in \mathrm{Aut}(\Gamma)$. Suppose $\alpha^{-1}(\gamma_i) = w_i \in \Gamma$ and $w_i = \gamma_{i_1}^{a_{i_1}} \cdots \gamma_{i_s}^{a_{i_s}}$. Using this expression of w_i, we compute the following:

$$\begin{aligned}\rho(w_i) &= \rho(\gamma_{i_1}^{a_{i_1}} \cdots \gamma_{i_s}^{a_{i_s}}) \\ &= \rho(\gamma_{i_1}^{a_{i_1}}) \cdots \rho(\gamma_{i_s}^{a_{i_s}}) \\ &= \rho(\gamma_{i_1})^{a_{i_1}} \cdots \rho(\gamma_{i_s})^{a_{i_s}} \\ &= H_{i_1}^{a_{i_1}} \cdots H_{i_s}^{a_{i_s}}.\end{aligned}$$

Therefore,

$$\alpha \cdot \rho = \rho(\alpha^{-1}(\gamma_1, \ldots, \gamma_r)) = (H_{1_1}^{a_{1_1}} \cdots H_{1_s}^{a_{1_s}}, \ldots, H_{i_1}^{a_{i_1}} \cdots H_{i_s}^{a_{i_s}}, \ldots, H_{r_1}^{a_{r_1}} \cdots H_{r_s}^{a_{r_s}}).$$

Since $H_{i_j} \in H$ and H is a subgroup, $\prod_{j=1}^{s} H_{i_j}^{a_{i_j}}$ is also in H. Consequently, $\alpha \cdot \rho \in H^r$. □

Corollary 2.2.3. *Let Γ and G be defined as in the lemma. Let $\rho_I \in \mathrm{Hom}(\Gamma, G)$ denote the trivial homomorphism defined by $\rho(\gamma_i) = I$ for all i, where I is the identity element of G. Then $\mathrm{Orb}(\rho_I) = \{\rho_I\}$ under the $\mathrm{Aut}(\Gamma)$ action.*

Proof. Clearly, $\{I\}$ is the trivial subgroup of G. Then the result follows from the above lemma. □

Therefore, the action is never transitive on the set $\mathrm{Hom}(\Gamma, G)$ if $G \neq \{I\}$. We are interested in checking if the action is transitive on the non-trivial points in the set of homomorphisms,

$$\mathrm{Hom}(\Gamma, G)^* := \mathrm{Hom}(\Gamma, G) \setminus \{\rho_I\}.$$

Similarly, we use $\mathfrak{X}_\Gamma(G)^*$ to denote the non-trivial points in the character variety.

Theorem 2.2.4 (Non-Transitivity Theorem)**.** *Let $\Gamma = \langle \gamma_1, ..., \gamma_r \mid R_i,\ i = 1, \ldots, s\rangle$ be a finitely presented group and G a group. Suppose there exists a subgroup, $H \subset G$ and homomorphisms, $\rho, \mu \in \mathrm{Hom}(\Gamma, G)$ such that $\rho(\gamma_i) \in H$ for all i and $\mu(\gamma_j) \in G \setminus H$ for* *some j. Then the action of* $\mathrm{Aut}(\Gamma)$ *on* $\mathrm{Hom}(\Gamma, G)^*$ *is not transitive. Moreover if* ρ *and* μ *are polystable, then the action of* $\mathrm{Out}(\Gamma)$ *on the character variety,* $\mathfrak{X}_\Gamma(G)^*$ *is not transitive whenever the character variety is defined.*

Proof. Suppose there exists $H \subset G$ and $\rho, \mu \in \mathrm{Hom}(\Gamma, G)$ as mentioned in the statement of the theorem. Then, $\rho(\gamma_i) \in H$ for all $i \in \{1, \dots, r\}$. Therefore, by Lemma 2.2.2, $\mathrm{Orb}(\rho) \subseteq H^r$. This implies that $\mu \notin \mathrm{Orb}(\rho)$. Hence, the action is not transitive on $\mathrm{Hom}(\Gamma, G)$.

Additionally, suppose ρ and μ are polystable. By definition of polystability, the orbits of ρ and μ are closed. Consequently, ρ and μ correspond to distinct elements in the character variety, $\mathfrak{X}_\Gamma(G)$. Since $\mathrm{Orb}(\rho) \neq \mathrm{Orb}(\mu)$, it follows that the action is not transitive on $\mathfrak{X}_\Gamma(G)$. □

2.2.2 An Application: $\Gamma = F_r$

Now, we look at two applications of the above theorem for the special case when Γ is free.

Necessary condition for transitivity on representation variety of free groups

Corollary 2.2.5. *Let* Γ *be a free group of rank* $r \geq 1$ *and* G *be a non-trivial group. If the* $\mathrm{Aut}(\Gamma)$*-action on the representation variety* $\mathrm{Hom}(\Gamma, G)^*$ *is transitive if* G *is a cyclic group of prime order. The converse is true only if* $r > 1$*.*

Proof. When Γ is free, $\mathrm{Hom}(\Gamma, G) \cong G^r$ by Corollary 2.0.3. First, we show that G has no proper non-trivial subgroup if and only if $G \cong \mathbb{Z}_p$ or $G = \{0\}$. Clearly, $\mathbb{Z}_p$ has no proper non-trivial subgroups. Conversely, if G has no proper subgroup, then for all $a \in G$ that is not equal to identity, $\langle a \rangle = G$. This implies G is cyclic. If G is infinite, then $G \cong \mathbb{Z}$, but $\mathbb{Z}$ has non-trivial proper subgroups, $n\mathbb{Z}$. Therefore, $\mathbb{Z}$ is finite. Let $G \neq \{e\}$. Now suppose $|G|$ has two prime divisors, say p and q. If $p \neq q$, then by Cauchy's theorem, G has two proper subgroups, H_p and H_q of order p and q respectively, which is a contradiction. Similarly, if $q = p$, then G has a proper subgroup of order of order p. Therefore, $|G|$ has a single prime divisor, p. Hence, $|G| = p$.

Suppose G is not cyclic of prime order. Then there exists a proper non-trivial subgroup, $H \subset G$. Since H is non-trivial, there exists a non-trivial element $(H_1, \ldots, H_r)$ in H^r. Similarly, $G^r \setminus H^r$ is non-empty because $H \neq G$. Therefore, there exists $\rho, \mu \in \mathrm{Hom}(\Gamma, G) \cong G^r$ such that ρ corresponds to $(H_1, \ldots, H_r)$ and μ to $(X_1, \ldots, X_r) \in G^r \setminus H^r$. Then the action is not transitive by Theorem 2.2.4.

Conversely, suppose $G = \mathbb{Z}_p$ and $r \geq 2$. Since G is cyclic, the minimal number of generators of G, say k, is 1. Let $\rho \in \mathrm{Hom}(F_r, \mathbb{Z}_p)$ be a non-trivial homomorphism. Then $\rho(F_r)$ is a subgroup of G. This implies $\rho(F_r) = \mathbb{Z}_p$. Hence ρ is surjective. By Theorem 2.3.8 in the next section, the $\mathrm{Aut}(\Gamma)$-action is transitive on the set of epimorphisms when Γ is free and $r \geq 2k$. Thus, the action is transitive on $\mathrm{Hom}(F_r, G)$ when $r \geq 2$.

We now look at the case when $\Gamma = F_1 \cong \mathbb{Z}$ and $G = \mathbb{Z}_p$. Recall that $\mathrm{Aut}(\mathbb{Z}) = \{I, -I\}$ where I represents the trivial homomorphism that sends everything to identity. Let 1 denote the generator of $\mathbb{Z}$. Since $\mathbb{Z}$ is free, the image of ρ can be any element of G. Therefore $|\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_p)| = p$. If $\rho \in \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_p)$, then $\mathrm{Orb}(\rho) = \{\rho, -\rho\}$. Since $|\mathrm{Orb}(\rho)| \leq 2$, $\mathrm{Aut}(\mathbb{Z})$ action cannot be transitive. This concludes the proof.

□

Non-transitivity on G-character varieties of free groups

Definition 2.2.1 ([30])**.** A maximal connected solvable subgroup of G is called a *Borel subgroup*. A Zariski closed subgroup P is *parabolic* if P contains a Borel subgroup.

A *Levi subgroup* of a Zariski closed subgroup $H \subset G$ is a Zariski closed, connected subgroup L such that H is a semidirect product of L and the unipotent radical of H.

Definition 2.2.2. Let G be a complex reductive algebraic group and Γ a finitely generated group. A representation $\rho : \Gamma \to G$ is *irreducible* if $\rho(\Gamma)$ is not contained in any proper parabolic subgroup of G. The homomorphism, ρ is *completely reducible*, if for every parabolic subgroup, $P \subset G$ containing $\rho(\Gamma)$, there is a Levi subgroup containing $\rho(\Gamma)$.

See [30], [55] for a detailed description of the complex reductive case and [5], [4] for a general linear reductive group over fields of positive characteristic, G-action on an affine G-variety. By Theorem 5, [54] an orbit of $\rho \in \mathrm{Hom}(\Gamma, G)$ is polystable if and only if it is ρ is completely reducible. Also see [55] and [4].

Corollary 2.2.6. *Let Γ be a free group of rank $r \geq 2$ and G a non-abelian complex reductive algebraic group. Then the $\mathrm{Out}(\Gamma)$ action is not transitive on the $\mathbb{F}_q$ points of G-character varieties of Γ.*

Proof. Recall that $\mathrm{Hom}(\Gamma, G)$ has a bijection to G^r. Let T denotes the maximal torus subgroup of G. The T-valued representations maps into the abelian locus of $\mathrm{Hom}(\Gamma, G)$. Therefore, if $\rho \in \mathrm{Hom}(\Gamma, G) \subseteq T$, then ρ is abelian. In particular, there exist a polystable point $\rho \in \mathrm{Hom}(\Gamma, G)$ such that $\rho(\Gamma) \subseteq T^r$. Since T is closed, connected and solvable, it is contained in a Borel subgroup of G, say B. Note that B is parabolic. An irreducible representation μ is vacuously completely reducible. Therefore, the orbit of μ is closed. Additionally, by definition, μ is not contained in any parabolic subgroups. So, μ is not contained in the closure of ρ if $\rho(\Gamma) \subseteq T^r$. By Proposition 29 in [55], the set of irreducible representations form a dense subset of $\mathrm{Hom}(F_r, G)$ when $r \geq 2$. In particular this implies that the set of irreducible representations is non-empty. Since there exists polystable homomorphisms, μ and ρ such that $\rho(\Gamma) \subseteq B$ and $\mu(\Gamma) \subseteq G \setminus B$, the result follows from the Non-Transitivity Theorem, Theorem 2.2.4. $\square$

Remark 5. In the next chapter, Proposition 3.3.1, we give an explicit proof to show that the action is not transitive on the free abelian SL_n-character variety of $\mathbb{Z}^r$.

Definition 2.2.3 (Exponent Canceling Groups, [41])**.** Given a set S, let F_S denote the free group on S. We say that a word $R \in F_S$ is *exponent-canceling* if R maps to the identity in the free Abelian group on S (in other words, R lies in the commutator subgroup of F_S). Let Γ be a finitely generated discrete group. If Γ admits a presentation $\langle \gamma_1, \dots, \gamma_r \mid \{R_i\}_i \rangle$ in which each word R_i is exponent-canceling, then we say that Γ is *exponent-canceling.* We will refer to a generating set in an exponent-canceling group Γ as standard if there is a presentation of Γ with these generators in which all relations are exponent-canceling. The number r of generators in a standard presentation will be called the *rank of* Γ; note the Abelianization of Γ is always of the form $\mathbb{Z}^r$.

Lawton and Ramras introduce the concept of exponent canceling groups in [41]. Examples of exponent-canceling groups include free groups, free Abelian groups, right-angled Artin groups, and fundamental groups of closed Riemann surfaces, as well as the universal central extensions of surface groups considered in [8]. The class of exponent-canceling groups is closed under free and direct products.

Corollary 2.2.7. *Let Γ be an exponent canceling group with rank $r \geq 1$ and G a non-abelian complex reductive algebraic group. If there exists a non-abelian polystable homomorphism in $\mathrm{Hom}(\Gamma, G)$, then $\mathrm{Out}(\Gamma)$-action on $\mathfrak{X}_\Gamma(G)$ is not transitive.*

Proof. Since Γ is exponent-canceling, the abelianization is of the form $\mathbb{Z}^r$. Therefore, as in the proof of the previous corollary, there exists an element $\mu \in \mathrm{Hom}(\Gamma, G)$ such that $\rho(\Gamma) \in \mathbb{Z}^r$ and has a polystable orbit. If there exists non-abelian polystable $\mu \in \mathrm{Hom}(\Gamma, G)$, the result follows by Theorem 2.2.4. $\square$

2.3 Large Orbit Theorem

2.3.1 Free-Type Groups

We first define free-type groups. The motivation is to classify groups with automorphism groups that exhibits properties similar to that of free groups.

Definition 2.3.1. Let Γ admits a presentation $\langle \gamma_1, \ldots, \gamma_r \mid \{S_i\}_i \rangle$ such that $\mathrm{Aut}(\Gamma)$ includes the following elementary automorphisms.

$$P(i,j) : \gamma_i \mapsto \gamma_j,\ \gamma_j \mapsto \gamma_i,\ \gamma_k \mapsto \gamma_k\ ;\ k \neq i,j\ \text{(permutation of coordinates)}$$

$$I(i) : \gamma_i \mapsto \gamma_i^{-1},\ \gamma_k \mapsto \gamma_k\ ;\ k \neq i\ \ \text{(inverting the coordinate)}$$

$$L(i,j) : \gamma_i \mapsto \gamma_j\gamma_i,\ \gamma_k \mapsto \gamma_k\ ;\ k \neq i\ \ \text{(Left multiplication by } j^{th} \text{ coordinate)}$$

$$R(i,j) : \gamma_i \mapsto \gamma_i\gamma_j,\ \gamma_k \mapsto \gamma_k\ ;\ k \neq i\ \ \text{(Right multiplication by } j^{th} \text{ coordinate)}$$

Then we call Γ to be a group of *free-type of n generators*.

It is well-known that the set of Nielsen transformations generate $\mathrm{Aut}(F_n)$. See [43], Section 3.5 for a detailed discussion. Let $\{x_1, \ldots, x_n\}$ be an ordered generating set of F_n. Then we consider the following Nielsen transformations that generate $\mathrm{Aut}(F_n)$.

N1 : Permute x_1 and x_2.

N2 : Cyclically permute $x_1 \mapsto x_2, x_2 \mapsto x_3, \ldots, x_n \mapsto x_1$

N3 : Replace x_1 with x_1^{-1}.

N4 : Replace x_1 with $x_1 \cdot x_2$.

The following lemma shows that the elementary transformations generate $\mathrm{Aut}(F_n)$.

Lemma 2.3.1. *The set of elementary operations,* $\{P(i,j), I(i), L(i,j), R(i,j)\}$ *and the set of Nielsen transformations* $\{N1, \ldots, N4\}$ *are equivalent generating sets of* $\mathrm{Aut}(F_n)$*.*

Proof. We first prove that the set of Nielsen transformations, $\{N1, \ldots, N4\}$, can be expressed in terms of the elementary automorphisms from the definition of free-type groups. The first, third and fourth Nielsen transformations are clearly, $P(1,2), I(1)$ and $R(1,2)$, respectively. The second Nielsen transformation can be written as a combination of $P(i,j)$ since the permutation group on n elements can be generated by transpositions (permutations of cycle length two).

Conversely, we show that we can generate each of the elementary automorphisms using Nielsen transformations. Since a transposition and cyclic permutation generates the whole group of permutations, $P(i,j)$ can be generated using N1 and N2. Once any permutation of the generators is allowed, it can be combined with N3 and N4 to obtain $I(i)$ and $R(i,j)$, respectively. Finally, $L(1,2) = \text{N4} \circ \text{N1}$ and combining it with permutations generates $L(i,j)$. $\square$

Corollary 2.3.2. *A free group of rank n is of free-type of n.*

Remark 6. The property that Γ is of free type is dependent on the presentation. The following example show that this property is not necessarily invariant under presentation.

Example 2.3.1. By Corollary 2.3.2, $F_2 = \langle a, b \rangle$ is of free-type. Now consider the group, $\Gamma = \langle a, b, c \mid c \rangle$. Then clearly, Γ is isomorphic to F_2. Now, consider the permutation automorphism, $P(2,3)$ defined by $a \mapsto c, c \mapsto a$. Then relation of the group, c is not preserved by $P(2,3)$. Therefore, Γ is not free-type of rank 3 with respect to this presentation. But Γ is free-type of 2 generators using the presentation of F_2. Theorem 2.3.6 provides an alternate explanation for the same. By Theorem 2.3.6, Γ is a group of free-type of 3 generators if and only $\Gamma = F_3/N$ where $N \subseteq F_3$ is a characteristic subgroup. As in the proof of Theorem 2.3.6, N is the smallest normal subgroup containing the relations of Γ. However, the smallest normal subgroup containing c is not characteristic in F_3 since c cannot be conjugate to a and b, therefore cannot include any automorphism that sends c to other generators.

Definition 2.3.2 (Nielsen Equivalence, [36])**.** Let G be a group. Any two tuples $T = (g_1, \ldots, g_k)$ and $T' = (g'_1, \ldots, g'_k) \in G^k$ are called elementary equivalent if one of the following holds.

1. There exists some $\sigma \in S_n$ such that $g'_i = g_{\sigma(i)}$ for $1 \leq i \leq k$.

2. There is some $1 \leq i \leq k$ such that $g'_i = g_i^{-1}$ and $g'_j = g_j$ for $j \neq i$.

3. There exists $1 \leq i, j \leq k$ such that $g_i' = g_i g_j^\epsilon$ and $\epsilon \in \{1, -1\}$. Furthermore, $g_k' = g_k$ for $k \neq i$.

The tuples T and T' are *Nielsen equivalent* if there exists a sequence of n-tuples, $T_0, T_1, \ldots, T_n$ such that $T = T_0 \sim T_1 \sim \cdots \sim T_n = T'$ such that T_{i-1} and T_i are elementary equivalent.

In [48] (see [49] for a translation), Nielsen introduced the idea of Nielsen equivalence and proved that any two generating k-tuples are Nielsen equivalent in free groups. Gruschko later generalized this result to free products of finitely generated discrete groups[29]. In general, understanding Nielsen equivalence of generating k-tuples is particularly difficult, and the problem becomes even more complex if $k > rank(G)$ where $rank(G)$ is the minimal size of a generating set of G. See [36] for an exposition of the topic and a study of Nielsen equivalence in small cancellation groups. In this context, a conjecture of Wiegold is of particular relevance, which states that if G is a finite simple group and $k \geq 3$, then any two generating k-tuples of G are Nielsen equivalent. In other words, this is equivalent to saying that the action of $\mathrm{Aut}(F_n)$ on the set of epimorphisms from F_n to G, denoted $\mathrm{Epi}(F_n, G)$, is transitive in this case. Our work proves a similar result for the case of free-type groups instead of free, and G is a finite group. However, we work with a weaker condition on the bounds of generators, $n \geq 2 \cdot rank(G)$, compared to the Wiegold conjecture.

Examples of free-type groups

First, we explicitly prove that free abelian groups, a type of p-groups and free nilpotent groups are free-type groups. We then show that all free-type groups arise as quotients of free groups by characteristic subgroups.

Lemma 2.3.3. *Let Γ be a free abelian group. Then Γ is of free-type.*

Proof. Let $\Gamma = \langle \gamma_1, \ldots, \gamma_r \mid \gamma_i \gamma_j \gamma_i^{-1} \gamma_j^{-1} = 1 \text{ for } 1 \leq i, j \leq r \rangle$. It suffices to show that the elementary automorphisms specified while defining free-type group preserves the relations of the group.

1. Applying $P(i,j)$ permutes γ_i and γ_j: $\gamma_i \mapsto \gamma_j$ and $\gamma_j \mapsto \gamma_i$. Then the relation $1 = \gamma_i\gamma_j\gamma_i^{-1}\gamma_j^{-1} \mapsto \gamma_j\gamma_i\gamma_j^{-1}\gamma_i^{-1} = 1$ is preserved. Similarly, the relations $1 = \gamma_i\gamma_k\gamma_i^{-1}\gamma_k^{-1} \mapsto \gamma_j\gamma_k\gamma_j^{-1}\gamma_k^{-1} = 1$ are also preserved. Therefore, $P(i,j)$ preserves all the relations of Γ.

2. By inverting the coordinate, we get:

$$\gamma_i\gamma_j\gamma_i^{-1}\gamma_j^{-1} \longmapsto \gamma_i^{-1}\gamma_j(\gamma_i^{-1})^{-1}\gamma_j^{-1} = \gamma_i^{-1}\gamma_j\gamma_i\gamma_j^{-1}$$

   Since γ_i and γ_j commutes, $\gamma_i^{-1}\gamma_j\gamma_i\gamma_j^{-1} = 1$.

3. Left multiplication by γ_j, the following relations are modified. The relation $\gamma_i\gamma_j = \gamma_j\gamma_i$ becomes $\gamma_j\gamma_i\gamma_j = \gamma_j\gamma_j\gamma_i$. Since γ_i and γ_j commutes, the new relation is also satisfied. By the same argument, the relations $\gamma_i\gamma_k = \gamma_k\gamma_i$ are satisfied for all $1 \leq k \leq r$.

4. By symmetry of the relations, the same argument as above shows that right multiplication preserves the relations.

Therefore, Γ is of free-type. □

Lemma 2.3.4. *Let Γ be a group such that order of every element in Γ is a fixed power of p that is, for all $g \in \Gamma$, $|g| = p^n$ for a fixed $n \geq 1$. Then Γ is of free-type.*

Proof. As in the previous proof, it suffices to show that the elementary transformations preserve the relations of Γ. Clearly, permuting γ_i with γ_j and inverting the coordinates preserves the relations since $\gamma_j^{p^n} = 1$ and $(\gamma^{-1})^{p^n} = 1$. Similarly left multiplication sends γ_i to $\gamma_i\gamma_j$ and $(\gamma_i\gamma_j)^{p^n} = 1$. Therefore Γ is of free-type. □

Remark 7. If $|\Gamma| = p^n$, then Γ is a p-group.

Definition 2.3.3 (See [3]). Let F_n be a free group of rank n and let $F_{n,r}$ be the quotient group $F_n/\gamma_{r+1}(F_n)$ where $\gamma_{r+1}(F_n)$ is the $(r+1)^{th}$ term of the lower central series of F_n. Then $F_{n,r}$ is the *free nilpotent group* of class r and rank n.

Lemma 2.3.5. *Let* Γ *be a free nilpotent group. Then* Γ *is of free-type.*

Proof. By the Theorem in [3], the generators for automorphism group of $F_{n,r}$, the free nilpotent group of rank n and class r includes the Nielsen automorphisms of the following type.

