ON ZETA FUNCTIONS OF MODULAR REPRESENTATIONS OF A DISCRETE GROUP

Harada, Shinya
Graduate School of Mathematics, Kyushu University

Moon, Hyunsuk
Department of Mathematics College of Natural Sciences, Kyungpook National University

出版情報：Kyushu University Preprint Series in Mathematics, 2007. 九州大学大学院数理学研究院
バージョン：
権利関係：

ON ZETA FUNCTIONS OF MODULAR REPRESENTATIONS OF A DISCRETE GROUP

SHINYA HARADA AND HYUNSUK MOON

Abstract. It is proved that the generating function defined by the numbers of isomorphism classes of absolutely irreducible representations of a finitely generated group G into $\mathrm{GL}_d(\mathbb{F}_{q^n})$ for various $n \geq 1$ is a rational function. It is also proved that the generating function defined by weighted sums over isomorphism classes of representations of G into $\mathrm{GL}_d(\mathbb{F}_{q^n})$ for various $n \geq 1$ is meromorphic over both the complex numbers and the p-adic complex numbers.

0. Introduction

Let G be a finitely generated group, $\mathbb{F}_q$ the finite field of q elements of characteristic p, and $\mathbb{F}_{q^n}$ the finite extension field of $\mathbb{F}_q$ of degree n. In this paper we study the *zeta functions*

$$Z(G,T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} T^n\right),$$

where the rational number N_n is the "mass" of the set of a certain class of representations $\rho : G \to \mathrm{GL}_d(\mathbb{F}_{q^n})$. By definition, $Z(G,T)$ is a formal power series with coefficients in $\mathbb{Q}$. We are interested in their rationality and meromorphy. If N_n is the number of all representations $\rho : G \to \mathrm{GL}_d(\mathbb{F}_{q^n})$ (for fixed G, d and q), then it is easy to prove the rationality of $Z(G,T)$ by reducing to the Weil conjecture (Theorem 1.1). The next and most natural case to consider will be the case where N_n is the number of isomorphism classes of all representations of G into $\mathrm{GL}_d(\mathbb{F}_{q^n})$, but this seems rather difficult. Instead, we first look at the absolutely irreducible representations. Here, we say that a representation $\rho : G \to \mathrm{GL}_d(\mathbb{F}_{q^n})$ is *absolutely irreducible* if the composite homomorphism $G \xrightarrow{\rho} \mathrm{GL}_d(\mathbb{F}_{q^n}) \to \mathrm{GL}_d(\overline{\mathbb{F}}_q)$ is irreducible, where $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$. Our first main result is the following:

2000 *Mathematics Subject Classification.* Primary 20C20; Secondary 14G10, 14N10, 11M41.

Key words and phrases. Zeta functions, modular representations.

Theorem 1 (Theorem 2.1)**.** *Let N_n^{ai} be the number of isomorphism classes of absolutely irreducible representations $\rho : G \to \mathrm{GL}_d(\mathbb{F}_{q^n})$. Then the power series*

$$Z_{\mathrm{ai}}(G,T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n^{\mathrm{ai}}}{n} T^n\right)$$

is a rational function in T.

This is proved in Section 2 by employing the theory of Procesi ([P]) concerning absolutely irreducible representations of a (non-commutative) ring into Azumaya algebras.

Another main result is on the zeta functions defined by the weighted sums of isomorphism classes of representations (Section 3). In this case we cannot expect in general that they are rational (for example, see Section 5). However, by considering them as functions in T on the complex plane or the p-adic complex plane, we prove the following result.

Theorem 2 (Theorem 3.1, Corollary 3.4)**.** *Put*

$$N_n^{\mathrm{wt}} := \sum_{\rho \in \mathrm{Hom}\,(G, \mathrm{GL}_d(\mathbb{F}_{q^n}))/\sim} \frac{1}{|\mathrm{Aut}\,(\rho)|},$$

where

$$\mathrm{Aut}\,(\rho) = \{M \in \mathrm{GL}_d(\mathbb{F}_{q^n}) \mid M\rho M^{-1} = \rho\}.$$

Then the power series

$$Z_{\mathrm{wt}}(G,T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n^{\mathrm{wt}}}{n} T^n\right)$$

is p-adically meromorphic on the p-adic complex plane $\mathbb{C}_p$ in the sense of Subsection 3.1*. Also, as a complex valued function, it converges in some neighborhood of $T = 0$, and is continued meromorphically to the whole complex plane $\mathbb{C}$.*

In the p-adic case, this is proved by showing that our $Z_{\mathrm{wt}}(G,T)$ is in fact an infinite product of rational functions which are essentially the zeta function in Theorem 1.1. In the complex case, we employ Behrend's trace formula ([Be]) for algebraic stacks to show the meromorphy.

Dwork proved the rationality of the congruence zeta functions ([D, Theorem 2]) by using a criterion for a formal power series to be a rational function when it is known to be meromorphic both over $\mathbb{C}$ and $\mathbb{C}_p$. It would be interesting to find a sufficient condition for G which implies the rationality of $Z_{\mathrm{wt}}(G,T)$.

In Section 4, we prove the rationality of another type of zeta function $Z_{\mathrm{Ig}}(G,T)$ (Proposition 4.1), which is the generating function defined by the numbers N_n^{Ig} of representations of G into the general linear group with coefficients in $\mathbb{Z}/p^n\mathbb{Z}$ in place of the finite field $\mathbb{F}_{q^n}$.

