Roditty-Gershon, E., Hall, C., & Keating, J. P. (2019). Variance of sums in arithmetic progressions of arithmetic functions associated with higher degree 0-functions in $F_q[t]$. *International Journal of Number Theory*, *16*(5), 1013-1030. https://doi.org/10.1142/S1793042120500529

VARIANCE OF ARITHMETIC SUMS AND L-FUNCTIONS IN $\mathbb{F}_q[t]$

CHRIS HALL, JONATHAN P. KEATING, AND EDVA RODITTY-GERSHON

Abstract. We compute the variances of sums in arithmetic progressions of arithmetic functions associated with certain L-functions of degree two and higher in $\mathbb{F}_q[t]$, in the limit as $q \to \infty$. This is achieved by establishing appropriate equidistribution results for the associated Frobenius conjugacy classes. The variances are thus related to matrix integrals, which may be evaluated. Our results differ significantly from those that hold in the case of degree-one L-functions (i.e. situations considered previously using this approach). They correspond to expressions found recently in the number field setting assuming a generalization of the pair-correlation conjecture. Our calculations apply, for example, to elliptic curves defined over $\mathbb{F}_q[t]$.

1. Introduction

1.1. **Analytic motivation.** Let $\Lambda(n)$ denote the von Mangoldt function, defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

The prime number theorem implies that

$$\sum_{n \leq x} \Lambda(n) = x + o(x),$$

as $x \to \infty$, determining the average of $\Lambda(n)$ over long intervals. In many problems one needs to understand sums over shorter intervals and in arithmetic progressions. This is significantly more difficult, because the fluctuations between different short intervals/arithmetic progressions can be large, and in many important cases we do not have rigorous results.

One may seek to characterize the fluctuations in these sums via their variances. These variances are the subject of several long-standing conjectures. For example, in the case of short intervals Goldston and Montgomery [GM87] have made the following conjecture

Conjecture 1.1.1 (Variance of primes in short intervals)**.** *For any fixed $\varepsilon > 0$,*

$$\int_1^X \Big(\sum_{X \leq n \leq x+h} \Lambda(n) - h \Big)^2 dx \sim hX \big(\log X - \log h \big)$$

uniformly for $1 \leq h \leq X^{1-\varepsilon}$.

It is natural to try to compute the variance in Conjecture 1.1.1 using the Hardy-Littlewood Conjecture

$$\sum_{n \leq X} \Lambda(n)\Lambda(n+k) \sim \mathfrak{S}(k)X \tag{1.1.2}$$

We are pleased to acknowledge support under EPSRC Programme Grant EP/K034383/1 LMF: L-Functions and Modular Forms. JPK is also grateful for support through a Royal Society Wolfson Research Merit Award and a Royal Society Leverhulme Senior Research Fellowship. We thank Nick Katz, Emmanuel Kowalski, and Zeev Rudnick for discussion and helpful comments. We also gratefully acknowledge the anonymous referees for reading the drafts very carefully and providing meticulous reports.

as $X \to \infty$, where $\mathfrak{S}(k)$ is the singular series, defined in terms of products over primes p and q

$$\mathfrak{S}(k) = \begin{cases} 2\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{\substack{q>2\\ q|k}}\frac{q-1}{q-2} & \text{if } k \text{ is even,} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

Montgomery and Soundararajan [MS04] proved that (1.1.2), together with an assumption concerning the implicit error term, implies a more precise asymptotic for the variance in Conjecture 1.1.1 when $\log X \le h \le X^{1/2}$, namely that it is equal to

$$hX\big(\log X - \log h - \gamma_0 - \log 2\pi\big) + O_\varepsilon\Big(h^{15/16}X(\log X)^{17/16} + h^2X^{1/2+\varepsilon}\Big),$$

where γ_0 is the Euler-Mascheroni constant.

An alternative approach to computing this variance follows from

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s},$$

which links statistical properties of $\Lambda(n)$ to those of the zeros of the Riemann zeta-function $\zeta(s)$. Taking this line, Goldston and Montgomery [GM87] proved that Conjecture 1.1.1 is equivalent to the following conjecture, due to Montgomery [Mon73], concerning the pair correlation of the non-trivial zeros of the zeta-function. Denoting the nontrivial zeros by $\frac{1}{2}+i\gamma$ and assuming the Riemann Hypothesis (so $\gamma \in \mathbb{R}$), let

$$\mathcal{F}(X,T) = \sum_{0<\gamma,\gamma'\le T} X^{i(\gamma-\gamma')}w(\gamma-\gamma'),$$

where $w(u) = \frac{4}{4+u^2}$.

Conjecture 1.1.3 (Montgomery's Pair Correlation Conjecture)**.** *For any fixed $A \ge 1$*

$$\mathcal{F}(X,T) \sim \frac{T\log T}{2\pi}$$

uniformly for $T \le X \le T^A$.

See also [Cha03] and [LPZ12], where lower order terms are considered in the equivalence.

There is a similar theory in the case of sums in arithmetic progressions. The Prime Number Theorem for arithmetic progression states that for a fixed modulus c, when A is coprime to c

$$\sum_{\substack{n\le X\\ n=A \bmod c}} \Lambda(n) \sim \frac{X}{\phi(c)}, \qquad \text{as } X\to\infty\ , \tag{1.1.4}$$

where $\phi(c)$ is the Euler totient function, giving the number of reduced residues modulo c. The variance of sums over different arithmetic progressions is then defined by

$$G(X,c) = \sum_{\substack{A \bmod c\\ \gcd(A,c)=1}} \left|\sum_{\substack{n\le X\\ n\equiv A \bmod c}} \Lambda(n) - \frac{X}{\phi(c)}\right|^2. \tag{1.1.5}$$

Asymptotic formulae are known when $G(X,c)$ is summed over a long range of values of c (c.f. [Mon70], [Hoo75b] and [Hoo74]), but much less is known concerning $G(X,c)$ itself. In the latter case, Hooley has made the following conjecture [Hoo75a].

Conjecture 1.1.6 (Variance of primes in arithmetic progressions)**.**

$$G(X,c) \sim X\log c.$$

Hooley was not specific about the size of c relative to X for which this asymptotic should hold. Friedlander and Goldston [FG96] have shown that in the range $c > X^{1+o(1)}$,

$$G(X, c) \sim X \log X - X - \frac{X^2}{\phi(c)} + O\left(\frac{X}{(\log X)^A}\right) + O((\log c)^3)\ . \tag{1.1.7}$$

This is a relatively straightforward range because it contains at most one prime. They conjecture that Hooley's asymptotic holds if $X^{1/2+\epsilon} < c < X$ and further conjecture that if $X^{1/2+\epsilon} < c < X^{1-\epsilon}$ then

$$G(X, c) \sim X \log c - X \cdot \left(\gamma_0 + \log 2\pi + \sum_{p|c} \frac{\log p}{p-1}\right)\ . \tag{1.1.8}$$

They show that both Conjecture 1.1.6 and (1.1.8) hold assuming the Hardy-Littlewood conjecture with small remainders. For $c < X^{1/2}$ relatively little seems to be known.

Conjectures 1.1.1 and 1.1.6 remain open, but their analogues in the function field setting have been proved in the limit of large field size [KR14]. Let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q[t]$ the ring of polynomials with coefficients in $\mathbb{F}_q$. Let $\mathcal{M} \subset \mathbb{F}_q[t]$ be the subset of monic polynomials and $\mathcal{M}_n \subset \mathcal{M}$ be the subset of polynomials of degree n. Let $\mathcal{I} \subset \mathcal{M}$ be the subset of irreducible polynomials and $\mathcal{I}_n = \mathcal{I} \cap \mathcal{M}_n$. The norm of a non-zero polynomial $f \in \mathbb{F}_q[t]$ is defined to be $|f| = q^{\deg f}$.

The von Mangoldt function is the function on $\mathcal{M}$ defined for $m \geq 1$ by

$$\Lambda(f) = \begin{cases} d & \text{if } f = \pi^m \text{ with } \pi \in \mathcal{I}_d \\ 0 & \text{otherwise.} \end{cases}$$

The Prime Polynomial Theorem in this context is the identity

$$\sum_{f \in \mathcal{M}_n} \Lambda(f) = q^n\ . \tag{1.1.9}$$

The analogue of Conjecture 1.1.1 is the following result, proved in [KR14]: for $h \leq n - 5$,

$$\frac{1}{q^n} \sum_{A \in \mathcal{M}_n} \left| \sum_{|f - A| \leq q^h} \Lambda(f) - q^{h+1} \right|^2 \sim q^{h+1}(n - h - 2) \tag{1.1.10}$$

as $q \to \infty$; note that $|\{f : |f - A| \leq q^h\}| = q^{h+1}$.

In the same vein, there is a function-field result, also established in [KR14], that is similar to Conjecture 1.1.6: fix $n \geq 2$, then, given a sequence of finite fields $\mathbb{F}_q$ and square-free polynomials $c \in \mathbb{F}_q[t]$ with $2 \leq \deg(c) \leq n + 1$, one has

$$\sum_{\substack{A \bmod c \\ \gcd(A,c)=1}} \left| \sum_{\substack{f \in \mathcal{M}_n \\ f \equiv A \bmod c}} \Lambda(f) - \frac{q^n}{\Phi(c)} \right|^2 \sim q^n(\deg(c) - 1) \tag{1.1.11}$$

as $q \to \infty$.

The asymptotic formulae (1.1.10) and (1.1.11) were established in [KR14] by expressing the variances as sums over families of L-functions. These L-functions can be expressed as the characteristic polynomials of matrices representing Frobenius conjugacy classes. In the limit as $q \to \infty$, these matrices become equidistributed in one of the classical compact groups and the sums become matrix integrals of a kind familiar in Random Matrix Theory. Evaluating these integrals leads to the expressions above.

This approach to computing variances has subsequently been applied to other arithmetic functions defined over function fields, including the Möbius function [KR16], the square of the Möbius function (i.e., the characteristic function of square-free polynomials) [KR16], square-full polynomials [RG17], and the generalized divisor functions [KRRGR18]. For overviews see [Rud14], [KRG16], and [Rod]. The arithmetic functions considered so far have all been associated with degree-one L-functions (or simple functions of these). Our main aim in this paper is to extend the theory to arithmetic functions associated with L-functions of degree two and higher. For example, our results apply to L-functions associated with elliptic curves defined over $\mathbb{F}_q[t]$, and one expects them to apply to all standard automorphic L-functions. This will require us to establish the appropriate equidistribution results for such L-functions. We achieve this using the machinery developed by Katz [Kat12].

The main reason for moving to higher-degree L-functions is the recent discovery in the number-field setting that one gets qualitatively new behaviour when the degree exceeds one [BKS16].

We summarize briefly now the results in [BKS16]. Let $\mathcal{S}$ denote the Selberg class L-functions. For $F \in \mathcal{S}$ primitive, write

$$F(s) = \sum_{n=1}^{\infty} \frac{a_F(n)}{n^s}.$$

Then $F(s)$ has an Euler product

$$F(s) = \prod_p \exp\left(\sum_{l=1}^{\infty} \frac{b_F(p^l)}{p^{ls}} \right) \tag{1.1.12}$$

and satisfies the functional equation

$$\Phi(s) = \varepsilon_F \overline{\Phi}(1-s),$$

where $\overline{\Phi}(s) = \overline{\Phi(\overline{s})}$ and

$$\Phi(s) = c^s \left(\prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j) \right) F(s),$$

for some $c > 0$, $\lambda_j > 0$, $\mathrm{Re}(\mu_j) \geq 0$ and $|\varepsilon_F| = 1$.

There are two important invariants of $F(s)$: the degree d_F and the conductor $\mathfrak{q}_F$, given by

$$d_F = 2\sum_{j=1}^{r} \lambda_j, \quad \mathfrak{q}_F = (2\pi)^{d_F} c^2 \prod_{j=1}^{r} \lambda_j^{2\lambda_j},$$

respectively. Another is m_F, the order of the pole at $s = 1$, which equals 1 for the Riemann zeta function and is expected to be 0 otherwise.

Let Λ_F be the arithmetic function defined by

$$\frac{F'(s)}{F(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda_F(n)}{n^s},$$

and let ψ_F be the function defined by

$$\psi_F(x) := \sum_{n \leq x} \Lambda_F(n).$$

The former will be the main focus of our attention.

A generalized prime number theorem of the form

$$\sum_{n \leq x} \Lambda_F(n) = m_F x + o(x)$$

is expected to hold. In analogy with the case of the Riemann zeta function, it is natural to consider the variance

$$\tilde{V}_F(X,h) := \int_1^X \Big|\psi_F(x+h) - \psi_F(x) - m_F h\Big|^2 dx$$

where $h \neq 0$. For example, when F represents an L-function associated with an elliptic curve, $\tilde{V}_F(X,h)$ is the variance of sums over short intervals involving the Fourier coefficients of the associated modular form evaluated at primes and prime powers; and in the case of Ramanujan's L-function, it represents the corresponding variance for sums involving the Ramanujan τ-function.

For most $F \in \mathcal{S}$ it is expected that

$$\sum_{n \leq X} \Lambda_F(n)\Lambda_F(n+h) = o(X) \text{ when } h \neq 0.$$

This might lead one to expect that $\tilde{V}_F(X,h)$ typically exhibits significantly different asymptotic behaviour than in the case when F is the Riemann zeta-function because in that case (1.1.2) plays a central role in our understanding of the variance. However, all principal L-functions are believed to look essentially the same from the perspective of the statistical distribution of their zeros; that is, it is conjectured that the zeros of all primitive L-functions have a limiting distribution which coincides with that of random unitary matrices, as in Montgomery's conjecture (1.1.3). It was proved in [BKS16], assuming the Generalized Riemann Hypothesis (GRH), that an extension of the pair correlation conjecture for the zeros that includes lower order terms (and which itself follows from the ratio conjecture of [CFZ08], along the lines of [CS07]) is equivalent to the formulae (1.1.13) and (1.1.14) below for $\tilde{V}_F(X,h)$ which generalize the Montgomery-Soundararajan formula (1.1).

If $0 < B_1 < B_2 \leq B_3 < 1/d_F$, then

$$\begin{aligned}\tilde{V}_F(X,h) &= hX\Big(d_F \log \frac{X}{h} + \log \mathfrak{q}_F - (\gamma_0 + \log 2\pi)d_F\Big) \\ &\quad + O_\varepsilon\big(hX^{1+\varepsilon}(h/X)^{c/3}\big) + O_\varepsilon\Big(hX^{1+\varepsilon}\big(hX^{-(1-B_1)}\big)^{1/3(1-B_1)}\Big)\end{aligned} \tag{1.1.13}$$

uniformly for $X^{1-B_3} \ll h \ll X^{1-B_2}$, for some $c > 0$.

Otherwise, if $1/d_F < B_1 < B_2 \leq B_3 < 1$,

$$\begin{aligned}\tilde{V}_F(X,h) &= \frac{1}{6}hX\Big(6\log X - \big(3 + 8\log 2\big)\Big) \\ &\quad + O_\varepsilon\big(hX^{1+\varepsilon}(h/X)^{c/3}\big) + O_\varepsilon\Big(hX^{1+\varepsilon}\big(hX^{-(1-B_1)}\big)^{1/3(1-B_1)}\Big)\end{aligned} \tag{1.1.14}$$

uniformly for $X^{1-B_3} \ll h \ll X^{1-B_2}$, for some $c > 0$.

If $d_F = 1$ there is only one regime of behaviour, governed by (1.1.13). When $\mathfrak{q}_F = 1$, this coincides exactly with (1.1); and when $\mathfrak{q}_F \neq 1$, it generalizes (1.1) in a straightforward way.

If $d_F > 1$ there are two ranges depending on the size of h. In the first range, $\tilde{V}_F(X,h)/h$ is proportional to $\log h$; in the second regime it is independent of h at leading order.

It is this kind of behaviour that we seek to understand better in the context of function fields. We shall focus on variances defined over arithmetic progressions rather than short intervals. In that case we are able to establish unconditional theorems, Theorem 1.2.3 and Theorem 9.0.1 below, which again exhibit the qualitatively new form of the variance when the degree is two or higher.

Our function field results can be used to motivate predictions for the variance of sums over arithmetic progressions of Λ_F in the number field context reviewed above. In order to illustrate these predictions, we focus now on two representative examples: elliptic curve L-functions and the Ramanujan L-function.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N defined over $\mathbb{Q}$. The associated L-function $F(s)$ will be denoted by $L(s,E)$ and is given by

$$L(s,E) = \prod_{p|N}(1 - a_p p^{-s-1/2})^{-1} \prod_{p\nmid N}(1 - a_p p^{-s-1/2} + p^{-2s})^{-1}$$

where a_p is the difference between $p+1$ and the number of points on the reduced curve mod p

$$a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

When $p \mid N$, then a_p is either 1, -1, or 0. In general, we have the Hasse bound on a_p, $|a_p| < 2\sqrt{p}$, hence we can write

$$\frac{a_p}{p^{1/2}} = 2\cos(\theta_p) = \alpha_p + \beta_p$$

where, for $p \nmid N$, one has $\alpha_p = e^{i\theta_p}$ and $\beta_p = e^{-i\theta_p}$ with $\theta_p \in [0,\pi]$ and for $p \mid N$, one has $\alpha_p = a_p$, and $\beta_p = 0$. Let Λ_E be the arithmetic function defined by the logarithmic derivative of $L(s,E)$:

$$\frac{L(s,E)'}{L(s,E)} = -\sum_{n=1}^{\infty} \Lambda_E(n) n^{-s}.$$

It follows that for $e \geq 1$

$$\Lambda_E(n) = \begin{cases} \log p \cdot (\alpha_p^e + \beta_p^e) & \text{if } n = p^e \text{ with } p \text{ prime} \\ 0 & \text{otherwise.} \end{cases}$$

Our results in the function field setting are analogous to computing the variance of the sum of Λ_E in arithmetic progressions

$$S_{x,c,E}(A) := \sum_{\substack{n \leq x \\ n = A \mod c}} \Lambda_E(n).$$

Our function field result (see Theorem 9.0.1) leads us to predict that for $x^\epsilon < c$, $\epsilon > 0$, the following holds:

$$\mathrm{Var}(S_{x,c,E}) \sim \frac{x}{\phi(c)} \min\{\log x, 2\log c\}.$$

This demonstrates the two regimes of behaviour. We can also detect the degree of the L-function in question as the coefficient of $\log c$.

Another example of a degree-two L-function is the Ramanujan L-function:

$$L(s,\tau) = \prod_p \left(1 - \frac{\tau(p)}{p^{s+11/2}} + \frac{1}{p^{2s}}\right)^{-1},$$

where τ is the Ramanujan tau function $\tau\colon \mathbb{N} \to \mathbb{Z}$ defined by the following identity:

$$\sum_{n\geq 1} \tau(n) q^n = q \prod_{n \geq 1}(1-q^n)^{24},$$

where $q = \exp(2\pi i z)$. Ramanujan conjectured (and his conjecture was proved by Deligne) that $|\tau(p)| \leq 2p^{11/2}$ for all primes p. Hence, as before, we can write

$$\frac{\tau(p)}{p^{11/2}} = 2\cos(\theta_p) = \alpha_p + \beta_p.$$

Let Λ_τ be the arithmetic function defined by the logarithmic derivative of $L(s,\tau)$:

$$\frac{L(s,\tau)'}{L(s,\tau)} = -\sum_{n=1}^{\infty} \Lambda_\tau(n) n^{-s}.$$

It follows that for $e \geq 1$

$$\Lambda_\tau(n) = \begin{cases} \log p \cdot (\alpha_p^e + \beta_p^e) & \text{if } n = p^e \text{ with } p \text{ prime} \\ 0 & \text{otherwise,} \end{cases}$$

Again we are led to speculate that for $x^\epsilon < c$ and $\epsilon > 0$, if

$$S_{x,c,\tau}(A) := \sum_{\substack{n \leq x \\ n = A \mod c}} \Lambda_\tau(n)$$

then the following holds:

$$\mathrm{Var}(S_{x,c,\tau}) \sim \frac{x}{\phi(c)} \min\{\log x, 2\log c\}.$$

1.2. **Function-field analogue.** Our results are quite general and to state them requires a good deal of notation and terminology to be explained. For this reason we postpone presenting them until later sections, when the necessary theory has been developed. To illustrate them however we first present below a special case of one of them, and then we sketch a proof.

Remark 1.2.1. For reference, our main results are Theorem 9.0.1 (see §9) and Theorem 12.3.1 (see §12). The former provides the variance estimates we need in terms of a matrix integral and the latter provides an application of these estimates to L-functions of abelian varieties. Two key ingredients used to prove these theorems are Theorem 10.0.4 (see §10) and Theorem 11.0.1 (see §11) which provide requisite equidistribution and big-monodromy results respectively.

Suppose q is an odd prime power, and let $E_{\mathrm{Leg}}/\mathbb{F}_q(t)$ be the Legendre curve, that is, the elliptic curve with affine model

$$y^2 = x(x-1)(x-t).$$

Over the ring $\mathbb{F}_q[t]$, this curve has bad multiplicative reduction at $t = 0, 1$ and good reduction everywhere else, so it has conductor $s = t(t-1)$. It also has additive reduction at ∞, so the L-function is given by an Euler product

$$L(T, E_{\mathrm{Leg}}/\mathbb{F}_q(t)) = \prod_{\pi \in \mathcal{P}} L(T^{\deg(\pi)}, E_{\mathrm{Leg}}/\mathbb{F}_\pi)^{-1}$$

where $\mathcal{P} \subset \mathbb{F}_q[t]$ is the subset of monic irreducibles and $\mathbb{F}_\pi$ is the residue field $\mathbb{F}_q[t]/\pi\mathbb{F}_q[t]$.

Each Euler factor of $L(T, E_{\mathrm{Leg}}/\mathbb{F}_q(t))$ is the reciprocal of a polynomial in $\mathbb{Q}[T]$ and satisfies

$$T\frac{d}{dT} \log L(T, E_{\mathrm{Leg}}/\mathbb{F}_\pi)^{-1} = \sum_{m=1}^{\infty} a_{\pi,m} T^m \in \mathbb{Z}[[T]].$$

Moreover, if we define Λ_{Leg} to be the function on the subset $\mathcal{M}$ of monic polynomials given by

$$\Lambda_{\mathrm{Leg}}(f) = \begin{cases} d \cdot a_{\pi,m} & \text{if } f = \pi^m \text{ with } \pi \in \mathcal{P} \text{ and } \deg(\pi) = d \\ 0 & \text{otherwise,} \end{cases}$$

then the L-function satisfies

$$T\frac{d}{dT} \log(L(T, E_{\mathrm{Leg}}/\mathbb{F}_q(t))) = \sum_{n=1}^{\infty} \left(\sum_{f \in \mathcal{M}_n} \Lambda_{\mathrm{Leg}}(f) \right) T^n.$$

Let $c \in \mathbb{F}_q[t]$ be monic and square free. For each $n \geq 1$ and each A in $\Gamma(c) = (\mathbb{F}_q[t]/c\mathbb{F}_q[t])^\times$, consider the sum

$$S_{n,c}(A) := \sum_{\substack{f \in \mathcal{M}_n \\ f \equiv A \bmod c}} \Lambda_{\mathrm{Leg}}(f). \tag{1.2.2}$$

Let A vary uniformly over $\Gamma(c)$, and consider the moments

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{|\Gamma(c)|}\sum_{A\in\Gamma(c)} S_{n,c}(A), \quad \mathrm{Var}[S_{n,c}(A)] = \frac{1}{|\Gamma(c)|}\sum_{A\in\Gamma(c)} |S_{n,c}(A) - \mathbb{E}[S_{n,c}(A)]|^2.$$

These moments (and the quantity $|\Gamma(c)|$) depend on q, so one can ask how they behave when we replace $\mathbb{F}_q$ by a finite extension, that is, let $q \to \infty$. Using the theory we develop in this paper one can prove the following theorem.

Theorem 1.2.3. *If* $\gcd(c, s) = t$ *and if* $\deg(c)$ *is sufficiently large, then*

$$|\Gamma(c)| \cdot \mathbb{E}[S_{n,c}(A)] = \sum_{\substack{f\in\mathcal{M}_n\\ \gcd(f,c)=1}} \Lambda_{\mathrm{Leg}}(f), \quad \lim_{q\to\infty} \frac{|\Gamma(c)|}{q^{2n}} \cdot \mathrm{Var}[S_{n,c}(A)] = \min\{n, 2\deg(c) - 1\}.$$

See Theorem 12.3.1. We sketch the proof below in §1.3.

Remark 1.2.4. This should be compared to (1.1.11). For definiteness, we could replace "sufficiently large" by $\deg(c) > 900$, but we do not believe this bound to be optimal. We also do not believe the hypothesis on $\gcd(c, s)$ is necessary (cf. Remark 11.0.2). We use it to deduce that certain monodromy groups are big. We do not have any examples of coprime c and s where we know the monodromy groups are *not* big.

Remark 1.2.5. The fact that the expression for the variance depends on $2\deg(c)$ is a direct consequence of the fact that the associated L-functions have degree two. (For an L-function of degree r, one will get a leading term of $r\deg(c)$ instead.) This then leads to there being two ranges of behaviour.

1.3. **Sketch of proof of Theorem.** The calculation of the first moment proceeds immediately from the definition (1.2.2). The first step in our proof of the rest of the theorem is to use Fourier analysis on the multiplicative group $\Gamma(c)$ and rewrite the first and second moments in terms of coefficients of twisted L-functions. Part of this step is to construct a two-dimensional ℓ-adic Galois representation

$$\rho_{\mathrm{Leg}} \colon G_K \to \mathrm{GL}(V),$$

and for each character φ in the dual group $\Phi(c) = \mathrm{Hom}(\Gamma(c), \bar{\mathbb{Q}}_\ell^\times)$, to define a twisted L-function

$$L_{\mathcal{C}}(T, \rho_{\mathrm{Leg}} \otimes \varphi) = \prod_{\pi\nmid c} L(T^{d_\pi}, (\rho_{\mathrm{Leg}} \otimes \varphi)_\pi)^{-1} = \exp\left(\sum_{n=1}^{\infty} b_{\rho_{\mathrm{Leg}}\otimes\varphi,n} \frac{T^n}{n}\right)$$

where $\mathcal{C}$ is the set of finite places dividing c and the infinite place. The reason for doing this is that one can then rewrite the moments using orthogonality of characters, and we show that, for any field embedding $\iota\colon \bar{\mathbb{Q}} \to \mathbb{C}$, one has

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)}\iota(b_{\rho_{\mathrm{Leg}}\otimes\mathbf{1},n}), \quad \mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)^2}\sum_{\varphi\in\Phi(c)^*} |\iota(b_{\rho_{\mathrm{Leg}}\otimes\varphi,n})|^2$$

where $S^* = S \smallsetminus \{\mathbf{1}\}$ for $S \subseteq \Phi(c)$.

The next step is to analyze the coefficients $b_{\rho_{\mathrm{Leg}}\otimes\varphi,n}$. It is relatively easy to show that they lie in $\bar{\mathbb{Q}}$. One can also interpret them cohomologically via a trace formula. Moreover, using Deligne's theorem one can show that, for some integer $R \geq 0$ and all φ in a subset $\Phi(c)_{\rho\,\mathrm{good}} \subseteq \Phi(c)$, the normalized L-function

$$L^*_{\mathcal{C}}(T, \rho_{\mathrm{Leg}} \otimes \varphi) = L_{\mathcal{C}}(T/q, \rho_{\mathrm{Leg}} \otimes \varphi) = \exp\left(\sum_{n=1}^{\infty} b^*_{\rho_{\mathrm{Leg}}\otimes\varphi,n} \frac{T^n}{n}\right)$$

is the reverse characteristic polynomial of a unitary matrix $\theta_{\rho,\varphi} \in U_R(\mathbb{C})$ which is unique up to conjugacy. Let

$$\Phi(c)_{\rho\,\mathrm{bad}} = \Phi(c) \smallsetminus \Phi(c)_{\rho\,\mathrm{good}}$$

so that we have

$$\frac{\phi(c)}{q^{2n}}\mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}} |\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 + \frac{1}{\phi(c)} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{bad}}} |\iota(b^*_{\rho_{\mathrm{Leg}}\otimes\varphi,n})|^2.$$

The subset $\Phi(c)_{\rho\,\mathrm{bad}}$ has density zero as $q \to \infty$, and Deligne's theorem also implies that the terms in the sum over bad characters are uniformly bounded. In particular,

$$\frac{\phi(c)}{q^{2n}}\mathrm{Var}[S_{n,c}(A)] \sim \frac{1}{|\Phi(c)^*_{\rho\,\mathrm{good}}|} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}} |\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2$$

as $q \to \infty$.

The final step in the proof is to show that

$$\frac{1}{|\Phi(c)^*_{\rho\,\mathrm{good}}|} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}} |\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 \sim \int_{U_R(\mathbb{C})} |\mathrm{Tr}(\theta^n)|^2 d\theta$$

with respect to Haar measure on $U_R(\mathbb{C})$. To do this, we must show that the $\theta_{\rho,\varphi}$ are equidistributed in $U_R(\mathbb{C})$. Roughly speaking, this is equivalent to showing that some accompanying monodromy group is big and is where the conditions on $\gcd(c,s)$ and $\deg(c)$ come into play. We say a bit more about this in the next section.

1.4. **Underlying equidistribution theorem.** The key ingredients we use to prove Theorem 1.2.3 and its generalizations are the Mellin transform and Katz's equidistribution theorem. More precisely, we start with a lisse sheaf $\mathcal{F}$ on a dense open $T \subseteq \mathbb{A}^1_t[1/s]$ and twist it by variable Dirichlet characters φ with square-free conductor c to obtain a family of lisse sheaves $\mathcal{F}_\varphi$ on $T[1/c]$; this family is a Mellin transform of $\mathcal{F}$. One can associate a monodromy group $\mathcal{G}_{\mathrm{arith}}$ to this family generated by Frobenius conjugacy classes $\mathrm{Frob}_{E,\varphi}$ for variable Dirichlet characters φ over finite extensions $E/\mathbb{F}_q$. A priori $\mathcal{G}_{\mathrm{arith}}$ is reductive and defined over $\bar{\mathbb{Q}}_\ell$, but Deligne's Riemann hypothesis allows us to associate the classes $\mathrm{Frob}_{E,\varphi}$ for 'good' φ to well-defined conjugacy classes in a compact form of the 'same' reductive group over $\mathbb{C}$. Katz's equidistribution theorem implies these classes are equidistributed.

For our applications, we need equidistribution in a unitary group $U_R(\mathbb{C})$, and thus we need $\mathcal{G}_{\mathrm{arith}}$ to be as big as possible, namely $\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$. We were only able to prove this is the case under the hypotheses that $\deg(c) \gg 1$ and that $\mathcal{F}$ has a unipotent block of exact multiplicity one about $t = \gcd(c,s) = 0$. While we do expect that one may encounter exceptions when $\deg(c)$ is small, we do not believe our lower bound on $\deg(c)$ is sharp. On the other hand, the hypothesis on the monodromy about the unique prime dividing $\gcd(c,s)$ was made in order to ensure we could exhibit elements of $\mathcal{G}_{\mathrm{arith}}$ whose existence helped ensure the group was big. We conjecture one still has big monodromy under the weaker hypothesis that $\gcd(c,s) = 1$.

1.5. **Overview.** The structure of this paper is as follows. We start in §2 by establishing notation and relatively basic facts that we need throughout the rest of the paper.

Throughout the first several sections of the paper we work over a global function field $K = \mathbb{F}_q(X)$, but starting in §5, we restrict to $K = \mathbb{F}_q(t)$. Throughout the entire paper we fix an ℓ-adic Galois representation

$$\rho \colon G_{K,\mathcal{S}} \to \mathrm{GL}(V)$$

where $G_{K,\mathcal{S}}$ is a quotient of the absolute Galois group G_K of K. We also fix a finite set of places $\mathcal{C}$ of K. Ultimately it consists of the place at infinity in $\mathbb{F}_q(t)$ and the finite places corresponding to primes dividing a square-free polynomial $c \in \mathbb{F}_q[t]$. The characters we twist by will be continuous homomorphisms

$$\varphi\colon G^{\mathrm{t}}_{K,\mathcal{C}} \to \bar{\mathbb{Q}}_\ell^\times$$

where $G^{\mathrm{t}}_{K,\mathcal{C}}$ is another quotient of G_K.

In §3, we define two L-functions: a partial L-function $L_{\mathcal{C}}(T,\rho)$ and the complete L-function $L(T,\rho)$. It is the coefficients of the former which appear in our moment formulas, but the latter is what might be called 'the' L-function of ρ. Both are defined via an Euler product: for the complete L-function, we use an Euler product over $\mathcal{P}$, the set of all places of K; for the other, we exclude the Euler factors over $\mathcal{C}$. They coincide if and only if the excluded (or missing) Euler factors are trivial. We recall the cohomological manifestation of each L-function and the trace formula. We also derive numerical invariants for ρ required for computing the degree of each L-function.

In §4, we consider twists of the representation ρ by tame ℓ-adic characters φ with conductor supported on $\mathcal{C}$. If one replaces ρ by $\rho\otimes\varphi$, then one can apply the material of §3 to define $L(T,\rho\otimes\varphi)$ and $L_{\mathcal{C}}(T,\rho\otimes\varphi)$. We provide an annotated version of those results in a manner which is convenient for us.

In §5, we revert to $K=\mathbb{F}_q(t)$ and define the von Mangoldt function Λ_ρ of our Galois representation. It is a multiplicative function $\mathcal{M}\to\bar{\mathbb{Q}}_\ell$ defined using the Euler factors $L(T,\rho_v)$ for the finite places in $\mathbb{F}_q(t)$, and for the trivial representation $\rho=\mathbf{1}$, one has, for $m\geq 1$,

$$\Lambda_{\mathbf{1}}(f) = \begin{cases} \deg(\pi) & f=\pi^m \text{ and } \pi \text{ irreducible} \\ 0 & \text{otherwise.} \end{cases}$$

For each $A\in\Gamma(c)$, we consider the sum

$$S_{n,c}(A) = \sum_{f\in\mathcal{M}_n(A)} \Lambda_\rho(f)$$

where $\mathcal{M}_n(A) = \{\, f \equiv A \bmod c \,\} \subseteq \mathcal{M}_n$. We regard the sum as random variable with values in $\bar{\mathbb{Q}}_\ell$ by varying A uniformly over $\Gamma(c)$ and express its moments as sums of coefficients of the partial L-functions $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ where φ varies over characters of $\Gamma(c)$.

In §6, we define purity and weights. Purity boils down to saying that, in the complex plane, some set of numbers lies on a circle centered at zero, and weight corresponds to the radius. These are the properties usually used to state some sort of Riemann hypothesis. We impose purity on the (zeros of the) Euler factors of $L(T,\rho\otimes\varphi)$ and use Deligne's theorem to deduce purity of its cohomology factors $P_i(T,\rho\otimes\varphi)$. A priori, these factors are polynomials in $\bar{\mathbb{Q}}_\ell[T]$, but in fact, Deligne's theorem implies they have coefficients in $\bar{\mathbb{Q}}$. His theorem also tells us what the weight of each cohomological factor should be, so we can use a field embedding $\iota\colon\bar{\mathbb{Q}}\to\mathbb{C}$ to regard the sums $S_{n,c}(A)$ as complex numbers.

In §7, we isolate conditions for a complete L-functions $L(T,\rho\otimes\varphi)$ to be a pure polynomial, and they hold for most φ. These are the L-functions for which a suitable normalization $L^*(T,\rho\otimes\varphi)$ has coefficients in $\bar{\mathbb{Q}}$ and is unitary, that is, equals the characteristic polynomial of a complex unitary matrix. We also isolate conditions for $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ to be a pure polynomial since it is the coefficients of these L-functions which appear in our moment calculations. They conditions imply the partial and complete L-functions are polynomials and coincide.