1. $O : x_1 \mapsto x_1^{-1} \ \ x_i \mapsto x_i, \ i \neq 1$
2. $U : x_1 \mapsto x_1 x_2^{-1} \ \ x_i \mapsto x_i, \ i \neq 1$
3. $P : x_1 \mapsto x_2, \ x_2 \mapsto x_1 \ \ x_i \mapsto x_i, \ i \neq 1, 2$
4. $Q : x_1 \mapsto x_2, \ x_2 \mapsto x_2 \dots x_{n-1} \mapsto x_n, \ x_n \mapsto x_1$

These are precisely the generators of the automorphism group of free group of rank n, F_n. Therefore, by the definition of group of free-type, the result follows. □

Remark 8. As a corollary, we obtain Lemma 2.3.3.

Definition 2.3.4 (Characteristic subgroup)**.** Let G be a group and N be a subgroup of G. Then N is called a *characteristic subgroup* of G if $\phi(N) \subseteq N$ for all $\phi \in \mathrm{Aut}(G)$.

Remark 9. The condition $\phi(N) \subseteq N$ for all $\phi \in \mathrm{Aut}(G)$ is equivalent to the stronger condition $\phi(N) = N$. This is true because $\phi^{-1} \in \mathrm{Aut}(G)$ and $\phi^{-1}(N) \subseteq N$ implies $N \subseteq \phi(N)$.

Theorem 2.3.6. *Let* G *be a group. Then* G *is of free-type of* n*-generators if and only if* $G \cong F_n/N$ *where* F_n *is the free group of rank* n *and* N *is a characteristic subgroup of* F_n.

Proof. In this proof, for $w, w_1, w_2 \in F_n$, we use wN to denote the coset of w in F_n/N and $w_1 w_2$ to denote the product of w_1 and w_2 in F_n. Since every conjugation map is an inner automorphism, N is a normal subgroup of F_n. Therefore, the group F_n/N is well-defined. First, we prove that F_n/N is a group of free-type if $N \subseteq F_n$ is characteristic. By definition, $\phi(N) = N$ for all $\phi \in \mathrm{Aut}(F_n)$. Let $\{\gamma_1, \dots, \gamma_n\}$ be a generating set of F_n.

Any automorphism ϕ of F_n is completely defined by $\phi(\gamma_i)$. Consider the induced map of automorphisms,

$$\begin{aligned} \Psi : \mathrm{Aut}(F_n) &\longrightarrow \mathrm{Aut}(F_n/N) \\ \Psi(\phi) &= \Psi_\phi \end{aligned}$$

where $\phi \in \mathrm{Aut}(F_n)$ and the map Ψ_ϕ is defined as follows:

$$\begin{aligned} \Psi_\phi : F_n/N &\rightarrow F_n/N \\ \gamma_i N &\mapsto \phi(\gamma_i)N. \end{aligned}$$

First we show that Ψ_ϕ is well defined. Suppose $w_1N = w_2N$ for $w_1, w_2 \in F_n$. This implies $w_1^{-1}w_2N = N$. Therefore

$$\Psi_\phi(w_1N) = \Psi_\phi(w_1(w_1^{-1}w_2N) = \Psi_\phi(w_2N).$$

Clearly, Ψ_ϕ is surjective since $\phi \in \mathrm{Aut}(F_n)$ is surjective. For $w \in F_n$, suppose $\Psi_\phi(wN) = \phi(w)N = N$. Then, $\phi(w) \in N$. Since ϕ is bijective, $\phi^{-1}(N) = N$. Therefore, $\phi(w) \in N$ implies $w \in N$. Thus, $wN = N$ and hence Ψ_ϕ is injective. To show that Ψ_ϕ is a homomorphism, suppose $w_1N, w_2N \in F_n/N$. Then,

$$\begin{aligned} \Psi_\phi(w_1N \cdot w_2N) &= \Psi_\phi(w_1w_2N) = \phi(w_1w_2)N \\ &= \phi(w_1)\phi(w_2)N = \phi(w_1)N \cdot \phi(w_2)N \\ &= \Psi_\phi(w_1N) \circ \Psi_\phi(w_2N) \end{aligned}$$

since ϕ is a homomorphism and $\phi(N) = N$. Thus $\Psi_\phi \in \mathrm{Aut}(F_n/N)$. Now we prove that Ψ

is well defined. Suppose $\phi_1 = \phi_2$ for $\phi_1, \phi_2 \in \mathrm{Aut}(F_n)$. Then,

$$\begin{aligned}
\Psi_{\phi_1}(wN) &= \phi_1(w)N \text{ for } w \in F_n \\
&= \phi_2(w)N = \Psi_{\phi_2}(wN) \\
\implies \Psi(\phi_1) &= \Psi(\phi_2)
\end{aligned}$$

To prove that Ψ is a homomorphism, let $\phi_1, \phi_2 \in \mathrm{Aut}(F_n)$,

$$\begin{aligned}
\Psi(\phi_1 \circ \phi_2) &= \Psi_{\phi_1 \circ \phi_2} \\
\Psi_{\phi_1 \circ \phi_2} &: \gamma_i N \mapsto \phi_1(\phi_2(\gamma_i))N \\
\phi_1(\phi_2(\gamma_i))N &= \Psi_{\phi_1}(\phi_2 N) = \Psi_{\phi_1} \circ \Psi_{\phi_2}.
\end{aligned}$$

Thus, $\Psi_{\phi_1 \circ \phi_2} = \Psi_{\phi_1} \circ \Psi_{\phi_2}$. Therefore, Ψ is a homomorphism. Thus $\phi \in \mathrm{Aut}(F_n)$ induces an automorphism of $\mathrm{Aut}(F_n/N)$. Conversely, suppose $H = \{\gamma_1, \ldots, \gamma_n \mid S_i\}$ is a group of free-type. We use following result by Von Dyck that demonstrates the relation between a presentation of F_n, a subgroup H of F_n and the quotient group F_n/H.

Proposition 2.3.7 (Proposition 2, [35])**.** *If $G = \langle X \mid R \rangle$ and $H = \langle X \mid S \rangle$, where $R \subseteq S \subseteq F(X)$, then there is an epimorphism $\phi : G \to H$ fixing every $x \in X$ and such that $\ker(\phi) = \overline{S \setminus R}$. Conversely, every factor group of $G = \langle X \mid R \rangle$ has a presentation $\langle X \mid S \rangle$ with $S \supseteq R$.*

Specifically, if $G = F_n$ and $H = \langle X \mid S \rangle$ with respect to which H is free-type where $S = \{S_k\}$ is the set of defining relations of H, then by the proposition $H = F_n/\overline{S}$. Here, $\overline{S}$ denotes the smallest normal subgroup that contains S in F_n. Let ϕ be any elementary automorphism from the definition of free-type groups. Note that $\phi \in \mathrm{Aut}(H)$ implies $S_k(\phi(\gamma_1, \ldots, \gamma_n)) = 1$ for all k. Since the elementary automorphisms are equivalent to Nielsen transformations (Lemma 2.3.1), which generate $\mathrm{Aut}(F_n)$, it follows that S_k is invariant under $\mathrm{Aut}(F_n)$ for all k, that is, $\mathrm{Aut}(F_n) \cdot \overline{S} = \overline{S}$. Thus $\overline{S}$ is a characteristic subgroup of F_n such that

$H = F_n/\overline{S}$. $\square$

2.3.2 Large Orbit of Free-Type Group Action

Let G be a finite group and Γ, a group of free-type with n generators.

Definition 2.3.5. A *generating G-vector* of length n is an n-tuple $a = (a_1, \dots, a_n)$ where $a_i \in G$ such that $\langle a_1, \dots, a_n \rangle = G$. Note that n need not be the length of a minimal generating set. We use the notation $V(G, n)$ to denote the set of generating G-vectors of length n.

The group $\mathrm{Aut}(\Gamma)$ acts on $\mathrm{Hom}(\Gamma, G)$ through $\sigma \cdot \rho = \rho \circ \sigma^{-1}$. In [24], Gilman shows that the set of epimorphisms form an $\mathrm{Aut}(\Gamma)$-orbit when Γ is free [Theorem 2]. Below, we generalize the result to free-type groups and prove the main theorem of the thesis.

Theorem 2.3.8. *Let G be a non-trivial finite group and Γ a group of free-type with $n \geq 2k$ generators where k denotes the minimal number of generators for G. Then $\mathrm{Aut}(\Gamma)$ acts on $\mathrm{Hom}(\Gamma, G)$ through $\sigma \cdot \rho = \rho \circ \sigma^{-1}$ and the action is transitive on the set of epimorphisms from Γ to G.*

Proof. Let G be a finite group with k minimum number of generators, and
$\Gamma = \{\gamma_1, \dots, \gamma_n \mid \ R_i \text{ for } 1 \leq i \leq s\}$ be a group of free-type. Let $\mathcal{E}(\Gamma, G)$ denote the set of all epimorphisms from Γ to G. Consider the action of $\mathrm{Aut}(\Gamma)$ on $\mathrm{Hom}(\Gamma, G)$ defined as, for $\rho \in \mathcal{E}$ and $\sigma \in \mathrm{Aut}(\Gamma)$,

$$\sigma \cdot \rho = \rho \circ \sigma^{-1}.$$

Define

$$\mathcal{S}_{\Gamma,G} := \{(a_1, \dots, a_n) \in G^n \mid R_i((a_1, \dots, a_n)) = 0 \text{ for } 1 \leq i \leq s\}$$

be the set of all points in G that satisfies the relations of Γ. Let $\Delta^n_{\Gamma,G} = V(G, n) \cap S_{\Gamma,G}$ be the set of all generating vectors of length n that satisfies the relations of Γ. For simplicity, we use the notation Δ for $\Delta^n_{\Gamma,G}$ throughout this proof. We claim that there is a bijection between $\mathcal{E}(\Gamma, G)$ and Δ. To prove this, consider the evaluation map

$$\begin{aligned} \mathfrak{e} : \mathcal{E}(\Gamma, G) &\rightarrow \Delta \\ \mathfrak{e}(\rho) &= (\rho(\gamma_1), \ldots, \rho(\gamma_n)), \quad \rho \in \mathcal{E}(\Gamma, G). \end{aligned}$$

Since ρ is surjective, $(\rho(\gamma_1), \ldots, \rho(\gamma_n))$ is a generating vector of G. This implies $\mathfrak{e}(\rho) \in V(G, n)$. The tuple $(\rho(\gamma_1), \ldots, \rho(\gamma_n))$ clearly satisfies the relations of Γ as ρ is a homomorphism. Therefore, $\mathfrak{e}(\rho) \in \mathcal{S}_{\Gamma,G}$. Thus $\mathfrak{e}$ is well defined. Suppose $\mathfrak{e}(\rho_1) = \mathfrak{e}(\rho_2)$. Then $\rho_1(\gamma_i) = \rho_2(\gamma_i)$ for all i, $1 \leq i \leq n$. Then implies $\rho_1 = \rho_2$ since $\{\gamma_1, \ldots, \gamma_n\}$ is a generating set. Thus $\mathfrak{e}$ is injective. To show that $\mathfrak{e}$ is surjective, suppose $(a_1, \ldots, a_n) \in \Delta$. Define ρ such that $\rho(\gamma_i) = a_i$. Since $R_i((a_1, \ldots, a_n)) = 0$, ρ is a homomorphism by Theorem 2.0.1. Since $\{a_1, \ldots, a_n\}$ is a generating set of G, $w = \prod_{i=1}^{n} a_i^{k_i}$ for any $w \in G$. Then

$$\rho\left(\prod_{i=1}^{n} \gamma_i^{k_i}\right) = \prod_{i=1}^{n} \rho(\gamma_i^{k_i}) = \prod_{i=1}^{n} \rho(\gamma_i)^{k_i} = \prod_{i=1}^{n} a_i^{k_i} = w.$$

Since $\prod_{i=1}^{n} \in \Gamma$, ρ is an epimorphism. This shows that $\mathfrak{e}$ is a bijection.

Now, we proceed to show that the action is transitive on the set of generating n vectors using the above correspondence. Let $\{g_1, \ldots, g_k\}$ be a minimal generating set of G. Fix the generating tuple, $(g_1, \ldots, g_k) \in G^k$. We will show that any $x = (x_1, \ldots, x_n) \in \Delta$ can be transformed to an element $w = (g_1, \ldots g_k, 1 \ldots, 1) \in \Delta$ through the action of $\mathrm{Aut}(G)$. Since $x = (x_1, \ldots, x_n)$ is a generating vector and k is the minimal number of generators of G, there exists $\{x_{i_1}, \ldots, x_{i_k}\}$ where $i_s \in \{1, \ldots, n\}$ such that $\langle x_{i_1}, \ldots, x_{i_k} \rangle = G$. We apply the following transformations on x:

1. *Permutation automorphism*, $P(i, j)$: First we rearrange the coordinates of x such that the k generating elements occupy the last k entries of x i.e., we obtain the tuple, $(x_{j_1}, \ldots, x_{j_{n-k}}, x_{i_1}, \ldots, x_{i_k})$.

2. *Left/Right Multiplication*, $L(i,j)$ or $R(i,j)$: Multiply the first k entries of the tuple above with its last k entries to convert the first k entries to $\{g_1, \ldots, g_k\}$. For example, take the above tuple $(x_{j_1}, \ldots, x_{j_{n-k}}, x_{i_1}, \ldots, x_{i_k})$. Since $(x_{j_1}, x_{i_1}, x_{i_2}, \ldots, x_{i_k})$ is a generating set, there exists integers, $\{a_1, \ldots, a_{i_k}\} \subset \mathbb{Z}$ such that

$$g_1 = x_{i_1}^{a_2} \cdot x_{i_2}^{a_3} \cdots x_{j_1}^{a_1} \cdot \cdots \cdot x_{i_k}^{a_{k+1}}.$$

   Thus, by repeatedly multiplying with the last k coordinates it is possible to convert $(x_{j_1}, \ldots, x_{j_{n-k}}, x_{i_1}, \ldots, x_{i_k}))$ to $(g_1, x_{j_2} \ldots, x_{j_{n-k}}, x_{i_1}, \ldots, x_{i_k})$. Similarly, since $n \geq 2r$, we can obtain $(g_1, \ldots, g_k, \ldots, x_{i_1}, \ldots, x_{i_k})$ through the action of these automorphisms.

3. *Left/Right Multiplication*, $L(i,j)$ or $R(i,j)$. Finally, we apply the multiplication transformations again to convert the last $n-k$ entries to 1. Since the first k entries at this stage form a generating set of G, $\{g_1, \ldots, g_k\}$, we use the same strategy from the previous step to convert the $(i_{k+1})^{th}$ coordinate to one. Similarly, we can continue to obtain $(g_1, \ldots, g_k, 1, 1 \ldots, 1)$.

This concludes the proof. We end by noting that since $\mathrm{Hom}(\Gamma, G)$ is closed under the action of $\mathrm{Aut}(\Gamma)$, it follows that $(g_1, \ldots, g_k, 1, \ldots, 1) \in \mathrm{Hom}(\Gamma, G)$. Additionally, since $(g_1, \ldots, g_k, 1, \ldots, 1)$ is a generating n-vector, $(g_1, \ldots, g_k, 1, \ldots, 1) \in \Delta$. □

Corollary 2.3.9. *If $G \cong \mathbb{Z}_p$, the cyclic group on n-generators, then the* $\mathrm{Aut}(\Gamma)$ *action is transitive on* $\mathrm{Hom}(\Gamma, G)^*$.

Proof. We use the same argument as in the proof of Corollary 2.2.5. Let $G \cong \mathbb{Z}_p$ and $\rho \in \mathrm{Hom}(\Gamma, G)$ be a non-trivial homomorphism. Then $\rho(\Gamma)$ is a non-trivial subgroup of $\mathbb{Z}_p$. Therefore, $\rho(\Gamma) = G$ and hence ρ is surjective. Therefore, all the non-trivial homomorphisms from Γ to G are epimorphisms. Therefore the result follows by the theorem. □

We end this section by introducing the concept of epi-transitive groups.

Definition 2.3.6 (Epi-transitive groups)**.** Let Γ be a finitely generated group. We say that Γ is *epi-transitive* if the action of $\mathrm{Aut}(\Gamma)$ is transitive on the set of epimorphisms $\mathrm{Epi}(\Gamma, G) \subseteq \mathrm{Hom}(\Gamma, G)$ for every non-abelian group, G.

Corollary 2.3.10. *If Γ is free-type, then Γ is epi-transitive.*

Proof. The result follows directly from Theorem 2.3.8. $\square$

Conjecture 2.3.11. *The group G is epi-transitive does not imply that G is a free-type group. We suspect that hyperbolic surface groups are examples of groups that are epi-transitive but not free-type.*

Chapter 3: Asymptotic Transitivity

3.1 Asymptotic Transitivity

Character varieties of surface groups over fields of characteristic zero have a well-defined geometric invariant measure. In this scenario, the concept of ergodicity determines how well a group action mixes the points in the variety. The action of a group G on a variety X is *ergodic* if $A \subset X$ is G-invariant implies A has measure zero or $X - A$ has measure zero. Since there is no well-defined notion of such a 'nice' invariant measure on the space of finite field points of the character varieties we work with, we introduce the concept of asymptotic transitivity to understand the extent of "mixing" under a group action.

Let $\mathbb{F}_q$ be the field of order $q = p^n$ where p is a prime and $\overline{\mathbb{F}}_q$ denote the algebraic closure of $\mathbb{F}_q$.

Definition 3.1.1. Let G be an group and X a variety defined over $\mathbb{Z}$. Suppose G acts rationally on X. Now consider the action of the group on the $\mathbb{F}_q$-points of the variety denoted by $X(\mathbb{F}_q)$. We say that the action is *asymptotically transitive* if

$$\lim_{q\to\infty} \frac{\max_{v\in X(\mathbb{F}_q)} \Big|\mathrm{Orb}(v)\Big|}{|X(\mathbb{F}_q)|} = 1.$$

Additionally, we define the *asymptotic ratio* as

$$\lim_{q\to\infty} \frac{\max_{v\in X(\mathbb{F}_q)} \Big|\mathrm{Orb}(v)\Big|}{|X(\mathbb{F}_q)|}$$

whenever the limit exists.

Using this terminology, the action is asymptotically transitive if the asymptotic ratio of the maximal orbit is one.

Remark 10. 1. Note that since $q = p^n$, $q \to \infty$ in multiple ways, $p \to \infty$ or $n \to \infty$ or $p^n \to \infty$. We require that the limit exists regardless of how $q \to \infty$.

2. In some instances, we write $p \to \infty$ and only consider $\mathbb{F}_p \cong \mathbb{Z}_p$.

3. The ideal situation is when $|\mathrm{Orb}(v)|$ and $|X(\mathbb{F}_q)|$ are polynomials or quasi-polynomials in q.

4. It is worthwhile to note that we only need the formulas for $|\mathrm{Orb}(v)|$ and $|X(\mathbb{F}_q)|$ to be defined for all but finitely many values of p.

3.1.1 Examples and Non-Examples

We first discuss some non-examples.

Definition 3.1.2. An integer r is called a quadratic residue modulo p if it is congruent to a perfect square modulo p.

Example 3.1.1. Consider the polynomial $f = x^2 + y^2 - b$ where $b \in \mathbb{F}_q$ and I, the ideal generated by f in $\Bbbk[x, y]$. Let X denote the variety of I. Since f has integer coefficients, we can look at the finite field points of the variety denoted by $X(\mathbb{F}_q) \subseteq \mathbb{F}_q \times \mathbb{F}_q$ where $q = p^m$. By Theorem 2.1 in [44], we calculate the number of points in the variety as follows:

$$|X(\mathbb{F}_q)| = \begin{cases} q-1 & \text{if } \ b \neq 0 \ \text{ and } -4 \text{ is a nonzero quadratic residue} \\ q+1 & \text{if } \ b \neq 0 \ \text{ and } -4 \text{ is a quadratic nonresidue} \end{cases}$$

Define the action of $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ on $X(\mathbb{F}_q)$ as

$$\begin{aligned} 0 \cdot (x, y) &= (x, y) \\ 1 \cdot (x, y) &= (y, x). \end{aligned}$$

Note that the action is well defined since the polynomial f is symmetric with respect to the coordinates. It can be easily verified that the above map is a group action. Then $|\mathrm{Orb}(v)| = 2$ for all $v \in X(\mathbb{F}_q)$. Therefore, $\max_{v \in X(\mathbb{F}_q)} \left|\mathrm{Orb}(v)\right| = 2$. Since the number of the points increase in the order of q, we have that

$$\lim_{q\to\infty} \frac{\left|\max_{v\in X(\mathbb{F}_q)} \mathrm{Orb}(v)\right|}{|X(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{2}{q\pm 1} = 0.$$

This is an example of an action that is not asymptotically transitive.

Remark 11. Note that if the maximum orbit size is a constant and $|X(\mathbb{F}_q)| \to \infty$, then the action cannot be asymptotically transitive.

Example 3.1.2. Let $p(x) = x$ be the polynomial and let X be the variety given by the ideal $J = \langle p \rangle \subseteq k[x, y]$ where k is a field. Denote by $X(\mathbb{F}_q)$ the finite field points of the variety as in the last example. Then note that $X(\mathbb{F}_q) = \{(0, k) \mid k \in \mathbb{F}_q\}$. Consequently,

$$|X(\mathbb{F}_q)| = q.$$

Define an action α on $X(\mathbb{F}_q)$ as follows:

$$\alpha(x, y) = (x, y + 1) \text{ for } (x, y) \in X(\mathbb{F}_q) \subseteq \mathbb{F}_q \times \mathbb{F}_q.$$

Note that the action is well defined as the action leaves the x coordinate invariant. Then

$$\alpha^n(x, y) = (x, y + n).$$

For any $y \in \mathbb{F}_q$ observe that $\{y + n \mid 1 \leq n \leq q\} = \mathbb{F}_q$ since the additive group is generated by 1. Therefore $\mathrm{Orb}((x, y)) = X(\mathbb{F}_q)$ for all $(x, y) \in X(\mathbb{F}_q)$.

Therefore, the action is transitive. Here, we have that

$$\frac{\max_{v \in X(\mathbb{F}_q)} \Big|\mathrm{Orb}(v)\Big|}{|X(\mathbb{F}_q)|} = 1$$

and hence the limit is also one.

Remark 12. Transitivity implies asymptotic transitivity. But the converse is not necessarily true. We are interested in the cases where the converse doesn't hold, that is, when the action is asymptotically transitive but not transitive.

Example 3.1.3. We now give a class of examples where the action is asymptotically transitive.