Although we do not treat the case, there is one more type of zeta function of representations of G. That is, in place of varying the degree n of the finite field $\mathbb{F}_{q^n}$, we vary the degree d of the general linear group $\mathrm{GL}_d(\mathbb{F}_q)$. In this direction, Chigira, Takegahara and Yoshida studied in [CTY] the generating function $1+\left(\sum_{d=1}^{\infty}|\mathrm{Hom}\,(G,\mathrm{GL}_d(\mathbb{F}_q))|T^d/|\mathrm{GL}_d(\mathbb{F}_q)|\right)$ of a finite group G and obtained interesting results on it.

Now we explain the motivation of this paper. In [M1], [MT1] and [MT2], the finiteness was investigated for the number of isomorphism classes of semisimple representations of the absolute Galois group G_K of an algebraic number field K into $\mathrm{GL}_d(\overline{\mathbb{F}}_p)$. Also, in [H], the first author studied the finiteness of mod p Galois representations of a local field. In [M2], an effective upper bound was given for the number of isomorphism classes of monomial mod p Galois representations with given Artin conductor. Thus we hope next to know more precise behavior of such numbers. However, it seems difficult to do that in general for profinite groups such as the absolute Galois group G_K. In this paper we attempt, as a first approximation, to do the same for a discrete group instead of a profinite group.

Our zeta functions may be used to define some invariants of certain geometric objects such as topological manifolds, knots (or links) and proper algebraic varieties over an algebraically closed field of characteristic zero as follows. For these objects X, their fundamental groups $\pi_1 = \pi_1(X)$ (or $\pi_1(S^3 \setminus X)$ if X is a knot or a link in the 3-sphere S^3) are defined, which are either finitely generated discrete groups or their profinite completions. Thus we may define a zeta function of X to be $Z(\pi_1, T)$ (or $Z(G,T)$ if π_1 is the profinite completion of a discrete group G). In the case of knots, Sink ([S]) has studied such zeta functions but of representations into $\mathrm{SL}_d(\mathbb{F}_{q^n})$ instead of $\mathrm{GL}_d(\mathbb{F}_{q^n})$.

Notation

Throughout this paper, G is an arbitrary finitely generated group. Denote by $\mathbb{F}_q$ the finite field of q elements, where q is a power of a prime number p. For a finite set S, its order is denoted by $|S|$ or $\sharp S$.

1. Rationality of $Z_{\mathrm{hom}}(G,T)$

Here we review the case where $N_n = N_n^{\mathrm{hom}}$ is the number of representations $\rho : G \to \mathrm{GL}_d(\mathbb{F}_{q^n})$. Since G is finitely generated, there exists an affine scheme $X_d(G)$ of finite type over $\mathbb{Z}$ such that $\mathrm{Hom}\,(G,\mathrm{GL}_d(R)) \simeq X_d(G)(R)$ for any commutative ring R (cf. [P, §1]). Then we can interpret N_n^{hom} as the number of $\mathbb{F}_{q^n}$-rational points of $X_d(G)$, and hence our zeta function

$Z_{\mathrm{hom}}(G,T) = \exp\left(\sum_{n=1}^{\infty} N_n^{\mathrm{hom}} T^n/n\right)$ is nothing but the congruence zeta function $Z(X_d(G),T) = \exp\left(\sum_{n=1}^{\infty} \sharp X_d(G)(\mathbb{F}_{q^n})T^n/n\right)$ of $X_d(G)$. By the work [D] of Dwork, this is known to be a rational function in T. Thus we have the following.

Theorem 1.1. *Let N_n^{hom} be the cardinality of* $\mathrm{Hom}\,(G, \mathrm{GL}_d(\mathbb{F}_{q^n}))$. *Then the power series*

$$Z_{\mathrm{hom}}(G,T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n^{\mathrm{hom}}}{n} T^n\right)$$

is a rational function in T.

2. Rationality of $Z_{\mathrm{ai}}(G,T)$

In this section we prove Theorem 2.1. Before that, we recall some notions in algebra. Let A be a commutative ring. We say that an A-algebra S is an *Azumaya algebra of degree d* if the following conditions are satisfied:

(1) S is a finitely generated projective A-module of rank d^2,
(2) the natural homomorphism $S \otimes_A S^\circ \to \mathrm{End}_A(S)$ given by $s \otimes s' \longmapsto (t \mapsto sts'^{-1})$, is an isomorphism,

where S° is the opposite ring of S. For example, the total matrix algebra $\mathrm{M}_d(A)$ is an Azumaya algebra of degree d over A. If A is a field, an Azumaya algebra over A is just a central simple algebra over A.

Let R be a (non-commutative) ring. Let S be an Azumaya algebra of degree d over A. A ring homomorphism $\rho : R \to S$ is called *absolutely irreducible* of degree d over A, if S is generated by $\mathrm{Im}(\rho)$ as an A-module. Two absolutely irreducible representations $\rho_1 : R \to S_1$ and $\rho_2 : R \to S_2$ over A are *equivalent* if there exists an A-algebra isomorphism $f : S_1 \to S_2$ such that $\rho_2 = f \circ \rho_1$.

Theorem 2.1. *Let N_n^{ai} be the number of isomorphism classes of absolutely irreducible representations $\rho : G \to \mathrm{GL}_d(\mathbb{F}_{q^n})$. Then the power series*

$$Z_{\mathrm{ai}}(G,T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n^{\mathrm{ai}}}{n} T^n\right)$$

is a rational function in T.

