370

ASTÉRISQUE

2015

DE LA GÉOMÉTRIE ALGÉBRIQUE
AUX FORMES AUTOMORPHES (II)

J.-B. BOST, P. BOYER, A. GENESTIER,
L. LAFFORGUE, S. LYSENKO, S. MOREL, B.C. NGÔ, eds.

ELLIPTIC CONVOLUTION, G_2, AND ELLIPTIC SURFACES

Nicholas M. KATZ

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Astérisque est un périodique de la Société Mathématique de France.

Numéro 370, 2015

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
smf@smf.univ-mrs.fr

Hindustan Book Agency
O-131, The Shopping Mall
Arjun Marg, DLF Phase 1
Gurgaon 122002, Haryana
Inde

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

Tarifs

Vente au numéro : 98 € ($ 147)

Abonnement Europe : 650 €, hors Europe : 689 € ($ 1033)

Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat : Nathalie Christiaën

Astérisque
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 01 44 27 67 99 • Fax : (33) 01 40 46 90 96
revues@smf.ens.fr • http://smf.emath.fr/

ISSN 0303-1179

ISBN 978-2-85629-806-0

Directeur de la publication : Marc Peigné

Astérisque
370, 2015, p. 197–205

ELLIPTIC CONVOLUTION, G_2, AND ELLIPTIC SURFACES

by

Nicholas M. Katz

Abstract. — We explain how the theory of elliptic convolution leads to situations with Tannakian monodromy group G_2. These situations are closely related to certain elliptic surfaces first enumerated by Beauville.

***Résumé* (Convolution elliptique, G_2, et surfaces elliptiques).** — On explique comment la théorie de la convolution elliptique conduit à des situations où le groupe de monodromie tannakien est G_2. Ces situations sont étroitement reliées à certaines surfaces elliptiques énumérées pour la première fois par Beauville.

1. Elliptic sums

Let k be a finite field, E/k an elliptic curve, and $f : E(k) \to \mathbb{C}$ a function on the finite abelian group $E(k)$. Given f, we define a function $S(f)$ of characters $\Lambda \in \mathrm{Hom}_{group}(E(k), \mathbb{C}^\times)$ by

$$S(f)(\Lambda) := \sum_{P \in E(k)} f(P)\Lambda(P).$$

This function $S(f)$ is the "Fourier transform" of f in the sense of finite abelian groups. Given two functions f, g on $E(k)$, their convolution is the function on $E(k)$ defined by

$$(f \star g)(P) := \sum_{R+S=P} f(R)g(S).$$

Their Fourier transforms are related by the usual identity $S(f \star g) = S(f)S(g)$, *i.e.*, for each Λ we have

$$S(f \star g)(\Lambda) = S(f)(\Lambda)S(g)(\Lambda).$$

2010 *Mathematics Subject Classification.* — 14D05, 14H52, 14J27, 20G41.
Key words and phrases. — Monodromy, convolution, elliptic curve, elliptic surface, exceptional group.

For a given function f, the moments of its Fourier transform $S(f)$, defined by

$$M_n(S(f)) := (1/\#E(k))\sum_{\Lambda} S(f)(\Lambda)^n$$

are thus given in terms of the multiple self-convolutions $f^{\star n}$ of f with itself by

$$(1/\#E(k))\sum_{\Lambda} S(f^{\star n})(\Lambda) = f^{\star n}(0).$$

For any writing of n as $a+b$ with a, b strictly positive integers, we thus have

$$M_n(S(f)) = (f^{\star n})(0) = \sum_{P} f^{\star a}(P) f^{\star b}(-P).$$

2. Elliptic equidistribution

Fix a prime number ℓ invertible in k, and an embedding ι of $\overline{\mathbb{Q}_\ell}$ into $\mathbb{C}$. There is an obvious notion of convolution of objects in $D^c_b(E, \overline{\mathbb{Q}_\ell})$, defined in terms of the addition map $sum : E \times_k E \to E$, by $(A, B) \mapsto A \star B := Rsum_\star(A \boxtimes B)$. If we attach to $A \in D^c_b(E, \overline{\mathbb{Q}_\ell})$ its trace function on $E(k)$, given by $f_{A,k}(P) := \mathrm{Trace}(Frob_{k,P}|A)$, then by the Lefschetz Trace Formula we have the identity $f_{A,k} \star f_{B,k} = f_{A\star B,k}$ of functions on $E(k)$.

In general, if A and B are each perverse sheaves on E, their convolution need not be perverse. To remedy that, we work first on $E_{\overline{k}}$, the extension of scalars of E to $\overline{k}$. We say that an object $A \in D^c_b(E_{\overline{k}}, \overline{\mathbb{Q}_\ell})$ has property $\mathcal{P}$ if, for all lisse rank one sheaves $\mathcal{L}$ on $E_{\overline{k}}$, we have

$$H^i(E_{\overline{k}}, A \otimes \mathcal{L}) = 0 \text{ for i} \neq 0.$$

We have the following lemma.