In §8, we partition $\Phi(c)$ into subsets of good and bad characters, and then we further partition the bad characters into mixed and heavy characters. A character φ is good if it makes sense to say that a certain renormalization $L^*_{\mathcal{C}}(T,\rho\otimes\varphi)$ of $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ is unitary, and otherwise it is bad, and $L^*_{\mathcal{C}}(T,\rho\otimes\varphi)$ is no longer unitary. If $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ is an impure polynomial, then φ is mixed, and if $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ is not even a polynomial, then φ is heavy since $L_{\mathcal{C}}(T,\rho\otimes\varphi)$ has poles of excess weight.

In §9, we return to our moment calculations. The main result of the section is that the second moment can be approximated using a matrix integral over some compact subgroup $\mathbb{K} \subseteq U_R(\mathbb{C})$, and one has control over the error term precisely when no non-trivial φ is heavy. At this stage, all we know about $\mathbb{K}$ is that each unitary $L^*_{\mathcal{C}}(T, \rho \otimes \varphi)$ corresponds to a unique conjugacy class $\theta_{\rho,\varphi} \subset \mathbb{K}$ and that the classes become equidistributed in $\mathbb{K}$ as $q \to \infty$. In later sections we give conditions for it to be big, that is, equal to $U_R(\mathbb{C})$.

In §10, we partition $\Phi(c)$ into cosets of a 'one-parameter' subgroup $\Phi(u)^\nu \subseteq \Phi(c)$, and then we attach a monodromy group to each coset $\varphi\Phi(u)^\nu$. We define what it means for one of these monodromy groups to be big, and then we define the big characters in $\Phi(c)$ to be those φ whose coset has big monodromy. We then show that if the density of big characters tends to one as $q \to \infty$, then the $\theta_{\rho,\varphi}$ are equidistributed in $\mathbb{K} = U_R(\mathbb{C})$. In this case we say the Mellin transform of ρ has big monodromy.

In §11, we prove a theorem which asserts that the Mellin transform of ρ has big monodromy provided ρ satisfies certain hypotheses. The material in this section rests heavily on the monumental works of Katz, most notably the monograph [Kat12]. In order to prove our result, we were forced to impose the condition that the (square-free) conductor s of ρ and the twisting conductor c satisfy $\deg(\gcd(c, s)) = 1$. We also imposed conditions on the local monodromy of ρ at the zero of $\deg(c, s)$. We used both of these hypotheses to deduce that the relevant monodromy groups contained an element so special that the group was forced to be big (e.g., for the specific example considered in Theorem 1.2.3 one obtains pseudoreflections). While the specific result we proved is new, it borrows heavily from the rich set of tools developed by Katz, and one familiar with his work will easily recognize the intellectual debt we owe him.

In §12, we bring everything together and show how Galois representations arising from (Tate modules of) certain abelian varieties satisfy the requisite properties to apply the theorems of the earlier sections. More precisely, we consider Jacobians of (elliptic and) hyperelliptic curves of arbitrary genus, the Legendre curve being one such example. Because we chose to work with hyperelliptic curves we were forced to assume q is odd. Nonetheless, we expect one can find other suitable examples in characteristic two.

There are four appendices to the paper containing material we needed for the results in Section 11. In the first we recall the definition and some basic facts about middle-extension sheaves. In the second we recall well-known formulas for Euler-Poincaré characteristic. In the third appendix we prove the group-theoretic result which asserts that a reductive subgroup of GL_R with the sort of special element alluded to above is big. In the last appendix we recall much of the abstract formalism required to define the monodromy groups which we want to show are big. While none of this material is new, it elaborates on some of the facts which we felt were not always easy to give a direct reference for in [Kat12]. In particular, our work should not be regarded as a substitute for Katz's original monograph, but we hope some readers will find it an acceptable and enriching complement to his masterful presentation.

2. Notation

Let $q = q_0^n$ be powers of a prime p and $\mathbb{F}_q$ be a finite field with q elements. We write $q \to \infty$ to mean $n \to \infty$.

Let X be a proper smooth geometrically connected curve over $\mathbb{F}_{q_0}$ and K be the function field $\mathbb{F}_q(X)$ (e.g., $X = \mathbb{P}^1_t$ and $K = \mathbb{F}_q(t)$). Let $\mathcal{P}$ be the set of places of K, and for each $v \in \mathcal{P}$, let $\mathbb{F}_v$ be its residue field and $d_v = [\mathbb{F}_v : \mathbb{F}_q]$ be its degree. We identify the elements of $\mathcal{P}$ with the closed points of X in the usual way.

Let K^{sep} be a separable closure of K and $\bar{\mathbb{F}}_q \subset K^{\mathrm{sep}}$ be the algebraic closure of $\mathbb{F}_q \subset K$. Let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and $G_{\mathbb{F}_q} = \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, and let $\bar{G}_K \subseteq G_K$ be the stabilizer of $\bar{\mathbb{F}}_q$ so that there is an exact sequence

$$1 \longrightarrow \bar{G}_K \longrightarrow G_K \longrightarrow G_{\mathbb{F}_q} \longrightarrow 1$$

of profinite groups. Given a quotient $G_K \twoheadrightarrow Q$ of profinite groups, we write $\bar{Q} \subseteq Q$ for the image of $\bar{G}_K$ and call it the *geometric subgroup*.

For each subset $\mathcal{S} \subset \mathcal{P}$, let $K_{\mathcal{S}} \subseteq K^{\mathrm{sep}}$ be the maximal subextension unramified *away* from $\mathcal{S}$ and $K_{\mathcal{S}}^{\mathrm{t}} \subseteq K_{\mathcal{S}}$ be the maximal subextension *tamely* ramfied over $\mathcal{S}$. Both extensions are Galois over K, so we write $G_{K,\mathcal{S}}$ and $G_{K,\mathcal{S}}^{\mathrm{t}}$ for their respective Galois groups. There is a commutative diagram

$$\begin{tikzcd} G_K \arrow[rr] \arrow[dr] & & G_{K,\mathcal{S}} \arrow[dl] \\ & G_{K,\mathcal{S}}^{\mathrm{t}} & \end{tikzcd} \tag{2.0.1}$$

of quotients.

For each $v \in \mathcal{P}$, we fix a place of K^{sep} over v and write $D(v) \subseteq G_K$ for its decomposition group; the latter is well defined up to conjugacy. Let $I(v) \subseteq D(v)$ be the inertia subgroup and $P(v) \subseteq I(v)$ be the wild inertia subgroup (i.e., the p-Sylow subgroup). The quotient $G_v = D(v)/I(v)$ is the absolute Galois group of $\mathbb{F}_v$, and we write $\mathrm{Frob}_v \in G_v$ for the Frobenius element $\mathrm{Frob}_q^{d_v}$ and $\mathrm{Frob}_v I(v)$ for its preimage in $D(v)$.

If $v \notin S$, then the inertia subgroup $I(v)$ is contained in the kernel of the horizontal map in (2.0.1). In particular, every element of the coset $\mathrm{Frob}_v I(v)$ maps to the same element of $G_{K,\mathcal{S}}$ which we denote $\mathrm{Frob}_v \in G_{K,\mathcal{S}}$.

Given a smooth geometrically connected curve U over $\mathbb{F}_q$, we write $\bar{U}$ for the base change curve $U \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$. We fix a geometric generic point $\bar{\eta}$ of U and write $\pi_1(U)$ and $\pi_1(\bar{U})$ for the arithmetic and geometric étale fundamental groups of U respectively. Moreover, if T is a second smooth geometrically connected curve over $\mathbb{F}_q$ and if $T \to U$ is a finite étale cover, then we implicitly suppose the geometric generic point of T maps to that of U and write $\pi_1(T) \to \pi_1(U)$ for the induced inclusion of fundamental groups.

Let $\ell \in \mathbb{Z}$ be a prime distinct from p and $\bar{\mathbb{Q}}_\ell$ be an algebraic closure of $\mathbb{Q}_\ell$. All sheaves on U we consider are constructible étale $\bar{\mathbb{Q}}_\ell$-sheaves, unless stated otherwise, and we write $H^i(\bar{U}, \mathcal{F})$ and $H^i_c(\bar{U}, \mathcal{F})$ for the étale cohomology groups of $\mathcal{F}$. For each integer n, we also write $\mathcal{F}(n)$ for the Tate twisted sheaf $\mathcal{F} \otimes_{\bar{\mathbb{Q}}_\ell} \bar{\mathbb{Q}}_\ell(n)$ and recall that

$$\det(1 - T\,\mathrm{Frob}_q \mid H^i(\bar{U}, \mathcal{F}(n))) = \det(1 - q^n T\,\mathrm{Frob}_q \mid H^i(\bar{U}, \mathcal{F})).$$

A similar identity holds for cohomology with compact supports (cf. [Del77, Proof of 6.1.13]). In particular, we have identities

$$\dim(H^i(\bar{U}, \mathcal{F}(n))) = \dim(H^i(\bar{U}, \mathcal{F})), \quad \dim(H^i_c(\bar{U}, \mathcal{F}(n))) = \dim(H^i_c(\bar{U}, \mathcal{F}))$$

for every i and n.

The sheaf $\mathcal{F}$ is lisse (or locally constant) on U if and only it corresponds to a continuous representation $\pi_1(U) \to \mathrm{GL}(V)$ from the étale fundamental group to a finite-dimensional $\bar{\mathbb{Q}}_\ell$ vector space V (cf. [Mil80, II.3.16.d]). In that case one has identifications

$$H^0(\bar{U}, \mathcal{F}) = V^{\pi_1(\bar{U})} \text{ and } H^2_c(\bar{U}, \mathcal{F}(2)) = V_{\pi_1(\bar{U})} \tag{2.0.2}$$

with the subspace of $\pi_1(\bar{U})$-invariants and quotient space of $\pi_1(\bar{U})$-coinvariants (see [Del77, Exp. 6, 1.18.d]).

3. L-functions

In this section, we recall the construction of two L-functions attached to a Galois representation of the absolute Galois group of a global function field K. A priori, both L-functions are given via Euler products, the essential difference being that one Euler product is over all places of K while the other excludes the Euler factors at a finite set of places of K. We call them the complete and partial L-functions respectively. Each will play a role in later sections, and in particular, when they differ, that is, when at least one omitted Euler factor is non-trivial, their roles will also differ. We do not elucidate the difference in this section, but we do give necessary and sufficient criteria for the L-functions to coincide.

As we recall, both L-functions have a cohomological genesis via the Grothendieck–Lefschetz trace formula. Therefore they can be expressed as rational functions, that is, quotients of polynomials in a single variable, and the polynomials are products of (reverse) characteristic polynomials of an operator acting on certain ℓ-adic cohomology groups. Given basic information about ρ, we show how to calculate the degrees of its L-functions, e.g., in terms of numerical invariants such as Swan and absolute conductors.

3.1. **Euler products.** Let $\mathcal{S} \subset \mathcal{P}$ be a finite subset of places. Let V be a finite-dimensional $\bar{\mathbb{Q}}_\ell$-vector space and ρ be a homomorphism

$$\rho\colon G_{K,\mathcal{S}} \to \mathrm{GL}(V)$$

which is continuous with respect to the profinite topologies.

The decomposition group $D(v)$ stabilizes the subspace $V_v = V^{I(v)}$, and the inertia subgroup $I(v)$ acts trivially on it, so there is a representation

$$\rho_v\colon G_v \to \mathrm{GL}(V_v).$$

The *Euler factor* of ρ at v is given by

$$L(T, \rho_v) := \det\left(1 - T\rho_v(\mathrm{Frob}_v) \mid V_v\right) \in \bar{\mathbb{Q}}_\ell[T],$$

and its degree equals the dimension of V_v.

Let $\mathcal{C} \subset \mathcal{P}$ be a finite subset. The *partial* and *complete L-functions* of ρ are the formal power series in $\bar{\mathbb{Q}}_\ell[T]$ with respective Euler products

$$L_{\mathcal{C}}(T, \rho) := \prod_{v \notin \mathcal{C}} L(T^{d_v}, \rho_v)^{-1} \quad \text{and} \quad L(T, \rho) := \prod_{v \in \mathcal{P}} L(T^{d_v}, \rho_v)^{-1}. \tag{3.1.1}$$

The ratio

$$M_{\mathcal{C}}(T, \rho) := L(T, \rho)/L_{\mathcal{C}}(T, \rho) = \prod_{v \in \mathcal{C}} L(T^{d_v}, \rho_v)^{-1}$$

is the reciprocal of a polynomial, and $M_{\mathcal{C}}(T, \rho) = 1$ iff $L(T, \rho) = L_{\mathcal{C}}(T, \rho)$.

3.2. **Galois modules versus sheaves.** While most of this paper uses the language of global fields, it is useful to adopt a geometric language. Certain readers will find the latter language more to their taste, and we acknowledge that many of our results may have a more appealing formulation in the language of geometry (and sheaves). However, we felt the language of Galois representations over global (function) fields was accessible to a broader audience, so we tried to do 'as much as possible' in that language.

3.3. **Middle extensions.** Recall X is a proper smooth geometrically connected curve over $\mathbb{F}_q$. Let $U \subseteq X$ be a dense Zariski open subset over $\mathbb{F}_q$. Let $\mathcal{F}$ be a sheaf on X and $\mathcal{F}_{\bar{\eta}}$ be its geometric generic stalk. The latter is a G_K-module, and up to replacing U by a dense open subset, it is even a module over the étale fundamental group $\pi_1(U)$, that is, $\mathcal{F}$ is *lisse* on U. Conversely, for every finite-dimensional $\bar{\mathbb{Q}}_\ell$-vector space V and continuous homomorphism $\pi_1(U) \to \mathrm{GL}(V)$, there is a lisse $\bar{\mathbb{Q}}_\ell$-sheaf on U whose stalk over $\bar{\eta}$ is the $\pi_1(U)$-module V.

There are two sheaves and morphisms one can associate to the inclusion $j \colon U \to X$: those in the diagram

$$j_! j^* \mathcal{F} \longrightarrow \mathcal{F} \longrightarrow j_* j^* \mathcal{F} \tag{3.3.1}$$

and constructed in Appendix A.

Definition 3.3.2. We say $\mathcal{F}$ is *supported on U* iff the first map of (3.3.1) is an isomorphism, and $\mathcal{F}$ is a *middle extension* iff the second map is an isomorphism for *every* j.

The following proposition shows that there is a canonical middle extension sheaf on X we can associate to ρ. We denote it by $\mathrm{ME}(\rho)$.

Proposition 3.3.3. *There is a middle extension $\mathcal{F}$ with $\mathcal{F}_{\bar{\eta}} = V$ as G_K-modules, and it is unique up to isomorphism.*

Proof. One can identify V_v with the stalk $\mathrm{ME}(\rho)_v$ and ρ_v with the restriction of $\pi_1(U) \to \mathrm{GL}(V)$ to the decomposition group $D(v) \subset \pi_1(U)$ See Proposition A.0.4 and compare [Mil80, 3.1.16]. ☐

Corollary 3.3.4. *Let $\mathcal{S}' \subset \mathcal{P}$ be a finite subset containing $\mathcal{S}$ and $\rho' \colon G_{K,\mathcal{S}'} \to \mathrm{GL}(V)$ be the composition of ρ with the natural quotient $G_{K,\mathcal{S}'} \twoheadrightarrow G_{K,\mathcal{S}}$. Then $\mathrm{ME}(\rho)$ and $\mathrm{ME}(\rho')$ are isomorphic.*

Proof. The quotient $G_K \to G_{K,\mathcal{S}}$ factors as $G_K \twoheadrightarrow G_{K,\mathcal{S}'} \twoheadrightarrow G_{K,\mathcal{S}}$, and $\mathrm{ME}(\rho')_{\bar{\eta}} = V = \mathrm{ME}(\rho)$ as G_K-modules. Since $\mathrm{ME}(\rho), \mathrm{ME}(\rho')$ are both middle extensions, Proposition 3.3.3 implies they are isomorphic. ☐

3.4. **Cohomological manifestation.** Suppose $Z = X \smallsetminus U$ equals $\mathcal{C}$. Then $L(T,\rho)$ and $L_{\mathcal{C}}(T,\rho)$ equal the L-functions of the sheaves $\mathrm{ME}(\rho)$ and $j_! j^* \mathrm{ME}(\rho)$ respectively. More precisely, the Euler products of the latter coincide with (3.1.1). Moreover, they all have the same Euler factors over U, hence $M_{\mathcal{C}}(T,\rho)$ has an Euler product over Z which coincides with that of the L-function of $\mathrm{ME}(\rho)$ over Z.

The étale cohomology groups of these sheaves are finite-dimensional $\bar{\mathbb{Q}}_\ell$-vector spaces, and Frob_q acts $\bar{\mathbb{Q}}_\ell$-linearly on them. In particular, we have characteristic polynomials

$$P_{\mathcal{C},i}(T,\rho) := \det\left(1 - T\,\mathrm{Frob}_q \mid H^i_c(\bar{U}, \mathrm{ME}(\rho))\right) \tag{3.4.1}$$

which are trivial for $i \neq 0,1,2$ since U a curve. Moreover, $P_{\mathcal{C},i}(T) = 1$ if U is an affine curve, that is, if $\mathcal{C}$ is non-empty, and then

$$L_{\mathcal{C}}(T,\rho) = P_{\mathcal{C},1}(T,\rho)/P_{\mathcal{C},2}(T,\rho). \tag{3.4.2}$$

Similarly, the characteristic polynomials

$$P_i(T,\rho) := \det(1 - T\,\mathrm{Frob}_q \mid H^i(\bar{X}, \mathrm{ME}(\rho))). \tag{3.4.3}$$

are trivial for $i \neq 0,1,2$ since X is a curve, and they satisfy

$$L(T,\rho) = \frac{P_1(T,\rho)}{P_0(T,\rho)P_2(T,\rho)}. \tag{3.4.4}$$

Finally, if $\mathcal{C} = \emptyset$ and thus $U = X$, then

$$P_{\emptyset,i}(T,\rho) = P_i(T,\rho) \text{ for all } i,$$

and thus $L(T,\rho) = L_\emptyset(T,\rho)$.

3.5. **Numerical invariants of ρ.** Let

$$\mathrm{rank}_v(\rho) := \deg(L(T,\rho_v)), \quad \mathrm{drop}_v(\rho) := \dim(V) - \mathrm{rank}_v(\rho),$$

and $\mathrm{Swan}_v(\rho)$ be the Swan conductor of V as an $\bar{\mathbb{Q}}_\ell[I(v)]$-module (see [Kat88, 1.6]). We call these and

$$\mathrm{drop}_{\mathcal{C}}(\rho) := \sum_{v\in\mathcal{C}} d_v \cdot \mathrm{drop}_v(\rho)$$

the *local invariants* of ρ. On the other hand, we call

$$\mathrm{rank}(\rho) := \dim(V), \quad \mathrm{drop}(\rho) := \sum_{v\in\mathcal{P}} d_v \cdot \mathrm{drop}_v(\rho), \quad \mathrm{Swan}(\rho) := \sum_{v\in\mathcal{P}} d_v \cdot \mathrm{Swan}_v(\rho)$$

and

$$r_\emptyset(\rho) := \deg(L(T,\rho)), \quad r_{\mathcal{C}}(\rho) := \deg(L_{\mathcal{C}}(T,\rho))$$

the *global invariants*.

Proposition 3.5.1. *Let g be the genus of $\bar{X}$. Then the Euler characteristics $\chi(\bar{X},\mathrm{ME}(\rho))$ and $\chi_c(\bar{U},\mathrm{ME}(\rho))$ (cf. (B.0.5)) satisfy*

$$r_\emptyset(\rho) = -\chi(\bar{X},\mathrm{ME}(\rho)) = (\mathrm{drop}(\rho)+\mathrm{Swan}(\rho)) - (2-2g)\cdot\mathrm{rank}(\rho) \tag{3.5.2}$$

and

$$r_{\mathcal{C}}(\rho) = -\chi_c(\bar{U},\mathrm{ME}(\rho)) = (\mathrm{drop}(\rho)-\mathrm{drop}_{\mathcal{C}}(\rho)+\mathrm{Swan}(\rho)) - (2-2g-\deg(\mathcal{C}))\cdot\mathrm{rank}(\rho). \tag{3.5.3}$$

Moreover, if $\mathrm{ME}(\rho)$ is supported on U (see Definition 3.3.2), then $\chi_c(\bar{U},\mathrm{ME}(\rho)) = \chi(\bar{X},\mathrm{ME}(\rho))$.

Proof. See Proposition B.1.1 and Corollary B.1.2. □

One deduces immediately that

$$r_{\mathcal{C}}(\rho) = r_\emptyset(\rho) + \deg(\mathcal{C})\cdot\mathrm{rank}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho). \tag{3.5.4}$$

3.6. **Trace formula.** The *local traces* of ρ are given by

$$a_{\rho,v,m} := \mathrm{Tr}\left(\rho_v(\mathrm{Frob}_v)^m \mid V_v\right) \text{ for } v\in\mathcal{P} \text{ and } m\geq 1, \tag{3.6.1}$$

and they satisfy

$$T\frac{d}{dT}\log L(T,\rho_v)^{-1} = \sum_{m=1}^{\infty} a_{\rho,v,m}T^m \text{ for } v\in\mathcal{P}. \tag{3.6.2}$$

Combining this with (3.1.1) yields the identity

$$T\frac{d}{dT}\log L_{\mathcal{C}}(T,\rho) = \sum_{n=1}^{\infty}\left(\sum_{md=n}\sum_{v\in\mathcal{P}_d\smallsetminus\mathcal{C}} d\cdot a_{\rho,v,m}\right)T^n \tag{3.6.3}$$

where $\mathcal{P}_d\subset\mathcal{P}$ is the finite subset of places of degree d.

Let $\bar{U}\subseteq\bar{X}$ be the open complement of $\mathcal{C}$. The *cohomological traces* of ρ are given by

$$b_{\rho,n} := \sum_{i=0}^{2}(-1)^i\cdot\mathrm{Tr}\left(\mathrm{Frob}_q \mid H^i_c(\bar{U},\mathrm{ME}(\rho))\right) \text{ for } n\geq 1$$

and they satisfy

$$T\frac{d}{dT}\log L_{\mathcal{C}}(T,\rho) = \sum_{n=1}^{\infty} b_{\rho,n}T^n. \tag{3.6.4}$$

Combining this with (3.6.3) yields the Grothendieck–Lefschetz trace formula

$$\sum_{md=n} \sum_{v \in \mathcal{P}_d \smallsetminus \mathcal{C}} d \cdot a_{\rho,v,m} = b_{\rho,n}. \tag{3.6.5}$$

See [Del77, Exp. 2, §3] for details.

4. Twisted L-functions

In this section, we apply the theory of the previous section to the twist of a Galois representation by a Dirichlet character. We start by defining the twist and its L-functions, and then we apply the theory from the previous section, e.g., to calculate the respective degrees.

4.1. **Twists by characters.** Let $\mathcal{S} \subset \mathcal{P}$ be a finite subset and V be a finite-dimensional $\bar{\mathbb{Q}}_\ell$-vector space. Let

$$\rho\colon G_{K,\mathcal{S}} \to \mathrm{GL}(V)$$

be a *Galois representation*, that is, a continuous homomorphism.

Let $\mathcal{C} \subset \mathcal{P}$ be a finite subset. An *ℓ-adic character with conductor supported on $\mathcal{C}$* is a continuous homomorphism

$$\varphi\colon G_{K,\mathcal{C}} \to \bar{\mathbb{Q}}_\ell^\times,$$

and we write $\Phi(\mathcal{C})$ for the set of all such characters which also have finite image. By definition, φ factors as a composite homomorphism

$$G_{K,\mathcal{C}} \twoheadrightarrow G_{K,\mathcal{C}}^{\mathrm{ab}} \to \bar{\mathbb{Q}}_\ell^\times$$

through the maximal abelian quotient. We say it is *tame* iff it factors as a composite homomorphism

$$G_{K,\mathcal{C}}^{\mathrm{ab}} \twoheadrightarrow G_{K,\mathcal{C}}^{\mathrm{t,ab}} \to \bar{\mathbb{Q}}_\ell^\times$$

through the maximal tame (abelian) quotient.

Let $\mathcal{R} = \mathcal{C} \cup \mathcal{S}$ so that there are natural quotients

$$G_{K,\mathcal{R}} \twoheadrightarrow G_{K,\mathcal{S}} \text{ and } G_{K,\mathcal{R}} \twoheadrightarrow G_{K,\mathcal{C}}.$$

Let ρ_R and φ_R be the respective compositions

$$\rho_R\colon G_{K,\mathcal{R}} \twoheadrightarrow G_{K,\mathcal{S}} \to \mathrm{GL}(V), \quad \varphi_R\colon G_{K,\mathcal{R}} \twoheadrightarrow G_{K,\mathcal{C}} \to \bar{\mathbb{Q}}_\ell^\times.$$

The *tensor product* of ρ and φ is the representation

$$\rho \otimes \varphi = (g \mapsto \rho_R(g)\varphi_R(g)) : \ G_{K,\mathcal{R}} \to \mathrm{GL}(V_\varphi)$$

where $V_\varphi = V$ as $\bar{\mathbb{Q}}_\ell$-vector spaces.

4.2. ***L*-functions.** The Euler factors of the L-functions of $\rho \otimes \varphi$ are given by

$$L(T, (\rho \otimes \varphi)_v) := \det(1 - T\,(\rho \otimes \varphi)_v(\mathrm{Frob}_v) \mid V_\varphi^{I(v)}),$$

and in particular,

$$L(T, (\rho \otimes \varphi)_v) = L(\varphi_{\mathcal{C}}(\mathrm{Frob}_v)T, \rho_v) \text{ for } v \notin \mathcal{C}. \tag{4.2.1}$$

Moreover, the partial and complete L-functions of $\rho \otimes \varphi$ satisfy

$$L_{\mathcal{C}}(T, \rho \otimes \varphi) := \prod_{v \notin \mathcal{C}} L(T^{d_v}, (\rho \otimes \varphi)_v)^{-1} = \prod_i P_{\mathcal{C},i}(T, \rho \otimes \varphi)^{(-1)^{i+1}}$$

and

$$L(T, \rho \otimes \varphi) := \prod_{v \in \mathcal{P}} L(T^{d_v}, (\rho \otimes \varphi)_v)^{-1} = \prod_i P_i(T, \rho \otimes \varphi)^{(-1)^{i+1}}$$

respectively where

$$P_{\mathcal{C},i}(T,\rho\otimes\varphi) := \det\left(1 - T\operatorname{Frob}_q \mid H^i_c(\bar{U},\mathrm{ME}(\rho\otimes\varphi))\right)$$

and

$$P_i(T,\rho\otimes\varphi) := \det(1 - T\operatorname{Frob}_q \mid H^i(\bar{X},\mathrm{ME}(\rho\otimes\varphi))).$$

Recall $\bar{U}\subset\bar{X}$ is the open complement of $\mathcal{C}$. Compare (3.1.1), (3.4.1), and (3.4.2).

4.3. **Numerical invariants.** Recall the numerical invariants defined in §3.5. We say a character φ is *tame* iff it factors through the maximal tame quotient $G_{K,\mathcal{C}}\twoheadrightarrow G^{\mathrm{t}}_{K,\mathcal{C}}$, or equivalently, $\mathrm{Swan}(\rho)$ vanishes. Let

$$r_{\mathcal{C}}(\rho\otimes\varphi) := \deg(L_{\mathcal{C}}(T,\rho\otimes\varphi))$$

as in §3.5.

Proposition 4.3.1. *If φ is tame, then*

$$r_{\mathcal{C}}(\rho\otimes\varphi) = r_{\mathcal{C}}(\rho) = \deg(L(T,\rho)) + (\deg(c)+1)\dim(V) - \mathrm{drop}_{\mathcal{C}}(\rho). \tag{4.3.2}$$

Proof. If φ is tame and g is the genus of $\bar{X}$, then Proposition 3.5.1 and Lemma B.1.3 imply

$$\begin{aligned} r_{\mathcal{C}}(\rho\otimes\varphi) &\overset{(3.5.3)}{=} (\mathrm{drop}(\rho\otimes\varphi) - \mathrm{drop}_{\mathcal{C}}(\rho\otimes\varphi) + \mathrm{Swan}(\rho\otimes\varphi)) - (2-2g-\deg(\mathcal{C}))\cdot\mathrm{rank}(\rho\otimes\varphi). \\ &\overset{B.1.3}{=} (\mathrm{drop}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho) + \mathrm{Swan}(\rho)) - (2-2g-\deg(\mathcal{C}))\cdot\mathrm{rank}(\rho) \\ &\overset{(3.5.3)}{=} r_{\mathcal{C}}(\rho) \\ &\overset{(3.5.4)}{=} r_{\emptyset}(\rho) + \deg(\mathcal{C})\cdot\mathrm{rank}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho). \end{aligned}$$

The proposition follows by observing that

$$r_{\emptyset}(\rho) = \deg(L(T,\rho)),\quad \deg(\mathcal{C}) = \deg(c)+1,\quad \mathrm{rank}(\rho) = \dim(V).$$

□

Remark 4.3.3. Observe $\deg(L_{\mathcal{C}}(T,\rho\otimes\varphi))$ is independent of φ.

4.4. **Trace formula.** By (4.2.1), we have

$$T\frac{d}{dT}\log L(T,(\rho\otimes\varphi)_v)^{-1} = \sum_{m=1}^{\infty}\varphi(\mathrm{Frob}_v)^m a_{\rho,v,m}T^m \text{ for } v\in\mathcal{P}\smallsetminus\mathcal{C}. \tag{4.4.1}$$

We also have

$$T\frac{d}{dT}\log L_{\mathcal{C}}(T,\rho\otimes\varphi) = \sum_{n=1}^{\infty} b_{\rho\otimes\varphi,n}T^n \tag{4.4.2}$$

where

$$b_{\rho\otimes\varphi,n} := \sum_{i=1}^{2}(-1)^i\cdot\mathrm{Tr}\left(\mathrm{Frob}_q \mid H^i_c(\bar{U},\mathrm{ME}(\rho\otimes\varphi))\right) \text{ for } n\geq 1.$$

Thus, we have the twisted Grothendieck-Lefschetz trace formula

$$\sum_{md=n}\sum_{v\in\mathcal{P}_d\smallsetminus\mathcal{C}} d\cdot\varphi(\mathrm{Frob}_v)^m a_{\rho,v,m} = b_{\rho\otimes\varphi,n}. \tag{4.4.3}$$

Compare (3.6.5).

5. Sums in Arithmetic Progressions

Throughout this section (and many of the remaining sections) we suppose that X is the projective t-line $\mathbb{P}^1_t$ and thus that $K = \mathbb{F}_q(t)$.

5.1. **Dirichlet characters.** Let $c \in \mathbb{F}_q[t]$ be monic and square free of degree $d \geq 1$, and let

$$\Gamma(c) := (\mathbb{F}_q[t]/c\,\mathbb{F}_q[t])^\times \text{ and } \Phi(c) := \mathrm{Hom}(\Gamma(c), \bar{\mathbb{Q}}^\times).$$

The latter are finite abelian groups and are non-canonically isomorphic of order equal to the Euler totient $\phi(c)$. Let $\mathcal{U}_\mathcal{C} \subset \mathcal{P}$ be the complement of the finite set

$$\mathcal{C} := \mathrm{supp}(c) = \{\, v \in \mathcal{P} : \mathrm{ord}_v(c) \neq 0 \,\}.$$

Then $\infty \in \mathcal{C}$ and $\Sigma_{v\in\mathcal{C}} \deg(v) = d + 1$.

The elements of u of $\mathcal{U}_\mathcal{C}$ are in natural bijection with the maximal ideals $\mathfrak{p}_u \subset \mathbb{F}_q[t]$ which do not contain c, and such an ideal is generated by a unique monic $\pi_u \in \mathfrak{p}_u$. In particular, abelian class field theory supplies both a well-defined element $\mathrm{Frob}_u \in G^{\mathrm{ab}}_{K,\mathcal{C}}$ and a homomorphism

$$\alpha_\mathcal{C} \colon G^{\mathrm{ab}}_{K,\mathcal{C}} \to \Gamma(c) \text{ with } \alpha_\mathcal{C}(\mathrm{Frob}_u) = \pi_u \bmod c \text{ for } u \in \mathcal{U}_\mathcal{C}.$$

This allows us to regard any character $\varphi \in \Phi(c)$ as a (continuous) composite homomorphism

$$\varphi \colon G_{K,\mathcal{C}} \twoheadrightarrow G^{\mathrm{t,ab}}_{K,\mathcal{C}} \twoheadrightarrow \Gamma(c) \to \bar{\mathbb{Q}}^\times.$$

We call the composite homomorphism a *tame Dirichlet character* and say it has *conductor supported in $\mathcal{C}$*.

5.2. **Von Mangoldt function.** Let $\mathcal{M} \subset \mathbb{F}_q[t]$ be the subset of monic polynomials, $\mathcal{I} \subset \mathcal{M}$ be the subset of irreducibles, and $\mathcal{I}_d \subset \mathcal{I}$ be the monics of degree d. There is a natural bijection between the finite places $v \in \mathcal{P} \smallsetminus \{\infty\}$ and the elements $\pi \in \mathcal{I}$ since $X = \mathbb{P}^1_t$. We write $v \colon \mathcal{I} \to \mathcal{P} \smallsetminus \{\infty\}$ for the map sending an irreducible to its corresponding place.

We define the *von Mangoldt function* of ρ to be the map $\Lambda_\rho \colon \mathcal{M} \to \bar{\mathbb{Q}}_\ell$ given by

$$\Lambda_\rho(f) = \begin{cases} d \cdot a_{\rho,v(\pi),m} & f = \pi^m \text{ where } m \geq 1 \text{ and } \pi \in \mathcal{I}_d \\ 0 & \text{otherwise.} \end{cases} \tag{5.2.1}$$

Recall $a_{\rho,v(\pi),m}$ is the local trace defined in (3.6.1), and in (3.6.2), it is completely determined by the Euler factor $L(T, \rho_v)$. We also define the *extension by zero* of $\varphi \in \Phi(c)$ to be the map $\varphi_! \colon \mathcal{M} \to \bar{\mathbb{Q}}_\ell$ given by

$$\varphi_!(f) = \begin{cases} \varphi(f + c\,\mathbb{F}_q[t]) & \text{if } \gcd(f, c) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

It is multiplicative and satisfies

$$\varphi_!(\pi) = \begin{cases} \varphi(\mathrm{Frob}_{v(\pi)}) & \text{if } \pi \nmid c \\ 0 & \text{otherwise} \end{cases} \quad \text{for } \pi \in \mathcal{I}.$$

There may be other multiplicative maps extending φ, but for our extension we have the identity

$$b_{\rho\otimes\varphi,n} = \sum_{f\in\mathcal{M}_n} \varphi_!(f)\Lambda_\rho(f) \text{ for } n \geq 1 \tag{5.2.2}$$

by (4.4.3). We observe that in the special case $\varphi = \mathbf{1}$ this simplifies to

$$b_{\rho,n} = \sum_{A\in\Gamma(c)} \sum_{f\in\mathcal{M}_n(A)} \Lambda_\rho(f) \tag{5.2.3}$$

where $\mathcal{M}_n(A) \subseteq \mathcal{M}_n$ is the subset of f satisfying $f \equiv A \bmod c$.

5.3. **Sums in random arithmetic progressions.** Consider the sum

$$S_{n,c}(A) := \sum_{f \in \mathcal{M}_n(A)} \Lambda_\rho(f) \text{ for } A \in \Gamma(c) \text{ and } n \geq 1 \tag{5.3.1}$$

where $\Lambda_\rho \colon \mathcal{M} \to \bar{\mathbb{Q}}_\ell$ is the von Mangoldt function of ρ.