Proof. Put $R = \mathbb{F}_q[G]$. Let

$$\begin{array}{rccc} \mathrm{AIr}_d(G): & (\text{Com. Rings}) & \longrightarrow & (\text{Sets}) \\ & B & \longmapsto & \mathrm{AIr}_d(G)(B) \end{array}$$

be the covariant functor from the category of commutative rings into the category of sets, which maps a commutative ring B to the set of isomorphism classes of absolutely irreducible representations of R into Azumaya algebras of degree d over B. By the theory of Procesi ([P]), there exists a scheme $U_d(G)$ of finite type over $\mathbb{Z}$ which represents $\mathrm{AIr}_d(G)$. Thus, for any commutative ring B, we have $\mathrm{AIr}_d(G)(B) = U_d(G)(B)$, where $U_d(G)(B)$ is the B-rational points of $U_d(G)$. Now we take $\mathbb{F}_{q^n}$ as B. Since the Brauer group $\mathrm{Br}(\mathbb{F}_{q^n}) = 0$ (cf. [W, Chapter 1, Theorem 1]), every Azumaya algebra of degree d over $\mathbb{F}_{q^n}$ is isomorphic to $\mathrm{M}_d(\mathbb{F}_{q^n})$ as $\mathbb{F}_{q^n}$-algebras. A representation $\rho : G \to \mathrm{GL}_d(\mathbb{F}_{q^n})$ of G induces a representation $\mathbb{F}_q[\rho] : \mathbb{F}_q[G] \to \mathrm{M}_d(\mathbb{F}_{q^n})$ of the group ring $\mathbb{F}_q[G]$. It is known that ρ is absolutely irreducible in the sense of Section 0 if and only if $\mathbb{F}_q[\rho]$ is absolutely irreducible in the above sense (cf. [Bo, §13, Proposition 5]). By the theorem of Skolem-Noether (cf. [Bo, §10, Corollaire]), every $\mathbb{F}_{q^n}$-algebra automorphism on $\mathrm{M}_d(\mathbb{F}_{q^n})$ is an inner automorphism. Thus there is a canonical bijection between the set of equivalence classes of absolutely irreducible representations of $\mathbb{F}_q[G]$ into $\mathrm{M}_d(\mathbb{F}_{q^n})$ and the set of equivalence classes of absolutely irreducible representations of G into $\mathrm{GL}_d(\mathbb{F}_{q^n})$. Hence we have

$$\mathrm{AIr}_d(G)(\mathbb{F}_{q^n}) = \left\{ \begin{array}{c} \text{isomorphism classes of absolutely} \\ \text{irreducible representations } \rho : G \to \mathrm{GL}_d(\mathbb{F}_{q^n}) \end{array} \right\}.$$

Thus the zeta function $Z_{\mathrm{ai}}(G, T)$ is equal to the congruence zeta function $Z(U_d(G), T)$ of $U_d(G)$. Hence $Z_{\mathrm{ai}}(G, T)$ is a rational function in T. □

3. Meromorphy of $Z_{\mathrm{wt}}(G, T)$

Let $\mathrm{Rep}\,(G, \mathrm{GL}_d(\mathbb{F}_{q^n}))$ be the set of isomorphism classes of representations $\rho : G \to \mathrm{GL}_d(\mathbb{F}_{q^n})$. We define

$$N_n^{\mathrm{wt}} := \sum_{\rho \in \mathrm{Rep}\,(G, \mathrm{GL}_d(\mathbb{F}_{q^n}))} \frac{1}{|\mathrm{Aut}\,(\rho)|},$$

where

$$\mathrm{Aut}\,(\rho) = \{M \in \mathrm{GL}_d(\mathbb{F}_{q^n}) \mid M\rho M^{-1} = \rho\}.$$

We define $Z_{\mathrm{wt}}(G, T)$ by the power series

$$Z_{\mathrm{wt}}(G, T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n^{\mathrm{wt}}}{n} T^n \right).$$

3.1. Meromorphy of $Z_{\mathrm{wt}}(G, T)$ over $\mathbb{C}_p$.

Let $\mathbb{C}_p$ be the completion of an algebraic closure of the p-adic number field $\mathbb{Q}_p$ and v the valuation of $\mathbb{C}_p$ normalized by $v(p) = 1$. We say that a power series $f(T)$ in $\mathbb{C}_p[\![T]\!]$ is *entire* if $f(T)$ converges on $\mathbb{C}_p$. Note that $f(T) = \sum_{n=0}^{\infty} a_n T^n$ is entire if and only if $v(a_n)/n \longrightarrow \infty$ as $n \longrightarrow \infty$. We say that a power series $f(T)$ in $\mathbb{C}_p[\![T]\!]$ is *p-adically meromorphic on* $\mathbb{C}_p$

if $f(T)$ is written in $\mathbb{C}_p[\![T]\!]$ as a quotient $g(T)/h(T)$ of entire power series $g(T)$, $h(T)$. Now we prove the following result.

Theorem 3.1. *The power series $Z_{\mathrm{wt}}(G,T)$ is p-adically meromorphic on $\mathbb{C}_p$.*

