REPRESENTATIONS OF FUNDAMENTAL GROUPS OF ABELIAN VARIETIES IN CHARACTERISTIC p

Brett Frankel

A DISSERTATION

in

Mathematics Presented to the Faculties of the University of Pennsylvania

in

Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy

2016

Supervisor of Dissertation

Ted Chinburg, Professor of Mathematics

Graduate Group Chairperson

David Harbater, Professor of Mathematics

Dissertation Committee:
Ted Chinburg, Professor of Mathematics
David Harbater, Professor of Mathematics
Jim Haglund, Professor of Mathematics

For Fatema, who so patiently uproots herself, time and again packing up and restarting her life and career, to accommodate my mathematical endeavors.

Acknowledgments

It is a pleasure to thank my advisor Ted Chinburg for his guidance and support over the past five years. Professors Ron Donagi, Julia Hartmann, Tony Pantev, Florian Pop, Steve Shatz, Henry Towsner, Scott Weinstein, and especially David Harbater have all contributed either to this thesis or to my mathematical development in noteworthy ways. I would also like to thank Aaron Silberstien and Zach Scherr for countless helpful discussions. I am grateful to Professor Fernando Rodriguez-Villegas for hosting me for a very productive week at the International Centre for Theoretical Physics. It was he who observed Corollary 14, and introduced me to both his theorem with Cameron Gordon [3] and the theorem of Frobenius, [1] from which one easily deduces Corollary 14. He also made me aware of Proposition 8. Bob Guralnick very helpfully referred me to both his paper with Sethuraman [4] and earlier work of Gerstenhaber [2] that made their way into this thesis. I have had many helpful and informative discussions with my classmates, among them Matti Åstrand, Max Gilula, Tyler Kelly, Jackie Lang, Anna Pun, Hua Qiang, Charlie Siegel, James Sundstrum, Siggy Tomaskovic-Moore, and Adam Topaz. Marcus Michelen and

Max Gilula provided help with formatting. I'd also like to thank the mathematics department staff: Janet Burns, Monica Pallanti, Paula Scarborough, Reshma Tanna and Robin Toney for their support.

Lastly, I wish to thank my friends and especially my family for their constant love and support. Graduate school can be a difficult and isolating experience, and I consider myself exceptionally fortunate not only to have completed my degree, but to be able to look back fondly at my graduate years.

ABSTRACT

REPRESENTATIONS OF FUNDAMENTAL GROUPS OF ABELIAN VARIETIES IN CHARACTERISTIC p

Brett Frankel

Ted Chinburg

Let A_g be an abelian variety of dimension g and p-rank $\lambda \leq 1$ over an algebraically closed field of characteristic $p > 0$. We compute the number of homomorphisms from $\pi_1^{\text{ét}}(A_g)$ to $GL_n(\mathbb{F}_q)$, where q is any power of p. We show that for fixed g, λ, and n, the number of such representations is polynomial in q. We show that the set of such homomorphisms forms a constructable set, and use the geometry of this space to deduce information about the coefficients and degree of the polynomial.

In the last chapter we prove a divisibility theorem about the number of homomorphisms from certain semidirect products of profinite groups into finite groups. As a corollary, we deduce that when $\lambda = 0$,

$$\frac{\# \operatorname{Hom}(\pi_1^{\text{ét}}(A_g), GL_n(\mathbb{F}_q))}{\# GL_n(\mathbb{F}_q)}$$

is a Laurent polynomial in q.

Contents

Chapter 1

Introduction

1.1 Representations of Fundamental Groups of Complex Algebraic Varieties

This thesis explores representations of the fundamental groups of certain algebraic varieties in characteristic $p > 0$. Before turning our attention to positive characteristic, it will be useful to survey some motivating examples over the complex numbers.

If X is a smooth projective complex variety, its fundamental group $\pi_1(X, x)$ is finitely generated. What follows will not depend on the choice of base point, so we will simply write $\pi_1(X)$. For any finitely-presented group $G = \langle \alpha_1, \cdots, \alpha_k | r_1, \cdots, r_m \rangle$, one may construct the variety of representations of G by associating to each representation $\rho : G \to GL_n(\mathbb{C})$ the point $(\rho(\alpha_1), \cdots, \rho(\alpha_k)) \subset GL_n(\mathbb{C})^k \subset \mathbb{A}^{kn^2}$. In fact, since $\mathbb{A}^{kn^2}$ is noetherian, only finite generation is necessary for this construction, not finite presentation. The set of all such representations is the locus in $GL_n(\mathbb{C})^k$ by the relations r_i, and each r_i is a closed condition, so we obtain a quasi-affine variety. (We will see in Proposition 7 that this construction is not always as well-behaved when G is profinite.) This construction does not depend on the choice of generating set; writing one generating set in term of another gives an isomorphism of the corresponding varieties. We then take the quotient of the conjugation action, but the resulting space is not separated. So we identify each representation with its semisimplification. This moduli space of representations of the fundamental group of X is called the *Character Variety* of X. [12]

In *Mixed Hodge Polynomials of Character Varieties*, [5] Hausel and Rodriguez-Villegas computed the number of homomorphisms from the fundamental group of a Riemann surface of genus g into $GL_n(\mathbb{F}_q)$. By van Kampen's theorem, this is equivalent to counting $2g$-tuples of matrices,

$$\begin{aligned} P(q) &= \#\operatorname{Hom}(\pi_1(X), GL_n(\mathbb{F}_q)) \\ &= \#\{(X_1, Y_1, \cdots, X_g, Y_g) : [X_1, Y_1][X_2, Y_2]\cdots[X_n, Y_n] = 1\}, \end{aligned}$$

where $[X_i, Y_i]$ denotes the commutator $XYX^{-1}Y^{-1}$. They also consider a twisted version of the problem, computing

$$\begin{aligned} R(q) &= \#\,\mathrm{Hom}_{twist}(\pi_1(X), GL_n(\mathbb{F}_q)) \\ &= \#\{(X_1, Y_1, \cdots, X_g, Y_g) : [X_1, Y_1][X_2, Y_2]\cdots[X_n, Y_n] = \zeta_n\}, \end{aligned}$$

where ζ_n is a primitive n^{th} root of 1.

The salient feature of both these counts is that, for fixed g and n, P and R are both polynomial functions of q. Another curious feature is that $P(q)$ is divisible by the order of $GL_n(\mathbb{F}_q)$. This phenomenon is explained in [3].

In the twisted case, PGL_n acts scheme-theoretically freely on $\mathrm{Hom}_{twist}(\pi_1(X), GL_n)$, and the GIT quotient $\mathcal{M}_n = \mathrm{Hom}_{twist}(\pi_1(X), GL_n)//PGL_n$ is the moduli space of twisted homomorphisms from $\pi_1(X)$ to GL_n. The polynomial point-counting formula is then used to produce the E-polynomial $E(\mathcal{M}_n, T)$ of $\mathcal{M}_n(\mathbb{C})$, which encodes information about the weight and Hodge filtrations on the cohomology of $\mathcal{M}_n$.

