Yuri Tschinkel

MATHEMATISCHES INSTITUT
UNIVERSITÄT GÖTTINGEN
SEMINARS SS 2004

Yuri Tschinkel
E-mail : `yuri@uni-math.gwdg.de`
Mathematisches Institut, Bunsenstr. 3-5, 37073 Göttingen.

CONTENTS

ABSTRACTS

Construction of relative motives with interesting étale realization using the middle convolution

We study the middle convolution of local systems on the punctured affine line in the singular and the étale case. We give a motivic interpretation of the middle convolution which yields information on the occurring determinants. Finally, we use these methods to realize special linear groups regularly as Galois groups over $\mathbb{Q}(t)$.

Arithmetic of Calabi–Yau Varieties

We address the modularity questions of Calabi–Yau varieties of dimension $\leqslant 3$ defined over $\mathbb{Q}$.

Counting rational points on cubic threefolds

This is a survey of recent results concerning rational points of bounded height on hypersurfaces of degree ≥ 3.

Derived equivalences in representation theory of finite groups

We survey recent results and conjectures in modular representation theory of finite groups.

l-adic Galois cohomology and the Suslin–Voevodsky theorem

We present the Suslin-Voevodsky theorem within the framework of continuous étale cohomology.

Supersingular elliptic curves and maximal quaternionic orders

We give an explicit version of the "Deuring correspondence" between supersingular elliptic curves and maximal quaternionic orders, by presenting a deterministic and explicit algorithm to compute it.

On the norm principle for quadratic forms

We prove a version of Knebusch's Norm Principle for finite étale extensions of semi-local Noetherian domains with infinite residue fields of characteristic different from 2. As an application we prove the case of Grothendieck's conjecture on principal homogeneous spaces for the spinor group of a quadratic form.

Zetafunktionen in der Gruppentheorie – mit Augenmerk auf p-adische Liegruppen

Sei G eine endlich erzeugte Gruppe. Für jede natürliche Zahl n ist die Anzahl der Untergruppen vom Index n in G endlich, und man kann die formale Dirichletreihe $\zeta_G(s) := \sum_{H \leqslant_f G} |G : H|^{-s}$ bilden. Unter geeigneten Bedingungen, z.B. falls G nilpotent ist, definiert $\zeta_G(s)$ eine analytische Funktion und besitzt zudem eine Eulerproduktzerlegung. Durch Betrachtung der lokalen Faktoren wird man dazu geführt, entsprechende Zetafunktionen für p-adische Liegruppen bzw. Liegitter zu untersuchen.

In meinem Vortrag habe ich versucht, einen Einblick in die junge und schnell wachsende Theorie dieser Zetafunktionen zu vermitteln.

Zariski chambers and stable base loci

In joint work with A. Küronya and T. Szemberg we study certain asymptotic invariants of linear series: the stable base locus and the volume. In particular we are interested in the question how these invariants behave under small perturbations in the Néron-Severi space. We show

Twisted Thom isomorphisms are introduced in Balmer–Witt theory. They are used to calculate the Witt groups of projective bundles and to approach the construction of push-forwards in this theory.

We consider the Bethe Ansatz Equation (BAE) related to the Gaudin model associated to a semisimple Lie group G. Given a solution of the BAE we construct a family of new solutions called a population. The populations are isomorphic to the flag variety associated to the Langlands dual Lie group $G^\vee$. The sl_N populations are in one-to-one correspondence with intersection points of appropriate Schubert cycles in the Grassmannian of N planes in the space of polynomials. Thus we relate the subjects of Bethe Ansatz and of Schubert Calculus.

We discuss several constructions of universal torsors over rational surfaces.

We are looking for a formulation of Manin's real multiplication question in higher rank. This question has at least two parts:

1. formalization of the linear algebra side of the story in terms of morphisms of algebraic groups analogous to Shimura and Deligne's point of view on the theory of complex multiplication.
2. noncommutative algebraic geometry.

Here we are interested mostly in the first part. We also recall some known results concerning the second part.

We discuss an algorithm for the construction of low genus curves whose Jacobians have complex multiplication by a given CM-field K. We present examples for genus 2 and 3.

Valuations on a field K are encoded in the absolute Galois group G_K of K: They are in one-to-one correspondence with the conjugacy classes of decomposition subgroups of G_K which (apart from few exceptions) can be characterized in group theoretic terms. Roughly speaking, decomposition subgroups of G_K are maximal subgroups of G_K with a Sylow-subgroup containing a non-trivial abelian normal subgroup. We sketch the main ideas of the proof.

The paper develops the local theory of one-dimensional birational anabelian geometry over almost arbitrary fields and indicates how the global theory should work. This generalizes corresponding results of Pop and Mochizuki over finitely generated and sub-p-adic fields.

INTRODUCTION

This volume contains lecture notes from the seminars

– Number Theory,
– Algebraic Geometry,
– Geometric methods in representation theory and Galois theory

which took place at the Mathematics Institute of the University of Göttingen during the Summer Term 2004. They have been arranged in chronological order. Almost all contributions report on recent work by the authors.

Yuri Tschinkel

September 12, 2004

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 1–7
Universität Göttingen, 2004

CONSTRUCTION OF RELATIVE MOTIVES WITH INTERESTING ÉTALE REALIZATION USING THE MIDDLE CONVOLUTION

M. Dettweiler
IWR, Universität Heidelberg, 69120 Heidelberg, Germany
E-mail : michael.dettweiler@iwr.uni-heidelberg.de

Abstract. We study the middle convolution of local systems on the punctured affine line in the singular and the étale case. We give a motivic interpretation of the middle convolution which yields information on the occurring determinants. Finally, we use these methods to realize special linear groups regularly as Galois groups over $\mathbb{Q}(t)$.

1. Introduction

If K is a field, then we set $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$, where K^{sep} denotes a separable closure of K. Let k be a number field. A profinite group G *occurs regularly as Galois group over* $k(t)$, if one has a surjection $\varphi : G_{k(t)} \to G$ such that the restriction of φ to $G_{\bar{k}(t)}$ is still surjective. If G is a finite group, then φ corresponds to a Galois cover of $\mathbb{P}^1_k$ with Galois group G. The regular inverse Galois problem asks, whether every finite group occurs regularly as Galois group over $\mathbb{Q}(t)$.

April 20th, 2004.

Our main motivation for studying the convolution stems from the fact that most of the regular Galois realizations for classical groups are obtained with methods, derived from Katz' middle convolution functor MC_χ, see [**Kat96**], [**DR00**]. The functor MC_χ can be viewed (under some restrictions, see [**DR03**]) as a functor from the category of local systems on the punctured affine line to itself.

Using the properties of the Katz functor, one was able to obtain many new families of classical groups regularly as Galois groups over the rational function field [**DR00**], [**Völ01**]. In fact, all previously known examples can be explained using MC_χ, except a few exceptional cases in low dimensions. Nevertheless, this method has its limitations: For example, it fails to produce groups like $\mathrm{SL}_n(\mathbb{F}_q)$ as Galois groups over $\mathbb{Q}(t)$. In this note, we outline a more general approach to the middle convolution, in order to overcome some of the limitations of the Katz functor.

The category of local systems of R-modules (i.e., locally free sheaves of R-modules of finite rank on X) on a topological space X is denoted by $\mathrm{LS}_R(X)$. Let $\mathrm{Rep}(R[\pi_1(X,x_0)])$ be the category of finite dimensional R-representations of the fundamental group $\pi_1(X,x_0)$. It is well known, that if X is a connected topological manifold, then $\mathrm{LS}_R(X)$ is equivalent to $\mathrm{Rep}(R[\pi_1(X,x_0)])$, by sending a local system $\mathscr{V}$ to its monodromy representation

$$\rho_{\mathscr{V}} : \pi_1(X,x_0) \to \mathrm{GL}(\mathscr{V}_{x_0}).$$

If $\mathbf{u}$, $\mathbf{v}$ are divisors on the complex affine line $\mathbb{A}^1(\mathbb{C})$, $\mathscr{V}_1 \in \mathrm{LS}_R(\mathbb{A}^1(\mathbb{C}) \setminus \mathbf{u})$ and $\mathscr{V}_2 \in \mathrm{LS}_R(\mathbb{A}^1(\mathbb{C}) \setminus \mathbf{v})$ are two local systems then one can form their *middle convolution product* $\mathscr{V}_1 * \mathscr{V}_2 \in \mathrm{LS}_R(\mathbb{A}^1(\mathbb{C}) \setminus \mathbf{u} * \mathbf{v})$, where $\mathbf{u} * \mathbf{v} \subseteq \mathbb{A}^1(\mathbb{C})$ is the *sum divisor*, see Section 2.

If X is a variety over a number field k, let $\mathrm{LS}_R^{\text{ét}}(X)$ denote the category of étale local systems of R-modules on X. The middle convolution of étale local systems (see Section 3) is defined in an analogous way as the middle convolution of local systems, using the higher direct image approach of [**DW03**]. By construction, the middle convolution $\mathscr{V}_1 * \mathscr{V}_2 \in \mathrm{LS}_R^{\text{ét}}(\mathbb{A}^1_k \setminus \mathbf{u} * \mathbf{v})$ of two local systems $\mathscr{V}_1 \in \mathrm{LS}_R^{\text{ét}}(\mathbb{A}^1_k \setminus \mathbf{u})$ and $\mathscr{V}_1 \in \mathrm{LS}_R^{\text{ét}}(\mathbb{A}^1_k \setminus \mathbf{v})$ gives rise to a Galois representation

$$G_{k(t)} \longrightarrow \pi_1(\mathbb{A}^1_k \setminus \mathbf{u} * \mathbf{v}, x) \xrightarrow{\rho_{\mathscr{V}_1 * \mathscr{V}_2}} \mathrm{GL}(\mathscr{V}_1 * \mathscr{V}_{2x}).$$

We are interested in the determination of these Galois representations (in the case where $k = \mathbb{Q}$).

Using the process of analytification, the geometric monodromy of $\rho_{\mathscr{V}_1 * \mathscr{V}_2}$ (i.e., $\rho_{\mathscr{V}_1 * \mathscr{V}_2}|_{\pi_1((\mathbb{A}^1_k \setminus \mathbf{u} * \mathbf{v}) \otimes \bar{k})}$) can be determined using the convolution of local systems on the punctured complex affine line and the results of [**DW03**].

We consider sequences of convolutions and tensor products of étale local systems with finite monodromy and find a geometric (motivic) interpretation for these sequences, see Section 4. An important consequence of the motivic interpretation is, that if $k = \mathbb{Q}$, then the determinants of the Galois representations restricted to $G_{\mathbb{Q}}$ are powers of the cyclotomic characters and finite characters. This is crucial for the Galois realizations of special linear groups, given in Section 5, where we outline a proof of the following result (see Thm. 5.1 and its Corollary):

Theorem 1.1. *The group* $\mathrm{SL}_{2m+1}(\mathbb{F}_q)$ *occurs regularly as Galois groups over* $\mathbb{Q}(t)$ *if* $m > \varphi(q-1)$ *(*φ *denoting the Euler* φ*-function) and* $q \equiv 1 \mod 4$.

2. Convolution of local systems

In this section all varieties will be defined over $\mathbb{C}$ and we will write $\mathbb{A}^1$, $\mathbb{P}^1, \ldots$ instead of $\mathbb{A}^1(\mathbb{C})$, $\mathbb{P}^1(\mathbb{C}), \ldots$ and view these objects equipped with their associated analytic structures.

For $r \in \mathbb{N}$, let $\mathscr{O}_r := \{P \subseteq \mathbb{C} \mid \#P = r\}$. For $\mathbf{u} := \{u_1, \ldots, u_p\} \in \mathscr{O}_p$ and $\mathbf{v} := (v_1, \ldots, v_q\} \in \mathscr{O}_q$ set

$$\mathbf{u} * \mathbf{v} := \{u_i + v_j \mid i = 1, \ldots, p,\ j = 1, \ldots, q\}.$$

Let $X_0 := \mathbb{A}^1 \setminus \mathbf{u}$, $Z_0 := \mathbb{A}^1 \setminus \mathbf{v}$ and $Y_0 := \mathbb{A}^1 \setminus \mathbf{u} * \mathbf{v}$. Set

$$\tilde{f}(x, y) := \prod_{i=1}^{p} (x - u_i) \prod_{j=1}^{q} (y - x - v_j) \prod_{i,j} (y - (u_i + v_j))$$

and let $f \in \mathbb{C}[x, y]$ be the associated reduced polynomial. One has $\tilde{f} \neq f$ if and only if $|\mathbf{u} * \mathbf{v}| \neq i \cdot j$. Let

$$\mathbf{u}^o := \{(x, y) \in \mathbb{A}^2 \mid f(x, y) = 0\},$$

and $U := \mathbb{A}^2 \setminus \mathbf{u}^o$. The set U is equipped with three maps which play a important role in all what follows: One the one hand, one has the projections

$$\mathrm{pr}_1 : U \longrightarrow X_0,\ (x, y) \longmapsto x$$

and

$$\mathrm{pr}_2 : U \longrightarrow Y_0,\ (x, y) \longmapsto y.$$

On the other hand, one has the *subtraction map*

$$\mathrm{q} : U \to Z_0,\ (x, y) \longmapsto y - x.$$

The embedding of $\mathbb{A}_2$ into $\mathbb{P}^1 \times \mathbb{A}^1$ induces an embedding $j : U \to \mathbb{P}^1 \times Z_0$. The composition of j with the second projection $\mathbb{P}^1 \times Z_0 \to Z_0$ is denoted by $\overline{\mathrm{pr}}_2$.

Let R be a principal ideal domain, $\mathscr{V}_1 \in \mathrm{LS}_R(X_0)$ and $\mathscr{V}_2 \in \mathrm{LS}_R(Z_0)$. Then the local system

$$\mathscr{V}_1 \circ \mathscr{V}_2 := \mathrm{pr}_1^* \mathscr{V}_1 \otimes \mathrm{q}^* \mathscr{V}_2$$

is a local system on U.

Definition 2.1. *The* middle convolution *of* $\mathscr{V}_1 \in \mathrm{LS}_R(X_0)$ *with* $\mathscr{V}_2 \in \mathrm{LS}_R(Z_0)$ *is the local system*

$$\mathscr{V}_1 * \mathscr{V}_2 := R^1(\overline{\mathrm{pr}}_2)_*(j_* \mathscr{V}_1 \circ \mathscr{V}_2) \in \mathrm{LS}_R(Y_0).$$

Remark 2.2. The name "convolution" is justified by the following observation: Let $\mathscr{V}_1 \in \mathrm{LS}_{\mathbb{C}}(X_0)$ and $\mathscr{V}_2 \in \mathrm{LS}_{\mathbb{C}}(Z_0)$ arise from differential systems with regular singularities via the Riemann-Hilbert correspondence (see [**Del70**]). If $\mathscr{V}_1$ and $\mathscr{V}_2$ are general local systems and if $f(x)$ is a local section of $\mathscr{V}_1$ and $g(y-x)$ is a local section of $\mathscr{V}_2$ then the usual convolution $\int_\sigma f(x)g(y-x)dx$ is a local section of $\mathscr{V}_1 * \mathscr{V}_2$, where σ is some homology cycle (compare to [**DR03**]).

The local system $\mathscr{V}_1 * \mathscr{V}_2$ corresponds to its monodromy representation $\rho_{\mathscr{V}_1 * \mathscr{V}_2}$ which can be explicitly determined using the variation of parabolic cohomology, see [**DW03**].

3. Convolution of étale local systems

Let k be a number field.

Definition 3.1. An étale local system $\mathscr{V}$ of R-modules on a smooth variety X over k is a *locally constant sheaf of R-modules* on the étale site $X_{\text{ét}}$ (in the sense of [**FK88**]) whose stalks are free R-modules of finite rank.

Let $\mathrm{LS}_R^{\text{ét}}(X)$ denote the category of étale local systems of R-modules on X. It is well known that one has an equivalence of categories:

$$\begin{array}{ccc} \mathrm{LS}_R^{\text{ét}}(X) & \cong & \mathrm{Rep}_R^{\text{cont}}(\pi_1^{\text{ét}}(X,x)) \\ \mathscr{V} & \longleftrightarrow & \rho_{\mathscr{V}}, \end{array}$$

where $\mathrm{Rep}_R^{\text{cont}}(\pi_1^{\text{ét}}(X,x))$ denotes the category of finite dimensional continuous R-representations of the étale fundamental group $\pi_1^{\text{ét}}(X,x)$.

In this section, we view the morphisms

$$\mathrm{pr}_1 : U \longrightarrow X_0,\ (x,y) \longmapsto x,$$
$$\mathrm{pr}_2 : U \longrightarrow Y_0,\ (x,y) \longmapsto y$$

and

$$\mathrm{q} : U \to Z_0,\ (x,y) \longmapsto y-x$$

as morphisms of varieties and assume, that they are defined over k. Let R be either a finite field $\mathbb{F}_q$, $q = l^k$, or a complete subring of $\overline{\mathbb{Q}}_l$.

Definition 3.2. The *middle convolution* of $\mathscr{V}_1 \in \mathrm{LS}_R^{\text{ét}}(X_0)$ with $\mathscr{V}_2 \in \mathrm{LS}_R^{\text{ét}}(Z_0)$ is the local system

$$\mathscr{V}_1 * \mathscr{V}_2 := R^1(\overline{\mathrm{pr}}_2)_*(j_*\mathscr{V}_1 \circ \mathscr{V}_2) \in \mathrm{LS}_R^{\text{ét}}(Y_0).$$

Since $\mathscr{V}_1 * \mathscr{V}_2$ is an étale local system, it corresponds to its monodromy representation $\rho_{\mathscr{V}_1 * \mathscr{V}_2} : \pi_1^{\text{ét}}(X) \to \mathrm{GL}_n(R)$. It follows from [**DW03**], Prop. 3.3, that the restriction of $\rho_{\mathscr{V}_1 * \mathscr{V}_2}$ to the geometric fundamental group $\pi_1^{\text{ét}}(X \otimes \bar{k}) \simeq \pi_1\widehat{(X(\mathbb{C})})$ can be explicitly computed, using Prop. 2.7 of [**DW03**].

4. Motivic interpretation of the middle convolution

We continue to use notations and assumptions of the last section. It follows from the definitions, that an irreducible étale local system $\mathscr{V} \in \mathrm{LS}_R(\mathbb{A}_k^1 \setminus \mathbf{u})$ with finite monodromy (i.e., $G := \mathrm{im}(\rho_{\mathscr{V}})$ is finite) corresponds to a pair $(\varphi|_{\mathscr{V}} : \tilde{X} \to \mathbb{A}_k^1 \setminus \mathbf{u}, p_\chi)$, where $\varphi|_{\mathscr{V}}$ is an unramified Galois cover of $\mathbb{A}_k^1 \setminus \mathbf{u}$ with Galois group G and $p_\chi \in E[G]$ is an idempotent which projects the regular representation to the induced irreducible representation $\chi : G \to \mathrm{GL}(\mathscr{V}_{x_0}) \simeq \mathrm{GL}_n(R)$.

Let $\mathscr{V}_1 \in \mathrm{LS}_R^{\text{ét}}(X_0)$ with $\mathscr{V}_2 \in \mathrm{LS}_R^{\text{ét}}(Z_0)$ be local systems with finite monodromy, corresponding to pairs $(\varphi_{\mathscr{V}_1} : \tilde{X}_0 \to X_0, p_{\chi_1})$ and $(\varphi_{\mathscr{V}_2} : \tilde{Z}_0 \to Z_0, p_{\chi_2})$. Let

$$\tilde{X}_0 \circ \tilde{Z}_0 := (\tilde{X}_0 \times_{X_0} U) \times_U (\tilde{Z}_0 \times_{Z_0} U).$$

Then the natural map $f : \tilde{X}_0 \circ \tilde{Z}_0 \to U$ is an unramified Galois cover with Galois group $G_1 \times G_2$. One can find an embedding $j : \tilde{X}_0 \circ \tilde{Z}_0 \to \overline{\tilde{X}_0 \circ \tilde{Z}_0}$, such that $\overline{\tilde{X}_0 \circ \tilde{Z}_0}$ has a smooth projective map $\bar{f}$ to $\mathbb{P}^1 \times Y_0$ which is a ramified Galois cover with Galois group $G_1 \times G_2$ and $\bar{f}|_{\tilde{X}_0 \circ \tilde{Z}_0} = f$.

The Leray spectral sequence of $\bar{\mathrm{pr}}_2 \circ \bar{f}$ yields the "motivic interpretation" of the convolution of two finite local systems: One has

$$\mathscr{V}_1 * \mathscr{V}_2 = p_{\chi_1 \otimes \chi_2}(R^1(\bar{\mathrm{pr}}_2)_*(\bar{f}(\underline{R}))\ ),$$

where $p_{\chi_1 \otimes \chi_2} \in R[G_1 \times G_2]$ cuts out the irreducible representation $\chi_1 \otimes \chi_2$, and $G_1 \times G_2$ acts via basechange on $R^1(\bar{\mathrm{pr}}_2)_*(\bar{f}(\underline{R}))$.

This approach can be iterated using the results of Bierstone and Milman [**BM97**]. This leads to the following result: Let $k = \mathbb{Q}$, $R = E_\lambda$ the completion of a number field E at a finite prime λ and let $\mathscr{V}$ be an étale local system of E_λ-modules which arises from iteratively convoluting finite local systems and scaling with one-dimensional étale local systems. Then

$$\det(\rho_{\mathscr{V}})|_{G_{\mathbb{Q}}} = \varepsilon \otimes \chi_l^n, \tag{1}$$

where χ_l is the l-adic cyclotomic character and $\varepsilon : G_{\mathbb{Q}} \to E^\times$ is a finite character (the absolute Galois group $G_{\mathbb{Q}}$ is considered as a subgroup of $G_{\mathbb{Q}(t)}$ via a section induced by a rational basepoint). A proof of Equation (1) uses the fact that the determinant is (by results of Serre and Faltings) the Galois representation associated to a Hecke character of $\mathbb{Q}$. Those Galois representations are known to be a product of a power of χ_l with a finite character.

5. Applications to the inverse Galois problem

The results of the last sections can be used to prove the following result:

Theorem 5.1. *Let l be an odd prime, $q = l^k$, $E := \mathbb{Q}(\zeta_{q-1} + \zeta_{q-1}^{-1}, \zeta_4)$ (where ζ_m, $m \in \mathbb{N}$, denotes a primitive root of unity), λ a finite prime of E and O_λ the valuation ring of E_λ. The projective special linear group $\mathrm{PSL}_n(O_\lambda)$ occurs regularly as Galois groups over $\mathbb{Q}(t)$, if $\mathrm{char}(\lambda)$ is odd, $n = 2r - 5$ and $r > 2 + \varphi(q-1)$.*

The following corollary follows immediately from reduction modulo λ, where λ lies over l :

Corollary 5.2. *The group $\mathrm{PSL}_n(\mathbb{F}_q)$ occurs regularly as Galois groups over $\mathbb{Q}(t)$ if $n = 2r - 5$, $r > 2 + \varphi(q-1)$ and $q \equiv 1 \mod 4$.*

The idea of the proof is the following: One considers suitable finite local systems over punctured affine lines over $\mathbb{Q}$. Their middle convolution yields a local system $\mathscr{V} \in \mathrm{LS}^{\text{ét}}_{E_\lambda}(X := \mathbb{A}^1_{\mathbb{Q}} \setminus \mathbf{u})$. Using the l-adic Fourier transform and some standard results on primitive reflection groups, one can show that the image of $\pi_1^{\text{ét}}(X \otimes \bar{\mathbb{Q}})$ under $\rho_{\mathscr{V}}$ is equal to $\mathrm{PSL}_n(O_\lambda)$. It follows then from Equation (1), that the occurring determinants which arise from $G_{\mathbb{Q}} \leqslant G_{\mathbb{Q}(t)}$ are contained, up to a Tate-twist, in the group of fourth roots of unity and can be neglected by a suitable scaling. This yields the result.

References

[BM97] E. Bierstone & P. D. Milman – Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant, *Invent. Math.* **128** (1997), no. 2, p. 207–302.

[Del70] P. Deligne – *Équations différentielles à points singuliers réguliers*, Springer-Verlag, Berlin, 1970, Lecture Notes in Mathematics, Vol. 163.

[DR00] M. Dettweiler & S. Reiter – An algorithm of Katz and its application to the inverse Galois problem, *J. Symbolic Comput.* **30** (2000), no. 6, p. 761–798, Algorithmic methods in Galois theory.

[DR03] M. Dettweiler & S. Reiter – On the middle convolution, 2003, preprint.

[DW03] M. Dettweiler & S. Wewers – Local systems associated to covers of the projective line, 2003, preprint.

[FK88] E. Freitag & R. Kiehl – *Étale cohomology and the Weil conjecture*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 13, Springer-Verlag, Berlin, 1988.

[Kat96] N. M. Katz – *Rigid local systems*, Annals of Mathematics Studies, vol. 139, Princeton University Press, Princeton, NJ, 1996.

[Völ01] H. Völklein – A transformation principle for covers of $\mathbb{P}^1$, *J. Reine Angew. Math.* **534** (2001), p. 156–168.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 9–29
Universität Göttingen, 2004

ARITHMETIC OF CALABI–YAU VARIETIES

N. Yui
Department of Mathematics and Statistics, Queen's University, Kingston, Ontario Canada K7L 3N6 • *E-mail :* yui@mast.queensu.ca

Abstract. We address the modularity questions of Calabi–Yau varieties of dimension $\leqslant 3$ defined over $\mathbb{Q}$.

1. Introduction

Definition 1.1. A smooth projective variety X of dimension d defined over $\mathbb{C}$ is called a *Calabi–Yau* variety if

(i) $H^i(X, \mathscr{O}_X) = 0$ for every i, $0 < i < d$, and

(ii) the canonical bundle $\mathscr{K}_X$ of X is trivial.

Introduce the Hodge numbers

$$h^{i,j}(X) := \dim H^j(X, \Omega^i_X).$$

Noriko Yui was partially supported by a Research Grant from NSERC, Canada, and a grant from DFG at Hannover.
April 21st, 2004.

Then X is a Calabi–Yau variety if

$$h^{i,0}(X) = 0 \quad \text{for every } i, 0 < i < d, \text{ and} \quad h^{0,d}(X) = p_g(X) = 1$$

where $p_g(X)$ is the geometric genus of X.

Example 1.2.

• If $d = 1$, a Calabi–Yau variety of dimension 1 is nothing but an elliptic curve (if it is equipped with a rational point).

• If $d = 2$, the conditions $h^{1,0}(X) = 0$ and $p_g(X) = 1$ imply that a Calabi–Yau variety of dimension 2 is a $K3$ surface.

• If $d = 3$, the conditions $h^{1,0}(X) = h^{2,0}(X) = 0$ and $p_g(X) = 1$ imply that a Calabi–Yau variety of dimension 3 is a Calabi–Yau threefold. Since a Calabi–Yau threefold is a Kähler manifold, it is necessary that $h^{1,1}(X) > 0$.

Numerical invariants and Hodge diamonds. Now we define the numerical invariants of Calabi–Yau varieties, and the Hodge diamonds.