Proof. Let $\mathcal{O}(\rho)$ be the orbit of ρ by the conjugate action of $\mathrm{GL}_d(\mathbb{F}_{q^n})$. Since $|\mathrm{GL}_d(\mathbb{F}_{q^n})| = |\mathcal{O}(\rho)| \times |\mathrm{Aut}\,(\rho)|$, we have

$$\begin{aligned} N_n^{\mathrm{wt}} &= \sum_{\rho\in\mathrm{Rep}\,(G,\mathrm{GL}_d(\mathbb{F}_{q^n}))} \frac{|\mathcal{O}(\rho)|}{|\mathrm{GL}_d(\mathbb{F}_{q^n})|} \\ &= \frac{1}{|\mathrm{GL}_d(\mathbb{F}_{q^n})|} \sum_{\rho\in\mathrm{Hom}\,(G,\mathrm{GL}_d(\mathbb{F}_{q^n}))} 1 \\ &= \frac{1}{|\mathrm{GL}_d(\mathbb{F}_{q^n})|} N_n^{\mathrm{hom}}, \end{aligned}$$

where $N_n^{\mathrm{hom}} = \sharp\mathrm{Hom}\,(G, \mathrm{GL}_d(\mathbb{F}_{q^n}))$. Since

$$|\mathrm{GL}_d(\mathbb{F}_{q^n})| = (-1)^d q^{\frac{d(d-1)}{2}n}(1-q^n)(1-q^{2n})\cdots(1-q^{dn}),$$

we have

$$|\mathrm{GL}_d(\mathbb{F}_{q^n})|^{-1} = (-1)^d q^{-\frac{d(d-1)}{2}n} \sum_{i_1\geq 0}\cdots\sum_{i_d\geq 0} q^{n(i_1+\cdots+di_d)}$$

in $\mathbb{C}_p$. Hence $Z_{\mathrm{wt}}(G,T)$ is written as follows in $\mathbb{C}_p[\![T]\!]$:

$$\begin{aligned} Z_{\mathrm{wt}}(G,T) &= \exp\left(\sum_{n=1}^{\infty} \frac{N_n^{\mathrm{wt}}}{n} T^n\right) \\ &= \prod_{i_1\geq 0}\cdots\prod_{i_d\geq 0} \exp\left(\sum_{n=1}^{\infty} \frac{(-1)^d N_n^{\mathrm{hom}}}{n}\left(q^{\frac{-d(d-1)}{2}+\sum_{j=1}^d ji_j} T\right)^n\right). \end{aligned}$$

It follows from Lemma 3.2 below that $Z_{\mathrm{wt}}(G,T)$ is p-adically meromorphic, by taking $f(T) = \exp\left(\sum_{n=1}^{\infty}(-1)^d N_n^{\mathrm{hom}} T^n/n\right) = Z_{\mathrm{hom}}(G,T)^{(-1)^d}$ which is a rational function in T by Theorem 1.1. $\square$

Lemma 3.2. *Let $f(T) = 1 + a_1T + \cdots$ be a power series in $\mathbb{C}_p[\![T]\!]$. Let $(q_i)_{i\geq 0}$ be a sequence in $\mathbb{C}_p$ such that $q_i \longrightarrow 0$. Denote by $F_f(T)$ the formal power series*

$$F_f(T) = \prod_{i=0}^{\infty} f(q_iT).$$

If $f(T)$ is entire (resp. p-adically meromorphic on $\mathbb{C}_p$), then $F_f(T)$ is also entire (resp. p-adically meromorphic on $\mathbb{C}_p$).

Proof. It is sufficient to consider the case where $f(T)$ is entire. We may assume that $\nu(a_n) \geq 0$ for all $n \geq 1$ since $F_{f_a}(T) = F_f(aT)$ for any $a \in \mathbb{C}_p$, where $f_a(T) = f(aT)$. We may also assume that $\nu(q_i) \geq 0$ for all $i \geq 0$ since $q_i \longrightarrow 0$. Write

$$F_f(T) = 1 + A_1T + A_2T^2 + \cdots,$$

where

$$A_n = \sum_{j_1+\cdots+j_r=n,\ j_1,\cdots,j_r\geq 1,\ 0\leq i_1<\cdots<i_r} a_{j_1}\cdots a_{j_r} q_{i_1}^{j_1}\cdots q_{i_r}^{j_r}.$$

Since $f(T)$ is entire and $q_i \longrightarrow 0$, for any $M > 0$ there exists a positive integer N such that $\nu(a_i) > iM$ and $\nu(q_i) > M$ for each $i \geq N$.

Now we prove $\nu(A_n)/n \longrightarrow \infty$ as $n \longrightarrow \infty$. For that, we calculate lower bounds for the valuations of all terms $a_{j_1}\cdots a_{j_r} q_{i_1}^{j_1}\cdots q_{i_r}^{j_r}$ in the above expression of A_n for $n > N^2$ by distinguishing the following two cases with respect to the length r.

(1) $1 \leq r \leq N$ case.

Let S be the set of indices $1 \leq k \leq r$ such that $j_k > N$. Since $j_1 + \cdots + j_r = n > N^2$, the set S is non-empty and we have

$$\sum_{k\in S} j_k = n - \sum_{k\notin S} j_k \geq n - N^2.$$

By the assumption that $\nu(a_i) > iM$ if $i \geq N$, we have

$$\nu\left(a_{j_1}\cdots a_{j_r} q_{i_1}^{j_1}\cdots q_{i_r}^{j_r}\right) \geq \nu\left(\sum_{k\in S} a_{j_k}\right) > \left(\sum_{k\in S} j_k\right) M \geq (n - N^2)M.$$

(2) $N < r \leq n$ case.

