Rigid Local Systems on $\mathbb{A}^1$ with finite monodromy

Nicholas M. Katz

Princeton University

Johns Hopkins, March 22, 2017
I begin with (a picture of) work of Igusa that had a huge influence on me.
FIBRE SYSTEMS OF JACOBIAN VARIETIES.*  

(III. Fibre Systems of Elliptic Curves.) 

By JUN-ICHI IGUSA.

To Zariski on his 60th birthday

1. Introduction. This is the third paper on fibre systems of Jacobian varieties. We shall apply some of our previous results [7, 9] to the simplest case of fibre systems of elliptic curves. In this way we get a geometric theory of elliptic modular functions with arbitrary level in the sense of Klein [11] for any characteristic which does not divide the level. Here we would like to state that no algebraic theory of modular functions has been available even in the case of characteristic zero. In fact, the known theory depends heavily either on Riemann's existence theorem or on the use of Eisenstein series.

The theory of modular functions in positive characteristic is useful in discussing arithmetic properties of modular functions in characteristic zero.

* Received September 2, 1958.

This work was partially supported by a research grant of the National Science Foundation. The content of this paper was discussed on March 18, 1958 in a seminar at Harvard University conducted by Professor Zariski.
To make the connection to my title, consider the one-parameter (t the parameter) family of elliptic curves

\[ y^2 - y = x^3 + tx. \]
If we look at this family in any characteristic other than 2 or 3, we see a non constant $j$-invariant, and hence an $\ell$-adic ($\ell \neq p$) monodromy group which is open in $SL(2, \mathbb{Z}_\ell)$. 
However, in these two characteristics 2 and 3, this family has finite monodromy, because all members are supersingular: in characteristic 2, the Hasse invariant is the coefficient of $xy$ in the equation, and in characteristic 3 it is the coefficient of $x^2$. 
For this example in characteristic 2, Artin-Schreier theory tells us that for $\psi$ the unique nontrivial additive character of $F_2$, extended to finite extensions $k/F_2$ by composition with the trace, we have
For \( t \in k \), the trace of \( \text{Frob}_k \) on the \( H^1 \) of the curve \( k \) given by \( y^2 - y = x^3 + tx \) is the character sum

\[
- \sum_{x \in k} \psi(x^3 + tx).
\]
The rigid local systems of my title are gotten in characteristic $p > 0$ by taking a finite field $k$ of characteristic $p$, a nontrivial additive character $\psi$ of $k$, an integer $D \geq 3$ which is prime to $p$, and looking at the character sums, one for each $t \in k$,

$$t \in k \mapsto - \sum_{x \in k} \psi (x^D + tx).$$

with a similar recipe over finite extensions.
We can also "decorate" these sums by choosing a multiplicative character $\chi$ of $k^\times$ and looking at the sums

$$t \in k \mapsto - \sum_{x \in k} \chi(x) \psi(x^D + tx).$$

[The convention here is that $1(0) = 1$ but $\chi(0) = 0$ for $\chi$ nontrivial.]
These sums are the trace function of a lisse $\mathbb{Q}_\ell$-sheaf on $\mathbb{A}^1/k$ (any $\ell \neq p$) 

$$\mathcal{F}(k, \psi, \chi, D).$$

It is pure of weight one, and has 

$$\text{rank} = D - 1 \text{ for } \chi = 1,$$

$$\text{rank} = D \text{ for } \chi \neq 1.$$ 

Its determinant $\det(\mathcal{F})$ is geometrically trivial (this uses $D \geq 3$).
This local system is geometrically irreducible and rigid because it is the Fourier transform of the rank one object \( L_\chi(x) \otimes L_\psi(x^D) \), and Fourier transform preserves both these properties.
One knows that when the characteristic $p$ is large compared to $D$, then the geometric monodromy group of this $\mathcal{F}$ is a connected, semisimple algebraic group over $\overline{\mathbb{Q}}_\ell$, either $SO$ or $SL$ or $Sp$, with the extra possibility of $G_2$ when $D = 7$. For example