• The k-th Betti number of X is

$$B_k(X) = \dim H^k(X, \mathbb{C}) = \dim H^k_{et}(\bar{X}, \mathbb{Q}_\ell).$$

Then $B_k(X) = 0$ for $k > 2d$, and the Poincaré duality implies that

$$B_k(X) = B_{2d-k}(X) \quad \text{for } k, 0 \leqslant k \leqslant d.$$

• There are symmetries of Hodge numbers:

$$h^{i,j}(X) = h^{j,i}(X),\ h^{p,q}(X) = h^{d-p,d-q}(X)$$

where the first identity follows from complex conjugation, and the second from the Serre duality. There is the Hodge decomposition

$$B_k(X) = \sum_{i+j=k} h^{i,j}(X)$$

and the Euler characteristic of X is given by

$$E(X) = \sum_{k=0}^{2d} (-1)^k B_k(X).$$

• The Hodge diamonds of elliptic curves, $K3$ surfaces and Calabi–Yau threefolds are given, respectively, as follows.

$$\begin{array}{ccc} & 1 & \\ 1 & & 1 \\ & 1 & \end{array}$$

Then

$$B_0 = B_2 = 1,\ B_1 = 2 \quad \text{and } E(X) = 0.$$

$$\begin{array}{ccccc}
 & & 1 & & \\
 & 0 & & 0 & \\
1 & & 20 & & 0 \\
 & 0 & & 0 & \\
 & & 1 & &
\end{array}$$

Then

$$B_0 = B_4 = 1,\ B_1 = B_3 = 0,\ B_2 = 22 \quad \text{and } E(X) = 24.$$

$$\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 0 & & 0 & & \\
 & 0 & & h^{1,1} & & 0 & \\
1 & & h^{2,1} & & h^{1,2} & & 1 \\
 & 0 & & h^{2,2} & & 0 & \\
 & & 0 & & 0 & & \\
 & & & 1 & & &
\end{array}$$

Then

$$B_0 = B_6 = 1,\ B_1 = B_5 = 0,\ B_2 = h^{1,1} = h^{2,2} = B_4,\ B_3 = 2(1 + h^{2,1})$$

and

$$E(X) = 2(h^{1,1} - h^{2,1}).$$

2. The L-series and zeta-function of Calabi–Yau varieties

We are interested in arithmetic and number theoretic properties of Calabi–Yau varieties, and we will consider Calabi–Yau varieties defined over number fields (e.g., $\mathbb{Q}$). Let X be a Calabi–Yau variety of dimension d defined over $\mathbb{Q}$. (By this we mean, the complexification of X is a Calabi–Yau variety.) There exists an integral model for X. Let p be a prime and assume that the reduction $X_p := X \bmod p$ is smooth over $\bar{\mathbb{F}}_p$. Such a prime p is called a *good* prime. For a good prime p, let Frob_p denote the Frobenius morphism on X induced from the p-th power map $x \mapsto x^p$. Let ℓ be a prime $\neq p$. Then Frob_p acts on the ℓ-adic étale cohomology groups $H^i_{et}(\bar{X}_p, \mathbb{Q}_\ell) \simeq H^i(\bar{X}, \mathbb{Q}_\ell)$ for $i = 0, 1, \ldots, 2d$. Let

$$P^i_p(T) := \det\left(1 - \mathrm{Frob}^*_p\, T \mid H^i_{et}(\bar{X}, \mathbb{Q}_\ell)\right)$$

be the characteristic polynomial of the endomorphism Frob^*_p on the étale ℓ-adic cohomology group, where T is an indeterminate. Then $P^i_p(T) \in 1 + T\mathbb{Z}[T]$ with

$\deg P_p^i = B_i$ (the i-th Betti number of X) and its reciprocal roots are algebraic integers with absolute value $p^{i/2}$ (Deligne).

Let $\mathscr{G} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group. Then there is an ℓ-adic étale Galois representation

$$\rho^i_{X,\ell} : \mathscr{G} \to GL(H^i_{et}(\bar{X}, \mathbb{Q}_\ell)).$$

In particular, using $\rho^i_{X,\ell}(\mathrm{Frob}_p)$, we define the i-th (cohomological) L-series of X.

Definition 2.1. The i-th (cohomological) L-series $L(X,s) = L(H^i_{et}(\bar{X}, \mathbb{Q}_\ell), s)$ is defined by the Euler product

$$L_i(X,s) := \prod_{p \neq \ell} \det(1 - \rho^i_{X,\ell}(\mathrm{Frob}_p)p^{-s})^{-1} \times (\text{similar factor at } p = \ell)$$

where the product runs over good primes. Digressing, we have

$$L_i(X,s) = \prod_{p \neq \ell} P_p^i(p^{-s})^{-1} \times (\text{similar factor at } p = \ell).$$

In particular, if $i = d =$ the dimension of X, we simply write $L(X,s)$ in place of $L_d(X,s)$ and its local factor by $P_p(T)$ instead of $P_p^d(T)$.

3. The modularity of elliptic curves over $\mathbb{Q}$

Now we address the modularity of dimension 1 Calabi–Yau varieties defined over $\mathbb{Q}$. Let E be an elliptic curve over $\mathbb{Q}$, and let Δ denote its discriminant. Then its L-series can be built up by counting the number of $\mathbb{F}_p$–rational points on E.

$$L(E,s) = \prod_p \frac{1}{1 - a(p)p^{-s} + \varepsilon(p)p^{1-2s}} = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

where p runs all primes, and

$$a(p) = \begin{cases} p + 1 - \#E(\mathbb{F}_p),\ \varepsilon(p) = 1 & \text{if } p \nmid \Delta \\ 0,\ \pm 1,\ \varepsilon(p) = 0 & \text{if } p \mid \Delta \end{cases}$$

Given a prime p, each local Euler p-factor of $L(E,s)$ can be determined explicitly using the above description. However, there are infinitely many Euler factors. A natural question is:

Is there any global function that determines the L-series $L(E,s)$?

The answer to this question comes from a quite different source. Indeed, this will take us to more analytic objects. So we will now define modular groups, modular forms and cusp forms. Let $\mathfrak{H}$ denote the upper-half complex plane and let $SL_2(\mathbb{Z})$ be the group of 2×2 integral matrices with determinant 1 and put $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\pm I_2$ where I_2 denotes the identity matrix of rank 2.

Definition 3.1. Let $N \geqslant 1$ be an integer, and let

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) \,|\, c \equiv 0 \pmod{N}\} \subset PSL_2(\mathbb{Z})$$

be a congruence subgroup of $PSL_2(\mathbb{Z})$.

Let k be a non-negative integer. A *modular form f of weight $k \geqslant 1$ on $\Gamma_0(N)$* is a complex-valued holomorphic function on $\mathfrak{H}$ satisfying the following transformation rule:

$$f(\frac{az+b}{cz+d}) = (cz+d)^k f(z) \quad \text{for } z \in \mathfrak{H} \text{ and } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

A *cusp form f of weight k on $\Gamma_0(N)$* is a modular form vanishing at all cusps of $\Gamma_0(N)$. In particular, f has a Fourier expansion (at ∞), and we can write

$$f(q) = \sum n = 1^{\infty} a_f(n)\, q^n \quad \text{with } q = e^{2\pi i z}.$$

The L-series of a cusp form f is defined by

$$L(f,s) := \sum_{n=1}^{\infty} \frac{a_f(n)}{n^s}$$

Now we state the result of Wiles et al. which proves the conjecture of Shimura and Taniyama in the affirmative.

Theorem 3.2. (Wiles et al. [**Wil95**], [**TW95**], [**BCDT01**]) *Let E be an elliptic curve over $\mathbb{Q}$. Then E is modular, that is, there is a cusp (new) form f of weight $2 = 1+1$ on $\Gamma_0(N)$ such that*

$$L(E,s) = L(f,s) \quad \text{i.e., } a(n) = a_f(n) \quad \forall n.$$

Here N is the conductor of E.

Remark 3.3. The proof of Wiles et al. is to compare the two 2-dimensional Galois representations arising from E and f. If these two 2-dimensional Galois representations are equivalent mod 3 (or mod 5), then they are equivalent, and establish the Shimura–Taniyama conjecture in the affirmative.

4. The modularity of singular (extremal) $K3$ surfaces

Now we will address the modularity of dimension 2 Calabi–Yau varieties, namely, $K3$ surfaces, defined over $\mathbb{Q}$.

Let X be an algebraic $K3$ surface. Let $NS(X)$ be the Néron–Severi group of X generated by algebraic cycles on X. Then $NS(X)$ is a free finitely generated abelian group. The $\mathbb{Z}$-rank of $NS(X)$ is called the *Picard number* of X and denoted by $\rho(X)$. Since $NS(X) \subseteq H^2(X,\mathbb{Z}) \cap H^{1,1}(X,\mathbb{R})$, the Picard number $\rho(X)$ is at most 20. A $K3$ surface X is equipped with the perfect pairing induced by the intersection pairing. Let $T(X) := NS(X)^{\perp}_{H^2(X,\mathbb{Z})}$ be the orthogonal complement of $NS(X)$ in $H^2(X,\mathbb{Z})$ with respect to this perfect pairing. Then $T(X)$ is a lattice of rank $22-\rho(X)$, and is called the group or the lattice of transcendental cycles on X.

Now we will single out a special class of $K3$ surfaces.

Definition 4.1. A $K3$ surface X is said to be a *singular* (or *extremal*) if $\rho(X) = 20$.

Now we consider a singular $K3$ surface X defined over $\mathbb{Q}$. The L-series of X is defined by

$$L(X,s) = (*) \prod_{p:\text{good}} P_p(p^{-s})^{-1}$$

where the product runs over all good primes (with $(*)$ indicates the factor corresponding to bad primes), and

$$P_p(T) = det(1 - \mathrm{Frob}_p^* T \mid H^2_{et}(\bar{X}, \mathbb{Q}_\ell))$$

is an integral polynomial of degree 22 whose reciprocal roots have the absolute value p. The decomposition of the lattices $H^2(X,\mathbb{Z}) = NS(X) \oplus T(X)$ induces the decomposition of the L-series $L(X,s)$:

$$L(X,s) = L(NS(X)\otimes\mathbb{Q}_\ell, s)\cdot L(T(X)\otimes\mathbb{Q}_\ell, s).$$

Remark 4.2. If we pass to a sufficiently large extension K of $\mathbb{Q}$ to ensure that all algebraic cycles are defined over K, then

$$L(NS(X_K)\otimes\mathbb{Q}_\ell, s) = \zeta_K(s-1)^{\rho(X_K)} = \zeta_K(s-1)^{20}$$

where $\zeta_K(s)$ is the Dedekind zeta-function of K. We should remark that the Picard number is an arithmetic invariant which is very sensitive to the field of definition of algebraic cycles. If not all algebraic cycles are defined over a fixed field, e.g., $\mathbb{Q}$, the problem of determining the L-series $L(NS(X)\otimes\mathbb{Q}_\ell), s)$ is still open.

Now we can state the modularity results for singular $K3$ surfaces.

Theorem 4.3. (Shioda and Inose [**SI77**]) *Every singular $K3$ surface X has a model defined over some number field K, and its Hasse–Weil zeta-function $\zeta(X_K, s)$ is given, up to a finite number of Euler factors, by*

$$\zeta(X_K, s) = \zeta_K(s)\zeta_K(s-1)^{20}L(s-1, \chi^2)L(s-1, \bar{\chi}^2)$$

where $\zeta_K(s)$ is the Dedekind zeta-function of K and $L(s, \chi^2)$ is the Hecke L-series with a suitable Grossencharacter χ^2.

A modular (cusp) form is not present in this theorem of Shioda and Inose. The modularity of singular $K3$ surfaces over $\mathbb{Q}$ in our sense has been established by Livné. Livné analyzed the two 2-dimensional Galois representations associated to the rank 2 motive $T(X)$.

Theorem 4.4. (Livné [**Liv95**]) *Let X be a singular $K3$ surface defined over $\mathbb{Q}$. Then X is modular. That is, the transcendental part $T(X)$ is modular and*

$$L(T(Y) \otimes \mathbb{Q}_\ell, s) = L(g, s)$$

where g is a cusp form of weight $3 = 2+1$ on some congruence subgroup $\Gamma_1(N)$ or $\Gamma_0(N)$ with a character. Here $\Gamma_1(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \,|\, a \equiv d \equiv 1 \pmod N\}$. Also the space of cusp forms of weight 3 on $\Gamma_0(N)$ is empty, so we ought to twist forms by a character.

In more representation theoretic formulation, this theorem can be stated as follows.

Theorem 4.5. (Livné [**Liv95**]) *Let π be the compatible family of 2-dimensional ℓ-adic Galois representations associated to $T(X)$ and let $L(\pi, s)$ be its L-series. Then there exists a unique cusp form g of weight 3, level the conductor of π and a Dirichlet (odd) character $\varepsilon(p) = (\frac{-d}{p})$ such that $L(\pi, s) = L(g, s)$.*

Remark 4.6. If X is no longer singular (extremal), the modularity question is still open. However, if X has Picard number $\rho(X) = 19$, X is equipped with a Shioda–Inose structure and consequently X is either a Kummer surface or a double cover of a Kummer surface ([**SI77**] and also [**Mor84**]). So there is the underlying elliptic curve which gives rise to Kummer surface, and the modularity of the transcendental part may be realized by taking the symmetric square of a cusp form of weight 2 associated to the underlying elliptic curve. In fact, this approach has been carried out by Ling Long [**Lon03**] for a certain family of $K3$ surfaces with Picard number 19.

5. The modularity for rigid Calabi–Yau threefolds over $\mathbb{Q}$

Now we will try to generalize the modularity results to Calabi–Yau threefolds defined over $\mathbb{Q}$. For Calabi–Yau threefolds, the Betti numbers B_2, B_3 are not fixed constants, nor the Euler characteristic. A natural question is:

Is there an absolute constant which bounds the absolute value of the Euler characteristic $E(X)$?

The current record for the upper bound for the absolute value of the Euler characteristic is $|E(X)| \leqslant 960$. This is based on available examples of Calabi–Yau threefolds constructed by physicists using Batyrev's reflexive polytopes. However, Miles Reid claims there should not be such a constant (based on his experience with MMP (Minimal Model Program)).

We first make a crude classification of Calabi–Yau threefolds.

Definition 5.1. A Calabi–Yau threefold X is said to be *rigid* if $h^{2,1} = 0$ (so that $B_3 = 2$). Otherwise, X is said to be *non-rigid*.

Remark 5.2. A rigid Calabi–Yau threefold is indeed the natural generalization of an elliptic curve. The third Betti number $B_3 = 2$ and accordingly there is a 2-dimensional Galois representation associated to it.

The modularity conjecture for rigid Calabi–Yau threefolds over $\mathbb{Q}$. *Let X be a rigid Calabi–Yau threefold defined over $\mathbb{Q}$. Then X is modular. That is, there exists a cusp form f of weight $4 = 3 + 1$ on some $\Gamma_0(N)$ such that*

$$L(X, s) = L(f, s),$$

up to a finite number of Euler factors. Here N is divisible only by primes of bad reduction.

This conjecture was formulated in M-H. Saito and Yui [**SY01**].

Remark 5.3.

1. This conjecture is a special case of the Fontaine–Mazur conjecture that *every irreducible odd 2-dimensional Galois representation "coming from geometry" should be modular, up to a Tate twist.*
2. Also this is a special case of the Serre conjecture about the modularity of the residual mod p 2-dimensional Galois representations attached to certain odd dimensional projective varieties over $\mathbb{Q}$.
3. This may be regarded as a concrete realization of the Langlands Program.

Explicit description of $L(X,s)$. Let X be a rigid Calabi–Yau threefold defined over $\mathbb{Q}$. Then X always has an integral model. Let p be a good prime, and let Frob_p be the Frobenius morphism. Then the characteristic polynomial $P_p(T)$ has the form

$$P_p(T) = 1 - t_3(p)T + p^3T^2 \in 1 + T\mathbb{Z}[T] \quad \text{with } |t_3(p)| \leqslant 2p^{3/2}$$

Then

$$L(X,s) = (*) \prod_{p:\text{good}} P_p(p^{-s})^{-1} = (*) \prod_{p:\text{good}} \frac{1}{1 - t_3(p)p^{-s} + p^{3-2s}}$$

where $(*)$ stands for the factors corresponding to bad primes.

As for elliptic curves over $\mathbb{Q}$, the local Euler p-factor of $L(X,s)$, that is, essentially $t_3(p)$, can be described in terms of the number of $\mathbb{F}_p$-rational points on X.

For each i, $0 \leqslant i \leqslant 6$, let

$$t_i(p) := \mathrm{trace}(\mathrm{Frob}_p^* \,|\, H^i_{et}(\bar{X}, \mathbb{Q}_\ell))$$

be the trace of the Frob_p^* on the étale ℓ-adic i-th cohomology group. Then the Lefschetz fixed point formula asserts that

$$\#X(\mathbb{F}_p) = \sum_{i=0}^{6} (-1)^i t_i(p) = t_0(p) - t_1(p) + t_2(p) - t_3(p) + t_4(p) - t_5(p) + t_6(p).$$

By the Poincaré duality on the étale ℓ-adic cohomology groups, we have

$$\#X(\mathbb{F}_p) = 1 + p^3 + (1+p)t_2(p) - t_3(p) \leqslant 1 + p^3 + (1+p)ph^{1,1} - t_3(p).$$

The inequality becomes an equality if all cycles in $H^{1,1}(X)$ are defined over $\mathbb{Q}$, in which case, we have

$$t_3(p) = 1 + p^3 + (1+p)p^{1,1} - \#X(\mathbb{F}_p).$$

Theorem 5.4. *Up to date, there are at least* 50 *rigid Calabi–Yau threefolds over* $\mathbb{Q}$ *for which the modularity is established.*

Methods. There are several methods for establishing the modularity for rigid Calabi–Yau (and for non-rigid Calabi–Yau) threefolds defined over $\mathbb{Q}$.

Method 1: The Serre–Faltings criterion.
Method 2: Wiles method.
Method 3: Algebraic correspondence (Tate's conjecture).
Method 4: Conifolds method.
Method 5: Intermediate Jacobians.

(We should remark that Methods 1 and 2 are exclusively for rigid Calabi–Yau threefolds, while the other Methods are applicable for rigid as well as for non-rigid Calabi–Yau threefolds.)

• **The Serre–Faltings criterion**:
Let f be a cusp form of weight 4 on some $\Gamma_0(N)$ and write

$$f(q)=\sum_{n=1}^{\infty}a_f(n)q^n \quad \text{with } q=e^{2\pi iz} \text{ and } a_f(1)=1$$

Suppose that
(Serre) $t_3(p)=a_f(p)$ for all good primes p;
(Faltings) $t_3(p)=a_f(p)$ for finitely many good primes p.
Then invoking the Chebotarev Density Theorem, the semisimplifications of the two 2-dimensional Galois representations associated to X and f are equivalent, so that $L(X,s)=L(f,s)$, up to a finite number of Euler factors.

• **Wiles method**:
In Wiles' proof of the Shimura–Taniyama conjecture for elliptic curves, prime $\ell=3$ played very crucial role (backed up by prime $\ell=5$). For rigid Calabi–Yau threefolds over $\mathbb{Q}$, a similar criterion has been established.

Theorem 5.5. (Dieulefait and Manoharmayum [**DM03**], You-Chiang Yi [**Yi**])
Let X be a rigid Calabi–Yau threefold defined over $\mathbb{Q}$. Suppose that X satisfies one of the following two conditions:
(1) X has good reduction at 3 and 7, or
(2) X has good reduction at 5 and some prime $p\equiv\pm2 \pmod 5$ with $t_3(p)$ not divisible by 5.
Then X is modular.

• **Algebraic Correspondence (Tate's conjecture)**
Given a rigid Calabi–Yau threefold over $\mathbb{Q}$, its modularity can be established by constructing an algebraic correspondence to a modular rigid Calabi–Yau threefold over $\mathbb{Q}$. This approach is based on the conjecture of Tate that
the isomorphism between two Galois representations is induced by an algebraic correspondence.

First we need to construct rigid Calabi–Yau threefolds over $\mathbb{Q}$, which are associated to modular groups. This has been done by C. Schoen.

Theorem 5.6. (Schoen [**Sch88**]; Cf. Beauville [**Bea82**]) *Let $\Gamma\subset PSL_2(\mathbb{Z})$ be a congruence subgroup of finite index, and let $C_\Gamma:=(\mathfrak{H}/\Gamma)^*$ be the modular curve. Let S_Γ be the universal family of elliptic curves over C_Γ. Let $Y:=S_\Gamma\times_{\mathbb{P}^1}S_\Gamma$ be the self-fiber product of S_Γ, and let X be a smooth resolution of*

Y. Then X is a rigid Calabi–Yau threefold when Γ is one of the following six groups:

$$\Gamma(3),\ \Gamma_1(4)\cap\Gamma(2),\ \Gamma_1(5),\ \Gamma_1(6),\ \Gamma_0(8)\cap\Gamma_1(4),\ \Gamma_0(9)\cap\Gamma_1(3).$$

Beauville [**Bea82**] determined explicit defining equations over $\mathbb{Q}$ for the rational elliptic surfaces S_Γ for the above modular groups.

Theorem 5.7. (Verill [**Yui03**]) *The six rigid Calabi–Yau threefolds constructed in Theorem 5.3 have explicit defining equations over $\mathbb{Q}$. Furthermore, they are all modular. That is, there is a cusp form f of weight 4 on Γ such that*

$$L(X,s)=L(f,s).$$

Now we will give one example of rigid Calabi–Yau threefold over $\mathbb{Q}$ whose modularity is established by constructing an explicit algebraic correspondence to one of the six modular rigid Calabi–Yau threefolds in Theorem 5.4.

Theorem 5.8. (M.H. Saito and N. Yui [**SY01**]) *Let V be the Verrill Calabi–Yau threefold over $\mathbb{Q}$ associated to the root lattice A_3. Then V is realized as a smooth (small) resolution of the hypersurface*

$$(x+y+z+w)(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}+\frac{1}{w})-\frac{(t-2)^2}{t}-4=0$$

in $\mathbb{P}^4\times\mathbb{P}^1$, and V is a rigid Calabi–Yau threefold with the Euler characteristic 100.

Let $S_{\Gamma_1(6)}$ be a rational elliptic surface defined by the hypersurface

$$(x+y+z)(xy+yz+zx)=(s+1)xyz$$

associated to $\Gamma_1(6)$. Let Y be the self-fiber product of $S_{\Gamma_1(6)}$ and let $\tilde{Y}$ be a crepant resolution of Y. Then there is an explicit birational transformation defined over $\mathbb{Q}$ from V to $\tilde{Y}$. This birational map is compatible with the Galois action, and induces an equivalence of the associated Galois representations. Consequently,

$$L(V,s)=L(\tilde{Y},s)=\eta(q)^2\eta(q^2)^2\eta(q^3)^2\eta(q^6)^2.$$

Remark 5.9.

1. Verrill [**Ver00**] has proved the modularity of V using the Serre–Faltings criterion. Also Dieulefait and Manoharmayum [**DM03**] and Yi [**Yi**] have established the modularity of V using Wiles method. The above proof of Saito and Yui is more geometric along the line of Tate's conjecture.

2. Recently, Schütt [**Sch03**] has applied the construction of Schoen to twisted self-fiber products $(S_{\Gamma_1(6)}, pr) \times_{\mathbb{P}^1} (S_{\Gamma_1(6)}, \pi \circ pr)$ where pr is the natural projection and π is a non-trivial automorphism of $\mathbb{P}^1$ interchanging $0, 1, \infty$. Choosing π appropriately, he obtained four more rigid Calabi–Yau threefolds over $\mathbb{Q}$ associated to cusp forms of weight 4 and level $10, 17, 21$ and 73. His method should work for other groups listed in Theorem 5.3.

• **Conifolds Method**:
This method has been developed by Candelas, de la Ossa and Villegas [**CdlORV03**], and works for one-parameter families of Calabi–Yau complete intersection threefolds. The Picard–Fuchs differential equations of these families turn out to be Gauss hypergeometric series. At conifold points (i.e., assigning special values to the parameter), certain one-parameter families give rise to rigid Calabi–Yau threefolds, and their modularity can be established studying periods of the families.

• **Intermediate Jacobians**:
This method has not yet produced results. I would like to mention this approach hoping that someone might work on it. The (Griffith) *intermediate Jacobian* of a Calabi–Yau threefold X is defined by

$$J^2(X) = \frac{H^{1,2}(X) \oplus H^{0,3}(X)}{H_3(X, \mathbb{Z})}.$$

In particular, if X is rigid, $J^2(X) \simeq \mathbb{C}/\mathbb{Z}^2$ is nothing but a complex torus (an abelian variety of dimension 1). We will now make a conjecture:

A rigid Calabi–Yau threefold over $\mathbb{Q}$ is modular if $J^2(X)$ is defined over $\mathbb{Q}$ (and hence modular).

One class of Calabi–Yau threefolds for which we might be able to get relations between intermediate Jacobians and Calabi–Yau threefolds is the class of rigid Calabi–Yau threefolds of CM type. We say that a rigid Calabi–Yau threefold X is *of CM type* if and only if the intermediate Jacobian $J^2(X)$ is of CM type (as an abelian variety of dimension 1).

Example 5.10. (X. Xarles and N. Yui [**XY**]) Let X be a rigid Calabi–Yau threefold defined over a number field F of CM type. Then the intermediate Jacobian $J^2(X)$ is an elliptic curve with CM by an imaginary quadratic field K, and has a model defined over F.

If χ is a Hecke character associated to $J^2(X)$, and suppose that

$$L(J^2(X), s) = \begin{cases} L(\chi, s) & \text{if } F \text{ does not contain } K \\ L(\chi, s)L(\bar{\chi}, s) & \text{if } F \text{ contains } K \end{cases}$$

then

$$L(X, s) = \begin{cases} L(\chi^3, s) & \text{if } F \text{ does not contain } K \\ L(\chi^3, s)L(\bar{\chi}^3, s) & \text{if } F \text{ contains } K \end{cases}$$

Consequently, X is modular.

Remark 5.11. Shioda and Inose [**SI77**] showed that the isomorphism classes of singular $K3$ surfaces is in one-to-one correspondence with the $SL_2(\mathbb{Z})$-equivalence classes of positive definite even binary quadratic forms. Consequently every singular $K3$ surface has a CM by an imaginary quadratic field (or an imaginary quadratic order). This example may be viewed as a generalization of the result of Shoida and Inose to rigid Calabi–Yau threefolds of CM type. The result of Shioda and Inose and this example provide evidence to the conjecture of Shafarevich that

A variety of CM type is defined over a number field, and its L-series is expressed as a product of the L-series of one-dimensional characters associated to the field of definition of the variety.

6. The modularity of non-rigid Calabi–Yau threefolds over $\mathbb{Q}$

Now we will address the modularity question for non-rigid Calabi–Yau threefolds defined over $\mathbb{Q}$. Let X be a non-rigid Calabi–Yau threefold. Then $h^{2,1} \neq 0$ so that $B_3 \geqslant 4$. Consequently, the Galois representation associated to X has dimension $\geqslant 4$, and the modularity question becomes increasingly more challenging, though the Langlands Program predicts that there should be some automorphic form(s) determining the L-series and zeta-functions. Up to date, we have constructed only a handful of examples of non-rigid Calabi–Yau threefolds and have established their modularity.

There are several methods to establish the modularity of non-rigid Calabi–Yau threefolds defined over $\mathbb{Q}$.

Method 1: When the B_3-dimensional Galois representation splits into a sum of 2-dimensional Galois representations, apply the method developed for rigid Calabi–Yau threefolds to these rank 2 motives.

Method 2: Construct *modular* non-rigid Calabi–Yau threefolds over $\mathbb{Q}$ (which are the non-rigid analogues of modular rigid Calabi–Yau threefolds discussed in Theorem 5.3 and Theorem 5.4.) To establish the modularity of a given non-rigid Calabi–Yau threefold, construct an algebraic correspondence to a modular non-rigid Calabi–Yau threefold (Tate's conjecture) as Saito and Yui [**SY01**] did for rigid Calabi–Yau threefolds in Theorem 5.5.

We will now give examples illustrating Method 1 and Method 2. For more complete list of examples, see Yui [**Yui03**].

Example of van Geemen and Nygaard [vGN95]. Let $Y \subset \mathbb{P}^7$ be the complete intersection defined by

$$\begin{aligned} Y_0^2 &= 2(X_0X_1 + X_2X_3) \\ Y_1^2 &= 2(X_0X_2 + X_1X_3) \\ Y_2^2 &= 2(X_0X_3 + X_1X_2) \\ Y_3^2 &= 2(X_0X_1 - X_2X_3) \end{aligned}$$

The singular locus of Y consists of 16 double points and 4 plane conics intersecting transversally, configured in a square.