The bridge from combinatorics to Hodge theory is given by the following theorem.

Theorem 1 (N. Katz, Appendix to [5]). *Let $\mathcal{X}$ be a scheme over a ring R, where R is finite type over $\mathbb{Z}$. Fix an embedding $R \hookrightarrow \mathbb{C}$ so that $X = \mathcal{X} \times_R \mathbb{C}$ is a variety (i.e., separated and finite type over $\mathbb{C}$). If there exists a polynomial $P_X(T) \in \mathbb{Z}[t]$ such that for all primes p and all powers of q of p, $\#(\mathcal{X} \times_R \bar{\mathbb{F}}_p)(\mathbb{F}_q) = P_X(q)$, then $P_X(T) = E(X, T)$.*

1.2 Fundamental Groups in Positive Characteristic

We are interested in extending the combinatorial results of [5] where the Riemann surface X is replaced by a variety over an algebraically closed field of characteristic p.

The most natural generalization of [5] is to consider a curve $C/\bar{\mathbb{F}}_p$. However, in positive characteristic, the étale fundamental group is a much more subtle object. In particular, there is not a single curve of genus greater than 1 for which an explicit presentation of the fundamental group is known. [10]

However, these fundamental groups have well-understood abelianization; the abelianization of the fundamental group of a curve is the fundamental group of the Jacobian variety, which is the dual of the Jacobian. Thus we will concern ourselves in this thesis with representations of fundamental groups of abelian varieties.

Let A_g be an abelian variety of dimension g. The p-torsion points of A form a vector space over $\mathbb{F}_p$ of dimension $0 \leq \lambda \leq g$. We call λ the p-rank of A_g. The fundamental group of A_g is given by

$$\begin{aligned}\pi_1^{\text{ét}}(A_g) &\cong \prod_{\ell \neq p} (\mathbb{Z}_\ell)^{2g} \times \mathbb{Z}_p^\lambda \\ &\cong (\hat{\mathbb{Z}}')^{2g-\lambda} \times \hat{\mathbb{Z}}^\lambda,\end{aligned}$$

where

$$\hat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n$$

is the profinite completion of the group of integers and

$$\hat{\mathbb{Z}}' = \varprojlim_{(n,p)=1} \mathbb{Z}/n$$

is the group of integers completed away from the prime p. We will write $\pi_1(A_g)$ instead of $\pi_1^{\text{ét}}(A_g)$ in the remainder of this thesis.

Let q be a power of p. A homomorphism $\pi_1(A_g) \to GL_n(\mathbb{F}_q)$ is determined by the image of the topological generators, so specifying a homomorphism is equivalent to choosing an ordered $2g$-tuple of pairwise commuting matrices, such that the first $2g - \lambda$ have order not divisible by p. In Chapter 2 we compute the number of homomorphisms $\pi_1(A_g) \to GL_n(\mathbb{F}_q)$, where q is a power of p and the p-rank of A_g is either 0 or 1. We also compute the number of homomorphisms up to conjugation in the p-rank 0 case. All three counting formulas are polynomial in q, depending on g and n but not on the characteristic.

Chapter 3 considers the space of all such representation, and relates the geometry of this space to certain features of the polynomial formulas in the previous chapter.

Chapter 4 gives the profinite analogue of a theorem of Gordon and Villegas, [3] and deduces as a corollary that when the $\lambda = 0$, $\text{Hom}(\pi_1(A_g), GL_n(\mathbb{F}_q))/\#GL_n(\mathbb{F}_q)$ is a Laurent polynomial in q.

Chapter 2

Counting Formulas

Our main reference in this chapter is Macdonald's *Symmetric Functions and Hall Polynomials.* [8] Throughout, p will be a prime number, and q will denote a power of p.

2.1 Some Linear Algebra

For any matrix $X \in GL_n(\mathbb{F}_q)$ we have an associated $\mathbb{F}_q[T]$-module structure on $\mathbb{F}_q^n$, where T acts by X. If X and Y induce isomorphic module structures on $\mathbb{F}_q^n$, then the isomorphism of $\mathbb{F}_q[T]$-modules defines an element of $GL_n(\mathbb{F}_q)$, so X and Y are conjugate. Note that $X \in GL_n(\mathbb{F}_q)$ has order prime to p if and only if X acts semisimply on $\mathbb{F}_q^n$. That is, X is diagonalizable over $\bar{\mathbb{F}}_q$. Since elements of order prime to p act semisimply, the associated $\mathbb{F}_q[T]$-module is a direct sum of simple modules of the form $\mathbb{F}_q[T]/f(T)$, where the $f(T)$ are irreducible but not necessarily distinct.

Matrices of order prime to p are thus uniquely characterized, up to conjugation, by their characteristic polynomials.

2.2 Polynomials and their Types

Definition 2. *A* type Λ *of* n *is a partition of* n *along with a refinement of its conjugate. That is, a partition* λ *of* n *along with partitions* λ^i *of the multiplicities of the entries* i *of* λ.

This is a slight generalization of what Macdonald calls a type in [8]. For example, the data $\lambda = (5\ 3\ 3\ 3\ 3\ 3\ 2\ 2\ 2\ 1\ 1) = (5^{(1)}\ 3^{(5)}\ 2^{(3)}\ 1^{(2)})$, $\lambda^5 = (1)$, $\lambda^4 = \emptyset$, $\lambda^3 = (2\ 2\ 1)$, $\lambda^2 = (2\ 1)$, $\lambda^1 = (2)$ give a type of 28. We shall write $\lambda \vdash n$ when λ is a partition of n, and $\Lambda \vDash n$ when Λ is a type of n. By

$$\prod_{(i,r)\in\Lambda} f(i,r)$$

we will mean the product taken over all pairs (i,r) such that $i \in \lambda$ and $r \in \lambda^i$. We index over λ without multiplicity, but over $r \in \lambda^i$ with multiplicity. So if

$$\Lambda = \begin{cases} \lambda = (3\ 3\ 3\ 3\ 3\ 1\ 1) \\ \lambda^3 = (2\ 2\ 1) \\ \lambda^1 = (2) \end{cases},$$

then

$$\prod_{(i,r)\in\Lambda} f(i,r) = f(3,2)^2 f(3,1) f(1,2).$$

We associate to an $n \times n$ matrix X a type $\Lambda \vDash n$ by considering the characteristic polynomial $c_X(T)$ of X. Factoring $c_X(T)$ into irreducible factors gives a partition of $\lambda \vdash n$, where the entries of λ are the degrees of the irreducible factors of $c_X(T)$, counted with multiplicity. We then take λ^i to be the partition consisting of the multiplicity of each distinct degree-i factor of $c_X(T)$.

For example, over $\mathbb{F}_3$, we associate $\lambda = (3\ 3\ 1\ 1\ 1\ 1\ 1\ 1)$, $\lambda^3 = (2)$, $\lambda^1 = (3\ 3)$ to the polynomial $(T^3 + 2T + 1)^2 (T-2)^3 (T-1)^3$.