Since $0 \leq i_1 < \cdots < i_r$, for any $k > N$ we have $i_k \geq N$ and hence $\nu(q_{i_k}) > M$. So we have

$$\nu(q_{i_1}^{j_1}\cdots q_{i_r}^{j_r}) > (n - (j_1 + \cdots + j_N))M.$$

Let T be the set of indices $1 \leq k \leq N$ such that $j_k \leq N$. If $j_k > N$, then we have $\nu(a_{j_k}) > j_k M$. Hence

$$\begin{aligned}
\nu\left(a_{j_1}\cdots a_{j_r} q_{i_1}^{j_1}\cdots q_{i_r}^{j_r}\right) &> \nu\left(a_{j_1}\cdots a_{j_N}\right) + (n - (j_1 + \cdots + j_N))\,M \\
&> \nu\left(\sum_{k\in T} a_{j_k}\right) + \left(n - \sum_{k\in T} j_k\right) M \\
&\geq \left(n - \sum_{k\in T} j_k\right) M \geq (n - N^2)M.
\end{aligned}$$

Thus we have

$$\nu(A_n) \geq (n - N^2)M$$

for any $n > N^2$. Hence we have $\nu(A_n)/n \longrightarrow \infty$ when $n \longrightarrow \infty$. We have finished the proof of the lemma. $\square$

3.2. **Meromorphy of $Z_{\mathrm{wt}}(G, T)$ over $\mathbb{C}$.**
Next we consider the power series $Z_{\mathrm{wt}}(G, T)$ as a complex valued function. To prove the meromorphy of $Z_{\mathrm{wt}}(G, T)$ over $\mathbb{C}$ we consider the quotient stack $[X/\mathrm{GL}_d]$ and use Behrend's theorem on the Lefschetz trace formula for algebraic stacks. For references on algebraic stacks, see for instance [G], the Appendix of [V] and [LMB]. Note that we view a stack as a category, rather than a 2-functor.

For the moment let $\mathbb{F}$ be an arbitrary field and $\mathbf{G}$ an affine smooth group scheme over $\mathbb{F}$. Let X be a scheme of finite type over $\mathbb{F}$ with a group action $X \times_{\mathbb{F}} \mathbf{G} \to X$ over $\mathbb{F}$. We denote by $(\mathrm{Sch}/\mathbb{F})$ the category of schemes over $\mathbb{F}$ and choose the étale topology on $(\mathrm{Sch}/\mathbb{F})$. We write the same symbol S for the algebraic stack over $\mathbb{F}$ corresponding to an $\mathbb{F}$-scheme $S \to \operatorname{Spec}\mathbb{F}$. Let $p_{[X/\mathbf{G}]} : [X/\mathbf{G}] \to (\mathrm{Sch}/\mathbb{F})$ be the quotient stack defined by this group action (cf. [G, Example 2.18]). Thus, $[X/\mathbf{G}]$ is a category whose objects are pairs (π, f) of a principal $\mathbf{G}$-bundle $\pi : E \to S$, where S is a scheme over $\mathbb{F}$, and a $\mathbf{G}$-equivariant morphism $f : E \to X$. A morphism from $(\pi' : E' \to S', f' : E' \to X)$ to $(\pi : E \to S, f : E \to X)$ is a pair $(\varphi : E' \to E, \psi : S' \to S)$ of morphisms such that the diagram

$$\begin{tikzcd} E' \arrow[r, "\varphi"] \arrow[d, "\pi'"'] & E \arrow[d, "\pi"] \\ S' \arrow[r, "\psi"'] & S \end{tikzcd}$$

is cartesian and $f' = f \circ \varphi$. The structure functor $p_{[X/\mathbf{G}]}$ maps $(\pi : E \to S, f : E \to X)$ to S. Since $\mathbf{G}$ is smooth over $\mathbb{F}$, the quotient stack $[X/\mathbf{G}]$ is algebraic in the sense of [LMB] (cf. [G, Example 2.29]), that is,

(1) the diagonal morphism $[X/\mathbf{G}] \to [X/\mathbf{G}] \times_{\mathbb{F}} [X/\mathbf{G}]$ is representable, separated and quasi-compact.
(2) There exist a scheme U over $\mathbb{F}$ and a smooth surjective morphism $U \to [X/\mathbf{G}]$.

A morphism $U \to [X/\mathbf{G}]$ as in (2) is called an *atlas* of $[X/\mathbf{G}]$. (A *morphism* $f : \mathfrak{X} \to \mathfrak{Y}$ of $\mathbb{F}$-stacks is a functor such that $p_{\mathfrak{X}} = p_{\mathfrak{Y}} \circ f$, where $p_{\mathfrak{X}}$ (resp. $p_{\mathfrak{Y}}$) is the structure functor of $\mathfrak{X}$ (resp. $\mathfrak{Y}$). For the definitions of properties (such as representability, separatedness, etc.) of morphisms of stacks, see [G, Section 2.2].)

Let $X \to [X/\mathbf{G}]$ be the morphism of $\mathbb{F}$-stacks corresponding to the pair $(X \times_{\mathbb{F}} \mathbf{G} \to X,\ X \times_{\mathbb{F}} \mathbf{G} \to X)$ by the Yoneda lemma (cf. [G, Example 2.29]), where the first is the trivial $\mathbf{G}$-bundle over X and the second is the morphism of the group action. It is known that this is an atlas of $[X/\mathbf{G}]$ (cf. [LMB, Exemples (4.6)]).