Take a resolution X of Y. Then X is a Calabi–Yau threefold with

$$h^{3,0} = 1,\ h^{2,1} = 1,\ h^{1,1} = 41.$$

So $B_3 = 4$, and there is a 4-dimensional Galois representation attached to X. Let $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL(H^3_{et}(\bar{X}, \mathbb{Q}_\ell))$ be the Galois representation. Let $i = \sqrt{-1}$ and let

$$[i] : (Y_0 : Y_1 : Y_2 : Y_3 : X_0 : X_1 : X_2 : X_3) \mapsto$$
$$(Y_0 : Y_2 : Y_1 : iY_3 : X_2 : X_3 : X_0 : X_1)$$

be an automorphism of X. Then $[i]$ induces a linear transformation on $H^3_{et}(\bar{X}, \mathbb{Q}_\ell)$. This splits the 4-dimensional Galois representation into a sum of two 2-dimensional Galois representations.

Theorem 6.1.
(a) The L-series is expressed in terms of the Hecke character ψ of $\mathbb{Q}(i)$:

$$L(X, s) = L(\psi^3, s)L(\psi, s-1)$$

(b) $L(X, s)$ occurs as a factor in the L-series $L(H^3_{et}(\bar{E}^3, \mathbb{Q}_\ell), s)$ where $E : y^2 = 1 + x^4$ is an elliptic curve with CM by $\mathbb{Z}[i]$.
(c) There exists an algebraic correspondence between X and E^3, which induces the isomorphism of the two Galois representations.
(d) X is realized as a Siegel modular threefold over $\mathbb{Q}$.

Remark 6.2. Recently, K. Hulek and H. Verrill [**HV**] have established the modularity of non-rigid Calabi–Yau threefolds over $\mathbb{Q}$ arising from the root lattice A_4. In their example, B_3-dimensional Galois representations also split into sums of 2-dimensional ones.

Now we will construct *modular* non-rigid Calabi–Yau threefolds over $\mathbb{Q}$ as Schoen [**Sch88**] and Verrill [**Yui03**] did for the rigid case.

Motivations for the examples of Livné and Yui [LY]. The motivation for these examples come from a rather unexpected source, i.e., a paper of Sun, Tan and Zuo [**STZ**] in which they considered Calabi–Yau threefold $f : X \to \mathbb{P}^1$ fibered by semi-stable $K3$ surfaces. Let $S \subset \mathbb{P}^1$ be a finite set of points over which f is non-smooth, and let $\Delta \subset X$ be the pull-back of S. Let $\omega_{X/\mathbb{P}^1}$ be the canonical sheaf. The Kodaira–Spencer maps $\theta^{2,0}$ and $\theta^{1,1}$ are, respectively, defined by

$$f_*\Omega^2_{X/\mathbb{P}^1}(\log\Delta) \stackrel{\theta^{2,0}}{\to} R^1 f_*\Omega^1_{X/\mathbb{P}^1}(\log\Delta)\otimes\Omega^1_{\mathbb{P}^1}(\log S) \stackrel{\theta^{1,1}}{\to} R^2 f_*(\mathscr{O}_{X/\mathbb{P}^1})\otimes\Omega^1_{\mathbb{P}^1}(\log S)^{\otimes 2},$$

and the iterated Kodaira–Spencer map is $\theta^{1,1}\theta^{2,0}$.

Also there is the Arakelov–Yau type inequality for X:

$$\deg f_*\omega_{X/\mathbb{P}^1} \leqslant \deg\Omega^1_{\mathbb{P}^1}(\log S).$$

Sun, Tan and Zuo [**STZ**] considered a $K3$-fibered Calabi–Yau threefold for which the Arakelov–Yau inequality reaches the upper bound and becomes an equality. In case of non-rigid Calabi–Yau threefolds, a stronger equality holds.

$$2 = \deg f_*\omega_{X/\mathbb{P}^1} = \begin{cases} \deg\Omega^1_{\mathbb{P}^1}(\log S) & \text{if } X \text{ is rigid} \\ \frac{1}{2}\deg\Omega^1_{\mathbb{P}^1}(\log S) & \text{if } X \text{ is non-rigid} \end{cases}$$

Theorem 6.3. (Sun, Tan and Zuo [**STZ**]) *Let $f : X \to \mathbb{P}^1$ be a Calabi–Yau threefold fibered by non-constant semi-stable $K3$ surfaces, reaching the Arakelov–Yau bound.*

(a) If the iterated Kodaira–Spencer map is non-zero, then f has at least four singular fibers. If f has exactly four singular fibers, then X is rigid, and is birational to one of the six rigid Calabi–Yau threefolds in Theorem 5.3 and Theorem 5.4.

(b) If the iterated Kodaira–Spencer map is zero, then f has at least six singular fibers. If f has exactly six singular fibers, then X is non-rigid, the general fibers have Picard number at least 18, *and $\mathbb{P}^1 \setminus S \simeq \mathfrak{H}/\Gamma$ for some subgroup of $PSL_2(\mathbb{Z})$ of index* 24.

Remark 6.4. The three authors used the terminology "modularity" in the title of their paper to refer to the fact that $\mathbb{P}^1 \setminus S$ is a modular variety.

For the rigid case (a), we have established the modularity in our sense, i.e., for the L-series. We are inspired to consider the modularity of the L-series for the non-rigid case (b).

Examples of Livné and Yui [LY]. Livné and Yui [**LY**] have constructed several examples of non-rigid Calabi–Yau threefolds which satisfy the conditions of Theorem 6.2 (b). Our idea of producing such examples is as follows. Let E be an elliptic curve and let Y be a singular $K3$ surface, both defined over $\mathbb{Q}$. We know that both E and Y are modular by the discussions in Section 3 and Section 4, respectively. We consider the product $Y \times E$, though it is not Calabi–Yau. If we choose Y appropriately, then there is an action of ± 1 on the product. Take the quotient $Y \times E/\pm 1$ and let X be its smooth resolution. Then we will show that X is a non-rigid Calabi–Yau threefold satisfying the conditions of Theorem 6.2 (b).

We now choose for Y a special type of $K3$ surfaces, namely, elliptic modular $K3$ surfaces. The concept of elliptic modular surfaces was introduced by Shioda [**Shi72**], and we will follow his exposition.

Definition 6.5. Let $\bar{\Gamma} \subset PSL_2(\mathbb{Z})$ be a genus zero, torsion-free congruence subgroup of index $\mu < \infty$. Then $\bar{\Gamma}$ can be lifted to a congruence subgroup $\Gamma \subset SL_2(\mathbb{Z})$ of finite index with the property that Γ has no elliptic elements of trance -2. Let $C_\Gamma := (\mathfrak{H}/\Gamma)^*$ be the corresponding modular curve. Consider the automorphism of $\mathfrak{H} \times \mathbb{C}$ defined by

$$(\tau, z) \mapsto (\frac{a\tau + b}{c\tau + d}, \frac{z + m\tau + n}{c\tau + d})$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, $\tau \in \mathfrak{H}$, $z \in \mathbb{C}$ and $(m, n) \in \mathbb{Z}^2$. The quotient of $\mathfrak{H} \times \mathbb{C}$ by this action defines a surface equipped with a morphism to C_Γ. The general fiber for $\tau \in \mathfrak{H}$ is an elliptic curve $E_{\Gamma,\tau}$ corresponding to the lattice $\mathbb{Z} + \tau\mathbb{Z}$. This is called an *elliptic modular surface* associated to Γ, and its geometric genus is given by $p_g = \frac{\mu}{12} - 1$.

We are interested in semi-stable elliptic modular $K3$ surfaces with maximal Picard number 20, that is, singular (extremal) $K3$ surfaces, and semi-stable means that an elliptic fibration has only singular fibers of type I_n, $n > 0$.

Theorem 6.6.

(a) (Sebbar [**Seb01**]) *There are nine semi-stable elliptic modular $K3$ surfaces with Picard number 20. They correspond to the congruence lifts to $SL_2(\mathbb{Z})$ of genus zero, torsion-free congruence subgroups of $PSL_2(\mathbb{Z})$ of index 24 and 6 cusps with cusp widths adding up to 24.*

index	*Number of cusps*	*Group*	*Cusp widths*	#
12	4	$\Gamma(3)$	$3,3,3,3$	
		$\Gamma_0(4)\cap\Gamma(2)$	$4,4,2,2$	
		$\Gamma_1(5)$	$5,5,1,1$	
		$\Gamma_0(6)$	$6,3,2,1$	
		$\Gamma_0(8)$	8.2.1.1	
		$\Gamma_0(9)$	$9,1,1,1$	
24	6	$\Gamma(4)$	$4,4,4,4,4,4$	#1
		$\Gamma_0(3)\cap\Gamma(2)$	$6,6,6,2,2,2$	#2
		$\Gamma_1(7)$	$7,7,7,1,1,1$	#3
		$\Gamma_1(8)$	$8,8,4,2,1,1$	#4
		$\Gamma_0(8)\cap\Gamma(2)$	$8,8,2,2,2,2$	#5
		$\Gamma(8;4,1,2)$	$8,4,4,4,2,2$	#6
		$\Gamma_0(12)$	$12,4,3,3,1,1$	#7
		$\Gamma_0(16)$	$16,4,1,1,1,1$	#8
		$\Gamma(16;16,2,2)$	$16,2,2,2,1,1$	#9

Here

$$\Gamma(8;4,1,2) := \{\pm\begin{pmatrix}1+4a & 2b\\ 4c & 1+4d\end{pmatrix},\ a\equiv c \pmod 2\}$$

and

$$\Gamma(16;16,2,2) := \{\pm\begin{pmatrix}1+4a & b\\ 8c & 1+4d\end{pmatrix},\ a\equiv c \pmod 2\}.$$

(b) (Livné and Yui [**LY**], Top and Yui [**TY**]) *In each of the nine singular elliptic modular $K3$ surfaces, there is an explicit defining equation over $\mathbb{Q}$ for it.*

(c) (Livné [**Liv95**]) *The nine singular elliptic modular $K3$ surfaces over $\mathbb{Q}$ are all modular. (Cf. Theorem 4.2 and Theorem 4.3.)*

Remark 6.7.

1. The cusps correspond to singularities of type I_n, and cusp widths coincide with multiplicities of singular fibers.

2. The groups of index 12 in the Table correspond to rational elliptic modular surfaces. These six groups were first found by Beauville [**Bea82**] and also by Schoen [**Sch88**], and then rediscovered by Sebbar [**Seb01**]. These groups are also discussed in Theorem 5.3 where the self-fiber products of these surfaces gave rise to six modular rigid Calabi–Yau threefolds defined over $\mathbb{Q}$ (cf. Theorem 5.4).

Now we will state the main results of Livneé and Yui [**LY**].

Theorem 6.8. *Let Y be one of the singular elliptic modular $K3$ surfaces in the Table. Let $T(Y)$ be the transcendental lattice of Y. Let E be an elliptic curve. Consider the product $Y \times E$. We view this product as a family of abelian surfaces over the base modular curve C_Γ. The fiber $A_t = A_{\Gamma,t}$ over each point $t \in C_\Gamma$ is the product of the fiber $E_{\Gamma,t}$ with E.*

(a) The product $Y \times E$ has the Hodge numbers

$$h^{0,3}(Y \times E) = 1,\ h^{1,0}(Y \times E) = 1 = h^{2,0}(Y \times E) \quad \text{and } B_3(Y \times E) = 44,$$

so that $Y \times E$ is not a Calabi–Yau threefold.

(b) The motive $T(Y \times E) = T(Y) \times H^1(E)$ is a submotive of $H^3(Y \times E)$. If both Y and E are defined over $\mathbb{Q}$, this submotive is modular, in the sense that its L-series is associated to cusp forms of weight 3 and 2. That is,

$$L(T(Y \times E), s) = L(g_Y \otimes g_E, s)$$

where g_Y is a weight 3 cusp form associated to $T(Y)$ and g_E is a weight 2 cusp form associated to E.

Now take the quotient $Y \times E/ \pm 1$, where we divide each fiber A_t of $Y \times E$ by ± 1 and then blow up the locus of points of order 2 (i.e., a Kummer construction). Let X denote a smooth resolution of $Y \times E/ \pm 1$.

Theorem 6.9. *For all groups Γ except for $\Gamma_1(7)$ of index 24 in the Table, the resolution X is a smooth Calabi–Yau threefold, and the following assertions hold for X*

(a) X non-rigid.

(b) The given fibration $f : X \to C_\Gamma$ is semi-stable, with vanishing (iterated) Kodaira–Spencer map.

(c) The Arakelov–Yau equality holds for X, that is, we have

$$deg\, f_*\omega_{X/\mathbb{P}^1} = 2 = \frac{1}{2} deg\, \Omega^1_{\mathbb{P}^1}(\log S)$$

where $S \subset \mathbb{P}^1$ is the finite set of six points above which f is non-smooth.

(d) X is modular.

Remark 6.10.

1. We note that in $PSL_2(\mathbb{R})$, the groups Γ of index 24 can be divided into four conjugacy classes: $\{\#1, \#5, \#8\}$, $\{\#2, \#7\}$, $\{\#4, \#6, \#9\}$, and $\{\#3\}$.
2. The groups $\#1, \#2, \#5$ and $\#6$ are all subgroups of $\Gamma(2)$. This guarantees that the 2-torsion points of the fiber A_t are distinct for all $t \in X_\Gamma$, and it follows that the locus of 2-torsion points is smooth and hence so is the blow up X. By the above remark, this holds true for all groups except for $\#3 = \Gamma_1(7)$. Also notice that all singular fibers are of type I_n, $n > 1$ with n even for these groups except for $\Gamma_1(7)$.
3. The group $\Gamma_1(7)$ is not a subgroup of $\Gamma(2)$ and the 2-torsion points introduce singularities. K. Hulek studied these singularities. A smooth resolution is no longer a Calabi–Yau threefold. However, its L-series is modular, indeed it is associated to a modular form of weight 3 and two kinds of modular forms of weight 2.

7. Open Problems

Problem 7.1. For elliptic curves over $\mathbb{Q}$, Shimura constructed a map from the set of Hecke eigenforms of weight 2 with rational Fourier coefficients on $\Gamma_0(N)$ to the isogeny classes of elliptic curves over $\mathbb{Q}$. What Wiles et al. established is that this Shimura map is onto, thereby proving the Shimura–Taniyama conjecture.

For rigid Calabi–Yau threefolds over $\mathbb{Q}$, a natural question is:

Which Hecke eigenforms of weight 4 *on* $\Gamma_0(N)$ *correspond to rigid Calabi–Yau threefolds over* $\mathbb{Q}$*?.*

In fact, this question has been raised by several people, e.g., B. Mazur, D. van Straten, B. van Geemen, K. Hulek.

Problem 7.2. In Examples of Livné and Yui [**LY**], singular $K3$ surfaces Y may be replaced by $K3$ surfaces with smaller Picard numbers, say, 19 or 18. In this case, the modularity for the product $Y \times E$ is still open. If the Picard number is 19, we know that the rank 3 motive $T(Y)$ is self-dual orthogonal via the cup product. By the structure theorem for $K3$ surfaces with Picard number 19 described in Remark 4.2, there should be a cusp form h of weight 2 on $GL(2)$ such that the symmetric square $\mathrm{Symm}^2 h$ should realize $T(Y)$. Then $T(Y \times E)$ may be realized by an automorphic form on $GL(6, \mathbb{Q})$. In particular, $L(\mathrm{Symm}^2 h \otimes g_E, s)$ has the expected analytic properties.

Problem 7.3. In case of rigid Calabi–Yau threefolds corresponding to the index 12 groups in the Table, Sun, Tan and Zuo [**STZ**] showed that they all reach the Arakelov–Yau bound. We also know that they are all modular by Theorem 5.4. In case of non-rigid Calabi–Yau threefolds, Livné and Yui [**LY**] showed that all eight (except for the case corresponding $\Gamma_1(7)$ as we did not compute it yet) reach the Arakelov–Yau bound and also they are all modular. A question is:

What is the implication of the Arakelov–Yau equalities to the modularity? Is it a necessary condition, or a sufficient condition, or both?

References

[BCDT01] C. Breuil, B. Conrad, F. Diamond & R. Taylor – On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), no. 4, p. 843–939.

[Bea82] A. Beauville – Les familles stables de courbes elliptiques sur $\mathbf{P}^1$ admettant quatre fibres singulières, *C. R. Acad. Sci. Paris Sér. I Math.* **294** (1982), no. 19, p. 657–660.

[CdlORV03] P. Candelas, X. de la Ossa & F. Rodriguez-Villegas – Calabi-Yau manifolds over finite fields. II, Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), Fields Inst. Commun., vol. 38, Amer. Math. Soc., Providence, RI, 2003, p. 121–157.

[DM03] L. Dieulefait & J. Manoharmayum – Modularity of rigid Calabi-Yau threefolds over $\mathbb{Q}$, Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), Fields Inst. Commun., vol. 38, Amer. Math. Soc., Providence, RI, 2003, p. 159–166.

[HV] K. Hulek & H. Verrill – On modularity of rigid and non-rigid Calabi-Yau varieties associated to the root lattice A_4, `arXiv:math.AG/0304169`.

[Liv95] R. Livné – Motivic orthogonal two-dimensional representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, *Israel J. Math.* **92** (1995), no. 1-3, p. 149–156.

[Lon03] L. Long – On a Shioda-Inose structure of a family of $K3$ surfaces, Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), Fields Inst. Commun., vol. 38, Amer. Math. Soc., Providence, RI, 2003, p. 201–207.

[LY] R. Livné & N. Yui – The modularity of certain non-rigid Calabi-Yau threefolds, `arXiv:math.AG/0304497`.

[Mor84] D. R. Morrison – On $K3$ surfaces with large Picard number, *Invent. Math.* **75** (1984), no. 1, p. 105–121.

[Sch88] C. Schoen – On fiber products of rational elliptic surfaces with section, *Math. Z.* **197** (1988), no. 2, p. 177–199.

[Sch03] M. Schütt – New examples of modular rigid Calabi–Yau threefolds, 2003, preprint.

[Seb01] A. Sebbar – Classification of torsion-free genus zero congruence groups, *Proc. Amer. Math. Soc.* **129** (2001), no. 9, p. 2517–2527.

[Shi72] T. Shioda – On elliptic modular surfaces, *J. Math. Soc. Japan* **24** (1972), p. 20–59.

[SI77] T. Shioda & H. Inose – On singular $K3$ surfaces, Complex analysis and algebraic geometry, Iwanami Shoten, Tokyo, 1977, p. 119–136.

[STZ] X. Sun, S.-L. Tan & K. Zuo – Families of K3 surfaces over curves satisfying the equality of Arakelov-Yau's type and modularity, CUHK-2002.

[SY01] M.-H. Saito & N. Yui – The modularity conjecture for rigid Calabi-Yau threefolds over Q, *J. Math. Kyoto Univ.* **41** (2001), no. 2, p. 403–419.

[TW95] R. Taylor & A. Wiles – Ring-theoretic properties of certain Hecke algebras, *Ann. of Math. (2)* **141** (1995), no. 3, p. 553–572.

[TY] J. Top & N. Yui – Explicit equations of some elliptic modular surfaces.

[Ver00] H. A. Verrill – The L-series of certain rigid Calabi-Yau threefolds, *J. Number Theory* **81** (2000), no. 2, p. 310–334.

[vGN95] B. van Geemen & N. O. Nygaard – On the geometry and arithmetic of some Siegel modular threefolds, *J. Number Theory* **53** (1995), no. 1, p. 45–87.

[Wil95] A. Wiles – Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)* **141** (1995), no. 3, p. 443–551.

[XY] X. Xarles & N. Yui – The modularity of Calabi–Yau threefolds of CM type, in preparation.

[Yi] Y.-C. Yi – On the modularity of a rigid Calabi–Yau threefold, to appear.

[Yui03] N. Yui – Update on the modularity of Calabi-Yau varieties, Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), Fields Inst. Commun., vol. 38, Amer. Math. Soc., Providence, RI, 2003, With an appendix by Helena Verrill, p. 307–362.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 31–36
Universität Göttingen, 2004

COUNTING RATIONAL POINTS ON CUBIC THREEFOLDS

T. D. Browning
Mathematical Institute, 24–29 St. Giles', Oxford OX1 3LB, U.K.
E-mail : browning@maths.ox.ac.uk

Abstract. This is a survey of recent results concerning rational points of bounded height on hypersurfaces of degree ≥ 3.

For any $n \geqslant 3$, let $X \subset \mathbb{P}^{n-1}$ be an irreducible hypersurface of degree d, where irreducibility is henceforth taken to mean geometric irreducibility. The purpose of this note is to discuss recent joint work with Professor Heath-Brown [**BHB**], in which we investigate the asymptotic behaviour of the quantity

$$N_U(B) = \#\{x \in U \cap \mathbb{P}^{n-1}(\mathbb{Q}) : H(x) \leqslant B\},$$

as $B \to \infty$. Here $U \subseteq X$ is an arbitrary open subset and $H : \mathbb{P}^{n-1}(\mathbb{Q}) \to \mathbb{R}_{\geqslant 0}$ is the usual projective height. Whenever $d = 1$ or 2 this quantity is very well understood, and it is not hard to establish the estimate

$$N_X(B) = c_X B^{n-d}\Big(1 + o(1)\Big),$$

for some constant $c_X > 0$. As the degree d increases, so the problem of describing $N_X(B)$ becomes harder. To illustrate this we consider the case $d = n = 5$ of quintic threefolds, in which setting it is not at all clear what to expect $N_X(B)$

October 27th, 2003.

to behave like as $B \to \infty$. For example we know of only one rational point on the variety

$$x_1^5 + x_2^5 + x_3^5 + x_4^5 = x_5^5.$$

This is the solution $\mathbf{x} = (27, 84, 110, 133, 144)$, as found by Lander and Parkin [**LP66**] in a computer search. It is interesting to remark that this provided the first counter-example to a conjecture of Euler that no kth power can be written as the sum of $k-1$ kth powers.

We now come to discuss the primary motivation of this work. This is the following conjecture of Heath-Brown [**HB02**, Conjecture 2].

Conjecture 1. *Suppose that $X \subset \mathbb{P}^{n-1}$ is an irreducible hypersurface of degree $d \geqslant 2$. Then we have*

$$N_X(B) = O(B^{n-2+\varepsilon}).$$

Here, and throughout this note, the implied constant may depend at most upon d, n and the choice of ε. One might also ask about bounds of the shape $N_X(B) = O_X(B^{n-2+\varepsilon})$, as in [**HB02**, Conjecture 1], where the implied constant is allowed to depend on the coefficients of F. However it transpires that estimates which are uniform in forms of fixed degree, and with a fixed number of variables, are much more useful in applications, and that in most cases results with weaker uniformity appear to be no easier to prove.

It should be clear that the bound's exponent in Conjecture 1 is in general essentially as sharp as can be hoped for. Indeed, whenever the hypersurface X is given by an equation of the form $x_1F_1(\mathbf{x}) = x_2F_2(\mathbf{x})$, so that X contains the plane $x_1 = x_2 = 0$, we automatically have $N_X(B) \gg B^{n-2}$. Clearly this can only happen when X is a singular variety. Whenever X is smooth and has degree $d \geqslant 3$, a conjecture of Batyrev and Manin [**BM90**] leads us to expect that the following bound should hold.

Conjecture 2. *Suppose that $X \subset \mathbb{P}^{n-1}$ is a smooth hypersurface of degree $d \geqslant 3$. Then there exists $\delta > 0$ such that*

$$N_X(B) = O(B^{n-2-\delta}).$$

Returning to the setting of arbitrary irreducible hypersurfaces, we have seen above that the bound in Conjecture 1 holds when $d = 2$, possibly with an implied constant that is allowed to depend upon X. In fact Heath-Brown has already established Conjecture 1 in the case of quadrics [**HB02**, Theorem 2], in addition to the cases $n = 3$ and $n = 4$ of curves and surfaces, for any degree [**HB02**, Theorems 3 and 9].

Thus Conjecture 1 only remains uncertain for hypersurfaces of degree and dimension at least 3. We now present a table which charts the progress made towards Conjectures 1 and 2 in recent years. For convenience we have focused only upon the case $n = 5$ of threefolds, although several of the cited results have higher dimensional analogues. The table presents values of $\theta_d \in \mathbb{R}$ for which an upper bound of the form

$$N_X(B) = O(B^{\theta_d+\varepsilon}),$$

holds for irreducible threefolds $X \subset \mathbb{P}^4$ of degree $d \geqslant 2$. As they appear in the literature, some of the estimates presented below are proved with an arbitrary dependence of the implied constant upon X. However, in each case a straightforward analysis of the proof reveals that the estimate is actually uniform in the appropriate class of threefolds of fixed degree.

θ_d	Restrictions?	Who?	How?
$3+\frac{1}{2}$	none	Serre [**Ser89**]	large sieve
$3+\frac{2}{5}$	X smooth	Fujiwara [**Fuj85**]	exponential sums
$3+\frac{1}{3}$	X smooth	Heath-Brown [**HB94**]	exponential sums
$3+\frac{1}{d}$	none	Pila [**Pil95**]	hyperplane sections
$3-\frac{1}{12}$	X smooth, $d \geqslant 4$	Browning [**Bro03**]	hyperplane sections
3	$d \geqslant 4$	Broberg & Salberger [**BS04**]	hyperplane sections

It is clear from the table that it only remains to treat the case of cubic threefolds. In the setting of smooth cubic threefolds Conjecture 2 can be replaced by the finer conjecture of Manin [**FMT89**], which predicts that the asymptotic formula

$$N_X(B) = c_X B^2\Big(1 + o(1)\Big)$$

should hold for some constant $c_X > 0$. However we are yet to establish even Conjecture 2 for smooth cubic threefolds, so the resolution of Manin's conjecture is still a distant prospect.

Nevertheless our first result fills a gap in the table described above, by establishing Conjecture 1 in the case $d = n - 2 = 3$ [**BHB**, Theorem 3].

Theorem 3. *Let $X \subset \mathbb{P}^4$ be an irreducible cubic threefold. Then we have*

$$N_X(B) = O(B^{3+\varepsilon}).$$

The main tool in the proof of Theorem 3 is a versatile result valid for irreducible hypersurfaces of any dimension, which shows that every point counted by $N_X(B)$ must lie on one of a small number of linear subspaces contained in X. The contribution from the points lying on linear spaces of dimension 0 (that is to say, from individual points) turns out to be satisfactory from the point of view of the Conjecture 1, while those lying on linear spaces of higher dimension cause most of the problem. Our second result [**BHB**, Theorem 2] illustrates this phenomenon.

Theorem 4. *Let $X \subset \mathbb{P}^{n-1}$ be an irreducible hypersurface of degree d. Then we have*

$$N_U(B) = O(B^{n-2+\varepsilon}),$$

where $U \subseteq X$ is the open subset formed by deleting the lines from X.

With little extra work, this result can be used to deduce the following consequence. This establishes Conjecture 1 for a wide class of hypersurfaces.

Corollary 5. *Let $X \subset \mathbb{P}^{n-1}$ be an irreducible hypersurface of degree d, which is not a union of lines. Then we have*

$$N_X(B) = O(B^{n-2+\varepsilon}).$$

It is now time to state the result that forms the backbone of Theorems 3 and 4. This is a special case of [**BHB**, Theorem 4].

Theorem 6. *Let $X \subset \mathbb{P}^{n-1}$ be an irreducible hypersurface of degree d. Then there exist linear spaces $M_1, \ldots, M_J \subseteq X$ defined over $\mathbb{Q}$, with $J = O(B^{n-2+\varepsilon})$, such that $0 \leqslant \dim M_j \leqslant n-2$ for $1 \leqslant j \leqslant J$ and*

$$\{x \in X \cap \mathbb{P}^{n-1}(\mathbb{Q}) : H(x) \leqslant B\} \subseteq \bigcup_{j=1}^{J} \{x \in M_j \cap \mathbb{P}^{n-1}(\mathbb{Q}) : H(x) \leqslant B\}.$$

We complete this note by briefly commenting upon how Theorem 6 can be used to deduce the previous results. Beginning with the deduction of Theorem 4 we simply note that if $x \in X$ lies on some linear space $M \subseteq X$ of dimension at least 1, then it trivially lies on some projective line contained in X. Thus it will not be counted by $N_U(B)$. Since a linear space of dimension zero is just a point, we clearly obtain

$$N_U(B) \ll \sum_{1 \leqslant j \leqslant J} 1 \ll B^{n-2+\varepsilon}.$$

The deduction of Theorem 3 is considerably harder, and the main problem arises from the fact that a singular cubic threefold can contain a large number of lines and planes. That the linear spaces contained in X are of central concern is already immediate from the statement of Theorem 6. Here we shall content ourselves with merely indicating how bad the situation can become.