Recall that the number of irreducible monic polynomials over $\mathbb{F}_q$ of degree i is

$$\frac{1}{i} \sum_{k|i} \mu(k) q^{i/k},$$

where μ is the Möbius function. [7]

Definition 3. *Denote by $\psi_\Lambda(q)$ the number of monic polynomials $p(T) \in \mathbb{F}_q(T)$ with factorization type Λ.*

Note that $\psi_\Lambda(T) \in \mathbb{Q}[T]$, but in general $\psi_\Lambda(T) \notin \mathbb{Z}[T]$. For instance, if $\lambda = (1\ 1)$, $\lambda^1 = (1\ 1)$, then

$$\phi_\Lambda(q) = \frac{(q-1)(q-2)}{2}.$$

2.3 Counting

We now count the number of homomorphisms from $\pi_1(A_g)$ to $GL_n(\mathbb{F}_q)$, where the p-rank of A_g is 0. This is equivalent to counting $2g$-tuples of commuting matrices $(X_1, \ldots, X_k)$ such that each X_i has order prime to p. Since the combinatorial arguments below do not make use of the fact that $2g$ is even, we may state a slightly stronger theorem.

Theorem 4. *The number of ordered k-tuples of pairwise-commuting, semisimple, invertible matricies with entries in $\mathbb{F}_q$ is*

$$\#GL_n(q) \sum_{\Lambda_1 \vDash n} \psi_{\Lambda_1}(q) \prod_{(i_1,r_1)\in\Lambda_1} \sum_{\Lambda_2 \vDash r_1} \psi_{\Lambda_2}(q^{i_1}) \prod_{(i_2,r_2)\in\Lambda_2} \cdots$$
$$\cdots \sum_{\Lambda_{k-1}\vDash r_{k-2}} \psi_{\Lambda_{k-1}}(q^{i_1 i_2 \cdots i_{k-2}}) \prod_{(i_{k-1},r_{k-1})\in\Lambda_{k-1}} \sum_{\Lambda_k \vDash r_{k-1}} \frac{\psi_{\Lambda_k}(q^{i_1 i_2 \cdots i_{k-1}})}{\prod_{(i_k,r_k)\in\Lambda_k} \#GL_{r_k}(q^{i_1 i_2 \cdots i_k})}.$$

For instance, the number of commuting semisimple pairs $(X, Y) \in GL_2(\mathbb{F}_q)^2$ is

$$\#GL_2(\mathbb{F}_q)\frac{(q^3+q^2-q+1)}{q} = q^6 - 3q^4 + 2q^3 + q^2 - 2q + 1.$$

In $GL_3(\mathbb{F}_q)$, the number of semisimple commuting pairs is

$$\#GL_3(\mathbb{F}_q)\frac{q^6-q^5-q^4+2q^3-q^2+q-1}{q^3}$$
$$=q^{12} - 2q^{11} - q^{10} + 4q^9 - q^8 - 4q^6 + 2q^5 + 3q^4 - 2q^3 + q^2 - 2q + 1.$$

Proof. We first prove the theorem for $k = 2$. Since semisimple matrices are characterized, up to conjugation, by their characteristic polynomials, we associate to each such conjugacy class a type Λ. There are by definition $\psi_\Lambda(q)$ conjugacy classes of type Λ. Suppose X_1 is any matrix of order prime to p, with associated type Λ. A matrix Y commutes with X_1 if and only if Y acts X-equivariantly on $\mathbb{F}_q^n$. That is, writing $\mathbb{F}_q^n$ as a sum of simple modules

$$\mathbb{F}_q^n \cong \bigoplus_j (\mathbb{F}_q[T]/f_j(T))^{r_j},$$

the action of Y is a $\mathbb{F}_q[T]$-automorphism of each $(\mathbb{F}_q[T]/f_j(T))^{r_j}$. Specifying such an action is given by an element of $GL_{r_j}(\mathbb{F}_{q^{\deg f_j}})$. The order of the centralizer of a semisimple matrix X_1 with type Λ is thus

$$\prod_{f_j} \# GL_{r_j}(\mathbb{F}_{q^{\deg f_j}}) = \prod_{(i,r)\in\Lambda} \# GL_r(\mathbb{F}_{q^i}). \tag{2.3.1}$$

The matrix X_2 commutes with X_1 and also must be semisimple, so X_2 acts semisimply on each $(\mathbb{F}_q[T]/f_j(T))^{r_j}$. A semisimple matrix $Y_j \in GL_{r_j}(\mathbb{F}_{q^{\deg f_j}})$ is determined, up to conjugacy, by its characteristic polynomial, or equivalently by a type $N = (\nu, \nu^\ell) \vDash r_j$ and a polynomial of type N in $\mathbb{F}_{q^{\deg f_j}}[T]$. By the same argument used to compute the cardinality of the centralizer of X_1, we see that index of the centralizer of $Y_j \in GL_{r_j}(\mathbb{F}_{q^{\deg f_j}})$ is

$$\frac{\#GL_{r_j}(\mathbb{F}_{q^{\deg f_j}})}{\prod\limits_{(\ell,s)\in N} \#GL_s(\mathbb{F}_{q^{\deg(f_j)\ell}})} .$$

The number of all such Y_j is therefore

$$\sum_{N \vDash r_j} \left(\psi_N(q^{\deg f_j}) \frac{\#GL_{r_j}(\mathbb{F}_{q^{\deg f_j}})}{\prod\limits_{(\ell,\nu)\in N} \#GL_s(\mathbb{F}_{q^{\deg(f_j)\ell}})} \right) . \tag{2.3.2}$$

So, if X_1 is semisimple with type Λ, the number of semisimple matrices X_2 commuting with X_1 is

$$\begin{aligned} &\prod_{f_j} \sum_{N \vDash r_j} \left(\psi_N(q^{\deg f_j}) \frac{\#GL_{r_j}(\mathbb{F}_{q^{\deg f_j}})}{\prod\limits_{(\ell,s)\in N} \#GL_s(\mathbb{F}_{q^{\deg(f_j)\ell}})} \right) \\ &= \prod_{(i,r)\in\Lambda} \sum_{N \vDash r} \left(\psi_N(q^i) \frac{\#GL_r(\mathbb{F}_{q^i})}{\prod\limits_{(\ell,s)\in N} \#GL_s(\mathbb{F}_{q^{i\ell}})} \right) . \end{aligned} \tag{2.3.3}$$

Given a semisimple matrix $X \in GL_n(\mathbb{F}_q)$, we have just computed both the number of matrices (2.3.1) that commute with X and the number of semisimple matrices (2.3.3) that commute with X. Note that both of these numbers depend only on the type associated to X, since the deg(f_j)'s are the entries of λ, and the r_j's are the entries of the corresponding $\lambda^{\deg f_j}$'s.