Let P be a property of morphisms of schemes which is local on source and target (cf. [K, Chapter 1 §1, Chapter 2 §3]) for the étale topology (for instance, P = flat, locally of finite type, smooth, etc.). We say that a morphism $f : \mathfrak{X} \to \mathfrak{Y}$ of algebraic $\mathbb{F}$-stacks *has property P* if there exist an atlas $Y' \to \mathfrak{Y}$ of $\mathfrak{Y}$ and an atlas $X' \to Y' \times_{\mathfrak{Y}} \mathfrak{X}$ of $Y' \times_{\mathfrak{Y}} \mathfrak{X}$ such that the composition of morphisms of stacks $X' \to Y' \times_{\mathfrak{Y}} \mathfrak{X} \to Y'$ in the diagram below has property P (as a morphism of schemes). (For more details, see [G, Section 2.5].)

$$\begin{array}{ccccc} X' & \longrightarrow & Y' \times_{\mathfrak{Y}} \mathfrak{X} & \longrightarrow & \mathfrak{X} \\ & & \big\downarrow & & \big\downarrow \\ & & Y' & \longrightarrow & \mathfrak{Y} \end{array}$$

By definition, if the scheme X over $\mathbb{F}$ has the property P, then the quotient stack $[X/\mathbf{G}]$ over $\mathbb{F}$ has the property P.

In what follows, we take a finite field $\mathbb{F}_q$ as $\mathbb{F}$, and assume $\mathbf{G}$ is a connected linear algebraic group over $\mathbb{F}_q$. Let $\mathfrak{X} \to (\mathrm{Sch}/\mathbb{F}_q)$ be an algebraic stack of finite type over $\mathbb{F}_q$ and let $\mathfrak{X}(\mathbb{F}_{q^n})$ be the subcategory of $\mathfrak{X}$ whose objects and arrows are above $\operatorname{Spec}\mathbb{F}_{q^n}$. In particular $\mathfrak{X}(\mathbb{F}_{q^n})$ is a *groupoid*, i.e., all morphisms in $\mathfrak{X}(\mathbb{F}_{q^n})$ are isomorphisms. For the groupoid $\mathfrak{X}(\mathbb{F}_{q^n})$ define its *mass* $\sharp\mathfrak{X}(\mathbb{F}_{q^n})$ as follows ([Be, Definition 3.2.1]):

$$\sharp\mathfrak{X}(\mathbb{F}_{q^n}) := \sum_{\xi \in \mathfrak{X}(\mathbb{F}_{q^n})/\sim} \frac{1}{|\operatorname{Aut}\xi|},$$

where $\operatorname{Aut}\xi$ is the automorphism group of ξ in the groupoid $\mathfrak{X}(\mathbb{F}_{q^n})$ and $\mathfrak{X}(\mathbb{F}_{q^n})/\sim$ is the set of isomorphism classes of objects of $\mathfrak{X}(\mathbb{F}_{q^n})$. Note that $\operatorname{Aut}\xi$ and $\mathfrak{X}(\mathbb{F}_{q^n})/\sim$ are finite sets (hence $\sharp\mathfrak{X}(\mathbb{F}_{q^n})$ is finite) since $\mathfrak{X}$ is of finite type over $\mathbb{F}_q$ (cf. [Be, lemma 3.2.2]). If $\mathfrak{X} = [X/\mathbf{G}]$, then we have

$$\sharp\mathfrak{X}(\mathbb{F}_{q^n}) = \sum_{x \in X(\mathbb{F}_{q^n})/\sim} \frac{1}{|\mathrm{Stab}\,(x)|},$$

where $\mathrm{Stab}\,(x)$ is the stabilizer of x by the group action $X(\mathbb{F}_{q^n}) \times \mathbf{G}(\mathbb{F}_{q^n}) \to X(\mathbb{F}_{q^n})$. This follows from the categorical equivalence between $\mathfrak{X}(\mathbb{F}_{q^n})$ and the category in which the objects are the elements of $X(\mathbb{F}_{q^n})$ and the morphisms from x to y are the elements of $\mathbf{G}(\mathbb{F}_{q^n})$ which send x to y by the group action. This is a consequence (of the proof) of [Be, Lemma 2.5.1] for $n = 1$ (this is stated only when X is smooth over $\mathbb{F}_q$, but the same proof applies to arbitrary schemes of finite type over $\mathbb{F}_q$) and of the natural categorical equivalence $\mathfrak{X}(\mathbb{F}_{q^n}) \simeq [X \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n} / \mathbf{G} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n}](\mathbb{F}_{q^n})$ in which $(E \to \operatorname{Spec} \mathbb{F}_{q^n},\ E \to X)$ corresponds to $(E \to \operatorname{Spec} \mathbb{F}_{q^n},\ E \to X \otimes_{\mathbb{F}_q} \mathbb{F}_{q^n})$.

We define the zeta function $Z(\mathfrak{X}, T)$ of $\mathfrak{X} = [X/\mathbf{G}]$ by

$$Z(\mathfrak{X}, T) = \exp\left(\sum_{n=1}^{\infty} \frac{\sharp \mathfrak{X}(\mathbb{F}_{q^n})}{n} T^n \right).$$

We know by [Be, Theorem 3.2.4] that if $\mathfrak{X} = [X/\mathbf{G}]$ is smooth over $\mathbb{F}_q$, then the zeta function $Z(\mathfrak{X}, T)$ converges absolutely in some neighborhood of $T = 0$ and is continued meromorphically to the whole complex plane $\mathbb{C}$.

Now we prove the following result.