For each n, we would like to regard the sum as a random variable on $\Gamma(c)$, e.g., so that we can speak of the mean and variance. If we were loathe to impose hypotheses on the range of Λ_ρ, we might consider the drastic measure of choosing a field isomorphism $\bar{\mathbb{Q}}_\ell \to \mathbb{C}$. Instead, we fix field embeddings $\iota \colon \bar{\mathbb{Q}} \to \mathbb{C}$ and $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_\ell$ and suppose the range of Λ_ρ is a subset of $\bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_\ell$. This allows us to define the elements

$$\mathbb{E}[S_{n,c}(A)] := \frac{1}{\phi(c)} \sum_{A \in \Gamma(c)} S_{n,c}(A), \tag{5.3.2}$$

$$\mathrm{Var}[S_{n,c}(A)] := \frac{1}{\phi(c)} \sum_{A \in \Gamma(c)} |\iota(S_{n,c}(A) - \mathbb{E}[S_{n,c}(A)])|^2 \tag{5.3.3}$$

in $\bar{\mathbb{Q}}$ and $\mathbb{C}$ respectively.

5.4. **Coefficients of L-functions.** Observe that, for each $A_1, A_2 \in \Gamma(c)$, one has

$$\frac{1}{\phi(c)} \sum_{\varphi \in \Phi(c)} \varphi(A_1)\bar{\varphi}(A_2) = \begin{cases} 1 & \text{if } A_1 = A_2 \\ 0 & \text{if } A_1 \neq A_2, \end{cases}$$

and thus by (5.2.2), one has

$$S_{n,c}(A) = \frac{1}{\phi(c)} \sum_{f \in \mathcal{M}_n} \Lambda_\rho(f) \sum_{\varphi \in \Phi(c)} \varphi_!(f)\bar{\varphi}_!(A) = \frac{1}{\phi(c)} \sum_{\varphi \in \Phi(c)} b_{\rho \otimes \varphi, n} \cdot \bar{\varphi}_!(A).$$

Therefore, if we write $\mathbf{1} \in \Phi(c)$ for the trivial character, then (5.3.2) becomes

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)^2} \sum_{\varphi \in \Phi(c)} b_{\rho \otimes \varphi, n} \sum_{A \in \Gamma(c)} \bar{\varphi}_!(A) = \frac{1}{\phi(c)} b_{\rho, \mathbf{1}, n}$$

since, for every $\varphi_1, \varphi_2 \in \Phi(c)$, one has

$$\frac{1}{\phi(c)} \sum_{A \in \Gamma(c)} \varphi_1(A)\bar{\varphi}_2(A) = \begin{cases} 1 & \text{if } \varphi_1 = \varphi_2 \\ 0 & \text{if } \varphi_1 \neq \varphi_2. \end{cases} \tag{5.4.1}$$

In particular, we have the identity

$$S_{n,c}(A) - \mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)} \sum_{\varphi \in \Phi(c)^*} b_{\rho \otimes \varphi, n} \cdot \bar{\varphi}(A) \quad \text{where} \quad \Phi(c)^* = \Phi(c) \smallsetminus \{\mathbf{1}\},$$

and (5.3.3) becomes

$$\begin{aligned} \mathrm{Var}[S_{n,c}(A)] &= \frac{1}{\phi(c)^3} \sum_{A \in \Gamma(c)} \sum_{\varphi_1, \varphi_2 \in \Phi(c)^*} b_{\rho \otimes \varphi_1, n} \overline{b_{\rho \otimes \varphi_2, n}} \cdot \bar{\varphi}_{1!}(A) \varphi_{2!}(A) \\ &= \frac{1}{\phi(c)^2} \sum_{\varphi \in \Phi(c)^*} |b_{\rho \otimes \varphi, n}|^2 \end{aligned}$$

by (5.4.1).

In summary, the function $S_{n,c}(A)$ of the random variable A satisfies

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)} b_{\rho\otimes\mathbf{1},n}, \quad \mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)^2} \sum_{\substack{\varphi\in\Phi(c)\\ \varphi\neq\mathbf{1}}} |\iota(b_{\rho\otimes\varphi,n})|^2. \tag{5.4.2}$$

In order to say anything meaningful about these numbers individually or as q grows, we need to impose additional hypotheses on ρ, e.g., that the Euler factors of $L(T,\rho)$ satisfy a suitable Riemann hypothesis. Doing so will enable us to apply Deligne's theorem and to rewrite the variance in terms of a matrix integral.

6. Purity and Weights

Let $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_\ell$ and $\iota\colon \bar{\mathbb{Q}} \to \mathbb{C}$ be field embeddings. Using these embeddings we can define what it means for a representation such as ρ to be pointwise ι-pure of some weight $w \in \mathbb{R}$. We do so by imposing a Riemann hypothesis on the zeros of each of the Euler factors, i.e., that they embed in $\mathbb{C}$ via ι and lie on a suitable circle centered at the origin. The property is local in that it places constraints on each of the Euler factors, and it does not immediately say anything global. To show that the partial and complete L-functions also satisfy a suitable Riemann hypothesis, one needs Deligne's theorem.

6.1. **Purity.** We say a polynomial in $\bar{\mathbb{Q}}_\ell[T]$ is *ι-pure of q-weight w* iff it is non-zero and each of its zeros $\alpha \in \bar{\mathbb{Q}}_\ell$ lies in $\bar{\mathbb{Q}}$ and satisfies

$$|\iota(\alpha)|^2 = (1/q)^w.$$

We also say it is *pure of q-weight w* iff it is ι-pure of q-weight w for every ι. More generally, we say it is *mixed of q-weights $\leq w$* iff it is a product of polynomials, each pure of q-weight $\leq w$.

Remark 6.1.1. Our terminology is unconventional in that we incorporate q, however, we need to make q explicit since we have not said where the polynomial comes from.

Remark 6.1.2. In many applications w is usually rational and often an integer.

6.2. **Riemann hypothesis.** We say the representation $\rho\otimes\varphi$ is *pointwise (ι-)pure of weight w* iff the Euler factor $L(T^{d_v}, (\rho\otimes\varphi)_v)$ is (ι-)pure of q-weight w for every $v \notin \mathcal{S}$.

Theorem 6.2.1. (Deligne) *If $\rho\otimes\varphi$ is pointwise (ι-)pure of weight w, then the cohomological factors $P_{i,\mathcal{C}}(T,\rho\otimes\varphi)$ are (ι-)mixed of q-weights $\leq w+n$ and the factors $P_i(T,\rho\otimes\varphi)$ both lie in $\bar{\mathbb{Q}}[T]$ and are (ι-)pure of q-weight $w+n$.*

Proof. See Theorems 1 and 2 of [Del80] for the respective assertions about $P_{i,\mathcal{C}}(T,\rho\otimes\varphi)$ and $P_i(T,\rho\otimes\varphi)$ in terms of the middle extension $\mathrm{ME}(\rho\otimes\varphi)$. The theorems are stated in terms of ι, but one can easily deduce the statement for pointwise pure $\rho\otimes\varphi$ by considering all ι simultaneously. □

The following lemma implies every twist $\rho\otimes\varphi$ is pointwise pure if and only if ρ is.

Lemma 6.2.2. *If $\rho = \rho\otimes\mathbf{1}$ is pointwise ι-pure of weight w, then so is $\rho\otimes\varphi$.*

Proof. Observe that $\zeta = \varphi_{\mathcal{C}}(\mathrm{Frob}_v)$ is a root of unity since $\Gamma(c)$ has finite order, hence $\zeta \in \bar{\mathbb{Q}}$ and $|\iota(\zeta)|^2 = 1$. If $v \notin \mathcal{C}$ and if $\alpha \in \bar{\mathbb{Q}}$ is a zero of $L(T,(\rho\otimes\varphi)_v)$, then (4.2.1) implies that α/ζ is a zero of $L(T,\rho_v)$. In particular, $|\alpha|^2 = |\alpha/\zeta|^2 = (1/q^{d_v})^w$, hence $L(T^{d_v},(\rho\otimes\varphi)_v)$ is ι-pure of q-weight w for almost all v. □

6.3. **Weight bound for missing Euler factors.** Let $\mathcal{F}$ be a middle-extension sheaf on X (e.g., $\mathrm{ME}(\rho \otimes \varphi)$). We say that $\mathcal{F}$ is *pointwise (ι-)pure of weight w* iff for some dense Zariski open subset $U \subseteq X$ on which $\mathcal{F}$ is lisse, the corresponding representation of $\pi_1(U)$ is pointwise (ι-)pure of weight w. In general, even for U maximal among such U, the complement $Z = X \smallsetminus U$ may be non-empty, and there may be mild degeneration among the zeros of the corresponding Euler factors.

Lemma 6.3.1. *Let $j\colon U \to X$ be the inclusion of a dense Zariski open subset and $Z = X \smallsetminus U$. If $\mathcal{F}$ is lisse on U and pointwise ι-pure of weight w, then*

$$\det(1 - T\mathrm{Frob}_q \mid H^0(\bar{Z}, j_*\mathcal{F})) = \prod_{z \in Z} L(T^{d_z}, \mathcal{F}_z)$$

is ι-mixed of q-weights $\leq w$.

Proof. See [Del80, 1.8.1]. □

7. Polynomial L-functions

A priori, the partial and complete L-functions are different and rational, that is, a quotient of two polynomials. We suppose that ρ is pointwise ι-pure of known weight so that we can speak of the weights of the zeros and poles of the L-functions. Under suitable additional conditions on φ, the L-functions of $\rho \otimes \varphi$ coincide, are polynomials, *and* are ι-pure of known q-weight. As we explain in the next section, these properties will allow us to associate a conjugacy class of unitary matrices to $\rho \otimes \varphi$.

7.1. **Semisimplicity.** Consider an exact sequence of $G_{K,\mathcal{S}}$-modules

$$0 \longrightarrow V_1 \longrightarrow V \longrightarrow V_2 \longrightarrow 0, \tag{7.1.1}$$

and let $\rho\colon G_{K,\mathcal{S}} \to \mathrm{GL}(V)$ and $\rho_i\colon G_{K,\mathcal{S}} \to \mathrm{GL}(V_i)$ for $i = 1, 2$ be the corresponding structure homomorphisms.

A priori, (7.1.1) does not split, but we say ρ is *arithmetically semisimple* iff the sequence splits for *every* $G_{K,\mathcal{S}}$-invariant subspace $V_1 \subseteq V$. By Clifford's theorem, the condition implies that ρ is *geometrically semisimple* since $\bar{G}_{K,\mathcal{S}}$ is normal in $G_{K,\mathcal{S}}$ (cf. [CR06, 49.2]): every $\bar{G}_{K,\mathcal{S}}$-invariant subspace of V has a $\bar{G}_{K,\mathcal{S}}$-invariant complement. We also say that ρ is *geometrically simple* iff ρ is irreducible and geometrically semisimple.

Lemma 7.1.2. *If ρ is geometrically simple, then so is $\rho \otimes \varphi$.*

Proof. If $W_\varphi \subseteq V_\varphi$ be a $\bar{G}_{K,\mathcal{R}}$-invariant subspace, then $W = W_\varphi \otimes \bar{\varphi}$ is a $\bar{G}_{K,\mathcal{R}}$-invariant subspace. Moreover, if ρ is geometrically simple, then W equals 0 or V, hence W_φ equals 0 or V_φ. □

7.2. **Invariants and coinvariants.** We say ρ has *trivial geometric invariants* iff the subspace in V of $\bar{G}_{K,\mathcal{S}}$-invariants is zero, and it has *trivial geometric coinvariants* iff the quotient space of $\bar{G}_{K,\mathcal{S}}$-coinvariants of V is zero. These properties are equivalent when ρ is geometrically semisimple.

Proposition 7.2.1. *If ρ is pointwise ι-pure, then it is geometrically semisimple, and in particular it has trivial geometric invariants if and only if it has trivial geometric coinvariants.*

Proof. One can rephrase semisimplicity for ρ in terms of semisimplicity for $\mathrm{ME}(\rho)$ (cf. [BBD82, 5.1.7]). It follows that both are geometrically semisimple if ρ is ι-pure (see [BBD82, 5.3.8]), and then the spaces of invariants and coinvariants are isomorphic, so both vanish or neither does. □

Corollary 7.2.2. *If ρ is pointwise ι-pure and has trivial geometric invariants, then $H^i(\bar{X}, \mathrm{ME}(\rho))$ and $H^i_c(\bar{U}, \mathrm{ME}(\rho))$ vanish for $i \neq 1$, and there is an exact sequence*

$$0 \longrightarrow H^0(\bar{Z}, \mathrm{ME}(\rho)) \longrightarrow H^1_c(\bar{U}, \mathrm{ME}(\rho)) \longrightarrow H^1(\bar{X}, \mathrm{ME}(\rho)) \longrightarrow 0. \tag{7.2.3}$$

Therefore $L(T, \rho) = P_1(T, \rho)$ and $L_{\mathcal{C}}(T, \rho) = P_{1,\mathcal{C}}(T, \rho)$.

Proof. Suppose ρ is pointwise ι-pure and has trivial geometric invariants so that Proposition 7.2.1 implies ρ has trivial geometric coinvariants. We claim $H^i(\bar{X}, \mathrm{ME}(\rho))$ vanishes for $i \neq 1$. The Corollary then follows by observing that (B.0.3) simplifies to (7.2.3) and that $H^2_c(\bar{U}, \mathrm{ME}(\rho))$ vanishes by (B.0.4).

The claim is independent of U, so up to shrinking U, we suppose $j^*\mathrm{ME}(\rho)$ is lisse. Then

$$H^0(\bar{X}, \mathrm{ME}(\rho)) = H^0(\bar{U}, \mathrm{ME}(\rho)) \text{ and } H^2(\bar{X}, \mathrm{ME}(\rho)) = H^2_c(\bar{U}, \mathrm{ME}(\rho))$$

are the subspace of $\pi_1(\bar{U})$-invariants and (a Tate twist of the) quotient space of $\pi_1(\bar{U})$-coinvariants respectively of V by (2.0.2). The claim is also independent of $\mathcal{S}$, so up to replacing $\mathcal{S}$ by a finite superset in $\mathcal{P}$, we suppose ρ factors through a natural quotient $\bar{G}_{K,\mathcal{S}} \twoheadrightarrow \pi_1(\bar{U})$. Then the cohomology spaces in question are the $\bar{G}_{K,\mathcal{S}}$-invariants and $\bar{G}_{K,\mathcal{S}}$-coinvariants of V, which are trivial by hypothesis, so $H^i(\bar{X}, \mathrm{ME}(\rho))$ vanishes for $i \neq 1$ as claimed. $\square$

7.3. **Pure polynomial L-functions.** In this section we present two theorems. They address the partial and complete L-functions of $\rho \otimes \varphi$ respectively. In both cases we focus on necessary and sufficient conditions for the L-function in question to be a polynomial.

Let $\mathbb{A}^1_t[1/c] \subseteq \mathbb{A}^1_t$ be the open complement of the locus $c = 0$. To say that a sheaf $\mathcal{F}$ on $\mathbb{P}^1_t$ is *supported on* $U \subseteq \mathbb{P}^1_t$ means that the stalks of $\mathcal{F}$ vanish over the points of the complement $Z = \mathbb{P}^1_t \smallsetminus U$.

Theorem 7.3.1. *The following are equivalent:*

(i) $M_\mathcal{C}(T, \rho) = 1$, that is, $\mathrm{ME}(\rho)$ is supported on $\mathbb{A}^1_t[1/c]$;

(ii) $L_\mathcal{C}(T, \rho)$ is a polynomial which is ι-pure of q-weight $w + 1$.

Note, $M_\mathcal{C}(T, \rho)$ is the L-function of the restriction of $\mathrm{ME}(\rho)$ to Z, so the former is trivial if and only if the latter is.

Proof. If (i) holds, then the subspace of $I(\infty)$-invariants of V is trivial, so a fortiori, the subspace of $\bar{G}_{K,\mathcal{S}}$-invariants is trivial. Therefore Corollary 7.2.2 implies $L_\mathcal{C}(T, \rho)$ equals $L(T, \rho) = P_1(T, \rho)$ and hence Theorem 6.2.1 implies (ii) holds.

If (ii) holds, then $P_{2,\mathcal{C}}(T, \rho)$ divides $P_{1,\mathcal{C}}(T, \rho)$ by (3.4.2). Theorem 6.2.1 implies $P_{2,\mathcal{C}}(T, \rho) = P_2(T, \rho)$ is ι-pure of q-weight $w + 2$, so it is coprime to $P_{1,\mathcal{C}}(T, \rho)$ and hence trivial. Therefore $H^2(\bar{X}, \mathrm{ME}(\rho))$ vanishes, and hence $H^0(\bar{X}, \mathrm{ME}(\rho))$ also vanishes since ρ is geometrically semisimple. That is, ρ has trivial geometric invariants. Moreover, $1/M_\mathcal{C}(T, \rho)$ is a polynomial which is ι-mixed of q-weights $\leq w$ by Lemma 6.3.1 while $L(T, \rho)$ is a polynomial which is ι-pure of q-weight w, so Corollary 7.2.2 implies (i) holds. $\square$

Now we turn to the complete L-function.

Theorem 7.3.2. *Suppose $\rho \otimes \varphi$ is pointwise ι-pure of weight w. Then the following assertions are equivalent:*

(i) the complete L-function $L(T, \rho \otimes \varphi)$ is in $\bar{\mathbb{Q}}(T)$ but not $\bar{\mathbb{Q}}[T]$;

(ii) the cohomological factors $P_0(T, \rho \otimes \varphi)$ and $P_2(T, \rho \otimes \varphi)$ are non-trivial polynomials in $\bar{\mathbb{Q}}[T]$;

(iii) the cohomological factor $P_2(T, \rho \otimes \varphi)$ is a non-trivial polynomial in $\bar{\mathbb{Q}}[T]$;

(iv) the twist $\rho \otimes \varphi$ has non-trivial geometric coinvariants;

(v) the twist $\rho \otimes \varphi$ has non-trivial geometric invariants and coinvariants.

If these assertions are not true, then

(vi) $L_\mathcal{C}(T, \rho \otimes \varphi)$ equals $P_{1,\mathcal{C}}(T, \rho \otimes \varphi)$ and is ι-mixed of q-weights $\leq w + 1$;

(vii) $L(T, \rho \otimes \varphi)$ is the largest ι-pure factor of q-weight $w+1$ of $L_{\mathcal{C}}(T, \rho \otimes \varphi)$.

Proof. First we prove the assertions are equivalent. On one hand, Theorem 6.2.1 implies that the cohomological factors $P_i(T, \rho)$ are relatively prime, so (i) and (ii) are equivalent. Moreover, (ii) and (v) (resp. (iii) and (iv)) are equivalent by (2.0.2) and (3.4.1). On the other hand, Proposition 7.2.1 implies that $P_0(T, \rho \otimes \varphi)$ is trivial if and only if $P_2(T, \rho \otimes \varphi)$ is trivial, so (ii) and (iii) are equivalent.

Now suppose the assertions are not true. On one hand, Corollary 7.2.2 implies

$$L(T, \rho \otimes \varphi) = P_1(T, \rho \otimes \varphi), \quad L_{\mathcal{C}}(T, \rho \otimes \varphi) = P_{1,\mathcal{C}}(T, \rho \otimes \varphi),$$

so both are polynomials as claimed. On the other hand, Theorem 6.2.1 implies $L(T, \rho \otimes \varphi)$ is ι-pure of q-weight $w+1$ and $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ is ι-mixed of q-weights $\leq w+1$ since $\rho \otimes \varphi$ is pointwise ι-pure of weight w. Moreover, Lemma 6.3.1 implies that $L_{\mathcal{C}}(T, \rho \otimes \varphi)/L(T, \rho \otimes \varphi) = 1/M_{\mathcal{C}}(T, \rho \otimes \varphi)$ is a polynomial which is ι-mixed of q-weights $\leq w$, so $L(T, \rho \otimes \varphi)$ is the largest ι-pure factor of $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ of q-weight $w+1$ as claimed. $\square$

Remark 7.3.3. Observe that $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ is 'usually' a pure polynomial of degree $r_{\emptyset}(\rho)$ (cf. Remark 4.3.3).

8. Trichotomy of Characters

Fix field embeddings $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_\ell$ and $\iota\colon \bar{\mathbb{Q}} \to \mathbb{C}$. We suppose throughout this section that ρ is pointwise ι-pure of weight w so that we can apply Deligne's theorem and talk about the weights of the zeros and poles of $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ as φ varies. Having done so, we partition $\Phi(c)$ into three classes of characters based the possible size of the summands of

$$\mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)^2} \sum_{\varphi \in \Phi(c) \smallsetminus \{\mathbf{1}\}} |\iota(b_{\rho\otimes\varphi,n})|^2. \tag{8.0.1}$$

In our classification, each $\varphi \in \Phi(c)$ is either good or bad (for ρ), and each bad character is either mixed or heavy. One one hand, one can show that most characters are good and that they're the ones for which we will regard

$$b^*_{\rho\otimes\varphi,n} := \frac{\iota(b_{\rho\otimes\varphi,n})}{q^{n(1+w)/2}}$$

as the trace of a unitary matrix. This will allow us to approximate the sum in (8.0.1) using a matrix integral. On the other hand, the heavy characters are those for which $|b^*_{\rho\otimes\varphi,n}|^2$ is unbounded as $q \to \infty$, and their number is bounded as $q \to \infty$.

8.1. Good versus bad.

We say that a character $\varphi \in \Phi(c)$ is *good for* ρ iff it belongs to the subset

$$\Phi(c)_{\rho\,\mathrm{good}} := \left\{ \varphi \in \Phi(c) : L_{\mathcal{C}}(T, \rho \otimes \varphi) = L(T, \rho \otimes \varphi) \in \bar{\mathbb{Q}}[T] \right\}, \tag{8.1.1}$$

and otherwise we say it is *bad for* ρ and define

$$\Phi(c)_{\rho\,\mathrm{bad}} := \Phi(c) \smallsetminus \Phi(c)_{\rho\,\mathrm{good}}.$$

As we will see, this coincides with Katz's classification of characters in [Kat12] (cf. Lemma 10.3.1).

By Theorem 7.3.2, the good characters are precisely those for which the partial L-function $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ has three properties: it is identical to the polynomial

$$P_{1,\mathcal{C}}(T, \rho) = \det(1 - T\,\mathrm{Frob}_q \mid H^1_c(\bar{\mathbb{A}}^1_t[1/c], \mathrm{ME}(\rho \otimes \varphi)));$$

it has degree $R = r_{\mathcal{C}}(\rho)$; it is ι-pure of q-weight $w+1$. Equivalently, they are the characters for which the normalized L-function

$$L^*_{\mathcal{C}}(T, \rho \otimes \varphi) = L_{\mathcal{C}}(T/(\sqrt{q})^{1+w}, \rho \otimes \varphi) \tag{8.1.2}$$

is a polynomial and ι-pure of q-weight zero.

In particular, if $\mathrm{std}\colon U_R(\mathbb{C}) \to \mathrm{GL}_R(\mathbb{C})$ is the inclusion $U_R(\mathbb{C}) \subseteq \mathrm{GL}_R(\mathbb{C})$, then for each good φ, there is a unique conjugacy class

$$\theta_{\rho,\varphi} \subset U_R(\mathbb{C}) \subseteq \mathrm{GL}_R(\mathbb{C})$$

such that $\iota(L^*_{\mathcal{C}}(T, \rho\otimes\varphi))$ equals the characteristic polynomial of $\mathrm{std}(\theta_{\rho,\varphi})$. Therefore, from the identity

$$T\frac{d}{dT}\iota(L^*_{\mathcal{C}}(T, \rho\otimes\varphi)) = \sum_{n=1}^{\infty} b^*_{\rho\otimes\varphi,n}T^n \tag{8.1.3}$$

one deduces that

$$b^*_{\rho\otimes\varphi,n} = -\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi})) \text{ for } \varphi \in \Phi(c)_{\rho\,\mathrm{good}} \tag{8.1.4}$$

and $n \geq 1$.

8.2. **Equidistributed matrices.** If we combine (8.0.1) with (8.1.4), then

$$\frac{\phi(c)}{q^{n(1+w)}}\mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}} |\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 + \frac{1}{\phi(c)} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{bad}}} |\iota(b^*_{\rho\otimes\varphi,n})|^2. \tag{8.2.1}$$

Definition 8.2.2. Let $\mathbb{K} \subseteq U_R(\mathbb{C})$ be a compact reductive subgroup, say a maximal compact subgroup of a reductive subgroup $G(\mathbb{C}) \subseteq \mathrm{GL}_R(\mathbb{C})$. The multiset

$$\Theta_{\rho,q} := \{\, \theta_{\rho,\varphi} : \varphi \in \Phi(c)_{\rho\,\mathrm{good}} \,\} \subseteq U_R(\mathbb{C})$$

becomes equidistributed in $\mathbb{K}$ *as* $q \to \infty$ iff it satisfies:

(i) $\mathbb{K} \cap \theta$ is non-empty, for any $\theta \in \Theta_{\rho,q}$ and any q;

(ii) for *any* continuous central function $f\colon \mathbb{K} \to \mathbb{C}$, one has

$$\lim_{q\to\infty} \frac{1}{|\Phi(c)^*_{\rho\,\mathrm{good}}|} \sum_{\varphi\in\Phi(c)^*_{\rho\,\mathrm{good}}} f(\theta_{\rho,\varphi}) = \int_{\mathbb{K}} f(\theta)d\theta \tag{8.2.3}$$

where $d\theta$ is probability Haar measure on $\mathbb{K}$.

The general theory of Katz tells us that, in favorable situations, some such $\mathbb{K}$ exists and is unique up to conjugation.

Remark 8.2.4. The Peter-Weyl theorem implies that proving 8.2.2.ii holds is equivalent to proving that (8.2.3) holds for every f of the form $f = \mathrm{Tr}\circ\Lambda$ where

$$\Lambda\colon \mathbb{K} \to \mathrm{GL}_{\dim(\Lambda)}(\mathbb{C})$$

is a finite-dimensional representation. One may even restrict to irreducible representations.

8.3. **Refining bad: mixed versus heavy.** There are two ways a character can be bad:

(i) either $L(T, \rho\otimes\varphi)$ is not a polynomial in $\bar{\mathbb{Q}}(T)$;

(ii) or $L(T, \rho\otimes\varphi)$ and $L_{\mathcal{C}}(T, \rho\otimes\varphi)$ are polynomials but not equal to each other in $\bar{\mathbb{Q}}[T]$.

What distinguishes the first case from the second is that $\iota(L(T, \rho\otimes\varphi))$ has poles some of which have excessive weight. More precisely, if the factor $P_2(T, \rho\otimes\varphi)$ of the denominator of $L(T, \rho\otimes\varphi)$ is non-trivial, then it ι-mixed of q-weights $\leq w+1$ but not ι-mixed of q-weights $\leq w$ (cf. Theorem 7.3.2).

Definition 8.3.1. We say that φ is *heavy for* ρ (or ρ*-heavy*) iff it lies in the subset

$$\Phi(c)_{\rho\,\mathrm{heavy}} := \{\, \varphi \in \Phi(c)_{\rho\,\mathrm{bad}} : L(T, \rho \otimes \varphi) \notin \bar{\mathbb{Q}}[T] \,\}.$$

Otherwise, we say that φ is *mixed for* ρ (or ρ*-mixed*) to mean it lies in the subset

$$\Phi(c)_{\rho\,\mathrm{mixed}} := \Phi(c)_{\rho\,\mathrm{bad}} \smallsetminus \Phi(c)_{\rho\,\mathrm{heavy}}.$$

Equivalently, φ is mixed for ρ if and only if $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ is a polynomial which is ι-mixed of q-weights $\leq w+1$ but not ι-pure of q-weight $w+1$.

Lemma 8.3.2. *Suppose ρ is geometrically simple and pointwise ι-pure and $\varphi \in \Phi(c)$. Then φ is heavy for ρ if and only if $\rho \otimes \varphi$ is geometrically isomorphic to the trivial representation.*

Proof. The essential point is that since $\rho \otimes \varphi$ is geometrically simple, the quotient space of geometric coinvariants $(V_\varphi)_{\bar{G}_{K,\mathcal{R}}}$ either vanishes or equals V_φ. The former occurs if and only if $\rho \otimes \varphi$ is geometrically isomorphic to the trivial representation, so the lemma follows from Theorem 7.3.2. ☐

Corollary 8.3.3. *Suppose ρ is geometrically simple and pointwise ι-pure, and let $r = \dim(V)$. Then $\Phi(c)_{\rho\,\mathrm{heavy}} \subseteq \{\mathbf{1}\}$ if and only if one of the following hold:*

(i) $r > 1$;

(ii) $r = 1$ and ρ is geometrically isomorphic to the trivial representation;

(iii) $r = 1$ and ρ is not geometrically isomorphic to a Dirichlet character in $\Phi(c)$.

Moreover, $\Phi(c)_{\rho\,\mathrm{heavy}} = \{\mathbf{1}\}$ if and only if (ii) *holds.*

Proof. Let $\varphi \in \Phi(c)$. Lemma 8.3.2 implies that φ is heavy for ρ if and only if $\rho \otimes \varphi$ is geometrically isomorphic to the trivial representation (and hence $r = 1$). By the contrapositive, φ is not heavy for ρ if and only if $r > 1$ or ρ is not geometrically isomorphic to $1/\varphi$. Therefore (i) or (iii) holds if and only if $\Phi(c)_{\rho\,\mathrm{heavy}}$ is empty, and (ii) holds if and only if $\Phi(c)_{\rho\,\mathrm{heavy}} = \{\mathbf{1}\}$. ☐

9. Variance Revisited

We have yet to make precise what we mean when we say that most characters are good or that most bad characters are mixed. Nonetheless, the following theorem shows how we can express the $\mathrm{Var}[S_{n,c}(A)]$ using our trichotomy of characters.

Theorem 9.0.1. *Let $\mathbb{K} \subseteq U_R(\mathbb{C})$ be a compact reductive subgroup and $d\theta$ be its Haar measure. Suppose that ρ is pointwise ι-pure of weight w, that $\Theta_{\rho,q}$ is equidistributed in $\mathbb{K}$ as $q \to \infty$, and that $\Phi(c)_{\rho\,\mathrm{heavy}} \subseteq \{\mathbf{1}\}$. Then*

$$\frac{\phi(c)}{q^{n(1+w)}} \cdot \mathrm{Var}[S_{n,c}(A)] = \frac{|\Phi(c)_{\rho\,\mathrm{good}}|}{|\Phi(c)|} \int_{\mathbb{K}} |\mathrm{Tr}(\theta^n)|^2 d\theta + O\left(\frac{|\Phi(c)_{\rho\,\mathrm{mixed}} \smallsetminus \{\mathbf{1}\}|}{|\Phi(c)|}\right)$$

as $q \to \infty$.

The proof is in §9.2.

Remark 9.0.2. Later we will prove:

$$|\Phi(c)_{\rho\,\mathrm{good}}| \sim |\Phi(c)|, \quad |\Phi(c)_{\rho\,\mathrm{mixed}} \smallsetminus \{\mathbf{1}\}| = O(|\Phi(c)|/q)$$

See Corollaries 10.3.2 and 10.3.3.

Remark 9.0.3. One can also show that

$$\int_{U_R(\mathbb{C})} |\mathrm{Tr}\,\mathrm{std}(\theta^n)|^2 \, d\theta = \min\{n, R\}. \tag{9.0.4}$$

See[1] [DE01, Th. 1].

9.1. **Archimedean bounds.**

Lemma 9.1.1. *If M is an invertible $d \times d$ matrix with coefficients in $\bar{\mathbb{Q}}_\ell$ and if* $\det(1 - M\,T)$ *is mixed of q-weights $\le w$, then* $\mathrm{Tr}(M) \in \bar{\mathbb{Q}}$ *and* $|\iota(\mathrm{Tr}(M))|^2 \le dq^w$ *for every field embedding* $\iota \colon \bar{\mathbb{Q}} \to \mathbb{C}$.

Proof. If M is invertible and $\psi(T) = \det(1 - M\,T)$ is mixed, there exist $\beta_1, \dots, \beta_d \in \bar{\mathbb{Q}}^\times$ such that

$$\psi(T) = \prod_{i=1}^{d}(1 - \beta_i T) = 1 - \mathrm{Tr}(M) \cdot T + \cdots + (-1)^d \cdot \det(M) \cdot T^d$$

and such that $\mathrm{Tr}(M) = \beta_1 + \cdots + \beta_m$ also lies in $\bar{\mathbb{Q}}$. Therefore, if $\iota \colon \bar{\mathbb{Q}} \to \mathbb{C}$ is a field embedding, then

$$|\mathrm{Tr}(M)|^2 = \left|\sum_{i=1}^{d} \iota(\beta_i)\right|^2 \le \sum_{i=1}^{d} |\iota(\beta_i)|^2 = dq^w$$

as claimed. □

Lemma 9.1.2. *Suppose ρ is pointwise ι-pure of weight w and $\varphi \in \Phi(c)$. If φ is heavy for ρ, then $|b^*_{\rho\otimes\varphi,n}|^2 = O(q^n)$, and otherwise $|b^*_{\rho\otimes\varphi,n}|^2 = O(1)$. Moreover, the bounds assume n tends to infinity and the implied constants depend only on ρ.*

Proof. Consider the Tate twist

$$\mathcal{F} := \mathrm{ME}(\rho \otimes \varphi) \otimes \bar{\mathbb{Q}}_\ell((1 + w)/2).$$

It is pointwise ι-pure of weight -1 since $\mathcal{F}$ is pointwise ι-pure of weight w, and its partial L-function is $L^*_{\mathcal{C}}(T, \rho \otimes \varphi)$. Therefore

$$b^*_{\rho\otimes\varphi,n} = -\mathrm{Tr}\left(\mathrm{Frob}_q^n \mid H^1_c(\bar{\mathbb{A}}^1_t[1/c], \mathcal{F})\right) + \mathrm{Tr}\left(\mathrm{Frob}_q^n \mid H^2_c(\bar{\mathbb{A}}^1_t[1/c], \mathcal{F})\right)$$

by (8.1.3). Moreover, the second term on the right vanishes unless φ is heavy, and

$$|\,\iota\left(\mathrm{Tr}\left(\mathrm{Frob}_q^n \mid H^i_c(\bar{\mathbb{A}}^1_t[1/c], \mathcal{F})\right)\right)|^2 = O(q^{n(i-1)})$$

by Theorem 6.2.1 and Lemma 9.1.1. □

9.2. **Proof of Theorem 9.0.1.** By (8.2.1) we have

$$\frac{\phi(c)}{q^{n(1+w)}} \mathrm{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)} \sum_{\varphi \in \Phi(c)^*_{\rho\,\mathrm{good}}} |\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 + \frac{1}{\phi(c)} \sum_{\varphi \in \Phi(c)^*_{\rho\,\mathrm{bad}}} |\iota(b^*_{\rho\otimes\varphi,n})|^2$$

for any $S \subseteq \Phi(c)$.

On one hand, by (8.2.3) we have

$$\lim_{q\to\infty} \frac{1}{\phi(c)} \sum_{\substack{\varphi \in \Phi(c)_{\rho\,\mathrm{good}} \\ \varphi \neq \mathbf{1}}} |\mathrm{Tr}(\mathrm{std}(\theta^n_{\rho,\varphi}))|^2 = \frac{|\Phi(c)_{\rho\,\mathrm{good}}|}{|\Phi(c)|} \int_{U_R(\mathbb{C})} |\mathrm{Tr}(\theta^n)|^2 d\theta.$$

On the other hand, by Lemma 9.1.2 we have

$$\frac{1}{\phi(c)} \sum_{\substack{\varphi \in \Phi(c)_{\rho\,\mathrm{bad}} \\ \varphi \neq \mathbf{1}}} |\iota(b^*_{\rho\otimes\varphi,n})|^2 = \frac{1}{|\Phi(c)|} \sum_{\substack{\varphi \in \Phi(c)_{\rho\,\mathrm{mixed}} \\ \varphi \neq \mathbf{1}}} O(1) + \frac{1}{|\Phi(c)|} \sum_{\substack{\varphi \in \Phi(c)_{\rho\,\mathrm{heavy}} \\ \varphi \neq \mathbf{1}}} O(q^n)$$

[1] NB: The reference [DS94, Th. 2] is sometimes used, but as explained in [DE01], the theorem is incorrectly stated.

$$= \frac{|\Phi(c)_{\rho\,\mathrm{mixed}} \smallsetminus \{\mathbf{1}\}|}{|\Phi(c)|} \cdot O(1) + \frac{|\Phi(c)_{\rho\,\mathrm{heavy}} \smallsetminus \{\mathbf{1}\}|}{|\Phi(c)|} \cdot O(q^n)$$

where the implied constants are independent of φ, and the last term vanishes if $\Phi(c)_{\rho\,\mathrm{heavy}} \subseteq \{\mathbf{1}\}$.