From these two computations, we see that the number of pairs (X_1, X_2) of commuting semisimple matrices in $GL_n(\mathbb{F}_q)$ is

$$\sum_{\Lambda \vDash n} \sum_{\psi(\Lambda)} \frac{\#GL_n(\mathbb{F}_q)}{\prod\limits_{(i,r)\in\Lambda} \#GL_r(\mathbb{F}_{q^i})} \prod_{(i,r)\in\Lambda} \sum_{N \vDash r} \left(\psi_N(q^i) \frac{\#GL_r(\mathbb{F}_{q^i})}{\prod\limits_{(\ell,s)\in N} \#GL_s(\mathbb{F}_{q^{i\ell}})} \right) \tag{2.3.4}$$

where the second sum is taken over polynomials with type Λ. Since

$$\frac{\#GL_n(\mathbb{F}_q)}{\prod\limits_{(i,r)\in\Lambda} \#GL_r(\mathbb{F}_{q^i})} \prod_{(i,r)\in\Lambda} \sum_{N \vDash r} \left(\psi_N(q^i) \frac{\#GL_r(\mathbb{F}_{q^i})}{\prod\limits_{(\ell,s)\in N} \#GL_s(\mathbb{F}_{q^{i\ell}})} \right)$$

depends only on Λ, we may simplify (2.3.4) by replacing the second summation with multiplication by $\psi_\Lambda(q)$. Thus (2.3.4) simplifies to

$$\#GL_n(\mathbb{F}_q) \sum_{\Lambda \vDash n} \psi_\Lambda(q) \prod_{(i,r)\in\Lambda} \sum_{N \vDash r} \frac{\psi_N(q^i)}{\prod\limits_{(\ell,s)\in N} \#GL_s(\mathbb{F}_{q^{i\ell}})}. \tag{2.3.5}$$

We now continue by induction. Suppose the number of pairwise commuting $(k-1)$-tuples of semisimple elements of $GL_n(\mathbb{F}_q)$ is

$$\#GL_n(q) \sum_{\Lambda_1 \vDash n} \psi_{\Lambda_1}(q) \prod_{(i_1,r_1)\in\Lambda_1} \sum_{\Lambda_2 \vDash r_1} \psi_{\Lambda_2}(q^{i_1}) \prod_{(i_2,r_2)\in\Lambda_2} \cdots$$

$$\cdots \sum_{\Lambda_{k-2} \vDash r_{k-3}} \psi_{\Lambda_{k-2}}(q^{i_1 i_2 \cdots i_{k-3}}) \prod_{(i_{k-2},r_{k-2})\in\Lambda_{k-2}} \sum_{\Lambda_{k-1} \vDash r_{k-2}} \frac{\psi_{\Lambda_{k-1}}(q^{i_1 i_2 \cdots i_{k-2}})}{\prod\limits_{(i_{k-1},r_{k-1})\in\Lambda_{k-1}} \#GL_{r_{k-1}}(q^{i_1 i_2 \cdots i_{k-1}})}.$$

Suppose further that for each possible action of $X_1, \ldots, X_{k-1}$ on $\mathbb{F}_q^n$, the action of X_{k-1} on an isotypic summands of the $\mathbb{F}_q[X_1, \ldots, X_{k-2}]$-module $\mathbb{F}_q^n$ has characteristic polynomials of type Λ_{k-1} as above when these isotypic summands are viewed as

$\mathbb{F}_{q^{i_1 i_2 \cdots i_{k-2}}}$-vector spaces. (We note that Λ_{2k-1} may be different for different summands; indeed, $\Lambda_{k-1} \vDash r_{k-2}$, and the symbol r_{k-2} takes on different values in different terms of the above formula).

Since X_k commutes with each X_ℓ, $1 \leq \ell < k$, then X_k acts on $\mathbb{F}_q^n$ by acting on each isotypic summand, which by induction are $\mathbb{F}_{q^{i_1 i_2 \cdots i_{k-2}}}[X_{k-1}]$-modules, or $\mathbb{F}_{q^{i_1 i_2 \cdots i_{k-1}}}$-vector spaces of dimension r_{k-1}. There are

$$\sum_{\Lambda_k \vDash r_{k-1}} \psi_{\Lambda_k}(q^{i_1 i_2 \cdots i_{k-1}})$$

conjugacy classes of semisimple elements of $GL_{r_{k-1}}(\mathbb{F}_{q^{i_1 i_2 \cdots i_{k-1}}})$. By (2.3.1), each conjugacy class has

$$\frac{\#GL_{r_{k-1}}(\mathbb{F}_{q^{i_1 i_2 \cdots i_{k-1}}})}{\prod\limits_{(i_k, r_k) \in \Lambda_k} \#GL_{r_k}(\mathbb{F}_{q^{i_1 i_2 \cdots i_k}})}$$

elements, for a total of

$$F(r_{k-1}) = \sum_{\Lambda_k \vDash r_{k-1}} \psi_{\Lambda_k}(q^{i_1 i_2 \cdots i_{k-1}}) \frac{\#GL_{r_{k-1}}(\mathbb{F}_{q^{i_1 i_2 \cdots i_{k-1}}})}{\prod\limits_{(i_k, r_k) \in \Lambda_k} \#GL_{r_k}(\mathbb{F}_{q^{i_1 i_2 \cdots i_k}})}$$

possible X_k-actions on $\mathbb{F}^{r_{k-1}}_{q^{i_1 i_2 \cdots i_{k-1}}}$. So by induction, the number of pairwise-commuting k-tuples of semisimple matrices in $GL_n(\mathbb{F}_q)$ is

$$\#GL_n(q) \sum_{\Lambda_1 \vDash n} \psi_{\Lambda_1}(q) \prod_{(i_1, r_1) \in \Lambda_1} \sum_{\Lambda_2 \vDash r_1} \psi_{\Lambda_2}(q^{i_1}) \prod_{(i_2, r_2) \in \Lambda_2} \cdots$$

$$\cdots \sum_{\Lambda_{k-1} \vDash r_{k-2}} \psi_{\Lambda_{k-1}}(q^{i_1 \cdots i_{k-2}}) \prod_{(i_{k-1}, r_{k-1}) \in \Lambda_{k-1}} \frac{1}{\#GL_{r_{k-1}}(q^{i_1 \cdots i_{k-1}})} F(r_{k-1}).$$

Canceling factors of $\#GL_{r_{k-1}}(q^{i_1\cdots i_{k-1}})$, the above formula simplifies to the statement of the theorem. □

Observation. *From the proof, we see that the formula in Theorem 4 is polynomial in q. This polynomial depends on n and k, but not on the characteristic.*

The next theorem computes $\#\operatorname{Hom}(\pi_1(A_g), GL_n(\mathbb{F}_q))$ when the p-rank of A_g is 1.