Let $\mathbb{G}(1,4)$ denote the Grassmannian parameterising lines in $\mathbb{P}^4$, and let $F_1(X) = \{L \in \mathbb{G}(1,4) : L \subset X\}$ denote the corresponding Fano variety of lines contained in X. Then a simple incidence correspondence argument reveals that

$$\dim F_1(X) \leqslant 3.$$

Whenever X is smooth it is well-known that $F_1(X)$ is a reduced and irreducible variety of dimension two. In this case it is relatively easy to deduce Theorem 3 from Theorem 6. It is worth remarking that Corollary 5 is of no use to us in this situation, since any cubic threefold is a union of lines.

Whenever X is singular it is perfectly possibly for X to contain a three dimensional family of lines. In fact there is an old result of Segre [**Seg48**] which shows that this only happens when X is either a cone or a scroll of planes. In the latter case one can go slightly further and show that X must take the shape

$$x_1x_2x_3 + x_1^2x_4 + x_2^2x_5 = 0.$$

This is done by considering generic hyperplane sections of X [**BHB**, Lemma 14], and may be of interest in its own right. In any case it is easy to see that this variety contains the family of planes

$$\lambda x_1 - \mu x_2 = \lambda\mu x_3 + \mu^2 x_4 + \lambda^2 x_5 = 0, \qquad [\lambda, \mu] \in \mathbb{P}^1,$$

in addition to the isolated plane $x_1 = x_2 = 0$. In particular it certainly contains a three dimensional family of lines. One of the main problems to contend with in the proof of Theorem 3 is that each rational plane contributes $\gg B^3$ to $N_X(B)$.

References

[BHB] T. Browning & D. Heath-Brown – Counting rational points on hypersurfaces, submitted.

[BM90] V. V. Batyrev & Y. I. Manin – Sur le nombre des points rationnels de hauteur borné des variétés algébriques, *Math. Ann.* **286** (1990), no. 1-3, p. 27–43.

[Bro03] T. D. Browning – A note on the distribution of rational points on threefolds, *Q. J. Math.* **54** (2003), no. 1, p. 33–39.

[BS04] N. Broberg & P. Salberger – Counting rational points on threefolds, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, p. 105–120.

[FMT89] J. Franke, Y. I. Manin & Y. Tschinkel – Rational points of bounded height on Fano varieties, *Invent. Math.* **95** (1989), no. 2, p. 421–435.

[Fuj85] M. Fujiwara – Upper bounds for the number of lattice points on hypersurfaces, Number theory and combinatorics. Japan 1984 (Tokyo, Okayama and Kyoto, 1984), World Sci. Publishing, Singapore, 1985, p. 89–96.

[HB94] D. R. Heath-Brown – The density of rational points on nonsingular hypersurfaces, *Proc. Indian Acad. Sci. Math. Sci.* **104** (1994), no. 1, p. 13–29, K. G. Ramanathan memorial issue.

[HB02] ______, The density of rational points on curves and surfaces, *Ann. of Math. (2)* **155** (2002), no. 2, p. 553–595.

[LP66] L. J. Lander & T. R. Parkin – Counterexample to Euler's conjecture on sums of like powers, *Bull. Amer. Math. Soc.* **72** (1966), p. 1079.

[Pil95] J. Pila – Density of integral and rational points on varieties, *Astérisque* (1995), no. 228, p. 4, 183–187, Columbia University Number Theory Seminar (New York, 1992).

[Seg48] B. Segre – Sulle v_n contenenti più di $\infty^{n-k}s_k$, i, ii, *Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Nat.* (1948), no. 5, p. 193–197, 275–180.

[Ser89] J.-P. Serre – *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, E15, Friedr. Vieweg & Sohn, Braunschweig, 1989.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 37–43
Universität Göttingen, 2004

DERIVED EQUIVALENCES IN REPRESENTATION THEORY OF FINITE GROUPS

S. Koshitani
Department of Mathematics, Faculty of Science, Chiba University, Chiba, 263-8522, Japan • *E-mail :* koshitan@math.s.chiba-u.ac.jp

Abstract. We survey recent results and conjectures in modular representation theory of finite groups.

1. Introduction

In modular representation theory of finite groups, we have had almost a unique pioneer, namely, Richard Brauer (1901–77). Early sixties of the last century he actually gave a nice survey talk [**Bra63**]. Now, in the subject we have many important and well-known problems, but many people would agree that the following might be the most important three conjectures of them. That is

1.1. Conjecture. Alperin's weight conjecture (1986) [**Alp87**].

1.2. Conjecture. Dade's conjecture (1990) [**Dad92**], [**Dad94**].

April 28th, 2004.

1.3. Conjecture. Broué's abelian defect group conjecture (1988) [**Bro90**], [**Bro94**], [**KZ98**].

However, these three conjectures essentially have an origin which was due to R. Brauer in [**Bra63**]. In the talk we shall concentrate on the third conjecture, namely, Broué's abelian defect group conjecture.

1.4. Morita equivalence. Let A and B be arbitrary (non-commutative) rings. Then, from the representation theoretical point of view, it seems reasonable that we consider A and B are the *same* if A and B have the same representations, that is to say, the categories Mod-A and Mod-B are equivalent, where Mod-A is the category of all right A-modules. We usually say that A and B are Morita equivalent if the condition holds, because there is a nice characterization of such an equivalence which is due to Kiiti Morita (1915–95) [**AF74**], §22. The easiest non-trivial example of Morita equivalences is the following. Take any (non-commutative) ring A and any positive integer n, and let $B := \mathrm{Mat}_n(A)$ be the full matrix ring over A of degree n. Then, A and B are Morita equivalent.

1.5. Notation/Definition. Throughout this note, let G be a finite group, let p be a prime and let kG be the group algebra of G over a field k. We use the notation Mod-A and $\mathrm{Mat}_n(A)$ as in 1.4. By mod-A for a ring A we denote the category of all finitely generated right A-modules, and by $D^b(\text{mod-}A)$ we denote the bounded derived category of mod-A. Moreover, for a positive integer n we write C_n and Σ_n for the cyclic group of order n and the symmetric group on n letters, respectively. Finally, $|G|$ means the order of G.

2. Representations of G over $\mathbb{C}$

As is well-known, in principle, finite-dimensional representations of G over $\mathbb{C}$ are completely understandable by the following theorem due to Wedderburn.

2.1. Theorem. (J. H. M. Wedderburn, 1907) There is an isomorphism

$$\mathbb{C}G \cong \mathrm{Mat}_{d_1}(\mathbb{C}) \times \cdots \times \mathrm{Mat}_{d_m}(\mathbb{C}) = \begin{pmatrix} \mathrm{Mat}_{d_1}(\mathbb{C}) & & 0 \\ & \ddots & \\ 0 & & \mathrm{Mat}_{d_m}(\mathbb{C}) \end{pmatrix}$$

of $\mathbb{C}$-algebras for positive integers $m, d_1, \cdots, d_m$. In particular, it holds that

(1) $|G| = \dim_{\mathbb{C}}(\mathbb{C}G) = \sum_{i=1}^{m} {d_i}^2$ and

(2) G is abelian if and only if $\mathbb{C}G$ is a commutative ring if and only if $d_1 = \cdots = d_m = 1$.

2.2. Examples.
(1) If G is abelian, then

$$\mathbb{C}G \ \cong \xrightarrow{|G|} \mathbb{C} \times \cdots \times \mathbb{C} \ = \begin{pmatrix} \mathbb{C} & & 0 \\ & \ddots & \\ 0 & & \mathbb{C} \end{pmatrix}.$$

(2) $\mathbb{C}\Sigma_3 \cong \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_2(\mathbb{C}) = \begin{pmatrix} \mathbb{C} & 0 & 0 \\ 0 & \mathbb{C} & 0 \\ 0 & 0 & \mathrm{Mat}_2(\mathbb{C}) \end{pmatrix}.$

3. Representations of G over a field k with prime characteristic p

3.1. Notation. In the rest of this note, let k be an algebraically closed field of characteristic $p > 0$. Then, we have representations of G over k and modules over kG as in Section 1. However, we do not have the Wedderburn's theorem 2.1 any more. Nevertheless, instead we do have the following theorem which is due to Maschke.

3.2. Theorem. (H. Maschke, 1898) The following assertions (1) and (2) are equivalent.

(1) There is an isomorphism

$$kG \cong \mathrm{Mat}_{d_1}(k) \times \cdots \times \mathrm{Mat}_{d_m}(k) = \begin{pmatrix} \mathrm{Mat}_{d_1}(k) & & 0 \\ & \ddots & \\ 0 & & \mathrm{Mat}_{d_m}(k) \end{pmatrix}$$

of k-algebras for positive integers $m, d_1, \cdots, d_m$.

(2) $p \nmid |G|$, namely, a Sylow p-subgroup P of G is trivial.

3.3. Slogan. A Sylow p-subgroup P of G determines (controls) most of all representations of G over k by looking at Theorem 3.2.

3.4. Definition. We can decompose kG into a direct product of indecomposable k-algebras (two-sided ideals of kG). Namely, we can write

$$_{kG}kG_{kG} = A_1 \times \cdots \times A_m$$

for a positive integer m where each A_i is an indecomposable two-sided ideal of kG. Each A_i is called a *block* (or a *block algebra*) of kG. In particular, let A_1 be a block of kG such that A_1 has a right ideal which is isomorphic to the trivial kG-module k_G, that is, the module k_G is given by the trivial representation $T: G \to \mathrm{GL}_1(k) = k^\times,\ g \mapsto 1$. Such A_1 is called the *principal block* or *principal block algebra* of kG.

Let R and S be two rings. As we have already looked at in 1.4, we say that R and S are *Morita equivalent* if the categories mod-A and mod-B are equivalent (this is because of the characterization by K. Morita [**AF74**], §22. On the other hand, let R and S be a finite dimensional k-algebras. Then, we say that R and S are derived (Rickard) equivalent if $D^b(\text{mod-}R)$ and $D^b(\text{mod-}S)$ are equivalent as triangulated categories. The reason why this is called a *Rickard equivalence* is that there is a wonderful characterization of the equivalence by Jeremy Rickard, which is completely a generalization of Morita equivalences [**Ric91**].

3.5. Remarks. Consider three statements (1)–(3).

(1) A and B are isomorphic as k-algebras.
(2) A and B are Morita equivalent.
(3) A and B are derived (Rickard) equivalent.

Then, we have (1) $\Rightarrow$ (2) $\Rightarrow$ (3).

3.6. Examples.
(1) $kC_p \cong k[X]/(X^p)$ as k-algebras, where $k[X]$ is the polynomial algebra over k with one variable.
(2) Let $p = 2$. Then, $k\Sigma_3 = A_1 \times A_2 \cong k[X]/(X^2) \times \mathrm{Mat}_2(k)$, as k-algebras.

3.7. Set up. Let p, k and G be as before, let P be a Sylow p-subgroup of G, and let $H = N_G(P)$. Then, as in 3.4 we have decompositions

$$_{kG}kG_{kG} = A_1 \times \cdots \times A_m \quad \text{and} \quad {}_{kH}kH_{kH} = B_1 \times \cdots \times B_n$$

of kG and kH, respectively, for positive integers m and n, where A_i and B_j are blocks of kG and kH, respectively for each i and j. Let $A = A_1$ and $B = B_1$ be the principal blocks of kG and kH, respectively. In the rest of this note we shall keep the notation here.

3.8. Remark. It is known that $B \cong k[P \rtimes E]$ as k-algebras, where E is a p'-group and $P \rtimes E$ is a semi-direct product of P by E (here $P \lhd P \rtimes E$).

3.9. Question/Conjecture. (R. Brauer) In the situation in 3.7, are A and B *similar*? If so, how do they resemble each other? More precisely speaking, are they derived (Rickard) equivalent or even Morita equivalent?

3.10. Examples.
(1) If G is p-solvable and P is abelian, the $A \cong B$ as k-algebras.
(2) Let $p = 2$, and let $G = \mathscr{A}_5$, the alternating group on 5 letters. Then, $P \cong C_2 \times C_2$ and $H \cong \mathscr{A}_4$, where $\mathscr{A}_4$ is the alternating group on 4 letters. Then, the two principal blocks A and B of kG and kH respectively are *not* Morita equivalent but derived (Rickard) equivalent.

4. Broué's abelian defect group conjecture

4.1. Broué's abelian defect group conjecture (ADGC). If P is abelian, then A and B should be derived (Rickard) equivalent, namely, $D^b(\text{mod-}A)$ and $D^b(\text{mod-}B)$ should be equivalent as triangulated categories.

4.2. Theorem. (J. Rickard [**Ric89b**], [**Ric91**]) Assume that A and B are derived (Rickard) equivalent. Then, the following holds:

(1) A and B have the same number of simple modules.
(2) $Z(A) \cong Z(B)$ as k-algebras, where $Z(A)$ is the center of A, and hence A and B have the same number of ordinary irreducible characters.
(3) There is a matrix $X \in GL_\ell(\mathbb{Z})$ such that $C_B = XC_A{}^tX$, where ℓ is the number in (1), C_A is the Cartan matrix of A and ${}^tX$ is the transposed matrix of X.

4.3. Results for Broué's ADGC 4.1. Broué's abelian defect group conjecture 4.1 holds if

(1) P is cyclic by Rickard [**Ric89a**] (note that he proves it not only for the principal blocks but also any block of kG),
(2) G is the symmetric group Σ_n by Chuang and Rouquier [**CR04**] (note that they prove it not only for the principal blocks but also any block of kG),
(3) G is p-solvable by Dade,
(4) $p = 2$ by Erdmann [**Erd90**], Rickard [**Ric96**], Rouquier [**Rou95**], Okuyama [**Oku98**], [**Oku00b**], [**Oku00a**], and Gollan and Okuyama [**GO97**],
((5) $p = 3$ and $P = C_3 \times C_3$ (elementary abelian group of order 9), by Koshitani and Kunugi [**KKW02**]. Note that they prove it based on initiated results of Puig [**Pui90**], Okuyama [**Oku98**], Okuyama and Waki [**OW98**], Koshitani and Kunugi [**KK01**], Kunugi [**Kun00**], Koshitani and Miyachi [**KM00**]; and also the classification of finite simple groups.

4.4. Remark. For the results on Broué's ADGC 4.1, visit the following Web Page done by J. Rickard:

`http://www.maths.bris.ac.uk/~majcr/adgc/adgc.html`

References

[AF74] F. W. Anderson & K. R. Fuller – *Rings and categories of modules*, Springer-Verlag, New York, 1974, Graduate Texts in Mathematics, Vol. 13.

[Alp87] J. L. Alperin – Weights for finite groups, The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), Proc. Sympos. Pure Math., vol. 47, Amer. Math. Soc., Providence, RI, 1987, p. 369–379.

[Bra63] R. Brauer – Representations of finite groups, Lectures on Modern Mathematics, Vol. I, Wiley, New York, 1963, p. 133–175.

[Bro90] M. Broué – Isométries parfaites, types de blocs, catégories dérivées, *Astérisque* (1990), no. 181-182, p. 61–92.

[Bro94] ______, Equivalences of blocks of group algebras, Finite-dimensional algebras and related topics (Ottawa, ON, 1992), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 424, Kluwer Acad. Publ., Dordrecht, 1994, p. 1–26.

[CR04] J. Chuang & R. Rouquier – 2004, preprint.

[Dad92] E. C. Dade – Counting characters in blocks. I, *Invent. Math.* **109** (1992), no. 1, p. 187–210.

[Dad94] ______, Counting characters in blocks. II, *J. Reine Angew. Math.* **448** (1994), p. 97–190.

[Erd90] K. Erdmann – *Blocks of tame representation type and related algebras*, Lecture Notes in Mathematics, vol. 1428, Springer-Verlag, Berlin, 1990.

[GO97] H. W. Gollan & T. Okuyama – Derived equivalences for the smallest janko group, 1997, preprint.

[KK01] S. Koshitani & N. Kunugi – The principal 3-blocks of the 3-dimensional projective special unitary groups in non-defining characteristic, *J. Reine Angew. Math.* **539** (2001), p. 1–27.

[KKW02] S. Koshitani, N. Kunugi & K. Waki – Broué's conjecture for non-principal 3-blocks of finite groups, *J. Pure Appl. Algebra* **173** (2002), no. 2, p. 177–211.

[KM00] S. Koshitani & H. Miyachi – The principal 3-blocks of four- and five-dimensional projective special linear groups in non-defining characteristic, *J. Algebra* **226** (2000), no. 2, p. 788–806.

[Kun00] N. Kunugi – Morita equivalent 3-blocks of the 3-dimensional projective special linear groups, *Proc. London Math. Soc. (3)* **80** (2000), no. 3, p. 575–589.

[KZ98] S. König & A. Zimmermann – *Derived equivalences for group rings*, Lecture Notes in Mathematics, vol. 1685, Springer-Verlag, Berlin, 1998, With contributions by Bernhard Keller, Markus Linckelmann, Jeremy Rickard and Raphaël Rouquier.

[Oku98] T. Okuyama – Some examples of derived equivalent blocks of finite groups, 1998, preprint, 19 pages.

[Oku00a] ———, Derived equivalences in sl(2,q), 2000, preprint.

[Oku00b] ———, Remarks on splendid tilting complexes, Proceedings of Representations of Finite and Algebraic Groups (N. Kawanaka, G. Michler & K. Uno, eds.), Osaka Univ., 2000, p. 171–179.

[OW98] T. Okuyama & K. Waki – Decomposition numbers of $\mathrm{Sp}(4, q)$, *J. Algebra* **199** (1998), no. 2, p. 544–555.

[Pui90] L. Puig – Algèbres de source de certains blocs des groupes de Chevalley, *Astérisque* (1990), no. 181-182, p. 9, 221–236.

[Ric89a] J. Rickard – Derived categories and stable equivalence, *J. Pure Appl. Algebra* **61** (1989), no. 3, p. 303–317.

[Ric89b] ———, Morita theory for derived categories, *J. London Math. Soc. (2)* **39** (1989), no. 3, p. 436–456.

[Ric91] ———, Derived equivalences as derived functors, *J. London Math. Soc. (2)* **43** (1991), no. 1, p. 37–48.

[Ric96] ———, Splendid equivalences: derived categories and permutation modules, *Proc. London Math. Soc. (3)* **72** (1996), no. 2, p. 331–358.

[Rou95] R. Rouquier – From stable equivalences to Rickard equivalences for blocks with cyclic defect, Groups '93 Galway/St. Andrews, Vol. 2, London Math. Soc. Lecture Note Ser., vol. 212, Cambridge Univ. Press, Cambridge, 1995, p. 512–523.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 45–52
Universität Göttingen, 2004

l-ADIC GALOIS COHOMOLOGY AND THE SUSLIN–VOEVODSKY THEOREM

Ph. Gille

UMR 8628 du C.N.R.S., Mathématiques, Bâtiment 425, Université de Paris-Sud, F-91405 Orsay, France • *E-mail :* gille@math.u-psud.fr

Abstract. We present the Suslin-Voevodsky theorem within the framework of continuous étale cohomology.

1. Introduction

Let k be a field and let k_s be a separable closure of k. We denote by Γ_k the absolute Galois group of k. Rost and Voevodsky [**Ros02**], [**Voe**] established the following result

Bloch-Kato's conjecture [**Kat80**]. *For any $q \geqslant 0$, $m \geqslant 1$, and m invertible in k, the Galois symbol*

$$h^q_{m,k} : K^M_q(k)/mK^M_q(k) \to H^q(k, \mu_m^{\otimes q})$$

is an isomorphism.

April 29th, 2004.

Let us begin by recalling the objects involved in this result. $K_q^M(k)$ is the group of the Milnor K–theory of k in degree q, i.e., the quotient of $(k^\times)^{\otimes q} = k^\times \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} k^\times$ by the subgroup generated by the $a_1 \otimes a_2 \otimes \cdots \otimes a_q$ for which there exists i with $a_i + a_{i+1} = 1$. We denote by $\{a_1, ..., a_q\}$ the class (or symbol) in $K_q^M(k)$ of $a_1 \otimes \cdots \otimes a_q$. The group $H^q(k, \mu_m^{\otimes q})$ is the Galois cohomology in degree q of the profinite group Γ_k with coefficients in $\mu_m^{\otimes q} = \mu_m(k_s) \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mu_m(k_s)$ (q times).

Kummer theory yields an isomorphism $k^\times/(k^\times)^m \xrightarrow{\sim} H^1(k, \mu_m)$, $a \mapsto (a)$, and the Galois symbol is then defined as the cup-product

$$h^q_{m,k}\big(\{a_1, ..., a_q\}\big) = (a_1) \cup \cdots \cup (a_q) \in H^q(k, \mu_l^{\otimes q}).$$

Let l be a fixed prime invertible in k. We denote by $\mathbb{Q}_l/\mathbb{Z}_l(q)$ the Galois module $= \varinjlim \mu_{l^n}^{\otimes q}$. We are interested in the following equivalent formulation of the Bloch–Kato's conjecture. (For $l = 2$, a different proof can be found in [**Mer96**].)

Theorem 1. ([**SV00**], Theorem 11.4) *The following are equivalent:*

i) *the group $H^q(F, \mathbb{Q}_l/\mathbb{Z}_l(q))$ is divisible for any field F/k,*
ii) *for any field F/k, the Galois symbol $h : K_q^M(F)/l \to H^q(F, \mu_l^{\otimes q})$ is an isomorphism,*
iii) *for any field extension F/k, the Galois symbol $h : K_q^M(F)/l \to H^q(F, \mu_l^{\otimes q})$ is surjective.*

In particular, the surjectivity of the Galois symbol implies its injectivity. The proof of this result is highly technical, making use of motivic theories and simplicial schemes. Our goal is to give a much simpler proof based on Galois cohomology. Following Tate ([**Tat76**], Section 2), the first assertion of the Theorem can be stated in terms of l–adic cohomology, i.e.,

i$'$) $\quad H^{q+1}(F, \mathbb{Z}_l(q))_{tors} = 0 \quad$ for any extension F/k.

On the other hand, the key step of the Merkurjev–Suslin theorem is:

Hilbert 90 **for** $\mathbf{K_2}$ [**MS82**] *Let L/k be a cyclic extension of degree l. Let σ be a generator of $\mathscr{G}al(L/k)$. Then the complex*

$$K_2^M(L) \xrightarrow{(1-\sigma)} K_2^M(L) \xrightarrow{N_{L/k}} K_2^M(k),$$

is exact. Here $N_{L/k}$ is the norm map for Milnor K-theory.

In view of the above, it seems natural to look for higher analogues of this Hilbert 90 statement that are equivalent to the Bloch-Kato's conjecture. This is exactly what we propose to do.

Notation.

• For all $i \geqslant 0$ and $m \geqslant 1$, we set

$$\mathbb{Z}/l^m\mathbb{Z}(i) = \mu_{l^m}^{\otimes i}, \quad \text{and} \quad \mathbb{Z}/l^m\mathbb{Z}(-i) = \mathrm{Hom}_{k_s-gr}(\mu_{l^m}^{\otimes i}, \mathbb{Z}/l^m\mathbb{Z}).$$

As before, $\mathbb{Q}_l/\mathbb{Z}_l(i) = \varinjlim \mu_{l^n}^{\otimes i}$,

• For an abelian group A and a positive integer n we let ${}_nA$ and A/n denote the kernel and cokernel respectively of the multiplication $A \xrightarrow{\times n} A$,

• A_{tors} is the maximal torsion subgroup of A and $A\{l\}$ the l–primary part A_{tors},

• $\mathscr{A}_b^{\mathbb{N}}$ is the abelian category of projective systems

$$\cdots \to A_n \to A_{n-1} \to \cdots \to A_1 \to A_0.$$

We denote by $\varprojlim\limits_n{}^1$ the first derived functor of the functor $\varprojlim\limits_n : \mathscr{A}_b^{\mathbb{N}} \to \mathscr{A}_b$ (higher derived functors are trivial).

2. Continuous Galois cohomology

Let G be a profinite group. If M is a $\mathbb{Z}_l$–module of finite type with a continuous action of G, with respect to the l-adic topology, we denote by $H^i(G, M)$ the l-adic cohomology groups of Tate [**Tat76**] defined with continuous cochains. The link with the classical theory is given by the Milnor's exact sequence (*loc. cit.*, Proposition 2.2)

$$0 \to \varprojlim_n{}^1 H^{q-1}(G, M/l^n) \to H^q(G, M) \to \varprojlim_n H^q(G, M/l^n) \to 0. \tag{1}$$

Since the groups $H^0(G, M/l^n)$ are finite and the system $\big(H^0(G, M/l^n)\big)$ satisfies the Mittag-Leffler's condition, we have

$$H^1(G, M) = \varprojlim_n H^1(G, M/l^n).$$

In particular,

$$\begin{aligned} H^1(G, \mathbb{Z}_l) &= \varprojlim_n H^1(G, \mathbb{Z}/l^n\mathbb{Z}) \\ &= \varprojlim_n \mathrm{Hom}_{gr}(G, \mathbb{Z}/l^n\mathbb{Z}) = \mathrm{Hom}_{gr,cont}(G, \mathbb{Z}_l), \end{aligned}$$

the last is the group of continuous homomorphisms from G to $\mathbb{Z}_l$. This theory carries cup-products, restriction maps $\mathrm{Res}^i : H^i(G,M) \to H^i(H,M)$ and corestriction maps $\mathrm{Cor}^i : H^i(H,M) \to H^i(G,M)$ for H open in G.

We assume that M is torsion free. The exact sequence

$$0 \to M \xrightarrow{\times l^m} M \to M/l^m \to 0$$

induces the exact sequence

$$(2) \qquad 0 \to H^q(G,M)/l^m \to H^q(G,M/l^m) \xrightarrow{\delta} {}_{l^m}H^{q+1}(G,M) \to 0.$$

Passing to the limit in m yields the exact sequence ([**Tat76**], Section 2)

$$(3) \qquad 0 \to H^q(G,M) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l/\mathbb{Z}_l \to H^q(G, M \otimes \mathbb{Q}_l/\mathbb{Z}_l) \xrightarrow{\delta} H^{q+1}(G,M)_{tors} \to 0.$$

Moreover, the group $H^q(G,M) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l/\mathbb{Z}_l$ is the maximal divisible subgroup of $H^q(G, M \otimes \mathbb{Q}_l/\mathbb{Z}_l)$.