Remark 9.2.1. While we do not need the result, we point out that (5.4.2) and Lemma 9.1.2 imply

$$\frac{\phi(c)}{q^{n(1+w)}} \cdot |\iota(\mathbb{E}[S_{n,c}(A)])|^2 = |b^*_{\rho,n}|^2 \ = \ O(1) \text{ for } q \to \infty$$

when ρ is pointwise ι-pure of weight w and φ is not heavy for ρ.

10. Big Monodromy Implies Equidistribution

In principle, one could try to exhibit equidistribution for all of $\Theta_{\rho,q}$ at once. Instead we follow Katz and (try to) prove simultaneous and uniform equidistribution for certain one-parameter families of characters. More precisely, we partition $\Phi(c)$ into cosets $\varphi\Phi(u)^\nu$ of a subgroup $\Phi(u)^\nu$ (defined in §10.2) and (try to) prove equidistribution for characters in

(10.0.1) $$\varphi\Phi(u)^\nu_{\rho\,\mathrm{good}} = \varphi\Phi(u)^\nu \cap \Phi(c)_{\rho\,\mathrm{good}}.$$

Doing so for a single coset is equivalent to showing that an associated monodromy group we denote $\mathcal{G}_{\mathrm{geom}}(\rho, \varphi\Phi(u)^\nu)$ equals $\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$. See §10.2, §10.3, and §10.4.

The monodromy group is an algebraic subgroup of $\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$. We say the former is *big* iff it equals the latter, and we write

(10.0.2) $$\Phi(c)_{\rho\,\mathrm{big}} = \{\, \varphi \in \Phi(c) : \mathcal{G}_{\mathrm{geom}}(\rho, \varphi\Phi(u)^\nu) \text{ is big} \,\}$$

for the subset of big characters. We say that the *Mellin transform* of ρ has *big monodromy* in $\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$ iff

(10.0.3) $$|\Phi(c)_{\rho\,\mathrm{big}}| \sim |\Phi(c)| \text{ as } n \to \infty$$

where $q = q_0^n$ for prime power q_0. We show that it implies $\Theta_{\rho,q}$ becomes equidistributed in $U_R(\mathbb{C})$. By Remark 8.2.4, it suffices to prove the following theorem.

Theorem 10.0.4. *Suppose ρ is pointwise ι-pure and φ is in $\Phi(c)_{\rho\,\mathrm{big}}$. Let $\Lambda\colon U_R(\mathbb{C}) \to \mathrm{GL}_{\dim(\Lambda)}(\mathbb{C})$ be a finite-dimensional representation. If $q = q_0^n$ is sufficiently large, then*

(10.0.5) $$\frac{1}{|\varphi\Phi(u)^\nu_{\rho\,\mathrm{good}}|} \sum_{\varphi' \in \varphi\Phi(u)^\nu_{\rho\,\mathrm{good}}} \mathrm{Tr}\,\Lambda(\theta_{\rho,\varphi'}) = \int_{U_R(\mathbb{C})} \mathrm{Tr}\,\Lambda(\theta)\,d\theta + o(1) \ \text{ as } n \to \infty,$$

and the implicit constant depends only on $r = \dim(V)$ and $\dim(\Lambda)$. In particular, if the Mellin transform of ρ has big monodromy, then $\Theta_{\rho,q}$ becomes equidistributed in $U_R(\mathbb{C})$ as $n \to \infty$.

The proof is in §10.5.

Remark 10.0.6. Observe that the q-weight w of ρ plays no role in the statement of the theorem. This is because we factored out the weight in the normalization (8.1.2). Another way to achieve the same renormalization is to replace ρ by an appropriate Tate twist so that $w = -1$ and $L^*_{\mathcal{C}}(T, \rho \otimes \varphi) = L_{\mathcal{C}}(T, \rho \otimes \varphi)$.

10.1. **Reduction to $\mathbb{G}_m$.** Recall $X = \mathbb{P}^1_t$ and $c \in \mathbb{F}_q[t] \subset K$ is monic and square free. Let $\mathbb{P}^1_u$ denote the projective u-line and $U_c = X \smallsetminus \mathcal{C}$. Moreover, let $L = \mathbb{F}_q(u) \to K$ the $\mathbb{F}_q$-linear field embedding generated by $u \mapsto c$ and corresponding to the finite cover $c\colon X \to \mathbb{P}^1_u$. The morphism has generic degree $n = \deg(c)$ and is generically etale since it has n distinct points over $u = 0$. It also fits in a commutative diagram

$$\begin{tikzcd} U_c \arrow[r] \arrow[d, "c"'] & X \arrow[d, "c"] & \mathcal{C} \arrow[l] \arrow[d, "c"] \\ \mathbb{G}_m \arrow[r] & \mathbb{P}^1_u & \mathcal{C}' = \{0, \infty\} \arrow[l] \end{tikzcd}$$

where the outer vertical maps are finite morphisms.

Let $\mathcal{R}$ be a finite set of places in L including those lying under $\mathcal{C} \cup \mathcal{S}$ and those which ramify in K/L, and let $U' \subset \mathbb{P}^1_u$ be the corresponding open complement. Then for each $\varphi \in \Phi(c)$, we have an induced representation

$$\mathrm{Ind}(\rho \otimes \varphi)\colon G_{L,\mathcal{R}} \to \mathrm{GL}(\mathrm{Ind}(V_\varphi))$$

where $\mathrm{Ind}(V_\varphi)$ is a vector space of dimension $n \cdot \dim(V_\varphi)$. The representation is the geometric generic fiber of $\mathcal{F} = c_*\mathrm{ME}(\rho \otimes \varphi)$, and the hypotheses on $\mathcal{R}$ imply $\mathcal{F}$ is lisse on $U' \subset \mathbb{P}^1_u$. (In fact, Proposition A.0.4 implies $\mathcal{F}$ and $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))$ are isomorphic on U'.). In particular, if $\bar{u}$ is a geometric closed point of $\mathbb{P}^1_u$, that is, the image of a closed point of $\bar{X}$, and if

$$c^{-1}(\bar{u}) = \{\bar{t}_1, \ldots, \bar{t}_m\} \subset \bar{X},$$

then the various geometric stalks satisfy

$$(c_*\mathcal{F})_{\bar{u}} = H^0(\bar{u}, c_*\mathcal{F}) = \oplus_{i=1}^m H^0(\bar{t}_i, \mathcal{F}) = \oplus_{i=1}^m \mathcal{F}_{\bar{t}_i} \tag{10.1.1}$$

as $\bar{\mathbb{Q}}_\ell$-vector spaces (cf. [Mil80, II.3.1.(e) and II.3.5.(c)]). Thus if $\mathcal{F}$ is supported on U_c, then $c_*\mathcal{F}$ is supported on $\mathbb{G}_m$.

Lemma 10.1.2. *If ρ is pointwise ι-pure of weight w, then so is* $\mathrm{Ind}(\rho \otimes \varphi)$.

Proof. Let $\bar{v}$ be a place in L not lying in $\mathcal{R}$, and let $v|\bar{v}$ denote any place in K lying over $\bar{v}$. Then

$$L(T^{\deg(\bar{v})}, \mathrm{Ind}(\rho \otimes \varphi)_{\bar{v}}) = \prod_{v|\bar{v}} L(T^{\deg(v)}, (\rho \otimes \varphi)_v).$$

by (10.1.1). In particular, Lemma 6.2.2 implies the factors on the right are ι-pure of q-weight w, so the left side is also ι-pure of q-weight w. □

The functorial properties of c_* yield canonical isomorphisms

$$H^i(\bar{X}, \mathcal{F}) = H^i(\bar{X}, c_*\mathcal{F}) \quad\text{and}\quad H^i_c(\bar{U}_c, \mathcal{F}) = H^i_c(\bar{\mathbb{G}}_m, c_*\mathcal{F}) \tag{10.1.3}$$

for each i. For example, c_* is exact since c is a finite map, so the first identity in (10.1.3) is a consequence of the (trivial) Leray spectral sequence (cf. [Mil80, II.3.6 and III.1.18]). In particular, the identities (3.4.2), (3.4.4), and (10.1.3) jointly imply that

$$L(T, \mathrm{ME}(\rho \otimes \varphi)) = L(T, c_*\mathrm{ME}(\rho \otimes \varphi)) \text{ and } L_{\mathcal{C}}(T, \mathrm{ME}(\rho \otimes \varphi)) = L_{\mathcal{C}'}(T, c_*\mathrm{ME}(\rho \otimes \varphi)) \tag{10.1.4}$$

for $\varphi \in \Phi(c)$.

10.2. **One-parameter families.** Recall $c \in \mathbb{F}_q[t] \subset K$ is monic and square free and $\mathbb{F}_q(u) \to K$ is the function-field embedding which sends u to c. The norm map $K \to \mathbb{F}_q(u)$ is multiplicative and sends $t - a$ to $(-1)^n u$ for $n = \deg(c)$ and $a \in \mathbb{F}_q$ a zero of c. It also induces homomorphisms

$$\nu\colon \Gamma(c) \to \Gamma(u) \quad \text{and} \quad \nu^*\colon \Phi(u) \to \Phi(c)$$

where

$$\Gamma(u) := (\mathbb{F}_q[u]/u\mathbb{F}_q[u])^\times \quad \text{and} \quad \Phi(u) := \mathrm{Hom}(\Gamma(u), \bar{\mathbb{Q}}_\ell^\times)$$

(see [Kat13, §2]). In particular, ν is surjective, so its dual ν^* is injective, and we can identify $\Phi(u)$ with its image $\Phi(u)^\nu$. Moreover, as the following lemma shows, twisting by elements of the coset $\varphi\Phi(u)^\nu$ is the 'same' as twisting by elements of $\Phi(u)$.

Lemma 10.2.1. *Let $\varphi \in \Phi(c)$ and $\alpha \in \Phi(u)$.*

(i) $c_*\mathrm{ME}(\rho \otimes \varphi)$ *is isomorphic to* $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))$.

(ii) $c_*\mathrm{ME}(\rho \otimes \varphi\alpha^\nu)$ *is isomorphic to* $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi) \otimes \alpha)$.

Proof. By [Kat02, 3.3.1], $c_*\mathrm{ME}(\rho \otimes \varphi)$ is a middle extension, and since it is generically equal to the middle extension sheaf $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))$, Proposition 3.3.3 implies part (i) holds.

Up to replacing ρ by $\rho \otimes \varphi$, we suppose without loss of generality that $\varphi = \mathbf{1}$. Let $T \subseteq \mathbb{P}^1_t$ be a dense Zariski open subset and $U = c(T)$. Suppose that $U \subseteq \mathbb{G}_m$ so that $c^*\mathrm{ME}(\alpha)$ is lisse on T, that the restriction $c\colon T \to U$ is étale, and that $\mathrm{ME}(\rho)$ is lisse on T. Let $i\colon T \to \mathbb{P}^1_t$ and $j\colon U \to \mathbb{P}^1_u$ be the inclusions. We have

$$\mathrm{ME}(\rho \otimes \alpha^\nu) \simeq i_*i^*(\mathrm{ME}(\rho \otimes \alpha^\nu)) \simeq i_*i^*(\mathrm{ME}(\rho) \otimes \mathrm{ME}(\alpha^\nu)) \simeq i_*i^*(\mathrm{ME}(\rho) \otimes c^*\mathrm{ME}(\alpha))$$

since each of the sheaves is a middle extensions and lisse on T. Therefore the projection formula implies

$$c_*\mathrm{ME}(\rho \otimes \alpha^\nu) \simeq c_*(i_*i^*(\mathrm{ME}(\rho) \otimes c^*\mathrm{ME}(\alpha))) \simeq j_*j^*(c_*\mathrm{ME}(\rho) \otimes \mathrm{ME}(\alpha))$$

since each of the sheaves is lisse on U and a middle extension on $\mathbb{P}^1_u$ (by part (i)) and since $c\colon T \to U$ is étale. Finally,

$$j_*j^*(c_*\mathrm{ME}(\rho) \otimes \mathrm{ME}(\alpha)) \simeq j_*j^*(\mathrm{ME}(\mathrm{Ind}(\rho)) \otimes \mathrm{ME}(\alpha)) \simeq \mathrm{ME}(\mathrm{Ind}(\rho) \otimes \alpha)$$

and thus part (ii) holds. □

10.3. **Counting good characters.** We say a character $\varphi \in \Phi(c)$ is *good for ρ* or simply *good* iff it lies in the subset $\Phi(c)_{\rho\,\mathrm{good}}$ defined in (8.1.1). When $c = t$ and thus $\mathbb{A}^1_t[1/c] = \mathbb{G}_m$, then our notion of good coincides with that of Katz's (cf. [Kat12, Chapter 3]). For general c, the following lemma shows how our notion relates to his via c_*:

Lemma 10.3.1. *If $\varphi \in \Phi(c)$ and $\alpha \in \Phi(u)$, then the following are equivalent:*

(i) $\varphi\alpha^\nu$ *is good for ρ;*

(ii) $\mathrm{ME}(\rho \otimes \varphi\alpha^\nu)$ *is supported on* $\mathbb{A}^1_t[1/c]$*;*

(iii) $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi) \otimes \alpha)$ *is supported on* $\mathbb{G}_m$*;*

(iv) $\alpha \in \Phi(u)$ *is good for* $c_*\mathrm{ME}(\rho \otimes \varphi)$.

Proof. Theorem 7.3.1 implies the first conditions (i) and (ii) are equivalent. Conditions (ii) and (iii) are equivalent by the identity in (10.1.1) for $\bar{u} \in \mathcal{C}'$. Finally, taking $c = t$ and applying the equivalence of (i) and (ii) yields the equivalence of (iii) and (iv). □

Let $\Phi(c)_{\rho\,\mathrm{bad}}$ be the complement $\Phi(c) \smallsetminus \Phi(c)_{\rho\,\mathrm{good}}$ and $\varphi\Phi(u)^\nu_{\rho\,\mathrm{bad}} = \Phi(c)_{\rho\,\mathrm{bad}} \cap \varphi\Phi(u)^\nu$.

Corollary 10.3.2. $|\varphi\Phi(u)^\nu_{\rho\,\mathrm{bad}}| \leq (1 + \deg(c)) \cdot \mathrm{rank}(\rho)$.

Proof. If $\varphi \in \Phi(c)_{\rho\,\mathrm{bad}}$, then φ it coincides with some tame character of ρ at some $v \in \mathcal{C}$, and there are at most $(1+\deg(c)) \cdot \mathrm{rank}(\rho)$ such characters. Compare [Kat12, pp. 12–13]. $\square$

Corollary 10.3.3. $|\Phi(c)_{\rho\,\mathrm{good}}| \sim |\Phi(c)|$ *as* $q \to \infty$.

Proof. Observe that Corollary 10.3.2 implies

$$|\Phi(c)| - |\Phi(c)_{\rho\,\mathrm{good}}| = |\Phi(c)_{\rho\,\mathrm{bad}}| = \sum_{\varphi\Phi(u)^\nu} |\Phi(u)^\nu_{\rho\,\mathrm{bad}}| \le O(|\Phi(c)|/|\Phi(u)^\nu|) = o(|\Phi(c)|)$$

as $q \to \infty$. $\square$

One can also show that

$$|\Phi(c_0)_{\rho\,\mathrm{good}}| \sim |\Phi(c_0)| \text{ as } q \to \infty \tag{10.3.4}$$

for any monic divisor $c_0 \mid c$.

10.4. **Tannakian monodromy groups.** Suppose $c = t$ and thus $\mathcal{C}' = \mathcal{C} = \{0, \infty\}$ and $\Phi(u) = \Phi(c)$. Suppose moreover that ρ is geometrically simple and $\dim(V) > 1$ so that no geometric subquotient of $\mathrm{ME}(\rho)$ is a Kummer sheaf.

Let $j\colon \mathbb{G}_m \to \mathbb{P}^1_u$ be the inclusion, let $j_0\colon \mathbb{G}_m \to \mathbb{A}^1_u$ be the inclusion map, and for each $\alpha \in \Phi(u)$, let

$$\omega_\alpha(\mathrm{ME}(\rho)) = H^1_c(\bar{\mathbb{A}}^1_u, j_{0*}j^*\mathrm{ME}(\rho \otimes \alpha)).$$

It is a $G_{\mathbb{F}_q}$-module, that is, Frob_q acts functorially, and it corresponds to a well-defined conjugacy class of elements $\mathrm{Frob}_{\mathbb{F}_q,\alpha} \subset \mathrm{GL}(\omega(\mathrm{ME}(\rho)))$ where $\omega(\mathrm{ME}(\rho)) = \omega_{\mathbf{1}}(\mathrm{ME}(\rho))$ and $\mathbf{1} \in \Phi(u)$ is the trivial character. Moreover, if α is good, then

$$\omega_\alpha(\mathrm{ME}(\rho)) = H^1_c(\bar{\mathbb{G}}_m, \mathrm{ME}(\rho \otimes \alpha)),$$

and in particular

$$L_{\mathcal{C}}(T, \rho \otimes \alpha) = \det(1 - \mathrm{Frob}_\alpha T \mid \omega(\mathrm{ME}(\rho))).$$

In a way we will not make precise here, the Frob_α ‘generate’ ℓ-adic reductive subgroups

$$\mathcal{G}_{\mathrm{geom}}(\rho, \Phi(u)^\nu) \subseteq \mathcal{G}_{\mathrm{arith}}(\rho, \Phi(u)^\nu) \subseteq \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$$

which are well-defined up to conjugacy. They are fundamental groups of certain Tannakian categories, and we call them the *Tannakian monodromy groups of* ρ. See Appendix D for details. We say the Mellin transform of ρ has *big Tannakian monodromy* iff $\mathcal{G}_{\mathrm{geom}}(\rho, \Phi(u)^\nu) = \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$.

For general c and $\varphi \in \Phi(c)$, we write

$$\mathcal{G}_{\mathrm{geom}}(\rho, \varphi\Phi(u)^\nu) \subseteq \mathcal{G}_{\mathrm{arith}}(\rho, \varphi\Phi(u)^\nu) \subseteq \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$$

for the Tannakian monodromy groups of $\mathrm{Ind}(\rho \otimes \varphi)$, and we say that the Mellin transform of $\rho \otimes \varphi$ has *big Tannakian monodromy* iff $\mathcal{G}_{\mathrm{geom}}(\rho, \varphi\Phi(u)^\nu) = \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$. Now the action of Frob_q on $\omega_\alpha(\mathrm{ME}(\rho \otimes \varphi))$ corresponds to a well-defined conjugacy class $\mathrm{Frob}_{\mathbb{F}_q,\alpha} \subset \mathcal{G}_{\mathrm{arith}}(\rho, \varphi\Phi(u)^\nu)$.

10.5. **Proof of Theorem 10.0.4.** We may suppose without loss of generality that Λ is irreducible since it is semisimple and $\mathrm{Tr}(\Lambda_1 \oplus \Lambda_2) = \mathrm{Tr}(\Lambda_1) + \mathrm{Tr}(\Lambda_2)$ for any representations Λ_1, Λ_2. Moreover, we have the Schur orthogonality relations

$$\int_{U_R(\mathbb{C})} \mathrm{Tr}\,\Lambda(\theta)\,d\theta = \begin{cases} 1 & \Lambda \text{ is the trivial representation} \\ 0 & \text{otherwise} \end{cases}$$

so to prove (10.0.5) we must show that

$$\text{(10.5.1)}\qquad \frac{1}{|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}|}\sum_{\varphi'\in\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}}\operatorname{Tr}\Lambda(\theta_{\rho,\varphi'}) = \begin{cases}1 & \Lambda \text{ is the trivial representation}\\ o(1) & \text{otherwise}\end{cases}$$

when q is large.

If q is sufficiently large, then Corollary 10.3.2 implies that

$$|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{bad}}| \leq (1+\deg(c))\cdot\operatorname{rank}(\rho) < |\varphi\Phi(u)^{\nu}|$$

and thus $\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}$ is non-empty. In particular, the left side of (10.5.1) is defined for large q, and it is identically 1 when Λ is the trivial representation. On the other hand, if Λ is non-trivial and if q is bigger than $(|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{bad}}|+1)^2$, then [Kat12, 7.5] implies that

$$\text{(10.5.2)}\qquad \frac{1}{|\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}|}\left|\sum_{\varphi'\in\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}}\operatorname{Tr}\Lambda(\theta_{\rho,\varphi'})\right| \leq (\dim(V)+\dim(\Lambda))\left(\frac{1}{\sqrt{q}}+\frac{1}{\sqrt{q}^3}\right).$$

Thus (10.5.1) holds, as claimed, and the implicit constant depends only on r and $\dim(\Lambda)$.

To complete the proof of the theorem we must show that $\Theta_{\rho,q}$ becomes equidistributed in $U_R(\mathbb{C})$. We observe that

$$\text{(10.5.3)}\qquad |\operatorname{Tr}\Lambda(\theta_{\rho,\varphi'})| \leq \dim(\Lambda) \text{ for } \varphi'\in\varphi\Phi(u)^{\nu}_{\rho\,\mathrm{good}}$$

Therefore

$$\sum_{\varphi\in\Phi(c)_{\rho\,\mathrm{good}}}\operatorname{Tr}\Lambda(\theta_{\rho,\varphi}) = \sum_{\varphi\in\Phi(c)_{\rho\,\mathrm{good}\,\cap\,\rho\,\mathrm{big}}}\operatorname{Tr}\Lambda(\theta_{\rho,\varphi}) + o(1)\cdot|\Phi(c)_{\rho\,\mathrm{good}}\smallsetminus\Phi(c)_{\rho\,\mathrm{good}\,\cap\,\rho\,\mathrm{big}}|$$

where

$$\Phi(c)_{\rho\,\mathrm{good}\,\cap\,\rho\,\mathrm{big}} = \Phi(c)_{\rho\,\mathrm{good}}\cap\Phi(c)_{\rho\,\mathrm{big}}.$$

In particular, if the Mellin transform of ρ has big monodromy, that is, if (10.0.3) holds, then

$$\frac{|\Phi(c)_{\rho\,\mathrm{good}}\smallsetminus\Phi(c)_{\rho\,\mathrm{good}\,\cap\,\rho\,\mathrm{big}}|}{|\Phi(c)_{\rho\,\mathrm{good}}|} = o(1) \text{ for } q\to\infty$$

and thus

$$\begin{aligned}\frac{1}{|\Phi(c)_{\rho\,\mathrm{good}}|}\sum_{\varphi\in\Phi(c)_{\rho\,\mathrm{good}}}\operatorname{Tr}\Lambda(\theta_{\rho,\varphi}) &\overset{(10.5.3)}{=} \frac{1}{|\Phi(c)_{\rho\,\mathrm{good}}|}\sum_{\varphi\in\Phi(c)_{\rho\,\mathrm{good}\,\cap\,\rho\,\mathrm{big}}}\operatorname{Tr}\Lambda(\theta_{\rho,\varphi}) + o(1)\cdot O(\dim(\Lambda))\\ &\overset{(10.0.5)}{=} \int_{U_R(\mathbb{C})}\operatorname{Tr}\Lambda(\theta)\,d\theta + o(1)\end{aligned}$$

as $q\to\infty$. Therefore $\Theta_{\rho,q}$ becomes equidistributed in $U_R(\mathbb{C})$ as claimed.

11. Exhibiting Big Monodromy

In this section we present sufficient criteria for the Mellin transform of ρ to have big monodromy and refer the interested reader to §12 for explicit examples of representations meeting these criteria. Before stating the main theorem, we make some hypotheses and introduce pertinent terminology.

Throughout this section, we suppose that $\gcd(s,c) = t-a$, for some $a\in\mathbb{F}_q$. One could easily argue that this is less general than supposing that s, c are relatively prime, however, we do not presently have a way to avoid our hypothesis. For ease of exposition, we also suppose that $a=0$ and observe that, up to performing an additive translation $t\mapsto t+a$, this represents no additional loss of generality.

For $t = 0, \infty$, we regard V_φ as an $I(t)$-module and then denote it $V_\varphi(t)$. We write $V_\varphi(t)^{\mathrm{unip}}$ for the maximal subspace of $V_\varphi(t)$ on which $I(t)$ acts unipotently. It is a direct summand of $V_\varphi(t)$, and each simple e-dimensional submodule of it is isomorphic to a common module $\mathrm{Unip}(e)$. We say $V_\varphi(t)$ has a *unique unipotent block of exact multiplicity one* iff, for a unique integer $e \geq 1$, some $I(t)$-submodule is isomorphic $\mathrm{Unip}(e)$ but no submodule is isomorphic to $\mathrm{Unip}(e) \oplus \mathrm{Unip}(e)$.

Theorem 11.0.1. *Suppose that* $\gcd(s, c) = t$ *and that* $\deg(c) \geq 3$. *Suppose moreover that* $V(0)$ *has a unique unipotent block of exact multiplicity one and that* ρ *is geometrically simple and pointwise pure. If* $r := \dim(V)$ *and* $\deg(c)$ *satisfy*

$$\deg(c) > \frac{1}{r}\left(72(r^2+1)^2 - r - \deg(L(T,\rho)) + \mathrm{drop}_{\mathcal{C}}(\rho)\right),$$

then the Mellin transform of ρ *has big monodromy.*

We prove the theorem in §11.11.

Remark 11.0.2. As the reader will notice, the proof of our theorem has a lot in common with tatz's proof of [Kat12, Th. 17.1]. We both need the hypothesis on $\gcd(c, s)$ and the structure of $V(0)^{\mathrm{unip}}$ in order to exhibit special elements of the relevant arithmetic monodromy groups. More precisely, the hypothesis that $\gcd(c, s) = t$ helps ensure that, for sufficiently many φ, some induced representation $\mathrm{Ind}(V_\varphi)$ has the property that $\mathrm{Ind}(V_\varphi)(0)^{\mathrm{unip}} = V(0)^{\mathrm{unip}}$ (cf. Lemma 11.10.1). The hypothesis on the structure of these coincident modules then leads to the desired element (cf. Lemma 11.7.4). We expect one can remove this hypothesis but do not know how to do so.

Remark 11.0.3. The hypothesis $\gcd(c, s) = t$ also plays a minor role in Proposition 11.9.1. However, one could easily make other hypotheses (e.g., $\gcd(c, s) = 1$) and still be able to proceed (cf. [Kat13, Th. 5.1]).

11.1. **Two norm maps.** This subsection recalls material from [Kat12, §2] and borrows heavily from *loc. cit.*

Let B be the finite $\mathbb{F}_q$-algebra $\mathbb{F}_q[t]/c\mathbb{F}_q[t]$. It is a direct product of finite extensions of $\mathbb{F}_q$ and hence étale since c is square free. More generally, for each finite extension $E/\mathbb{F}_q$, the $\mathbb{F}_q$-algebra

$$B_E = B \otimes_{\mathbb{F}_q} E$$

is étale and has the structure of a free B-module of rank $d = [E : \mathbb{F}_q]$.

Let $\mathbb{B}$ be the functor from the category of $\mathbb{F}_q$-algebras to itself defined for an $\mathbb{F}_q$-algebra R by

$$\mathbb{B}(R) = R[t]/cR[t].$$

It is the functor $R \mapsto B_R = B \otimes_{\mathbb{F}_q} R$. In fact, $\mathbb{B}(R)$ even has the structure of an étale R-algebra which is free of rank $\deg(c)$. In particular, for each $\mathbb{F}_q$-algebra R, there is a norm map $\mathbb{B}(R) \to R$ which is part of a transformation

$$\mathrm{Norm}_{B/\mathbb{F}_q} \colon \mathbb{B} \to \mathrm{id}_{\mathbb{F}_q-\mathrm{algebras}}$$

between $\mathbb{B}$ and the identity functor on the category of $\mathbb{F}_q$-algebras.

Let $\mathbb{B}^\times$ be the functor from the category of $\mathbb{F}_q$-algebras to the category of groups defined by

$$\mathbb{B}^\times(R) = (R[t]/cR[t])^\times.$$

It is the composition of $\mathbb{B}$ with the functor $A \mapsto A^\times$ of $\mathbb{F}_q$-algebras. Moreover, the restriction of the norm map $\mathbb{B}(R) \to R$ to the group of units yields a homomorphism

$$\nu_R \colon \mathbb{B}^\times(R) \to R^\times,$$

and in particular, $\nu_{\mathbb{F}_q}$ is the map ν of §10.2.

For each finite extension $E/\mathbb{F}_q$, let $\mathbb{B}_E$, $\mathbb{B}_E^\times$ be the functors on variable $\mathbb{F}_q$-algebras R defined by

$$\mathbb{B}_E(R) = B_E \otimes_{\mathbb{F}_q} R, \quad \mathbb{B}_E^\times(R) = (B_E \otimes_{\mathbb{F}_q} R)^\times$$

respectively.

On one hand, $\mathbb{B}_E$ takes values in the category of $\mathbb{F}_q$-algebras. However, $\mathbb{B}_E(R)$ also has the structure of an étale B_R-algebra which is free of rank d as a B_R-module since

$$B_E \otimes_{\mathbb{F}_q} R = B \otimes_{\mathbb{F}_q} E \otimes_{\mathbb{F}_q} R = B_R \otimes_{\mathbb{F}_q} E$$

and since B_E is an étale B-algebra which is free of rank d as a B-module. In particular, there is a transformation

$$\mathrm{Norm}_{E/\mathbb{F}_q} \colon \mathbb{B}_E \to \mathbb{B}$$

between the functors $\mathbb{B}_E$ and $\mathbb{B}$.

On the other hand, $\mathbb{B}_E^\times$ takes values in the category of groups and is even a smooth commutative group scheme. More precisely, $\mathbb{B}^\times$ is a group scheme over $\mathbb{F}_q$ of multiplicative type (i.e., a torus), and $\mathbb{B}_E^\times$ is the torus $\mathrm{Res}_{E/\mathbb{F}_q}(\mathbb{B}^\times)$ over $\mathbb{F}_q$ given by extending scalars to E and then taking the Weil restriction of scalars of $\mathbb{B}^\times$ back down to $\mathbb{F}_q$ (cf. [BLR90, §7.6]). Moreover, the transformation $\mathrm{Norm}_{E/\mathbb{F}_q}$ induces a transformation

$$\mathrm{Norm}_{E/\mathbb{F}_q} \colon \mathbb{B}_E^\times \to \mathbb{B}^\times$$

which is even an étale surjective homomorphism of tori. In particular, since

$$\mathbb{B}_E^\times(\mathbb{F}_q) = \mathbb{B}^\times(E) = (E[t]/cE[t])^\times$$

one obtains a second norm map

$$\nu_E' \colon (E[t]/cE[t])^\times \to (\mathbb{F}_q[t]/c\mathbb{F}_q[t])^\times$$

which is a surjective homomorphism by Lang's theorem.

11.2. **Characters of a twisted torus.** Let $E/\mathbb{F}_q$ be a finite extension and $\Phi_E(c)$ be the dual group $\mathrm{Hom}(\mathbb{B}^\times(E), \bar{\mathbb{Q}}_\ell^\times)$ so that $\Phi_{\mathbb{F}_q}(c) = \Phi(c)$. Suppose that c splits completely over E, and let $a_1, \ldots, a_n \in E$ be the zeros of c so that $c = \prod_{i=1}^n (t - a_i)$ in $E[t]$.

For each E-algebra R, the Chinese Remainder Theorem implies that there is a unique algebra isomorphism

$$R[t]/cR[t] \to \prod_{i=1}^n R[t]/(t-a_i)R[t] \tag{11.2.1}$$

which sends the residue class of t to the tuple $(a_1, \ldots, a_n)$ of residue class representatives. Writing it as an isomorphism $\mathbb{B}(R) \to R^n$ and restricting to units yields a group isomorphism $\mathbb{B}^\times(R) \to (R^\times)^n$. As R varies over E-algebras, the latter isomorphisms in turn yield an isomorphism of tori $\sigma \colon \mathbb{B}^\times \to \mathbb{G}_m^n$ over E. In particular, applying Weil restriction of scalars from E to $\mathbb{F}_q$ yields an isomorphism

$$\mathrm{Res}_{E/\mathbb{F}_q}(\sigma) \colon \mathbb{B}_E^\times \to \mathbb{G}_{m,E}^n$$

of tori over $\mathbb{F}_q$ where $\mathbb{G}_{m,E} = \mathrm{Res}_{E/\mathbb{F}_q}(\mathbb{G}_m)$.

There is a unique permutation $\phi \in \mathrm{Sym}([n])$ where $[n] = \{1, 2, \ldots, n\}$ satisfying $a_{\phi^{-1}(i)} = a_i^q$ since c is square free and has coefficients in $\mathbb{F}_q$. While σ does not descend to a morphism $\mathbb{B}^\times \to \mathbb{G}_m^n$ in general, we can use ϕ to construct a twisted form $\mathbb{T}$ of $\mathbb{G}_m^n$ over $\mathbb{F}_q$ such that σ is the pullback of a morphism $\mathbb{B}^\times \to \mathbb{T}$ over $\mathbb{F}_q$. More precisely, we define the twisted Frobenius τ on $\mathbb{T} = \mathbb{G}_m^n$ as the composition

$$(b_1, \ldots, b_n) \mapsto (b_1^q, \ldots, b_n^q) \mapsto (b_{\phi(1)}^q, \ldots, b_{\phi(n)}^q)$$

of the usual Frobenius automorphism and a permutation of the coordinates of $\mathbb{G}_m^n$. One can easily verify that τ^d is the dth power of the usual Frobenius and thus $\mathbb{T}$ is indeed a twist of $\mathbb{G}_m^n$ (cf. [Car85, Sec. 1.17 and Ch. 3] or [PR94, §2.1.7]). Moreover, one can also show that $(a_1, \dots, a_n)$ is fixed by τ and even that

$$\mathbb{T}(\mathbb{F}_q) = \mathbb{T}^{\tau=1} = \mathbb{B}^\times(\mathbb{F}_q).$$

In particular, by precomposing with τ we obtain the automorphism $\tau_E^\vee$ on

$$\operatorname{Hom}(\mathbb{T}(E), \bar{\mathbb{Q}}_\ell^\times) = \operatorname{Hom}(\mathbb{G}_m^n(E), \bar{\mathbb{Q}}_\ell^\times) = \operatorname{Hom}(E^\times, \bar{\mathbb{Q}}_\ell^\times)^n$$

given by

$$\tau_E^\vee \colon (\varphi_1, \dots, \varphi_n) \mapsto (\varphi_{\phi^{-1}(1)}^q, \dots, \varphi_{\phi^{-1}(n)}^q). \tag{11.2.2}$$

Composition of $\operatorname{Res}_{E/\mathbb{F}_q}(\sigma)$ with the projection $\mathbb{G}_{m,E}^n \to \mathbb{G}_{m,E}$ onto the ith factor yields a surjective homomorphism

$$\pi_i \colon \mathbb{B}_E^\times \to \mathbb{G}_{m,E}$$

of tori over $\mathbb{F}_q$. In particular, taking duals of the respective groups of E-rational points and using the bijections $\mathbb{G}_{m,E}(\mathbb{F}_q) = \mathbb{G}_m(E) = E^\times$ yields an isomorphism

$$\sigma_E^\vee \colon \prod_{i=1}^n \operatorname{Hom}(E^\times, \bar{\mathbb{Q}}_\ell^\times) \ni (\varphi_1, \dots, \varphi_n) \mapsto \prod_{i=1}^n \varphi_i \pi_i \in \Phi_E(c).$$

We observe that since ν_E' is surjective its dual $\nu_E'^\vee$ is a monomorphism $\Phi(c) \to \Phi_E(c)$ and thus we can identify $\Phi(c)$ with a subset of $\operatorname{Hom}(E^\times, \bar{\mathbb{Q}}_\ell^\times)^n$. More precisely, it is the subgroup of characters fixed by $\tau_E^\vee$ and thus

$$(\sigma_E^\vee)^{-1}(\nu_E'^\vee(\Phi(c))) = \{\, (\varphi_1, \dots, \varphi_n) \in \operatorname{Hom}(E^\times, \bar{\mathbb{Q}}_\ell^\times)^n : \varphi_{\phi(i)} = \varphi_i^q \text{ for } i \in [n] \,\}. \tag{11.2.3}$$

11.3. **Characters with distinct components.** We say that a character $\varphi \in \Phi_E(c)$ *has distinct components* iff it lies in the subset

$$\Phi_E(c)_{\text{distinct}} = \left\{ \sigma_E^\vee(\varphi_1, \dots, \varphi_n) \in \Phi_E(c) : \varphi_i \neq \varphi_j \text{ for } 1 \le i < j \le n \right\},$$

and we define the corresponding subset of $\Phi(c)$ as the intersection

$$\Phi(c)_{\text{distinct}} = \Phi_E(c)_{\text{distinct}} \cap \nu_E'^\vee(\Phi(c))$$

where $\nu_E'^\vee \colon \Phi(c) \to \Phi_E(c)$ is the dual of ν_E'.