Lemma 2.1. — *Let $A \in D^c_b(E_{\overline{k}}, \overline{\mathbb{Q}_\ell})$ have property $\mathcal{P}$. Then A is perverse.*

Because lisse rank one $\mathcal{L}$'s on $E_{\overline{k}}$ are primitive in the sense that $sum^\star(\mathcal{L}) \cong \mathcal{L} \boxtimes \mathcal{L}$, the A's with property $\mathcal{P}$ are stable by convolution. Thus perverse sheaves with property $\mathcal{P}$ are stable by convolution. An irreducible perverse sheaf on $E_{\overline{k}}$ has property $\mathcal{P}$ unless it is an $\mathcal{L}[1]$.

Corollary 2.2. — *The perverse sheaves on $E_{\overline{k}}$ with property $\mathcal{P}$ form a neutral Tannakian category, with convolution as the tensor operation, δ_0 as the identity, $N \mapsto N^\vee := [P \mapsto -P]^\star DN$ as the dual, and "dim"$(N) := \chi(E_{\overline{k}}, N) = h^0(E_{\overline{k}}, N)$. For any lisse rank one $\mathcal{L}$ on $E_{\overline{k}}$, $N \mapsto H^0(E_{\overline{k}}, N \otimes \mathcal{L})$ is a fibre functor.*

Remark 2.3. — Just as in Gabber-Loeser [**Ga-Loe**], the abelian category structure on the above Tannakian category is the one induced by viewing it **not** as a full subcategory of the category *Perv* of all perverse sheaves on $E_{\overline{k}}$, but rather as the quotient category *Perv*/*Neg* of *Perv* by the subcategory *Neg* consisting of those perverse sheaves which are of Euler characteristic zero, or (equivalently) of the form $\mathcal{F}[1]$ for $\mathcal{F}$ a lisse sheaf on $E_{\overline{k}}$, or (equivalently) successive extensions of objects $\mathcal{L}[1]$. The irreducible (resp. semisimple) objects in $Perv/Neg$ are just the irreducible (resp. semisimple) perverse sheaves with property $\mathcal{P}$. The semisimple perverse sheaves with property $\mathcal{P}$ themselves form a Tannakian category; its structure of abelian category is equal to the naive one.

We now return to working on E/k. Recall that for a character Λ of $E(k)$, the Lang torsor construction [**De-ST**, 1.4] gives a lisse rank one sheaf $\mathcal{L}_\Lambda$ on E, whose trace function on $E(k)$ is Λ. The perverse sheaves on E which, pulled back to $E_{\overline{k}}$, have property $\mathcal{P}$, themselves form a neutral Tannakian category. For each character Λ of $E(k)$, $N \mapsto H^0(E_{\overline{k}}, N \otimes \mathcal{L}_\Lambda)$ is a fibre functor. The action of $Frob_k$ on $H^0(E_{\overline{k}}, N \otimes \mathcal{L}_\Lambda)$ is an automorphism of this fibre functor, so gives a conjugacy class $Frob_{k,\Lambda}$ in the Tannakian group $G_{arith,N}$ attached to N. Notice in passing that, by the Lefschetz trace formula,

$$\mathrm{Trace}(Frob_k | H^0(E_{\overline{k}}, N \otimes \mathcal{L}_\Lambda)) = \sum_{P \in E(k)} \mathrm{Trace}(Frob_{k,P} | N) \Lambda(P)$$

is the value at Λ of the elliptic sum $S(f_{N,k})$ attached to the trace function $f_{N,k}$ of N on $E(k)$.

Suppose N is perverse on E, has property $\mathcal{P}$, is arithmetically semisimple, is ι-pure of weight zero, and has dimension $n :=$ "dim"(N). Denote by $G_{arith,N}$, respectively $G_{geom,N}$, the Tannakian groups attached to N on E , respectively on $E_{\overline{k}}$. In general we have inclusions of reductive $\overline{\mathbb{Q}_\ell}$-algebraic groups

$$G_{geom,N} \lhd G_{arith,N} \subset GL(\text{“}dim\text{”}(N)).$$

Pick a maximal compact subgroup K of $G_{arith,N}(\mathbb{C})$. The semisimplification (in the sense of Jordan decomposition) $Frob^{ss}_{k,\Lambda}$ of the conjugacy class $Frob_{k,\Lambda}$ intersects K in a single conjugacy class $\theta_{k,\Lambda}$ of K. Via the inclusion of $K \subset G_{arith,N}(\mathbb{C})$ into $GL(n)$, we have

$$\det(1 - T\theta_{k,\Lambda}) = \det(1 - T Frob_k | H^0(E_{\overline{k}}, N \otimes \mathcal{L}_\Lambda)),$$

so in particular

$$\begin{aligned}\mathrm{Trace}(\theta_{k,\Lambda}) &= \mathrm{Trace}(Frob_k | H^0(E_{\overline{k}}, N \otimes \mathcal{L}_\Lambda)) \\ &= \sum_{P \in E(k)} \mathrm{Trace}(Frob_{k,P} | N) \Lambda(P).\end{aligned}$$

Exactly as in [**Ka-CE**, 1.1, 7.3], Deligne's Weil II results [**De-Weil II**, 3.3.1] and the Tannakian formalism give the following theorem.

Theorem 2.4. — *In the above situation, suppose $G_{geom,N} = G_{arith,N}$. Then as L/k runs over larger and larger finite extension fields of k, the conjugacy classes $\{\theta_{L,\Lambda}\}_{\Lambda \text{ char. of } E(L)}$ become equidistributed in the space $K^\#$ of conjugacy classes of K, for its "Haar measure" of total mass one.*