$$\mathcal{F}(k, \psi, 1, \text{odd } D) : Sp(D - 1)$$

$$\mathcal{F}(k, \psi, 1, \text{even } D) : SL(D - 1)$$

$$\mathcal{F}(k, \psi, \chi_2, \text{even } D) : SL(D)$$

$$\mathcal{F}(k, \psi, \chi_2, \text{odd } D \neq 7) : SO(D)$$

$$\mathcal{F}(k, \psi, \chi_2, 7) : G_2$$

when $p >> D \geq 3$. 


Back in 1986, Dan Kubert was coming to my graduate course, and in it he explained a method of proving that certain of the \( \mathcal{F}(k, \psi, \chi, D) \) had finite geometric monodromy groups. They include

\[
\begin{align*}
\mathcal{F}(\mathbb{F}_q, \psi, 1, q + 1), \\
\mathcal{F}(\mathbb{F}_q, \psi, 1, (q + 1)/2), \ q \ \text{odd} \\
\mathcal{F}(\mathbb{F}_q, \psi, \chi_2, (q + 1)/2), \ q \ \text{odd} \\
\mathcal{F}(\mathbb{F}_q, \psi, 1, (q^n + 1)/(q + 1)), \ n \ \text{odd}, \\
\mathcal{F}(\mathbb{F}_{q^2}, \psi, \chi, (q^n + 1)/(q + 1)), \ n \ \text{odd}, \ \chi \neq 1, \ \chi^{q+1} = 1.
\end{align*}
\]
In hindsight, I had already seen some of these, but only very recently did I understand that those that I had seen fell under Kubert’s results. They were

$$\mathcal{F}(\mathbb{F}_2, \psi, 1, 3),$$

a $q + 1$ case, the elliptic curve family we started off with,

$$\mathcal{F}(\mathbb{F}_5, \psi, \chi_2, 3),$$

a $(q + 1)/2$ case, which gave $PSL(2, 5)$, but which I had “seen” as $A_5$, 
\[ \mathcal{F}(\mathbb{F}_3, \psi, \chi_2, 7), \]
a \((q^3 + 1)/(q + 1)\) case, which gave \(SU(3, 3)\), a finite subgroup of \(G_2\), and
\[ \mathcal{F}(\mathbb{F}_{13}, \psi, \chi_2, 7), \]
a \((q + 1)/2\) case, which gave \(PSL(2, 13)\), another finite subgroup of \(G_2\).
For $q$ odd, the local system 

$$\mathcal{F}(\mathbb{F}_q, \psi, 1, (q + 1)/2)$$

has rank

$$(q - 1)/2,$$

and the local system 

$$\mathcal{F}(\mathbb{F}_q, \psi, \chi_2, (q + 1)/2)$$

has rank

$$(q + 1)/2.$$

For $q \geq 5$ odd, the group $SL(2, q)$ has, after the trivial representation, two irreducible representations of dimension