Lemma 11.3.1. *$\Phi(c)_{\text{distinct}}$ is well defined, that is, it does not depend upon our choice of E.*

Proof. Let E'/E be a finite extension and observe that the norm map $E'^\times \to E^\times$ is surjective so induces a monomorphism

$$\operatorname{Hom}(E^\times, \bar{\mathbb{Q}}_\ell^\times) \to \operatorname{Hom}(E'^\times, \bar{\mathbb{Q}}_\ell^\times),$$

and thus

$$\Phi_E(c)_{\text{distinct}} = \Phi_{E'}(c)_{\text{distinct}} \cap \Phi_E(c).$$

In particular, if $E''/\mathbb{F}_q$ is a second finite extension over which c splits completely and if E' contains the compositum EE'', then

$$\Phi_E(c)_{\text{distinct}} \cap \nu_E'^\vee(\Phi(c)) = \Phi_{E'}(c)_{\text{distinct}} \cap \nu_{E'}'^\vee(\Phi(c)) = \Phi_{E''}(c)_{\text{distinct}} \cap \nu_{E''}'^\vee(\Phi(c))$$

and $\Phi(c)_{\text{distinct}}$ is indeed well defined. $\square$

Let $c = \prod_{j=1}^r \pi_i \in \mathbb{F}_q[t]$ be a factorization into monic irreducibles. The quotient $E_j = \mathbb{F}_q[t]/\pi_j\mathbb{F}_q[t]$ is a finite extension of $\mathbb{F}_q$ of degree $n_j = \deg(\pi_j)$. It is also the splitting field of π_j and thus may be embedded in E. Moreover, there are bijections

$$\Phi(c) = \prod_{j=1}^r \Phi(\pi_j) = \prod_{j=1}^r \mathrm{Hom}(E_j^\times, \bar{\mathbb{Q}}_\ell^\times), \quad \Phi_E(c) = \prod_{j=1}^r \Phi_E(\pi_j) = \prod_{j=1}^r \mathrm{Hom}(E^\times, \bar{\mathbb{Q}}_\ell^\times)^{n_j} \tag{11.3.2}$$

given by applying the Chinese Remainder Theorem.

For each monic factor c_0 of c in $\mathbb{F}_q[t]$, let $\Phi(c_0)_{\mathrm{distinct}}$ be the subset of $\Phi(c_0)$ defined similarly as above but with c_0 in lieu of c. One can easily verify that it does not depend upon the polynomial c of which c_0 is a factor.

Lemma 11.3.3. $|\Phi(\pi_j)_{\mathrm{distinct}}| \sim |\Phi(\pi_j)|$, *for each* $j \in [r]$, *as* $q \to \infty$.

Proof. Let $j \in [r]$, and suppose without loss of generality that $a_1, \dots, a_{n_j}$ are the zeros of π_j and $\phi(i) \equiv i + 1 \bmod n_j$ for $i \in [n_j]$. Then by (11.2.3) and (11.3.2) there is an identification

$$\Phi(\pi_j) \quad = \quad \{\, (\varphi_1, \dots, \varphi_{n_j}) \in \mathrm{Hom}(E_j^\times, \bar{\mathbb{Q}}_\ell^\times)^{n_j} : \varphi_{i+1} = \varphi_i^q \text{ for } i \in [n_j - 1] \,\}.$$

since any $\varphi \in \mathrm{Hom}(E^\times, \bar{\mathbb{Q}}_\ell^\times)$ factors through an inclusion $E_j^\times \to E^\times$ if $\varphi^{q^{n_j}} = \varphi$.

The groups $E_j^\times$ and $\mathrm{Hom}(E_j^\times, \bar{\mathbb{Q}}_\ell^\times)$ are cyclic and non-canonically isomorphic, so let g and χ be respective generators. Then we have a further identifications

$$\begin{aligned} \Phi(\pi_j) \quad &= \quad \{\, (\chi^{e_1}, \dots, \chi^{e_{n_j}}) \in \mathrm{Hom}(E_j^\times, \bar{\mathbb{Q}}_\ell^\times)^{n_j} : e_{i+1} \equiv q e_i \bmod q^{n_j} - 1 \text{ for } i \in [n_j - 1] \,\} \\ &= \quad \{\, (g^{e_1}, \dots, g^{e_{n_j}}) \in (E_j^\times)^{n_j} : e_{i+1} \equiv q e_i \bmod q^{n_j} - 1 \text{ for } i \in [n_j - 1] \,\}. \end{aligned}$$

From this last identification one easily deduces an identification between $\Phi(\pi_j)_{\mathrm{distinct}}$ and the set

$$\{\, (g^{e_1}, \dots, g^{e_{n_j}}) \in (E_j^\times)^{n_j} : e_{i+1} \equiv q e_i \bmod q^{n_j} - 1 \text{ for } i \in [n_j - 1] \text{ and } \mathbb{F}_q(g^{e_1}) = E_j \,\},$$

and thus

$$|\Phi(\pi_j)_{\mathrm{distinct}}| = |\{\, g^e \in E_j^\times : e \in [q^{n_j} - 1] \text{ and } E_j = \mathbb{F}_q(g^e) \,\}|.$$

Finally, it is well known that the cardinality of the righthand set is asymptotic to $q^{n_j} - 1$ as $q \to \infty$ (cf. [Ros02, 2.2]), and thus

$$|\Phi(\pi_j)| = |\mathrm{Hom}(E_j^\times, \bar{\mathbb{Q}}_\ell^\times)| = |E_j^\times| = q^{n_j} - 1 \sim |\Phi(\pi_j)_{\mathrm{distinct}}| \text{ for } q \to \infty$$

as claimed. □

Corollary 11.3.4. *If* c_0 *is a monic factor of* c *in* $\mathbb{F}_q[t]$, *then* $|\Phi(c_0)_{\mathrm{distinct}}| \sim |\Phi(c_0)|$ *as* $q \to \infty$.

Proof. Suppose without loss of generality that $c = \pi_1 \cdots \pi_s$ with $s \in [r]$ so that there is a bijection

$$\Phi(c_0) = \prod_{j=1}^s \Phi(\pi_j).$$

This bijection in turn induces an inclusion

$$\Phi(c_0)_{\mathrm{distinct}} \to \prod_{j=1}^s \Phi(\pi_j)_{\mathrm{distinct}}$$

whose coimage is bounded above by $\prod_{j=1}^s (\deg(c_0) - n_j)$ since an element of the codomain lies in the image if (and only if) the components are pairwise distinct. In particular,

$$|\Phi(c_0)_{\mathrm{distinct}}| \sim \prod_{j=1}^s |\Phi(\pi_j)_{\mathrm{distinct}}| \overset{\text{Lemma 11.3.3}}{\sim} \prod_{j=1}^s |\Phi(\pi_j)| \text{ for } q \to \infty$$

as claimed. □

11.4. **Properties of H_c^2.** Let X be a smooth geometrically connected curve over $\mathbb{F}_q$, let $T \subseteq X$ be a dense Zariski open subset, and let $\mathcal{F}$ be a sheaf on X.

Lemma 11.4.1. *There is an isomorphism $H_c^2(\bar{T}, \mathcal{F}) \to H_c^2(\bar{X}, \mathcal{F})$.*

Proof. See [Del77, §6, Remarques 1.18 (d)] and also [Del80, §1.4, (1.4.1b)]. □

Let $\mathcal{G}$ be a sheaf on X and $\mathcal{G}^\vee$ be its dual. Suppose $\mathcal{F}$ and $\mathcal{G}$ are lisse on T, and thus so is $\mathcal{G}^\vee$. Let $\rho\colon \pi_1(T) \to \mathrm{GL}(V)$, $\omega\colon \pi_1(T) \to \mathrm{GL}(W)$, and $\omega^\vee\colon \pi_1(T) \to \mathrm{GL}(W^\vee)$ be the respective corresponding representations.

Lemma 11.4.2. *Suppose $\mathcal{F}$ and $\mathcal{G}$ are lisse and geometrically simple on T.*

(i) $\dim(H_c^2(\bar{T}, \mathcal{F} \otimes \mathcal{G}^\vee)) = \dim(\mathrm{Hom}_{\pi_1(\bar{T})}(W, V)) \leq 1$.

(ii) $\dim(H_c^2(\bar{T}, \mathcal{F} \otimes \mathcal{G}^\vee)) = 1$ *if and only if $\mathcal{F}$ and $\mathcal{G}$ are geometrically isomorphic on T.*

Proof. Use [Del77, §6, Remarques 1.18 (d)] and Schur's lemma [CR06, 27.3]. Compare [Kat96, §7.0]. □

11.5. **Invariant scalars.** Let $\lambda \in \bar{\mathbb{F}}_q^\times$. If we identify $\mathbb{G}_m$ with $\mathbb{P}_u^1 \smallsetminus \{0, \infty\}$ and regard λ as an element of $\mathbb{G}_m(\bar{\mathbb{F}}_q)$, then multiplication by it (i.e., translation) induces an automorphism of $\mathbb{P}_u^1$ over $\bar{\mathbb{F}}_q$ which we also denote $\lambda\colon \mathbb{P}_u^1 \to \mathbb{P}_u^1$. We say λ is an *invariant scalar* of $\mathcal{G}$ iff the direct image $\lambda_*\mathcal{G}$ is geometrically isomorphic to $\mathcal{G}$. For example, 1 is an invariant scalar for every $\mathcal{G}$, and every λ is an invariant scalar of the constant sheaf $\bar{\mathbb{Q}}_\ell$.

Let $\alpha\colon \pi_1(\mathbb{G}_m) \to \bar{\mathbb{Q}}_\ell^\times$ be a tame character. The corresponding sheaf $\mathcal{L}_\alpha = \mathrm{ME}(\alpha)$ is a so-called Kummer sheaf.

Lemma 11.5.1. *Every $\lambda \in \bar{\mathbb{F}}_q^\times$ is an invariant scalar of $\mathcal{L}_\alpha$.*

Proof. The tame fundamental group of $\mathbb{G}_m$ is a quotient and completely generated by the images of the inertia groups $I(0)$ and $I(\infty)$. The character α is completely determined by these images, and translation by λ does not change how $I(0)$ and $I(\infty)$ act since it fixes both 0 and ∞. Therefore $\lambda_*\mathcal{L}_\alpha$ and $\mathcal{L}_\alpha$ are lisse and geometrically isomorphic on $\mathbb{G}_m$, and λ is an invariant scalar of $\mathcal{L}_\alpha$. □

Corollary 11.5.2. *λ is an invariant scalar of $\mathcal{G}$ if and only if it is an invariant scalar of $\mathcal{G} \otimes \mathcal{L}_\alpha$*

In particular, the answer to the question of whether or not λ is an invariant scalar of $c_*\mathrm{ME}(\rho \otimes \varphi)$ depends only on the coset $\varphi\Phi(u)^\nu$.

Proof. The sheaves $\lambda_*\mathcal{L}_\alpha$ and $\mathcal{L}_\alpha$ are lisse and geometrically isomorphic on $\mathbb{G}_m$ by Lemma 11.5.1. Moreover,

$$\lambda_*(\mathcal{G} \otimes \mathcal{L}_\alpha) \otimes (\mathcal{G} \otimes \mathcal{L}_\alpha)^\vee = \lambda_*\mathcal{G} \otimes (\lambda_*\mathcal{L}_\alpha \otimes \mathcal{L}_\alpha^\vee) \otimes \mathcal{G}^\vee,$$

so $\lambda_*\mathcal{G} \otimes \mathcal{G}^\vee$ and $\lambda_*(\mathcal{G} \otimes \mathcal{L}_\alpha) \otimes (\mathcal{G} \otimes \mathcal{L}_\alpha)^\vee$ are lisse and geometrically isomorphic on $\mathbb{P}_u^1 \smallsetminus \{0, \infty\}$. Thus λ is an invariant scalar of $\mathcal{G}$ if and only if it is an invariant scalar of $\mathcal{G} \otimes \mathcal{L}_\alpha$. □

The following lemma gives a cohomological criterion for detecting invariant scalars.

Lemma 11.5.3. *Let $\lambda \in \bar{\mathbb{F}}_q^\times$. Suppose $\lambda_*\mathcal{G}$ and $\mathcal{G}$ are lisse and geometrically simple on U. Then the following are equivalent:*

(i) λ *is an invariant scalar of* $\mathcal{G}$;

(ii) $H_c^2(\bar{U}, \lambda_*\mathcal{G} \otimes \mathcal{G}^\vee) \neq 0$;

(iii) $H^2(\bar{\mathbb{P}}_u^1, \lambda_*\mathcal{G} \otimes \mathcal{G}^\vee) \neq 0$.

Proof. Lemma 11.4.2 implies the equivalence of (1) and (2), and Lemma 11.4.1 implies the equivalence of (2) and (3). □

11.6. **Avoiding invariant scalars.** Consider the affine plane curve

$$X_\lambda : \lambda c(x_1) = c(x_2),$$

and let $\pi_i \colon X_\lambda \to \mathbb{A}^1_t$ be the map $(x_1, x_2) \mapsto x_i$. They are part of a commutative diagram

$$\begin{tikzcd} X_\lambda \arrow[r, "\pi_2"] \arrow[d, "\pi_1"'] \arrow[dr, dotted, "\pi"] & \mathbb{A}^1_t \arrow[d, "c"] \\ \mathbb{A}^1_t \arrow[r, "\lambda c"'] & \mathbb{A}^1_u \end{tikzcd}$$

where $\pi = c\pi_2 = \lambda c\pi_1$. Moreover, the maps c and λc are generically étale of degree $n = \deg(c)$, thus their fiber product π is generically étale of degree n^2. Let $g \colon X_\lambda \to \mathbb{A}^1_t \times \mathbb{A}^1_t$ be the product map (π_1, π_2).

Let $E/\mathbb{F}_q$ be a finite extension over which c splits and $Z = \{a_1, \dots, a_n\} \subseteq E$ be the zeros of c.

Lemma 11.6.1. *X_λ is smooth over the n^2 points of $Z \times_{\mathbb{A}^1_u} Z = Z \times Z$.*

Proof. The subset $Z \subset \mathbb{A}^1_t$ is the vanishing locus of c and λc, hence $Z \times_{\mathbb{A}^1_u} Z = Z \times Z$. Moreover,

$$\frac{\partial}{\partial x_2}(\lambda c(x_1) - c(x_2)) = c'(x_2) = \sum_{i=1}^{n} \prod_{j \neq i} (x - a_j)$$

does not vanish at any $a_i \in Z$ since c is square free, so X_λ is smooth at every $(a_i, a_j) \in Z \times Z$. $\square$

Consider the external tensor product sheaf

$$\mathcal{E}_{\rho\otimes\varphi,\lambda} := \mathrm{ME}(\rho \otimes \varphi) \boxtimes \mathrm{ME}(\rho \otimes \varphi)^\vee = \pi_1^* \mathrm{ME}(\rho \otimes \varphi) \otimes \pi_2^* \mathrm{ME}(\rho \otimes \varphi)^\vee$$

on $\mathbb{A}^1_t \times \mathbb{A}^1_t$ and the tensor product sheaf

$$\mathcal{T}_{\rho\otimes\varphi,\lambda} := \lambda c_* \mathrm{ME}(\rho \otimes \varphi) \otimes c_* \mathrm{ME}(\rho \otimes \varphi)^\vee$$

on $\mathbb{P}^1_u$. They have respective generic ranks r^2 and $(nr)^2$ since both $\mathrm{ME}(\rho \otimes \varphi)$ and its dual have generic rank r and since c has degree n.

Let $T_\lambda \subseteq X_\lambda$ be a smooth dense Zariski open subset and $U_\lambda = \pi(T_\lambda)$. Up to shrinking T_λ, we suppose that $\mathcal{E}_{\rho\otimes\varphi,\lambda}$ is lisse on T_λ and that π is étale over U_λ.

Lemma 11.6.2. *The sheaves $\pi_* g^*(\mathcal{E}_{\rho\otimes\varphi,\lambda})$ and $\mathcal{T}_{\rho\otimes\varphi,\lambda}$ are lisse and isomorphic on U_λ.*

Proof. Consider the commutative diagram

$$\begin{tikzcd} T_\lambda \arrow[r, "g"] \arrow[d, "\pi"'] & \pi_1(T_\lambda) \times \pi_2(T_\lambda) \arrow[r, "i"] \arrow[d, "h"] & \mathbb{A}^1_t \times \mathbb{A}^1_t \arrow[d, "(\lambda c, c)"] \\ U_\lambda \arrow[r, "\Delta"'] & U_\lambda \times U_\lambda \arrow[r, "j"'] & \mathbb{A}^1_u \times \mathbb{A}^1_u \end{tikzcd}$$

where i and j are the canonical inclusions, h is induced by $(\lambda c, c)$, and Δ is the diagonal map. On one hand, h is étale, so $h_* i^*(\mathcal{E}_{\rho\otimes\varphi,\lambda})$ is lisse on $U_\lambda \times U_\lambda$ and therefore $\Delta^* h_* i^*(\mathcal{E}_{\rho\otimes\varphi,\lambda})$ is lisse on U_λ. On the other hand, there are canonical isomorphisms

$$\pi_* g^*(\mathcal{E}_{\rho\otimes\varphi,\lambda}) \simeq \pi_*(\pi_1, \pi_2)^* i^*(\mathcal{E}_{\rho\otimes\varphi,\lambda}) \simeq \Delta^* h_* i^*(\mathcal{E}_{\rho\otimes\varphi,\lambda}) \simeq \Delta^* j^* (\lambda c, c)_*(\mathcal{E}_{\rho\otimes\varphi,\lambda}) \simeq \Delta^* j^* \mathcal{T}_{\rho\otimes\varphi,\lambda}$$

on U_λ. $\square$

The contrapositive of the following corollary gives us a way to show some λ is *not* an invariant scalar.

Corollary 11.6.3. *Suppose ρ is geometrically simple and $\varphi \in \Phi(c)$. Then the following are equivalent:*

(i) λ is an invariant scalar of $c_*\mathrm{ME}(\rho \otimes \varphi)$;

(ii) $H^2_c(\bar{U}_\lambda, \mathcal{T}_{\rho\otimes\varphi,\lambda}) \neq 0$.

They imply

(iii) $H^2_c(\bar{T}_\lambda, \mathcal{E}_{\rho\otimes\varphi,\lambda}) \neq 0$.

Proof. Lemmas 11.5.3 and 11.6.2 imply the equivalence of (1) and (2). If $\pi_1(U_\lambda) \to \mathrm{GL}(V)$ is the representation corresponding to $\mathcal{T}_\lambda$, then $V^{\pi_1(U_\lambda)} \subseteq V^{\pi_1(T_\lambda)}$ so (2.0.2) and (2) imply (3). □

The following proposition was inspired by [Kat02, Proof of Th. 5.1.3].

Proposition 11.6.4. *Suppose* $\deg(c) \geq 2 + \deg(\gcd(c, s))$ *and* $\varphi \in \Phi(c)_{\mathrm{distinct}}$.

(i) If ρ is geometrically irreducible, then so is $\mathrm{ME}(\rho \otimes \varphi)$.

(ii) $\lambda = 1$ is the only invariant scalar of $c_*\mathrm{ME}(\rho \otimes \varphi)$.

Proof. Let $E/\mathbb{F}_q$ be a splitting field of c and $a_1, a_2 \in E$ be zeros of c which are distinct from each other and the zeros of s. Let $\varphi_1, \varphi_2 \in \mathrm{Hom}(E^\times, \bar{\mathbb{Q}}_\ell^\times)$ be the corresponding components of $(\sigma_E^\vee)^{-1}(\nu_E'^\vee(\varphi))$ as an element of $(\sigma_E^\vee)^{-1}(\Phi_E(c))$ (compare (11.2.3) and (11.3.2)). Then φ_1, φ_2 are distinct characters, so $\alpha = \varphi_1/\varphi_2$ is a non-trivial character.

Let $\lambda \in \bar{\mathbb{F}}_q^\times$ be an arbitrary scalar. If $\lambda \neq 1$, then for each component $T'_\lambda \subseteq T_\lambda$ over $\bar{\mathbb{F}}_q$, there is a smooth point $t' = (t'_1, t'_2) \in T'_\lambda(\bar{\mathbb{F}}_q)$ satisfying $\{t'_1, t'_2\} = \{a_1, a_2\}$. The map π is étale over 0 since c is square free, hence we can use π to identify $I(t')$ with $I(0)$. We can also identify $I(t'_1)$ and $I(t'_2)$ with $I(0)$.

On one hand, the stalk of $\mathrm{ME}(\rho \otimes \varphi)$ at $t = t'_i$ and the stalk at $t = 0$ of $\bar{\mathbb{Q}}_\ell^r \otimes \mathcal{L}_{\varphi_i}$ are isomorphic as $I(0)$-modules since $s(a_i) \neq 0$. Moreover, the stalk of $\mathcal{E}_{\rho\otimes\varphi,\lambda}$ at t' and the stalk at $u = 0$ of $\bar{\mathbb{Q}}_\ell^{r^2} \otimes \mathcal{L}_\varphi$ are isomorphic as $I(0)$-modules. On the other hand, the latter stalks have no $I(0)$-invariants since φ is non-trivial, so a fortiori, the geometric generic stalk of $\mathcal{E}_{\rho\otimes\varphi,\lambda}$ has no $\pi_1(\bar{T}_\lambda)$-invariants. Therefore (2.0.2) implies $H^2_c(\bar{T}_\lambda, \mathcal{E}_{\rho\otimes\varphi,\lambda})$ vanishes for $\lambda \neq 1$, and hence the contrapositive of Corollary 11.6.3 implies $\lambda = 1$ is the only invariant scalar of $c_*\mathrm{ME}(\rho \otimes \varphi)$. □

11.7. **Baby theorem.** In this subsection we prove a simplified version of Theorem 11.0.1.

Let U be a dense Zariski open subset of $\mathbb{G}_m = \mathbb{P}^1_u \smallsetminus \{0, \infty\}$ and $\theta\colon \pi_1(U) \to \mathrm{GL}(W)$ be a continuous representation to a finite-dimensional $\bar{\mathbb{Q}}_\ell$-vector space W. Let $\Phi(u)$ be the dual of $\Gamma(u) = (\mathbb{F}_q[u]/u\mathbb{F}_q[u])^\times$ (cf. §10.2). For $u = 0, \infty$, let $W(u)$ denote W regarded as an $I(u)$-module and $W(u)^{\mathrm{unip}}$ be its maximal submodule where $I(u)$ acts unipotently. If θ is geometrically simple and pointwise pure of weight w and if $\dim(W) > 1$, then we can associate to θ a pair of Tannakian monodromy groups

$$\mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u)) \subseteq \mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u)) \subseteq \mathrm{GL}_{R, \bar{\mathbb{Q}}_\ell}$$

for $R = \chi(\bar{\mathbb{G}}_m, \mathrm{ME}(\theta))$ (see §D.14 and Theorem D.7.1).

Theorem 11.7.1. *Suppose that θ is geometrically simple and pointwise pure of weight w, that* $\dim(W) > 1$ *or that θ does not factor through the composed quotient $\pi_1(U) \twoheadrightarrow \pi_1(\mathbb{G}_m) \twoheadrightarrow \pi_1^t(\mathbb{G}_m)$, and that $\lambda = 1$ is the only invariant scalar of* $\mathrm{ME}(\theta)$. *Suppose moreover that $W(0)^{\mathrm{unip}}$ has dimension at most r and a unique unipotent block of exact multiplicity one and that $R > 72(r^2+1)^2$. Finally, suppose $W(\infty)^{\mathrm{unip}} = 0$. Then $\mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u))$ equals $\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$.*

The proof consists of a few steps and will occupy the remainder of this section.

Let $G = \mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u))$ and $H = \mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u))$.

Lemma 11.7.2. *G and H are reductive and there is an exact sequence*

$$1 \to H \to G \to T \to 1$$

for some torus T over $\bar{\mathbb{Q}}_\ell$.

Proof. Observe that $\mathrm{ME}(\theta)$ is geometrically simple yet is not a Kummer sheaf since otherwise one would have $\dim(W) = 1$ and θ would factor through $\pi_1(U) \twoheadrightarrow \pi_1^{\mathrm{t}}(\mathbb{G}_m)$. Moreover, θ is geometrically simple and pointwise pure of weight w by hypothesis. Therefore the lemma follows from Proposition D.14.1.i. □

A priori G or H could be disconnected, so let G^0 and H^0 be the respective identity components.

Lemma 11.7.3. *G^0 and H^0 are (Lie-)irreducible subgroups of $\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$.*

Proof. This follows from [Kat12, Th. 8.2 and Cor. 8.3] since $\lambda = 1$ is the only invariant scalar of $\mathrm{ME}(\theta)$. □

Let $\mu_m \colon (\bar{\mathbb{Q}}^\times)^m \to \mathbb{Z}^m$ be the mth weight multiplicity map for $m = R$ given in Definition C.1.2.

Lemma 11.7.4. *There exist an element $g \in G^0$ and an eigenvalue tuple $\gamma \in (\bar{\mathbb{Q}}_\ell^\times)^R$ of g satisfying the following:*

(i) $\gamma = (\gamma_1, \dots, \gamma_R)$ lies in $(\bar{\mathbb{Q}}^\times)^R$ and thus $\det(g) = \gamma_1 \cdots \gamma_R$ lies in $\bar{\mathbb{Q}}^\times$;

(ii) $|\iota(\det(g))|^2 = (1/q)^w$ for some $w \neq 0$ and every field embedding $\iota \colon \bar{\mathbb{Q}} \to \mathbb{C}$;

(iii) $c = \mu_R(\gamma)$ satisfies $\mathrm{len}(c) \leq r + 1$ and $1 = c_{\mathrm{len}(c)} < c_{\mathrm{len}(c)-1}$ and $c_2 \leq r$.

Proof. This follows from Proposition D.14.1.ii with $g = f^c$ for any element $f \in \mathrm{Frob}_{\mathbb{F}_q,\mathbf{1}}$ and for $c = [G : G^0]$. More precisely, if $\alpha = (\alpha_1, \dots, \alpha_R)$ is an eigenvalue tuple of f, then all the α_i lie in $\bar{\mathbb{Q}}$, all the non-zero weights $w_1, \dots, w_n$ of the α_i are negative since $W(\infty)^{\mathrm{unip}}$ vanishes, one has $1 \leq n \leq r$ since $1 \leq \dim(W(0)^{\mathrm{unip}}) \leq r$, there is a unique non-zero weight of multiplicity one since $W(0)^{\mathrm{unip}}$ has a unique unipotent block of exact multiplicity one, and the weight zero has multiplicity $R - n \geq R - r > 1$. Hence it suffices to take $\gamma \in (\bar{\mathbb{Q}}^\times)^R$ to be the eigenvalue tuple with $\gamma_i = \alpha_i^c$ for $1 \leq i \leq R$ and w to be $(w_1 + \cdots + w_n)c$. □

Corollary 11.7.5. $\det(H)$ *equals* $\bar{\mathbb{Q}}_\ell^\times$.

Proof. Follows from Lemma 11.7.4.ii and the argument in [Kat12, Proof of Th. 17.1] using the element g in Lemma 11.7.4. □

Let $[G^0, G^0]$ be the derived subgroup of G^0.

Lemma 11.7.6. $[G^0, G^0]$ *equals* $\mathrm{SL}_{R,\bar{\mathbb{Q}}_\ell}$.

Proof. Combine Lemmas 11.7.3 and 11.7.4 to deduce that the hypotheses of Theorem C.4.1 hold, and thus G^0 equals one of $\mathrm{SL}_R(\bar{\mathbb{Q}}_\ell)$ or $\mathrm{GL}_R(\bar{\mathbb{Q}}_\ell)$. The derived subgroup of both of these groups equals $\mathrm{SL}_R(\bar{\mathbb{Q}}_\ell)$. □

We may now complete the proof of the theorem. First, we have inclusions

$$[G^0, G^0] \subseteq [G, G] \subseteq [\mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}, \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}] = \mathrm{SL}_{R,\bar{\mathbb{Q}}_\ell},$$

and Lemma 11.7.6 implies the outer terms are equal, so the inclusions are equalities. Moreover, Lemma 11.7.2 implies H is normal in G and G/H is abelian, so H contains $[G, G] = \mathrm{SL}_{R,\bar{\mathbb{Q}}_\ell}$, and hence, by Corollary 11.7.5, $H = \mathrm{GL}_{R,\bar{\mathbb{Q}}_\ell}$ as claimed.

11.8. **Frobenius reciprocity.** Let $c\colon T \to U$ be a finite étale map of smooth geometrically connected curves over $\mathbb{F}_q$. Let $\mathcal{F}$ (resp. $\mathcal{G}$) be a lisse sheaf on T (resp. U) and $\pi_1(T) \to \mathrm{GL}(V)$ (resp. $\pi_1(U) \to \mathrm{GL}(W)$) be the corresponding representation. Let $\mathcal{F}^\vee$ be the dual of $\mathcal{F}$ and $\pi_1(T) \to \mathrm{GL}(V^\vee)$ be the corresponding representation.

Lemma 11.8.1. *$c_*(\mathcal{F}^\vee)$ is isomorphic to the dual of $c_*\mathcal{F}$.*

Proof. See [Kat02, Lem. 3.1.3]. □

Therefore we may unambiguously write $c_*\mathcal{F}^\vee$.

Proposition 11.8.2. $\dim(H^2_c(\bar{T}, c^*\mathcal{G} \otimes \mathcal{F}^\vee)) = \dim(H^2_c(\bar{U}, \mathcal{G} \otimes c_*\mathcal{F}^\vee))$.

Proof. Let $H = \pi_1(\bar{T})$ and $G = \pi_1(\bar{U})$. We suppose that V (resp. W) is a left H-module (resp. G-module), and define $\mathrm{Ind}_H^G(V)$ to be the (Mackey) induced module $\mathrm{Hom}_G(\bar{\mathbb{Q}}_\ell[H], V)$ and $\mathrm{Res}_H^G(W)$ to be the restricted module W regarded as a left H-module. Then Frobenius reciprocity implies that there is a bijection of vector spaces

$$\mathrm{Hom}_H(\mathrm{Res}_H^G(W), V) \to \mathrm{Hom}_G(W, \mathrm{Ind}_H^G(V))$$

given by $\psi \mapsto (w \mapsto (r \mapsto \psi(rv)))$ (cf. [Kat02, §3.0]). Moreover, Lemma 11.4.2 implies that

$$\dim(H^2_c(\bar{T}, c^*\mathcal{G} \otimes \mathcal{F}^\vee)) = \dim(\mathrm{Hom}_H(\mathrm{Res}_H^G(W), V))$$

and that

$$\dim(H^2_c(\bar{U}, \mathcal{G} \otimes c_*\mathcal{F}^\vee)) = \dim(\mathrm{Hom}_G(W, \mathrm{Ind}_H^G(V))),$$

so the proposition follows immediately. □

11.9. **Begetting simplicity.** In this section we give a criterion for $\mathrm{Ind}(\rho \otimes \varphi)$ to be geometrically simple. Our argument was inspired by [Kat13, Proof of Th. 5.1.1].

Proposition 11.9.1. *Let $\varphi \in \Phi(c)_{\mathrm{distinct}}$. Suppose that $\gcd(c, s) = t$, that $\deg(c) \geq 2$, and that $\varphi(\Gamma(t)) = 1$. If ρ is geometrically simple, then so are $\rho \otimes \varphi$ and $\mathrm{Ind}(\rho \otimes \varphi)$.*

Proof. Let $T \subseteq \mathbb{P}^1_t$ be a dense Zariski open subset and $U = c(T)$. Up to shrinking T, we suppose that $\mathcal{F} = \mathrm{ME}(\rho \otimes \varphi)$ is lisse over T and that c is étale over U.

Suppose that ρ is geometrically simple and thus so is $\rho \otimes \varphi$. Let $\mathcal{G} = c_*\mathcal{F}^\vee$ (cf. Lemma 11.8.1), and observe that Lemma 10.2.1.i implies that $\mathcal{G}$ and $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))^\vee$ are isomorphic over U. We wish to show that $\dim(H^2(\bar{U}, \mathcal{G} \otimes \mathcal{G}^\vee)) = 1$ so that Lemma 11.4.2 implies that $\mathrm{ME}(\mathrm{Ind}(\rho \otimes \varphi))$ is geometrically simple over U, that is, that $\mathrm{Ind}(\rho \otimes \varphi)$ is geometrically simple. In fact, Lemma 11.4.1 and Proposition 11.8.2 imply that

$$\dim(H^2_c(\bar{\mathbb{P}}^1_u, \mathcal{G} \otimes \mathcal{G}^\vee)) = \dim(H^2_c(\bar{U}, c_*\mathcal{F} \otimes c_*\mathcal{F}^\vee)) = \dim(H^2_c(\bar{T}, c^*c_*\mathcal{F} \otimes \mathcal{F}^\vee)),$$

so it suffices to show the last term equals 1.

The functor c^* is left adjoint to the functor c_* since c is finite (cf. [Mil80, II.3.14]), so the identify map $c_*\mathcal{F} \to c_*\mathcal{F}$ induces an adjoint $c^*c_*\mathcal{F} \to c$. Generically it is the trace map $\mathrm{Ind}(V_\varphi) \to V_\varphi$ and thus is surjective (cf. [Mil80, V.1.12]). Let $\mathcal{K}$ be the kernel so that we have an exact sequence of sheaves

$$0 \to \mathcal{K} \to c^*c_*\mathcal{F} \to \mathcal{F} \to 0. \tag{11.9.2}$$

These sheaves and $\mathcal{F}^\vee$ are all lisse over T, so the sequence

$$0 \to \mathcal{K} \otimes \mathcal{F}^\vee \to c^*c_*\mathcal{F} \otimes \mathcal{F}^\vee \to \mathcal{F} \otimes \mathcal{F}^\vee \to 0 \tag{11.9.3}$$

is exact on T. In particular, we have a corresponding exact sequence of cohomology

$$H^2_c(\bar{U}, \mathcal{K} \otimes \mathcal{F}^\vee) \to H^2_c(\bar{T}, c^*c_*\mathcal{F} \otimes \mathcal{F}^\vee) \to H^2_c(\bar{T}, \mathcal{F} \otimes \mathcal{F}^\vee) \to H^3_c(\bar{T}, \mathcal{K} \otimes \mathcal{F}^\vee)$$

the last term of which vanishes. The hypothesis that $\mathcal{F}$ is geometrically simple implies the penultimate term has dimension 1 by Lemma 11.4.2, so it suffices to show that the first term vanishes.