Let H be an open normal subgroup of G such that the quotient $G/H = \Gamma$ is cyclic of order l. Fix a generator σ of Γ and set $N = 1 + \sigma + \cdots + \sigma^{n-1} \in \mathbb{Z}_l[\Gamma]$. We shall use the norm morphism $N : \mathbb{Z}_l \to \mathbb{Z}_l[\Gamma]$ mapping 1 to N and the augmentation map $\varepsilon : \mathbb{Z}_l[\Gamma] \to \mathbb{Z}_l$ defined by $\varepsilon(\sum_i a_i \sigma^i) = \sum_i a_i$. We have $\varepsilon \circ N = \times l$ and the exact sequence

$$0 \to \mathbb{Z}_l \xrightarrow{N} \mathbb{Z}_l[\Gamma] \xrightarrow{1-\sigma} \mathbb{Z}_l[\Gamma] \xrightarrow{\varepsilon} \mathbb{Z}_l \to 0.$$

We set $I = \mathrm{Ker}(\varepsilon)$, $J = \mathrm{Coker}(N)$ and consider the resulting isomorphism $(1-\sigma) : J \xrightarrow{\sim} I$. After tensoring the short exact sequences

$$0 \to I \to \mathbb{Z}_l[\Gamma] \to \mathbb{Z}_l \to 0$$

and

$$0 \to \mathbb{Z}_l \to \mathbb{Z}_l[\Gamma] \to J \to 0$$

with $\otimes_{\mathbb{Z}_l} M$, we may use Shapiro's lemma to obtain the commutative diagram

$$\begin{tikzcd}
H^q(G,M) \arrow[r, "\mathrm{Res}^q"] & H^q(H,M) \arrow[r] & H^q(G, M \otimes_{\mathbb{Z}_l} J) \arrow[r] \arrow[d, "(1-\sigma)"'] & H^{q+1}(G,M) \arrow[r, "\mathrm{Res}^{q+1}"] & H^{q+1}(H,M) \\
H^{q-1}(G,M) \arrow[r, "\mathrm{Cor}^{q-1}"] & H^{q-1}(G,M) \arrow[r, "\delta"] & H^q(G, M \otimes_{\mathbb{Z}_l} I) \arrow[r] & H^q(H,M) \arrow[r, "\mathrm{Cor}^q"] & H^q(G,M).
\end{tikzcd}$$

The map $H^q(H,M) \to H^q(H,M)$ is given by $1-\sigma$. A diagram chase yields the exact sequence

$$(4) \qquad H^q(G,M) \to H^q(H,M)^{1-\sigma} \to H^{q-1}(G,M)/\mathrm{Cor}^{q-1}\big(H^{q-1}(H,M)\big)$$
$$\xrightarrow{\varphi} \mathrm{Ker}(\mathrm{Res}^{q+1}) \to \mathrm{Ker}(\mathrm{Cor}^q)/(1-\sigma)H^q(H,M) \to 0.$$

We now focus on the case of $G = \Gamma_k$, with l-adic modules $\mathbb{Z}_l(i) := \varprojlim \mu_{l^n}^{\otimes i}$. We have

$$H^1(k, \mathbb{Z}_l(1)) = \varprojlim_n H^1(k, \mu_{l^n}) = \varprojlim_n k^\times / k^{\times l^n}.$$

In other words, the group $H^1(k, \mathbb{Z}_l(1))$ is the l–adic completion of $k^\times$. We then have a canonical map $h_1 : k^\times \to H^1(k, \mathbb{Z}_l(1))$. Tate defined the l-adic Galois symbol ([**Tat76**], Theorem 3.1) by

$$h_k^q : K_q^M(k) \to H^q(k, \mathbb{Z}_l(q)), \quad \{a_1, \cdots, a_q\} \mapsto h(a_1) \cup \cdots \cup h(a_q).$$

This symbol lifts the usual Galois symbol

$$h_{l^m,k}^q : K_q^M(k)/l^m \to H^q(k, \mu_{l^m}^{\otimes m}).$$

Note that we have the following commutative diagram of complexes

$$\begin{array}{ccccc} K_q^M(L) & \xrightarrow{(1-\sigma)} & K_q^M(L) & \xrightarrow{N_{L/k}} & K_q^M(k) \\ \downarrow{\scriptstyle h_L^q} & & \downarrow{\scriptstyle h_L^q} & & \downarrow{\scriptstyle h_k^q} \\ H^q(L, \mathbb{Z}_l(q)) & \xrightarrow{(1-\sigma)} & H^q(L, \mathbb{Z}_l(q)) & \xrightarrow{\mathrm{Cor}_k^L} & H^q(k, \mathbb{Z}_l(q)), \end{array}$$

and the link with the problem of Hilbert 90 for Milnor's K–theory thereof.

3. l-adic formulations of the Bloch-Kato conjecture

We consider the following two assertions:

"l-adic Hilbert 90 in degree q". *For any extension F/k and for any cyclic extension E/F of degree l with Galois group $\mathbb{Z}/l\mathbb{Z} = \langle \sigma \rangle$, the complex*

$$H^q(L, \mathbb{Z}_l(q)) \overset{(1-\sigma)}{\longrightarrow} H^q(L, \mathbb{Z}_l(q)) \overset{\mathrm{Cor}_k^L}{\longrightarrow} H^q(k, \mathbb{Z}_l(q))$$

is exact.

"l-adic Hilbert 90 for symbols in degree q". *Let F/k be a field extension and E/F a cyclic extension of degree l with Galois group $\mathbb{Z}/l\mathbb{Z} = \langle \sigma \rangle$. If*

$$\beta \in \mathrm{Im}\Big(K_q^M(E) \to H^q(E, \mathbb{Z}_l(q)) \Big),$$

is such that there exists $\beta_0 \in H^q(F, \mathbb{Z}_l(q))$ satisfying

$$\mathrm{Cor}_F^E(\beta) = l\beta_0,$$

then

$$\beta - \mathrm{Res}_F^E(\beta_0) \in (1 - \sigma) \cdot H^q(E, \mathbb{Z}_l(q)).$$

We can now state our main result.

Theorem 2. *The following are equivalent:*

i) *The group $H^q(F, \mathbb{Q}_l/\mathbb{Z}_l(q))$ is divisible for any field F/k,*
ii) *l-adic Hilbert 90 in degree q,*
iii) *l-adic Hilbert 90 for symbols in degree q,*
iv) *For any field extension F/k, the Galois symbol $h_{l,F} : K_q^M(F)/l \to H^q(F)$ is an isomorphism,*
v) *For any field extension F/k, the Galois symbol $h_{l,F} : K_q^M(F)/l \to H^q(F)$ is surjective.*

Let us sketch the proof which goes by induction on $q \geqslant 1$. A key point is to use the exact sequence (4) for a given cyclic extension L/k of prime degree l. We need then a character $\chi \in H^1(k, \mathbb{Z}/l\mathbb{Z})$ defining L/k and a generator $\sigma \in \mathscr{G}al(L/k)$. These yield the following exact sequence

$$(5) \qquad H^{q-1}(k, \mathbb{Z}_l(q)) \xrightarrow{\cup\delta(\chi)} \mathrm{Ker}\big[H^{q+1}(k, \mathbb{Z}_l(q)) \to H^{q+1}(L, \mathbb{Z}_l(q))\big] \xrightarrow{\rho}$$
$$\mathrm{Ker}\big[H^q(L, \mathbb{Z}_l(q)) \xrightarrow{\mathrm{Cor}_k^L} H^q(k, \mathbb{Z}_l(q))\big]/(1-\sigma)H^n(L, \mathbb{Z}_l(q)) \to 0.$$

i) $\Longrightarrow$ ii): We have $H^{q+1}(k, \mathbb{Z}_l(q))_{tors} = 0$ and in particular
$$\mathrm{Ker}\big(H^{q+1}(k, \mathbb{Z}_l(q)) \to H^{q+1}(L, \mathbb{Z}_l(q))\big) = 0.$$
The exact sequence (5) implies then that the complex

$$H^q(L, \mathbb{Z}_l(q)) \xrightarrow{(1-\sigma)} H^q(L, \mathbb{Z}_l(q)) \xrightarrow{\mathrm{Cor}_k^L} H^q(k, \mathbb{Z}_l(q))$$

is exact.

ii) $\Longrightarrow$ iii): obvious.

iii) $\Longrightarrow$ iv): This is the non-trivial part of the argument. By the Bass–Tate lemma, we may work only with an element $\beta = h\Big(\sum_i \{c_i, b_i\}\Big) \in H^q(L, \mathbb{Z}_l(q)))$ with $c_i \in L^\times$ and $b_i \in K_q^{M-1}(k)$. We may assume that k contains a primitive l-root of unity ζ. By hypothesis, we have
$$l\,\beta_0 = N_{L/k}(\beta) = h\Big(\sum_i \{N_{L/k}(c_i), b_i\}\Big).$$
At this point we observe for future reference that the problem of l-adic Hilbert 90 for symbols admits a "versal" case (analogous to that of the versal torsors.

See ([**GMS03**], Section 5.1). We may assume that $L = k(\sqrt[l]{s})$ for some $s \in k^\times$. This allows us then to think of the extension L/k as the specialization at $t = s$ of the extension $k(t')/k(t)$ where $(t')^l = t$. For each c_i as above, we consider the Severi–Brauer variety of the cyclic $k(t)$-algebras of degree l

$$A_\zeta\big(N_{L/k}(c_i), t\big),$$

of presentation $X^l = N_{L/k}(c_i)$, $Y^l = t$, and $XY = \zeta YX$. Let $F/k(t)$ be the compositum of the function fields of these varieties [(1)]. There exists some functions $g_i \in F' = F.k(t')$ with $t' = \sqrt[l]{t}$ satisfying $N_{L/k}(c_i) = N_{F'/F}(g_i)$. We may check that $h_L\Big(\sum_i \{c_i, b_i\}\Big) - \mathrm{Res}_k^L(\beta_0)$ is essentially a specialization at $t = s$ of the "versal" element

$$h_{F'}\Big(\sum_i \{g_i, b_i\}\Big) - \mathrm{Res}_k^{F'}(\beta_0) \in \mathrm{Ker}\Big(H^q(F', \mathbb{Z}_l(q)) \overset{\mathrm{Cor}_F^{F'}}{\longrightarrow} H^q(F, \mathbb{Z}_l(q))\Big).$$

The proof is now finished by a short argument using Jannsen's theory of étale cohomology [**Jan88**] (see [**Gil**] for details).

iv) $\Longrightarrow$ v): obvious.

v) $\Longrightarrow$ i): Since the Galois symbol $K_q^M(k)/l \to H^q(k, \mu_l^{\otimes q})$ is surjective, so is the map $H_q(k, \mathbb{Z}_l(q)))/l \to H^q(k, \mu_l^{\otimes q})$. It follows from the exact sequence (2.1.2) that ${}_lH^{q+1}(k, \mathbb{Z}_l(q)) = 0$. Thus $H^{q+1}(k, \mathbb{Z}_l(q))_{tors} = 0$ and we conclude that $H^q(k, \mathbb{Q}_l/\mathbb{Z}_l(q))$ is divisible.

Acknowledgment. I would like to thank Arturo Pianzola for his help in improving the exposition of this short note.

References

[Gil] P. Gille – Symbole galoisien l-adique et conjecture de Bloch–Kato, preprint (2003), `www.mathematik.uni-bielefeld.de/LAG/`.

[GMS03] S. Garibaldi, A. Merkurjev & J.-P. Serre – *Cohomological invariants in Galois cohomology*, University Lecture Series, vol. 28, American Mathematical Society, Providence, RI, 2003.

[Jan88] U. Jannsen – Continuous étale cohomology, *Math. Ann.* **280** (1988), no. 2, p. 207–245.

(1) If $l = 2$, this is the projective conic of equation $x^2 - a_i y^2 = tz^2$ in $\mathbf{P}^2_{k(t)}$ where $a_i = N_{L/k}(c_i)$.

[Kat80] K. KATO – A generalization of local class field theory by using K-groups. II, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **27** (1980), no. 3, p. 603–683.

[Mer96] A. S. MERKUR′EV – On the norm residue homomorphism for fields, Mathematics in St. Petersburg, Amer. Math. Soc. Transl. Ser. 2, vol. 174, Amer. Math. Soc., Providence, RI, 1996, p. 49–71.

[MS82] A. S. MERKUR′EV & A. A. SUSLIN – K-cohomology of Severi-Brauer varieties and the norm residue homomorphism, *Izv. Akad. Nauk SSSR Ser. Mat.* **46** (1982), no. 5, p. 1011–1046, 1135–1136.

[Ros02] M. ROST – Norm varieties and algebraic cobordism, *Proceedings of the International Congress of Mathematicians, Vol. I (Beijing, 2002)* (Beijing), Higher Ed. Press, 2002, p. 649.

[SV00] A. SUSLIN & V. VOEVODSKY – Bloch-Kato conjecture and motivic cohomology with finite coefficients, The arithmetic and geometry of algebraic cycles (Banff, AB, 1998), NATO Sci. Ser. C Math. Phys. Sci., vol. 548, Kluwer Acad. Publ., Dordrecht, 2000, p. 117–189.

[Tat76] J. TATE – Relations between K_2 and Galois cohomology, *Invent. Math.* **36** (1976), p. 257–274.

[Voe] V. VOEVODSKY – On motivic cohomology with Z/lZ coefficients, preprint (2003), `www.math.uiuc.edu/K-theory/`.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 53–60
Universität Göttingen, 2004

SUPERSINGULAR ELLIPTIC CURVES AND MAXIMAL QUATERNIONIC ORDERS

J.M. Cerviño

Mathematisches Institut der Georg-August Universität Göttingen, Bunsenstr. 3-5, 37073 Göttingen, Germany • *E-mail :* cervino@uni-math.gwdg.de

Abstract. We give an explicit version of the "Deuring correspondence" between supersingular elliptic curves and maximal quaternionic orders, by presenting a deterministic and explicit algorithm to compute it.

1. Introduction

In this note all fields of positive characteristic will be either finite or function fields of curves defined over a finite algebraic extension of $\mathbb{F}_p$. Elliptic curve means often isomorphy class of elliptic curves. All quadratic forms have integral coefficients. For details see [**Cn**].

Let k be a finite field of characteristic p with fixed algebraic closure $\bar{k}$. Let E be an elliptic curve over k and $k(E)$ its function field. Such a curve is called *supersingular* if one, and hence all, of the following equivalences are satisfied:

1. $E(\overline{k})$ has no p torsion;
2. $\mathrm{End}_{\overline{k}}(E)$ is a 4-dimensional $\mathbb{Z}$-lattice;

May 4th, 2004.

3. $k(E)$ has no cyclic (separable and unramified) p-extensions.

Around the 30's Helmut Hasse proved the Riemann hypothesis for zeta functions of elliptic curves. He was also the first to observe, that besides the two well known cases of endomorphism rings of elliptic curves - namely $\mathbb{Z}$ or an order in an imaginary quadratic field extension of $\mathbb{Q}$, the so called *complex multiplication* case -, it was also possible to have an order of a definite quaternion algebra when the base field had positive characteristic. Max Deuring was able to compute the discriminant of this definite algebra. In [**Deu41b**] he proved that the algebra ramifies at p and at ∞. Furthermore in [**Deu41a**] he proved that the endomorphism rings of elliptic curves over a finite field of characteristic p are maximal orders in the quaternion algebra $\mathbb{Q}_{\infty,p}$ (the subindex shows the ramification places of the algebra), and that all maximal orders types of that algebra appear as endomorphism rings of supersingular elliptic curves over $\overline{\mathbb{F}_p}$.

In this note, we recall this correspondence, describe an explicit and deterministic algorithm to compute it and illustrate this algorithm in a concrete example.

2. Deuring correspondence

In the introduction we said that Deuring proved that every maximal order type (isomorphy class) of the quaternion algebra $\mathbb{Q}_{\infty,p}$ appears as an endomorphism ring of a supersingular elliptic curve over $\overline{\mathbb{F}_p}$. But a bijection does not hold in this picture. In order to explain a bijection, we use the property (3) of supersingular elliptic curves.

In [**HW36**] Hasse and Witt study under which conditions a function field of characteristic p possesses cyclic unramified p-extensions. For the case of elliptic function fields they give an invariant A depending on the j invariant of the elliptic function field, such that $A = 0$ if and only if the elliptic function field has no cyclic unramified p-extensions, and therefore by (3), if and only if the elliptic curve is supersingular. This A invariant, called the *Hasse-Witt invariant* of the function field, is actually a polynomial in j, which was first computed in [**Deu41a**, page 201]. With this easily computable polynomial we can find the explicit equations for all the supersingular elliptic curves over $\overline{\mathbb{F}_p}$. Moreover, this Hasse-Witt polynomial factors over $\mathbb{F}_p[j]$ with factors of degree at most 2. Now we state the *Deuring correspondence*:

Theorem 2.1. [**Deu41a**] *Let p be a prime, and let $A(T) \in \mathbb{F}_p[T]$ be the characteristic p Hasse-Witt polynomial. For any $j_0 \in \overline{\mathbb{F}_p}$ denote by $E(j_0)$ any*

elliptic curve in the isomorphy class of those with j-invariant j_0. Then $A(T)$ factors as a product of at most degree 2 polynomials (in $\mathbb{F}_p[T]$) and to these factors correspond bijectively the maximal order types of the quaternion algebra $\mathbb{Q}_{\infty,p}$. The bijection is as follows:
for any irreducible factor A_i of A, choose a root, say $j_0 \in \mathbb{F}_{p^2}$; then:

$$A_i \;\mapsto\; \mathrm{End}_{\overline{\mathbb{F}_p}}(E(j_i)).$$

So, to make this correspondence explicit means to be able to compute the endomorphism ring of any supersingular elliptic curve (up to isomorphy), that means to compute the order type of the endomorphism ring. Let us take a look at the problem in two particular cases.

Example 2.2. *Consider two illustrative cases, $p = 29$ and $p = 37$.*

Case $p = 29$:

Here the Hasse-Witt polynomial is $A_{29}(T) = T(T-2)(T+4)$, and there are only three supersingular elliptic curves over $\overline{\mathbb{F}_{29}}$, namely $E(0)$, $E(2)$ and $E(25)$. In the quaternion algebra over $\mathbb{Q}$ ramified only at ∞ and 29 there are three isomorphy classes of maximal orders. Their $\mathbb{Z}$-bases can be computed explicitly as in **[Piz80]** *(see also the implementations made by F. Rodriguez-Villegas,* `http://www.ma.utexas.edu/users/villegas/cnt/`*). Instead we are going to avoid the computation of such bases until the very end of the algorithm, and we label those maximal order types by $\mathscr{O}_1$, $\mathscr{O}_2$, $\mathscr{O}_3$.*

Case $p = 37$:

Here $A_{37}(T) = (T-8)(T^2-6T-6)$. This is the first prime where the Hasse-Witt polynomial has a nonlinear factor. The supersingular elliptic curves here are $E(8)$, $E(3+10\sqrt{2})$ and $E(3-10\sqrt{2})$. As explained in (2.1), the last two curves have the same endomorphism ring type, hence there are only two maximal order types in $\mathbb{Q}_{\infty,37}$, say $\mathscr{O}_1$ and $\mathscr{O}_2$.

The problem is to determine which supersingular elliptic curve corresponds to which order type. This will be solved at the end of this paper.

Note that David Kohel in his Berkeley thesis **[Koh96]** (using a different approach) proved a theorem which says that for any given supersingular elliptic curve E *there exists* an algorithm to compute four linearly independent endomorphisms of E, with running time $O(p^{3/2})$ (Theorem 75, loc.cit.). In

the proof he computes the discriminant of the suborder generated by the independent endomorphisms found in his theorem, but cannot control it, and then cannot assure that the result is a $\mathbb{Z}$-basis of the endomorphism ring[(1)].
We propose an algorithm that, for a given prime p, returns a list of pairs $(E_\lambda, \{1, e_1^\lambda, e_2^\lambda, e_3^\lambda\})$, where E_λ runs over all supersingular elliptic curves over $\overline{\mathbb{F}_p}$ and the second coordinate is a $\mathbb{Z}$-basis of the endomorphism ring of E_λ. Since we reduce this problem to a problem of computing on one side representation numbers and on the other graphs of isogenies, by [**Piz80**] (for computing the representation numbers) and [**Mes86**] (for the isogenies graph complexity) we have that the theoretical complexity of our algorithm is $O(p^{5/2})$, much better than the complexity of the already implemented version in PARI, which is more or less $O(p^4)$. Observe that this algorithm gives *all* the bases of endomorphism rings of supersingular elliptic curves over $\overline{\mathbb{F}_p}$ and Kohel's more flexible theoretical algorithm works for one curve at a time, at the expense of loosing certainty, on whether one obtains a base of the maximal order or a base of a finite index sub-order.

2.1. Brandt-Sohn correspondence. We want to explain briefly a connection between maximal order types of the quaternion algebras $\mathbb{Q}_{\infty,p}$ and ternary quadratic forms of discriminant $-p$. In [**Bra43**] Brandt constructs maximal orders of quaternion algebras from ternary lattices *via* Clifford algebras. His idea was then exploited by Friedhelm Sohn in his Dissertation [**Soh57**], where he proves the following:

Theorem 2.3. *There exists an explicit bijection between the classes of ternary quadratic forms of discriminant $-p$ and the maximal order types of the quaternion algebra $\mathbb{Q}_{\infty,p}$.*

Indeed, given any ternary quadratic form

$$f = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{23}x_2x_3$$

with $a_{ij} \in \mathbb{Z}$ we associate the $\mathbb{Z}$-order with basis $1, e_1, e_2, e_3$ where:

$$\begin{aligned} e_i^2 &= a_{jk}e_i - a_{jj}a_{kk}, \\ e_ie_j &= a_{kk}(a_{ij} - e_k), \\ e_je_i &= a_{1k}e_1 + a_{2k}e_2 + a_{3k}e_3 - a_{ik}a_{jk}, \end{aligned} \tag{1}$$

with (i, j, k) any even permutation of $\{1, 2, 3\}$ (see [**Brz95**]). Therefore once we know a complete set of representatives of the equivalence classes of ternary

[(1)]See Theorem 84 loc.cit. for conditions when the algorithm gives a base of the endomorphism ring and comment thereafter.

quadratic forms of discriminant $-p$, we can directly compute the $\mathbb{Z}$-bases of all maximal order types of $\mathbb{Q}_{\infty,p}$. Now, since all the quadratic forms of discriminant $-p$ belong to the same genus, we can use an algorithm of Rainer Schulze-Pillot [**SP91**] based on the ℓ-*neighbors* concept introduced by Martin Kneser to compute a representative for each equivalence class, therefore given any prime number p we can compute the bases of representatives for all the maximal order types of $\mathbb{Q}_{\infty,p}$.

3. The algorithm

We now state a key theorem assuring that the algorithm works.

Theorem 3.1. [**Sch97**] *The theta series determine the equivalence classes of definite ternary quadratic forms over $\mathbb{Q}$. This means that any two definite ternary quadratic forms over $\mathbb{Q}$ are integrally equivalent if and only if they have the same representation numbers.*

Recall, that the representation numbers of a definite quadratic form f of dimension d are the:

$$r(f,n) := \#\{x \in \mathbb{Z}^d \mid f(x) = n\};\ n \in \mathbb{Z};$$

and then the theta series for f is:

$$\vartheta(z) := \sum_{n\in\mathbb{Z}} exp(2\pi i r(f,n)z);\ z \in \mathbb{H}.$$

It is a classical result that these theta series are in fact modular forms of weight $d/2$ and level the level of the quadratic form; see [**SP84**] in particular for the case $d = 3$. Since there is only one genus for discriminant $-p$, all the theta series corresponding to quadratic forms of discriminant $-p$ have the same Eisenstein part, and therefore they differ, if at all, in the cuspidal part. C.L. Siegel in his papers on the analytic theory of quadratic forms gives an explicit bound to decide whether a cusp form is zero or not. This bound grows like $p/12$.

Moreover Schiemann gives also a bound $b(p)$, which in our case depends only on the discriminant, such that for any two definite quadratic forms f, g of discriminant $-p$ holds:

$$r(f,n) = r(g,n)\ \forall\, n \in \mathbb{Z} \text{ with } |n| \leqslant b(p) \Rightarrow f \text{ and } g \text{ are integrally equivalent.}$$

For computational purposes Siegel's bound is better for us and we use it in the implementation; but asymptotically they are the same.

Now let us go back to our problem. After (3.1), we can distinguish between any two non-equivalent definite ternary quadratic forms and hence by (2.3), between any two maximal order types and finally by Deuring's correspondence (2.1) between two supersingular elliptic curves, and all this by means of looking at the representation numbers up to a fixed bound given by, say Siegel, of a set of representatives of the equivalence classes of ternary quadratic forms of discriminant $-p$ (by reduction theory, there are canonical representatives, which are called *reduced ternary quadratic forms*).

So in order to comlete our algorithm, we must be able to pin-point the supersingular elliptic curves using the data from the representation numbers of the reduced ternary quadratic forms. Let us state this in our concrete examples. We write a ternary quadratic form like in (and from) the table of Brandt-Intrau **[BI58]**, namely $f = \begin{pmatrix} a_{11} & a_{22} & a_{33} \\ a_{23} & a_{13} & a_{12} \end{pmatrix}$.

***Example 3.2* (Continued).** *Case $p = 29$:*

We compute the three reduced ternary quadratic forms of discriminant -29: $f_1 = \begin{pmatrix} 1 & 3 & 3 \\ 2 & 0 & 1 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 1 & 0 \end{pmatrix}$ $f_3 = \begin{pmatrix} 1 & 1 & 10 \\ 0 & 1 & 1 \end{pmatrix}$; which correspond to the maximal orders $\mathcal{O}_1, \mathcal{O}_2$ and $\mathcal{O}_3$.

Case $p = 37$:

The two reduced ones in this case are: $f_1 = \begin{pmatrix} 2 & 2 & 3 \\ 0 & 2 & 1 \end{pmatrix}$ and $f_2 = \begin{pmatrix} 1 & 2 & 5 \\ 1 & 1 & 0 \end{pmatrix}$.

Now our problem is to assign to each supersingular elliptic curve of Example (2.2) *one of these ternary quadratic forms.*

To acomplish this, we must pass the information on the side of quadratic forms and their representation numbers to the side of elliptic curves and isogenies. Before we make this explicit in the following proposition, we introduce some notation.
Let f be any quadratic form and denote by $\mathcal{O}_f$ it's associated order according to (2.3). For any order $\mathcal{O}$ in $\mathbb{Q}_{\infty,p}$ define: $\Gamma_b(\mathcal{O}) := \{(tr(\alpha), nr(\alpha)) \in \mathbb{Z}^2 \mid \alpha \in \mathcal{O}$ and $nr(\alpha) \leqslant b\}$, where tr and nr are the reduced trace and reduced norm of the quaternion algebra. Set $\Gamma(\mathcal{O}) = \Gamma_{b_S}(\mathcal{O})$, where b_S is the Siegel bound.

Proposition 3.3. *Let $\{f_1, \ldots, f_t\}$ be a complete set of representatives of reduced ternary quadratic forms of discriminant $-p$. Then the sets $\Gamma(\mathcal{O}_{f_i}) \subset \mathbb{Z}^2$*

for $i = 1, \ldots, t$ are all different, i.e., these subsets characterize univocally the maximal order types in $\mathbb{Q}_{\infty,p}$.

Now we make the simple observation:

Corollary 3.4. *Since the trace and norm on elements of the order correspond to the trace and (separable) degree of the endomorphisms of the elliptic curves, we conclude, that the sets:*

$$\Delta(E) := \{(trace(\varphi), deg(\varphi)) \in \mathbb{Z}^2 \mid \varphi \in \mathrm{End}_{\overline{\mathbb{F}_p}}(E) \text{ and } deg(\varphi) \leqslant b_S\},$$

characterize the supersingular elliptic curves of characteristic p.

Consequently, we must only have to compute the sets $\Gamma(\mathscr{O}_f)$ and $\Delta(E)$ for f running through all the reduced ternary quadratic forms of discriminant $-p$ and E over all the supersingular elliptic curves of characteristic p, and then establish the bijection just by comparing these sets. We make this clear in our:

***Example 3.5* (Continued).** *Case $p = 29$:*

$\Gamma_{[3]}(\mathscr{O}_{f_1}) = \{(-1,3); (1,3); (0,3)\}$;
$\Gamma_{[3]}(\mathscr{O}_{f_2}) = \{(2,3); (-2,3)\}$;
$\Gamma_{[3]}(\mathscr{O}_{f_3}) = \{(-3,3); (3,3); (0;3)\}$; *where the subscript* [3] *denotes simply the subset of norm* 3 *elements of* Γ. *On the elliptic curve side, we simply construct all quotients of the supersingular elliptic curves of degree* 3 *using* **[V71́]** *and for the trace one can avoid easily the polynomial running time algorithms to do it, since one knows the possible traces, so by testing one gets that:* $\Gamma_{[3]}(\mathscr{O}_{f_1}) = \Delta_{[3]}(E(2))$, $\Gamma_{[3]}(\mathscr{O}_{f_2}) = \Delta_{[3]}(E(25))$ *and* $\Gamma_{[3]}(\mathscr{O}_{f_3}) = \Delta_{[3]}(E(0))$.

Case $p = 37$:

Here the sets $\Gamma_{[3]}(\mathscr{O}_{f_1})$ and $\Gamma_{[3]}(\mathscr{O}_{f_2})$ are also different, but we do it with degree 5 isogenies and get: $\Gamma_{[5]}(\mathscr{O}_{f_1}) = \{(0,5)\}$ and $\Gamma_{[5]}(\mathscr{O}_{f_2}) = \{(-1,5); (1,5)\}$. By comparing with the Δ's of the elliptic curves we get: $\Gamma_{[5]}(\mathscr{O}_{f_1}) = \Delta_{[5]}(E(3\pm 10\sqrt{2}))$ and $\Gamma_{[5]}(\mathscr{O}_{f_2}) = \Delta_{[5]}(E(8))$.