Lemma 3.1.1. *Let G acts rationally on a variety X defined over $\mathbb{Z}$. Suppose $W(\mathbb{F}_q)$ is a subset of $X(\mathbb{F}_q)$ such that the action is transitive on $W(\mathbb{F}_q)$ for all q and for every q let $\{V_i(\mathbb{F}_q)\}_{i=1}^m$ be a finite non-empty collection of disjoint subsets such that $V_i(\mathbb{F}_q) \not\subseteq W(\mathbb{F}_q)$ for $1 \leq i \leq m$. Additionally, suppose the action is stable on $Y(\mathbb{F}_q) := W(\mathbb{F}_q) \bigcup (\bigcup_{i \in I} V_i(\mathbb{F}_q))$ for all q. If, $W(\mathbb{F}_q)$ and $V_i(\mathbb{F}_q)$ have polynomial (monic) growth as q increases such that the order of growth of $V_i(\mathbb{F}_q)$ is less than that of $W(\mathbb{F}_q)$ as $q \to \infty$ for $1 \leq i \leq m$, then the action is asymptotically transitive on $Y(\mathbb{F}_q)$.*

Proof. By assumption, the action is stable on $Y(\mathbb{F}_q)$. Clearly $W(\mathbb{F}_q) \cap V(\mathbb{F}_q) = \emptyset$ since the action is transitive on $W(\mathbb{F}_q)$ and $V_i(\mathbb{F}_q) \not\subseteq W(\mathbb{F}_q)$. Therefore, $|Y(\mathbb{F}_q)| = |W(\mathbb{F}_q)| + \sum_{i=1}^{m} |V(\mathbb{F}_q)|$. Suppose the order of growth of points in $W(\mathbb{F}_q)$ is s and that of $V_i(\mathbb{F}_q)$ is t_i. By assumption, $s > t_1, \ldots, t_m$. Let $w \in W(\mathbb{F}_q) \subset Y(\mathbb{F}_q)$. Then the asymptotic ratio of the orbit of w is given by

$$\lim_{q \to \infty} \frac{|\mathrm{Orb}(w)|}{|Y(\mathbb{F}_q)|} = \lim_{q \to \infty} \frac{|W(\mathbb{F}_q)|}{|Y(\mathbb{F}_q)|} = \lim_{q \to \infty} \frac{q^s + a_1 q^{s-1} + \cdots + a_s}{q^s + q^{t_1} + \cdots + q^{t_m} + \text{lower terms}} = 1$$

since q^s is the leading term of both numerator and denominator. $\square$

Corollary 3.1.2. *Let $X(\mathbb{F}_q)$ and $W(\mathbb{F}_q)$ be as defined in the theorem. If the number of points in V_i is constant for all $1 \leq i \leq m$ and the order of growth of size of $W(\mathbb{F}_q)$ is at least one, then the action is asymptotically transitive on $Y(\mathbb{F}_q) := W(\mathbb{F}_q) \bigcup_{i\in I} V_i(\mathbb{F}_q)$.*

We now give an example where this corollary applies.

Example 3.1.4. Let Γ be a finitely presented group and $G(\mathbb{F}_q)$ be any group obtained as finite field points of an algebraic group G defined over $\mathbb{Z}$. For example, $\mathrm{SL}_n(\mathbb{F}_q)$ denote the finite field points of SL_n. Consider the action of $\mathrm{Out}(\Gamma)$ on $\mathrm{Hom}(\Gamma, G)$ as defined in Lemma 2.2.1. Let $\rho \in \mathrm{Hom}(\Gamma, G)$ such that $|\mathrm{Orb}(\rho)| \geq q$ for all $q \geq 2$. From Corollary 2.2.3, we know that $|\mathrm{Orb}(I)| = 1$ where I denotes the identity homomorphism. By letting $W(\mathbb{F}_q) = \mathrm{Orb}(\rho)$ and $V(\mathbb{F}_q) = \mathrm{Orb}(I)$, the action is asymptotically transitive on $Y(\mathbb{F}_q) = W(\mathbb{F}_q) \cup V(\mathbb{F}_q)$.

Remark 13. In general, we can choose $V_i(\mathbb{F}_q)$ to be the orbit of a fixed point of bounded over q. Additionally, if the action is transitive on $X(\mathbb{F}_q)$, except for a finite set of points, not depending on q for all values of q, then the action is asymptotically transitive on $X(\mathbb{F}_q)$.

Example 3.1.5. We recall the discussion from Section 1.2 about the example where Bourgain, Gamburd and Sarnak, [7], studied the $\mathbb{Z}/p\mathbb{Z}$ points of the Markoff equation given by

$$x_1^2 + x_2^2 + x_3^2 - 3x_1x_2x_3 = 0. \tag{3.1}$$

They were interested in the action of the group Γ of affine integral morphisms of the affine 3-space generated by the permutations of the coordinates and Vieta involutions. Their results yield strong approximation property for the Markoff equation for most primes which implies asymptotic transitivity. In [13], Chen shows that for all but finitely many primes p, the group of Markoff automorphisms acts transitively on the nonzero $\mathbb{F}_p$-points of the Markoff equation. This result proves that the action is asymptotically transitive on this variety.

This example is closely related to the relative character variety of one-holed torus. As explained in Section 1.1.5, in the one-holed torus case where the fundamental group is F_2, the free group on two generators, and $G = \mathrm{SL}(2, \mathbb{C})$, the the relative λ-character variety is obtained by fixing the boundary component which is the trace of the commutator,

$$\operatorname{tr}(XYX^{-1}Y^{-1}) = x^2 + y^2 + z^2 - xyz - 2 = \lambda.$$

[See Appendix A.0.1 for a derivation of this identity.] When $\lambda = -2$, this equation reduces to $x^2 + y^2 + z^2 - xyz = 0$ which is similar to Equation (3.1). One natural question to ask is whether the action is asymptotically transitive on the relative character variety of $\mathfrak{X}_{F_2}(\mathrm{SL}_2(\mathbb{F}_q))$ for all values of λ. In the following sections, we look at the case when the commutator equals identity, that is, $\lambda = 2$.

3.2 Stratification and E-polynomials of $\mathrm{SL}_n(\mathbb{F}_q)$ - Character Varieties of $\mathbb{Z}^r$

We now explore the asymptotic transitivity of the outer automorphism group action of $\mathbb{Z}^r$ on $\mathrm{SL}_n(\mathbb{F}_q)$-character varieties of $\mathbb{Z}^r$ for $n = 2, 3$. Along the way, we compute the E-polynomial, also known as the Hodge-Deligne polynomial or Serre polynomial of these free abelian SL_2- and SL_3-character varieties.

The strategy is to stratify the space, $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_n(\mathbb{F}_q))$ based on the stabilizer type under the conjugation action. We then count the orbits in each stratum and use this information to calculate the E-polynomial. See Section 1.1.3 for a discussion of E-polynomials.

Elementary results on $\mathbb{F}_q$

We first prove some well-known results about properties of finite fields that will be used in subsequent sections.

Definition 3.2.1. Let $\Bbbk$ be a field. Then $r \in \Bbbk$ is an nth *root of unity* if $r^n = 1$ and a *primitive* nth root of unity if, in addition, n is the smallest integer of $k = 1, \ldots, n$ for which $r^k = 1$. A primitive nth root of unity generates a cyclic group of order n.

The following lemma classifies the finite fields with a primitive cube root of unity.

Lemma 3.2.1. *Let $\mathbb{F}_q$ denotes the finite field with $q = p^k$ elements. Then $\mathbb{F}_q$ has a cube root of unity $\lambda \neq 1$ if only if*

1. $p \equiv 1 \mod 3$ *or*

2. $p \equiv -1 \mod 3$ *and k is even.*

Proof. Note that $q = p^k$ where p is a prime. The multiplicative group, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is cyclic. Since $|\mathbb{F}_q^*| = q - 1$, $\mathbb{F}_q$ has a primitive cube root of unity if and only if three divides $q - 1$. Then p is congruent to $0, 1$ or $-1 \mod 3$. We will address the three cases separately.

- If $p \equiv 0 \mod 3$, then $q \equiv 0 \mod 3$. Therefore, $3 \nmid q - 1$.

- If $p \equiv 1 \mod 3$, then $q \equiv 1 \mod 3$. Consequently, $3 \mid q - 1$.

- When $p \equiv -1 \mod 3$, then $q \equiv (-1)^k \mod 3$. Hence, $3 \mid q - 1$ if and only if k is even.

This proves the result. □

Remark 14. In general $\mathbb{F}_q$ has a primitive nth root of unity if and only if n divides $q - 1$.

Lemma 3.2.2. *Let $\mathbb{F}_q$ be a finite field with $q = p^k$ elements. Then $\mathbb{F}_q$ has* $\gcd(n, q-1)$ *nth roots of unity.*

Proof. The multiplicative group, $\mathbb{F}^*$ is cyclic of order $q - 1$. Let a be a generator of the group. Now the problem reduces to finding the number of elements $x \in \mathbb{F}_q^*$ such that $x^n = 1$. If $x = a^m$, then $(a^m)^n = a^{mn} = 1$. This implies mn is divisible by $q - 1$. If $d = \gcd(n, q-1)$, $(q-1)|mn$ if and only if $\frac{q-1}{d}$ divides $m\frac{n}{d}$. Therefore, $\frac{q-1}{d}$ divides m. Consequently, the roots of unity forms a subgroup generated by $a^{\frac{q-1}{d}}$ with d elements. This concludes the proof. $\square$

Corollary 3.2.3. *Let $\mathbb{F}_q$ be a finite field with $q = p^k$ elements. Then the number of primitive cube roots of unity in $\mathbb{F}_q$, if it exists, is 2.*

Proof. From the above lemma, the number of cube roots of unity is $\gcd(3, q-1) = 1$ or 3. Since one is a cube root of unity for all q, this implies that the number of primitive roots of unity is at most two. Since only the identity element has order one, the result follows. $\square$

Corollary 3.2.4. *If $q = p^k$, the number of square roots of unity in $\mathbb{F}_q$ is one if $p = 2$ and two if p is odd.*

Proof. If p is even, then so is $q = p^k$. Then $q - 1$ is odd and $\gcd(2, q-1) = 1$. Similarly, if p is odd, $\gcd(2, q-1)$ is 2. $\square$

Properties of $\mathrm{SL}_n(\mathbb{F}_q)$ and $\mathrm{GL}_n(\mathbb{F}_q)$.

We look at some properties of the matrix groups which will be repeatedly used in the subsequent sections. These are well-known results found in different references. For matrix groups, G, e.g., $\mathrm{GL}_n(\mathbb{F}_q), \mathrm{SL}_n(\mathbb{F}_q)$ etc. , we use $\mathcal{D}(G)$ to denote the set of diagonal matrices in G. Let F_r be the free group of rank r.

Lemma 3.2.5. *The following are true.*

1. $|\mathrm{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}) = \prod_{i=0}^{n-1}(q^n - q^i)$.

2. $|\mathrm{SL}_n(\mathbb{F}_q)| = \frac{1}{(q-1)}(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1}) = \frac{1}{(q-1)}\prod_{i=0}^{n-1}(q^n - q^i)$.

3. $|\mathcal{D}(\mathrm{GL}_n(\mathbb{F}_q))| = (q-1)^n$

4. $|\mathcal{D}(\mathrm{SL}_n(\mathbb{F}_q))| = (q-1)^{n-1}$.

5. $|\mathrm{Hom}(F_r, \mathrm{GL}_n(\mathbb{F}_q)| = \prod_{i=0}^{n-1}(q^n - q^i)$

6. $|\mathrm{Hom}(F_r, \mathrm{SL}_n(\mathbb{F}_q)| = \frac{1}{(q-1)}\prod_{i=0}^{n-1}(q^n - q^i)$

Proof. We count the number for possibilities of each row of a matrix in $\mathrm{GL}_n(\mathbb{F}_q)$.

1. Let $A = [a_{ij}]_{i,j=1}^n \in \mathrm{GL}_n(\mathbb{F}_q)$. Then there are q possibilities for a_{1i} for $1 \leq i \leq n$. Therefore, after subtracting the zero row, there are total $q^n - 1$ possibilities for the first row. Similarly, the second row has $q^n - q$ possibilities, after discarding q linear multiples of the first row.

   The third row is linearly independent of the first and second row. There are q^2 distinct linear combinations of first and second rows and hence we have $q^n - q^2$ combinations for the third row. Continuing in a similar fashion, we obtain the total number of matrices possible to be $\prod_{i=0}^{n-1}(q^n - q^i)$.

2. The key idea in the proof is the fact that $\mathrm{SL}_n(\mathbb{F}_q)$ is the kernel of the determinant map from $\mathrm{GL}_n(\mathbb{F}_q)$. Consider the determinant map on $\mathrm{GL}_n(\mathbb{F}_q)$,

$$\begin{aligned} \det : \mathrm{GL}_n(\mathbb{F}_q) &\longrightarrow \mathbb{F}_q^* \\ A &\longmapsto \det(A) \end{aligned}$$

   Note that this is surjective since, for every $\lambda \in \mathbb{F}_q^*$,

$$I_\lambda = \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{F}_q)$$

   such that $\det(I_\lambda) = \lambda$.

This is a group homomorphism since $\det(AB) = \det(A) \cdot \det(B)$. Then

$$\ker(\det) = \{A \in \mathrm{GL}_n(\mathbb{F}_q) \mid \det(A) = 1\} = \mathrm{SL}_n(\mathbb{F}_q).$$

Therefore, by First Isomorphism Theorem,

$$\begin{aligned}
\frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{SL}_n(\mathbb{F}_q)|} &= |\mathbb{F}_q^*| = q - 1 \\
|\mathrm{SL}_n(\mathbb{F}_q)| &= \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{q-1} \\
&= \frac{\prod_{i=0}^{n-1} (q^n - q^i)}{q-1}.
\end{aligned}$$

3. Suppose A is an $n \times n$ diagonal matrix. To count the number of possible entries for A, it suffices to compute the number of n-tuples whose product is non-zero. This is the same as counting the number of n tuples with entries from $\mathbb{F}_q^*$. Since there are $q - 1$ choices for each entry, it follows that we have $(q - 1)^n$ combinations.

4. Let $D = [d_i]_{i=1}^n$ be in $\mathcal{D}(\mathrm{SL}_n(\mathbb{F}_q))$ such that d_i denote the entry at the i^{th} diagonal entry. We have $(q - 1)$ possibilities for each the entries, $d_1, d_2, \ldots, d_{(n-1)}$. Then $d_n = \frac{1}{d_1 \cdots d_{(n-1)}}$. Therefore there are $(q - 1)^{n-1}$ choices for D.

5. To prove 4 and 5, recall that by Corollary 2.0.3, $\mathrm{Hom}(F_r, G)$ is in bijective correspondence with G^r. Then the results follow from part 1 and 2 of this lemma.

This concludes the proof. □

Lemma 3.2.6. *The set of homomorphisms,* $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_n(\mathbb{F}_q))$ *is in bijective correspondence with the set of pairwise commuting r tuples of* $\mathrm{SL}_n(\mathbb{F}_q)$,

$$\{(A_1, \ldots, A_r) \mid A_i A_j = A_j A_i \ \ \textit{for } 1 \leq i, j, \leq r\}.$$

Proof. Recall that $\mathbb{Z}^r$ has the presentation, $\{(\gamma_1, \ldots, \gamma_r) \mid \gamma_i \gamma_j \gamma_i^{-1} \gamma_j^{-1} \text{ for } 1 \leq i, j \leq r\}$. Then the result follows by Lemma 2.0.2. □

This motivates us to consider properties of commuting tuples and simultaneously diagonalizable tuples.

Lemma 3.2.7. *Let $(A_1, \ldots, A_r) \in \mathrm{SL}_n(\mathbb{F}_q)^r$. Then there exists $P \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$ such that $(PA_1P^{-1}, \ldots, PA_rP^{-1})$ is diagonal if and only if there exist a $Q \in \mathrm{GL}_n(\overline{\mathbb{F}}_q)$ with the same property, i.e, $(QA_1Q^{-1}, \ldots, QA_rQ^{-1})$ is diagonal.*

Proof. If there exists $P \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$ such that $(PA_1P^{-1}, \ldots, PA_rP^{-1})$ is an r-tuple of diagonal matrices, then let $Q = P$ since $\mathrm{SL}_n(\overline{\mathbb{F}}_q) \subseteq \mathrm{GL}_n(\overline{\mathbb{F}}_q)$. Conversely, suppose there exists $Q \in \mathrm{GL}_n(\overline{\mathbb{F}}_q)$ such that the tuple $(QA_1Q^{-1}, \ldots, QA_rQ^{-1})$ is diagonal. Now let $P = \frac{1}{\det Q} \cdot Q$ so that P has determinant 1. Additionally, since multiplying a matrix is scaling of the entries, it follows that $(PA_1P^{-1}, \ldots, PA_rP^{-1})$ is diagonal. □

Lemma 3.2.8. *Let $(A_1, ..., A_r) \in \mathrm{SL}_n(\mathbb{F}_q)^r$ be simultaneously diagonalizable by a matrix $P \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$. Then $A_iA_j = A_jA_i$ for $1 \leq i, j \leq r$.*

Proof. Suppose $(A_1, ..., A_r)$ is simultaneously diagonalizable. Then, there exists $P \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$ such that $PA_iP^{-1} = D_i$ where $D_i \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$ is a diagonal matrix for $1 \leq i \leq m$. Since $D_iD_j = D_jD_i$ for all $1 \leq i, j \leq m$,

$$\begin{aligned} A_iA_j &= P^{-1}D_iPP^{-1}D_jP \\ &= P^{-1}D_iD_jP \\ &= P^{-1}D_jD_iP \\ &= P^{-1}D_jPP^{-1}D_iP \\ &= A_jA_i. \end{aligned}$$

□

Conjugation Action and Stabilizer

First, we want to count the conjugation orbits in $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_n(\mathbb{F}_q))$ for $n = 2, 3$ i.e., the number of homomorphisms equivalent up to conjugation. To this end, we define the conjugation action of $\mathrm{SL}_n(\mathbb{F}_q)$ on $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_n(\mathbb{F}_q))$,

$$A \cdot \rho = A\rho A^{-1}.$$

Let $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_n(\mathbb{F}_q))/\mathrm{SL}_n(\mathbb{F}_q)$ denote the set of orbits under the above action. We first identify the elements in $\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_n(\mathbb{F}_q)))$ that corresponds to a closed conjugation orbits which parameterizes the character variety, $\mathfrak{X}_{\mathbb{Z}^r}(\mathrm{SL}_n(\mathbb{F}_q))$. In [19], Florentino and Lawton prove that there is a homeomorphism between the space of polystable orbits and the GIT quotient. By Proposition 3.1 in [19], for a finitely generated group abelian group Γ and a complex reductive algebraic group G, the set of polystable points, $\mathrm{Hom}(\Gamma, G)^{ps}$ is equivalent to $\mathrm{Hom}(\Gamma, G_{ss}) = \{\rho \in \mathrm{Hom}(\Gamma, G) \mid \rho(\gamma_i) \in G_{ss}, i = 1, \ldots, r\}$ where G_{ss} denote the semisimple points in G. Therefore, the polystable points are homomorphisms, ρ such that $\rho(\gamma_i)$ is simultaneously diagonalizable for all i, $1 \leq i \leq r$.

Stabilizer

Definition 3.2.2. Two tuples $(A_1, \ldots, A_r)$ and $(B_1, \ldots, B_r)$ in $\mathrm{SL}_n(\mathbb{F}_q)^r$ are said to have the same stabilizer type if $|\mathrm{Stab}(A_1, \ldots A_r)| = |\mathrm{Stab}(B_1, \ldots B_r)|$.

The following lemma characterizes the stabilizer of a single matrix under conjugation action.

Lemma 3.2.9. *Let $D = [d_{ii}]_{i=1}^n \in \mathrm{GL}_n(\Bbbk)$ be a diagonal matrix with entries from a field, $\Bbbk$. Suppose $G_D \subseteq \mathrm{GL}_n(\Bbbk)$ is the set of all matrices that commute with D. Then*

$$G_D = \left\{ [a_{ij}]_{i,j=1}^n \mid a_{ij} = 0 \text{ if } d_{ii} \neq d_{jj} \text{ and } \; a_{ij} \in \Bbbk \text{ if } d_{ii} = d_{jj} \right\}.$$

Proof. Let $A = [a_{ij}]$ and $D = [d_{ij}]$ be such that $AD = DA$. We compare the ij-th entry of AD and DA.

$$\begin{aligned} [AD]_{ij} &= \sum_{k=1}^{n} a_{ik} d_{kj} = a_{ij} d_{jj} \\ [DA]_{ij} &= \sum_{k=1}^{n} d_{ik} a_{kj} = d_{ii} a_{ij} \end{aligned}$$

Note that $AD = DA$ if and only if $a_{ij} d_j = d_i a_{ij}$ which is true only if $a_{ij}(d_j - d_i) = 0$. Since $a_{ij}, d_i, d_j \in \Bbbk$ are not zero divisors, $d_i \neq d_j$ implies $a_{ij} = 0$. Suppose $d_i = d_j$. Then $a_{ij}(d_j - d_i) = 0$ for any value of $a_{ij} \in \Bbbk$. Therefore, the result follows. □

Corollary 3.2.10. *Suppose $D \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$ is a diagonal matrix such that all the diagonal entries are distinct. If $A \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$ such that $AD = DA$, then A is diagonal.*

Proof. The proof follows directly from Lemma 3.2.9. □

Definition 3.2.3. For $A \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)$, define the centralizer of A,

$$G_A := \{P \in \mathrm{GL}_n(\overline{\mathbb{F}}_q) \mid PA = AP\}.$$

We can now compute the stabilizer of a tuple $(A_1, \ldots, A_r) \in \mathrm{SL}_n(\mathbb{F}_q)$ in terms of the centralizers of A_i.

Lemma 3.2.11. *Let $(A_1, \ldots, A_r) \in \mathrm{SL}_n(\overline{\mathbb{F}}_q)^{\times r}$. Consider the conjugation action of $\mathrm{GL}_n(\overline{\mathbb{F}}_q)$ defined by $P \cdot (A_1, ..., A_r) = (PA_1P^{-1}, ..., PA_rP^{-1})$. Then*

$$\mathrm{Stab}_{\mathrm{SL}_n(\overline{\mathbb{F}}_q)}((A_1, ..., A_r)) = G_{A_1} \cap G_{A_2} \cap \ldots \cap G_{A_r}.$$

Proof.

$$
\begin{aligned}
\mathrm{Stab}((A_1, .., A_r)) &= \{P \in \mathrm{GL}_n(\mathbb{F}_q) \mid P \cdot (A_1, .., A_r) = (A_1, .., A_r)\} \\
&= \{P \mid (PA_1P^{-1}, .., PA_rP^{-1}) = (A_1, .., A_r)\} \\
&= \{P \mid PA_1P^{-1} = A_1,\ PA_2P^{-1} = A_2, \dots, PA_rP^{-1} = A_r\} \\
&= \{P_1 \mid P_1A_1 = A_1P_1\} \cap \{P_2 \mid P_2A_2 = A_2P_2\} \cap \cdots \cap \{P_r \mid P_rA_r = A_rP_r\} \\
&= G_{A_1} \cap G_{A_2} \cap \cdots \cap G_{A_r}.
\end{aligned}
$$

□

Classifying pairwise commuting tuples

In this section, we look at pairs of matrices over finite field that commutes pairwise.