Theorem 5. *The number of ordered k-tuples of invertible, pairwise-commuting matrices $(X_1, \ldots, X_{k-1}, Y)$ such that the X_i are all semisimple is*

$$\#GL_n(q) \sum_{\Lambda_1 \vDash n} \psi_{\Lambda_1}(q) \prod_{(i_1,r_1)\in\Lambda_1} \sum_{\Lambda_2\vDash r_1} \psi_{\Lambda_2}(q^{i_1}) \prod_{(i_2,r_2)\in\Lambda_2} \cdots$$
$$\cdots \sum_{\Lambda_{k-2}\vDash r_{k-3}} \psi_{\Lambda_{k-2}}(q^{i_1 i_2\cdots i_{k-3}}) \prod_{(i_{k-2},r_{k-2})\in\Lambda_{k-2}} (q^{i_1\cdots i_{k-2}} - 1)(q^{i_1\cdots i_{k-2}})^{r_{k-2}-1}.$$

Proof. As in the inductive step of the theorem, we assume the number of pairwise commuting $(k-2)$-tuples of semisimple elements of $GL_n(\mathbb{F}_q)$ is

$$\#GL_n(q) \sum_{\Lambda_1 \vDash n} \psi_{\Lambda_1}(q) \prod_{(i_1,r_1)\in\Lambda_1} \sum_{\Lambda_2\vDash r_1} \psi_{\Lambda_2}(q^{i_1}) \prod_{(i_2,r_2)\in\Lambda_2} \cdots$$
$$\cdots \sum_{\Lambda_{k-3}\vDash r_{k-4}} \psi_{\Lambda_{k-3}}(q^{i_1 i_2\cdots i_{k-4}}) \prod_{(i_{k-3},r_{k-3})\in\Lambda_{k-3}} \sum_{\Lambda_{k-2}\vDash r_{k-3}} \frac{\psi_{\Lambda_{k-2}}(q^{i_1 i_2\cdots i_{k-3}})}{\prod_{(i_{k-2},r_{k-2})\in\Lambda_{k-2}} \#GL_{r_{k-2}}(q^{i_1 i_2\cdots i_{k-2}})}.$$

As before, for each possible action of $X_1, \ldots, X_{k-2}$ on $\mathbb{F}_q^n$, the action of X_{k-2} on an isotypic summands of the $\mathbb{F}_q[X_1, \ldots, X_{k-3}]$-module $\mathbb{F}_q^n$ has characteristic polynomials of type Λ_{k-2} as above when these isotypic summands are viewed as $\mathbb{F}_{q^{i_1 i_2\cdots i_{k-3}}}$-vector spaces.

Thus it suffices to count the number of pairs X_{k-1}, Y which act on each isotypic summand of the $\mathbb{F}_q[X_1, \dots, X_{k-2}]$-module $\mathbb{F}_q^n$. By assumption, these summands are of the form $\mathbb{F}_{q^{i_1 \cdots i_{k-2}}}^{r_{k-2}}$.

Let $\mathcal{O}$ be the orbit, under the conjugation action in $GL_{r_{k-2}}(\mathbb{F}_{q^{i_1 \cdots i_{k-2}}})$, of a matrix of order prime-to-p. Given any X_{k-1}, we will denote by A its restriction to the isotypic summand in question, and similarly B will denote the restriction of Y. For any $A \in \mathcal{O}$, the number of nonsingular matrices B that commute with A is the order of the centralizer of A. The number of elements in $\mathcal{O}$ is the index of the centralizer of A. Thus there are precisely $\#GL_{r_{k-2}}(\mathbb{F}_{q^{i_1 \cdots i_{k-2}}})$ pairs (A, B) such that A and B commute and $A \in \mathcal{O}$. So to compute the number of pairs (A, B) with $[A, B] = 1$ and $|A|$ prime to p, we need only count the number of possible conjugacy classes A. These are in bijection with characteristic polynomials, of which there are $(q^{i_1 \cdots i_{k-2}})^{r_{k-2}-1}(q^{i_1 \cdots i_{k-2}} - 1)$.

Thus the number of pairwise commuting k-tuples of invertible $n \times n$ matrices $(X_1, \dots, X_{k-1}, Y)$, of which all but possibly the last have order prime to p, is

$$\#GL_n(q) \sum_{\Lambda_1 \vDash n} \psi_{\Lambda_1}(q) \prod_{(i_1, r_1) \in \Lambda_1} \sum_{\Lambda_2 \vDash r_1} \psi_{\Lambda_2}(q^{i_1}) \prod_{(i_2, r_2) \in \Lambda_2} \cdots$$

$$\cdots \sum_{\Lambda_{k-3} \vDash r_{k-4}} \psi_{\Lambda_{k-3}}(q^{i_1 \cdots i_{k-4}}) \prod_{(i_{k-3}, r_{k-3}) \in \Lambda_{k-3}} \sum_{\Lambda_{k-2} \vDash r_{k-3}} \frac{\psi_{\Lambda_{k-2}}(q^{i_1 \cdots i_{k-3}}) \#(A, B)}{\prod_{(i_{k-2}, r_{k-2}) \in \Lambda_{k-2}} \#GL_{r_{k-2}}(q^{i_1 \cdots i_{k-2}})},$$

where

$$\#(A,B) = \prod_{(i_{k-2},r_{k-2})\in\Lambda_{k-2}} \#GL_{r_{k-2}}(\mathbb{F}_{q^{i_1\cdots i_{k-2}}})(q^{i_1\cdots i_{k-2}})^{r_{k-2}-1}(q^{i_1\cdots i_{k-2}}-1).$$

After cancellation we arrive at the statement of the theorem. □

Theorem 6. *The number of conjugacy classes of k-tuples of pairwise-commuting, invertible, semisimple matrices is*

$$\begin{aligned}&\#\{(X_1,\ldots,X_k)\}/\sim= \\ &\sum_{\Lambda_1\vDash n}\psi_{\Lambda_1}(q)\prod_{(i_1,r_1)\in\Lambda_1}\sum_{\Lambda_2\vDash r_1}\psi_{\Lambda_2}(q^{i_1})\prod_{(i_2,r_2)\in\Lambda_2}\cdots \\ &\cdots\sum_{\Lambda_{k-1}\vDash r_{k-2}}\psi_{\Lambda_{k-1}}(q^{i_1i_2\cdots i_{k-2}})\prod_{(i_{k-1},r_{k-1})\in\Lambda_{k-1}}(q^{i_1\cdots i_{k-1}})^{r_{k-1}-1}(q^{i_1\cdots i_{k-1}}-1).\end{aligned}$$

Proof. Observe that $Y\in GL_n(\mathbb{F}_q)$ stabilizes $(X_1,\ldots,X_k)$ if and only if it commutes with each X_ℓ. Writing $Z(X_1,\ldots,X_k)$ for the order of the stabilizer of $(X_1,\ldots,X_k)$ and applying the orbit-stabilizer lemma,

$$\begin{aligned}\#\{(X_1,\ldots,X_k)\}/\sim &= \sum_{\{(X_1,\ldots,X_k)\}}\frac{Z(X_1,\ldots,X_k)}{\#GL_n(\mathbb{F}_q)} \\ &= \frac{1}{\#GL_n(\mathbb{F}_q)}\sum_{\{(X_1,\ldots,X_k)\}}Z(X_1,\ldots,X_k) \\ &= \frac{1}{\#GL_n(\mathbb{F}_q)}\sum_{\{(X_1,\ldots,X_k,Y)\}}1\end{aligned}$$

where the last sum is taken over $k+1$-tuples pairwise commuting semisimple matrices

$(X_1, \ldots, X_k, Y)$ with all X_ℓ semisimple. The value of this sum was computed in Theorem 5. $\square$

Chapter 3

The Space of Representations

In this chapter, A_g will be an abelian variety with p-rank 0, as before. However, all statements apply if the p-rank of A_g is 1, mutatis mutandi. All schemes below are reduced. Recall that a subset of affine (or projective) space is said to be *constructable* if it may be expressed as a Boolean combination of Zariski-closed sets. [9]

Fix n, and let $R = \mathrm{Hom}(\pi_1(A_g), GL_n(\bar{\mathbb{F}}_q))$. Recall that a representation of $\pi_1(A_g)$ is given by a choice of $2g$ invertible matrices X^k, $1 \leq i \leq 2g$, such that these matrices are pairwise commuting and each have order relatively prime to p. Assigning a matrix $(X^k_{ij})_{1\leq i,j\leq n}$ to each generator, we may view R as a subset of $\mathbb{A}^{2gn^2}$.