Thus we are able to establish the correspondence between supersingular elliptic curves and reduced ternary quadratic forms, and therefore by using formula (1) we compute directly the bases of the endomorphism rings and finish our algorithm.

References

[BI58] H. Brandt & O. Intrau – Tabellen reduzierten positiver ternärer quadratischer Formen, *Abh. Sächs. Akad. Wiss. Math.-nat. Kl.* **45** (1958), no. 4.

[Bra43] H. Brandt – Zur Zahlentheorie der Quaternionen, *Jber. Deutsch. Math.-Verein.* **53** (1943), p. 23–57.

[Brz95] J. Brzezinski – Definite quaternion orders of class number one, *J. Thééor. Nombres Bordeaux* **7** (1995), no. 1, p. 93–96.

[Cn] J. M. Cerviño – Supersingular elliptic curves and maximal quaternionic orders, `http://arxiv.org/pdf/math.NT/0404538`.

[Deu41a] M. Deuring – Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* (1941), p. 197–272.

[Deu41b] ———, Theorie der Korrespondenzen algebraischer Funktionenkörper II, *J. reine angew. Math.* **183** (1941), p. 25–36.

[HW36] H. Hasse & E. Witt – Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p, *Mh. Math. Phys.* **43** (1936), p. 477–492.

[Koh96] D. Kohel – Endomorphism rings of elliptic curves over finite fields, Ph.D. Thesis, University of California at Berkeley, 1996, p. 96.

[Mes86] J.-F. Mestre – Sur la methóde des graphes, exemples et applications, Proceedings of the international conference on class numbers and fundamental units, Nagoya University, 1986, p. 217–242.

[Piz80] A. Pizer – An algorithm for computing modular forms on $\Gamma_0(N)$, *J. Algebra* **64** (1980), no. 2, p. 340–390.

[Sch97] A. Schiemann – Ternary positive definite quadratic forms are determined by their Theta series, *Math. Ann.* **308** (1997), no. 3, p. 507–517.

[Soh57] F. Sohn – Beiträge zur Zahlentheorie der ternären quadratischen Formen und der Quaternionenalgebren, Ph.D. Thesis, Westfälische Wilhelms-Universität zu Münster, 1957, p. 87.

[SP84] R. Schulze-Pillot – Thetareihen positiv definiter quadratischer Formen, *Invent. Math.* **75** (1984), no. 2, p. 283–299.

[SP91] R. Schulze-Pillot – An algorithm for computing genera of ternary quadratic and quaternary quadratic forms, Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC), Bonn, 1991, p. 134–143.

[V́71] J. Vélu – Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. A-B* **273** (1971), p. 238–241.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 61–64
Universität Göttingen, 2004

ON THE NORM PRINCIPLE FOR QUADRATIC FORMS

K. Zainoulline
Fakultät für Mathematik Universität Bielefeld, D-33501 Bielefeld, Germany
E-mail : kirill@Mathematik.Uni-Bielefeld.de

Abstract. We prove a version of Knebusch's Norm Principle for finite étale extensions of semi-local Noetherian domains with infinite residue fields of characteristic different from 2. As an application we prove the case of Grothendieck's conjecture on principal homogeneous spaces for the spinor group of a quadratic form.

1. Generalities

This note describes joint work with I. Panin and M. Ojanguren. All announced results are published in Preprints SFB478 Universität Münster, no. 299, 2003.

The subject of our discussion starts with the well-known classical result on quadratic forms by M. Knebusch [**Kne71**]. To formulate it we introduce some notation.

Let E/F be a finite field extension of degree n (we assume that the characteristic of all fields is different from 2). We denote by $N_F^E : E^* \to F^*$ the norm map of the extension E/F.

May 5, 2004.

Let (V, q) be a quadratic space over F of rank m, i.e., there is given a non-singular quadratic form $q : V \to F$ with $m = \dim V$. Observe that extending the scalars we get the quadratic space (V_E, q_E) over E (here $V_E = V \otimes_F E$ and $q_E = q \otimes_F E$).

For any finite field extension E/F we denote by $D_q(E)$ the group generated by the non-zero elements of E represented by the form q_E. Observe that there are obvious inclusions $(E^*)^2 \subset D_q(E) \subset E^*$. Hence, we have defined a functor

$$D_q : fields/F \to abelian\ groups$$

The result of Knebusch says that D_q respects the norm map or, more precisely, it says

***Theorem 1.1* (Knebusch).** *There is an inclusion of subgroups of F^**

$$N_F^E(D_q(E)) \subset D_q(F).$$

Here we prove a similar result for any finite étale extension S/R of semi-local Noetherian domains with infinite residue fields. Namely,

Theorem 1.2. *Let R be a semi-local Noetherian domain with infinite residue fields. Let S/R be a finite étale R-algebra (not necessary a domain) with infinite residue fields. Let (V, q) be a quadratic space over R of rank m. Let (V_S, q_S) be the base change of (V, q) via the extension S/R. Let $D_q(R)$ (resp. $D_q(S)$) be the group generated by the invertible elements of R (resp. S) represented by the form q.*

Then there is an inclusion between the subgroups of R^*

$$N_R^S(D_q(S)) \subset D_q(R),$$

where N_R^S is the norm map for the finite étale extension S/R.

The idea of the proof. Unfortunately, the proof of Knebusch can not be extended directly to the case of semi-local rings (it simply fails in this case). Hence, in oder to provide the generalization of Knebusch's results one has to use completely different arguments. These are, so called, "general position arguments". Informally speaking, these arguments are based on the following simple fact

> Let $\mathbb{A}_F^n$ be an affine space over an infinite field F. Then any two non-empty Zariski open subsets of $\mathbb{A}_F^n$ have non-zero intersection. And, moreover, this intersection contains an F-rational point.

In fact, the original proof of Knebusch gives an idea how to reformulate the proof in terms of "an existence of a rational point in the intersection of some open subsets". Recall that it goes by induction on the degree n of extension. In order to make the induction step we have to provide some finite field extension of degree strictly less than n. The latter is the same as to find a polynomial of degree strictly less than n which satisfies some relations. And here is the point – we identify the set of coefficients of this polynomial with an affine space and reformulate all the relations in terms of open subsets. Then the existence of a rational point in the intersection means that there exists the desired polynomial. □

2. Applications

The proven result is also called "A Norm Principle for Quadratic Forms" and has many important consequences in the theory of quadratic forms. One of the consequences is related with the famous Grothendieck's conjecture on Principal Homogeneous Spaces. This conjecture was formulated almost 40 years ago and is still open. It says the following

Conjecture 2.1. *Let G be a flat reductive group scheme over a semi-local regular ring R. Let K be the quotient field of R. Then the induced map*

$$H^1_{et}(R,G) \to H^1_{et}(K,G)$$

has trivial kernel. In other words, any G-bundle which is rationally trivial is (Zariski) locally trivial.

One of our main results says

Theorem 2.2. *The Conjecture is true for the case $G = Spin_q$ is a spinor group of a quadratic form q and R is a semi-local regular ring containing an infinite field. Hence, modulo the previous known cases, the conjecture is true for all algebraic groups of classical type excluding a spinor group $Spin_{(A,\sigma)}$ of a quadratic pair.*

The idea of the proof. It turns out that the "Norm Principle" is the key ingredient in the proof of Grothendieck's Conjecture. Namely, consider the part of the long exact sequence associated with $Spin_q$

$$SO_q(R) \xrightarrow{SN} H^1_{et}(R,\mu_2) \to H^1_{et}(R, Spin_q) \to H^1_{et}(R, SO_q),$$

where SN is the spinor norm. Observe that the conjecture is true for SO_q. Thus, in oder to show that the induced map $H^1_{et}(R, Spin_q) \to H^1_{et}(K, Spin_q)$ has trivial kernel it is enough to show this on the cokernels of the spinor norms, i.e., for the abelian presheaf $coker(SN)$. By the results of the author it is known that for any presheaf with transfers F the induced map $F(R) \to F(K)$ is injective. Hence, it is enough to produce the transfer map for the presheaf

$coker(SN)$. Finally, consider the usual norm map on $H^1_{et}(-,\mu_2)$. By the Norm Principle it is well-defined on the quotients by the images of SN, i.e., on the cokernels. And we are done. $\square$

References

[Kne71] M. Knebusch – Ein Satz über die Werte von quadratischen Formen über Körpern, *Invent. Math.* **12** (1971), p. 300–303.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 65–74
Universität Göttingen, 2004

ZETAFUNKTIONEN IN DER GRUPPENTHEORIE – MIT AUGENMERK AUF p-ADISCHE LIEGRUPPEN

B. Klopsch
Mathematisches Institut, Heinrich-Heine-Universität, Düsseldorf
E-mail : klopsch@math.uni-duesseldorf.de

Abstract. Sei G eine endlich erzeugte Gruppe. Für jede natürliche Zahl n ist die Anzahl der Untergruppen vom Index n in G endlich, und man kann die formale Dirichletreihe $\zeta_G(s) := \sum_{H \leqslant_f G} |G : H|^{-s}$ bilden. Unter geeigneten Bedingungen, z.B. falls G nilpotent ist, definiert $\zeta_G(s)$ eine analytische Funktion und besitzt zudem eine Eulerproduktzerlegung. Durch Betrachtung der lokalen Faktoren wird man dazu geführt, entsprechende Zetafunktionen für p-adische Liegruppen bzw. Liegitter zu untersuchen.

In meinem Vortrag habe ich versucht, einen Einblick in die junge und schnell wachsende Theorie dieser Zetafunktionen zu vermitteln.

1. Einleitung

In der ersten Hälfte des zwanzigsten Jahrhunderts bestand nach den enormen Fortschritten in der algebraischen Zahlentheorie zunächst die Hoffnung, eine entsprechende, aber vielleicht ganz neuartige "nicht-kommutative" Theorie für Schiefkörper zu entwickeln. Es stellte sich jedoch bald heraus, daß das Studium der endlichen Schiefkörpererweiterungen von $\mathbb{Q}$ keine großen Überraschungen bereithielt.

May 6th, 2004.

Vor etwa zwanzig Jahren wagten Fritz Grunewald und Dan Segal einen viel weiteren Schritt ins Nicht-kommutative, indem sie begannen, endlich erzeugte, nilpotente Gruppen auf ihre arithmetischen Eigenschaften hin zu untersuchen. Ein zentrales Objekt in der algebraischen Zahlentheorie ist die Dedekindsche Zetafunktion. Nach ihrem Vorbild läßt sich für jede endlich erzeugte Gruppe G die formale Dirichletreihe $\zeta_G(s) := \sum_{H \leqslant_f G} |G : H|^{-s}$ bilden. Falls G nicht "zu viele" Untergruppen von endlichem Index besitzt, konvergiert $\zeta_G(s)$ auf einer rechten komplexen Halbebene $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \alpha\}$, $\alpha \in \mathbb{R}$, und definiert so eine analytische Funktion. Für die Klasse der endlich erzeugten, nilpotenten Gruppen wurden grundlegende Eigenschaften dieser Zetafunktionen erstmals in den achtziger Jahren aufgedeckt [**GSS88**]. Seitdem hat es, auch auf dem eng benachbarten Gebiet Untergruppenwachstum, eine rasante Entwicklung gegeben; davon zeugt die kürzlich erschienene Monographie [**LS03**]. Klassische Zetafunktionen, die algebraischen Gruppen zugeordnet sind, erscheinen nunmehr in einem neuen Licht [**dSL96**], und erst kürzlich wurde entdeckt, daß die Zetafunktion $\zeta_G(s)$ einer endlich erzeugten, nilpotenten Gruppe G eng zusammenhängt mit dem Zählen von Punkten auf gewissen G zugeordneten Varietäten [**dSG00**].

Im folgenden möchte ich, nicht zuletzt anhand von konkreten Beispielen, einen Eindruck davon vermitteln, was die Hauptergebnisse und die anstehenden Herausforderungen auf diesem jungen Forschungsgebiet sind. Dabei erlaube ich mir, auch einige weniger gewichtige eigene Resultate mitzuteilen. Thematisch ähnlich ausgerichtet und teilweise ausführlicher geschrieben ist das Kapitel "Zeta Functions of Groups" in [**dSSS00**].

2. Begriffsbildung und erste markante Beispiele

Sei G eine Gruppe. Für $n \in \mathbb{N}$ schreiben wir

$$a_n(G) := \#\{H \leqslant G \mid |G : H| = n\} \quad \text{und} \quad s_n(G) := \sum_{k=1}^{n} a_k(G).$$

Wir wollen voraussetzen, daß $a_n(G)$ für jede natürliche Zahl n endlich ist. (Dies ist sicherlich der Fall, wenn G endlich erzeugt ist.) Uns interessieren dann die arithmetischen Eigenschaften der Folge $a_n(G)$, $n \in \mathbb{N}$, und asymptotische Abschätzungen für das Wachstum der Folge $s_n(G)$, $n \in \mathbb{N}$. Zu diesem Zweck bilden wir die formale Dirichletreihe

$$\zeta_G(s) := \sum_{H \leqslant_f G} |G : H|^{-s} = \sum_{n=1}^{\infty} a_n(G) n^{-s}.$$

Augenscheinlich geschieht dies in Analogie zur Dedekindschen Zetafunktion eines Zahlkörpers, die auf gleiche Weise durch das Zählen von Idealen im zugehörigen Ganzheitsring entsteht. Die Invariante

$$\alpha(G) := \inf\{\beta \in \mathbb{R} \mid s_n(G) = O(n^\beta)\} = \limsup \frac{\log s_n(G)}{\log n} \in [0, \infty]$$

mißt den (polynomiellen) Grad des Untergruppenwachstums von G. Ist $\alpha(G) < \infty$, so besitzt die Gruppe G polynomielles Untergruppenwachstum (oder abkürzend PSG für den englischen Ausdruck "polynomial subgroup growth").

Ist G eine PSG Gruppe, so konvergiert $\zeta_G(s)$ punktweise absolut auf der rechten Halbebene $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \alpha(G)\}$ und definiert dort eine holomorphe Funktion. Unter der (schwachen) Zusatzbedingung $\alpha(G) \neq 0$ divergiert die Reihe $\zeta_G(s)$ für $s = \alpha(G)$, und $\alpha(G)$ stimmt überein mit der sogenannten Konvergenzabzisse von $\zeta_G(s)$. Unser Ziel besteht nun darin, die analytischen Eigenschaften der Zetafunktion $\zeta_G(s)$ besser zu verstehen und diese anschließend in Verbindung zu setzen mit den algebraischen Eigenschaften der Gruppe G.

Wir schließen diesen Abschnitt mit zwei wegweisenden Beispielen, die schon seit nunmehr zwanzig Jahren einen gewissen Vorzeigestatus besitzen.

Beispiel 2.1. *Sei $G := \mathbb{Z}^d$ die freie abelsche Gruppe vom Rang d. Ein Induktionsargument zeigt, daß*

$$\zeta_G(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-d+1)$$

ist, wobei $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ die Riemannsche Zetafunktion bezeichnet. Wir erhalten $\alpha(G) = d$ und mittels eines einfachen Tauberschen Satzes präzise asymptotische Abschätzungen für $s_n(G)$:

$$s_n(G) \sim d^{-1}\zeta(d)\zeta(d-1)\cdots\zeta(2)n^d \qquad \text{für } n \to \infty.$$

Im einfachsten nicht-trivialen Fall $d = 2$ gilt wegen $\zeta(2) = \pi^2/6$ beispielsweise

$$s_n(G) \sim (\pi^2/12)n^2 \qquad \text{für } n \to \infty.$$

Offenbar besitzt $\zeta_G(s)$ eine meromorphe Fortsetzung auf ganz $\mathbb{C}$.

Beispiel 2.2. *Sei $G = \langle x, y \mid [[x,y],x] = [[x,y],y]\rangle$ die diskrete Heisenberggruppe. Wir bemerken, daß G sich konkret realisieren läßt als Gruppe aller oberen 3×3 Dreiecksmatrizen über $\mathbb{Z}$ mit Einträgen 1 auf der Diagonalen. Eine nicht-triviale Rechnung zeigt:*

$$\zeta_G(s) = \zeta(s)\zeta(s-1)\zeta(2s-2)\zeta(2s-3)\zeta(3s-3)^{-1}.$$

Hieraus erkennt man, daß $\alpha(G) = 2$ ist und $\zeta_G(s)$ an der Stelle $s = 2$ einen Pol zweiter Ordnung besitzt. Ein geeigneter Tauberscher Satz liefert:

$$s_n(G) \sim \frac{\zeta(2)^2}{2\zeta(3)} n^2 (\log n) \qquad \textit{für } n \to \infty.$$

Offensichtlich läßt sich $\zeta_G(s)$ meromorph auf ganz $\mathbb{C}$ fortsetzen.

3. Welche Gruppen haben polynomielles Untergruppenwachstum?

Ist G eine Gruppe, so bildet $R(G) := \bigcap\{N \trianglelefteq G \mid |G : N| < \infty\}$ eine charakteristische Untergruppe von G. Offenbar gilt $a_n(G) = a_n(G/R(G))$ für alle $n \in \mathbb{N}$, und das Untergruppenwachstum von G besagt wenig über die algebraische Struktur von $R(G)$. Es ist daher sinnvoll, sich auf solche Gruppen G zu beschränken, für die $R(G) = 1$ ist; diese heißen residuell-endlich.

***Satz 3.1* (Lubotzky, Mann, Segal [LMS93]).** *Sei G eine endlich erzeugte, residuell-endliche Gruppe. Dann sind äquivalent:*
(1) *G hat polynomielles Untergruppenwachstum;*
(2) *G enthält eine Untergruppe von endlichem Index, welche auflösbar und von endlichem Rang ist.*

Definitionsgemäß besitzt eine Gruppe H endlichen Rang, falls es eine natürliche Zahl d gibt, so daß sich jede endlich erzeugte Untergruppe von H schon von d Elementen erzeugen läßt. Endliche Gruppen und Untergruppen der additiven Gruppe $\mathbb{Q}^+$ besitzen diese Eigenschaft. Ist H eine residuell-endliche, auflösbare Gruppe von endlichem Rang, so gibt es eine endliche Kette von Untergruppen $1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_r = H$, wobei jede Faktorgruppe H_i/H_{i-1} entweder endlich oder Untergruppe von $\mathbb{Q}^+$ ist. Ein Induktionsargument liefert die Implikation von (2) nach (1) in Satz 3.1.

Die andere Richtung, von (1) nach (2), ist viel schwieriger einzusehen. Sei G eine endlich erzeugte, residuell-endliche Gruppe mit PSG. Der Nachweis, daß G die Bedingung (2) erfüllt, beruht auf mehreren Schritten, die wir nur grob skizzieren können:

(i) Ergebnisse der Theorie der endlichen Gruppen (inklusive der Klassifikation der endlichen einfachen Gruppen) erlauben es, die möglichen Isomorphietypen der oberen Kompositionsfaktoren von G einzuschränken.
(ii) Mittels geeigneter Linearisierungsmethoden reduziert man das Problem auf den Fall, daß G linear über einem Körper der Charakteristik Null ist.
(iii) Unter Verwendung des Primzahlsatzes zeigt man, daß (unendliche) halbeinfache arithmetische Gruppen niemals PSG haben. Aufgrund der

"Lubotzky-Alternative" (Stichwort "starke Approximation für lineare Gruppen") folgt, daß G eine auflösbare Untergruppe von endlichem Index besitzt.

(iv) Zum Schluß ist (unter Verwendung der Auflösbarkeit) nachzuweisen, daß G zudem endlichen Rang hat.

Bemerkung 3.2. Rein gruppentheoretisch betrachtet, stellt sich die Frage: Was passiert, wenn wir statt Untergruppen von endlichem Index Untergruppen von endlicher Ordnung zählen? Klassische Arbeiten von Baer, Černikov, et al. beschreiben die Struktur von Gruppen, die für jedes $n \in \mathbb{N} \cup \{\infty\}$ nur endlich viele Elemente der Ordnung n besitzen. Derartige Gruppen scheinen jedoch keine interessante arithmetische Struktur zu tragen; vgl. [**Klo03b**].

Eine wichtige Unterklasse der PSG-Gruppen bilden die endlich erzeugten, nilpotenten Gruppen; diese sind automatisch residuell-endlich und besitzen endlichen Rang. Sei G eine endlich erzeugte, nilpotente Gruppe. Die bekannte Tatsache, daß jede endliche, nilpotente Gruppe direktes Produkt seiner Sylow-Untergruppen ist, führt zu der Eulerproduktzerlegung

$$\zeta_G(s) = \prod_p \zeta_{G,p}(s),$$

wobei das Produkt über alle Primzahlen p zu bilden ist und die lokalen Faktoren $\zeta_{G,p} = \sum_{k=0}^{\infty} a_{p^k}(G) p^{-ks}$ jeweils Untergruppen zählen, deren Index in G eine Potenz von p ist. Jede Untergruppe der nilpotenten Gruppe G ist subnormal in G. Daher ist für jedes p der lokale Faktor $\zeta_{G,p}(s)$ zugleich die Zetafunktion der pro-p Vervollständigung $\widehat{G}_p$ von G. Es liegt daher nahe, etwas allgemeiner das Untergruppenwachstum von (topologisch) endlich erzeugten pro-p Gruppen zu untersuchen. Das folgende Resultat fußt auf Lazards herausragender Arbeit [**Laz65**], die übrigens für das gesamte Gebiet in entscheidender Weise eine Art Katalysatorrolle gespielt hat.

Satz 3.3. *Eine pro-p Gruppe besitzt genau dann polynomielles Untergruppenwachstum, wenn sie p-adisch analytisch ist.*

Es gibt also zwei sehr unterschiedliche, interessante Klassen von Gruppen, deren Zetafunktionen wir verstehen möchten: (1) endlich erzeugte, nilpotente Gruppen und (2) kompakte p-adische Liegruppen. Innerhalb dieser Klassen finden sich durchaus auch ganz konkrete Gruppen von besonderem Interesse, wie z.B. die Serie $\mathrm{SL}_d(\mathbb{Z}_p)$, $d \in \mathbb{N}$.

4. Methoden, Ergebnisse und offene Fragen

Sei G eine kompakte p-adische Liegruppe. Dann besitzt G eine offene uniforme pro-p Untergruppe U, und die Berechnung von $\zeta_G(s)$ läßt sich auf endlich viele, den Nebenklassen von U in G zugeordnete Zetafunktionen zurückführen. Wir beschränken uns der Übersicht halber auf den denkbar einfachsten Fall, nämlich $G = U$. Dann kann $\zeta_G(s)$ (bis auf einen konstanten Vorfaktor) als p-adisches Integral der Gestalt

$$\int_{V \subseteq \mathbb{Z}_p^m} |f(\mathbf{v})|_p |g(\mathbf{v})|_p^s d\mu$$

geschrieben werden, wobei sowohl der Integrationsbereich V als auch die Funktionen f, g von der Struktur von G abhängen. Die Integration erstreckt sich über ausgewählte, aber nicht eindeutig zugeordnete Erzeugendensysteme fester Länge für die Untergruppen von G; diese werden parametrisiert durch Vektoren $\mathbf{v} \in V \subseteq \mathbb{Z}_p^m$. Im Integranden beschreibt $|g(\mathbf{v})|_p$ den Index der $\mathbf{v}$ zugeordneten Untergruppe von G, und das Gewicht $|f(\mathbf{v})|_p$ trägt der Tatsache Rechnung, daß die gleiche Untergruppe aufgrund verschiedener Erzeugendensysteme mehrfach gezählt wird.

Als einfachstes Beispiel geben wir eine Integraldarstellung für die freie abelsche pro-p Gruppe $\mathbb{Z}_p^d$ an. Jede Untergruppe von $\mathbb{Z}_p^d$ kann von d Elementen erzeugt werden, und jedes d-Tupel in $\mathbb{Z}_p^d$ läßt sich in einer $d \times d$ Matrix über $\mathbb{Z}_p$ zusammenfassen. Es gilt

$$\zeta_{\mathbb{Z}_p^d}(s) = (1 - p^{-1})^{-d} \int_V |\lambda_{11}|_p^{s-1} |\lambda_{22}|_p^{s-2} \cdots |\lambda_{dd}|_p^{s-d} d\mu,$$

wobei der Integrationsbereich aus allen oberen Dreiecksmatrizen besteht:

$$V = \{(\lambda_{ij}) \in \mathrm{Mat}_d(\mathbb{Z}_p) \mid \lambda_{ij} = 0 \text{ if } i > j\}.$$

Dieses spezielle Integral läßt sich leicht ausführen; man erhält

$$\zeta_{\mathbb{Z}_p^d}(s) = \zeta_p(s)\zeta_p(s-1) \cdots \zeta_p(s-d+1),$$

wobei $\zeta_p(s) = \sum_{k=0}^{\infty} p^{-ks}$ den lokalen p-Faktor der Riemannschen Zetafunktion bezeichnet; vgl. Beispiel 2.1. Im allgemeinen ist die explizite Berechnung derartiger Integrale aber äußerst schwierig. Ergebnisse der p-adischen Modelltheorie zeigen immerhin, daß $\zeta_G(s) = \Phi(p^{-s})/\Psi(p^{-s})$ eine rationale Funktion über $\mathbb{Q}$ in p^{-s} ist; vgl. [**dS93**]. Dies bedeutet anschaulich, daß die Folge $a_{p^k}(G)$, $k \in \mathbb{N}$, ab einem bestimmten Punkt eine lineare Rekursionsgleichung erfüllt.

Jede kompakte p-adische Liegruppe besitzt eine offene pro-p Untergruppe U, die auf natürliche Weise die Struktur eines $\mathbb{Z}_p$-Liegitters $L = L_U$ trägt. Unter geeigneten Bedingungen (z.B. $\dim(U) \leqslant p$) bildet jede Untergruppe von

U zugleich ein Lieteilgitter von L und umgekehrt; siehe [**Klob**]. Für solche Liegruppen U genügt es also, die entsprechende Zetafunktion $\zeta_L(s)$ des zugehörigen $\mathbb{Z}_p$-Liegitters $L = L_U$ zu bestimmen. Die wenigen, bislang explizit bekannten Zetafunktionen wurden allesamt als Zetafunktionen von Liegittern berechnet. Die "einfachste" einfache $\mathbb{Q}_p$-Liealgebra $\mathfrak{sl}_2(\mathbb{Q}_p)$ enthält das $\mathbb{Z}_p$-Liegitter $\mathfrak{sl}_2(\mathbb{Z}_p)$. Eine nicht-triviale Rechnung [**Ila99**] zeigt für $p \geqslant 3$:

$$\zeta_{\mathfrak{sl}_2(\mathbb{Z}_p)} = \zeta_p(s)\zeta_p(s-1)\zeta_p(2s-1)\zeta_p(2s-2)\zeta_p(3s-1)^{-1}. \tag{4.1}$$

Ein entsprechender Ausdruck für die Zetafunktion von $\mathfrak{sl}_2(\mathbb{Z}_2)$ ist inzwischen auch bekannt [**dST02**]; der Einfachheit halber möchte ich mich im weiteren aber auf den Fall $p \geqslant 3$ beschränken.

Die Formel (4.1) zeigt insbesondere, daß die Anzahl der Lieteilgitter mit Index p^n in $\mathfrak{sl}_2(\mathbb{Z}_p)$ von der Größenordnung np^n ist. Shalev äußerte daraufhin die Vermutung, daß pro-p Gruppen mit linear beschränktem Untergruppenwachstum notwendigerweise auflösbar sind. Nun besitzt der Chevalley-Typ A_1 neben $\mathfrak{sl}_2(\mathbb{Q}_p)$ genau eine weitere $\mathbb{Q}_p$-Form, nämlich $\mathfrak{sl}_1(\mathbb{D}_p)$, wobei $\mathbb{D}_p$ die (bis auf Isomorphie eindeutig bestimmte) zentral-einfache $\mathbb{Q}_p$-Divisionsalgebra vom Index 2 bezeichnet. Sei Δ_p die maximale $\mathbb{Z}_p$-Ordnung von $\mathbb{D}_p$. Es war tatsächlich eine kleine Überraschung, als ich feststellte, daß das $\mathbb{Z}_p$-Liegitter $\mathfrak{sl}_1(\Delta_p)$ im Gegensatz zu $\mathfrak{sl}_2(\mathbb{Z}_p)$ lineares Teilgitterwachstum vorweist. Genauer gilt [**Klo03a**]:

$$\zeta_{\mathfrak{sl}_1(\Delta_p)} = \zeta_p(s)\zeta_p(2s-1)\zeta_p(2s-2). \tag{4.2}$$

Insbesondere ist die Anzahl der Lieteilgitter mit Index p^n in $\mathfrak{sl}_1(\Delta_p)$ von der Größenordnung p^n. Weitere Überlegungen, auf die ich nicht näher eingehen möchte, führen zu einer vollständigen Beschreibung der pro-p Gruppen mit linear beschränktem Untergruppenwachstum [**Klo03c**].