Lemma 3.2.12. *Let A, B be commuting matrices. If λ is an eigenvalue of A, then B preserves the λ-eigenspace of A.*

Proof. By hypothesis, $AB = BA$. We show that if u is a λ-eigenvector of A, Bu is also a λ-eigenvector of A. Since u is a λ-eigenvector of A, $Au = \lambda u$. Then,

$$A(Bu) = ABu = BAu = B(Au) = B\lambda u = \lambda Bu.$$

Therefore, $Bu \in \mathrm{Eig}_\lambda(A)$. □

Lemma 3.2.13. *Let V be a finite dimensional vector space over a field $\Bbbk$ and $T \in \mathrm{End}(V)$ be a linear operator on V. Then each distinct monic divisor of the minimal polynomial, p_T, of T over $\Bbbk$ corresponds to a distinct T-invariant subspace of V.*

Proof. Let $f(x)$ be the minimal polynomial of $T \in \mathrm{End}(V)$. Suppose $f_1(x,) \dots, f_s(x)$ are the distinct factors of $f(x)$. Now, consider the map from distinct monic factors of T to distinct T-invariant subspaces, defined as:

$$f_i \mapsto \ker(f_i(T)).$$

To prove that this map is well defined, we first show that all kernels of S that commute with T are T-invariant. Suppose $v \in \ker(T)$. Then $Tv = 0$.

$$TSv = STv = S0 = 0.$$

Thus, $S(\ker(T)) \subseteq \ker(S)$. Since polynomials in T commute with T, $\ker(f_i(T))$ is a T-invariant subspace of V. Therefore the map is well defined. We now prove that the map is injective.

Suppose $W_i = \ker(f_i(T)) = \ker(f_j(T)) = W_j$. Then, f_i is the minimal polynomial of $T|_{W_i}$ and f_j is the minimal polynomial of W_j. Since $W_i = W_j$, this implies that $f_i = f_j$. Therefore, the map is injective. □

Lemma 3.2.14. *Let $\Bbbk$ be a field and let V be a $\Bbbk$-vector space. Let $T : V \to V$ be a linear transformation. Then the characteristic polynomial of T is irreducible over $\Bbbk$ if and only if T has no non-trivial invariant subspaces.*

Proof. We prove the contrapositive. Let p_T denote the characteristic polynomial over $\Bbbk$. If $p_T =$ is reducible then p_T has a proper monic divisor, $q(x)$. As in the above proof of Lemma 3.2.13, $\ker(q(T))$ is a non-trivial invariant subspace of T.

Conversely, suppose W is a T-invariant subspace. Then T can be expressed in a block triangular form $\begin{pmatrix} U_1 & S \\ 0 & U_2 \end{pmatrix}$ by expressing T on a basis that extends a basis of W. Thus, $p_T = p_{U_1} \cdot p_{U_2}$ where U_1 corresponds to $T|_W$ and U_2 corresponds to $T|_{V \setminus W}$. Therefore p_T is reducible. □

For a matrix A, let $\mathrm{char}(A)$ denote the characteristic polynomial of A.

Lemma 3.2.15. *Let $A, B \in \mathrm{SL}_n(\mathbb{F}_q)$ such that $AB = BA$ and $\mathrm{char}(A)$ is irreducible over $\mathbb{F}_q$ for $n = 2, 3$. Then B is either central or has an irreducible characteristic polynomial.*

Proof. Clearly if B is central, $AB = BA$. Suppose B is not scalar. If B is reducible, then $\mathrm{char}(B)$ has a non-trivial divisor $f(x)$. As in the proof of Lemma 3.2.13, $\ker(f(B))$ is an invariant subspace of A. If $\mathrm{char}(B)$ is reducible, then $\ker(f(B))$ is a non-trivial A invariant subspace of A and hence gives a contradiction. Therefore, the characteristic polynomial $\mathrm{char}(B)$ is irreducible.

Remark 15. Note that here the characteristic polynomial and minimal polynomial of A are the same.

□

We use the following well-known result without proof.

Lemma 3.2.16. *For $n \leq 3$, two matrices A and B are similar if and only if they have the same characteristic and minimal polynomial.*

Our goal is to count the number of distinct diagonal matrices, D, over $\mathbb{F}_q$ such that D is conjugate to a matrix over $\mathbb{F}_q$. We first count the stabilizer of such a matrix under the conjugation action when the characteristic polynomial is irreducible.

Lemma 3.2.17. *Let $\mathrm{SL}_n(\mathbb{F}_q)$ act on the set of diagonal matrices in $\mathrm{SL}_n(\mathbb{F}_q)$ by conjugation. If A is such that its characteristic polynomial, $\mathrm{char}(A)$, is irreducible over $\mathbb{F}_q$, then the size of the stabilizer of A, G_A, is $\frac{q^n-1}{q-1}$.*

Proof. Let $A \in \mathrm{SL}_n(\mathbb{F}_q)$ where $n = 2, 3$. Let $\mathrm{SL}_n(\mathbb{F}_q)$ acts on $\mathrm{SL}_n(\mathbb{F}_q)$ as follows:

$$P \cdot D = PDP^{-1}.$$

By Lemma 3.2.16, the set of matrices conjugate to A has the same characteristic and minimal polynomial. Since $\mathrm{char}(A)$ is irreducible over $\mathbb{F}_q$, $\mathrm{char}(A)$ is the same as the minimal polynomial of A. Consequently, $B \in \mathrm{SL}_n(\mathbb{F}_q)$ is in the orbit of A if and only if char(B) = char(A). To calculate $|G_A|$, we begin by computing the order of the orbit and then apply the Orbit-Stabilizer theorem. We use the following result from [53] to compute the size of Orb(A). Let M_n denote the set of all matrices with entries in $\mathbb{F}_q$.

Theorem 1 , [53]. *Let $f(x) \in \mathbb{F}_q(x)$ be an irreducible polynomial of degree n. Then, the number of matrices in M_n with characteristic polynomial f is $\prod_{i=1}^{n-1}(q^n - q^i)$.*

Therefore, $|\text{Orb}(A)| = \prod_{i=1}^{n-1}(q^n - q^i)$. From Lemma 3.2.5, $|\text{SL}_n(\mathbb{F}_q)| = \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i)$. Then, by the Orbit-Stabilizer Theorem, for $n = 2, 3$

$$G_A = \text{Stab}(A) = \frac{|\text{SL}_n(\mathbb{F}_q)|}{|\text{Orb}(A)|} = \frac{\prod_{i=1}^{n-1}(q^n - q^i)}{\frac{\prod_{i=0}^{n-1}(q^n - q^i)}{q-1}} = \frac{q^n - 1}{q - 1.}$$

Therefore, the result follows. $\square$

Corollary 3.2.18. *Let $A \in \text{SL}_n(\mathbb{F}_q)$ be such that* char(A) *is an irreducible polynomial over $\mathbb{F}_q$ for $n = 2, 3$. If G_A is the number of matrices that commute with A, then*

$$|G_A| = \begin{cases} q + 1 & \textit{when } n = 2 \\ q^2 + q + 1 & \textit{when } n = 3. \end{cases}$$

Proof. By definition, [see 3.2.3], $G_A = \{P \mid PAP^{-1} = A\} = \{P \mid PA = AP\}$. Therefore, $G_A \subseteq \text{SL}_n(\mathbb{F}_q)$ is the set of all matrices that commute with A. The size of G_A can be calculated from the previous lemma. $\square$

Definition 3.2.4 (Splitting field of a polynomial, [17])**.** Let F be a field and $f(x) \in F$. An extension field K of F is called a splitting field for the polynomial $f(x) \in F[x]$ if $f(x)$

factors completely into linear factors (or split completely) in $K[x]$ and $f(x)$ does not factor completely into linear factors over any proper subfield of K containing F.

We will use the following proposition from [17], Section 13.5, Proposition 37, page 549 repeatedly in this chapter.

Proposition 3.2.19 ([17], Proposition 37)**.** *Every irreducible polynomial over a finite field $\mathbb{F}$ is separable. A polynomial in $\mathbb{F}[x]$ is separable if and only if it is the product of distinct irreducible polynomials in $\mathbb{F}[x]$.*

Lemma 3.2.20. *Let $A \in \mathrm{SL}_3(\mathbb{F}_q)$ and $\mathrm{char}(A) = (x-a)(x^2+sx-\frac{1}{a})$ be such that $(x^2+sx+\frac{1}{a})$ is irreducible over $\mathbb{F}_q$. Then if $B \in \mathrm{SL}_2(\mathbb{F}_q)$ is such that $AB = BA$, then $\mathrm{char}(B) = (x-b)(x^2+tx-\frac{1}{b})$ such that $(x^2+tx-\frac{1}{b})$ is irreducible over $\mathbb{F}_q$ or $\mathrm{char}(B) = (x-d)(x-c)(x-c)$ where $c, d \in \mathbb{F}_q$.*

Proof. Let $A \in \mathrm{SL}_3(\mathbb{F}_q)$ be such that $\mathrm{char}(A) = (x-a)(x^2+sx-\frac{1}{a})$ where $x^2+sx+\frac{1}{a}$ is irreducible over $\mathbb{F}_q$. By Proposition 3.2.19, $(x^2+sx+\frac{1}{a})$ has distinct roots over a splitting field. Therefore, $(x^2+sx+\frac{1}{a}) = (x-a)(x-a_1)(x-a_2)$ over a splitting field of $(x^2+tx-\frac{1}{b})$, such that $a \in \mathbb{F}_q$, $a_1 \neq a_2$ and $a_1, a_2 \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$. Let W_a, W_{a_1} and W_{a_2} denote the corresponding eigenspaces one-dimensional eigenspaces. If $AB = BA$, B preserves W_a , W_{a_1} and W_{a_2} by Lemma 3.2.12. Therefore, $\mathrm{char}(B)$ cannot be irreducible over $\mathbb{F}_q$. Clearly, if B is central, B commutes with A. By Lemma 3.2.12, B preserves the eigenspaces of A. Therefore, B shares common eigenvectors with A. Since $A \in \mathrm{SL}_3(\mathbb{F}_q)$ and $a \in \mathbb{F}_q$, note that $W_a \in \mathbb{F}_q^3$. Similarly, since $a_1, a_2 \in \overline{\mathbb{F}}_q$, and $A \in \mathrm{SL}_3(\mathbb{F}_q)$, eigenvector of $a_i \notin \mathbb{F}_q^3$ for $i = 1, 2$. Therefore, $\mathrm{char}(B) \neq (x-c_1)(x-c_2)(x-c_3)$ where $c_1 \neq c_2 \neq c_3$ since this would imply that A preserve the eigenspaces W_{c_1}, W_{c_2} and W_{c_3} which is a contradiction. $\square$

3.2.1 $\mathrm{SL}_2(\mathbb{F}_q)$ - character varieties of $\mathbb{Z}^r$

First, we recall the following corollary of Lemma 3.2.5.

Corollary 3.2.21. *The following are true:*

1. $|\mathrm{GL}_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)$

2. $|\mathrm{SL}_2(\mathbb{F}_q)| = \frac{1}{(q-1)}(q^2-1)(q^2-q) = q^3 - q$

3. $|\mathcal{D}(\mathrm{GL}_2(\mathbb{F}_q))| = (q-1)^2$

4. $|\mathcal{D}(\mathrm{SL}_2(\mathbb{F}_q))| = (q-1)$.

Our first goal is to count the number of simultaneously diagonalizable r tuples of matrices in $\mathrm{SL}_2(\mathbb{F}_q)^r$. Before counting, we make few observations.

1. There are two ways by which a tuple is simultaneously diagonalizable. The tuple can be diagonalized by a matrix in $\mathrm{SL}_2(\mathbb{F}_q)$ or it could be diagonalizable over an extension field, say $\mathrm{SL}_2(\overline{\mathbb{F}}_q)$.

2. The characteristic polynomial defines a matrix in $\mathrm{SL}_2(\mathbb{F}_q)$ upto conjugation.

3. For $A \in \mathrm{SL}_2(\mathbb{F}_q)$, since $\det(A) = 1$, the characteristic polynomial of A, $\mathrm{char}(A)$, is of the form $x^2 + ax + 1$ where $a = \mathrm{tr}(A)$.

Keeping these in mind, we begin by counting polynomials with constant term one over $\mathbb{F}_q$.

Counting Characteristic polynomials

Lemma 3.2.22. *Let $\mathbb{F}_q$ be a finite field with $q = p^k$ elements where p is odd. Suppose $p(x)$ is a monic degree two polynomial over $\mathbb{F}_q$ with constant term one. Then the following are true:*

1. *The number of polynomials with repeated roots is* 2.

2. *The number of polynomials with distinct roots is* $\frac{q-3}{2}$.

3. *The number of polynomials that are irreducible over $\mathbb{F}_q$ is* $\frac{q-1}{2}$.

Proof. Let $p(x)$ be an irreducible degree two monic polynomials with constant term one i.e., $p(x) = x^2 + ax + 1$ for $a \in \mathbb{F}_q$. Note that $p(x)$ is completely determined by a and there are exactly q choices for a.

Case 1: $p(x) = (x - \lambda)(x - \lambda)$

Note that $\lambda^2 = 1$. Therefore, by Lemma 3.2.2, number of choices for λ is:

$$\begin{cases} 2 : \text{if p is odd} \\ 1 : \text{if p is even.} \end{cases}$$

Case 2: $p(x) = (x - \lambda)(x - \frac{1}{\lambda})$ where $\lambda \neq \frac{1}{\lambda}$.

Since λ is invertible, $\lambda \neq 0$. Therefore, there are $(q - 1)$ choices for λ. To get the count when $\lambda \neq \frac{1}{\lambda}$ we discount the previous case where $\lambda = \frac{1}{\lambda}$. Since this results in choosing λ and $1/\lambda$ twice, we divide by two to get the number of distinct polynomials.

$$\begin{cases} \frac{q-3}{2} : \text{p is odd} \\ \frac{q-2}{2} : \text{p is even.} \end{cases}$$

Case 3: $p(x)$ is irreducible ($\lambda \in \overline{\mathbb{F}}_q$).

Recall that there are q degree two monic polynomials with constant term one. So, we subtract the number of reducible polynomials to obtain the number of irreducible degree three polynomials.

$$\text{When } p \text{ is odd} : q - \left(\frac{q-3}{2} - 2\right) = \frac{q-1}{2}$$

$$\text{When } p \text{ is even} : q - \left(\frac{q-2}{2} - 2\right) = \frac{q}{2}.$$

$\square$

Stratification

Now we classify the set of diagonal matrices, $\mathcal{D}(\mathrm{SL}_2(\overline{\mathbb{F}}_q))^r$.

$$
\begin{aligned}
\text{Reducible tuples: } \mathcal{D}_1^r(\mathrm{SL}_2(\mathbb{F}_q)) &:= \{(D_1, \dots, D_r) \mid \text{ there exists } i \text{ such that} \\
&\quad D_i \text{ is not scalar, for } 1 \leq i \leq r\}. \\
\text{Central tuples: } \mathcal{D}_2^r(\mathrm{SL}_2(\mathbb{F}_q)) &:= \{(D_1, \dots, D_r) \mid \ D_i \text{ is scalar} \\
&\quad \text{for all } i \in \{1, \dots, r\}\}. \\
\text{Irreducible tuples: } \overline{\mathcal{D}}_2^r(\mathrm{SL}_2(\mathbb{F}_q)) &:= \{(D_1, \dots, D_r) \mid \text{ there exists } i \in \{1, \dots, r\} \\
&\quad \text{such that } \mathrm{char}(D_i) \text{ is irreducible over } \mathbb{F}_q\}.
\end{aligned}
$$

For simplicity, we are dropping the symbol $\mathrm{SL}_2(\mathbb{F}_q)$ throughout this subsection when it is clear from the context. We use the above to define the strata as follows:

$$
\begin{aligned}
\text{Reducible Stratum: } \mathcal{T}^r_{\mathcal{D}_1} &:= \{(A_1, ..., A_r) \in \mathrm{SL}_2(\mathbb{F}_q)^r \mid \text{there exists } P \in \mathrm{GL}_2(\overline{\mathbb{F}}_q) \\
&\quad \text{such that } (PA_1P^{-1}, ..., PA_rP^{-1}) \in \mathcal{D}_1^r\}. \\
\text{Central Stratum: } \mathcal{T}^r_{\mathcal{D}_2} &:= \{(A_1, ..., A_r) \in \mathrm{SL}_2(\mathbb{F}_q)^r \mid \text{there exists } P \in \mathrm{GL}_2(\overline{\mathbb{F}}_q) \\
&\quad \text{such that } (PA_1P^{-1}, ..., PA_rP^{-1}) \in \mathcal{D}_2^r\}. \\
\text{Irreducible Stratum: } \mathcal{T}^r_{\overline{\mathcal{D}}_2} &:= \{(A_1, ..., A_r) \in \mathrm{SL}_2(\mathbb{F}_q)^r \mid \text{there exists } P \in \mathrm{GL}_2(\overline{\mathbb{F}}_q) \\
&\quad \text{such that } (PA_1P^{-1}, ..., PA_rP^{-1}) \in \overline{\mathcal{D}}_2^r\}.
\end{aligned}
$$

Remark 16. Upto simultaneous permutation of diagonal entries, each diagonal tuple, $(D_1, \dots, D_r) \in \mathcal{D}(\mathrm{SL}_2(\mathbb{F}_q))^r$ represents a unique equivalence class of simultaneously diagonalizable r-tuple of matrices. Therefore, to count the number of polystable orbits in

$\mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_2(\mathbb{F}_q))$, it suffices to count $|\mathcal{D}(\mathrm{SL}_2(\mathbb{F}_q))^r|$.

Counting Orbits

Theorem 3.2.23. *Let $\mathcal{D}_1^r, \mathcal{D}_2^r$ and $\overline{\mathcal{D}_2^r}$ be as defined above. Then the size of each set is given by the following.*

1. $|\mathcal{D}_1^r| = \begin{cases} 2^r \text{ when } p \text{ is odd} \\ 1^r \text{ when } p \text{ is even} \end{cases}$

2. $|\mathcal{D}_2^r| = \begin{cases} \frac{(q-1)^r - 2^r}{2} \text{ when } p \text{ is odd} \\ \frac{(q-1)^r - 1^r}{2} \text{ when } p \text{ is even} \end{cases}$

3. $|\overline{\mathcal{D}_2^r}| = \begin{cases} \frac{(q+1)^r - 2^r}{2} \text{ when } p \text{ is odd} \\ \frac{(q+1)^r - 1^r}{2} \text{ when } p \text{ is even .} \end{cases}$

Proof. 1. Central stratum

Let $A \in \mathrm{SL}_2(\mathbb{F}_q)$ be central i.e., $AP = PA$ for all $P \in \mathrm{SL}_2(\overline{\mathbb{F}}_q)$. Therefore, $PAP^{-1} = A$ for all P. Consequently, $G_A = \mathrm{SL}_2(\mathbb{F}_q)$ and the orbit of A under conjugation consists of the single element, A . From Lemma 3.2.2, we have the following count of the central elements and hence that of the central stratum.

$$|\mathcal{D}_2^r| = \begin{cases} 2^r \text{ when } p \text{ is odd} \\ 1^r \text{ when } p \text{ is even .} \end{cases}$$

2. Reducible Stratum

Let $(A_1, \ldots, A_r) \in \mathcal{T}_{\mathcal{D}_2}$. Then there exists k such that A_k is not diagonalizable to a central element. By Corollary 3.2.10, $G_{D_k} = \mathcal{D}(\mathrm{SL}_2(\mathbb{F}_q))$, the set of diagonal matrices in $\mathrm{SL}_2(\mathbb{F}_q)$. By Lemma 3.2.11, $\mathrm{Stab}((A_1,\ldots,A_r)) = G_{A_1}\cap\ldots\cap G_{A_r}$ the set of diagonal matrices. Note that each element in $\mathcal{D}_2^r$ contributes to one orbit and exactly one orbit in $\mathcal{T}_{\mathcal{D}_2}$ since any element in $\mathcal{D}_2^r$ has no non-trivial permutations possible. To compute the size of $\mathcal{D}_2^r$, it suffices to count all the diagonal tuples in $\mathrm{SL}_2(\mathbb{F}_q)$ and then subtract the number of central elements. From Lemma 3.2.5, the number of diagonal elements in $\mathrm{SL}_2(\mathbb{F}_q)$ is $q-1$. Consequently, the number of tuples of diagonal elements in $\mathrm{SL}_2(\mathbb{F}_q)$ is $\mathcal{D}_1^r \cup \mathcal{D}_2^r = (q-1)^r$. Since $\mathcal{D}_1^r$ and $\mathcal{D}_2^r$ are disjoint by definition, it follows that

$$|\mathcal{D}_2^r| = (q-1)^r - |\mathcal{D}_1^r| = (q-1)^r - 2^r.$$

To obtain the number of distinct orbits we divide by the number of simultaneous permutations. Note that at least for some entry A_k of $(A_1,\ldots,A_r)$, there are two permutations possible that provides a distinct element in $\mathcal{D}_1^r$. So dividing by two, we get that the number of distinct orbits as follows:

$$|\mathcal{D}_1^r| = \begin{cases} \frac{(q-1)^r-2^r}{2} \text{ when } p \text{ is odd} \\ \frac{(q-1)^r-1^r}{2} \text{ when } p \text{ is even }. \end{cases}$$

3. Irreducible Stratum

   Suppose $(D_1,\ldots,D_r) \in \overline{\mathcal{D}_1^r}$. Then there exists $k \in \{1,\ldots,r\}$ such that D_k has eigenvalues in $\mathbb{F}_q \setminus \mathbb{F}_q$. Then by Lemma 3.2.15, D_i has an irreducible characteristic polynomial or is scalar. First we calculate the number of matrices with irreducible degree two polynomials. By Lemma 3.2.22, we know that the number of irreducible degree two polynomials is

$$\begin{cases} \frac{q-1}{2} \text{ when } p \text{ is odd} \\ \frac{q}{2} \text{ when } p \text{ is even.} \end{cases}$$

Since for each such polynomial, we have two distinct diagonal matrices possible by permuting the diagonal entries, it follows that there are $(q-1)$ such matrices possible. By adding the number of central elements in each case, we obtain that there are $q+1$ and $q+2$ choices possible respectively when p is odd and p is even. Finally, we subtract the central elements to obtain the desired count:

$$|\overline{\mathcal{D}}_1^r| = \begin{cases} \frac{(q+1)^r-2^r}{2} \text{ when } p \text{ is odd} \\ \frac{(q+1)^r-1^r}{2} \text{ when } p \text{ is even }. \end{cases}$$

□

Corollary 3.2.24. *The E-polynomial of the* $\mathrm{SL}_2(\mathbb{F}_q)$ *character variety of free abelian group of rank r, $\mathbb{Z}^r$ is* $\frac{(q+1)^r}{2} + \frac{(q-1)^r}{2}$.