We will now show that for fixed n and g, the set $R = \mathrm{Hom}(\pi_1(A_g), GL_n(\bar{\mathbb{F}}_q))$ of all representations may be considered a constructible set.

Proposition 7. *R is constructable.*

Proof. The requirement that the matrices pairwise commute defines a closed affine subscheme. We may specify that the matrices are (simultaneously) diagonalizable with the statement that there exists an invertible matrix C (with coordinates $C^{i,j}$, $1 \leq i, j \leq n$) so that CX^kC^{-1} is diagonal for each k. This last statement requires an existential quantifier, and thus does not necessarily define a subscheme, but it is a first order statement in the sense of model theory, and hence the space of representations is a definable subset of $\mathbb{A}^{2gn^2}$. Since the theory of algebraically closed fields admits quantifier elimination, [9] every definable set is in fact constructable, i.e. a Boolean combination of closed subschemes. □

Alternatively, since we are considering simultaneously diagonalizable matrices, one may write the diagonalization of each X_k as an element of a torus, and then define a morphism $GL_n \times \mathbb{G}_m^{2gn} \to \mathbb{A}^{2gn^2}$, $(C, X_1, \ldots, X_{2g}) \mapsto (C^{-1}X_1C, \ldots, C^{-1}X_{2g}C)$. By Chevalley's Theorem, [9] the image of this morphism, which is equal to R, is constructable. □

Since R is constructable, we may write $R = (R_1 - R_1') \cup (R_2 - R_2') \cup \ldots \cup (R_t - R_t')$, where each R_i is a projective variety and R_i' is a (possibly empty) closed subscheme of R_i. Alternatively, since R is contained in affine space, we may choose each R_i and R_i' to be affine.

Proposition 8. *Let $P(T)$ be the polynomial such that $P(q) = \#R(\mathbb{F}_q)$, the number of $\mathbb{F}_q$-rational points of R. Then $P(T) \in \mathbb{Z}[T]$.*

This argument is not new, and can be found in the appendix of [5] by Katz.

Proof. Chose q so that each R_i and R_i' is defined over $\mathbb{F}_q$. Let

$P(T) = a_0 + a_1T + \ldots a_dT^d$. Then the zeta function $Z(R,T)$ is defined to be

$$Z(R,T) = \exp(\sum_{n=0}^{\infty} R(\mathbb{F}_{q^n})T^n/n) = \exp(\sum_{n=0}^{\infty} P(q^n)T^n/n)$$

On the other hand, each R_i and R_i' is a projective variety, each $Z(R_i,T)$ and $Z(R_i',T)$ is rational, and

$$Z(R,T) = \prod_i \frac{Z(R_i,T)}{Z(R_i',T)}.$$

Writing

$$Z(R,T) = \frac{(1-\alpha_1T)\cdots(1-\alpha_rT)}{(1-\beta_1T)\cdots(1-\beta_sT)}$$

in lowest terms and taking logs, we see that

$$\begin{aligned}\sum_{j=1}^{r}\log(1-\alpha_jT) - \sum_{k=1}^{s}\log(1-\beta_kT) &= \log Z(R,T)\\ &= \sum_{n=0}^{\infty} P(q^n)T^n/n\\ &= \sum_{n=0}^{\infty}\sum_{i=0}^{d} a_iq^{in}T^n/n.\end{aligned}$$

And so, taking derivatives,

$$\sum_{k=1}^{s}\frac{\beta_k}{1-\beta_kT} - \sum_{j=1}^{r}\frac{\alpha_j}{1-\alpha_jT} = \frac{\partial}{\partial T}Z(R,T) = \sum_{n=0}^{\infty}\sum_{i=1}^{d} a_iq^{in}T^{n-1} = \sum_{i=1}^{d}\frac{a_iq^i}{1-q^iT}.$$

Comparing poles, each α_j and β_k must be a power of q. Comparing numerators we see that for each i, either a_i is the number of k such that $\beta_k = q^i$, or $-a_i$ is the number of j for which $\alpha_j = q^i$. □

From the above proof, we see that the leading coefficient of $P(T)$ is the multiplicity of $(1 - \beta_s T)$ in the denominator of $Z(R, T)$.

Theorem 9 (R. Guralnick, B. Sethuraman [4]). *Let V be the variety of commuting k-tuples of $n \times n$ matrices. If $\Delta \subset V$ denotes the union of the discriminant loci, i.e. the set on which at least one matrix has a repeated eigenvalue, then the the closure of $R - \Delta$ is an irreducible component of V. The dimension of this component is $n^2 + (k-1)n$.*

Corollary 10. *The degree of $P(T)$ is at least $n^2 + (2g-1)n$.*

Proof. Let $D \subset V$ be the union of the determinant loci, the set on which at least one matrix is not invertible. Note that $V \supset R \supset V - (\Delta \cup D)$. Then we may decompose $R = (R_1 - R_1') \cup (R_2 - R_2') \cup \ldots \cup (R_t - R_t')$, where R_1 is the closure of $V - \Delta$, $R_1' = \Delta \cup D$, and all $R_i \subset (\Delta \cup D)$ for all $i > 1$. By theorem 9, the closure of $R_1 - \Delta$ is irreducible, and is thus equal to the closure of $R_1 - (\Delta \cup D)$ because D is closed. From the proof of Proposition 8, the degree of $P(T)$ is $\sup_i \dim R_i$, and $\dim R_1 = n^2 + (k-1)$. □

Theorem 11 (Gerstenhaber [2]). *The variety of commuting pairs of matrices is irreducible.*

Corollary 12. *When $g = 1$, $P(T)$ is monic of degree $n^2 + (2g-1)n$.*

Proof. Since the variety V of pairs of commuting matrices is irreducible, we may write $R_1 = V$ and $R_1' = \Delta \cup D$, and $V \supset R \supset V - (\Delta \cup D)$ as in the proof of Corollary 10. All remaining R_i are contained in $\Delta \cup D$, which is a closed subvariety of an irreducible variety and therefore of strictly lower dimension. □