Theorem 3.3. *Let $\mathbf{G}$ be a connected linear algebraic group over $\mathbb{F}_q$. Let X be a scheme of finite type over $\mathbb{F}_q$ with a group action $X \times_{\mathbb{F}_q} \mathbf{G} \to X$ over $\mathbb{F}_q$. Let $\mathfrak{X}$ be the quotient stack $[X/\mathbf{G}]$ over $\mathbb{F}_q$. Then the power series $Z(\mathfrak{X}, T)$ converges absolutely in a neighborhood of $T = 0$, and it is continued meromorphically to the whole complex plane $\mathbb{C}$.*

Proof. First note that we may assume X is reduced, since we consider only $\mathbb{F}_{q^n}$-rational points. Let X_{sm} be the smooth locus of X (which is open and dense by [Gro, Corollaire 6.8.7, Proposition 17.15.12]) and X_{nsm} the closed subset $X \smallsetminus X_{\mathrm{sm}}$ endowed with the reduced induced subscheme structure. Since $\mathbf{G}$ acts on X_{sm} and X_{nsm} respectively, we have $X(\mathbb{F}_{q^n}) = X_{\mathrm{sm}}(\mathbb{F}_{q^n}) \sqcup X_{\mathrm{nsm}}(\mathbb{F}_{q^n})$ with $\mathbf{G}(\mathbb{F}_{q^n})$-action on $X_{\mathrm{sm}}(\mathbb{F}_{q^n})$ and $X_{\mathrm{nsm}}(\mathbb{F}_{q^n})$. Hence we have $\sharp\mathfrak{X}(\mathbb{F}_{q^n}) = \sharp[X_{\mathrm{sm}}/\mathbf{G}](\mathbb{F}_{q^n}) + \sharp[X_{\mathrm{nsm}}/\mathbf{G}](\mathbb{F}_{q^n})$.

Put $X_0 := X$ and $X_1 := X_{\mathrm{nsm}}$. We have $\dim X_1 < \dim X$ since X_{sm} is a dense open subset of X. We can repeat this argument to obtain a sequence

$$X_0 \supset X_1 \supset \cdots \supset X_r$$

of closed subschemes of X with $\dim X_0 > \dim X_1 > \cdots > \dim X_r = 0$. Note in particular that X_r is étale over $\mathbb{F}_q$. Thus

$$\sharp\mathfrak{X}(\mathbb{F}_{q^n}) = \sharp\mathfrak{X}_0(\mathbb{F}_{q^n}) + \sharp\mathfrak{X}_1(\mathbb{F}_{q^n}) + \cdots + \sharp\mathfrak{X}_r(\mathbb{F}_{q^n}),$$

where $\mathfrak{X}_i$ is the quotient stack $[X_{i,\mathrm{sm}}/\mathbf{G}]$. Then we have

$$Z(\mathfrak{X}, T) = Z(\mathfrak{X}_0, T) \cdots Z(\mathfrak{X}_r, T).$$

Since each factor $Z(\mathfrak{X}_i, T)$ is meromorphic over $\mathbb{C}$, this proves Theorem 3.3. □

Now we go back to our situation; thus $\mathbf{G} = \mathrm{GL}_d$ and X is the affine scheme $X_d(G) \otimes_{\mathbb{Z}} \mathbb{F}_q$ (cf. Section 1). In this case the mass $\sharp\mathfrak{X}(\mathbb{F}_{q^n})$ for the corresponding algebraic stack $\mathfrak{X} = [X/\mathrm{GL}_d]$ is equal to N_n^{wt} defined at the beginning of this section. Hence $Z(\mathfrak{X}, T)$ is equal to $Z_{\mathrm{wt}}(G, T)$. As a corollary of Theorem 3.3, we have the following.

Corollary 3.4. *The power series $Z_{\mathrm{wt}}(G,T)$ converges absolutely in a neighborhood of $T = 0$, and it is continued meromorphically to the whole complex plane $\mathbb{C}$.*

4. Rationality of $Z_{\mathrm{Ig}}(G,T)$

Here we consider representations of G into $\mathrm{GL}_d(\mathbb{Z}/p^n\mathbb{Z})$. Put $N_n^{\mathrm{Ig}} := \sharp\mathrm{Hom}\,(G, \mathrm{GL}_d(\mathbb{Z}/p^n\mathbb{Z}))$. Define the power series $Z_{\mathrm{Ig}}(G,T)$ by

$$Z_{\mathrm{Ig}}(G,T) := \sum_{n=0}^{\infty} N_n^{\mathrm{Ig}} T^n.$$

For this type of zeta function we have the following result.

Proposition 4.1. *The power series $Z_{\mathrm{Ig}}(G,T)$ is a rational function.*

Proof. Let $X_d(G) = \mathrm{Spec}\,(A_d(G))$ be the affine scheme associated with G as in the proof of Theorem 1.1; thus the commutative ring $A_d(G)$ has the property that $\mathrm{Hom}\,(G, \mathrm{GL}_d(\mathbb{Z}/p^n\mathbb{Z})) \simeq \mathrm{Hom}\,(A_d(G), \mathbb{Z}/p^n\mathbb{Z})$ for all $n \geq 1$. Since $A_d(G)$ is finitely generated, it is presented as $A_d(G) \simeq \mathbb{Z}[x_1, \cdots, x_m]/(f_1, \cdots, f_r)$, where $f_1, \cdots, f_r \in \mathbb{Z}[x_1, \cdots, x_m]$ are non-constant polynomials. Then we have $N_n^{\mathrm{Ig}} = \sharp\{a \in (\mathbb{Z}/p^n\mathbb{Z})^m \mid f_i(a) \equiv 0 \bmod p^n\}$. Thus our zeta function $Z_{\mathrm{Ig}}(G,T)$ is nothing but the Igusa zeta function associated with $(f_1, \cdots, f_r)$, and is known to be rational by Igusa ([I]) in the $r = 1$ case and Meuser ([Me]) in the general case. □

The generating function defined by the numbers of isomorphism classes of representations of G into $\mathrm{GL}_d(\mathbb{Z}/p^n\mathbb{Z})$ may also have good properties such as rationality, though we have no results at present.

5. example

Here we calculate the zeta functions explicitly for free groups.