Let $E/\mathbb{F}_q$ be a splitting field of c, let $a_1, \ldots, a_n \in E$ be the zeros of c, and let

$$(\varphi_1, \ldots, \varphi_n) = (\sigma_E^\vee)^{-1}(\nu_E'^\vee(\varphi)) \in \operatorname{Hom}(E^\times, \bar{\mathbb{Q}}_\ell^\times)^n$$

as in (11.2.3). We suppose without loss of generality that $a_1 = 0$ and thus $s(a_2)\cdots s(a_n) \neq 0$ since $\gcd(c, s) = t$.

Let $H = \pi_1(\bar{T})$ and $G = \pi_1(\bar{U})$, and let $H \to \mathrm{GL}(V_\varphi)$ and $G \to \mathrm{GL}(\operatorname{Ind}_H^G(V_\varphi))$ be the representations corresponding to $\mathcal{F}$ and $c_*\mathcal{F}$ respectively. The exact sequences (11.9.2) and (11.9.3) correspond to exact sequences of H-modules

$$0 \to K \to R \to V_\varphi \to 0 \tag{11.9.4}$$

and

$$0 \to K \otimes V_\varphi^\vee \to R \otimes V_\varphi^\vee \to V_\varphi \otimes V_\varphi^\vee \to 0$$

where $R = \operatorname{Res}_H^G(\operatorname{Ind}_H^G(V_\varphi))$. We claim the first term of the latter sequence has no $I(0)$-convariants so a fortiori has no $\pi_1(\bar{T})$-coinvariants, and hence $H^2(\bar{T}, \mathcal{K} \otimes \mathcal{F}^\vee)$ vanishes as claimed.

The translation map $t \mapsto t + a_i$ induces an isomorphism $I(0) \simeq I(a_i)$ for each $i \in [n]$, so we can regard $V_\varphi(a_i)$ as an $I(0)$-module. In fact, we have isomorphisms of $I(0)$-modules

$$R(0) \simeq \bigoplus_{i=1}^n V_\varphi(a_i), \quad K(0) \simeq \bigoplus_{i=2}^n V_\varphi(a_i), \quad (K \otimes V_\varphi^\vee)(0) \simeq \bigoplus_{i=2}^n (\bar{\mathbb{Q}}_\ell^{r-1} \otimes \varphi_i^{-1}).$$

More precisely, the first isomorphism corresponds to the fact that the geometric stalks of $c^*c_*\mathcal{F}$ and $\mathcal{F}$ satisfy $(c^*c_*\mathcal{F})_0 = \oplus_{c(a)=0}\mathcal{F}_a$ since c is étale over $u = 0$ (cf. (10.1.1)); the second isomorphism uses (11.9.4) and the assumption that $a_1 = 0$ to identify $K(0)$ with $R(0)/V_\varphi(0)$; and the last isomorphism uses that $s(a_2)\cdots s(a_n) \neq 0$, that is, $\mathcal{C} \smallsetminus \{a_1\}$ lies in the locus of lisse reduction of $\mathrm{ME}(\rho \otimes \varphi)^\vee$.

The hypothesis that $\Gamma(t)$ is in the kernel of φ implies that $V_\varphi(0) \simeq V(0)$ as $I(0)$-modules. Moreover, $\varphi_2, \ldots, \varphi_n$ are all non-trivial since they are distinct from the trivial character φ_1 by hypothesis, so each of the summands $(\bar{\mathbb{Q}}_\ell^{r-1} \otimes \varphi_i^{-1})$ has *trivial* $I(0)$-coinvariants. Therefore $K \otimes V_\varphi^\vee$ has trivial $\pi_1(\bar{T})$-coinvariants as claimed. ☐

11.10. **Preserving unipotent blocks.** For each monic divisor c_0 of c in $\mathbb{F}_q[t]$, consider the subset

$$\Phi(c_0)_{\rho\,\mathrm{good}} = \{\, \varphi \in \Phi(c_0) : \mathrm{ME}(\rho \otimes \varphi) \text{ is supported on } \mathbb{A}_t^1[1/c_0] \,\}.$$

If ρ is the trivial representation, then it consists of the odd primitive characters of conductor c_0.

For $t = 0, \infty$, let $V_\varphi(t)$ denote V_φ regarded as an $I(t)$-module. Similarly, for $u = 0, \infty$, let $\operatorname{Ind}(V_\varphi)(u)$ denote $\operatorname{Ind}(V_\varphi)$ regarded as an $I(u)$-module, and let $\operatorname{Ind}(V_\varphi)(u)^{\mathrm{unip}}$ be the maximal submodule of $\operatorname{Ind}(V_\varphi)(u)$ where $I(u)$ acts unipotently. We say that $\operatorname{Ind}(V_\varphi)(0)$ (resp. $V_\varphi(0)$) has a *unipotent block of dimension e and exact multiplicity m* iff it has an $I(0)$-submodule isomorphic to $U(e)^{\oplus m}$ but no $I(0)$-submodule isomorphic to $U(e)^{\oplus m+1}$.

Lemma 11.10.1. *Suppose* $\gcd(c, s) = t$, *and let* $c_0 = c/t$ *and* $\varphi \in \Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}$. *Then*

- *(i)* $\operatorname{Ind}(V_\varphi)(0)$ *has a unipotent block of dimension e and exact multiplicity m if and only if $V(0)$ does;*
- *(ii)* $\operatorname{Ind}(V_\varphi)(\infty)^{\mathrm{unip}} = 0$.

Proof. On one hand, $V_\varphi(z)^{\mathrm{unip}} = 0$ for every $z \in \mathcal{C} \smallsetminus \{0\}$ since φ is in $\Phi(c_0)_{\rho\,\mathrm{good}}$ and $\gcd(c_0, s) = 1$. Moreover, $V_\varphi(0)$ and $V(0)$ are isomorphic as $I(0)$-modules since $\varphi(\Gamma(t)) = 1$. Therefore the only unipotent blocks of $\operatorname{Ind}(V_\varphi)(0)$ are those coming from $V_\varphi(0)$, and all such blocks contribute identical blocks to $V_\varphi(0)$ (cf. [Mil80, II.3.1.(e) and II.3.5.(c)]), so (i) holds. On the other hand, every unipotent block of $\mathrm{Ind}(V_\varphi)(\infty)$ contributes to $V_\varphi(\infty)^{\mathrm{unip}}$, and the latter vanishes since φ is good for ρ, so (ii) holds. ☐

11.11. **Proof of Theorem 11.0.1.** Recall that R is given by

$$R := r_{\mathcal{C}}(\rho) = (\deg(c)+1)r + \deg(L(T,\rho)) - \mathrm{drop}_{\mathcal{C}}(\rho) \tag{11.11.1}$$

and it equals $\deg(L_{\mathcal{C}}(T,\rho\otimes\varphi))$ for all $\varphi \in \Phi(c)$ (see Proposition 4.3.1).

Lemma 11.11.2. $R > 72(r^2+1)^2$

Proof. Follows from (11.11.1) and the hypothesis on $\deg(c)$ in the statement of the theorem. ☐

Let $c_0 = c/t$.

Lemma 11.11.3. *Suppose $\varphi \in \Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}$. Then the following hold:*

(i) $\mathrm{Ind}(\rho\otimes\varphi)$ *is geometrically simple;*

(ii) $\dim(\mathrm{Ind}(V_\varphi)(0)^{\mathrm{unip}}) = \dim(V_\varphi(0)^{\mathrm{unip}})$ *and* $\mathrm{Ind}(V_\varphi)(0)$ *has a unique unipotent block of exact multiplicity one;*

(iii) $\mathrm{Ind}(V_\varphi)(\infty)^{\mathrm{unip}} = 0$.

Proof. Part (i) follows from Proposition 11.9.1 since φ is in $\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)$, since ρ is geometrically simple, and since $\deg(c) \geq 2$. Parts (ii) and (iii) follow from Lemma 11.10.1 since φ is also in $\Phi(c_0)_{\rho\,\mathrm{good}}$ and since $V(0)$ has a unique unipotent block of exact multiplicity one. ☐

Corollary 11.11.4. $(\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}) \subseteq \Phi(c)_{\rho\,\mathrm{big}}$.

Proof. Let $\varphi \in \Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}$, and let $\theta = \mathrm{Ind}(\rho\otimes\varphi)$ and $W = \mathrm{Ind}(V_\varphi)$. Then Lemmas 11.11.3 and 10.1.2 imply that $\theta = \mathrm{Ind}(\rho\otimes\varphi)$ is geometrically simple and pointwise pure of weight w since $\varphi \in \Phi(c)_{\mathrm{distinct}}$. Moreover, $\dim(W) = \deg(c)\cdot\dim(V) > 2$ since $\deg(c) \geq 2$, and Proposition 11.6.4 implies that $\lambda = 1$ is the only invariant scalar of $\mathrm{ME}(\theta) \simeq c_*\mathrm{ME}(\rho\otimes\varphi)$ since $\deg(c) \geq 3$ and $\varphi \in \Phi(c)_{\mathrm{distinct}}$. Lemma 11.11.3 also implies that $W(0)$ has a unique unipotent block of exact multiplicity one, that $\dim(W(0)^{\mathrm{unip}}) = \dim(V(0)^{\mathrm{unip}}) \leq \dim(V) = r$, and that $W(\infty)^{\mathrm{unip}} = 0$. Finally, Lemma 11.11.2 implies $R > 72(r^2+1)^2$. Therefore the hypotheses of Theorem 11.7.1 hold, and hence $\varphi \in \Phi(c)_{\rho\,\mathrm{big}}$. ☐

Corollary 11.11.5. $(\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}})\Phi(u)^\nu \subseteq \Phi(c)_{\rho\,\mathrm{big}}$.

Proof. Follows from Corollary 11.11.4 since $\Phi(c)_{\rho\,\mathrm{big}}$ is a union of cosets $\varphi\Phi(u)^\nu$. ☐

Let $\varphi \in \Phi(c)$ and $\varphi\Phi(u)^\nu$ be the corresponding coset.

Lemma 11.11.6. $|\varphi\Phi(u)^\nu \cap \Phi(c_0)| = 1$.

Proof. We must show that there is a unique element $\alpha \in \Phi(u)$ satisfying $\varphi\alpha^\nu(\Gamma(t)) = 1$. Since $\gcd(s,c) = t$, we can speak of the component of φ at $t = 0$: it is the character given by restricting χ to the subgroup $\Gamma(t) \subseteq \Gamma(c)$. There is a unique element of $\Phi(u)^\nu$ with the same component at $t = 0$, call it β^ν. Then $\alpha = 1/\beta$ is the desired character. ☐

We need one more estimate to complete the proof of the theorem.

Lemma 11.11.7. $|\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)_{\rho\,\mathrm{good}}| \sim |\Phi(c_0)_{\mathrm{distinct}}| \sim |\Phi(c_0)|$ *as* $q \to \infty$.

Proof. We observe that there are natural inclusions

$$\left(\Phi(c_0)_{\mathrm{distinct}} \smallsetminus \cup_{\pi|c_0}\Phi(c_0/\pi)\right) \subseteq (\Phi(c)_{\mathrm{distinct}} \cap \Phi(c_0)) \subseteq \Phi(c_0)_{\mathrm{distinct}}$$

since an element of $\Phi(c_0)_{\text{distinct}}$ will fail to lie in $\Phi(c)_{\text{distinct}}$ only if one of its $\deg(c_0)$ components is trivial, that is, if it lies in $\Phi(c_0/\pi)$ for some prime factor $\pi \mid c_0$. Intersecting with $\Phi(c_0)_{\rho\,\text{good}}$ gives further inclusions

$$\big((\Phi(c_0)_{\rho\,\text{good}} \cap \Phi(c_0)_{\text{distinct}}) \smallsetminus \cup_{\pi|c_0}\Phi(c_0/\pi)\big) \subseteq (\Phi(c)_{\text{distinct}} \cap \Phi(c_0)_{\rho\,\text{good}}) \subseteq \Phi(c_0)_{\text{distinct}}.$$

Finally, we know that

$$|\Phi(c_0)_{\rho\,\text{good}}| \overset{(10.3.4)}{\sim} |\Phi(c_0)| \overset{11.3.4}{\sim} |\Phi(c_0)_{\text{distinct}}|, \quad |\cup_{\pi|c_0}\Phi(c_0/\pi)|/|\Phi(c)| \ll 1/q = o(1)$$

and hence

$$\big|(\Phi(c_0)_{\rho\,\text{good}} \cap \Phi(c_0)_{\text{distinct}}) \smallsetminus \cup_{\pi|c_0}\Phi(c_0/\pi)\big| \sim |\Phi(c_0)|$$

as $q \to \infty$. □

Corollary 11.11.8. *$|(\Phi(c)_{\text{distinct}} \cap \Phi(c_0)_{\rho\,\text{good}})\Phi(u)^\nu| \sim |\Phi(c)|$ for $q \to \infty$.*

Proof. Combine Lemma 11.11.6 and Lemma 11.11.7. □

The theorem now follows by observing that

$$|\Phi(c)| \overset{\text{Cor. 11.11.8}}{\sim} |(\Phi(c)_{\text{distinct}} \cap \Phi(c_0)_{\rho\,\text{good}})\Phi(u)^\nu| \overset{\text{Cor. 11.11.5}}{\leq} |\Phi(c)_{\rho\,\text{big}}| \leq |\Phi(c)|$$

and thus

$$|\Phi(c)_{\rho\,\text{big}}| \sim |\Phi(c)|$$

for $q \to \infty$.

$\therefore$ The Mellin transform of ρ has big monodromy as claimed and Theorem 11.0.1 holds.

12. Application to Explicit Abelian Varieties

In this section we apply the theory developed in the previous sections to representations coming from (the Tate modules of) a general class of abelian varieties. More precisely, we give an explicit family of abelian varieties for which we can show the corresponding representations satisfy the hypotheses of Theorem 11.0.1. Our principal application, of which Theorem 1.2.3 is a special case, is Theorem 12.3.1.

Throughout this section we suppose that q is an odd prime power so that we can speak of hyperelliptic curves. One who is interested in even characteristic or in L-functions whose Euler factors have odd degree is encouraged to consider Kloosterman sheaves (e.g., see [Kat88, 7.3.2]).

12.1. **Some hyperelliptic curves and their Jacobians.** Let g be a positive integer. In this section we construct an explicit family of abelian varieties which give rise to Galois representations we can easily show satisfy the hypotheses Theorem 10.0.4. One member of this family is an elliptic curve, the Legendre curve, and it has affine model

$$X_{\text{Leg}} : y^2 = x(x-1)(x-t).$$

It is isomorphic to its own Jacobian, and the general abelian varieties in our family will be Jacobians of curves. More precisely, we fix a monic square free $f \in \mathbb{F}_q[x]$ of degree $2g$ and consider the projective plane curve X/K with affine model

$$X : y^2 = f(x)(x-t). \tag{12.1.1}$$

For technical reasons we will eventually suppose that f has a zero a in $\mathbb{F}_q$, and up to the change of variables $x \mapsto x + a$, we will suppose that $a = 0$. We do not need this hypothesis yet since the discussion in this section does not use it.

The curve X has genus g. If $g > 1$, it is a so-called hyperelliptic curve, and otherwise it is an elliptic curve. Either way its Jacobian J is a g-dimensional principally polarized abelian variety over K. See [CFA+06] for more information about hyperelliptic curves and their Jacobians.

For each finite place $v = \pi$, one can define a reduction $X/\mathbb{F}_\pi$ starting with the reduction of (12.1.1) modulo π.

Lemma 12.1.2. *The monic polynomial $s = f(t) \in \mathbb{F}_q[t]$ satisfies the following:*

(i) if $\pi \nmid s$, then $X/\mathbb{F}_\pi$ is a smooth projective curve of genus g;

(ii) if $\pi \mid s$, then $X/\mathbb{F}_\pi$ is smooth away from a single node and has genus $g - 1$.

Proof. The essential point is that, for any monic polynomial $h(x)$ with coefficients in a field F of characteristic not two, the affine curve $y^2 = h(x)$ is smooth iff h is a square free polynomial. More generally, if $h = h_1 h_2^2$ where $h_1, h_2 \in F[x]$ are square free and relatively prime, then the following hold:

(i) the map $(x, y) \mapsto (x, y/h_2(x))$ induces a birational map from $y^2 = h_1(x)$ to $y^2 = h(x)$;

(ii) the $\deg(h_2)$ points (x, y) satisfying $h_2(x) = y = 0$ are so-called nodes of $y^2 = h(x)$;

(iii) the map in (1) corresponds to blowing up the nodes in (2);

(iv) the curve $y^2 = h_1(x)$ is smooth of genus $\lfloor(\deg(h_1) - 1)/2\rfloor$ since h_1 is square free;

(v) both curves have one (resp. two) points at infinity if $\deg(h)$ is odd (resp. even).

(Compare [Har77, Ex. I.5.6].) The proof of the lemma will consist of showing that we are in this general situation.

Let $t_0 \in \mathbb{F}_\pi$ satisfy $t \equiv t_0 \bmod \pi$, and let $h_0(x) := f(x)(x - t_0) \in \mathbb{F}_\pi[x]$. The polynomial $f(x)$ is square free by hypothesis, so $h_0(x)$ is square free iff $f(t_0) = 0$, or equivalently, $\pi \mid s$. In particular, if $\pi \nmid s$, then h_0 is square free and $y^2 = h_0(x)$ is smooth of genus g. Otherwise, $h_0 = h_1 h_2^2$ where $h_1 = f/(x - t_0)$ and $h_2 = x - t_0$ are coprime (since f is square free), and thus $y^2 = h_0(x)$ is smooth away from the node $(t_0, 0)$ and birational to the curve $y^2 = h_1(x)$ which is smooth of genus $g - 1$. □

Remark 12.1.3. One can also define a reduction $X/\mathbb{F}_\infty$ by writing $t = 1/u$ and clearing denominators, and one eventually finds that $X/\mathbb{F}_\infty$ has genus zero. However, the arguments are subtler and beyond the scope of this article, so we omit them.

For example, X_{Leg} has smooth reduction away from $t = 0, 1, \infty$, over $t = 0, 1$ its reduction is a so-called node, and over $t = \infty$ it is a so-called cusp. Since it is isomorphic to its Jacobian, these are sometimes referred to as good, multiplicative, and additive reduction respectively. However, in general, one needs to construct separately reductions $J/\mathbb{F}_\pi$, for every π, and also a reduction $J/\mathbb{F}_\infty$.

Lemma 12.1.4.

(i) If $\pi \nmid s$, then $J/\mathbb{F}_\pi$ is the Jacobian of $X/\mathbb{F}_\pi$ so is a g-dimensional abelian variety;

(ii) If $\pi \mid s$, then $J/\mathbb{F}_\pi$ is an extension of an abelian variety by a one-dimensional torus.

Proof. Both statements are easy consequences of Lemma 12.1.2. More precisely, if $X/\mathbb{F}_\pi$ is projective and smooth away from n nodes, then $J/\mathbb{F}_\pi$ is an extension of a $(g - n)$-dimensional abelian variety by an n-dimensional torus. See [BLR90, 9.2.8] and keep in mind Lemma 12.1.2. □

Remark 12.1.5. One can also show that $J/\mathbb{F}_\infty$ is a g-dimensional additive linear algebraic group, but demonstrating it directly is harder and requires a finer statement than the claim in Remark 12.1.3.

One can regard the various reductions of J as the special fibers of the (identity component of the) Néron model of J/K over $\mathbb{P}^1_t$. However, for our purposes, Lemma 12.1.4 contains all the information we need about the model. More precisely, we only need to know the respective dimensions g_π, m_π, and a_π of the good, multiplicative, and additive parts of $J/\mathbb{F}_\pi$. Thus

$$(g_\pi, m_\pi, a_\pi) = \begin{cases} (g,0,0) & \text{if } \pi \nmid s \\ (g-1,1,0) & \text{if } \pi \mid s \end{cases} \tag{12.1.6}$$

by Lemma 12.1.4. In §12.2 we will show that

$$(g_\infty, m_\infty, a_\infty) = (0,0,g)$$

as claimed in Remark 12.1.5.

12.2. **Tate modules.** Let ℓ be a prime distinct from the characteristic p of $\mathbb{F}_q$. For each $m \geq 0$, let $J[\ell^m] \subseteq J(\bar{K})$ be the subgroup of ℓ^m-torsion; it is isomorphic to $(\mathbb{Z}/\ell^m)^{2g}$ and hence is a finite Galois module. Multiplication by ℓ induces an epimorphism $J[\ell^{m+1}] \twoheadrightarrow J[\ell^m]$, for each m, and the $\mathbb{Z}_\ell$-Tate module of J is the projective limit

$$T_\ell(J) := \varprojlim J[\ell^m].$$

Concretely one can regard $T_\ell(J)$ as the set

$$\{\, (P_0, P_1, \ldots) : P_m \in J[\ell^m] \text{ and } \ell P_{m+1} = P_m \text{ for } m \geq 0 \,\}.$$

It is even a Galois $\mathbb{Z}_\ell$-module (since the action of G_K and multiplication by ℓ commute), and it is isomorphic to ${\mathbb{Z}_\ell}^{2g}$ as a $\mathbb{Z}_\ell$-module (cf. [ST68, §1]).

Let V be the vector space $T_\ell(J) \otimes_{\mathbb{Z}_\ell} \bar{\mathbb{Q}}_\ell$ and $G_K \to \mathrm{GL}(V)$ be the corresponding Galois representation. For each $v \in \mathcal{P}$, let $V(v)$ denote V as an $I(v)$-module and let $V(v)^{\mathrm{unip}}$ be the maximal submodule where $I(v)$ acts unipotently.

Proposition 12.2.1. *Let $v \in \mathcal{P}$, and let g_z and m_z be the respective dimensions of the abelian and multiplicative part of $J/\mathbb{F}_v$ Then*

$$V(v)^{\mathrm{unip}} \simeq U(1)^{\oplus 2g_v} \oplus U(2)^{\oplus m_v}.$$

Proof. This is a general fact about Tate modules of abelian varieties. See [Gro72, Exp. IX, §2.1]. □

Let $\mathcal{S} = \{\pi \in \mathcal{P} : \pi \mid s\} \cup \{\infty\}$ where $s = f(t)$ as in Lemma 12.1.2. Then by Proposition 12.2.1, the action of G_K on V induces a representation

$$\rho \colon G_{K,\mathcal{S}} \to \mathrm{GL}(V)$$

since

$$\dim(V^{I(v)}) = \dim(V) = 2g \text{ for } v \in \mathcal{P} \smallsetminus \mathcal{S}$$

by (12.1.6).

Lemma 12.2.2. *ρ is geometrically simple and pointwise pure of weight one, and it satisfies*

$$\mathrm{drop}_v(\rho) = \begin{cases} 0 & v \in \mathcal{P} \smallsetminus \mathcal{S} \\ 1 & v \in \mathcal{S} \smallsetminus \{\infty\} \\ 2g & v = \infty \end{cases}, \quad \mathrm{Swan}(\rho) = 0.$$

Proof. The values $\mathrm{drop}_v(\rho)$ for $v \neq \infty$ follow directly from (12.1.6) since

$$\mathrm{drop}_v(\rho) = \dim(V) - \dim(V^{I(v)}) = 2g - 2g_v - m_v$$

by Proposition 12.2.1. For the assertions about geometric simplicity and weight and about $\mathrm{drop}_\infty(\rho)$ and $\mathrm{Swan}(\rho)$ we refer to [KS99, 10.1.9 and 10.1.17] (cf. [Hal08, §5] for a related discussion about $J[\ell]$). □

Corollary 12.2.3. *$L(T, J/K) = 1$, that is, it is a polynomial and* $\deg(L(T, J/K)) = 0$.

Proof. The representation ρ is geometrically simple and $\dim(V) = 2g > 0$, so ρ has trivial geometric invariants. Moreover, it is pointwise pure of weight $w = 1$, so Theorem 7.3.2 implies $L(T, \rho)$ is a polynomial of degree

$$r_\emptyset(\rho) \overset{(3.5.2)}{=} \mathrm{drop}(\rho) + \mathrm{Swan}(\rho) - 2 \cdot \dim(V) \overset{12.2.2}{=} (\deg(f) \cdot 1 + 1 \cdot 2g) + 0 - 2 \cdot 2g = 0$$

as claimed. $\square$

Let $c \in \mathbb{F}_q[t]$ be monic and square free and $\mathcal{C} \subset \mathcal{P}$ be the finite subset consisting of ∞ and $v(\pi)$ for every prime factor π of c (cf. §4).

Lemma 12.2.4. *For every $\varphi \in \Phi(c)$, the representation $\rho \otimes \varphi$ is geometrically simple and pointwise pure of weight one, and φ is not heavy.*

Proof. Lemma 7.1.2 implies that $\rho \otimes \varphi$ is geometrically simple since ρ is. Moreover, it has trivial geometric invariants since $\dim(V) = 2g > 1$, so φ is not heavy. Finally, Lemma 6.2.2 implies that it is pointwise pure of weight $w = 1$ since ρ is. $\square$

Corollary 12.2.5. *If $\varphi \in \Phi(c)$, then $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ is a polynomial and*

$$\deg(L_{\mathcal{C}}(T, \rho \otimes \varphi)) = 2g \cdot \deg(c) - \deg(\gcd(c, s)).$$

Proof. By Lemma 12.2.4 the hypotheses of Theorem 7.3.2 hold, and hence $L_{\mathcal{C}}(T, \rho \otimes \varphi)$ is a polynomial of degree

$$r_{\mathcal{C}}(\rho) \overset{(4.3.2)}{=} \deg(L(T, \rho)) + (\deg(c) + 1) \dim(V) - \mathrm{drop}_{\mathcal{C}}(\rho) = 2g \cdot (\deg(c) + 1) - \mathrm{drop}_{\mathcal{C} \cap \mathcal{S}}(\rho).$$

The corollary follows by observing that

$$\mathrm{drop}_{\mathcal{C} \cap \mathcal{S}}(\rho) = \sum_{v \in \mathcal{C} \cap \mathcal{S}} d_v \cdot \mathrm{drop}_v(\rho) = \deg(\gcd(c, s)) \cdot 1 + \mathrm{drop}_\infty(\rho)$$

and that $\mathrm{drop}_\infty(\rho) = 2g$. $\square$

12.3. **Arithmetic application.** In this section we show how to apply our main theorem to the example given above. Let $\mathcal{M} \subset \mathbb{F}_q[t]$ be the subset of monic polynomials, $\mathcal{I} \subset \mathcal{M}$ and $\mathcal{M}_n \subset \mathcal{M}$ be the subsets of irreducibles and polynomials of degree n respectively, and $\mathcal{I}_d = \mathcal{M}_d \cap \mathcal{I}$. Recall that $K = \mathbb{F}_q(t)$ and that $\pi \mapsto v(\pi)$ induces a bijection $\mathcal{I} \to \mathcal{P} \smallsetminus \{\infty\}$.

The Euler factor at $v = \infty$ of the L-function of J is trivial since $\mathrm{drop}_\infty(\rho) = \dim(V)$, and thus the complete L-function satisfies

$$L(T, J/K) = \prod_{\pi \in \mathcal{I}} L(T^{\deg(\pi)}, J/\mathbb{F}_\pi)^{-1} = \prod_{v \in \mathcal{P}} L(T^{d_v}, \rho_v)^{-1} = L_f(T, \rho).$$

Similarly, for the partial L-function of ρ, we have

$$L_{\mathcal{C}}(T, \rho) = \prod_{v \in \mathcal{P} \smallsetminus \mathcal{C}} L(T^{d_v}, \rho_v)^{-1} = \prod_{\substack{\pi \in \mathcal{I} \\ \pi \nmid c}} L(T^{\deg(\pi)}, J/\mathbb{F}_\pi)^{-1}.$$

For each $\pi \in \mathcal{I}$, the Euler factor $L(T, J/\mathbb{F}_\pi)^{-1}$ is the reciprocal of a polynomial with coefficients in $\mathbb{Z}$ so satisfies

$$T \frac{d}{dT} \log(L(T, J/\mathbb{F}_\pi)) = \sum_{n=1}^{\infty} a_{\pi,n} T^n$$

for integers $a_{\pi,n} \in \mathbb{Z}$.

The complete L-function is also a polynomial with coefficients in $\mathbb{Z}$, and it satisfies

$$T\frac{d}{dT}\log(L(T,J/K)) = T\frac{d}{dT}\log(L_f(T,\rho)) = \sum_{n=1}^{\infty}\left(\sum_{f\in\mathcal{M}_n}\Lambda_\rho(f)\right)T^n$$

where $\Lambda_\rho(f)\colon \mathcal{M}\to\mathbb{Z}$ is the von Mangoldt function of ρ defined in (5.2.1) by

$$\Lambda_\rho(f) = \begin{cases} d\cdot a_{\pi,n} & f=\pi^m \text{ and } \pi\in\mathcal{I}_d \\ 0 & \text{otherwise.}\end{cases}$$

Similarly, the partial L-function of ρ is a polynomial with coefficients in $\mathbb{Z}$ and satisfies

$$T\frac{d}{dT}L_{\mathcal{C}}(T,\rho) = \sum_{n=1}^{\infty}\left(\sum_{\substack{f\in\mathcal{M}_n\\ \gcd(f,c)=1}}\Lambda_\rho(f)\right)T^n.$$

For A in $\Gamma(c)=(\mathbb{F}_q[t]/c\mathbb{F}_q[t])^\times$ and positive integer n, we defined the sum $S_{n,c}(A)$ in (5.3.1) by

$$S_{n,c}(A) = \sum_{\substack{f\in\mathcal{M}_n\\ f\equiv A \bmod c}}\Lambda_\rho(f).$$

We then defined the expected value and variance of this sum as A varies uniformly over $\Gamma(c)$ by

$$\mathbb{E}[S_{n,c}(A)] = \frac{1}{\phi(c)}\sum_{A\in\Gamma(c)}S_{n,c}(A),\ \operatorname{Var}[S_{n,c}(A)] = \frac{1}{\phi(c)}\sum_{A\in\Gamma(c)}|S_{n,c}(A)-\mathbb{E}[S_{n,c}(A)]|^2$$

respectively where $\phi(c)=|\Gamma(c)|$ (see (5.4.2)).

Theorem 12.3.1. *Suppose that* $\gcd(c,s)=t$ *and that* $\deg(c)>\frac{1}{2g}(72(4g^2+1)^2+1)$*. Then*

$$\phi(c)\cdot\mathbb{E}[S_{n,c}(A)] \;=\; \sum_{\substack{f\in\mathcal{M}_n\\ \gcd(f,c)=1}}\Lambda_\rho(f) \text{ and } \lim_{q\to\infty}\frac{\phi(c)}{q^{2n}}\cdot\operatorname{Var}[S_{n,c}(A)] = \min\{n, 2g\cdot\deg(c)-1\}.$$

Proof. This will follow from applying Theorems 11.0.1, 10.0.4, and 9.0.1 successively, the last with Remarks 9.0.2 and 9.0.3 in mind. To complete the proof we show that all the hypotheses of the first theorem are met.

Lemma 12.2.4 implies that ρ is pointwise pure of weight $w=1$ and that $\Phi(c)_{\rho\,\text{heavy}}$ is empty[2]. Moreover, Proposition 12.2.1 implies that $V(0)$ has a unique unipotent block of dimension two and no other unipotent block of multiplicity one (since $2g-2\neq 1$), hence Theorem 11.0.1 implies that the Mellin transform of ρ has big monodromy since $\gcd(c,s)=t$ and since

$$\deg(c) > \frac{1}{2g}(72((2g)^2+1)^2-2g-0+(1+2g)) = \frac{1}{2g}(72(4g^2+1)^2+1).$$

Therefore the hypotheses of Theorem 11.0.1 hold as claimed. □

Taking $g=1$ and $f=x(x-1)$ yields Theorem 1.2.3 from §1.

[2]There *are* mixed characters, but as shown the proof of Theorem 9.0.1, they do not contribute to the main term of the variance estimate.

Appendix A. Middle Extension Sheaves

Recall the following notation:

X : a proper smooth geometrically connected curve over $\mathbb{F}_q$;

U : dense Zariski open subset of X defined over $\mathbb{F}_q$;

K : function field $\mathbb{F}_q(X)$;

$\mathcal{P}$: set of places of K;

$\mathcal{C}$: finite subset of $\mathcal{P}$;

G_K : absolute Galois group $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$;

$I(v)$: inertia subgroup in G_K of $v \in \mathcal{P}$;

$G_{K,\mathcal{C}}$: quotient of G_K by normal closure of $\langle\, I(v) \mid v \in \mathcal{P} \smallsetminus \mathcal{C}\,\rangle$;

ℓ : prime in $\mathbb{N}$ coprime to q;

$\mathcal{F}$: sheaf on X;

$\mathcal{G}$: sheaf on U.

All sheaves in this section are constructible and étale with coefficients in $\bar{\mathbb{Q}}_\ell$.

Let $j\colon U \to X$ be the inclusion of a dense Zariski open subset. Given $\mathcal{G}$ (e.g., the pullback sheaf $\mathcal{F}|_U = j^*\mathcal{F}$), there are two[3] functorial extensions of $\mathcal{G}$ to a sheaf on all of X we wish to consider: the extension by zero $j_!\mathcal{G}$ and the direct image $j_*\mathcal{G}$. As $\mathcal{F}$ and $\mathcal{G}$ vary we have

$$\mathrm{Hom}_X(j_!\mathcal{G}, \mathcal{F}) = \mathrm{Hom}_U(\mathcal{G}, j^*\mathcal{F}) \quad \text{and} \quad \mathrm{Hom}_X(\mathcal{F}, j_*\mathcal{G}) = \mathrm{Hom}_U(j^*\mathcal{F}, \mathcal{G}),$$

that is, the functors $j_!, j_*$ are adjoints of j^* (cf. [Mil80, II.3.14.a]). In particular, the adjoints of the identity $j^*\mathcal{F} \to j^*\mathcal{F}$ are maps of the form $j_!j^*\mathcal{F} \to \mathcal{F}$ and $\mathcal{F} \to j_*j^*\mathcal{F}$ called *adjunction maps*. We say that $\mathcal{F}$ is *supported on U* iff the first map is an isomorphism, and $\mathcal{F}$ is a *middle extension* iff the second map is an isomorphism for *every* j.

Lemma A.0.1.

(i) If $j^*\mathcal{F}$ is lisse and $\mathcal{F} \to j_*j^*\mathcal{F}$ is an isomorphism, then $\mathcal{F}$ is a middle extension.

(ii) If $\mathcal{G}$ is lisse, then $j_*\mathcal{G}$ is a middle extension.

Proof. Let $U' \subseteq X$ be a dense Zariski open and $U'' = U \cap U'$. Consider the commutative diagram

$$\begin{tikzcd} U'' \arrow[r, "i'"] \arrow[d, "i"'] & U' \arrow[d, "j'"] \\ U \arrow[r, "j"'] & X \end{tikzcd}$$

of inclusions and the corresponding commutative diagram

$$\begin{tikzcd} \mathcal{F} \arrow[rr] \arrow[d] & & j_*j^*\mathcal{F} \arrow[d] \\ j'_*j'^*\mathcal{F} \arrow[r] & (ij)_*(ij)^*\mathcal{F} = (i'j')_*(i'j')^*\mathcal{F} \end{tikzcd} \tag{A.0.2}$$

of adjunction maps.

[3]One can also consider hybrid versions such as $j''_!j'_*\mathcal{G}$ for inclusions $j'\colon U \to U'$ and $j''\colon U'' \to X$, but we do not need such versions.