Die explizite Formel (4.2) spielt auch eine Rolle bei der Lösung eines weiteren von Shalev angeregten Problems: Jede profinite Gruppe G mit der Eigenschaft, daß $a_n(G) < n$ für fast alle $n \in \mathbb{N}$ ist, besitzt eine offene zentrale, prozyklische Untergruppe; siehe [**Kloa**].

Ein wichtiges offenes Problem besteht darin, geeignete Methoden zur Berechnung weiterer Zetafunktionen zu entwickeln. Besonders naheliegend ist

Problem 4.1. *Bestimme $\zeta_G(s)$ für $G = \mathrm{SL}_d^1(\mathbb{Z}_p)$, $d \geqslant 3$, bzw. berechne die entsprechenden Zetafunktionen für die $\mathbb{Z}_p$-Liegitter $\mathfrak{sl}_d(\mathbb{Z}_p)$.*

Anhand der Formeln (4.1) und (4.2) läßt sich ein auffälliges, allgemein auftretendes Phänomen illustrieren: Es gelten die Funktionalgleichungen

$$\zeta_{\mathfrak{sl}_2(\mathbb{Z}_p)}(s)|_{p\to p^{-1}} = -p^{-3s+3}\zeta_{\mathfrak{sl}_2(\mathbb{Z}_p)}(s),$$
$$\zeta_{\mathfrak{sl}_1(\Delta_p)}(s)|_{p\to p^{-1}} = -p^{-5s+3}\zeta_{\mathfrak{sl}_1(\Delta_p)}(s).$$

Problem 4.2. *Für welche pro-p Gruppen G mit PSG erfüllt die zugehörige Zetafunktion eine Funktionalgleichung der Form*

$$\zeta_G(s)|_{p\mapsto p^{-1}} = \pm p^{as+b}\zeta_G(s)$$

mit $a, b \in \mathbb{Z}$? Woran liegt das? (Insbesondere sind diese Fragen für die lokalen Faktoren einer endlich erzeugten, nilpotenten Gruppe von großem Interesse.)

Während es bei der Untersuchung von Zetafunktionen p-adischer Liegruppen oftmals gerade auf die Eigentümlichkeiten der zugrundeliegenden Primzahl p ankommt, steht bei den nilpotenten Gruppen das Zusammenspiel der lokalen Faktoren "bis auf endlich viele" im Vordergrund. Der folgende Satz stellt einen Höhepunkt der bislang entwickelten Theorie dar.

***Satz 4.3* (du Sautoy, Grunewald [dSG00]).** *Sei G eine (unendliche) endlich erzeugte, nilpotente Gruppe. Dann gelten:*

(i) *Die Konvergenzabzisse $\alpha(G)$ ist rational.*
(ii) *Die Funktion $\zeta_G(s)$ besitzt eine meromorphe Fortsetzung auf eine rechte komplexe Halbebene, die $\alpha(G)$ enthält.*
(iii) *Für $n \to \infty$ besteht die asymptotische Abschätzung $s_n(G) \sim cn^{\alpha}(\log n)^{\beta}$, wobei $c \in \mathbb{R}$, $\alpha = \alpha(G)$ und $\beta \in \mathbb{N}_0$. Hierbei gibt $\beta + 1$ die Polordnung von $\zeta_G(s)$ bei $s = \alpha$ an.*

Der Beweis beginnt mit der bereits erwähnten Integraldarstellung für die lokalen Zetafunktionen einer endlich erzeugten, nilpotenten Gruppe G: Es gibt endlich viele Polynome $f_0, f_1, \ldots, f_r, g_0, g_1, \ldots, g_r \in \mathbb{Q}[X_1, \ldots, X_d]$, so daß für fast alle Primzahlen p gilt:

$$\zeta_{G,p}(s) = a_{p,0}^{-1} \int_{V_p} |f_0(\mathbf{x})|_p |g_0(\mathbf{x})|_p^s d\mu,$$

wobei $V_p = \{\mathbf{x} \in \mathbb{Z}_p^d \mid |f_i(\mathbf{x})|_p \geqslant |g_i(\mathbf{x})|_p \text{ für } 1 \leqslant i \leqslant r\}$ und $a_{p,0} \neq 0$ einfach nur einen Skalierungsfaktor darstellt. Integrale von dieser Gestalt heißen Kegelintegrale, da der Integrationsbereich bei geeigneter Interpretation eine kegelförmige Gestalt besitzt. Eine Auswertung des Integrals, zu der im allgemeinen zunächst die Singularitäten im Integrationsbereich aufgelöst werden müssen, liefert die Formel

$$a_{p,0}\zeta_{G,p}(s) = a_{p,0} + \sum_{I \in \mathscr{S}} c_p(I) P_I(p, p^{-s}),$$

wobei $\mathscr{S}$ eine endliche Menge (Boolescher Kombinationen) von algebraischen Varietäten über $\mathbb{Z}$ bezeichnet, die Koeffizienten $c_p(I)$ jeweils die Anzahl der $\mathbb{F}_p$-Punkte auf der Reduktion von I modulo p angeben und jedes $P_I(Y_1, Y_2)$ eine rationale Funktion über $\mathbb{Q}$ darstellt.

Eine Lang-Weil-Abschätzung für die Anzahl von $\mathbb{F}_p$-Punkten auf den Varietäten I modulo p liefert (i). Mit Hilfe von Artin L-Funktionen konstruiert man die in (ii) versprochene meromorphe Fortsetzung. Eine Anwendung geeigneter Tauberscher Sätze liefert schließlich (iii).

Derjenige Schritt, der im Moment am wenigsten durchschaut wird, ist das Auflösen der Singularitäten im Integrationsbereich. Nur in besonders einfachen Fällen ist dies praktisch durchführbar. Was für Varietäten mit welcher Art von Singularitäten als Integrationsbereich auftreten können ist weitgehend unbekannt. Eine diesbezüglich interessante Konstruktion findet sich in [**dS01**].

Ein wichtiges Problem besteht darin, die Abhängigkeit der lokalen Faktoren $\zeta_{G,p}(s)$ von p genauer zu klären. In diesem Zusammenhang besteht unter anderem das folgende

Problem 4.4. *Sei $F = F_{c,d}$ die freie nilpotente Gruppe der Klasse c mit $d \geqslant 2$ Erzeugenden. Existiert dann eine rationale Funktion $P(X,Y) \in \mathbb{Q}(X,Y)$, so daß für fast alle Primzahlen p gilt $\zeta_{F,p}(s) = P(p, p^{-s})$?*

In den Spezialfällen $c \in \{1, 2\}$ oder $d = 2$ ist die Antwort bekannt und fällt positiv aus; vgl. Beispiel 2.2.

Zum Schluß sei bemerkt, daß ein enger Zusammenhang besteht zwischen Problem 4.4 und der berühmten PORC-Vermutung von Higman. Letztere, falls wahr, gibt Auskunft über die Anzahl der Isomorphietypen endlicher Gruppen von Primzahlpotenzordnung: Für jedes $n \in \mathbb{N}$ gibt es eine Zahl $r \in \mathbb{N}$ und Polynome $f_1, \ldots, f_r \in \mathbb{Z}[X]$, so daß für jede Primzahl p die Anzahl der (Isomorphietypen von) Gruppen der Ordnung p^n gleich $f_j(p)$ ist, wobei $j \equiv_r p$ zu wählen ist. (Die Abkürzung PORC steht sinngemäß für "Polynomial On Residue Classes".) Details über die Verbindung mit Problem 4.4 finden sich in [**dS00**].

References

[dS93] M. du Sautoy, *Finitely generated groups, p-adic analytic groups and Poincaré series*, Ann. Math. **137** (1993), 639–670.

[dS00] ———, *Counting p-groups and nilpotent groups*, Publ. Math., Inst. Hautes Étud. Sci. **92** (2000), 63–112.

[dS01] ———, *A nilpotent group and its elliptic curve: non-uniformity of local zeta functions of groups*, Isr. J. Math. **126** (2001), 269–288.

[dSG00] M. du Sautoy and F. Grunewald, *Analytic properties of zeta functions and subgroup growth*, Ann. Math. **152** (2000), 793–833.

[dSL96] M. du Sautoy and A. Lubotzky, *Functional equations and uniformity for local zeta functions of nilpotent groups*, Am. J. Math. **118** (1996), 39–90.

[dSSS00] M. du Sautoy, D. Segal, and A. Shalev (eds.), *New Horizons in pro-p Groups*, Progress in Mathematics, vol. 184, Birkhäuser, Boston-Basel-Berlin, 2000.

[dST02] M. du Sautoy and G. Taylor, *The zeta function of $\mathfrak{sl}_2$ and resolution of singularities*, Math. Proc. Camb. Philos. Soc. **132** (2002), 57–73.

[GSS88] F. Grunewald, D. Segal, and G. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), 185–223.

[Ila99] I. Ilani, *Zeta functions related to the group* $\mathrm{SL}_2(\mathbb{Z}_p)$, Isr. J. Math. **109** (1999), 157–172.

[Kloa] B. Klopsch, *Groups with less than n subgroups of index n*, to appear in Math. Ann.

[Klob] ______, *On the Lie theory of p-adic analytic groups*, to appear in Math. Z.

[Klo03a] ______, *Pro-p groups with linear subgroup growth*, Math. Z. **245** (2003), 335–370.

[Klo03b] ______, *Subgroup growth: the unfamiliar twin*, unpublished manuscript, 2003.

[Klo03c] ______, *Zeta functions related to the pro-p group* $\mathrm{SL}_1^1(\Delta_p)$, Math. Proc. Camb. Philso. Soc. **135** (2003), 45–57.

[Laz65] M. Lazard, *Groupes analytiques p-adiques*, Publ. Math., Inst. Hautes Étud. Sci. **26** (1965), 389–603.

[LMS93] A. Lubotzky, A. Mann, and D. Segal, *Finitely generated groups of polynomial subgroup growth*, Isr. J. Math. **82** (1993), 363–371.

[LS03] A. Lubotzky and D. Segal, *Subgroup growth*, Progress in Mathematics, vol. 212, Birkhäuser, Basel-Boston-Berlin, 2003.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 75–82
Universität Göttingen, 2004

ZARISKI CHAMBERS AND STABLE BASE LOCI

T. Bauer
FB Mathematik und Informatik, Philipps-Universität Marburg, Hans-Meerwein-Straße, D-35032 Marburg, Germany
E-mail : tbauer@Mathematik.Uni-Marburg.de

Abstract. In joint work with A. Küronya and T. Szemberg we study certain asymptotic invariants of linear series: the stable base locus and the volume. In particular we are interested in the question how these invariants behave under small perturbations in the Néron-Severi space. We show that both invariants lead to a partition of the big cone into suitable subcones, and that – somewhat surprisingly – these two partitions coincide. This phenomenon is explained by the fact that both problems are closely related to the variation of the Zariski decomposition, which is an interesting problem quite on its own.

1. Generalities

We report here on our recent joint work [**BKS**] with A. Küronya and T. Szemberg on asymptotic invariants of linear series. Let us start by considering three questions.

Stable base loci. Let X be a smooth projective variety and L a line bundle on X. We denote by $\mathrm{SB}(L)$ the *stable base locus* of L, i.e., the intersection of the base loci of the linear series $|kL|$ for all positive integers k. More generally, we

---

May 12th, 2004.

will consider the stable base loci of $\mathbb{Q}$-line bundles L by passing to an integral multiple of L; this is well-defined, since the stable base locus is invariant under taking multiples (i.e. tensor powers) of the line bundle.

Stable base loci were recently studied by Nakamaye ([**Nak00**], [**Nak03**]). He showed in particular that for a big and nef divisor L, an ample divisor A, and for small $\varepsilon > 0$, the stable base locus $\mathrm{SB}(L - \varepsilon A)$ is the union of all subvarieties $V \subset X$ such that $L^{\dim V} \cdot V = 0$. So in particular the stable base locus remains constant when a big and nef line bundle is perturbed in anti-ample directions. We ask quite generally:

Question 1. *How does* $\mathrm{SB}(L)$ *vary when* L *moves in the big cone of* X*?*

One needs to be a bit more precise here: the stable base locus is not invariant under numerical equivalence, and hence it is not a function on the big cone. Following [**ELM**$^+$] we therefore consider a modified version of the stable base locus, the *stabilized base locus*, defined as

$$\mathrm{B}_+(L) = \mathrm{SB}(L - A) \ ,$$

where A is a sufficiently small ample bundle. These stabilized base loci in fact turn out to be numerical invariants.

Volumes. Consider a line bundle L on a smooth projective variety X of dimension n. The Riemann–Roch problem is concerned with the study of the behaviour of $h^0(X, kL)$ as a function of k. While the exact determination of these dimensions is difficult in general, they grow typically (i.e. for big line bundles) like k^n. The *volume* of L, introduced by Cutkosky, is then defined as

$$\mathrm{vol}_X(L) =_{\mathrm{def}} \limsup_k \frac{h^0(X, kL)}{k^n/n!} .$$

This concept readily extends to $\mathbb{Q}$-divisors, and in fact it has recently been established (in [**Laz**]) that it defines a continuous function on the Néron-Severi space. It is thus natural to ask:

Question 2. *How does* $\mathrm{vol}(L)$ *vary when* L *moves in the big cone of* X*?*

Zariski decompositions. Let now X be a smooth projective surface. Recall [**Zar62**], [**KMM87**, Theorem 7.3.1] that a (pseudo-)effective $\mathbb{R}$-divisor D on X admits a unique Zariski decomposition, i.e., there exists a unique effective $\mathbb{R}$-divisor $N_D = \sum_{i=1}^m a_i N_i$ such that

(i) $P_D = D - N_D$ ist nef,
(ii) N_D is either zero or its intersection matrix $(N_i \cdot N_j)$ is negative definite,
(iii) $P_D \cdot N_i = 0$ for $i = 1, \ldots, m$.

The Zariski decomposition is determined by the numerical equivalence class of D, so it makes sense to study it as a function on the Néron-Severi space. We ask:

Question 3. *How does the Zariski decomposition of L vary when L moves in the big cone of X?*

Each of the three problems leads to a decomposition of the big cone into subsets where the invariant in question behaves nicely. Our result [**BKS**] says that, somewhat surprisingly, on surfaces the underlying decompositions in fact agree:

Theorem. *Let X be a smooth projective surface over the complex numbers. Then there is a locally finite decomposition of the big cone of X into rational locally polyhedral subcones such that the following holds:*

(i) *In each subcone the support of the negative part of the Zariski decomposition of the divisors in the subcone is constant.*
(ii) *On each of the subcones the volume function is given by a single polynomial of degree two.*
(iii) *In the interior of each of the subcones the stable base loci are constant.*

As Zariski decompositions do not in general exist on higher-dimensional varieties, part (i) is specific to surfaces. On the other hand, it is natural to ask for higher-dimensional analogues of statements (ii) and (iii). A statement as clean as that of the theorem above, however, cannot be expected: already in dimension three there are examples where the volume is not locally polynomial (see [**BKS**], Section 3.3); and the subsets, where the stable base locus is constant, need not have rational boundaries (see [**BKS**], Example 2.11). Nonetheless it would be interesting to know whether the statements (ii) and (iii) might have higher-dimensional analogues at least for certain types of varieties.

2. The decomposition

In this section we will focus on explaining the decomposition of the big cone as stated in the theorem. Our purpose is to convey some feeling for the geometry underlying the three problems in question, and to sketch the main ideas. Details and complete proofs can be found in [**BKS**].

Consider an $\mathbb{R}$-divisor D on a smooth projective surface X with Zariski decomposition

$$D = P_D + N_D \ .$$

We consider the set of *null curves* and the set of *negative curves* of D, defined as

$$\operatorname{Null}(D) =_{\text{def}} \{\, C \mid C \text{ irreducible curve with } D \cdot C = 0 \,\}$$

and

$$\operatorname{Neg}(D) =_{\text{def}} \{\, C \mid C \text{ irreducible component of } N_D \,\}$$

respectively. On always has $\operatorname{Neg}(D) \subset \operatorname{Null}(P_D)$, but it may well happen that some of the null curves do not appear as components of N_D.

Now we can specify the subcones of the big cone mentioned in the theorem. To this end, consider for a big and nef $\mathbb{R}$-divisor P the set

$$\Sigma_P = \{\, D \in \operatorname{Big}(X) \mid \operatorname{Neg}(D) = \operatorname{Null}(P) \,\} \ .$$

It is immediate to check – using the properties of the Zariski decomposition – that Σ_P is a convex cone. (It will in general be neither open nor closed.) One shows (see [**BKS**], Lemma 1.6) that these cones yield a decomposition of the big cone, i.e.,

$$\operatorname{Big}(X) = \bigcup_{P \text{ big and nef}} \Sigma_P \ , \tag{1}$$

where $\Sigma_P = \Sigma_{P'}$ or $\Sigma_P \cap \Sigma_{P'} = \varnothing$ for any two big and nef $\mathbb{R}$-divisors P and P'. The main point in proving (1) is that, given a big divisor D, one is able to find a big and nef divisor P such that $\operatorname{Neg}(D) = \operatorname{Null}(P)$.

As far as part (i) of the theorem is concerned, two things remain to be shown.

Proposition 4.

(a) *The cone Σ_P is locally polyhedral.*
(b) *The decomposition (1) is locally finite.*

(See [**BKS**], Proposition 1.10 and Proposition 1.15.) In order to prove assertion (a), we provide an explicit description of Σ_P as follows:

$$\overline{\Sigma}_P \cap \operatorname{Big}(X) = (\operatorname{Big}(X) \cap \operatorname{Face}(P)) + V^{\geqslant 0}(\operatorname{Null}(P)) \ . \tag{2}$$

Here

$$\operatorname{Face}(P) =_{\text{def}} \operatorname{Null}(P)^{\perp} \cap \operatorname{Nef}(X)$$

is the smallest face of the nef cone that contains P, and $V^{\geqslant 0}(\operatorname{Null}(P))$ denotes the cone generated by the null curves of P. As the part of the nef cone that is contained in the big cone is locally polyhedral ([**BKS**], Corollary 1.4), statement (a) follows.

The description of the chambers in (2) is particularly instructive as it shows that each chamber Σ_P corresponds to a face of the nef cone. This fact is also illustrated in the example that we provide in Section 3.

Turning to assertion (b), suffice it to say that it is essentially a consequence of the

Main Lemma ([BKS], Lemma 1.14). *If D is a big $\mathbb{R}$-divisor and A an ample $\mathbb{R}$-divisor, then*

$$\operatorname{Neg}(D+\lambda A) \subset \operatorname{Neg}(D) \qquad \text{for all } \lambda \geqslant 0 \ .$$

The nice fact about the main lemma is that it admits a pleasant elementary proof, which shows exactly how Zariski decompositions behave when a divisor moves in ample directions.

Sketch of Proof. Let $D = P + \sum_{i=1}^r a_i N_i$ be the Zariski decomposition of D. We show:

($*$) *There is a real number $\lambda_0 > 0$ and there are decreasing affine-linear functions f_i on $\mathbb{R}$ such that for $0 \leqslant \lambda \leqslant \lambda_0$ the Zariski decomposition of $D+\lambda A$ is given as*

$$D+\lambda A = \left(P + \lambda A + \sum_{i=1}^r (a_i - f_i(\lambda))N_i \right) + \sum_{i=1}^r f_i(\lambda) N_i \ ,$$

and such that λ_0 is a zero of one of the functions f_i.

From this statement our lemma follows by induction on r. Turning to the proof of ($*$), let us for real numbers $x_1, \ldots, x_r$ consider the divisor

$$P' =_{\text{def}} P + \lambda A + \sum_{i=1}^r (a_i - x_i) N_i \ .$$

The Zariski decomposition of $D+\lambda A$ is $P' + \sum_{i=1}^r x_i N_i$ if and only if the following conditions are satisfied:

$$0 \leqslant x_i \leqslant a_i \qquad \text{for } i = 1, \ldots, r, \tag{3}$$

$$P' \cdot N_i = 0 \qquad \text{for } i = 1, \ldots, r, \tag{4}$$

$$P' \text{ is nef.} \tag{5}$$

As $P + \lambda A$ is ample, condition (5) follows from (3) and (4). Condition (4) is equivalent to a system of linear equations in the indeterminates x_i, whose coefficient matrix is just the intersection matrix $S =_{\text{def}} (N_i \cdot N_j)$. As S is invertible, there is certainly no problem in solving for the x_i, but the whole point is whether the solutions x_i satisfy (3), i.e., whether $x_i \leqslant a_i$ for all i. Luckily, this is a consequence of the following statement:

($**$) *Let $S = (s_{ij})$ be a negative definite $r \times r$-matrix over the reals such that $s_{ij} \geqslant 0$ for $i \neq j$. Then all entries of the inverse matrix S^{-1} are $\leqslant 0$.*

Finally, the proof of $(**)$ is a nice exercise in linear algebra. (To be honest, the argument that we found is slightly tricky. In case of doubt see [**BKS**, Lemma 4.1].) $\square$

Note that the proof of the main lemma in fact shows exactly how the Zariski decomposition of $D + \lambda A$ varies as a function of λ: The coefficients of the negative part $N_{D+\lambda A}$ are decreasing affine-linear functions of λ, and as soon as one of these functions reaches zero, the component in question disappears from the negative part.

Let us conclude this section by briefly commenting on parts (ii) and (iii) of the theorem. For (iii) we show in [**BKS**] that for every rational divisor class D in the interior of a chamber the stable base locus $\mathrm{SB}(D)$ is given by the support of the negative part N_D of the Zariski decomposition, and that the stable base locus agrees with the stabilized base locus $\mathrm{B}_+(D)$. The essential point for (ii) is that the growth of $h^0(X, kD)$ is determined by the positive part in the Zariski decomposition of D.

3. Example: Two-point blow-up of the plane

Consider the blow-up $X \to \mathbb{P}^2$ of the projective plane in two points. On X there are exactly three irreducible curves with negative self-intersection: the exceptional divisors E_1 and E_2, and the proper transform E_3 of the line through the two blown-up points, whose class is $L - E_1 - E_2$. These three curves generate the closure of the big cone.

Figure 1 shows a cross-section of the (closure of the) big cone. The nef cone has five faces that contain big divisors, leading to five chambers:

- the chamber Σ_A of an ample class A (so that Σ_A is just the ample cone),
- chambers $\Sigma_{Q_1}, \Sigma_{Q_2}, \Sigma_{Q_3}$ associated to divisors Q_1, Q_2, Q_3 on the boundary of the nef cone as indicated in Figure 1,
- the chamber Σ_L.

Note that – in accordance with (2) – the dimension of a face and the number of the corresponding null curves add up to the dimension of the chamber, i.e., the Picard number of X:

divisor	dimension of face	null curves
A	3	0
Q_i	2	1
L	1	2

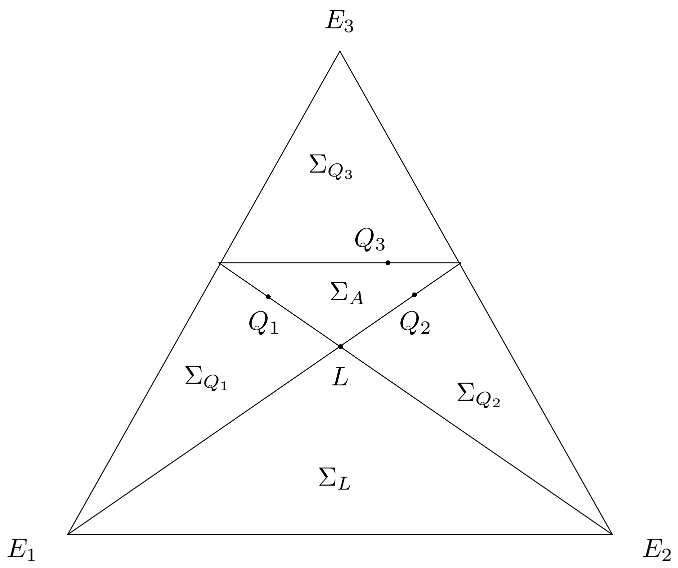

FIGURE 1. Two-point blow-up of the projective plane. The big cone consists of five chambers: Σ_A, Σ_{Q_1}, Σ_{Q_2}, Σ_{Q_3}, Σ_L.

More information about the general situation on del Pezzo surfaces, as well as on K3 surfaces, can be found in Sections 3.1 and 3.2 of [**BKS**].

References

[BKS] T. BAUER, A. KÜRONYA & T. SZEMBERG – Zariski chambers, volumes, and stable base loci, to appear.

[ELM+] L. EIN, R. LAZARSFELD, M. MUSTAŢĂ, M. NAKAMAYE & M. POPA – Asymptotic invariants of base loci, `arXiv AG 0308116`.

[KMM87] Y. KAWAMATA, K. MATSUDA & K. MATSUKI – Introduction to the minimal model problem, Algebraic geometry, Sendai, 1985, Adv. Stud. Pure Math., vol. 10, North-Holland, Amsterdam, 1987, p. 283–360.

[Laz] R. LAZARSFELD – Positivity in Algebraic Geometry, book in preparation.

[Nak00] M. NAKAMAYE – Stable base loci of linear series, *Math. Ann.* **318** (2000), no. 4, p. 837–847.

[Nak03] ———, Base loci of linear series are numerically determined, *Trans. Amer. Math. Soc.* **355** (2003), no. 2, p. 551–566 (electronic).

[Zar62] O. Zariski – The theorem of Riemann-Roch for high multiples of an effective divisor on an algebraic surface, *Ann. of Math. (2)* **76** (1962), p. 560–615.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 83–89
Universität Göttingen, 2004

MOTIVIC GALOIS GROUPS OF 1-MOTIVES: A SURVEY

C. Bertolin
D-MATH HG G 33.4, ETHZ-Zentrum, CH-8092 Zürich, Switzerland
E-mail : bertolin@math.ethz.ch

Abstract. We investigate the structure of the motivic Galois groups of 1-motives defined over a field of characteristic 0.

1. Introduction

In this note we review the main results of [**Ber03**] and [**Ber04**].

Let k be a field of characteristic 0 and let $\overline{k}$ be its algebraic closure. Let $\mathscr{T}$ be a Tannakian category over k. The tensor product of $\mathscr{T}$ allows us to define the notion of Hopf algebras in the category $\mathrm{Ind}\mathscr{T}$ of Ind-objects of $\mathscr{T}$. The category of affine group $\mathscr{T}$-schemes is the opposite of the category of Hopf algebras in $\mathrm{Ind}\mathscr{T}$.

The *fundamental group* $\pi(\mathscr{T})$ *of* $\mathscr{T}$ is the affine group $\mathscr{T}$-scheme $\mathrm{Sp}(\Lambda)$, whose Hopf algebra Λ is endowed for each object X of $\mathscr{T}$ with a morphism $X \longrightarrow \Lambda \otimes X$ functorial in X, and is universal for these properties. Those morphisms $\{X \longrightarrow \Lambda \otimes X\}_{X \in \mathscr{T}}$ define *an action of the fundamental group* $\pi(\mathscr{T})$ *on each object of* $\mathscr{T}$. For each fibre functor ω of $\mathscr{T}$ over a k-scheme

May 19th, 2004.

S, $\omega\pi(\mathscr{T})$ is the affine group S-scheme $\underline{\mathrm{Aut}}_S^{\otimes}(\omega)$ which represents the functor which associates to each S-scheme T, $u : T \longrightarrow S$, the group of automorphisms of $\otimes$-functors of the functor $u^*\omega$.