Example 5.1. Let $G = F_r$ be the free group of rank r. Then we have $N_n^{\mathrm{hom}} = |\mathrm{GL}_d(\mathbb{F}_{q^n})|^r$. Since $|\mathrm{GL}_d(\mathbb{F}_{q^n})| = q^{nd(d-1)/2}(q^n - 1)\cdots(q^{dn} - 1)$ and $\exp\left(\sum_{n=1}^{\infty}(q^kT)^n/n\right) = 1/(1 - q^kT)$, we have

$$Z_{\mathrm{hom}}(F_r, T) = \prod_{0 \leq j_1, \cdots, j_d \leq r} (1 - q^{rd^2 - (j_1 + \cdots + dj_d)}T)^{(-1)^{j_1 + \cdots + j_d + 1}\binom{r}{j_1}\cdots\binom{r}{j_d}},$$

where $\binom{r}{j}$ is the binomial coefficient.

Since $N_n^{\mathrm{wt}} = |\mathrm{GL}_d(\mathbb{F}_{q^n})|^{-1} N_n^{\mathrm{hom}}$ (see Subsection 3.1), we also have

$$\begin{aligned}
& Z_{\mathrm{wt}}(F_r, T) \\
= \ & \exp\left(\sum_{n=1}^{\infty} \frac{|\mathrm{GL}_d(\mathbb{F}_{q^n})|^r}{n|\mathrm{GL}_d(\mathbb{F}_{q^n})|} T^n\right) \\
= \ & \begin{cases} \displaystyle\prod_{j_1,\cdots,j_d \geq 0} \left(1 - \frac{1}{q^{d^2} q^{j_1+\cdots+d j_d}} T\right)^{-1}, & \text{if } r = 0. \\ \displaystyle\prod_{0 \leq j_1,\cdots,j_d \leq r-1} (1 - q^{(r-1)d^2 - (j_1+\cdots+d j_d)} T)^{(-1)^{j_1+\cdots+j_d+1} \binom{r-1}{j_1} \cdots \binom{r-1}{j_d}}, & \text{if } r \geq 1. \end{cases}
\end{aligned}$$

This shows that $Z_{\mathrm{wt}}(F_r, T)$ is a rational function when $r \geq 1$, whereas $Z_{\mathrm{wt}}(1, T)$ is not a rational function.

Acknowledgment

The authors are grateful to Professor Yuichiro Taguchi for many suggestions and on valuable advice for the composition of this paper.

References

[Be] Kai A. Behrend, *The Lefschetz trace formula for algebraic stacks*, Invent. Math. **112** (1993), 127–149.

[Bo] Nicolas Bourbaki, *Éléments de mathématique, Algèbre*, Chapitre **8**, Actualités Sci. Ind. **1261**, Hermann, Paris, 1958.

[CTY] Naoki Chigira, Yugen Takegahara, and Tomoyuki Yoshida, *On the number of homomorphisms from a finite group to a general linear group*, J. Algebra **232** (2000), 236–254.

[D] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.

[G] Tomás L. Gómez, *Algebraic stacks*, Proc. Indian Acad. Sci. Math. Sci. **111** (2001), 1–31.

[Gro] Alexander Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas*, Inst. Hautes Études Sci. Publ. Math. (1967).

[H] Shinya Harada, *On the finiteness of mod p Galois representations of a local field*, to appear in the Tohoku Math. J. (2) **59** (2007).

[I] Jun-ichi Igusa, *Forms of higher degree*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics, vol. **59**, Tata Institute of Fundamental Research, Bombay, 1978.

[K] Donald Knutson, *Algebraic spaces*, Springer-Verlag, Berlin, 1971.

[LMB] Gérard Laumon and Laurent Moret-Bailly, *Champs algébriques*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. Springer-Verlag, Berlin, 2000.

[Me] Diane Meuser, *On the rationality of certain generating functions*, Math. Ann. **256** (1981), 303–310.

[M1] Hyunsuk Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), 156–165.

[M2] ———, *The number of monomial mod p Galois representations with bounded conductor*, Tohoku Math. J. (2) **55** (2003), 89–98.

[MT1] Hyunsuk Moon and Yuichiro Taguchi, *Mod p Galois representations of solvable image*, Proc. Amer. Math. Soc. **129** (2001), 2529–2534.

[MT2] ———, *Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations*, Doc. Math. (2003), no. Extra Vol., 641–654 (electronic), Kazuya Kato's fiftieth birthday.

[P] Claudio Procesi, *Deformations of representations*, Methods in ring theory (Levico Terme, 1997), Lecture Notes in Pure and Appl. Math., vol. **198**, Dekker, New York, 1998, pp. 247–276.

[S] Jeffrey M. Sink, *A zeta-function for a knot using* $\mathrm{SL}_2(\mathbb{F}_{p^s})$ *representations*, Knots in Hellas '98 (Delphi), Ser. Knots and Everything, vol. **24**, World Sci. Publishing, River Edge, NJ, 2000, pp. 452–470.

[V] Angelo Vistoli, *Intersection theory on algebraic stacks and on their moduli spaces*, Invent. Math. **97** (1989), 613–670.

[W] André Weil, *Basic number theory*, Classics in Mathematics, Springer-Verlag, Berlin, 1995.

Shinya Harada
Graduate School of Mathematics
Kyushu University
Fukuoka 812-8581, Japan
s.harada@math.kyushu-u.ac.jp

Hyunsuk Moon
Department of Mathematics
College of Natural Sciences
Kyungpook National University
Daegu 702-701, Korea
hsmoon@knu.ac.kr