Suppose $\mathcal{G}$ is lisse. On one hand, this implies the map $\mathcal{G} \to i_* i^* \mathcal{G}$ is an isomorphism, so the right map of (A.0.2) is an isomorphism when $\mathcal{G} = j^* \mathcal{F}$. In particular, if the top map of (A.0.2) is also an isomorphism, then the left map must also be an isomorphism, for *every* j', hence (i) holds. On the other hand, the direct image map $j_* \mathcal{G} \to j_* i_* i^* \mathcal{G}$ is also an isomorphism. It even coincides with the adjunction map $j_* \mathcal{G} \to j'_* j'^* j_* \mathcal{G}$ via the functorial identities $j_* i_* i^* \mathcal{G} = j'_* i'_* i^* \mathcal{G} = j'_* j'^* j_* \mathcal{G}$, so (ii) holds. ☐

Lemma A.0.3. *Suppose $\mathcal{F}$ is a middle extension. If $j^* \mathcal{F} \simeq \mathcal{G}$ on U, then $\mathcal{F} \simeq j_* \mathcal{G}$ on X.*

Proof. Let $j_* j^* \mathcal{F} \to \mathcal{F}$ be the inverse of the adjunction map $\mathcal{F} \to j_* j^* \mathcal{F}$, and let $j^* \mathcal{F} \to \mathcal{G}$ and $\mathcal{G} \to j^* \mathcal{F}$ be mutually inverse morphisms. Then the composed maps

$$\mathcal{F} \to j_* j^* \mathcal{F} \to j_* \mathcal{G} \quad \text{and} \quad j_* \mathcal{G} \to j_* j^* \mathcal{F} \to \mathcal{F}$$

are mutually inverse. ☐

Let $\bar{\eta}$ be a geometric generic point of X and V be a finite-dimensional $\bar{\mathbb{Q}}_\ell[G_{K,\mathcal{C}}]$-module. The following proposition shows that there is a canonical middle extension sheaf on X we can associate to V (cf. [Mil80, 3.1.16]).

Proposition A.0.4. *There is a middle extension $\mathcal{F}$ with $\mathcal{F}_{\bar{\eta}} = V$ as $G_{K,\mathcal{C}}$-modules, and it is unique up to isomorphism.*

Proof. Suppose $U \subseteq X$ is the open complement corresponding to $\mathcal{C}$ so that the structure map $G_K \to \mathrm{GL}(V)$ factors through the quotient $G_K \twoheadrightarrow G_{K,\mathcal{C}}$ and so that we can identify $G_{K,\mathcal{C}}$ with the étale fundamental group $\pi_1(U, \bar{\eta})$. Then there is a lisse sheaf $\mathcal{G}$ on U corresponding to the representation $\pi_1(U, \bar{\eta}) \to \mathrm{GL}(V)$ through which $G_K \to \mathrm{GL}(V)$ factors, and it is unique up to isomorphism. In particular, $\mathcal{G}$ and $\mathcal{F} = j_* \mathcal{G}$ is are middle extension sheaves by Lemma A.0.1.ii and $\mathcal{F}_{\bar{\eta}} = \mathcal{G}_{\bar{\eta}} = V$ as $G_{K,\mathcal{C}}$-modules. Every isomorphism $\mathcal{F}_{\bar{\eta}} \simeq V$ of $G_{K,\mathcal{C}}$-modules extends to an isomorphism $j^* \mathcal{F} \to \mathcal{G}$ of lisse sheaves, and Lemma A.0.3 implies the latter extends to an isomorphism $\mathcal{F} \simeq j_* \mathcal{G}$. ☐

Appendix B. Euler Characteristics

We continue the notation of the previous section. Let $j\colon U \to X$ be the inclusion of a dense Zariski open subset and $\mathcal{F}$ be a sheaf on U. Then there is an exact sequence

$$0 \longrightarrow j_! \mathcal{F} \longrightarrow j_* \mathcal{F} \longrightarrow \mathcal{S}_{\mathcal{F}} \longrightarrow 0$$

where $\mathcal{S}_{\mathcal{F}}$ is a skyscraper sheaf supported on $Z = X \smallsetminus U$, and the corresponding long exact sequence of (étale) cohomology (over $\bar{\mathbb{F}}_q$) can be written

$$\cdots \to H^i(\bar{Z}, \mathcal{S}_{\mathcal{F}}) \to H^{i+1}_c(\bar{U}, \mathcal{F}) \to H^{i+1}(\bar{X}, j_* \mathcal{F}) \to \cdots \tag{B.0.1}$$

where $n \in \mathbb{Z}$.

Lemma B.0.2. *There exist exact sequences*

$$0 \to H^0_c(\bar{U}, \mathcal{F}) \to H^0(\bar{X}, j_* \mathcal{F}) \to H^0(\bar{Z}, \mathcal{S}_{\mathcal{F}}) \to H^1_c(\bar{U}, \mathcal{F}) \to H^1(\bar{X}, j_* \mathcal{F}) \to 0 \tag{B.0.3}$$

and

$$0 \longrightarrow H^2_c(\bar{U}, \mathcal{F}) \longrightarrow H^2(\bar{X}, j_* \mathcal{F}) \longrightarrow 0 \tag{B.0.4}$$

and all other cohomology groups in (B.0.1) *vanish.*

Proof. The first term of (B.0.1) vanishes unless $n = 0$ since $\dim(Z) = 0$, and the other two terms vanish for $n+1 \neq 0, 1, 2$ since U and X are curves. Therefore (B.0.1) breaks into the pieces (B.0.3) and (B.0.4), and all other terms vanish. ☐

If $U = X$, then the middle term of (B.0.3) vanishes, and otherwise the first term vanishes since any curve $U \subsetneq X$ is affine. Either way, the Euler characteristics

$$\chi(\bar{X}, j_*\mathcal{F}) := \sum_{n=0}^{2}(-1)^n \dim(H^i(\bar{X}, j_*\mathcal{F})), \quad \chi_c(\bar{U}, j_*\mathcal{F}) := \sum_{n=0}^{2}(-1)^n \dim(H^i_c(\bar{U}, j_*\mathcal{F})), \tag{B.0.5}$$

and $\chi(\bar{Z}, \mathcal{S}_{\mathcal{F}}) = \dim(H^0(\bar{Z}, \mathcal{S}_{\mathcal{F}}))$ satisfy

$$\chi(\bar{X}, j_*\mathcal{F}) - \chi_c(\bar{U}, \mathcal{F}) = \chi(\bar{Z}, \mathcal{S}_{\mathcal{F}}) = \sum_{z\in Z} \deg(z) \cdot \dim(\mathcal{F}_{\bar{\eta}}^{I(z)}). \tag{B.0.6}$$

B.1. **Middle Extensions.** Let ρ be a Galois representation and $\mathrm{ME}(\rho)$ be the corresponding middle-extension sheaf.

Proposition B.1.1. *Let g be the genus of $\bar{X}$. Then*

$$\chi(\bar{X}, \mathrm{ME}(\rho)) = (2-2g)\cdot \mathrm{rank}(\rho) - (\mathrm{drop}(\rho) + \mathrm{Swan}(\rho))$$

Proof. Suppose $\mathrm{ME}(\rho)$ is lisse on U; we may since $\mathrm{ME}(\rho)$ is a middle extension. On one hand, the Euler-Poincare formula, as proved by Raynaud [Ray95, Th. 1], asserts

$$\chi_c(\bar{U}, \mathrm{ME}(\rho)) = \chi_c(\bar{U})\cdot \mathrm{rank}(\rho) - \mathrm{Swan}(\rho), \quad \chi_c(\bar{U}) = 2-2g-\deg(Z).$$

On the other hand, a short calculation shows

$$\chi(\bar{Z}, \mathrm{ME}(\rho)) = \deg(Z)\cdot \mathrm{rank}(\rho) - \mathrm{drop}(\rho)$$

since U is open and dense in X and hence Z is finite, and thus

$$\chi(\bar{X}, \mathrm{ME}(\rho)) = \chi_c(\bar{U}, \mathrm{ME}(\rho)) + \chi(\bar{Z}, \mathrm{ME}(\rho)) = (2-2g)\cdot\mathrm{rank}(\rho) - \mathrm{drop}(\rho) - \mathrm{Swan}(\rho)$$

as claimed. □

Let $\mathcal{C} \subset \mathcal{P}$ be the subset of places corresponding to the finite complement $Z = X \smallsetminus U$.

Corollary B.1.2. *If $\mathrm{ME}(\rho)$ is supported on U, then $\chi_c(\bar{U}, \mathrm{ME}(\rho)) = \chi(\bar{X}, \mathrm{ME}(\rho))$, and*

$$\chi_c(\bar{U}, \mathrm{ME}(\rho)) = (2-\deg(\mathcal{C}))\cdot\mathrm{rank}(\rho) - (\mathrm{drop}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho) + \mathrm{Swan}(\rho))$$

in general.

Proof. If $\mathrm{ME}(\rho)$ is supported on U, then $\mathrm{drop}_{\mathcal{C}}(\rho) = \deg(\mathcal{C})\cdot\mathrm{rank}(\rho)$, so it suffices to show (3.5.3) holds in general. Recall that $Z = \mathcal{C}$, so the desired identity follows easily from the identities

$$\chi_c(\bar{U}, \mathrm{ME}(\rho)) = \chi(\bar{X}, \mathrm{ME}(\rho)) - \chi(\bar{Z}, \mathrm{ME}(\rho))$$

and

$$\chi(\bar{Z}, \mathrm{ME}(\rho)) = \deg(\mathcal{C})\cdot\mathrm{rank}(\rho) - \mathrm{drop}_{\mathcal{C}}(\rho)$$

and (3.5.2). □

Let φ be a character of conductor supported by $\mathcal{C}$.

Lemma B.1.3.

(i) If φ is tame, then $\mathrm{Swan}(\rho\otimes\varphi) = \mathrm{Swan}(\rho)$.

(ii) $\mathrm{drop}(\rho\otimes\varphi) - \mathrm{drop}(\rho) = \mathrm{drop}_{\mathcal{C}}(\rho\otimes\varphi) - \mathrm{drop}_{\mathcal{C}}(\rho)$.

Proof. If $v \in \mathcal{P}$, then $\mathrm{Swan}_v(\rho \otimes \varphi) = \mathrm{Swan}_v(\rho)$ since tensoring with tamely ramified character (e.g., φ) does not change the local Swan conductor. Moreover, if $v \notin \mathcal{C}$, then V and V_φ are isomorphic as $I(v)$-modules (since φ has conductor supported on $\mathcal{C}$). Hence $L(T, \rho_v)$ and $L(T, (\rho \otimes \varphi)_v)$ have the same degree, and in particular,

$$\mathrm{drop}_v(\rho \otimes \varphi) - \mathrm{drop}_v(\rho) = \deg(L(T, \rho_v)) - \deg(L(T, (\rho \otimes \varphi)_v)) = 0$$

when $v \notin \mathcal{C}$. □

Appendix C. Detecting a Big Subgroup of GL_R

Let R be a positive integer and G be a connected reductive subgroup of $\mathrm{GL}_R(\bar{\mathbb{Q}}_\ell)$, and suppose G acts irreducibly on $\bar{\mathbb{Q}}_\ell^R$. The main goal of this section is to state and prove a theorem of the following form:

Claim C.0.1. *If G contains a suitable element g, then $G = \mathrm{SL}_R(\bar{\mathbb{Q}}_\ell)$ or $G = \mathrm{GL}_R(\bar{\mathbb{Q}}_\ell)$.*

We give explicit conditions on g after introducing some terminology and preliminary results.

C.1. Weight multiplicity map.

Let m be a positive integer and $[m] = \{1, \ldots, m\}$.

Definition C.1.1. A *weight partition map* of an element $\alpha = (\alpha_1, \ldots, \alpha_m)$ in $(\bar{\mathbb{Q}}^\times)^m$ is a map $w_\alpha \colon [m] \to [m]$ satisfying the following for every $i, j \in [m]$:

$$w_\alpha(i) = w_\alpha(j) \text{ iff } |\iota(\alpha_i)| = |\iota(\alpha_j)|; \quad |w_\alpha^{-1}(i)| \geq |w_\alpha^{-1}(j)| \text{ if } i \leq j.$$

The fibers of w_α partition the indices $i \in [m]$ according to the corresponding weights $-\log_q |\iota(\alpha_i)|^2$ and are ordered according to size.

In general, α may have multiple weight partition maps, but all will induce the same partition of $[m]$, have the same range, and yield the same map $[m] \to \mathbb{Z}$ given by $i \mapsto |w_\alpha^{-1}(i)|$. In particular, if w_α is a weight partition map of α and if $\sigma \in \mathrm{Sym}(m)$, then the composed map $w_\alpha \sigma$ is also a weight partition map of α.

Definition C.1.2. The *mth weight multiplicity map* is the map

$$\mu_m \colon (\bar{\mathbb{Q}}^\times)^m \to \mathbb{Z}^m$$

which sends an element α to the tuple $\lambda = (\lambda_1, \ldots, \lambda_m)$ satisfying $\lambda_i = |w_\alpha^{-1}(i)|$ for some weight partition map w_α and every $i \in [m]$.

Definition C.1.3. For any $\lambda = \mu_m(\alpha)$, let $\mathrm{len}(\lambda) = \max\{1 \leq i \leq m : \lambda_i \neq 0\}$.

Observe that $[\mathrm{len}(\lambda)]$ is the range of any weight partition map w_α of α and $(\lambda_1, \ldots, \lambda_{\mathrm{len}(\lambda)})$ is a partition of m.

Example C.1.4. Let $\lambda = \mu_5(1, -1, q, -q, q^2)$. Then $\lambda = \mu_5(q^2, -q, q, -1, 1) = (2, 2, 1, 0, 0)$, and thus $\mathrm{len}(\lambda) = 3$ and $(2, 2, 1)$ is a partition of 5.

Lemma C.1.5. *Let $\alpha, \beta \in (\bar{\mathbb{Q}}^\times)^m$, and let $s \in \bar{\mathbb{Q}}^\times$ and $\sigma \in \mathrm{Sym}(m)$. Suppose $\beta_i = s\alpha_{\sigma(i)}$ for every $i \in [m]$. Then $\mu_m(\alpha) = \mu_m(\beta)$.*

Proof. Let w_α, w_β be respective weight partition maps of α, β. Then for every $i, j \in [m]$, one has

$$w_\beta(i) = w_\beta(j) \iff |\iota(\beta_i)| = |\iota(\beta_j)| \iff |\iota(\alpha_{\sigma(i)})| = |\iota(\alpha_{\sigma(j)})| \iff w_\alpha\sigma(i) = w_\alpha\sigma(j).$$

In particular, the weight partition maps $\sigma w_\alpha, w_\beta$ of α, β respectively coincide, so $\mu_m(\alpha) = \mu_m(\beta)$ as claimed. □

C.2. **Tensor indecomposability.** Let $m, n \geq 2$ be integers, let $\alpha \in (\bar{\mathbb{Q}}^\times)^m$, $\beta \in (\bar{\mathbb{Q}}^\times)^n$, and $\gamma \in (\bar{\mathbb{Q}}^\times)^{mn}$ be elements, and let $a = \mu_m(\alpha)$, $b = \mu_n(\beta)$, $c = \mu_{mn}(\gamma)$. We regard α and β as respective tuples of eigenvalues of matrices $A \in \mathrm{GL}_m(\bar{\mathbb{Q}})$ and $B \in \mathrm{GL}_n(\bar{\mathbb{Q}})$. We also suppose that γ is an eigenvalue tuple of the tensor product $A \otimes B$, and thus there exists a bijection $\tau \colon [m] \times [n] \to [mn]$ satisfying

$$\gamma_{\tau(i,j)} = \alpha_i \beta_j \text{ for } (i,j) \in [m] \times [n].$$

Let $w_\alpha, w_\beta, w_\gamma$ be weight partition maps of α, β, γ respectively.

Lemma C.2.1. *There exists a unique map* $\kappa \colon [\mathrm{len}(a)] \times [\mathrm{len}(b)] \to [\mathrm{len}(c)]$ *which makes the following diagram commute:*

$$\begin{tikzcd} {[m] \times [n]} \arrow[r, "\tau"] \arrow[d, "w_\alpha \times w_\beta"'] & {[mn]} \arrow[d, "w_\gamma"] \\ {[\mathrm{len}(a)] \times [\mathrm{len}(b)]} \arrow[r, "\kappa"'] & {[\mathrm{len}(c)].} \end{tikzcd}$$

In particular,

$$c_k = \sum_{\kappa(i,j)=k} a_i b_j. \tag{C.2.2}$$

Proof. To see that such a map exists observe that $w_\gamma \tau$ factors through $w_\alpha \times w_\beta$ since

$$\begin{aligned} (w_\alpha \times w_\beta)(i_1, j_1) = (w_\alpha \times w_\beta)(i_2, j_2) \quad &\Longleftrightarrow \quad |\alpha_{i_1}| = |\alpha_{i_2}| \text{ and } |\beta_{j_1}| = |\beta_{j_2}| \\ &\Longrightarrow \quad |\alpha_{i_1}\beta_{j_1}| = |\alpha_{i_2}\beta_{j_2}| \\ &\Longleftrightarrow \quad |\gamma_{\tau(i_1,j_1)}| = |\gamma_{\tau(i_2,j_2)}| \\ &\Longleftrightarrow \quad w_\gamma\tau(i_1, j_1) = w_\gamma\tau(i_2, j_2) \end{aligned}$$

for every $i_1, i_2 \in [m]$ and $j_1, j_2 \in [n]$. To see that the map is unique, observe that the left vertical map of the diagram is surjective and that the map must satisfy $l \mapsto w_\gamma\tau(i,j)$ for any (i,j) in $(w_\alpha \times w_\beta)^{-1}(l)$. Finally, (C.2.2) follows from the identities

$$c_k = |w_\gamma^{-1}(k)| = |(\tau \circ w_\gamma)^{-1}(k)| = |(w_\alpha \times w_\beta \circ \kappa)^{-1}(k)| = \sum_{\kappa(i,j)=k} |(w_\alpha \times w_\beta)^{-1}(i,j)| = \sum_{\kappa(i,j)=k} a_i b_j.$$

□

Example C.2.3. Let $\alpha = (1, 1, q)$, $\beta = (1, q, q)$, and $\gamma = (1, 1, q, q, q, q, q, q^2, q^2)$. The maps w_α and w_β are canonical and given by

$$w_\alpha(i) = \begin{cases} 1 & i = 1, 2 \\ 2 & i = 3 \end{cases}, \quad w_\beta(j) = \begin{cases} 2 & j = 1 \\ 1 & j = 2, 3 \end{cases}.$$

The maps τ and w_γ are not canonical, so we choose

$$\tau(i,j) = 3(j-1) + i, \quad w_\gamma(j) = \begin{cases} 2 & i = 1, 2 \\ 1 & j = 3, \ldots, 7 \\ 3 & i = 8, 9 \end{cases}.$$

Then one has $a = b = (2, 1, 0)$ and $c = (4, 2, 2, 0, 0, 0, 0, 0, 0)$, and also

$$w_\gamma\tau(i,j) = \begin{cases} 1 & (i,j) = (1,1), (2,1) \\ 3 & (i,j) = (3,2), (3,2) \\ 2 & \text{otherwise} \end{cases}$$

for $(i,j) \in [3]\times[3]$. Therefore, the domain and codomain of κ are $[2]\times[2]$ and $[3]$ respectively, and

$$\kappa(i,j) = \begin{cases} 1 & (i,j) = (1,1),(2,2) \\ 2 & (i,j) = (1,2) \\ 3 & (i,j) = (2,1) \end{cases}$$

for $(i,j) \in [2]\times[2]$.

Lemma C.2.4. *For each $l \in [\mathrm{len}(a)]$, the restriction of κ to $\{l\}\times[\mathrm{len}(b)]$ is injective, and in particular,* $\mathrm{len}(b) \leq \mathrm{len}(c)$.

Proof. Recall that $[\mathrm{len}(a)]$ and $[\mathrm{len}(b)]$ are the respective ranges of w_α and w_β, so suppose $i \in [m]$ and $j_1, j_2 \in [n]$. Moreover, one has

$$\begin{aligned} \kappa(w_\alpha(i), w_\beta(j_1)) = \kappa(w_\alpha(i), w_\beta(j_2)) \quad &\iff \quad w_\gamma\tau(i,j_1) = w_\gamma\tau(i,j_2) \\ &\iff \quad |\gamma_{\tau(i,j_1)}| = |\gamma_{\tau(i,j_2)}| \\ &\iff \quad |\alpha_i\beta_{j_1}| = |\alpha_i\beta_{j_2}| \\ &\iff \quad w_\beta(j_1) = w_\beta(j_2), \end{aligned}$$

and thus the restriction of κ to $\{w_\alpha(i)\}\times[\mathrm{len}(b)]$ is injective as claimed. ☐

Let r be a positive integer.

Lemma C.2.5.

(i) If $c_{\mathrm{len}(c)} \leq r$, then $a_{\mathrm{len}(a)} \leq r$ and $b_{\mathrm{len}(b)} \leq r$.

(ii) If $a_1 > r$ (resp. $b_1 > r$), then $c_{\mathrm{len}(b)} > r$ (resp. $c_{\mathrm{len}(a)} > r$).

Proof. For part (i), we prove the contrapositive. More precisely, if $k \in [\mathrm{len}(c)]$, then one has

$$c_k \overset{(\mathrm{C.2.2})}{=} \sum_{\kappa(i,j)=k} a_i b_j \geq a_{\mathrm{len}(a)} b_{\mathrm{len}(b)} \geq \max\{a_{\mathrm{len}(a)}, b_{\mathrm{len}(b)}\},$$

and thus $c_{\mathrm{len}(c)} > r$ if $a_{\mathrm{len}(a)} > r$ or $b_{\mathrm{len}(b)} > r$. Thus (i) holds.

For part (ii), we suppose, without loss of generality, that $a_1 > r$ and show that $c_{\mathrm{len}(b)} > r$. We first observe that Lemma C.2.4 implies the integers $\kappa(1,1),\ldots,\kappa(1,\mathrm{len}(b))$ are distinct. Moreover, for each $l \in [\mathrm{len}(b)]$, one has

$$c_{\kappa(1,l)} \geq a_1 b_l > r \cdot 1 = r.$$

Therefore at least $\mathrm{len}(b)$ integers in the monotone decreasing sequence $c_1,\ldots,c_{\mathrm{len}(b)}$ exceed r, and thus (ii) holds. ☐

The following proposition is the main result of this subsection. We will use it to deduce that a certain representation is tensor indecomposable whenever $mn \gg r$.

Proposition C.2.6. *Suppose $c_{\mathrm{len}(c)} = 1 < \mathrm{len}(c)$ and $c_2 \leq r$. If $\mathrm{len}(c) \leq r+1$, then $m,n \leq r^2+1$ and thus $mn \leq (r^2+1)^2$.*

Proof. Lemma C.2.5.i implies that $a_{\mathrm{len}(a)} = b_{\mathrm{len}(b)} = 1$ since $c_{\mathrm{len}(c)} = 1$. Therefore $\mathrm{len}(a) \geq 2$ and $\mathrm{len}(b) \geq 2$ since $m \geq 2$ and $n \geq 2$ respectively, and moreover, $c_2 \geq c_{\mathrm{len}(a)}$ or $c_2 \geq c_{\mathrm{len}(b)}$. Hence the contrapositive of Lemma C.2.5.ii implies $a_1 \leq r$ and $b_1 \leq r$ since $c_2 \leq r$. In particular, if $\mathrm{len}(c) \leq r+1$, then Lemma C.2.4 implies $\mathrm{len}(a), \mathrm{len}(b) \leq r+1$, and thus

$$m = \sum_{i=1}^{\mathrm{len}(a)} a_i \leq ra_1 + a_{\mathrm{len}(a)} \leq r^2+1, \quad n = \sum_{j=1}^{\mathrm{len}(b)} b_j \leq rb_1 + b_{\mathrm{len}(b)} \leq r^2+1$$

as claimed. ☐

C.3. **Pairing avoidance.** Let n be a positive integer and I be the $n \times n$ identity matrix. We define the orthogonal and symplectic groups of matrices by

$$\mathrm{O}_n(\bar{\mathbb{Q}}) = \left\{ M \in \mathrm{GL}_n(\bar{\mathbb{Q}}) : MM^t = I \right\}$$

and

$$\mathrm{Sp}_{2n}(\bar{\mathbb{Q}}) = \left\{ M \in \mathrm{GL}_{2n}(\bar{\mathbb{Q}}) : MPM^t = P \text{ for } P = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \right\}$$

respectively.

Lemma C.3.1. *Suppose $h \in \mathrm{GL}_m(\bar{\mathbb{Q}})$ where $m = n$ (resp. $m = 2n$) and $hgh^{-1} \in \mathrm{O}_n(\bar{\mathbb{Q}})$ (resp. $hgh^{-1} \in \mathrm{Sp}_{2n}(\bar{\mathbb{Q}})$) . Let $\alpha \in (\bar{\mathbb{Q}}^\times)^m$ be a tuple of the eigenvalues of g and $a = \mu_m(\alpha)$. Then some involution $\pi \in \mathrm{Sym}(\mathrm{len}(a))$ satisfies the following:*

(i) $a_i = a_{\pi(i)}$ for every $i \in [\mathrm{len}(a)]$;

(ii) π has at most one fixed point.

Proof. Since g and hgh^{-1} have the same eigenvalues, we suppose without loss of generality that $h = 1$. The involution $s \mapsto 1/s$ of $\bar{\mathbb{Q}}^\times$ induces a permutation of the eigenvalues of elements of $\mathrm{O}_n(\bar{\mathbb{Q}})$ and $\mathrm{Sp}_{2n}(\bar{\mathbb{Q}})$. The latter is an involution $\sigma \in \mathrm{Sym}(m)$ with the property that, for any weight partition map w_α of α and every $i \in [m]$, one has

$$w_\alpha(i) = w_\alpha\sigma(i) \iff |\alpha_i| = |\alpha_{\sigma(i)}| \iff |\alpha_i| = |1/\alpha_i| \iff |\alpha_i| = 1.$$

The involution in question is given by $w_\alpha(i) \mapsto w_\alpha\sigma(i)$ for every $i \in [m]$; recall w_α maps onto $[\mathrm{len}(a)]$. □

The following is the main result of this subsection. We will use it to show that some subgroup of $\mathrm{GL}_m(\bar{\mathbb{Q}})$ fails to preserve non-degenerate pairings which are either symmetric or alternating.

Proposition C.3.2. *Let g be an element of $\mathrm{GL}_m(\bar{\mathbb{Q}})$, $\alpha \in (\bar{\mathbb{Q}}^\times)^m$ be a tuple of its eigenvalues, and $a = \mu_m(\alpha)$. If there exist i, j such that a_i, a_j are distinct from each other and from all a_k for $k \neq i, j$, then g is not conjugate to an element of $\mathrm{O}_m(\bar{\mathbb{Q}})$. If moreover $m = 2n$, then g is not conjugate to an element of $\mathrm{Sp}_{2n}(\bar{\mathbb{Q}})$.*

Proof. We prove the contrapositive. More precisely, if $hgh^{-1} \in \mathrm{O}_m(\bar{\mathbb{Q}})$ (resp. $hgh^{-1} \in \mathrm{Sp}_{2n}(\bar{\mathbb{Q}})$) for some $h \in \mathrm{GL}_m(\bar{\mathbb{Q}})$ and if $\pi \in \mathrm{Sym}(\mathrm{len}(a))$ is an involution satisfying the properties of Lemma C.3.1, then $\pi(i) = i$ for at most one i. Therefore, for all but at most one i and for $j = \pi(i)$, one has $i \neq j$ and $a_i = a_j$. In particular, there is at most one i such that $a_i \neq a_j$ for $j \neq i$. □

C.4. **Main theorem.** In this section we state and prove the main result of this appendix.

Theorem C.4.1. *Let r, R be positive integers and G be a connected reductive subgroup of $\mathrm{GL}_R(\bar{\mathbb{Q}}_\ell)$. Let $g \in G$ be an element and $\gamma \in (\bar{\mathbb{Q}}_\ell^\times)^R$ be an eigenvector tuple of g. Suppose that G is irreducible, that γ lies in $(\bar{\mathbb{Q}}^\times)^R$, and that $c = \mu_R(\gamma)$ satisfies $1 < \mathrm{len}(c) \leq r + 1$ and $1 = c_{\mathrm{len}(c)} < c_{\mathrm{len}(c)-1}$ and $c_2 \leq r$. If $R > 72(r^2 + 1)^2$, then either $G = \mathrm{SL}_R(\bar{\mathbb{Q}}_\ell)$ or $G = \mathrm{GL}_R(\bar{\mathbb{Q}}_\ell)$.*

The proof will occupy the remainder of this subsection.

Since G is algebraic, it contains the semisimplification of g, an element for which γ is also an eigenvector. Hence we replace g by its semisimplification and suppose without loss of generality that g is semisimple. We also replace G and g by the conjugates $h^{-1}Gh$ and $h^{-1}gh$ by a suitable element $h \in \mathrm{GL}_R(\bar{\mathbb{Q}}_\ell)$ so that we may suppose without loss of generality that g is the diagonal matrix $\mathrm{diag}(\gamma_1, \ldots, \gamma_R)$.

Let $V = \bar{\mathbb{Q}}_\ell^R$ and f be the diagonal matrix

$$f = \mathrm{diag}(|\iota(\gamma_1)|, \ldots, |\iota(\gamma_R)|).$$

We claim we may regard f as an element of $\mathrm{GL}_R(\bar{\mathbb{Q}}_\ell)$. More precisely, it is an element of $\mathrm{GL}_R(\iota(\bar{\mathbb{Q}})) \subset \mathrm{GL}_R(\mathbb{C})$ since $|\iota(\gamma_i)|^2 = \iota(\gamma_i)\overline{\iota(\gamma_i)}$ lies in the algebraically closed subfield $\iota(\bar{\mathbb{Q}}) \subset \mathbb{C}$ and thus so does $|\iota(\gamma_i)|$. Replacing G, g, f by conjugates by a suitable common permutation matrix, we suppose without loss of generality that $|\iota(\gamma_1)|$ is an eigenvalue of f of multiplicity c_1.

Lemma C.4.2. *f is a semisimple element of G such that $f - |\iota(\gamma_1)| \in \mathrm{End}(V)$ has rank at most r^2.*

Proof. For some sequence $e_1, \dots, e_n$ of tuples $e_i = (e_{i,1}, \dots, e_{i,m}) \in \mathbb{Z}^m$, the intersection of G with the subgroup of diagonal matrices in $\mathrm{GL}_R(\bar{\mathbb{Q}}_\ell)$ consists of all matrices $\mathrm{diag}(\alpha_1, \dots, \alpha_m)$ satisfying

$$\prod_{i=1}^m \alpha_i^{e_{1,i}} = \prod_{i=1}^m \alpha_i^{e_{2,i}} = \cdots = \prod_{i=1}^m \alpha_i^{e_{n,i}} = 1.$$

By hypothesis, g lies in this intersection, and thus

$$|\iota(\prod_{i=1}^m \gamma_i^{e_{1,i}})| = |\iota(\prod_{i=1}^m \gamma_i^{e_{2,i}})| = \cdots = |\iota(\prod_{i=1}^m \gamma_i^{e_{n,i}})| = |\iota(1)|$$

or equivalently

$$\prod_{i=1}^m |\iota(\gamma_i)|^{e_{1,i}} = \prod_{i=1}^m |\iota(\gamma_i)|^{e_{2,i}} = \cdots = \prod_{i=1}^m |\iota(\gamma_i)|^{e_{n,i}} = 1.$$

Therefore f is a diagonal (hence semisimple) element of G as claimed. It remains to show $f - |\iota(\gamma_1)| \in \mathrm{End}(V)$ has rank at most r^2. Indeed, exactly c_1 of its eigenvalues equal $|\iota(\gamma_1)|$, hence the rank of $f - |\iota(\gamma_1)|$ is

$$R - c_1 \leq \sum_{i=2}^{\mathrm{len}(c)} c_i \leq r \cdot r = r^2$$

by our hypotheses on c. $\square$

Let $[G, G]$ be the derived (i.e., commutator) subgroup of G. Observe that G acts irreducibly on $V = \bar{\mathbb{Q}}_\ell^R$ by hypothesis, so its center $Z(G)$ consists entirely of scalars and G is an almost product of $[G, G]$ and $Z(G)$. In particular, $[G, G]$ is a connected semisimple group which also acts irreducibly on V, and for some $a \in \bar{\mathbb{Q}}_\ell^\times$, the scalar multiple af lies in $[G, G]$.

Let $\mathfrak{g} \subseteq \mathfrak{gl}_R = \mathrm{End}(V)$ be the Lie algebra of $[G, G]$. We claim $\mathfrak{g}$ is simple. On one hand, $\mathfrak{g}$ is a semisimple irreducible Lie subalgebra of $\mathfrak{gl}_R$ since $[G, G]$ is semisimple and acts irreducibly on V. It also contains af, and Lemma C.4.2 implies that $\dim((af - a|\iota(\gamma_1)|)V) \leq r^2$, hence the contrapositive of Proposition C.2.6 implies that V is not tensor decomposable as a representation of $\mathfrak{g}$. On the other hand, $\mathfrak{g}$ has a decomposition $\mathfrak{g} = \prod_{i=1}^n \mathfrak{g}_i$ with respect to simple Lie subalgebras $\mathfrak{g}_1, \dots, \mathfrak{g}_n \subseteq \mathfrak{g}$, and thus V has a tensor decomposition $V = \bigotimes_{i=1}^n V_i$ where $\mathfrak{g}_i$ acts faithfully on V_i. In particular, $n = 1$ since V is not tensor decomposable, and thus $\mathfrak{g}$ is simple as claimed. (Compare [Kat02, proof of Th. 1.4.3].)

We now apply the following theorem to deduce that $\mathfrak{g}$ is one of $\mathfrak{sl}(V)$, $\mathfrak{so}(V)$, or $\mathfrak{sp}(V)$.

Theorem C.4.3. (Zarhin) *Let $\mathfrak{g} \subseteq \mathrm{End}(V)$ be a simple Lie subalgebra, and suppose that $\mathfrak{g}$ acts irreducibly on V. Let $(a, f) \in \bar{\mathbb{Q}}_\ell \times \mathfrak{g}$ and $r = \mathrm{rank}(f - a)$. If $R = \dim(V) > 72r^2$, then $\mathfrak{g}$ is one of $\mathfrak{sl}(V)$, $\mathfrak{so}(V)$, or $\mathfrak{sp}(V)$.*

Proof. See [Zar90, Lem. 4 and Th. 6]. These results refer to constants D and D_2 respectively, and in the proofs one finds $D = 1/8$ and $D_2 = 9/D = 72$ suffice. The latter is the source of the constant 72 in the hypothesis $R > 72r^2$. Compare [Kat02, Th. 1.4.4]. $\square$

To complete the proof of the theorem it suffices to rule out $\mathfrak{g} = \mathfrak{so}(V)$ and $\mathfrak{g} = \mathfrak{sp}(V)$ or equivalently to show that G preserves neither an orthogonal nor a symplectic pairing. However, our hypotheses on c together with the contrapositive of Proposition C.3.2 implies that G preserves neither such type of pairing, so $\mathfrak{g} = \mathfrak{sl}(V)$ as claimed. That is, $[G, G]$ is $\mathrm{SL}(V)$ and G is equal to one of $\mathrm{SL}(V)$ or $\mathrm{GL}(V)$.

Appendix D. Perverse Sheaves and the Tannakian Monodromy Group

D.1. **Category of perverse sheaves.** Given a smooth curve X over a perfect field $\mathbb{F}$, we can speak of the so-called derived category $D_c^b(X, \bar{\mathbb{Q}}_\ell)$. Its objects M are complexes of constructible $\bar{\mathbb{Q}}_\ell$-sheaves on X over $\mathbb{F}$ whose cohomology complex

$$\cdots \longrightarrow \mathcal{H}^{-1}(M) \longrightarrow \mathcal{H}^0(M) \longrightarrow \mathcal{H}^1(M) \longrightarrow \cdots$$

is bounded and whose cohomology sheaves $\mathcal{H}^i(M)$ are all constructible. There is a well-defined dual object DM, the Verdier dual of M. Moreover, for each $n \in \mathbb{Z}$, there is a well-defined shifted complex $M[n]$ which satisfies $\mathcal{H}^i(M[n]) = \mathcal{H}^{i+n}(M)$.