Chapter 4

A Divisibility Theorem for Profinite Groups

4.1 Introduction and Statement of Theorem

In "On the divisibility of $\#\operatorname{Hom}(\Gamma, G)$ by $|G|$," [3] Cameron Gordon and Fernando Rodriguez-Villegas prove that for a finitely-generated group $\tilde{\Gamma}$, $\tilde{\Gamma}$ has infinite abelianization if and only if it satisfies the divisibility condition in the paper's title for all finite groups G. This extends a result of Louis Solomon [13] which proves the same, assuming $\tilde{\Gamma}$ has a presentation with more generators than relations. Using their notation, $\#$ will denote the cardinality of a set, while $|\cdot|$ will be the order of either a finite group or an element of a finite group. By *homomorphism*, we will always mean a continuous homomorphism, where where countable groups are given the discrete topology. In this chapter, we state and prove the following profinite analogue of the theorem in [3]:

Theorem 13. *Let S be a set of primes (not necessarily finite), and let $\hat{\mathbb{Z}}_S = \varprojlim \mathbb{Z}/n$, where the the inverse limit is taken over all natural numbers n not divisible by any prime in S. Then for any topologically finitely generated profinite group Γ and finite group G,*

$$\frac{\#\operatorname{Hom}(\Gamma \rtimes \hat{\mathbb{Z}}_S, G)}{|G|} \in \mathcal{S}^{-1}\mathbb{Z},$$

where $\Gamma \rtimes \hat{\mathbb{Z}}_S$ is any semidirect product of Γ and G, and $\mathcal{S}$ is the multiplicative set generated by the elements of S. Conversely, if $\tilde{\Gamma}$ is topologically finitely generated and

$$\frac{\#\operatorname{Hom}(\tilde{\Gamma}, G)}{|G|} \in \mathcal{S}^{-1}\mathbb{Z}$$

for all finite groups G, then there exists a Γ with $\tilde{\Gamma} \cong \Gamma \rtimes \hat{\mathbb{Z}}_S$.

Remark. *This result is precisely the profinite version of [3], because a finitely generated group has infinite abelianiztion if and only if it is of the form $\Gamma \rtimes \mathbb{Z}$.*

Corollary 14. *Let $P(T)$ be as in the previous section, i.e. the unique polynomial such that $P(q) = \operatorname{Hom}(\pi_1(A_g), GL_n(\mathbb{F}_q))$ whenever q is a power of p, and denote by $G(T)$ the polynomial such that $G(q) = \#GL_n(\mathbb{F}_q)$. Then*

$$\frac{P(T)}{\#GL_n(\mathbb{F}_q)} \in \mathbb{Z}[T, \frac{1}{T}].$$

Proof. Choose $S = \{p\}$. Writing $\pi_1(A_g) \cong (\hat{\mathbb{Z}}')^{2g} \cong (\hat{\mathbb{Z}}')^{2g-1} \times \hat{\mathbb{Z}}' \cong (\hat{\mathbb{Z}}')^{2g-1} \times \hat{\mathbb{Z}}_S$, we see that for all q, $P(q)/\#GL_n(\mathbb{F}_q)$ is a rational number whose denominator is divisible only by the prime p. Thus $T^n\frac{P(T)}{G(T)} \in \mathbb{Q}[T]$ for sufficiently large n. Since $G(T)$ is monic, $T^n\frac{P(T)}{G(T)} \in \mathbb{Z}[T]$. □

4.2 Proof (first statement)

In this section we prove that for any topologically finitely generated Γ, the number of homomorphisms from $\Gamma \rtimes \hat{\mathbb{Z}}_S$ to G, when divided by $|G|$, has denominator divisible only by primes in S.

We first recall a theorem of Frobenius. [1] (See [6] for a short elementary proof.)

Theorem 15. *If H is a finite group and $n \mid |H|$, then the number of elements of H with order dividing n is a multiple of n.*

Lemma 16. *Let G be a finite group, and H a subgroup of order $p^r m$, with $p \nmid m$. Choose $g \in N_G(H)$ with $|g|$ a power of p. Then the set $\{x \in Hg : |x| \text{ is a power of } p\}$ has cardinality divisible by p^r.*

Proof. We may assume that $g \notin H$, for otherwise the lemma follows from Theorem 15, and then reduce to the case that $G = \langle H, g\rangle$, since it suffices to prove the lemma for this subgroup. Let p^s be the least positive integer with $g^{p^s} \in H$.

By Theorem 15, the number of elements of G with p-power order is a multiple of p^{r+s}, and the number of such elements in $K = \langle H, g^p\rangle$ is a multiple of p^{r+s-1}. Thus the number of elements of $G \backslash K$ with p-power order is a multiple of p^{r+s-1}.

Let $x \in G \backslash K$ be of p-power order. Then we may write $x = yg^t$ with $y \in H$ and $p \nmid t$. The group $\mathbb{Z}/(p^{r+s})^\times$ acts on the set of of all such x, $n \cdot x = x^n$. The orbit of x under this action is the set of generators of $\langle x \rangle$, and $\langle x \rangle$ surjects onto $\langle g \rangle / \langle g^{p^s} \rangle$. Each orbit inside $G \backslash K$ therefore contains the same number of elements in each coset of the form Hg^u with $p \nmid u$. $G \backslash K$ is the union of $\varphi(p^s) = p^{s-1}(p-1)$ cosets of H, so the number of elements of Hg with p-power order is equal to
$\#\{x \in G \backslash K : |x| \text{ is a power of } p\}/\varphi(p^s)$, and is thus divisible by p^r. □

For any $p \notin S$ we may write $\Gamma \rtimes \hat{\mathbb{Z}}_S \cong (\Gamma \rtimes \hat{\mathbb{Z}}_{S \cup \{p\}}) \rtimes \mathbb{Z}_p$. Therefore, we have reduced the statement of the theorem to the following:

Proposition 17. *Suppose Γ is any topologically finitely generated profinite group, and let v_p denote the p-adic valuation on the integers. Then*

$$v_p\left(\frac{\#\operatorname{Hom}(\Gamma \rtimes \mathbb{Z}_p, G)}{|G|}\right) \geq 0.$$

The proof of the proposition is now a straightforward modification of the argument in [3].