Proof. We can obtain the E-polynomial of the $\mathrm{SL}_2(\mathbb{F}_q)$ character variety by computing the cardinality of polystable orbit space. Since we calculated the number of polystable orbits in each stratum, the total number of orbits is obtained as follows

$$\begin{aligned} \frac{(q+1)^r-2^r}{2} + \frac{(q-1)^r-2^r}{2} + 2^r &= \frac{(q+1)^r}{2} + \frac{(q-1)^r}{2} \text{ when } p \text{ is odd} \\ \frac{(q+1)^r-1^r}{2} + \frac{(q-1)^r-1^r}{2} + 1^r &= \frac{(q+1)^r}{2} + \frac{(q-1)^r}{2} \text{ when } p \text{ is even }. \end{aligned}$$

Therefore, the E-polynomial is $\frac{(q+1)^r}{2} + \frac{(q-1)^r}{2}$. □

Remark 17. This agrees with the result in [11] by Cavazos and Lawton.

3.2.2 $\mathrm{SL}_3(\mathbb{F}_q)$ - character varieties of $\mathbb{Z}^r$

As in the case when $n = 2$, the following result follows from Lemma 3.2.5.

Corollary 3.2.25. *The following are true:*

1. $|\mathrm{GL}_3(\mathbb{F}_q)| = (q^3-1)(q^3-q)(q^3-q^2)$

2. $|\mathrm{SL}_3(\mathbb{F}_q)| = \frac{1}{(q-1)}(q^3-1)(q^3-q)(q^3-q^2)$

3. $|\mathcal{D}(\mathrm{GL}_3(\mathbb{F}_q))| = (q-1)^3$

4. $|\mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))| = (q-1)^2$.

Counting Characteristic Polynomials

Before counting degree three monic polynomials with constant term one over $\mathbb{F}_q$, we make a few useful observations. Let $p(x)$ be a degree three monic polynomial over $\mathbb{F}_q$. Note that there are three major types of polynomials over finite fields:

1. *Completely reducible over the base field* (all roots are in $\mathbb{F}_q$)

   If $p(x)$ is completely reducible over $\mathbb{F}_q$, then there are three different cases possible for its roots:

   (a) three repeated roots

   (b) exactly two repeated roots

   (c) three distinct roots.

   Throughout this section, we use the term completely reducible to indicate matrices with $p(x)$ as characteristic polynomial.

2. *Irreducible over the base field* (no roots in $\mathbb{F}_q$)

   Recall that all irreducible polynomials over finite fields are separable [refer Proposition 3.2.19] . Therefore, if $p(x)$ is irreducible, then all the roots are distinct.

3. *Partially reducible over the base field* (only some roots are in the base field)

   If $p(x)$ is partially reducible, then all the roots are distinct and exactly one of them will be in $\mathbb{F}_q$. Note that it is not possible to have exactly two roots in the base field since it would imply that the third root calculated as the inverse of the product of other two roots is also in the base field.

Remark: We can further classify these polynomials based on the multiplicities of the roots which we will do later.

We prove the following known result before proceeding to count each of the above mentioned types.

Lemma 3.2.26. *The number of irreducible monic polynomials of degree two over* $\mathbb{F}_q$ *is* $\frac{q^2-q}{2}$.

Proof. Let $p(x) = x^2 + bx + c$ be a degree two monic polynomial over $\mathbb{F}_q$, that is $b, c \in \mathbb{F}_q$. Then there are q^2 such polynomials since there are q choices for both b and c. Then $p(x)$ is either reducible or irreducible over $\mathbb{F}_q$. If $p(x)$ is reducible, then $p(x) = (x - \mu_1)(x - \mu_2)$ where $\mu_1, \mu_2 \in \mathbb{F}_q$. Then we have two different cases, $\mu_1 \neq \mu_2$ and $\mu_1 = \mu_2$.

$\mu_1 \neq \mu_2$: This is exactly the same as choosing two elements μ_1, μ_2 from $\mathbb{F}_q$ out of the q elements. Therefore, the number of such possibilities is $\binom{q}{2} = \frac{q^2-q}{2}$.

$\mu_1 = \mu_2$: For each $a \in \mathbb{F}_q$, we have the polynomial $(x - a)(x - a)$ and these are exactly all the reducible polynomials over $\mathbb{F}_q$. Hence, there are q such polynomials.

Therefore, the total number of reducible polynomials is the sum of the above two cases which can be calculated as

$$\frac{q^2 - q}{2} + q = \frac{q^2 + q}{2}. \tag{3.2}$$

Thus, there are $\frac{q^2+q}{2}$ reducible polynomials. Subtracting this from the total number of degree two monic polynomials gives us the desired number

$$q^2 - \frac{q^2 + q}{2} = \frac{q^2 - q}{2}. \tag{3.3}$$

□

Theorem 3.2.27. *We have the following count for monic polynomials of degree three with constant term one over $\mathbb{F}_q$ where $q = p^k$:*

1. *Number of reducible ones with three repeated roots is*

$$\begin{cases} 3 & \textit{if } p \equiv 1 \mod 3 \quad \textit{or} \quad p \equiv -1 \mod 3 \textit{ and } k \textit{ is even} \\ 1 & \textit{if } p \equiv 0 \mod 3 \quad \textit{or} \quad p \equiv -1 \mod 3 \textit{ and } k \textit{ is odd.} \end{cases}$$

2. *Number of reducible ones with exactly two repeated roots is*

$$\begin{cases} (q-4) & \textit{if } p \equiv 1 \mod 3 \quad \textit{or} \quad p \equiv -1 \mod 3 \textit{ and } k \textit{ is even} \\ (q-2) & \textit{if } p \equiv 0 \mod 3 \quad \textit{or} \quad p \equiv -1 \mod 3 \textit{ and } k \textit{ is odd.} \end{cases}$$

3. *Number of reducible ones with three distinct roots is*

$$\begin{cases} \frac{q^2-5q+10}{6} & \textit{if } p \equiv 1 \mod 3 \quad \textit{or} \quad p \equiv -1 \mod 3 \textit{ and } k \textit{ is even} \\ \frac{(q-3)(q-2)}{6} & \textit{if } p \equiv 0 \mod 3 \quad \textit{or} \quad p \equiv -1 \mod 3 \textit{ and } k \textit{ is odd .} \end{cases}$$

4. *Number of polynomials with exactly one root in the base field is $\frac{q^2-q}{2}$.*

5. *Number of irreducible degree three polynomials with constant term one is:*

$$\begin{cases} \frac{q^2+q-2}{3} & \textit{if } p \equiv 1 \mod 3 \quad \textit{or} \quad p \equiv -1 \mod 3 \textit{ and } k \textit{ is even} \\ \frac{q^2+q}{3} & \textit{if } p \equiv 0 \mod 3 \quad \textit{or} \quad p \equiv -1 \mod 3 \textit{ and } k \textit{ is odd.} \end{cases}$$

Proof. Let $p(x) = x^3 + ax^2 + bx - 1$. Since there are q choices each for a and b, there are

q^2 polynomials of degree three with constant term one. We classify and count them below based on the multiplicity of roots.

1. If $p(x) = (x-a)(x-a)(x-a)$, then $a^3 = 1$ which implies a is a cube root of unity. Conversely for any cubic root of unity, λ, $(x-\lambda)^3$ is such a polynomial. So it suffices to count the cube roots of unity. From Lemma 3.2.2, we get that the number of cube roots of unity is $\gcd(3, q-1)$. Note that $3|(q-1)$ iff $(q-1) \equiv 0 \mod 3$ which is true if and only if $q \equiv 1 \mod 3$. Since $q = p^k$,

$$\begin{aligned} p \equiv 0 \mod 3 \quad &\text{implies} \quad q \equiv 0 \mod 3 \text{ for } k \geq 1 \\ p \equiv 1 \mod 3 \quad &\text{implies} \quad q \equiv 1 \mod 3 \text{ for } k \geq 1 \\ p \equiv -1 \mod 3 \quad &\text{implies} \quad q \equiv (-1)^k \mod 3 \text{ for } k \geq 1. \end{aligned}$$

   Therefore, $\gcd(3, (q-1)) = 3$ iff $q \equiv 1 \mod 3$ or $q \equiv -1 \mod 3$ and k is even. Hence the result follows.

2. If $p(x)$ has exactly two roots, then $p(x) = (x-a)(x-a)(x-1/a)$ where $1/a \neq a$. Therefore, $p(x)$ is completely determined by the choice of a. Note that $a \neq 0$. Out of the $(q-1)$ choices for a we only need to discount the case when $a = 1/a$. But $a = 1/a$ if and only if $a^3 = 1$. Hence, after subtracting the number of cubic roots of unity from part one, we get the result,

$$\begin{cases} (q-1)-3 = (q-4) & \text{if } p \equiv 1 \mod 3 \quad \text{or} \quad p \equiv -1 \mod 3 \text{ and } k \text{ is even} \\ (q-1)-1 = (q-2) & \text{if } p \equiv 0 \mod 3 \quad \text{or} \quad p \equiv -1 \mod 3 \text{ and } k \text{ is odd.} \end{cases}$$

3. Suppose $p(x)$ has three distinct roots. Then $p(x) = (x-a)(x-b)(x-1/(ab))$ where $a \neq b \neq 1/(ab)$. There are $(q-1)$ choices for a and $(q-2)$ choices for b. But this includes the cases where $a = 1/ab$ and $b = 1/ab$. Note that this is exactly twice the

count from part two. In addition, since any permutation of a, b and $1/ab$results in the same polynomial $p(x)$, we divide by 3! to get the final count. Therefore, the number of irreducible polynomials is

$$\begin{cases} ((q-1)(q-2)-2(q-4))\frac{1}{6} = \frac{q^2-5q+10}{6} & \text{if } p \equiv 1 \mod 3 \\ & \text{or } p \equiv -1 \mod 3 \text{ and } k \text{ is even} \\ ((q-1)(q-2)-2(q-2))\frac{1}{6} = \frac{q^2-5q+6}{6} & \text{if } p \equiv 0 \mod 3 \\ & \text{or } p \equiv -1 \mod 3 \text{ and } k \text{ is odd} . \end{cases}$$

4. Suppose $p(x)$ has exactly one root in $\mathbb{F}_q$. Then $p(x) = (x^2 + ax + b)(x - 1/b)$ where $x^2 + ax + b$ is an irreducible degree two polynomial. By Lemma 3.2.26, there are exactly $\frac{q^2-q}{2}$ such polynomials. Thus, the result follows.

5. Since the total number of polynomials possible is q^2, to get the number of irreducible polynomials, we subtract the sum of the rest of the cases from q^2. When $p \equiv 1 \mod 3$ or $p \equiv -1 \mod 3$ and k is even, we have

$$q^2 - \left(\frac{q^2-5q+10}{6}\right) - (q-4) - 3 - \left(\frac{q^2-q}{2}\right) = \frac{q^2+q-2}{3}.$$

If $p \equiv 0 \mod 3$ or $p \equiv -1 \mod 3$ and k is odd, then

$$q^2 - \left(\frac{q^2-5q+6}{6}\right) - (q-2) - 1 - \left(\frac{q^2-q}{2}\right) = \frac{q^2+q}{3}.$$

This concludes the proof.

Stratification

Recall the action of $\mathrm{SL}_3(\overline{\mathbb{F}}_q)$ on $\mathrm{SL}_3(\overline{\mathbb{F}}_q)^r$ by simultaneous conjugation. We look at the stabilizer of this action in $\mathrm{SL}_3(\mathbb{F}_q)$. We use the notation $\mathrm{Stab}((A_1,\ldots,A_r))_{\mathrm{SL}_3(\mathbb{F}_q)}$ to denote $\mathrm{Stab}((A_1,\ldots,A_r)) \cap \mathrm{SL}_3(\mathbb{F}_q)$. The following lemma characterizes the types of stabilizer subgroups of $\mathrm{SL}_3(\mathbb{F}_q)$ under its action on $\mathrm{SL}_3(\mathbb{F}_q)^r$.

Lemma 3.2.28. *Let $(A_1,\ldots,A_r)$ be a tuple in $\mathrm{SL}_3(\mathbb{F}_q)^r$ that is simultaneously diagonalizable to $(D_1,\ldots,D_r) \in \mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))^r$, the set of all r-tuples of diagonal matrices in $\mathrm{SL}_3(\mathbb{F}_q)^r$. Then there are three different stabilizer types under the simultaneous conjugation action. They are as follows:*

1. *If D_i is scalar for all $1 \leq i \leq r$, then $\mathrm{Stab}((A_1,\ldots,A_r))_{\mathrm{SL}_3(\mathbb{F}_q)} = \mathrm{SL}_3(\mathbb{F}_q)$, the whole group .*

2. *If there exists at least one D_i such that all the entries of D_i are distinct, then $\mathrm{Stab}((A_1,\ldots,A_r)) = \mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))$, the set of diagonal matrices.*

3. *Let d_{i_k} denote the k^{th} row entry of the matrix D_i. If there exists exactly one pair $s,t \in \{1,2,3\}$ such that $d_{i_s} = d_{i_t}$ for all $1 \leq i \leq r$, that is, same two rows have repeated entries for all coordinates D_i and not all D_i is scalar, then*

$$\begin{aligned} |\mathrm{Stab}((A_1,\ldots,A_r))_{\mathrm{SL}_3(\mathbb{F}_q)}| &= |\{B=[b_{xy}] \mid b_{xx}, b_{i_s i_t}, b_{i_t i_s} \in \mathbb{F}_q \\ &\qquad \textit{and } b_{xy} = 0 \textit{ for all other entries}\}|. \end{aligned}$$

4. *Suppose D_k doesn't have any distinct entries for all k, $1 \leq k \leq r$. Now, if there exists distinct i,j such that D_i and D_i both has two repeated entries but at different rows, i.e., $d_{i_s} = d_{i_t}$ and $d_{j_x} = d_{j_y}$ but $\{i_s, i_t\} \neq \{j_x, j_y\}$, then $\mathrm{Stab}((A_1,\ldots,A_r)) = \mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))$, the set of diagonal matrices.*

Proof. We use Lemma 3.2.9 and Lemma 3.2.11 repeatedly to prove this result.

1. Since the central elements, D_i commute with all the elements of the group for all $1 \leq i \leq r$, the result follows from Lemma 3.2.11.

2. Suppose there exists i such that D_i has distinct diagonal entries. Then, by Corollary 3.2.10, $G_{D_i} = \mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))$. Then for $j \neq i$, there are two possibilities:

   1. If the entries of D_j are distinct, then $G_{D_j} = \mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))$.

   2. If D_j has repeated entries in which case $G_{D_j} \supseteq G_{D_i}$ by Corollary 3.2.10.

   Hence, $\mathrm{Stab}((D_1, \ldots, D_r)) = G_{D_1} \cap \ldots \cap G_{D_r} = G_{D_i} = \mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))$ by Lemma 3.2.11. Therefore, $\mathrm{Stab}((D_1, \ldots, D_r)) = \mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))$.

   Note that here $\mathrm{Stab}((A_1, \ldots, A_r)) = \mathrm{Stab}((D_1, \ldots, D_r))$ since $\mathcal{D}(\mathrm{SL}_3(F_q))$ is a normal subgroup of $\mathrm{SL}_3(\mathbb{F}_q)$.

3. Suppose there exists at least one i such that A_i has exactly two repeated eigenvalues. We fix this i throughout this proof. Then A_i is diagonalizable to D_i with exactly two repeated diagonal entries, say $d_{i_s} = d_{i_t}$ for all i, where $1 \leq i \leq r$. By Lemma 3.2.9, $BD_i = D_iB$ implies $B = [b_{xy}]$ where $b_{xx}, b_{i_ti_s}, b_{i_si_t} \in \mathbb{F}_q$ and $b_{xy} = 0$ otherwise. Let A_j be such that $1 \leq j \leq r$ and $j \neq i$, then there are two possibilities for A_j. In the first case, A_j has two exactly two repeated eigenvalues and will be diagonalizable to D_j with exactly two repeated entries, $d_{j_s} = d_{j_t}$. Then $G_{D_j} = G_{D_i}$ by the same explanation above. This implies $G_{D_i} \cap G_{D_j} = G_{D_i}$. The second possibility is that D_j is scalar. Then $G_{D_j} = \mathrm{SL}_3(\mathbb{F}_q)$. Consequently, $G_{D_i} \cap G_{D_j} = G_{D_i}$. Thus in both cases,

$$\begin{aligned} \mathrm{Stab}((D_1, \ldots, D_r))_{\mathrm{SL}_3(\mathbb{F}_q)} &= G_{D_1} \cap \cdots \cap G_{D_r} = G_{D_i} \\ &= \{B = [b_{xy}] \mid b_{xx}, b_{i_ti_s}, b_{i_si_t} \in \mathbb{F}_q \text{ and } b_{xy} = 0 \text{ otherwise}\}. \end{aligned}$$

   Since $|\mathrm{Stab}((D_1, \ldots, D_r))_{\mathrm{SL}_3(\mathbb{F}_q)}| = |\mathrm{Stab}((A_1, \ldots, A_r))_{\mathrm{SL}_3(\mathbb{F}_q)}|$, the result follows.

4. Suppose A_i has exactly two repeated eigenvalues such that D_i has two repeated entries $d_{i_s} = d_{i_t}$. Let A_j be such that D_j has repeated entries, $D_{j_k} = D_{j_l}$ where $\{i_s, i_t\} \neq$

$\{j_k, j_l\}$. Then as in the proof of part 3, by Lemma 3.2.9, we have the following

$$G_{D_i} = \left\{ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \middle| \; a_{xx}, a_{i_s i_t}, a_{i_t i_s} \in \Bbbk \text{ and } a_{xy} = 0 \text{ for all other entries} \right\}$$

$$G_{D_j} = \left\{ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \middle| \; a_{xx}, a_{j_k j_l}, a_{j_l j_k} \in \Bbbk \text{ and } a_{xy} = 0 \text{ for all other entries} \right\}$$

Since $\{i_s, i_t\} \neq \{j_k, j_l\}$,

$$G_{D_i} \cap G_{D_j} = \left\{ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \middle| \; a_{xx} \in \Bbbk \text{ and } a_{xy} = 0 \text{ for all other entries} \right\}$$

is the set of all diagonal matrices in $\mathrm{SL}_3(\mathbb{F}_q)$. Since $\mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q)) \subseteq G_{D_h}$ for all h, $1 \leq h \leq r$, it follows that $G_{D_1} \cap G_{D_2} \cdots G_{D_r} = \mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))$.

$\square$

Now we stratify the space, $\mathrm{Hom}^*(\mathbb{Z}^r, \mathrm{SL}_3(\mathbb{F}_q)) =$
$\{\rho \in \mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_3(\mathbb{F}_q)) \mid \mathrm{Orb}(\rho)_{\mathrm{SL}_3(\overline{\mathbb{F}}_q)} \text{ is Zariski closed in } \mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_3(\mathbb{F}_q))\}$ based on stabilizer type under the conjugation action and the field where the eigenvalues exist. Let $D_i \in \mathcal{D}(\mathrm{SL}_3(\overline{\mathbb{F}}_q))$ i.e., a diagonal matrix in $\mathrm{SL}_3(\overline{\mathbb{F}}_q)$.

1. Reducible tuples: $\mathcal{D}_1^r(\mathrm{SL}_3(\mathbb{F}_q)) := \{(D_1, \ldots, D_r) \mid$ there exists i such that D_i has distinct diagonal entries where $i \in \{1, \ldots r\}\}$

2. Repeating tuples: $\mathcal{D}_2^r(\mathrm{SL}_3(\mathbb{F}_q)) := \{(D_1, \ldots, D_r) \mid$ there exists i such that

D_i has exactly two distinct diagonal entries where $i \in \{1, \dots r\}\}$

3. Central tuples: $\mathcal{D}_3^r(\mathrm{SL}_3(\mathbb{F}_q)) := \{(D_1, \dots, D_r) \mid\ D_i$ is central for all $i \in \{1, \dots r\}\}$

4. Irreducible tuples: $\overline{\mathcal{D}}_3^r(\mathrm{SL}_3(\mathbb{F}_q)) := \{(D_1, \dots, D_r) \mid$ there exists $i \in \{1, \dots, r\}$ such that all entries of $D_i \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q\}$

5. Partially Reducible tuples: $\overline{\mathcal{D}}_3^r(\mathrm{SL}_3(\mathbb{F}_q)) := \{(D_1, \dots, D_r) \mid$ there exists $i \in \{1, \dots, r\}$ such that exactly two entries of $D_i \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q\}$

Since it is clear from the context, we drop the $\mathrm{SL}_3(\mathbb{F}_q)$ from the notation for tuples throughout the discussion in this section. Let $(A_1, ..., A_r) \in \mathrm{Hom}(\mathbb{Z}^r, \mathrm{SL}_3(\mathbb{F}_q))$. We then use define the following strata:

$$
\begin{aligned}
\text{1. Reducible Stratum: } \mathcal{T}_{\mathcal{D}_1}^r &:= \{(A_1, ..., A_r) \mid \text{there exists } P \in \mathrm{GL}_3(\overline{\mathbb{F}}_q) \\
&\qquad \text{such that } (PA_1P^{-1}, ..., PA_rP^{-1}) \in \mathcal{D}_1^r\}. \\
\text{2. Repeating Stratum: } \mathcal{T}_{\mathcal{D}_2}^r &:= \{(A_1, ..., A_r) \mid \text{there exists } P \in \mathrm{GL}_3(\overline{\mathbb{F}}_q) \\
&\qquad \text{such that } (PA_1P^{-1}, ..., PA_rP^{-1}) \in \mathcal{D}_2^r\}. \\
\text{3. Central Stratum: } \mathcal{T}_{\mathcal{D}_3}^r &:= \{(A_1, ..., A_r) \mid \text{there exists } P \in \mathrm{GL}_3(\overline{\mathbb{F}}_q) \\
&\qquad \text{such that } (PA_1P^{-1}, ..., PA_rP^{-1}) \in \mathcal{D}_3^r\} \\
\text{4. Irreducible Stratum: } \mathcal{T}_{\overline{\mathcal{D}}_3}^r &:= \{(A_1, ..., A_r) \mid \text{there exists } P \in \mathrm{GL}_3(\overline{\mathbb{F}}_q) \\
&\qquad \text{such that } (PA_1P^{-1}, ..., PA_rP^{-1}) \in \overline{\mathcal{D}}_3^r\} \\
\text{5. Partially Reducible Stratum: } \mathcal{T}_{\overline{\mathcal{D}}_{22}}^r &:= \{(A_1, ..., A_r) \mid \text{there exists } P \in \mathrm{GL}_3(\overline{\mathbb{F}}_q) \\
&\qquad \text{such that } (PA_1P^{-1}, ..., PA_rP^{-1}) \in \overline{\mathcal{D}}_2^r\}.
\end{aligned}
$$

$\square$

Weyl Group Action

Let $(D_1, \dots, D_r)$ be a tuple of diagonal matrices in $\mathrm{SL}_3(\overline{\mathbb{F}}_q)$ and suppose there exists $P \in \mathrm{GL}_3(\overline{\mathbb{F}}_q)$ such that $(PD_1P^{-1}, \dots, PD_rP^{-1}) = (A_1, \dots, A_r)$. Let $D = \begin{pmatrix} d_{11} & 0 & \\ 0 & d_{22} & 0 \\ 0 & 0 & d_{33} \end{pmatrix}$ be in $\mathrm{SL}_3(\overline{\mathbb{F}}_q)$. The number of possible permutations of D is given by the conjugation action of the Weyl group on the maximal torus

$$\mathcal{W} = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}.$$

Note that for $W_i \in \mathcal{W}$, $W_i D W_i^{-1}$ is just permutation of its entries. We classify below the elements of $\mathcal{D}_3^r$ based on number of distinct permutations possible under the action of $\mathcal{W}$.