We say that M is *semi-perverse* iff $\mathcal{H}^0(M)$ is punctual and $\mathcal{H}^i(M)$ vanishes for $i > 0$ and that M is *perverse* iff M and DM are semi-perverse. We write $\mathrm{Perv}(X, \bar{\mathbb{Q}}_\ell)$ for the full subcategory of perverse objects in $D_c^b(X, \bar{\mathbb{Q}}_\ell)$. It is an abelian category thus one can speak of subquotients of its objects as well as kernels and cokernels of its morphisms. It is common to call its objects perverse sheaves despite the fact that they are *complexes* of sheaves.

There is a natural functor from the category of constructible $\bar{\mathbb{Q}}_\ell$-sheaves on X over k to $D_c^b(X, \bar{\mathbb{Q}}_\ell)$: it sends a sheaf $\mathcal{F}$ to a complex concentrated at $i = 0$ and takes a morphism to the unique extension to a morphism of complexes. The image of this functor is not stable under duality though: if $\mathcal{F}^\vee$ is the dual of $\mathcal{F}$, then $D\mathcal{F}$ is isomorphic to $\mathcal{F}^\vee(1)[2]$. If instead one sends sends each $\mathcal{F}$ to $\mathcal{F}(1/2)[1]$, then self-dual objects are taken to self-dual objects and middle-extension sheaves are taken to perverse sheaves.

D.2. **Purity.** Let X be a smooth curve over $\mathbb{F}_q$. We say an object M in $D_c^b(X, \bar{\mathbb{Q}}_\ell)$ is *ι-mixed of weights $\leq w$* iff $\mathcal{H}^i(M)$ is pointwise ι-mixed of weights $\leq w + i$ for every i, and then $M[n]$ is ι-mixed of weights $w + n$. We also say M is *ι-pure of weight w* iff M is ι-mixed of weights $\leq w$ and DM is ι-mixed of weights $\leq -w$, and then $M[n]$ is ι-pure of weight $w + n$. Finally, we say M is *pure of weight w* iff it is ι-pure of weight w for every field embedding $\iota\colon \bar{\mathbb{Q}} \to \mathbb{C}$.

D.3. **Subobjects and subquotients.** Let $(\mathcal{C}, \oplus)$ be an abelian category, let $\mathbf{0}$ be its zero object, and let M, N be a pair of objects in $\mathcal{C}$.

We say that N is a *subobject* of M and write $N \subseteq M$ iff there is a monomorphism $N \hookrightarrow M$ in $\mathcal{C}$. More generally, we say N of M is a *subquotient* of M iff there exist an object S, a monomorphism $S \hookrightarrow M$, and an epimorphism $S \twoheadrightarrow N$ all in $\mathcal{C}$. Equivalently, N is a subquotient of M iff there exist an object Q, an epimorphism $M \twoheadrightarrow Q$, and a monomorphism $N \hookrightarrow Q$ all in $\mathcal{C}$.

Proposition D.3.1. *If $M \in \mathrm{Perv}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ is ι-pure of weight w, then so is every subquotient N.*

Proof. See [BBD82, 5.3.1]. □

Given a pair $N_1, N_2 \subseteq M$ of subobjects, we write $N_1 \subseteq N_2 \subseteq M$ iff $N_1 \subseteq N_2$ and, for the corresponding monomorphisms, $N_1 \hookrightarrow M$ equals the composition $N_1 \hookrightarrow N_2 \hookrightarrow M$. We also write $N_1 = N_2 \subseteq M$ iff $N_1 \subseteq N_2 \subseteq M$ and $N_2 \subseteq N_1 \subseteq M$. For example, if M is an object in $\mathrm{Perv}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ and if ϕ is the Frobenius automorphism of $\bar{M}$, then the subobjects $N \subseteq M$ give rise to precisely those subobjects $\bar{N} \subseteq \bar{M}$ satisfying $\bar{N} = \phi(\bar{N}) \subseteq \bar{M}$.

D.4. **Kummer sheaves.** Let $\mathbb{G}_m = \mathbb{P}^1_u \smallsetminus \{0, \infty\}$ over $\mathbb{F}_q$, and let $\pi_1^{\mathrm{t}}(\mathbb{G}_m)$ be the tame étale fundamental group, that is, the maximal quotient of $\pi_1(\mathbb{G}_m)$ whose kernel contains the p-Sylow subgroups of $I(0)$ and $I(\infty)$. It lies in an exact sequence

$$1 \to \pi_1^{\mathrm{t}}(\bar{\mathbb{G}}_m) \to \pi_1^{\mathrm{t}}(\mathbb{G}_m) \to \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \to 1$$

where $\pi_1^{\mathrm{t}}(\bar{\mathbb{G}}_m)$ is the image of $\pi_1(\bar{\mathbb{G}}_m)$ via the tame quotient $\pi_1(\mathbb{G}_m) \twoheadrightarrow \pi_1^{\mathrm{t}}(\mathbb{G}_m)$.

We say a constructible sheaf on $\bar{\mathbb{P}}^1$ is a *Kummer sheaf* iff it is a middle-extension sheaf which is lisse of rank one on $\bar{\mathbb{G}}_m$ and for which the corresponding representation factors through the quotient $\pi_1(\bar{\mathbb{G}}_m) \twoheadrightarrow \pi_1^{\mathrm{t}}(\bar{\mathbb{G}}_m)$. Equivalently, the Kummer sheaves are the middle-extension sheaves $\mathcal{L}_\rho$ on $\bar{\mathbb{P}}^1$ associated to a continuous character $\rho\colon \pi_1^{\mathrm{t}}(\bar{\mathbb{G}}_m) \to \bar{\mathbb{Q}}_\ell^\times$.

D.5. **Middle convolution on $\mathcal{P}$.** Let $\pi\colon \mathbb{G}_m \times \mathbb{G}_m \to \mathbb{G}_m$ be the multiplication map on $\mathbb{G}_m$ over $\mathbb{F}_q$. Using it one can define two additive bifunctors on $D^b_c(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$ corresponding to two flavors of multiplicative convolution:

$$M \star_! N := R\pi_!(M \boxtimes N), \quad M \star_* N := R\pi_*(M \boxtimes N).$$

There is a canonical map $M \star_! N \to M \star_* N$, but it need not be an isomorphism in general. However, if both convolution objects lie in $\mathrm{Perv}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$, then one can speak of the image of the map and define

$$M *_{\mathrm{mid}} N := \mathrm{Image}(M \star_! N \to M \star_* N).$$

This observation led Katz to define the full subcategory $\mathcal{P}$ of $\mathrm{Perv}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$ whose objects are all M for which $N \mapsto M \star_! N$ and $N \mapsto M \star_* N$ take perverse sheaves to perverse sheaves (see [Kat96, §2.6] and [Kat12, Ch. 2]). Among other things, it includes perverse sheaves $\mathcal{F}[1]$ for $\mathcal{F}$ a simple middle-extension sheaf on $\bar{\mathbb{G}}_m$ of generic rank at least two. Moreover, it is an additive category with respect to the usual direct sum of sheaves. Katz called the resulting additive bifunctor on $\mathcal{P}$ middle convolution.

D.6. **The category $\mathcal{P}_{\mathrm{arith}}$.** Let $D^b_c(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell) \to D^b_c(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$ be the "extension of scalars" functor which sends an object of M over $\mathbb{F}_q$ to the object $\bar{M} = M \times_{\mathbb{F}_q} \bar{\mathbb{F}}_q$. It maps objects of $\mathrm{Perv}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ to objects of $\mathrm{Perv}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$, and we define $\mathcal{P}_{\mathrm{arith}}$ to be the full subcategory of $\mathrm{Perv}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ whose objects M are those for which $\bar{M}$ lies in $\mathcal{P}$. Among other things, $\mathcal{P}_{\mathrm{arith}}$ contains perverse sheaves $\mathcal{F}[1]$ for $\mathcal{F}$ a geometrically simple middle-extension sheaf on $\mathbb{G}_m$ over $\mathbb{F}_q$ which is of generic rank at least two.

Once again we have the two flavors of multiplicative convolution

$$M \star_! N := R\pi_!(M \boxtimes N), \quad M \star_* N := R\pi_*(M \boxtimes N).$$

for any pair of objects M, N in $\mathrm{Perv}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$. We can also define middle convolution on $\mathcal{P}_{\mathrm{arith}}$ as before

$$M *_{\mathrm{mid}} N := \mathrm{Image}(M \star_! N \to M \star_* N).$$

for any pair of objects M, N in $\mathcal{P}_{\mathrm{arith}}$.

Proposition D.6.1. *If M and N are ι-pure of weights m and n respectively, then $M *_{\mathrm{mid}} N$ is ι-pure of weight $m + n$.*

Proof. Our argument is essentially that of [Kat12, Ch. 4]. On one hand, $M \boxtimes N$ is ι-pure of weight $m + n$ on $\mathbb{G}_m \times \mathbb{G}_m$, hence [Del80, 3.3.1] and Proposition D.3.1 imply $M \star_! N$ and its perverse quotient $M *_{\mathrm{mid}} N$ are ι-mixed of weight $m + n$. On the other hand, DM and DN are ι-pure of weights m and n respectively, and

$$\begin{aligned} D(M *_{\mathrm{mid}} N) &= \mathrm{Image}(D(M \star_* N) \to D(M \star_! N)) \\ &= \mathrm{Image}(DM \star_! DN \to DM \star_* DN) \quad = \quad DM *_{\mathrm{mid}} DN \end{aligned}$$

hence $D(M *_{\mathrm{mid}} N)$ is ι-mixed weights $\leq m+n$ (cf. [Del80, 6.2]). Thus $M *_{\mathrm{mid}} N$ is ι-pure of weight $m+n$ as claimed. $\square$

D.7. **The category** $\mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$**.** Gabber and Loeser defined an object M in $\mathrm{Perv}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$ to be *negligible* iff its Euler characteristic $\chi(\bar{\mathbb{G}}_m, M)$ vanishes (see [GL96, pg. 529]), or equivalently, it is isomorphic to a successive extension of shifted Kummer sheaves $\mathcal{L}_\rho[1]$ (cf. [GL96, 3.5.3]). They showed that the full subcategory $\mathrm{Negl}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$ of $\mathrm{Perv}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$ whose objects are the negligible sheaves is a thick subcategory of the abelian category (see [GL96, 3.5.2]), and thus one can speak of the quotient category

$$\mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell) := \mathrm{Perv}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)/\mathrm{Negl}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell).$$

They then proceeded to show that $\mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$ is a neutral Tannakian category (see [GL96, 3.7.5] and [DMOS82, II.2.19]).

Theorem D.7.1. *The composite map $\mathcal{P} \to \mathrm{Perv}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell) \to \mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$ induces an equivalence of categories such that:*

(i) middle convolution on $\mathcal{P}$ induces a tensor product $\otimes$ on $\mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$;

(ii) the unit object $\mathbf{1}$ corresponds to the skyscraper sheaf $i_*\bar{\mathbb{Q}}_\ell$ for $i\colon \{1\} \to \bar{\mathbb{G}}_m$ the inclusion;

(iii) the dual $M^\vee$ of an object M is the object $[x \mapsto 1/x]^* DM$;

(iv) the dimension $\dim(M)$ of an object M is $\chi(\bar{\mathbb{G}}_m, M)$;

(v) a fiber functor is $M \mapsto H^0(\bar{\mathbb{A}}^1_u, j_{0!}M)$ for $j_0\colon \mathbb{G}_m \to \mathbb{A}^1_u$ the inclusion.

See [GL96, 3.7.2] and [Kat12, Ch. 2 and Ch. 3].

D.8. **The category** $\mathrm{Tann}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$**.** Let $\mathrm{Negl}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ be the full subcategory of $\mathrm{Perv}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ whose objects M are those for which $\bar{M}$ lies in $\mathrm{Negl}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$, and let

$$\mathrm{Tann}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell) := \mathrm{Perv}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)/\mathrm{Negl}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell).$$

Like $\mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$, the quotient category is an abelian category and even a neutral Tannakian category with tensor product $\otimes$ given by middle convolution. Moreover, the "extension of scalars" functor induces a functor

$$\mathrm{Tann}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell) \to \mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$$

which also call the "extension of scalars" functor.

Proposition D.8.1. *Suppose $M, N \in \mathrm{Tann}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ are ι-pure of weights m and n respectively. Then $M^\vee$, $N^\vee$, and $M \otimes N$ are ι-pure of weights m, n, and $m+n$ respectively.*

Proof. The Verdier duals DM and DN are ι-pure of weights m and n respectively, hence so are the Tannakian duals $M^\vee = [x \mapsto 1/x]^* DM$ and $N^\vee = [x \mapsto 1/x]^* DN$. Moreover, Proposition D.6.1 implies that $M \otimes N = M *_{\mathrm{mid}} N$ is ι-pure of weight $m+n$. $\square$

D.9. **Semisimple abelian categories.** We say that M is *simple* iff the only subobjects $N \subseteq M$ in $\mathcal{C}$ are isomorphic to $\mathbf{0}$ or M. More generally, we say that M is *semisimple* iff it is isomorphic to a finite direct sum $N_1 \oplus \cdots \oplus N_m$ of simple subobjects $N_1, \ldots, N_m \subseteq M$. We say that $\mathcal{C}$ is *semisimple* iff each of its objects is semisimple.

Proposition D.9.1. *If $M \in \mathrm{Tann}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ is ι-pure of weight zero, then $\langle \bar{M} \rangle$ is semisimple.*

Proof. If $N_1, N_2 \in \mathrm{Tann}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ are ι-pure of weight zero, then so is $N_1 \oplus N_2$. Therefore Proposition D.6.1 implies that $T^{a,b}(M)$ is pure of weight zero, for every $a, b \geq 0$, and [BBD82, 5.3.8] implies that $T^{a,b}(\bar{M})$ is semisimple. $\square$

D.10. **Tannakian monodromy group.** Let k be an algebraically closed field of characteristic zero and $\mathbf{Vec}_k$ be the category of finite-dimensional vector spaces over k. It is well known that the latter yields a rigid abelian tensor category $(\mathbf{Vec}_k, \otimes)$ with respect to the usual operators $\oplus$ and $\otimes$ of vector spaces and with unit object $\mathbf{1} = k$.

Let $(\mathcal{C}, \otimes)$ be a neutral Tannakian category over k. Thus $(\mathcal{C}, \otimes)$ is a rigid abelian tensor category whose unit object $\mathbf{1}$ satisfies $k = \mathrm{End}(\mathbf{1})$ and for which there exists a fiber functor ω, that is, an exact faithful k-linear tensor functor $\omega \colon \mathcal{C} \to \mathbf{Vec}_k$. For example, $\mathbf{Vec}_k$ is a neutral Tannakian category and the identity functor $\mathbf{Vec}_k \to \mathbf{Vec}_k$ is a fiber functor. More generall, given an affine group scheme G over k, the category $\mathbf{Rep}_k(G)$ of linear representations of G on finite-dimensional k-vector spaces yields a neutral Tannakian category $(\mathbf{Rep}_k(G), \otimes)$, and the forgetful functor $\mathbf{Rep}_k(G) \to \mathbf{Vec}_k$ is a fiber functor.

Given an object M of $\mathcal{C}$, its dual $M^\vee$, and non-negative integers a, b, let

$$T^{a,b}(M) := M^{\otimes a} \oplus (M^\vee)^{\otimes b}$$

and let $\langle M \rangle$ be the full tensor subcategory of $\mathcal{C}$ whose objects consist of all subobjects of $T^{a,b}(M)$ for all $a, b \geq 0$. For each automorphism $\gamma \in \mathrm{Aut}_{\mathcal{C}}(M)$, let $\gamma^\vee \in \mathrm{Aut}_{\mathcal{C}}(M^\vee)$ be the corresponding dual automorphism and $T^{a,b}(\gamma) \in \mathrm{Aut}_{\mathcal{C}}(T^{a,b}(M))$ be the induced automorphism.

Let $\mathbf{Alg}_k$ be the category of k-algebras and $\mathbf{Set}$ be the category of sets. Given a pair ω_1, ω_2 of fiber functors $\mathcal{C} \to \mathbf{Vec}_k$ and an object M in $\mathcal{C}$, one can define a functor

$$\underline{\mathrm{Isom}}^{\otimes}(\omega_1|M, \omega_2|M) \colon \mathbf{Alg}_k \to \mathbf{Set}$$

by sending a k-algebra R to the set

$$\{\, \gamma \in \mathrm{Isom}_R(\omega_1(M)_R, \omega_2(M)_R) : T^{a,b}(\gamma)(\omega_1(N)) \subseteq \omega_2(N) \text{ for all } a, b \geq 0 \text{ and } N \subseteq T^{a,b}(M) \,\}$$

where $\omega_i(M)_R = \omega_i(M) \otimes_k R$ and

$$\mathrm{Isom}_R(\omega_1(M)_R, \omega_2(M)_R) = \{\, \gamma \in \mathrm{Hom}_R(\omega_1(M)_R, \omega_2(M)_R) : \gamma \text{ is invertible } \}.$$

Similarly, given a single fiber functor $\omega \colon \mathcal{C} \to \mathbf{Vec}_k$ and object M in $\mathcal{C}$, one can define a functor

$$\underline{\mathrm{Aut}}^{\otimes}(\omega|M) \colon \mathbf{Alg}_k \to \mathbf{Set}$$

as the functor $\underline{\mathrm{Isom}}^{\otimes}(\omega|M, \omega|M)$.

Theorem D.10.1. *Let ω_1, ω_2 be fiber functors $\mathcal{C} \to \mathbf{Vec}_k$ and M be an object of $\mathcal{C}$.*

(i) $\underline{\mathrm{Aut}}^{\otimes}(\omega_i|M)$ is representable by an algebraic group scheme $G_{\omega_i|M}$ over k;

(ii) if $\langle M \rangle$ is semisimple, then $G_{\omega_i|M}$ is reductive;

(iii) $\underline{\mathrm{Isom}}^{\otimes}(\omega_1|M, \omega_2|M)$ is represented by an affine scheme over k which is a $G_{\omega_1|M}$-torsor;

See [DMOS82, II.2.11, II.2.20, II.2.28, and II.3.2].

We call the group scheme $G_{\omega_i|M}$ in the theorem the *Tannakian monodromy group* of $\langle M \rangle$ with respect to ω_i.

Theorem D.10.2. *Let $\omega \colon \mathrm{Perv}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell) \to \mathbf{Vec}_k$ be a fiber functor over $\bar{\mathbb{F}}_q$ and $M \in \mathrm{Perv}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$. If M is pure of weight zero, then $G_{\omega|\bar{M}}$ is reductive.*

Proof. This follows from Proposition D.9.1 and Theorem D.10.1.ii. $\square$

D.11. **Geometric versus arithmetic monodromy.** For every object M in $\mathrm{Tann}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ and all integers $a, b \geq 0$, the "extension of scalars" functor sends a subobject $N \subseteq T^{a,b}(M)$ to a subobject $\bar{N} \subseteq T^{a,b}(\bar{M})$. Moreover, composing the functor with a fiber functor ω on $\mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell)$ yields a fiber functor on $\mathrm{Tann}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$ which we also denote ω. Thus there is a natural transformation

$$\underline{\mathrm{Aut}}^{\otimes}(\omega|\bar{M}) \to \underline{\mathrm{Aut}}^{\otimes}(\omega|M)$$

and a corresponding monomorphism of Tannakian monodromy groups

$$G_{\omega|\bar{M}} \to G_{\omega|M}.$$

We call $G_{\omega|\bar{M}}$ and $G_{\omega|M}$ the *geometric* and *arithmetic Tannakian monodromy groups* of M with respect to ω respectively.

Proposition D.11.1. *Suppose M is in* $\mathrm{Tann}(\mathbb{G}_m/\mathbb{F}_q, \bar{\mathbb{Q}}_\ell)$ *and is pure of weight zero.*

(i) $G_{\omega|\bar{M}}$ is a normal subgroup of $G_{\omega|M}$

(ii) If M is arithmetically semisimple, then $G_{\omega|M}/G_{\omega|\bar{M}}$ is a torus, and thus $G_{\omega|M}$ is reductive.

Proof. Proposition D.9.1 implies that $\bar{M}$ is semisimple, so part (1) follows from [Kat12, Th. 6.1]. Therefore we can speak of the quotient $G_{\omega|M}/G_{\omega|\bar{M}}$, and [Kat12, Lem. 7.1] implies it is a quotient of M is arithmetically semisimple. Moreover, Proposition D.10.2 implies that $G_{\omega|\bar{M}}$ is reductive, so part (2) follows by observing that the extension of a torus by a reductive group is reductive. □

D.12. **Frobenius element.** Let ω be a fiber functor $\mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell) \to \mathbf{Vec}_k$, let $E/\mathbb{F}_q$ be a finite extension, and let M be in $\mathrm{Tann}(\mathbb{G}_m/E, \bar{\mathbb{Q}}_\ell)$. The geometric Frobenius element of $\mathrm{Gal}(\bar{\mathbb{F}}_q/E)$ induces a well-defined automorphism ϕ_E of $\bar{M}$. By applying ω, one obtains a well-defined k-linear automorphism of $\omega(\bar{M})$, that is, an element of $\mathrm{GL}(\omega(\bar{M})) = \mathrm{GL}(\omega(M))$. It is even an element of $G_{\omega|M}$ since, for every $N \subseteq T^{a,b}(M)$ and $a, b \geq 0$, one has

$$\bar{N} = T^{a,b}(\phi_E)(\bar{N}) \subseteq T^{a,b}(\bar{M})$$

and thus

$$\omega(\bar{N}) = T^{a,b}(\phi_E)(\omega(\bar{N})) \subseteq \omega(T^{a,b}(\bar{M})) = T^{a,b}(\omega(M)).$$

We call $\omega(\phi_E)$ the *geometric Frobenius element* of $G_{\omega|M}$.

D.13. **Frobenius conjugacy classes.** Let ω_1, ω_2 be fiber functors $\mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell) \to \mathbf{Vec}_k$, let M be an element of $\mathrm{Tann}(\mathbb{G}_m, \bar{\mathbb{Q}}_\ell)$, and let π be an element of $\underline{\mathrm{Isom}}^{\otimes}(\omega_1|M, \omega_2|M)(k)$. Then Theorem D.10.1.iii implies that the map $g \mapsto \pi g$ induces a bijection

$$G_{\omega_1|M} \to \underline{\mathrm{Isom}}^{\otimes}(\omega_1|M, \omega_2|M).$$

Moreover, the map $g_2 \mapsto g_2^{\pi} = \pi^{-1} g_2 \pi$ induces an isomorphism $G_{\omega_2|M} \to G_{\omega_1|M}$. While the map is not canonical (since π is not), the conjugacy class

$$\mathrm{Frob}_{\omega_2|M} = \{\, \omega_2(\phi)^{\pi g_1} : g_1 \in G_{\omega_1|M}(k) \,\} \subset G_{\omega_1|M}(k)$$

is well defined. We call it the *geometric Frobenius conjugacy class* of $\omega_2|M$ in $G_{\omega_1|M}$.

For each finite extension $E/\mathbb{F}_q$ and each character $\rho \in \Phi_E(u)$, let $\mathcal{L}_\rho$ be the corresponding Kummer sheaf on $\mathbb{G}_m$ over E and $\omega_\rho \colon \mathrm{Tann}(\bar{\mathbb{G}}_m, \bar{\mathbb{Q}}_\ell) \to \mathbf{Vec}_k$ be the functor given by

$$M \mapsto H^0(\bar{\mathbb{A}}^1_u, j_{0!}(M \otimes \mathcal{L}_\rho)).$$

It is a fiber functor by [Kat12, 3.2], and $\omega_{\mathbf{1}}$ is the fiber functor of Theorem D.7.1.v. We write

$$\mathrm{Frob}_{E,\rho} \subset G_{\omega_{\mathbf{1}}|M}$$

for the corresponding geometric Frobenius conjugacy class of $\omega_\rho|M_E$ where $M_E = M \times_{\mathbb{F}_q} E$.

Let $m = \dim(\omega_\rho(M))$ and $n \in \{0, 1, \ldots, m\}$. We say that $\omega_\rho(M)$ is *mixed of weights* $w_1, \ldots, w_m$ iff there exists an eigenvector tuple $\alpha = (\alpha_1, \ldots, \alpha_m) \in (\bar{\mathbb{Q}}_\ell^\times)^m$ of any element of $\mathrm{Frob}_{E,\rho}$ such that $\alpha \in (\bar{\mathbb{Q}}^\times)^m$ and such that

$$|\iota(\alpha_i)|^2 = (1/|E|)^{w_i} \text{ for } 1 \leq i \leq m$$

for every field embedding $\iota\colon \bar{\mathbb{Q}} \to \mathbb{C}$. We also say that $\omega_\rho(M)$ is *mixed of non-zero weights* $w_1, \ldots, w_n$ iff it is mixed of weights $w_1, \ldots, w_m$ with $w_{n+1} = \cdots = w_m = 0$.

D.14. **Monodromy for pure middle-extension sheaves.** Let $U \subseteq \mathbb{G}_m$ be a dense Zariski open subset over $\mathbb{F}_q$. Let $\theta\colon \pi_1(U) \to \mathrm{GL}(W)$ be a continuous representation to a finite-dimensional $\bar{\mathbb{Q}}_\ell$-vector space W and $\mathcal{F}$ be the restriction to $\mathbb{G}_m$ of the associated middle-extension sheaf $\mathrm{ME}(\theta)$ on $\mathbb{P}^1_u$. Suppose that θ is pointwise pure of weight w so that $M = \mathcal{F}((1+w)/2)[1]$ is pure of weight zero. Suppose moreover that θ is geometrically simple and that it does not factor through the composed quotient $\pi_1(U) \twoheadrightarrow \pi_1(\mathbb{G}_m) \twoheadrightarrow \pi_1^{\mathrm{t}}(\mathbb{G}_m)$ so that M lies in $\mathcal{P}_{\mathrm{arith}}$.

Let $\Phi(u)$ be the dual of $\Gamma(u) = (\mathbb{F}_q[u]/u\mathbb{F}_q[u])^\times$ (cf. §10.2). We define the *geometric* and *arithmetic Tannakian monodromy groups* of (the Mellin transformation of) θ to be

$$\mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u)) := G_{\boldsymbol{\omega_1}|\bar{M}}, \quad \mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u)) := G_{\boldsymbol{\omega_1}|M}.$$

For $u = 0, \infty$, let $W(u)$ denote W regarded as an $I(u)$-module, and let $W(u)^{\mathrm{unip}}$ be the maximal submodule of $W(u)$ where $I(u)$ acts unipotently. Moreover, let $e_{u,1}, \ldots, e_{u,d_u}$ be positive integers integers satisfying

$$W(u)^{\mathrm{unip}} \simeq U(e_{u,1}) \oplus \cdots \oplus U(e_{u,d_u})$$

as $I(u)$-modules where $U(e)$ denotes the irreducible e-dimensional $I(u)$-module on which $I(u)$ acts unipotently.

Proposition D.14.1.

(i) The groups $\mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u))$ and $\mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u))$ are reductive, and there is an exact sequence

$$1 \to \mathcal{G}_{\mathrm{geom}}(\theta, \Phi(u)) \to \mathcal{G}_{\mathrm{arith}}(\theta, \Phi(u)) \to T \to 1$$

for some torus T over $\bar{\mathbb{Q}}_\ell$.

(ii) For each finite extension $E/\mathbb{F}_q$ and each $\alpha \in \Phi_E(u)$, the stalk $\omega_\rho(M)$ is mixed of non-zero weights $-e_{0,1}, \ldots, -e_{0,d_0}, e_{\infty,1}, \ldots, e_{\infty,d_\infty}$.

Proof. Part (1) follows from Proposition D.11.1, and part (2) follows from [Kat12, Th. 16.1]. ☐

References

[BBD82] A. A. Beĭlinson, J. Bernstein, and P. Deligne, *Faisceaux pervers*, Analysis and topology on singular spaces, I (Luminy, 1981), 1982, pp. 5–171. MR751966 ↑7.2, D.3, D.9

[BKS16] H. M. Bui, J. P. Keating, and D. J. Smith, *On the variance of sums of arithmetic functions over primes in short intervals and pair correlation for L-functions in the Selberg class*, J. Lond. Math. Soc. (2) **94** (2016), no. 1, 161–185. MR3532168 ↑1.1, 1.1

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 ↑11.1, 12.1

[Car85] Roger W. Carter, *Finite groups of Lie type*, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication. MR794307 ↑11.2

[CFA+06] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. MR2162716 ↑12.1

[CFZ08] Brian Conrey, David W. Farmer, and Martin R. Zirnbauer, *Autocorrelation of ratios of L-functions*, Commun. Number Theory Phys. **2** (2008), no. 3, 593–636. MR2482944 ↑1.1

[Cha03] Tsz Ho Chan, *More precise pair correlation of zeros and primes in short intervals*, J. London Math. Soc. (2) **68** (2003), no. 3, 579–598. MR2009438 ↑1.1

[CR06] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original. MR2215618 ↑7.1, 11.4

[CS07] J. B. Conrey and N. C. Snaith, *Applications of the L-functions ratios conjectures*, Proc. Lond. Math. Soc. (3) **94** (2007), no. 3, 594–646. MR2325314 ↑1.1

[DE01] Persi Diaconis and Steven N. Evans, *Linear functionals of eigenvalues of random matrices*, Trans. Amer. Math. Soc. **353** (2001), no. 7, 2615–2633. MR1828463 ↑9.0.3, 1

[Del77] P. Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, Vol. 569, Springer-Verlag, Berlin-New York, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. MR0463174 ↑2, 2, 3.6, 11.4, 11.4

[Del80] Pierre Deligne, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252. MR601520 ↑6.2, 6.3, 11.4, D.6

[DMOS82] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin-New York, 1982. MR654325 ↑D.7, D.10

[DS94] Persi Diaconis and Mehrdad Shahshahani, *On the eigenvalues of random matrices*, J. Appl. Probab. **31A** (1994), 49–62. Studies in applied probability. MR1274717 ↑1

[FG96] J. B. Friedlander and D. A. Goldston, *Variance of distribution of primes in residue classes*, Quart. J. Math. Oxford Ser. (2) **47** (1996), no. 187, 313–336. MR1412558 ↑1.1

[GL96] Ofer Gabber and François Loeser, *Faisceaux pervers l-adiques sur un tore*, Duke Math. J. **83** (1996), no. 3, 501–606. MR1390656 ↑D.7, D.7

[GM87] Daniel A. Goldston and Hugh L. Montgomery, *Pair correlation of zeros and primes in short intervals*, Analytic number theory and Diophantine problems (Stillwater, OK, 1984), 1987, pp. 183–203. MR1018376 ↑1.1, 1.1

[Gro72] Alexander Grothendieck, *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, Berlin-New York, 1972. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Avec la collaboration de M. Raynaud et D. S. Rim. MR0354656 ↑12.2

[Hal08] Chris Hall, *Big symplectic or orthogonal monodromy modulo l*, Duke Math. J. **141** (2008), no. 1, 179–203. MR2372151 (2008m:11112) ↑12.2

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 ↑12.1

[Hoo74] C. Hooley, *On the Barban-Davenport-Halberstam theorem. II*, J. London Math. Soc. (2) **9** (1974/75), 625–636. MR0382203 ↑1.1

[Hoo75a] C. Hooley, *The distribution of sequences in arithmetic progressions* (1975), 357–364. MR0498441 ↑1.1

[Hoo75b] Christopher Hooley, *On the Barban-Davenport-Halberstam theorem. I*, J. Reine Angew. Math. **274/275** (1975), 206–223. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III. MR0382202 ↑1.1

[Kat02] Nicholas M. Katz, *Twisted L-functions and monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, NJ, 2002. ↑10.2, 11.6, 11.8, 11.8, C.4, C.4

[Kat03] Nicholas M. Katz, *A semicontinuity result for monodromy under degeneration*, Forum Math. **15** (2003), no. 2, 191–200. MR1956963 ↑

[Kat12] Nicholas M. Katz, *Convolution and equidistribution*, Annals of Mathematics Studies, vol. 180, Princeton University Press, Princeton, NJ, 2012. Sato-Tate theorems for finite-field Mellin transforms. MR2850079 ↑1.1, 1.5, 8.1, 10.3, 10.3, 10.5, 11.0.2, 11.1, 11.7, 11.7, D.5, D.6, D.7, D.11, D.13, D.14

[Kat13] Nicholas M. Katz, *On a question of Keating and Rudnick about primitive Dirichlet characters with squarefree conductor*, Int. Math. Res. Not. IMRN **14** (2013), 3221–3249. MR3085758 ↑10.2, 11.0.3, 11.9

[Kat88] Nicholas M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, vol. 116, Princeton University Press, Princeton, NJ, 1988. MR955052 ↑3.5, 12

[Kat96] Nicholas M. Katz, *Rigid local systems*, Annals of Mathematics Studies, vol. 139, Princeton University Press, Princeton, NJ, 1996. ↑11.4, D.5

[KR14] Jonathan P. Keating and Zeév Rudnick, *The variance of the number of prime polynomials in short intervals and in residue classes*, Int. Math. Res. Not. IMRN **1** (2014), 259–288. MR3158533 ↑1.1, 1.1, 1.1, 1.1

[KR16] Jonathan Keating and Zeev Rudnick, *Squarefree polynomials and Möbius values in short intervals and arithmetic progressions*, Algebra Number Theory **10** (2016), no. 2, 375–420. MR3477745 ↑1.1

[KRG16] Jonathan P. Keating and Edva Roditty-Gershon, *Arithmetic correlations over large finite fields*, Int. Math. Res. Not. IMRN **3** (2016), 860–874. MR3493436 ↑1.1

[KRRGR18] J. P. Keating, B. Rodgers, E. Roditty-Gershon, and Z. Rudnick, *Sums of divisor functions in $\mathbb{F}_q[t]$ and matrix integrals*, Math. Z. **288** (2018), no. 1-2, 167–198. MR3774409 ↑1.1

[KS99] Nicholas M. Katz and Peter Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999. MR1659828 (2000b:11070) ↑12.2

[LPZ12] Alessandro Languasco, Alberto Perelli, and Alessandro Zaccagnini, *Explicit relations between pair correlation of zeros and primes in short intervals*, J. Math. Anal. Appl. **394** (2012), no. 2, 761–771. MR2927496 ↑1.1

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR559531 ↑2, 3.3, 10.1, 10.1, 11.9, 11.10, A, A

[Mon70] H. L. Montgomery, *Primes in arithmetic progressions*, Michigan Math. J. **17** (1970), 33–39. MR0257005 ↑1.1

[Mon73] H. L. Montgomery, *The pair correlation of zeros of the zeta function* (1973), 181–193. MR0337821 ↑1.1

[MS04] Hugh L. Montgomery and K. Soundararajan, *Primes in short intervals*, Comm. Math. Phys. **252** (2004), no. 1-3, 589–617. MR2104891 ↑1.1

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen. MR1278263 ↑11.2

[Ray95] Michel Raynaud, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*, Séminaire Bourbaki, Vol. 9, 1995, pp. Exp. No. 286, 129–147. MR1608794 ↑B.1

[RG17] E. Roditty-Gershon, *Square-full polynomials in short intervals and in arithmetic progressions*, Res. Number Theory **3** (2017), 3:3. MR3597214 ↑1.1

[Rod] Brad Rodgers, *Arithmetic functions in short intervals and the symmetric group*, arXiv:1609.02967. ↑1.1

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657 ↑11.3

[Rud14] Zeev Rudnick, *Some problems in analytic number theory for polynomials over a finite field* (2014). ↑1.1

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR0236190 (38 #4488) ↑12.2

[Zar90] Yu. G. Zarhin, *Linear simple Lie algebras and ranks of operators*, The Grothendieck Festschrift, Vol. III, 1990, pp. 481–495. MR1106920 ↑C.4

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF WESTERN ONTARIO, LONDON, ON, CANADA, N6A 5B7

SCHOOL OF MATHEMATICS, UNIVERSITY OF BRISTOL, BRISTOL BS8 1TW, UK

SCHOOL OF MATHEMATICS, UNIVERSITY OF BRISTOL, BRISTOL BS8 1TW, UK