Proof. A homomorphism $\Phi : \Gamma \rtimes \mathbb{Z}_p$ is determined by its restriction $\phi = \Phi\Big|_\Gamma$ and the image of $1 \in \mathbb{Z}_p$, which is an element $g \in G$ such that the order of g is a power of p, subject to the condition that $\phi((-1)\gamma(1)) = g^{-1}\phi(\gamma)g$ for all $\gamma \in \Gamma$. In particular, this condition ensures that g normalizes $\phi(\Gamma)$, and thus normalizes the centralizer C_ϕ of $\phi(\Gamma)$. Observe that if a pair (ϕ, g) determines a well-defined homomorphism

$\Gamma \rtimes \mathbb{Z}_p \to G$ as above, then so does (ϕ, x) if and only if $|x|$ is a power of p and $x \in C_\phi g$. Thus

$$\begin{aligned}
&\#\operatorname{Hom}(\Gamma \rtimes \mathbb{Z}_p, G) \\
=&\sum_\phi \#\{g \in G : |g| \text{ is a power of } p,\ g^{-1}\phi(\gamma)g = \phi((-1)\gamma 1)\ \forall\ \gamma \in \Gamma\},
\end{aligned}$$

where the sum is taken over all ϕ which are restrictions of homomorphisms from $\Gamma \rtimes \mathbb{Z}_p$, ie. those ϕ for which there exists such a g. We let G act by conjugation on the set of homomorphisms restricted to Γ. The stabilizer of ϕ under this action is C_ϕ. Denoting by the orbit of ϕ by $[\phi]$, each element of $[\phi]$ extends to the same number of homomorphisms on $\Gamma \rtimes \mathbb{Z}_p$. For each $[\phi]$ choose a representative ϕ and an element $g_\phi \in G$ such that (ϕ, g_ϕ) determines a homomorphism.

$$\begin{aligned}
&\#\operatorname{Hom}(\Gamma \rtimes \mathbb{Z}_p, G) \\
=&\sum_\phi \#\{g \in G : |g| \text{ is a power of } p,\ g^{-1}\phi(\gamma)g = \phi((-1)\gamma 1)\ \forall\ \gamma \in \Gamma\} \\
=&\sum_{[\phi]} \frac{|G|}{|C_\phi|}\#\{g \in G : |g| \text{ is a power of } p,\ g^{-1}\phi(\gamma)g = \phi((-1)\gamma 1)\ \forall\ \gamma \in \Gamma\} \\
=&\sum_{[\phi]} \frac{|G|}{|C_\phi|}\#\{x \in C_\phi g_\phi : |x| \text{ is a power of } p\}.
\end{aligned}$$

The proposition follows by applying Lemma 16 to the coset $C_\phi g_\phi$. □

4.3 Proof of the Converse

We have the following proposition:

Lemma 18. *Let S and $\mathcal{S}$ be as above, and $\tilde{\Gamma}$ a topologically finitely generated profinite group. Suppose that for all finite groups G, $\#\operatorname{Hom}(\tilde{\Gamma}, G)/|G| \in \mathcal{S}^{-1}\mathbb{Z}$. Then $\tilde{\Gamma}$ has*

$$\hat{\mathbb{Z}}_S = \varprojlim_{\substack{(n,p)=1 \\ \forall p \in S}} \mathbb{Z}/n$$

as a quotient.

Proof. Suppose $\tilde{\Gamma}$ does not surject onto

$$\varprojlim_{\substack{(n,p)=1 \\ \forall p \in S}} \mathbb{Z}/n.$$

Then for some prime $\ell \notin S$ and sufficiently large m, $\tilde{\Gamma}$ does not surject onto $\mathbb{Z}/\ell^m$. All homomorphisms from $\tilde{\Gamma}$ to abelian ℓ-groups factor through the maximal pro-abelian ℓ-quotient of $\tilde{\Gamma}$, which is itself a quotient of $(\mathbb{Z}/\ell^{m-1})^r$, where $\tilde{\Gamma}$ is topologically generated by r generators. But there are at most $\ell^{r(m-1)}$ homomorphisms $(\mathbb{Z}/\ell^{m-1})^r \to \mathbb{Z}/\ell^s$. Taking $s > r(m-1)$ and $G = \mathbb{Z}/\ell^s$, we see that $\#\operatorname{Hom}(\tilde{\Gamma}, G)$ is not a multiple of $|G|$, and thus is not an element of $\mathcal{S}^{-1}\mathbb{Z}$. □

All that remains to be shown is that $\tilde{\Gamma}$ is a semidirect product, which follows from the proposition below.

Proposition 19. *Let $f : H \to \hat{\mathbb{Z}}_S$ be a continuous surjection of profinite groups. Then f has a continuous section with closed image.*

Proof. Let $h \in H$ with $f(h) = 1$. Consider the closed subgroup $\overline{< h >}$ generated by h. It is isomorphic to a product $\prod_{p \in I} \mathbb{Z}_p \times \prod_{p \notin I} \mathbb{Z}/p^{n_p}$, where I is a set of primes. The order of h, as a supernatural number, is divisible by the order of $1 \in \hat{\mathbb{Z}}_S$, and so S is contained in the complement of I (See [11]). Thus $\overline{< h >}$ has a direct factor K isomorphic to $\hat{\mathbb{Z}}_S$, which is a closed subgroup of H. K is topologically generated by the image k of h under the projection map $\overline{< h >} \to K$, and $f(k) = 1$. So H has a closed subgroup K which is abstractly isomorphic to $\hat{\mathbb{Z}}_S$, and f sends a topological generator of K to a topological generator of $\hat{\mathbb{Z}}_S$. The restriction of f to K is thus an isomorphism, and therefore admits a section. □

Remark. *We have in fact proven a stronger statement than the theorem. Namely, it suffices to check that $\# \operatorname{Hom}(\tilde{\Gamma}, G)/|G| \in \mathcal{S}^{-1}\mathbb{Z}$ only for groups of the form $G = \mathbb{Z}/p^e$, where $p \notin S$.*

Bibliography

[1] F. G. Frobenius. Verallgemeinerung des Sylow'schen satzes. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, pages 981–993, 1895.

[2] M. Gerstenhaber. On dominance and varieties of commuting matrices. *Annals of Mathematics*, 73:324–348, 1961.

[3] C. Gordon and F. Rodriguez-Villegas. On the divisibility of $\#Hom(\Gamma, G)$ by $|G|$. *Journal of Algebra*, 350(1):300–307, 2012.

[4] R. M. Guralnick and B. A. Sethuraman. Commuting pairs and triples of matrices and related varieties. *Linear Algebra and its Applications*, 310(1-3):139–148, 2000.

[5] T. Hausel and F. Rodriguez-Villegas. Mixed Hodge polynomials of character varieties. *Inventiones Mathematicae*, 174:555–624, 2008.

[6] M. I. Isaacs and G. R. Robinson. On a theorem of Frobenius: Solutions of $x^n = 1$ in finite groups. *The American Mathematical Monthly*, 99(4):352–354, 1992.

[7] S. Lang. *Algebra.* Number 217 in Graduate Texts in Mathematics. Springer-Verlag, New York, revised third edition, 2000.

[8] I. G. MacDonald. *Symmetric Functions and Hall Polynomials.* Oxford Mathematical Monographs. Oxford University Press, New York, second edition, 1995.

[9] D. Marker. *Model Theory: An Introduction.* Number 217 in Graduate Texts in Mathematics. Springer-Verlag, New York, 2000.

[10] R. Pries and K. Stevenson. A survey of Galois theory of curves in characteristic p. *Fields Institute Communications*, 60:169–191, 2011.

[11] J-P. Serre. *Galois Cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, corrected second printing of the second edition, 2002.

[12] C. T. Simpson. Moduli of representations of the fundamental group of a smooth projective variety I. *Publications mathématiques de l'I.H.E.S.*, 79:47–129, 1994.

[13] L. Solomon. The solution of equations in groups. *Archiv der mathematik*, 20(3):241–247, 1969.