Lemma 3.2.29. *Let $(A_1, \dots, A_r) \in \mathrm{SL}_3(\mathbb{F}_q)^r$ be diagonalizable to the tuple $(D_1, \dots, D_r) \in \mathrm{SL}_3(\mathbb{F}_q)^r$. Then the following are true.*

1. *If there exists i such that D_i has distinct entries, then all the six permutations of D_i and consequently that of $(D_1, \dots, D_r) \in \mathrm{SL}_3(\mathbb{F}_q)$ are distinct.*

2. *Suppose there exists i, j such that D_i and D_i both has two repeated entries but at different rows, i.e., $d_{i_s} = d_{i_t}$ and $d_{j_x} = d_{j_y}$ but $\{i_s, i_t\} \neq \{j_x, j_y\}$. Then, $(D_1, \dots, D_r)$ has six distinct permutations.*

3. *If D_i has two repeated entries at the same position, say $d_{i_s} = d_{i_t}$, and D_i is not scalar for all $1 \leq i \leq r$, then there are exactly three distinct permutations of $(D_1, \dots, D_r) \in \mathrm{SL}_3(\mathbb{F}_q)$.*

4. *If for all i, D_i is a scalar matrix, then $(D_1, \ldots, D_r) \in \mathrm{SL}_3(\mathbb{F}_q)$ has no distinct permutations.*

Proof. 1. Suppose $D_i = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix}$ where $d_1 \neq d_2 \neq d_3 \neq d_1$. Then for $W \in \mathcal{W}$, $WD_iW^{-1} = D_i$ if and only if W is identity since any other W permutes the rows of D. Consequently, $(WD_1W^{-1}, \ldots, WD_rW^{-1}) = (D_1, \ldots, D_r)$ if and only if W is the identity matrix.

2. Let D_i and D_j be such that $\{i_s, i_t\}$ denotes the rows of D_i with repeated entries and $\{j_x, j_y\}$ that of D_j and $\{i_s, i_t\} \neq \{j_x, j_y\}$. Since $\{i_s, i_t\}, \{j_x, j_y\} \subseteq \{1, 2, 3\}$, it follows that $\{i_s, i_t\} \cup \{j_x, j_y\} = \{1, 2, 3\}$. Let $W \neq I$. Then W permutes at least two rows, say u, v. If $u, v \in \{i_s, i_t\}$, i.e., W does not permute any elements in D_i, then since $\{i_s, i_t\} \neq \{j_x, j_y\}$, either $u \notin \{j_x, j_y\}$ or $v \notin \{j_x, j_y\}$. Since two distinct entries of D_j are permuted by W, it follows that $WD_jW^{-1} \neq D_j$. Consequently, $(WD_1W^{-1}, \ldots, WD_rW^{-1}) \neq (D_1, \ldots, D_r)$. Therefore, D has six distinct permutations.

3. WLOG, assume all the D_i has the following form. $D_i = \begin{pmatrix} d_i & 0 & 0 \\ 0 & d_i & 0 \\ 0 & 0 & \frac{1}{d_i^2} \end{pmatrix}$ such that $d_i \neq \frac{1}{d_i^2}$. Note that the position of $\frac{1}{d_i^2}$ is determined by that of the repeated entries. Therefore, it suffices to count number of distinct ways of choosing two rows to place the d_is. This is given exactly by $\binom{3}{2}$. Therefore, there are exactly 3 matrices in $\mathcal{W}$ such that $WD_iW^{-1} \neq D_i$. Since all the D_i has the same form, it follows that D has exactly three distinct simultaneous permutations by $\mathcal{W}$.

□

Lemma 3.2.30. *Let $A \in \mathrm{SL}_3(\mathbb{F}_q)$ be such that* $\mathrm{char}(A)$ *is not completely reducible over $\mathbb{F}_q$. If A is diagonalizable to $D \in \mathrm{SL}_3(\overline{\mathbb{F}}_q)$, then all the entries of D are distinct. Furthermore, let $(A_1, \ldots, A_r)$ be an element of the irreducible stratum such that $A_i = A$ for some i. Then $(A_1, \ldots, A_r)$ has exactly three distinct permutations if* $\mathrm{char}(A)$ *is irreducible.*

Proof. Suppose $D \in \mathrm{SL}_3(\overline{\mathbb{F}}_q) \backslash \mathrm{SL}_3(\mathbb{F}_q)$. Then there are two possibilities for the characteristic polynomial, $\mathrm{char}(D) = p(x) : (x-a)(x^2+bx+1/a)$ or x^3+ax^2+bx+1.

- $p(x) = x^3+ax^2+bx+1$: By Proposition 3.2.19, $p(x)$ is separable. Therefore, if $\mathrm{char}(D) = x^3+ax^2+bx+1$, then D has distinct entries.

- If $\mathrm{char}(D) = (x-a)(x^2+bx+1/a)$ such that $a \in \mathbb{F}_q$, then (x^2+bx+1/a) has two distinct roots say d_1, d_2. Since irreducible polynomials are separable over finite fields, $d_1 \neq d_2$. Clearly, $d_1, d_2 \neq a$ since $a \in \mathbb{F}_q$. Therefore, D has six distinct entries.

Now suppose $\mathrm{char}(A)$ is irreducible. We proceed to show that a tuple containing A has exactly three distinct permutations. From Lemma 3.2.17, the size of the set of matrices that commute with A, $|G_A|$ is q^2+q+1. Therefore, if $(A_1, \ldots, A_r)$ is such that $A_i = A$ for some A, then $A_j \in G_A$ for $1 \leq j \leq r$. By Lemma 3.2.15, any matrix A_j that commutes with A is either a central element or has irreducible characteristic polynomial. We know the number of central elements. Let m_3 denotes the number of permutations of A in $\mathrm{SL}_3(\mathbb{F}_q)$ and k denote the number of irreducible degree three polynomials. If d_3 denotes the number of central elements in $\mathrm{SL}_3(\mathbb{F}_q)$, then using Theorem 3.2.27,

$$m_3 = \frac{|G_A - d_3|}{k} = \begin{cases} \frac{q^2+q+1-3}{\frac{q^2+q-2}{3}} = 3 \text{ if } p \equiv 1 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is even} \\ \frac{q^2+q+1-1}{\frac{q^2+q}{3}} = 3; \text{ if } p \equiv 0 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is odd.} \end{cases}$$

□

We denote the center of a group G by $Z(G)$. In particular, $Z(\mathrm{GL}_2(\mathbb{F}_q))$ denotes the center of $\mathrm{GL}_2(\mathbb{F}_q)$, the set of scalar matrices with entries from $\mathbb{F}_q$. We use $\mathcal{D}(\mathrm{GL}_2(\overline{\mathbb{F}}_q \setminus \mathbb{F}_q))$ to denote the set of all two by two diagonal matrices such that the entries are strictly in the extension field $\overline{\mathbb{F}}_q$ but not in $\mathbb{F}_q$.

Lemma 3.2.31. *Let $A \in \mathrm{SL}_3(\mathbb{F}_q)$ and $\mathrm{char}(A) = p(x)(x-b)$ be such that $p(x) = (x^2 - ax + \frac{1}{b})$ is irreducible over $\mathbb{F}_q$. Then there is a bijective correspondence between the orbits in $\mathcal{T}^r_{D_{22}}$ and the set of commuting tuples in $(\mathcal{D}(\mathrm{GL}_2(\overline{\mathbb{F}}_q \setminus \mathbb{F}_q) \cup Z(\mathrm{GL}_2(\mathbb{F}_q)))^{\times r} \setminus Z(\mathrm{GL}_2(\mathbb{F}_q))^r$.*

Proof. Let $A_i \in \mathrm{SL}_3(\mathbb{F}_q)$ and $\mathrm{char}(A_i) = p(x)(x - \lambda_i)$ be such that $p(x) = (x^2 - ax + \frac{1}{\lambda_i})$ is irreducible over $\mathbb{F}_q$. Consider the tuple $A = (A_1, \ldots, A_r)$ such that $A_iA_j = A_jA_i$ for $1 \leq j \leq r$. By Lemma 3.2.20, $(A_1, \ldots, A_r)$ is simultaneously diagonalizable to a tuple $D = (D_1, \ldots, D_r) \in \mathrm{SL}_3(\mathbb{F}_q)^r$ of the following form up to simultaneous permutation.

$$\left(\begin{bmatrix} \lambda_{1_1} & 0 & 0 \\ 0 & \lambda_{1_2} & 0 \\ 0 & 0 & \lambda_1 \end{bmatrix}, \ldots, \begin{bmatrix} \lambda_{i_1} & 0 & 0 \\ 0 & \lambda_{i_2} & 0 \\ 0 & 0 & \lambda_i \end{bmatrix}, \ldots, \begin{bmatrix} \lambda_{r_1} & 0 & 0 \\ 0 & \lambda_{r_2} & 0 \\ 0 & 0 & \lambda_r \end{bmatrix} \right)$$

where $\lambda_j \in \mathbb{F}_q$ and $\lambda_{j_1}, \lambda_{j_2} \in \mathrm{SL}_2(\overline{\mathbb{F}}_q) \setminus \mathbb{F}_q$ for $1 \leq j \leq r$ or $\lambda_{j_1} = \lambda_{j_2} \in \mathbb{F}_q$ for $i \neq 2$. We choose the element $D = (D_1, \ldots, D_r)$ with the basefield entry in the third row to denote the orbit of $(A_1, \ldots, A_r)$. Note that for each D_j, the upper block $D'_j = \begin{pmatrix} \lambda_{j_1} & 0 \\ 0 & \lambda_{j_2} \end{pmatrix} \in \mathrm{GL}_2(\overline{\mathbb{F}}_q \setminus \mathbb{F}_q) \cup \mathbb{Z}(\mathrm{GL}_2(\mathbb{F}_q))$. The D'_j is unique up to permutation of entries for a fixed D_j. For the orbit of $[(A_1, \ldots, A_r)]$ denoted by $[D_1, \ldots, D_r]$ we define a map as explained below. Let $\mathcal{C} := (\mathcal{D}(\mathrm{GL}_2(\overline{\mathbb{F}}_q) \setminus \mathbb{F}_q) \cup Z(\mathrm{GL}_2(\mathbb{F}_q)))$ and

$$\mathcal{W}_2 := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}.$$

Recall that $\mathcal{C}^r/\mathcal{W}_2$ denote the orbits in $\mathcal{C}^r$ under the Weyl group action and $\mathcal{T}^r_{D_{22}}/G$ denote the set of conjugation orbits in the partially reducible stratum of $\mathrm{SL}_3(\mathbb{F}_q)^r$. Define the following map:

$$\begin{aligned} \Phi : \mathcal{T}_{\mathcal{D}_{22}}/G &\longrightarrow \mathcal{C}^r \setminus Z(\mathrm{GL}_2(\mathbb{F}_q)^r) \\ (D_1, \ldots, D_r) &\longmapsto (D'_1, \ldots, D'_r) \end{aligned}$$

The map is clearly well defined. Suppose $(D'_1, \ldots, D'_r) = (C'_1, \ldots, C'_r)$. Then, by definition D'_j and C'_j are permutations of each other which implies these are in the same Weyl group orbit of $\mathcal{T}_{\overline{D}_2}$. To show surjectivity, let $(D'_1, \ldots, D'_r)$ denote an element of $\mathcal{C}^r \setminus Z(\mathrm{GL}_2(\mathbb{F}_q))^r$. Then, there exists a matrix $P' \in \mathrm{SL}_2(\overline{\mathbb{F}}_q)$ such that $(P'D'_1P'^{-1}, \ldots, P'D'_rP'^{-1}) = (A'_1, \cdots, A'_r) \in \mathrm{GL}_2(\mathbb{F}_q)^r$. Consider the block matrices

$$(D_1, \ldots, D_r) = \left(\begin{pmatrix} D'_1 & 0 \\ 0 & \frac{1}{\det(D'_1)} \end{pmatrix}, \ldots, \begin{pmatrix} D'_r & 0 \\ 0 & \frac{1}{\det(D'_r)} \end{pmatrix} \right)$$

Clearly each $D_i \in \mathrm{SL}_3(\mathbb{F}_q)$ by construction. Furthermore, define $P = \begin{pmatrix} P' & 0 \\ 0 & 1 \end{pmatrix}$ and $A = \begin{pmatrix} A' & 0 \\ 0 & \frac{1}{\det(D'_r)} \end{pmatrix}$. Then $P \in \mathrm{GL}_3(\overline{\mathbb{F}}_q)$ and $\det(A) = 1$ since $\det(A') = \det(D')$. It is easy to verify by block multiplication that $PD_iP^{-1} = A_i$. Therefore, $\phi([(A_1, \ldots, A_r)]) = (D'_1, \ldots, D'_r)$. Therefore, the map is surjective. $\square$

Counting the Orbits

Theorem 3.2.32. *Let the strata $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \overline{\mathcal{D}}_2, \overline{\mathcal{D}}_3$ be defined previously. Then the number of distinct orbits in each stratum is as follows.*

1. *Central Stratum*

$$\begin{cases} 3^r & \text{if } p \equiv 1 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is even} \\ 1^r & \text{if } p \equiv 0 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is odd}. \end{cases}$$

2. *Repeating Stratum*

$$\begin{cases} (q-1)^r - 3^r & \text{if } p \equiv 1 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is even} \\ (q-1)^r - 1^r & \text{if } p \equiv 0 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is odd}. \end{cases}$$

3. *Reducible Stratum*

$$\begin{cases} \frac{(q-1)^{2r}}{6} - \frac{(q-1)^r}{2} + 3^{r-1} & \text{if } p \equiv 1 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is even} \\ \frac{(q-1)^{2r}}{6} - \frac{(q-1)^r}{2} + \frac{1}{3} & \text{if } p \equiv 0 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is odd}. \end{cases}$$

4. *Irreducible Stratum*

$$\begin{cases} \frac{\left(q^2+q+1\right)^r}{3} - 3^{r-1} & \text{if } p \equiv 1 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is even} \\ \frac{\left(q^2+q+1\right)^r}{3} - \frac{1}{3} & \text{if } p \equiv 0 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is odd}. \end{cases}$$

5. *Partially Reducible Stratum*

$$\begin{cases} \frac{\left(q^2-1\right)^r}{2} - \frac{(q-1)^r}{2} & \text{if } p \equiv 1 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is even} \\ \frac{\left(q^2-1\right)^r}{2} - \frac{(q-1)^r}{2} & \text{if } p \equiv 0 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ is odd}. \end{cases}$$

Proof. Below, we give the proof for the case when $p \equiv 1 \mod 3$ or $p \equiv -1 \mod 3$ and k is even. We give the corresponding count for the case $p \equiv 0 \mod 3$ or $p \equiv -1 \mod 3$ and k is odd in brackets whenever applicable.

1. *Central Stratum:* By Theorem 3.2.27, number of central elements is 3 (or 1). Therefore, the result follows.

2. *Repeating Stratum:* Let $(D_1, \ldots, D_r)$ represent a diagonal tuple in this stratum. Then, D_i has exactly two repeated eigenvalues at fixed positions for all $1 \leq i \leq r$ or D_i is central. From Theorem 3.2.27, there are $(q-4)$ (or $(q-2)$) elements with exactly two repeated eigenvalues. Counting these with the central elements gives $(q-1)$ possibilities for each D_i and $(q-)^r$ for the total number of such tuples. Finally, we subtract the central elements which gives the desired count. Note that this is the number of such tuples up to Weyl group action. Since each such tuple can have 3 such permutations by Lemma 3.2.29, the total number of tuples is $3((q-1)^r - 3^r)$ (or $3((q-1)^r - 1^r)$).

3. *Reducible Stratum*: We count the number of diagonal tuples, $(D_1, \ldots, D_r)$ with entries from $\mathbb{F}_q$ such that there exists i for which D_i has distinct entries. It suffices to subtract the counts of the previous two strata from all the diagonal matrices in $\mathrm{SL}_3(\mathbb{F}_q)$. By Corollary 3.2.25, $\mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q)) = (q-1)^2$. Therefore, there are a total of $(q-1)^{2r}$ diagonal tuples in $\mathrm{SL}_3(\mathbb{F}_q)^r$. Subtracting the repeating and central strata and dividing by 6 to account for the Weyl group action [Lemma 3.2.29], we get the following

$$\begin{aligned} \frac{(q-1)^{2r} - 3((q-1)^r - 3^r) - 3^r}{6} &= \frac{(q-1)^{2r}}{6} - \frac{(q-1)^r}{2} - 3^{r-1} \\ \frac{(q-1)^{2r} - 3((q-1)^r - 1^r) - 1^r}{6} &= \frac{(q-1)^{2r}}{6} - \frac{(q-1)^r}{2} - \frac{1}{3}. \end{aligned}$$

   Now we add the counts from previous two parts to obtain total count for the basefield stratum, that is the number of orbits that are completely in the base field.

$$\begin{aligned} 3^r + (q-1)^r - 3^r + \frac{(q-1)^{2r}}{6} - \frac{(q-1)^r}{2} - 3^{r-1} &= \frac{(q-1)^{2r}}{6} + \frac{(q-1)^r}{2} - 3^{r-1} \\ 1^r + (q-1)^r - 1^r + \frac{(q-1)^{2r}}{6} - \frac{(q-1)^r}{2} - \frac{1}{3} &= \frac{(q-1)^{2r}}{6} + \frac{(q-1)^r}{2} - \frac{1}{3}. \end{aligned}$$

4. *Irreducible stratum:* Let $(A_1, \ldots, A_r)$ be a tuple in the irreducible stratum. Recall that for any A_i, a commuting element A_j is an element of the stabilizer, G_{A_i} under the conjugation action as explained in the proof of Lemma 3.2.30. By Lemma 3.2.17, $|G_{A_i}| = q^2 + q + 1$. Therefore, there are $(q^2 + q + 1)$ choices for each A_i. Additionally, from Lemma 3.2.30, we know that the number of distinct permutations possible for such a tuple is 3. Since $|G_A|$ includes the elements from the central stratum, we can obtain the orbits in the irreducible stratum by discounting the central stratum:

$$\begin{aligned} \frac{(q^2+q+1)^r - 3^r}{3} &= \frac{(q^2+q+1)^r}{3} - 3^{r-1} \\ \frac{(q^2+q+1)^r - 1^r}{3} &= \frac{(q^2+q+1)^r}{3} - \frac{1}{3} \end{aligned}$$

5. *Partially reducible stratum* : From Lemma 3.2.31, it suffices to compute $|(\mathcal{D}(\mathrm{GL}_2(\overline{\mathbb{F}}_q \setminus \mathbb{F}_q) \cup Z(\mathrm{GL}_2(\mathbb{F}_q)))^r \setminus Z(\mathrm{GL}_2(\mathbb{F}_q))^r|$ up to the action of Weyl group as in the proof of Lemma 3.2.31. Suppose $D_i \in \mathcal{D}(\mathrm{GL}_2(\overline{\mathbb{F}}_q \setminus \mathbb{F}_q)$. Then $\mathrm{char}(D_i)$ is an irreducible degree two polynomial. By Lemma 3.2.26, there are $\frac{q^2-q}{2}$ such polynomials and $|Z(\mathrm{GL}_2(\mathbb{F}_q))| = q - 1$. Therefore,

$$|\mathcal{D}(\mathrm{GL}_2(\overline{\mathbb{F}}_q \setminus \mathbb{F}_q)) \cup Z(\mathrm{GL}_2(\mathbb{F}_q))| = \frac{2(q^2 - q + q - 1)}{2} = q^2 - 1.$$

Therefore, we obtain the number of distinct orbits in

$(\mathcal{D}(\mathrm{GL}_2(\overline{\mathbb{F}}_q \setminus \mathbb{F}_q)) \cup Z(\mathrm{GL}_2(\mathbb{F}_q)))^r \setminus Z(\mathrm{GL}_2(\mathbb{F}_q))^r$ as

$$\frac{(q^2-1)^r}{2} - \frac{(q-1)^r}{2}.$$

□

Corollary 3.2.33. *The E-polynomial of the* $\mathrm{SL}_3(\mathbb{C})$*-character variety of* $\mathbb{Z}^r$ *is*

$$\frac{(q-1)^{2r}}{6} + \frac{(q^2-1)^r}{2} + \frac{(q^2+q+1)^r}{3}.$$

Proof. We obtain the E-polynomial by adding the number of all the closed orbits over $\mathbb{F}_q$. When $p \equiv 1 \mod 3$ or $p \equiv -1 \mod 3$ and k is even , we get

$$3^r + (q-1)^r - 3^r + \frac{(q-1)^{2r}}{6} - \frac{(q-1)^r}{2} + 3^{r-1} + \frac{(q^2-1)^r}{2} - \frac{(q-1)^r}{2} + \frac{(q^2+q+1)^r}{3} - 3^{r-1}$$

$$= \frac{(q-1)^{2r}}{6} + \frac{(q^2-1)^r}{2} + \frac{(q^2+q+1)^r}{3}$$

Similarly, if $p \equiv 0 \mod 3$ or $p \equiv -1 \mod 3$ and k is odd , we have

$$1 + (q-1)^r - 1 + \frac{(q-1)^{2r}}{6} - \frac{(q-1)^r}{2} + \frac{1}{3} + \frac{(q^2-1)^r}{2} - \frac{(q-1)^r}{2} + \frac{(q^2+q+1)^r}{3} - \frac{1}{3}$$

$$= \frac{(q-1)^{2r}}{6} + \frac{(q^2-1)^r}{2} + \frac{(q^2+q+1)^r}{3}.$$

□

This agrees with the formulae by Lawton-Muñoz in [40] and Florentino-Silva in [22]. This is a new proof of this result.