$$(q - 1)/2,$$

and it has two of dimension

$$(q + 1)/2.$$
For $n$ odd, the local system
\[ \mathcal{F}(\mathbb{F}_q, \psi, 1, (q^n + 1)/(q + 1)), \ n \text{ odd}, \]
has rank
\[ (q^n + 1)/(q + 1) - 1, \]
and each of the $q$ local systems
\[ \mathcal{F}(\mathbb{F}_q^2, \psi, \chi, (q^n + 1)/(q + 1)), \ n \text{ odd}, \chi \neq 1, \chi^{q+1} = 1, \]
has rank
\[ (q^n + 1)/(q + 1). \]
For $n$ odd and with the exception of $(n = 3, q = 2)$, the group $SU(n, q)$ has, after the trivial representation, one irreducible representation of dimension
\[ (q^n + 1)/(q + 1) - 1, \]
and it has $q$ irreducible representations of dimension
\[ (q^n + 1)/(q + 1). \]
THIS CANNOT BE AN ACCIDENT.
We formulate the obvious conjecture: that the geometric monodromy group is what the numerology suggests:
for
\[ \mathcal{F} ( \mathbb{F}_q, \psi, 1, (q + 1)/2) , \]
the image of \( SL(2, q) \) in one of its irreducible representations of
dimension \((q – 1)/2\); for
\[ \mathcal{F} ( \mathbb{F}_q, \psi, \chi_2, (q + 1)/2) \]
the image of \( SL(2, q) \) in one of its irreducible representations of
dimension \((q + 1)/2\); [And you get the other representation of
the same dimension by changing \( \psi \) to \( x \mapsto \psi(ax) \) for \( a \in \mathbb{F}_q^\times \) a
nonsquare.]
For $n$ odd and with the exception of $(n = 3, q = 2)$, the geometric monodromy group of

$$\mathcal{F}(\mathbb{F}_q, \psi, 1, (q^n + 1)/(q + 1)), \ n \text{ odd},$$

is the image of $SU(n, q)$ in its unique irreducible representation of dimension $(q^n + 1)/(q + 1) - 1$; and for each of the $q$ local systems

$$\mathcal{F}(\mathbb{F}_{q^2}, \psi, \chi, (q^n + 1)/(q + 1)), \ n \text{ odd}, \ \chi \neq 1, \ \chi^{q+1} = 1,$$

it is the image of $SU(n, q)$ in one of its $q$ irreducible representations of dimension $(q^n + 1)/(q + 1)$; [And, when $q$ is odd, taking $\chi = \chi_2$ should give the unique irreducible representations of dimension $(q^n + 1)/(q + 1)$ which is orthogonal.]
Here is the current status of these conjectures.
In the $SL(2, q)$ case, it is known for $q = p \geq 5$, using group theory results of Brauer, Feit, and Tuan that go back fifty years. [The only geometric inputs are that the geometric monodromy representation is unimodular, primitive (not induced), of dimension $(p \pm 1)/2$, and the image group has order divisible by $p$.]
The situation for $SL(2, q)$, $q \geq 5$ odd, is more complicated, and relies heavily on work of Dick Gross, itself based on Deligne-Lusztig. This work gives a good handle on the representations which factor through $PSL(2, q)$, which are those of ours whose dimension $(q \pm 1)/2$ is odd. There is then a trick to pass to the other ones of ours, those whose dimension $(q \pm 1)/2$ is even. At present, this trick only works for those $q$ such that 2 is a square in $\mathbb{F}_q$, i.e., for those $q$ which are $\pm 1$ mod 8.
The situation for $SU(n, q)$, $n \geq 3$ odd, is this.
For $n \geq 5$ odd, nothing is known.
For $n = 3$ and $q \geq 3$, we know nothing when $q$ is even. When $q$ is odd, what we do know is again based on (the same) work of Dick Gross. This gives us a good handle on those representations that factor through $PSU(3, q)$. 
Fortunately, the group $SU(3, q)$ has a trivial center unless $q$ is 2 mod 3. Thus when $q$ is not 2 mod 3, the groups $SU(3, q)$ and its quotient $PSU(3, q)$ coincide, and the conjecture is known for $SU(3, q)$. When $q$ is 2 mod 3, then we know the conjecture for

$$\mathcal{F}(\mathbb{F}_q, \psi, \chi_2, (q + 1)/2)$$

and for those

$$\mathcal{F}(\mathbb{F}_{q^2}, \psi, \chi, (q^n + 1)/(q + 1)), \text{ } n \text{ odd, } \chi \neq 1, \chi^{q+1} = 1,$$

whose $\chi$ has $\chi^{(q+1)/3} = 1$. 
MUCH REMAINS TO BE DONE.