3.3 Asymptotic Transitivity on SL_n- character varieties of $\mathbb{Z}^r$

In this section, we first show that the action of $\mathrm{Out}(\mathbb{Z}^r) = \mathrm{GL}_r(\mathbb{Z})$ is not transitive on the SL_n-character varieties of free abelian groups. We then provide an upper bound for the asymptotic ratio in these cases and prove that the action is not asymptotically transitive on the character variety either. This is in contrast to the Markoff case as shown by Bourgain, Gamburd, and Sarnak in [7]. More details can be found in Section 1.2.

Non-transitive on SL_n - character varieties of free abelian groups

Proposition 3.3.1. *Let Γ be the free abelian group on r generators. Then the $\mathrm{Out}(\Gamma)$ action is not transitive on the $\mathbb{F}_q$ points of SL_n-character varieties of $\mathbb{Z}^r$.*

Proof. Let $\mathbb{Z}^r$ be the free abelian group on $r \geq 1$ generators. Consider the set of all diagonal matrices, $\mathcal{D}(\mathrm{SL}_n(\mathbb{F}_q)) \subset \mathrm{SL}_n(\mathbb{F}_q)$. Note that $|\mathcal{D}(\mathrm{SL}_n(\mathbb{F}_q))| = (q-1)^{n-1}$. For any $D = [d_{ii}]_{i=1}^n \in \mathcal{D}(\mathrm{SL}_n(\mathbb{F}_q))$, there are $(q-1)$ choices for each d_i when $1 \leq i \leq n-1$ and $d_{nn} = \frac{1}{d_{11}\cdots d_{(n-1)(n-1)}}$. Observe that the set of diagonal matrices, $\mathcal{D}(\mathrm{SL}_n(\mathbb{F}_q))$, forms a subgroup of $\mathrm{SL}_n(\mathbb{F}_q)$. Any tuple $(D_1, \ldots, D_r\ ) \in \mathcal{D}(\mathrm{SL}_n(\mathbb{F}_q))^r$ is simultaneously diagonalizable and corresponds to a closed orbit and consequently to an element in the character variety, $\mathfrak{X}_{\mathbb{Z}^r}(\mathrm{SL}_n(\mathbb{F}_q))$. Now, consider a matrix $A \in \mathrm{SL}_n(\mathbb{F}_q)$ such that $\mathrm{char}(A)$ is irreducible. Then A is similar to a diagonal matrix $D \in \mathrm{SL}_n(\overline{\mathbb{F}}_q) \setminus \mathrm{SL}_n(\mathbb{F}_q)$. If I_n denotes the identity matrix of rank n, then $(A, I_n, \ldots, I_n) \in \mathrm{SL}_n(\mathbb{F}_q)^r \setminus \mathcal{D}(\mathrm{SL}_n(\mathbb{F}_q)^r$ corresponds to an element in $\mathfrak{X}_{\mathbb{Z}^r}(\mathrm{SL}_n(\mathbb{F}_q)$. Therefore, by Theorem 2.2.4, the action is not transitive. $\square$

We state a corollary of the Subgroup Lemma[Lemma 2.2.2] which will be useful for the following discussion.

Corollary 3.3.2. *Let $\Gamma = \langle \gamma_1, \ldots, \gamma_r \rangle$ be a finitely generated group and G a reductive affine algebraic group over $\mathbb{Z}$. Let $\rho \in \mathrm{Hom}(\Gamma, G)$ be such that $(\rho(\gamma_1), \ldots, \rho(\gamma_r)) = (H_1, \ldots, H_r) \in G^r$. If $\langle H_1, \ldots, H_r \rangle$ denote the subgroup generated by $\{H_1, \ldots, H_r\}$ in G, then with respect to the $\mathrm{Aut}(\Gamma)$-action, $\mathrm{Orb}((\rho(\gamma_1), \ldots, \rho(\gamma_r))) \subseteq \langle H_1, \ldots, H_r \rangle^r$.*

Proof. Since $(H_1, \ldots, H_r) \in \langle (H_1, \ldots, H_r) \rangle$, the result follows from the subgroup lemma. $\square$

3.3.1 Asymptotic Transitivity on SL_2 - character variety of $\mathbb{Z}^r$

Theorem 3.3.3. *The action of* $\mathrm{Out}(\mathbb{Z}^r)$ *on* SL_2*-character variety of* $\mathbb{Z}^r$ *is not asymptotically transitive. Furthermore, the asymptotic ratio of the orbits of elements in the character variety is bounded above by* $\frac{1}{2}$.

Proof. We consider each stratum and look at the subgroups within the stratum. Refer to 3.2.1 for the stratification and the size of each stratum as well as a count for the number of orbits in each stratum. Recall that each element in the character variety corresponds to a tuple of diagonal elements (up to conjugation in $\mathrm{SL}_2(\overline{\mathbb{F}}_q)$).

1. The set of central elements, $Z(\mathrm{SL}_2(\mathbb{F}_q))$, in $\mathrm{SL}_2(\mathbb{F}_q)$ forms a subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$.

2. The set of diagonal elements, $\mathcal{D}(\mathrm{SL}_2(\mathbb{F}_q))$, also is a subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$.

3. The set of irreducible diagonal tuples, $\mathcal{D}_{irr}(\mathrm{SL}_2(\mathbb{F}_q))$ along with the central elements form the stabilizer subgroup by Lemma 3.2.17.

Let $[(D_1, D_2, \ldots, D_r)] \in \mathfrak{X}_{\mathbb{Z}^r}(\mathrm{SL}_2(\mathbb{F}_q))$ where $D_i \in \mathrm{SL}_2(\mathbb{F}_q)$. Then, D_i is the element of one of the three subgroups mentioned above say, H. Then, $D_j \in H$ for every $1 \leq j \leq r$ by Lemma 3.2.15. Consequently, the size of the orbits are bounded above by $|H^r|$. Since, in this case, H^r is the same as that of the strata, we look at the counts from Theorem 3.2.23. Now we calculate an upper bound for the asymptotic ratio of orbits of elements in each of the three subgroups. Let $D = (D_1, \ldots, D_r) \in Z(\mathrm{SL}_2(\mathbb{F}_q))^r$. Then the asymptotic ratio of $\mathrm{Orb}((D_1, \ldots, D_r))$ is

$$\lim_{q \to \infty} \frac{|\mathrm{Orb}((D_1, \ldots, D_r))|}{|\mathfrak{X}_{\mathbb{Z}^r}(\mathrm{SL}_2(\mathbb{F}_q))|}.$$

The size of the character variety is given by the E-polynomial in Corollary 3.2.24 as

$$\frac{(q+1)^r}{2}+\frac{(q-1)^r}{2}.$$

1. Central Orbit: If $(D_1,\dots,D_r)\in Z(\mathrm{SL}_2(\mathbb{F}_q))^r$, then the asymptotic ratio is bounded above by

$$\begin{aligned}\lim_{q\to\infty}\frac{2^r}{\frac{(q+1)^r}{2}+\frac{(q-1)^r}{2}} &= 0, \text{ when } p \text{ is odd}\\ \lim_{q\to\infty}\frac{1^r}{\frac{(q+1)^r}{2}+\frac{(q-1)^r}{2}} &= 0, \text{ when } p \text{ is even .}\end{aligned}$$

2. Reducible Orbit: If $(D_1,\dots,D_r)\in \mathcal{D}(\mathrm{SL}_2(\mathbb{F}_q))^r$, then the ratio is bounded by

$$\begin{aligned}\lim_{q\to\infty}\frac{\frac{(q-1)^r-2^r}{2}}{\frac{(q+1)^r}{2}+\frac{(q-1)^r}{2}} &= \lim_{q\to\infty}\frac{(q-1)^r-2^r}{(q+1)^r+(q-1)^r}=\frac{1}{2} \text{ when } p \text{ is odd}\\ \lim_{q\to\infty}\frac{\frac{(q-1)^r-1^r}{2}}{\frac{(q+1)^r}{2}+\frac{(q-1)^r}{2}} &= \lim_{q\to\infty}\frac{(q-1)^r-1^r}{(q+1)^r+(q-1)^r}=\frac{1}{2} \text{ when } p \text{ is even}\end{aligned}$$

3. Irreducible Orbit: Similarly, when $(D_1,\dots,D_r)\in(\mathcal{D}_{irr}(\mathrm{SL}_2(\mathbb{F}_q))\cup Z(\mathrm{SL}_2(\mathbb{F}_q)))^r\setminus Z(\mathrm{SL}_2(\mathbb{F}_q))^r$, then the ratio is bounded by

$$\begin{aligned}\lim_{q\to\infty}\frac{\frac{(q+1)^r-2^r}{2}}{\frac{(q+1)^r}{2}+\frac{(q-1)^r}{2}} &= \frac{1}{2} \text{ when } p \text{ is odd}\\ \lim_{q\to\infty}\frac{\frac{(q+1)^r-1^r}{2}}{\frac{(q+1)^r}{2}+\frac{(q-1)^r}{2}} &= \frac{1}{2} \text{ when } p \text{ is even .}\end{aligned}$$

Note that we are assuming the transitivity within each stratum for these calculations. But it is not clear that this is true even though there are reasons to believe it could be true as seen in the $\mathrm{SL}_2(\mathbb{F}_2)$ case. Therefore the above count gives only the upper bound for the asymptotic ratio and not the actual value of the ratio for each orbit. Hence, the only possible asymptotic ratios for orbits are 0 and $\frac{1}{2}$. This concludes the proof.

$\square$

3.3.2 Asymptotic Transitivity on SL_3 - character variety of $\mathbb{Z}^r$

Corollary 3.3.4. *The E-polynomial of the* $\mathrm{SL}_3(\mathbb{C})$*-character variety of* $\mathbb{Z}^2$ *is* $q^4 + q^2 + 1$.

Proof. By Corollary 3.2.33 , the E-polynomial of $\mathrm{SL}_3(\mathbb{C})$-character variety of $\mathbb{Z}^r$ is

$$\frac{(q-1)^{2r}}{6} + \frac{(q^2-1)^r}{2} + \frac{(q^2+q+1)^r}{3}.$$

Substituting $r = 2$ and simplifying obtains $q^4 + q^2 + 1$. $\square$

Proposition 3.3.5. *The action of* $\mathrm{Out}(\mathbb{Z}^r)$ *on* SL_3*-character variety of* $\mathbb{Z}^r$ *is not asymptotically transitive. Furthermore, the asymptotic ratio of the orbits of elements in the character variety is bounded above by* $\frac{1}{2}$.

Proof. We use the same strategy as in the proof of $\mathrm{SL}_2(\mathbb{F}_q)$ character variety of $\mathbb{Z}^r$. We consider each stratum and find the subgroups within each stratum. Recall that the diagonal tuples represents the polystable points and hence consists of the elements of the character variety, $\mathfrak{X}_{\mathbb{Z}^r}(\mathrm{SL}_3(\mathbb{F}_q))$. Let $(A_1, \ldots, A_r)$ be an element of a stratum $\mathcal{T}$. Then $(A_1, \ldots, A_r)$ is simultaneously diagonalizable to a tuple $(D_1, \ldots, D_r)$, unique up to Weyl group action. We use the equivalence class of $[(D_1, \ldots, D_r)]$ to represent the element in $\mathfrak{X}_{\mathbb{Z}^r}(\mathrm{SL}_3(\mathbb{F}_q))$. Now we look at possible orbits of $[(D_1, \ldots, D_r)]$ in each stratum and calculate a bound for the asymptotic ratio of the orbits. Recall the definition of each stratum from previous section.

1. Basefield Subgroup Tuples: This includes the set of all tuples with coordinate entries from the set of diagonal elements in $\mathrm{SL}_3(\mathbb{F}_q)$. We have that $(D_1, \ldots, D_r) \in \mathcal{D}(\mathrm{SL}_3(\mathbb{F}_q))^r$. This form a subgroup of $\mathrm{SL}_3(\mathbb{F}_q)$. Note that this subgroup is the union of reducible, repeatable and central tuples as defined in previous section.

2. Central Tuples: The central elements form a subgroup.

3. Partially Reducible Subgroup Tuples: Up to permutation, this set is isomorphic to $\mathrm{GL}_2(\mathbb{F}_q)$ and hence form a subgroup.

4. Irreducible Subgroup Tuples: See the proof of Proposition 3.2.19 to recall that this set along with the central elements form a subgroup.

Now, we compute the asymptotic ratio for the orbits in each of these stratum.

1. Basefield Orbit

$$\lim_{q\to\infty} \frac{\frac{(q-1)^{2r}}{6} + \frac{(q-1)^r}{2} + 3^{r-1}}{\frac{(q-1)^{2r}}{6} + \frac{(q^2-1)^r}{2} + \frac{(q^2+q+1)^r}{3}} = \frac{1}{6} \quad \text{if } p \equiv 1 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ even}$$

$$\lim_{q\to\infty} \frac{\frac{(q-1)^{2r}}{6} + \frac{(q-1)^r}{2} + \frac{1}{3}}{\frac{(q-1)^{2r}}{6} + \frac{(q^2-1)^r}{2} + \frac{(q^2+q+1)^r}{3}} = \frac{1}{6} \quad \text{if } p \equiv 0 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ odd.}$$

2. Partially Reducible Orbit

$$\lim_{q\to\infty} \frac{\frac{(q^2-1)^r-(q-1)^r}{2}}{\frac{(q-1)^{2r}}{6} + \frac{(q^2-1)^r}{2} + \frac{(q^2+q+1)^r}{3}} = \frac{1}{2} \quad \text{for all } \; p.$$

3. Irreducible Orbit

$$\lim_{q\to\infty} \frac{\frac{\left(q^2+q+1\right)^r-3^r}{3}}{\frac{(q-1)^{2r}}{6}+\frac{(q^2-1)^r}{2}+\frac{(q^2+q+1)^r}{3}} = \frac{1}{3} \quad \text{if } p \equiv 1 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ even}$$

$$\lim_{q\to\infty} \frac{\frac{\left(q^2+q+1\right)^r-\frac{1}{3}}{3}}{\frac{(q-1)^{2r}}{6}+\frac{(q^2-1)^r}{2}+\frac{(q^2+q+1)^r}{3}} = \frac{1}{3} \quad \text{if } p \equiv 0 \mod 3 \text{ or } p \equiv -1 \mod 3 \text{ and } k \text{ odd.}$$

This concludes the proof. □

Relative character variety

We end this thesis by looking at a relative character variety in $\mathrm{SL}_3(\mathbb{F}_q)$-character variety of F_2 by fixing the commutator to be a non-trivial central element. We prove that there is exactly one point in such a character variety when it is non-empty. See Section 1.1.5 to recall the discussion of relative character variety.

Proposition 3.3.6. *Suppose $A_1, B_1, A_2, B_2 \in \mathrm{SL}_3(\mathbb{F}_q)$ such that $A_iB_iA_i^{-1}B_i^{-1} = \lambda I$ where $\lambda \neq 0, 1$ and $i = 1, 2$. Then there exists $g \in \mathrm{SL}_3(\overline{\mathbb{F}}_q)$ such that $gA_1g^{-1} = A_2$ and $gB_1g^{-1} = B_2$.*

Proof. First, we prove the following claim.

Claim: If $AB = \lambda BA$, then $A^3 = B^3 = I$.

Proof of Claim: Note that $A = \lambda BAB^{-1}$.

$$1 = \det(ABA^{-1}B^{-1}) = \det(\lambda I) = \lambda^3 \implies \lambda = \sqrt[3]{1} \quad \text{where } \lambda \neq 1.$$

Since $ABA^{-1}B^{-1} = \lambda I$, $A = \lambda BAB^{-1}$. This implies the following

$$\mathrm{tr}(A) = \mathrm{tr}(\lambda BAB^{-1}) = \lambda \cdot \mathrm{tr}(BAB^{-1}).$$

Similarly, $A^{-1} = B^{-1}A^{-1}\lambda B = \lambda B^{-1}AB$, $\text{tr}(A^{-1}) = \text{tr}(\lambda B^{-1}A^{-1}B) = \lambda \cdot \text{tr}(B^{-1}A^{-1}B))$. Since $\text{tr}(A = \text{tr}(BAB^{-1})$ and $\lambda \neq 1$, this gives $\text{tr}(A) = 0$. Similarly, $\text{tr}(A^{-1}) = 0$. Therefore, using Cayley Hamilton Theorem,

$$A^3 - \text{tr}(A)A^2 + \text{tr}(A^{-1})A - \det(A)I = 0 \implies A^3 - I = 0.$$

Thus, $A^3 = I$ which proves the claim.

Now choose $A_0 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^2 \end{bmatrix}$ and $B_0 := \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$. Suppose ω is an eigenvalue of A with eigenvector v. Then $Av = \omega v$. This implies $A^2 v = \omega^2 v$ and $A^3 v = \omega^3 v = v$ since $A^3 = I$. Therefore, $\omega^3 = 1$ which implies $\omega = \sqrt[3]{1}$. So all eigenvalues of A are cube roots of unity. Note that it is not possible that 1 is the only eigenvalue as $A \neq I$. Therefore, the eigenvalues of A includes at least 1 and λ which implies that λ^2 is also an eigenvalue. Consequently, A is similar to a matrix of the type A_0 that is $A = PAP^{-1}$ for $P \in \text{GL}(\overline{\mathbb{F}_q})$. Now we claim that $B = PB_0P^{-1}$. To prove the claim, let $E_\omega(A_1)$ be the eigenspace of A.

Claim: $B(E_\lambda(A) = E_{\omega\lambda}(A)$.

Proof of Claim: If $v \in E_\lambda(A)$, then $Av = \lambda v$. Then, $A(Bv) = \omega BAv = \omega\lambda(Bv)$. Therefore, $Bv \in E_{\omega\lambda}(A)$.

Conversely, suppose $v' \in E_{\omega\lambda}(A)$. Then, $Av' = \omega\lambda v'$. We want to show that $v' = Bv$ where $v \in E_\lambda(A)$.

$$\begin{aligned} B^{-1}Av' &= \omega\lambda B^{-1}v' \\ \omega A(B^{-1}v') &= \omega\lambda(B^{-1}v') \end{aligned}$$

This implies that $v := B^{-1}v' \in E_\lambda(A)$. Therefore, $Bv = v'$. This completes the proof of the claim.

Since A is the diagonal matrix A_0, the eigenspaces of $1, \omega, \omega^2$ are orthogonal and hence linearly independent. By the previous claim, B permutes the eigenvectors of A as follows:

$$\begin{aligned} E_1(A) &\longmapsto E_\omega A \\ E_\omega(A) &\longmapsto E_\omega^2 A \\ E_\omega^2(A) &\longmapsto E_1 A \end{aligned}$$

which corresponds to multiplication by the permutation matrix B_0. So $B = B_0$. But note that $A_0 = P^{-1}AP$. Then $B_0 = P^{-1}BP$. This implies that $PA_0P^{-1} = A$ and $PB_0P^{-1} = B$.

Now by letting $A = A_1$ and $B = B_1$, we get that there exists $P \in \mathrm{GL}_3(\overline{\mathbb{F}_q})$ such that

$$PA_0P^{-1} = A_1 \text{ and } PB_0P^{-1} = B_1 \implies P^{-1}A_1P = A_0 \text{ and } P^{-1}B_1P = B_0. \tag{3.4}$$

Similarly, there exists $Q \in \mathrm{GL}_3(\overline{\mathbb{F}_q})$ such that

$$QA_0Q^{-1} = A_2 \text{ and } QB_0Q^{-1} = B_2. \tag{3.5}$$

Then from 3.4 and 3.5, we get that

$$\begin{aligned} A_2 = QP^{-1}A_1PQ^{-1} &= (QP^{-1})A_1(QP^{-1})^{-1} \\ B_2 = QP^{-1}B_1PQ^{-1} &= (QP^{-1})B_1(QP^{-1})^{-1} \end{aligned}$$

thereby proving the proposition. □

Corollary 3.3.7. *The* $\mathrm{Out}(\Gamma)$*-action on the relative character variety of* $\mathfrak{X}_{F_2}(\mathrm{SL}_3(\mathbb{F}_q))$ *obtained by fixing the value of the boundary component to be a non-trivial central element is vacuously transitive when* $p \equiv 1 \mod 3$ *or* $p \equiv -1 \mod 3$ *and* k *is even.*

Proof. By Lemma 3.2.1, $\mathbb{F}_q$ has a nontrivial cubic root of unity when $p \equiv 1 \mod 3$ or

$p \equiv -1 \mod 3$ and k is even. By the previous proposition, there is a single point in the relative character variety. Thus the result follows. $\square$

Appendix A: Appendix

A.0.1 Deriving the Boundary Condition for the Relative Character Variety of the One-holed Torus

In the one-holed torus case with $\pi = F_2$, the free group on two generators, and $G = \mathrm{SL}(2,\mathbb{C})$, the character variety is isomorphic to the affine 3-space, as a consequence of Fricke-Vogt theorem. An exposition of this result can be found in [26]. The isomorphism is given by:

$$\tau : [\rho] \longmapsto (x, y, z) := (\mathrm{tr}(\rho(X)), \mathrm{tr}(\rho(Y)), \mathrm{tr}(\rho(XY)))$$

where $X, Y \in \mathrm{SL}(2,\mathbb{C})$ are images of the generators under ρ. From (1.2), the relative character variety is obtained from the relative representation variety given by

$$\mathrm{Hom}_b(\pi, \mathrm{SL}(2,\mathbb{C})) := \{\rho \in \mathrm{Hom}(\pi, \mathrm{SL}(2,\mathbb{C})) \mid \mathrm{tr}(\rho(b_1)) = \lambda \text{ for } \lambda \in \mathbb{C}\}.$$

Since the boundary component corresponds to the commutator, the problem reduces to fixing the trace of the commutator. In other words, for $\lambda \in \mathbb{C}$, the λ-relative character variety $\mathfrak{X}^{\lambda}_{F_2}(\mathrm{SL}(2,\mathbb{C}))$ is the set of equivalence classes $[\rho]$ such that

$$\mathrm{tr}\ (\rho(XYX^{-1}Y^{-1})) = \lambda$$

for any pair of generators, X, Y of F_2.

Lemma A.0.1. *If* $\mathrm{tr}(X) = x, \mathrm{tr}(Y) = y$ *and* $\mathrm{tr}(XY) = z$*, then*

$$\mathrm{tr}(XYX^{-1}Y^{-1}) = x^2 + y^2 + z^2 - xyz - 2.$$

Proof. First we establish some basic identities of the traces. Since every 2×2 matrix, A

satisfies its characteristic equation, we get

$$A^2 - \mathrm{tr}(A)A + \det(A)\mathrm{I}_n = 0.$$

If $A \in \mathrm{SL}(2, \mathbb{C})$, this equation reduces to

$$A^2 - \mathrm{tr}(A)A = -\mathrm{I}_2.$$

Post multiplying by A^{-1}, we obtain,

$$A - \mathrm{tr}(A)\mathrm{I}_2 \quad = \quad -A^{-1}$$

Thus, we obtain the following trace identities

$$\begin{aligned} A + A^{-1} &= \mathrm{tr}(A)\mathrm{I}_2 && && \text{(A.1)} \\ \mathrm{tr}(A) + \mathrm{tr}(A^{-1}) &= 2\mathrm{tr}(A) && \text{[By taking trace of both sides of (3)]} \\ \mathrm{tr}(A) &= \mathrm{tr}(A^{-1}) && \text{[By simplifying (4)]} && \text{(A.2)} \end{aligned}$$

Multiplying Equation (A.1) by B and then taking the trace, we get

$$\begin{aligned} \mathrm{tr}(BA) + \mathrm{tr}(BA^{-1}) &= \mathrm{tr}(B)\mathrm{tr}(A) \\ \mathrm{tr}(BA) &= \mathrm{tr}(B)\mathrm{tr}(A) - \mathrm{tr}(BA^{-1}) && \text{(A.3)} \end{aligned}$$

Now that we have established some basic identities that allows us to simplify the trace of products of matrices, we can compute the trace of the commutator.

Applying (A.3), we get

$$\mathrm{tr}(XYX^{-1}Y^{-1}) = \mathrm{tr}(XYX^{-1})\mathrm{tr}(Y^{-1}) - \mathrm{tr}(XYX^{-1}Y).$$

We know from (A.1) that $\mathrm{tr}(Y^{-1}) = \mathrm{tr}(Y) = y$. Also $\mathrm{tr}(XYX^{-1}) = \mathrm{tr}(Y) = y$ as conjugate matrices have same trace. It only remains to compute $\mathrm{tr}(XYX^{-1}Y)$ which can be done by using (A.3) again.

$$\begin{aligned}\mathrm{tr}(XYX^{-1}Y) &= \mathrm{tr}(XY)\mathrm{tr}(X^{-1}Y) - \mathrm{tr}(X^2) \\ &= z(xy - z) - (x^2 - 2) \\ &= xyz - z^2 - x^2 + 2\end{aligned}$$

where

$$\begin{aligned}\mathrm{tr}(X^{-1}Y) &= \mathrm{tr}(X^{-1})\mathrm{tr}(Y) - \mathrm{tr}(X^{-1}Y^{-1}) \\ &= xy - \mathrm{tr}((YX)^{-1}) \\ &= xy - \mathrm{tr}(YX) && [\mathrm{tr}(A) = \mathrm{tr}(A^{-1})] \\ &= xy - \mathrm{tr}(XY) && [\mathrm{tr}(AB) = \mathrm{tr}(BA)] \\ &= xy - z.\end{aligned}$$

Therefore,

$$\begin{aligned}\mathrm{tr}(XYX^{-1}Y^{-1}) &= \mathrm{tr}(XYX^{-1})\mathrm{tr}(Y^{-1}) - \mathrm{tr}(XYX^{-1}Y) \\ &= y^2 - (xyz - z^2 - z^2 + 2) \\ &= x^2 + y^2 + z^2 - xyz - 2.\end{aligned}$$

$\square$

Then the polynomial κ parameterized by λ, defined as follows, gives the relative character varieties

$$\kappa_\lambda(x, y, z) = x^2 + y^2 + z^2 - xyz - 2 - \lambda.$$

A.0.2 $\mathrm{Out}(\Gamma)$ action on character variety

Lemma A.0.2. *Let Γ be a finitely presented group and G a complex affine algebraic reductive group. Then the outer automorphisms of Γ, denoted by $\mathrm{Out}(\Gamma)$, acts on the GIT quotient $\mathrm{Hom}(\Gamma, G) /\!/ G$.*

Proof. The automorphism $\mathrm{Aut}(\Gamma)$ acts on $\mathrm{Hom}(\Gamma, G)$ as follows:

$$\tau \cdot \rho = \rho \circ \tau^{-1}.$$

1. First we prove that this is an action.

   Since composition of homomorphisms is a homomorphism, $\rho \circ \tau^{-1} \in \mathrm{Hom}(\Gamma, G)$ and hence the action is well defined. Note that $e \cdot \rho = \rho \circ e^{-1} = \rho \circ e = \rho$ where e is the identity element of $\mathrm{Aut}(\Gamma)$. Finally,

$$\begin{aligned}
(\tau \circ \sigma) \cdot \rho &= \rho \circ (\tau \circ \sigma)^{-1} \\
&= \rho \circ (\sigma^{-1} \circ \tau^{-1}) \\
&= (\rho \circ \sigma^{-1}) \circ \tau^{-1} \\
&= \tau \cdot (\rho \circ \sigma^{-1}) \\
&= \tau \cdot (\sigma \cdot \rho).
\end{aligned}$$

   Therefore this is indeed a group action.

2. *The action extends to a coaction on the coordinate ring.*

   By Lemma 2.0.2, $\mathrm{Hom}(\Gamma, G)$ maps injectively to G^r by evaluation map and hence inherits the structure of a subvariety G^r. Let I be the ideal defining $\mathrm{Hom}(\Gamma, G)$ in $\mathbb{C}[G^r]$. Then the coordinate ring of the variety is given by

$$\mathbb{C}[\mathrm{Hom}(\Gamma, G)] \cong \mathbb{C}[x_1, ..., x_N]/I.$$

Suppose $f + I \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)]$ and $\sigma \in \mathrm{Aut}(\Gamma)$. Then we prove that the action of $\mathrm{Aut}(\Gamma)$ extends to the coordinate ring as follows:

$$\begin{aligned} \sigma \cdot (f + I) &= f(\sigma^{-1} \cdot \rho) + I \\ &= f(\rho(\sigma^{-1})^{-1}) + I \\ &= f(\rho \circ \sigma) + I. \end{aligned}$$

First, we show that the action is well defined on the representatives of the cosets. For $h \in I$, $\sigma \in \mathrm{Aut}(\Gamma)$ and $\rho \in \mathrm{Hom}(\Gamma, G)$,

$$\sigma \cdot (h(\rho)) = h(\rho \circ \sigma)).$$

Since $\rho \circ \sigma \in \mathrm{Hom}(\Gamma, G)$ and I is the ideal of the variety $\mathrm{Hom}(\Gamma, G)$, $h(\rho \circ \sigma) = 0$ for all $\rho \in \mathrm{Hom}(\Gamma, G)$ and $\sigma \in \mathrm{Aut}(\Gamma)$. Thus, $\mathrm{Aut}(\Gamma)$ action is trivial on I.

Clearly,

$$e \cdot (f + I) = f(\rho \circ e) + I = f(\rho) + I = f + I.$$

Finally,

$$\begin{aligned} (\sigma\tau) \cdot (f + I) &= f((\sigma \circ \tau)^{-1} \cdot \rho) + I \\ &= f((\tau^{-1} \circ \sigma^{-1}) \cdot \rho) + I \\ &= f(\tau^{-1} \cdot (\sigma^{-1} \cdot \rho)) + I \\ &= \tau \cdot f(\sigma^{-1} \cdot \rho) + I \\ &= \sigma \cdot (\tau \cdot f(\rho)) + I \end{aligned}$$

Therefore, this is a well-defined action on the coordinate ring.

3. $\mathrm{Aut}(\Gamma)$ *acts on the invariant subring* $\mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$.

There is an injection from $\mathrm{Hom}(\Gamma, G) \hookrightarrow G^r$ given by

$$\phi : \rho \longmapsto (\rho(\gamma_1), \rho(\gamma_2), ..., \rho(\gamma_r)).$$

See Lemma 2.0.2. Therefore, G acts on $\mathrm{Hom}(\Gamma, G)$ by simultaneous conjugation,

$$g \cdot \rho = g\rho g^{-1} = (g\rho(\gamma_1)g^{-1}, ..., g\rho(\gamma_r)g^{-1}) \in G^r.$$

This extends to a coaction on the ring of polynomials $\mathbb{C}[\mathrm{Hom}(\Gamma, G)]$ given by

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

Then the ring of invariants is defined as

$$\mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G := \{f \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)] \mid g \cdot f = f\}.$$

It suffices to prove that the invariant subring $\mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$ is invariant under the action of $\mathrm{Aut}(\Gamma)$ defined earlier.

Let $f + I \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$. Then $f(g\rho g^{-1}) + I = f(\rho) + I$ for all $g \in G$ and all $\rho \in \mathrm{Hom}(\Gamma, G)$. We need to prove that $\sigma \cdot (f + I) \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$ for all $\sigma \in \mathrm{Aut}(\Gamma)$. Since $\rho \circ \sigma \in \mathrm{Hom}(\Gamma, G)$,

$$g \cdot (\sigma \cdot f(\rho) + I) = f(g^{-1}(\rho \circ \sigma^{-1})g) + I = f(\rho \circ \sigma^{-1}) + I = \sigma \cdot f(\rho) + I$$

because $f + I \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$. Therefore,

$$\sigma \cdot (f + I) = f(\rho \circ \sigma) + I \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G.$$

4. $\mathrm{Out}(\Gamma)$ *acts on* $\mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$.

Let $\mathrm{Inn}(\Gamma)$ denote the set of all inner automorphisms of Γ. It is enough to show that for $\alpha \in \mathrm{Inn}(\Gamma)$ and $f \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$, $\alpha \cdot (f + I) = f + I$. Since $\alpha \in \mathrm{Inn}(\Gamma)$, the map $\alpha : \Gamma \longrightarrow \Gamma$ is given by $\alpha(w) = vwv^{-1}$ for $v, w \in \mathrm{Inn}(\Gamma)$. By definition, $\alpha \cdot (f + I) = f(\rho \circ \alpha^{-1}) + I$. Let γ_i be one of the generators of Γ. Then,

$$f(\rho \circ \alpha(\gamma_i)) + I = f(\rho(v\gamma_i v^{-1})) + I.$$

Since ρ is a homomorphism,

$$f(\rho(v\gamma_i v^{-1})) + I = f(\rho(v)\rho(\gamma_i)\rho(v^{-1})) + I.$$

Let $g = \rho(v)$ for $g \in G$. Then $g^{-1} = \rho(v)^{-1} = \rho(v^{-1})$. So,

$$f(\rho(v)\rho(\gamma_i)\rho(v^{-1})) + I = f(g\rho(\gamma_i)g^{-1}) + I.$$

Since $f \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$, $f(g\rho(\gamma_i g^{-1})) = f(\rho)$ for all $g \in G$. Hence,

$$f(g\rho(\gamma_i)g^{-1}) + I = f(\rho(\gamma_i)) + I$$

for $1 \leq i \leq r$. Consequently,

$$\alpha \cdot (f + I) = f(\rho \circ \alpha) + I = f + I$$

for all $f \in \mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$ and $\alpha \in \mathrm{Inn}(\Gamma)$.

5. $\mathrm{Out}(\Gamma)$ *acts on the character variety*

Let $A := \mathbb{C}[\mathrm{Hom}(\Gamma, G)]^G$. Then $\mathrm{Hom}(\Gamma, G) /\!/ G := \mathrm{Spec}_{\max}(A)$. We will show that action of G on A induces an action on the character variety, $\mathfrak{X}_\Gamma(G) := \mathrm{Hom}(\Gamma, G) /\!/ G$. Note that the action of the group G on A is a homomorphism from $G \to \mathrm{Aut}(A)$ given by $g \longmapsto \alpha_g$. We prove that each automorphism of A induces an action on the set of maximal ideals.

***Claim**: Let A be a commutative ring with unity and $\alpha_g : A \to A$ be an automorphism of A. Then α_g induces a bijection on the set of maximal ideals of A denoted by* $\mathrm{Spec}_{\max}(A)$.

Proof. Let M be a maximal ideal of A. Then $M \neq A$. We will show that $\alpha_g(M)$ is a maximal ideal of A. Note that $\alpha_g(M) \subset N$ for some maximal ideal N of A. Since α_g is surjective, $\alpha_g^{-1}(N)$ is a maximal ideal of A. But $M \subseteq \alpha_g^{-1}(N)$. By maximality of M and surjectivity of α_g, it follows that $\alpha_g^{-1}(N) = M$. Therefore, $N = \alpha_g(\alpha_g^{-1}(N)) = \alpha_g(M)$ is maximal in A. □

Thus, each automorphism α_g of the ring A permutes the set of maximal ideals of A. Clearly, $e \cdot M = \alpha_e(M) = M$. Now suppose $g, h \in G$. Then

$$\begin{aligned} (gh)(M) &= (\alpha_g \circ \alpha_h)(M) \\ &= \alpha_g \cdot (\alpha_h \cdot M) \end{aligned}$$

since α defines an action on A. Therefore, $\mathrm{Out}(\Gamma)$ acts on $\mathrm{Hom}(\Gamma, G) /\!/ G$.

□

Bibliography

[1] Linear Diophantine Equations. `http://gauss.math.luc.edu/greicius/Math201/Fall2012/Lectures/linear-diophantine.article.pdf`. Accessed: 2022-04-19.

[2] Mason Experimental Geometry Lab. `http://meglab.wikidot.com/research:summer2017`. Accessed: 2022-01-30.

[3] S. Andreadakis. Generators for $\operatorname{Aut} G$, G free nilpotent. *Arch. Math. (Basel)*, 42(4):296–300, 1984.

[4] Michael Bate, Haralampos Geranios, and Benjamin Martin. Orbit closures and invariants. *Math. Z.*, 293(3-4):1121–1159, 2019.

[5] Michael Bate, Benjamin Martin, Gerhard Röhrle, and Rudolf Tange. Closed orbits and uniform S-instability in geometric invariant theory. *Trans. Amer. Math. Soc.*, 365(7):3643–3673, 2013.

[6] Jérémy Blanc and Immanuel Stampfli. Automorphisms of the plane preserving a curve. *Algebr. Geom.*, 2(2):193–213, 2015.

[7] Jean Bourgain, Alexander Gamburd, and Peter Sarnak. Markoff triples and strong approximation. *Comptes Rendus Mathematique*, 354(2):131–135, 2016.

[8] Steven B. Bradlow, Oscar Garcia-Prada, and Peter B. Gothen. Homotopy groups of moduli spaces of representations. *Topology*, 47(4):203–224, 2008.

[9] John R. Britnell and Mark Wildon. On types and classes of commuting matrices over finite fields. *J. Lond. Math. Soc. (2)*, 83(2):470–492, 2011.

[10] Jean-Philippe Burelle and Sean Lawton. Dynamics on nilpotent character varieties. *arXiv e-prints*, page arXiv:2111.11922, 2021.

[11] Samuel Cavazos and Sean Lawton. E-polynomial of $\mathrm{SL}_2(\mathbb{C})$-character varieties of free groups. *Internat. J. Math.*, 25(6):1450058, 27, 2014.

[12] Alois Cerbu, Elijah Gunther, Michael Magee, and Luke Peilen. The cycle structure of a Markoff automorphism over finite fields. *J. Number Theory*, 211:1–27, 2020.

[13] William Chen. Nonabelian level structures, nielsen equivalence, and markoff triples. page arXiv:2011.12940v2, 2021.

[14] Pierre Deligne. Théorie de Hodge. II. *Inst. Hautes Études Sci. Publ. Math.*, (40):5–57, 1971.

[15] Pierre Deligne. Théorie de Hodge. III. *Inst. Hautes Études Sci. Publ. Math.*, (44):5–77, 1974.

[16] Igor Dolgachev. *Lectures on invariant theory*, volume 296 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2003.

[17] David S. Dummit and Richard M. Foote. *Abstract algebra*. Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[18] Benson Farb and Dan Margalit. *A primer on mapping class groups*, volume 49 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 2012.

[19] Carlos Florentino and Sean Lawton. Topology of character varieties of Abelian groups. *Topology Appl.*, 173:32–58, 2014.

[20] Carlos Florentino, Azizeh Nozad, and Alfonso Zamora. Generating series for the e-polynomial of the $\mathrm{GL}(n, \mathbb{C})$-character varieties. *arXiv: Algebraic Geometry*, 2020.

[21] Carlos Florentino, Azizeh Nozad, and Alfonso Zamora. Serre polynomials of SL_n- and PGL_n-character varieties of free groups. *J. Geom. Phys.*, 161:Paper No. 104008, 21, 2021.

[22] Carlos Florentino and Jaime Silva. Hodge-Deligne polynomials of character varieties of free abelian groups. *Open Math.*, 19(1):338–362, 2021.

[23] Tsachik Gelander. On deformations of F_n in compact Lie groups. *Israel J. Math.*, 167:15–26, 2008.

[24] Robert Gilman. Finite quotients of the automorphism group of a free group. *Canadian J. Math.*, 29(3):541–551, 1977.

[25] William M. Goldman. Ergodic theory on moduli spaces. *Ann. of Math. (2)*, 146(3):475–507, 1997.

[26] William M. Goldman. An exposition of results of Fricke. *arXiv e-prints*, page arXiv:math/0402103v2, 2004.

[27] William M. Goldman. An ergodic action of the outer automorphism group of a free group. *Geom. Funct. Anal.*, 17(3):793–805, 2007.

[28] William M. Goldman, Sean Lawton, and Eugene Z. Xia. The mapping class group action on SU(3)-character varieties. *Ergodic Theory Dynam. Systems*, 41(8):2382–2396, 2021.

[29] I. Gruschko. Über die Basen eines freien Produktes von Gruppen. *Rec. Math. [Mat. Sbornik] N.S.*, 8 (50):169–182, 1940.

[30] Clément Guérin, Sean Lawton, and Daniel Ramras. Bad representations and homotopy of character varieties. *Annales Henri Lebesgue*, 5:93–140, Feb 2022.

[31] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[32] Tamás Hausel and Fernando Rodriguez-Villegas. Mixed Hodge polynomials of character varieties. *Invent. Math.*, 174(3):555–624, 2008. With an appendix by Nicholas M. Katz.

[33] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[34] Wolfram Research, Inc. Mathematica, Version 12.3. Champaign, IL, 2021.

[35] D. L. Johnson. *Presentations of groups*, volume 15 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, second edition, 1997.

[36] Ilya Kapovich and Richard Weidmann. Nielsen equivalence in a class of random groups. *J. Topol.*, 9(2):502–534, 2016.

[37] Ahmet Küçük. The fundamental group of an oriented surface of genus n with k boundary surfaces. *Appl. Math. Comput.*, 160(1):141–145, 2005.

[38] Sean Lawton. Generators, relations and symmetries in pairs of 3×3 unimodular matrices. *J. Algebra*, 313(2):782–801, 2007.

[39] Sean Lawton. Poisson geometry of $\mathrm{SL}(3, \mathbb{C})$-character varieties relative to a surface with boundary. *Trans. Amer. Math. Soc.*, 361(5):2397–2429, 2009.

[40] Sean Lawton and Vicente Muñoz. E-polynomial of the $\mathrm{SL}(3, \mathbb{C})$-character variety of free groups. *Pacific J. Math.*, 282(1):173–202, 2016.

[41] Sean Lawton and Daniel Ramras. Covering spaces of character varieties. *New York J. Math.*, 21:383–416, 2015. With an appendix by Nan-Kuo Ho and Chiu-Chu Melissa Liu.

[42] Marina Logares, Vicente Muñoz, and P. E. Newstead. Hodge polynomials of $\mathrm{SL}(2, \mathbb{C})$-character varieties for curves of small genus. *Rev. Mat. Complut.*, 26(2):635–703, 2013.

[43] Wilhelm Magnus, Abraham Karrass, and Donald Solitar. *Combinatorial group theory: Presentations of groups in terms of generators and relations.* Interscience Publishers [John Wiley & Sons], New York-London-Sydney, 1966.

[44] Juan Mariscal. The zeta function of generalized markoff equations over finite fields. *UNLV Theses, Dissertations, Professional Papers, and Capstones*, 2002.

[45] Martin Mereb. On the E-polynomials of a family of Sl_n-character varieties. *Math. Ann.*, 363(3-4):857–892, 2015.

[46] Yair N. Minsky. On dynamics of $Out(F_n)$ on $\mathrm{PSL}_2(\mathbb{C})$ characters. *Israel J. Math.*, 193(1):47–70, 2013.

[47] Masayoshi Nagata. Invariants of a group in an affine ring. *J. Math. Kyoto Univ.*, 3:369–377, 1963/64.

[48] Jakob Neilsen. Om regning med ikke kommutative faktoren og deus anvendelse i gruppeteorien. *Mat. Tidskr. B*, pages 77–94, 1927.

[49] Jakob Nielsen. *Jakob Nielsen: collected mathematical papers. Vol. 1.* Contemporary Mathematicians. Birkhäuser Boston, Inc., Boston, MA, 1986. Edited and with a preface by Vagn Lundsgaard Hansen.

[50] Frederic Palesi. Ergodic actions of mapping class groups on moduli spaces of representations of non-orientable surfaces. *Geom. Dedicata*, 151:107–140, 2011.

[51] Doug Pickrell and Eugene Z. Xia. Ergodicity of mapping class group actions on representation varieties. I. Closed surfaces. *Comment. Math. Helv.*, 77(2):339–362, 2002.

[52] Doug Pickrell and Eugene Z. Xia. Ergodicity of mapping class group actions on representation varieties. II. Surfaces with boundary. *Transform. Groups*, 8(4):397–402, 2003.

[53] Tovohery Hajatiana Randrianarisoa. The number of matrices over $\mathbb{F}_q$ with irreducible characteristic polynomial. *arXiv: Commutative Algebra*, 2014.

[54] R. W. Richardson. Conjugacy classes of n-tuples in Lie algebras and algebraic groups. *Duke Math. J.*, 57(1):1–35, 1988.

[55] Adam S. Sikora. Character varieties. *Trans. Amer. Math. Soc.*, 364(10):5173–5208, 2012.

[56] Ser Peow Tan, Yan Loi Wong, and Ying Zhang. The $\mathrm{SL}(2,\mathbb{C})$ character variety of a one-holed torus. *Electron. Res. Announc. Amer. Math. Soc.*, 11:103–110, 2005.

[57] Karen Vogtmann. Automorphisms of free groups and outer space. In *Proceedings of the Conference on Geometric and Combinatorial Group Theory, Part I (Haifa, 2000)*, volume 94, pages 1–31, 2002.

[58] Richard Weidmann. Generating tuples of free products. *Bull. Lond. Math. Soc.*, 39(3):393–403, 2007.

Curriculum Vitae

Cigole Thomas graduated with an Integrated BS-MS degree in Mathematics from the Indian Institute of Science Education and Research Mohali India in 2015. She has been enrolled as a Ph.D. student in the Department of Mathematics at George Mason University since 2016. She received her Master of Science in Mathematics from George Mason University in 2018.