If $\mathscr{T}(k)$ is a Tannakian category generated by motives defined over k (in an appropriate category of mixed realizations), the fundamental group $\pi(\mathscr{T}(k))$ is called the *motivic Galois group* $\mathscr{G}_{\mathrm{mot}}(\mathscr{T}(k))$ *of* $\mathscr{T}(k)$ and for each embedding $\sigma : k \longrightarrow \mathbb{C}$, the fibre functor ω_σ "Hodge realization" furnishes the $\mathbb{Q}$-algebraic group

$$\omega_\sigma \mathscr{G}_{\mathrm{mot}}(\mathscr{T}) = \mathrm{Spec}\,\big(\omega_\sigma(\Lambda)\big) = \underline{Aut}_{\mathbb{Q}}^{\otimes}(\omega_\sigma)$$

which is the *Hodge realization of the motivic Galois group of* $\mathscr{T}(k)$.

Example 1.1.

1. The main theorem on neutral Tannakian categories says that the Tannakian category $\mathrm{V}ec(k)$ of finite dimensional k-vector spaces is equivalent to the category of finite-dimensional k-representations of $\mathrm{Spec}\,(k)$. In this case, affine group $\mathscr{T}$-schemes are affine group k-schemes and $\pi(\mathrm{V}ec(k))$ is $\mathrm{Spec}\,(k)$.
2. Let $\mathscr{T} = \mathrm{R}ep_k(G)$ be the Tannakian category of k-representations of an affine group k-scheme G. The affine group $\mathscr{T}$-schemes are affine k-schemes endowed with an action of G and the fundamental group $\pi(\mathscr{T})$ of $\mathscr{T}$ is G endowed with its action on itself by inner automorphisms (see [**Del89**] 6.3).
3. Let $\mathscr{T}_0(k)$ be the *Tannakian category of Artin motives over* k, i.e., the Tannakian sub-category of the Tannakian category of mixed realizations for absolute Hodge cycles (see [**Jan90**] I 2.1) generated by pure realizations of 0-dimensional varieties over k. The motivic Galois group $\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_0(k))$ of $\mathscr{T}_0(k)$ is the affine group $\mathbb{Q}$-scheme $\mathrm{Gal}(\overline{k}/k)$ endowed with its action on itself by inner automorphisms. Denote it by $\mathscr{GAL}(\overline{k}/k)$. In particular, for any fibre functor ω over $\mathrm{Spec}\,(\mathbb{Q})$ of $\mathscr{T}_0(k)$, the affine group scheme $\omega(\mathscr{GAL}(\overline{k}/k)) = \underline{Aut}_{\mathrm{Spec}\,(\mathbb{Q})}^{\otimes}(\omega)$ is canonically isomorphic to $\mathrm{Gal}(\overline{k}/k)$.
4. The motivic Galois group $\mathscr{G}_{\mathrm{mot}}(\mathbb{Z}(0))$ of the unit object $\mathbb{Z}(0)$ of $\mathscr{T}_0(k)$ is the affine group $\langle\mathbb{Z}(0)\rangle^{\otimes}$-scheme $\mathrm{Sp}(\mathbb{Z}(0))$. For each fibre functor "Hodge realization" ω_σ, we have $\omega_\sigma\big(\mathscr{G}_{\mathrm{mot}}(\mathbb{Z}(0))\big) := \mathrm{Spec}\big(\omega_\sigma(\mathbb{Z}(0))\big) = \mathrm{Spec}(\mathbb{Q})$, which is the Mumford-Tate group of $\mathrm{T}_\sigma(\mathbb{Z}(0))$.
5. Let $\langle\mathbb{Z}(1)\rangle^{\otimes}$ be the Tannakian category over $\mathbb{Q}$ defined by the k-torus $\mathbb{Z}(1)$. The motivic Galois group $\mathscr{G}_{\mathrm{mot}}(\mathbb{Z}(1))$ of the torus $\mathbb{Z}(1)$ is the affine group $\langle\mathbb{Z}(1)\rangle^{\otimes}$-scheme $\mathbb{G}_m$ defined by the $\mathbb{Q}$-scheme $\mathbb{G}_{m/\mathbb{Q}}$. For each fibre

functor "Hodge realization" ω_σ, we have that $\omega_\sigma\big(\mathbb{G}_m\big) = \mathbb{G}_{m/\mathbb{Q}}$, which is the Mumford-Tate group of $\mathrm{T}_\sigma(\mathbb{Z}(1))$.

6. If k is algebraically closed, the motivic Galois group of motives of CM-type over k is the Serre group (cf. [**Mil94**] 4.8).
7. The *Tannakian category* $\mathscr{T}_1(k)$ *of 1-motives over* k is the Tannakian sub-category of the Tannakian category of mixed realizations (for absolute Hodge cycles) generated by mixed realizations of 1-motives over k. Recall that a 1-motive $M = [X \xrightarrow{u} G]$ over k consists of
   - a group scheme X over k, which is locally for the étale topology, a constant group scheme defined by a finitely generated free $\mathbb{Z}$-module,
   - a semi-abelian variety G defined over k, i.e., an extention of an abelian variety A by a torus $Y(1)$, which cocharacter group Y,
   - a morphism $u : X \longrightarrow G$ of group schemes over k.

   1-motives are mixed motives of level $\leqslant 1$: the weight filtration W_* on M is $\mathrm{W}_i(M) = M$ for each $i \geqslant 0$, $\mathrm{W}_{-1}(M) = G$,$\mathrm{W}_{-2}(M) = Y(1)$, $\mathrm{W}_j(M) = 0$ for each $j \leqslant -3$. If $\mathrm{Gr}_n^{\mathrm{W}} = \mathrm{W}_n/\mathrm{W}_{n-1}$, we have the quotients $Gr_0^{\mathrm{W}}(M) = X, Gr_{-1}^{\mathrm{W}}(M) = A$ and $Gr_{-2}^{\mathrm{W}}(M) = Y(1)$. We will denote by $W_{-1}\mathscr{T}_1(k)$ (resp. $\mathrm{Gr}_0^W \mathscr{T}_1(k)$, ...) the Tannakian sub-category of $\mathscr{T}_1(k)$ generated by all $W_{-1}M$ (resp. $\mathrm{Gr}_0^W M$, ...) with M a 1-motive. With this notation we can easily compute the following motivic Galois groups
   - $\mathscr{G}_{\mathrm{mot}}(\mathrm{Gr}_0^W \mathscr{T}_1(k)) = \mathscr{G}\mathscr{A}\mathscr{L}(\overline{k}/k)$,
   - $\mathscr{G}_{\mathrm{mot}}(\mathrm{Gr}_{-2}^W \mathscr{T}_1(k)) = \mathscr{G}\mathscr{A}\mathscr{L}(\overline{k}/k) \times \mathbb{G}_m$.
   - $\mathscr{G}_{\mathrm{mot}}(\mathrm{Gr}_0^W \mathscr{T}_1(\overline{k})) = \mathscr{G}_{\mathrm{mot}}(\mathscr{T}_0(\overline{k})) = \mathrm{Sp}(\mathbb{Z}(0))$
   - $\mathscr{G}_{\mathrm{mot}}(\mathrm{Gr}_{-2}^W \mathscr{T}_1(\overline{k})) = \mathbb{G}_m$.

2. Motivic Galois theory

For each Tannakian sub-category $\mathscr{T}'$ of $\mathscr{T}$, let $H_{\mathscr{T}}(\mathscr{T}')$ be the kernel of the faithfully flat morphism of group $\mathscr{T}$-schemes $I : \pi(\mathscr{T}) \longrightarrow i\pi(\mathscr{T}')$ corresponding to the inclusion functor $i : \mathscr{T}' \longrightarrow \mathscr{T}$. In particular we have the short exact sequence of group $\pi(\mathscr{T})$-schemes

$$0 \longrightarrow H_{\mathscr{T}}(\mathscr{T}') \longrightarrow \pi(\mathscr{T}) \longrightarrow i\pi(\mathscr{T}') \longrightarrow 0.$$

In [**Del89**] 6.6, Deligne proves that the Tannakian category $\mathscr{T}'$ is equivalent, as tensor category, to the sub-category of $\mathscr{T}$ generated by those objects on which the action of $\pi(\mathscr{T})$ induces a trivial action of $H_{\mathscr{T}}(\mathscr{T}')$. In particular, this implies that the fundamental group $\pi(\mathscr{T}')$ of $\mathscr{T}'$ is isomorphic to the group $\mathscr{T}$-scheme $\pi(\mathscr{T})/H_{\mathscr{T}}(\mathscr{T}')$. The group $\mathscr{T}$-scheme $H_{\mathscr{T}}(\mathscr{T}')$ characterizes the Tannakian sub-category $\mathscr{T}'$. In fact we have a clear dictionary between Tannakian sub-categories of $\mathscr{T}$ and normal affine group sub-$\mathscr{T}$-schemes of the fundamental group $\pi(\mathscr{T})$ of $\mathscr{T}$:

Theorem 2.1. *There is bijection between the Tannakian sub-categories of $\mathscr{T}$ and the normal affine group sub-$\mathscr{T}$-schemes of $\pi(\mathscr{T})$, which associates*

- to each Tannakian sub-category $\mathscr{T}'$ of $\mathscr{T}$, the kernel $H_{\mathscr{T}}(\mathscr{T}')$ of the morphism of $\mathscr{T}$-schemes $I : \pi(\mathscr{T}) \longrightarrow i\pi(\mathscr{T}')$ corresponding to the inclusion $i : \mathscr{T}' \longrightarrow \mathscr{T}$;

- to each normal affine group sub-$\mathscr{T}$-scheme H of $\pi(\mathscr{T})$, the Tannakian sub-category $\mathscr{T}(H)$ of objects of $\mathscr{T}$ on which the action of $\pi(\mathscr{T})$ induces a trivial action of H.

3. The case of motives of level $\leqslant 1$

In order to study the category $\mathscr{T}_1(k)$ of motives of level $\leqslant 1$, in [**Ber04**] we have applied the above theorem to some sub-categories of $\mathscr{T}_1(k)$. The weight filtration W_* of 1-motives induces an increasing filtration W_* of 3 steps on the motivic Galois group $\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))$ which we describe through the action of $\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))$ on the generators of $\mathscr{T}_1(k)$: For each 1-motive M over k, we have that

- $W_0(\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))) = \mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))$
- $W_{-1}(\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))) = \{g \in \mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)) \mid (g-id)M \subseteq W_{-1}(M),$ $(g-id)W_{-1}(M) \subseteq W_{-2}(M), (g-id)W_{-2}(M) = 0\}$,
- $W_{-2}(\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))) = \{g \in \mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)) \mid (g-id)M \subseteq W_{-2}(M),$ $(g-id)W_{-1}(M) = 0\}$,
- $W_{-3}(\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))) = 0.$

According to the motivic analogue of [**Bry83**] §2.2, $\mathrm{Gr}_0^W(\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)))$ is a reductive group sub-$\mathscr{T}_1(k)$-scheme of $\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))$ and $W_{-1}(\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)))$ is the unipotent radical of $\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))$. Each of these 3 steps $\mathrm{W}_{-i}(\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)))$ $(i = 0, 1, 2)$ can be reconstructed as intersection of group sub-$\mathscr{T}_1(k)$-schemes of $\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))$ associated to Tannakian sub-categories of $\mathscr{T}_1(k)$ through the bijection 2.1:

Lemma 3.1.

1. $W_{-1}(\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))) = \cap_{i=-1,-2} H_{\mathscr{T}_1(k)}(\mathrm{Gr}_i^W \mathscr{T}_1(k))$,
2. $W_{-2}(\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))) = H_{\mathscr{T}_1(k)}(W_{-1}\mathscr{T}_1(k)) = H_{\mathscr{T}_1(k)}(\mathrm{W}_0/W_{-2}\mathscr{T}_1(k))$.

The explicit computation of these group sub-$\mathscr{T}_1(k)$-schemes involved in the above lemma will provide four exact short sequences of group sub-$\mathscr{T}_1(k)$-schemes of $\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k))$:

Theorem 3.2. *We have the following diagram of affine group $\mathscr{T}_1(k)$-schemes*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Res}_{\overline{k}/k}\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(\overline{k})) & \longrightarrow & \mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)) & \longrightarrow & \mathscr{G}\mathscr{A}\mathscr{L}(\overline{k}/k) & \longrightarrow & 0 \\
 & & \uparrow & & || & & \uparrow & & \\
0 & \longrightarrow & \mathrm{Res}_{\overline{k}/k}H_{\mathscr{T}_1(\overline{k})}(\langle\mathbb{Z}(1)\rangle^{\otimes}) & \longrightarrow & \mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)) & \longrightarrow & \mathscr{G}\mathscr{A}\mathscr{L}(\overline{k}/k)\times\mathbb{G}_m & \longrightarrow & 0 \\
 & & \uparrow & & || & & \uparrow & & \\
0 & \longrightarrow & W_{-1}\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)) & \longrightarrow & \mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)) & \longrightarrow & \mathscr{G}_{\mathrm{mot}}(\mathrm{Gr}_*^W\mathscr{T}_1(k)) & \longrightarrow & 0 \\
 & & \uparrow & & || & & \uparrow & & \\
0 & \longrightarrow & W_{-2}\mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)) & \longrightarrow & \mathscr{G}_{\mathrm{mot}}(\mathscr{T}_1(k)) & \longrightarrow & \mathscr{G}_{\mathrm{mot}}(W_{-1}\mathscr{T}_1(k)) & \longrightarrow & 0
\end{array}$$

where all horizontal short sequences are exact and where the vertical arrows on the left are inclusions and those on the right are surjections.

4. The case of a 1-motive

Let $M = [X \xrightarrow{u} G]$ be a 1-motive defined over k. The motivic Galois group $\mathscr{G}_{\mathrm{mot}}(M)$ of M is the fundamental group of the Tannakian sub-category $\langle M\rangle^{\otimes}$ of $\mathscr{T}_1(k)$ generated by M, i.e., the affine group $\langle M\rangle^{\otimes}$-scheme $\mathrm{Sp}(\Lambda)$, where Λ is the Hopf algebra of $\langle M\rangle^{\otimes}$ universal for the following property: for each object X of $\langle M\rangle^{\otimes}$, there is a morphism $\lambda_X : X^{\vee}\otimes X \longrightarrow \Lambda$ functorial in X. The morphisms $\{\lambda_X\}$, which can be rewritten in the form $X \longrightarrow X\otimes\Lambda$, define an action of the group $\mathscr{G}_{\mathrm{mot}}(M)$ on each object X of $\langle M\rangle^{\otimes}$, and in particular on itself. The main result of **[Ber03]** is that

Theorem 4.1. *The unipotent radical $W_{-1}(\mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(M))$ of the Lie algebra of $\mathscr{G}_{\mathrm{mot}}(M)$ is the semi-abelian variety defined by the adjoint action of the graded $\mathrm{Gr}_*^W(W_{-1}\mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(M))$ on itself.*

The idea of the proof is as follows: First recall that according to **[Del74]** (10.2.14), having M is equivalent to having the 7-uplet $(X, Y^{\vee}, A, A^*, v, v^*, \psi)$ where

- X and $Y^{\vee}$ are two group k-schemes, which are locally for the étale topology, constant group schemes defined by a finitely generated free $\mathbb{Z}$-module;
- A and A^* are two abelian varieties defined over k, dual to each other;
- $v : X \longrightarrow A$ and $v^* : Y^{\vee} \longrightarrow A^*$ are two morphisms of group k-schemes;
- ψ is a trivialization of the pull-back $(v, v^*)^*\mathscr{P}_A$ by (v, v^*) of the Poincaré biextension $\mathscr{P}_A$ of (A, A^*).

Observe that the 4-uplet $(X, Y^\vee, A, A^*)$ corresponds to the pure part of the 1-motive, i.e., it defines the pure motives underlying M, and the 3-uplet (v, v^*, ψ) represents the "mixity" of M.

Consider the motive $E = W_{-1}(\underline{\mathrm{End}}(\mathrm{Gr}_*^W M))$: it is a split 1-motive of weight -1 and -2 obtained from the endomorphisms of the graded $\mathrm{Gr}_*^W M$ of M. The composition of endomorphisms endowed E with a Lie algebra structure $(E, [\,,\,])$, whose crochet $[\,,\,]$ corresponds to a $\Sigma - X^\vee \otimes Y(1)$-torsor $\mathscr{B}$ living over $A \otimes X^\vee + A^* \otimes Y$. The action of E on the motive $\mathrm{Gr}_*^W(M)$ is described by a morphism

$$E \otimes \mathrm{Gr}_*^W(M) \longrightarrow \mathrm{Gr}_*^W(M)$$

which endowed the motive $\mathrm{Gr}_*^W(M)$ with a structure of $(E, [\,,\,])$-module.

Denote by $b = (b_1, b_2)$ the k-rational point $b = (b_1, b_2)$ of the abelian variety $A \otimes X^\vee + A^* \otimes Y$ defining the morphisms $v : X \longrightarrow A$ and $v^* : Y^\vee \longrightarrow A^*$. Let B be the smallest abelian sub-variety of $X^\vee \otimes A + A^* \otimes Y$ containing this point $b = (b_1, b_2)$. The restriction $i^*\mathscr{B}$ of the $\Sigma - X^\vee \otimes Y(1)$-torsor $\mathscr{B}$ by the inclusion $i : B \longrightarrow X^\vee \otimes A \times A^* \otimes Y$ is a $\Sigma - X^\vee \otimes Y(1)$-torsor over B. Denote by Z_1 the smallest $\mathrm{Gal}(\overline{k}/k)$-module of $X^\vee \otimes Y$ such that the torus $Z_1(1)$, that it defines, contains the image of the restriction $[\,,\,] : B \otimes B \longrightarrow X^\vee \otimes Y(1)$ of the Lie crochet to $B \otimes B$. The direct image $p_* i^*\mathscr{B}$ of the $\Sigma - X^\vee \otimes Y(1)$-torsor $i^*\mathscr{B}$ by the projection $p : X^\vee \otimes Y(1) \longrightarrow (X^\vee \otimes Y/Z_1)(1)$ is a trivial $\Sigma - (X^\vee \otimes Y/Z_1)(1)$-torsor over B. We denote by $\pi : p_* i^*\mathscr{B} \longrightarrow (X^\vee \otimes Y/Z_1)(1)$ the canonical projection. The morphism $u : X \longrightarrow G$ defines a point $\widetilde{b}$ in the fibre of $\mathscr{B}$ over b. We denote again by $\widetilde{b}$ the points of $i^*\mathscr{B}$ and of $p_* i^*\mathscr{B}$ over the point b of B. Let Z be the smallest sub-$\mathrm{Gal}(\overline{k}/k)$-module of $X^\vee \otimes Y$, containing Z_1 and such that the sub-torus $(Z/Z_1)(1)$ of $(X^\vee \otimes Y/Z_1)(1)$ contains $\pi(\widetilde{b})$. If we put $Z_2 = Z/Z_1$, we have that $Z(1) = Z_1(1) \times Z_2(1)$.

With these notations, the unipotent radical $W_{-1}(\mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(M))$ of the Lie algebra of $\mathscr{G}_{\mathrm{mot}}(M)$ is the extension of the abelian variety B by the torus $Z(1)$ defined by the adjoint action of $(B + Z(1), [\,,\,])$ on itself. Since in the construction of B and $Z(1)$ are involved only the parameters v, v^* and u, *the computation of the unipotent radical* $W_{-1}(\mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(M))$ *of the Lie algebra of* $\mathscr{G}_{\mathrm{mot}}(M)$ *depends only on the 3-uplet* (v, v^*, ψ), *i.e., on the "mixity" of the 1-motive* M.

Example 4.2.

1. Let M be the split 1-motive $\mathbb{Z} \oplus A \oplus \mathbb{G}_m$. In this case all is trivial: $W_{-1}(\mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(M)) = B = Z(1) = 0$.

2. Let $M = [\mathbb{Z} \xrightarrow{u} \mathscr{E}]$ be a 1-motive over k defined by $u(1) = P$ with P a non-torsion k-rational point of the elliptic curve $\mathscr{E}$. We have that the torus $Z(1)$ is trivial and the unipotent radical $W_{-1}(\mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(M))$ is the elliptic curve $B = \mathscr{E}$.
3. Let $M = [\mathbb{Z} \xrightarrow{u} \mathbb{G}_m^3 \times A]$ be a 1-motive over k defined by $u(1) = (q_1, q_2, 1, 0)$ with q_1, q_2 two elements of $\mathbb{G}_m(k) - \mu_\infty$ multiplicatively independents (μ_∞ is the group of roots of the unity in $\overline{k}$). In this example the abelian variety B is trivial and the unipotent radical $W_{-1}(\mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(M))$ is the torus $Z(1) = \mathbb{G}_m^2$.

With the above notations we have also that

Proposition 4.3. *The derived group of the unipotent radical $W_{-1}(\mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(M))$ of the Lie algebra of $\mathscr{G}_{\mathrm{mot}}(M)$ is the torus $Z_1(1)$.*

Proposition 4.4.

$$\dim \mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(M) = \dim B + \dim Z(1) + \dim \mathrm{Lie}\,\mathscr{G}_{\mathrm{mot}}(\mathrm{Gr}_*^W M).$$

References

[Ber03] C. Bertolin – Le radical unipotent du groupe de Galois motivique d'un 1-motif, *Math. Ann.* **327** (2003), no. 3, p. 585–607.

[Ber04] ———, Motivic Galois theory for motives of level $\leqslant 1$, 2004, submited.

[Bry83] J.-L. Brylinski – 1-motifs et formes automorphes (théorie arithmétique des domaines de Siegel), 1983, Publ. Math. Univ. Paris VII, 15.

[Del74] P. Deligne – Théorie de Hodge. III, *Inst. Hautes Études Sci. Publ. Math.* (1974), no. 44, p. 5–77.

[Del89] P. Deligne – Le groupe fondamental de la droite projective moins trois points, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, p. 79–297.

[Jan90] U. Jannsen – *Mixed motives and algebraic K-theory*, Lecture Notes in Mathematics, vol. 1400, Springer-Verlag, Berlin, 1990, With appendices by S. Bloch and C. Schoen.

[Mil94] J. S. Milne – Motives over finite fields, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, p. 401–459.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 91–94
Universität Göttingen, 2004

ALGEBRAIC INDEPENDENCE IN $K_0(\mathrm{Var}_k)$

N. Naumann
NWF-I Mathematik, Universität Regensburg, 93040 Regensburg, Germany
E-mail : niko.naumann@mathematik.uni-regensburg.de

Abstract. We give sufficient cohomological criteria for the classes of given varieties over a field k to be algebraically independent in the Grothendieck ring of varieties over k and construct some examples.

In this note we review the main results of [**Nau**]. Let k be a field. The Grothendieck ring of varieties over k, denoted $K_0(\mathrm{Var}_k)$, was defined by A. Grothendieck in [**Gro01**]:

The abelian group $K_0(\mathrm{Var}_k)$ is generated by the isomorphism classes $[X]$ of separated k-schemes of finite type X/k subject to the relations

$$[X] = [Y] + [X - Y]$$

for $Y \subset X$ a closed subscheme. Multiplication is given by

$$[X_1] \cdot [X_2] := [X_1 \times_k X_2];$$

it makes $K_0(\mathrm{Var}_k)$ a commutative ring with unit $[\mathrm{Spec}(k)]$.

May 25th, 2004.

By its very definition $K_0(\mathrm{Var}_k)$ is the value group of the universal Euler-Poincaré characteristic with compact support for varieties over k and is thus a fundamental invariant of the algebraic geometry over k. The most outstanding result on the structure of $K_0(\mathrm{Var}_k)$ for k of characteristic zero is a presentation of the ring $K_0(\mathrm{Var}_k)$ in terms of generators and relations anticipated by E. Looijenga and proved by his student F. Bittner [**Bit04**]. B. Poonen showed that for k of characteristic zero a linear combination of the classes of suitable abelian varieties is a zero divisor in $K_0(\mathrm{Var}_k)$ [**Poo02**] and J. Kollár has computed the subring of $K_0(\mathrm{Var}_k)$ generated by the classes of conics for suitable base fields k [**Kol**]. A deep problem pertaining to the structure of $K_0(\mathrm{Var}_k)$ is the rationality of motivic zeta-functions posed by M. Kapranov [**Kap**] on which there has been recent progress due to M. Larsen and V. Lunts [**LL**]. This problem is intimately related to the finite-dimensionality of motives, c.f. [**And**] for an exposition. Furthermore, the ring $K_0(\mathrm{Var}_k)$ plays a central rôle in the theory of motivic integration, c.f. [**Loo02**]. The talk was dedicated to the following problem about the structure of $K_0(\mathrm{Var}_k)$.

Given varieties X_i/k, when are their classes $[X_i] \in K_0(\mathrm{Var}_k)$ algebraically independent?

We give a number of sufficient cohomological conditions for this to be the case and construct some examples. Our main results are also valid in positive characteristic where there is no known theorem about the structure of $K_0(\mathrm{Var}_k)$.
Denote by $\mathrm{Rep}_{G_k}\mathbb{Q}_l$ the category of l-adic Galois representations and by W the weight-filtration. The aforementioned sufficient cohomological conditions are the following.

Theorem 1. *Let k be finitely generated and let $X_1, \ldots, X_n/k$ be separated and of finite type and assume that $\mathrm{Gr}_0^W(X_i) \in \mathbb{Z} \subseteq K_0(\mathrm{Rep}_{G_k}\mathbb{Q}_l)$ for all i and that the $\mathrm{Gr}_1^W(X_i)$ are algebraically independent in $K_0(\mathrm{Rep}_{G_k}\mathbb{Q}_l)$. Then the $[X_i]$ are algebraically independent in $K_0(\mathrm{Var}_k)$.*

Corollary 2. Let k be finitely generated and let $X_1, \ldots, X_n/k$ be proper and smooth. Then, if the $[H_c^1(\overline{X}_i)]$ are algebraically independent in $K_0(\mathrm{Rep}_{G_k}\mathbb{Q}_l)$, so are the $[X_i]$ in $K_0(\mathrm{Var}_k)$.

The study of algebraic (in)dependence of Galois-representations such as the $[H_c^1(\overline{X}_i)]$ in the ring of virtual Galois-representaions $K_0(\mathrm{Rep}_{G_k}\mathbb{Q}_l)$ is reduced, using Tannaka-theory, to studying algebraic (in)dependence in $K_0(\underline{\mathrm{Rep}}_{\mathbb{Q}_l} G)$ for suitable (not neccessarily connected) reductive algebraic groups $G/\mathbb{Q}_l$. It is fun to note the complications arising from this possible non-connectedness: Fix $G/\mathbb{Q}_l$ such that G/G^0 is constant and G^0 is split reductive. The structure of both $K_0(\underline{\mathrm{Rep}}_{\mathbb{Q}_l} G/G^0)$ and $K_0(\underline{\mathrm{Rep}}_{\mathbb{Q}_l} G^0)$ is well understood, but it seems difficult to determine the structure of $K_0(\underline{\mathrm{Rep}}_{\mathbb{Q}_l} G)$ itself (except in trivial special cases, e.g. $G \simeq G^0 \times G/G^0$). Here is an example illustrating the significance of this for our main problem of algebraic independence in the Grothendick ring of varieties.

Theorem 3. *Let k be a finite field and let $E_1, E_2/k$ be non-isogeneous ordinary elliptic curves. Let E_2'/k be the quadratic twist of E_2, and consider the abelian surfaces $A_1 := E_1 \times E_2$ and $A_2 := E_1 \times E_2'$ over k and the associated Galois representations $V_i := H_c^1(\overline{A_i}) \in \mathrm{Rep}_{G_k}\mathbb{Q}_l$. Let $k \subset L$ be the unique quadratic extension of k inside $\overline{k}$. Then:*

i) $\mathrm{Res}_{G_L}^{G_k}(V_1) \simeq \mathrm{Res}_{G_L}^{G_k}(V_2)$.

ii) *The classes $[V_1]$ and $[V_2]$ are algebraically independent in $K_0(\mathrm{Rep}_{G_k}\mathbb{Q}_l)$.*

In particular, the classes $[A_1]$ and $[A_2]$ are algebraically independent in $K_0(\mathrm{Var}_k)$.

Remark 4. The representations V_1 and V_2 are algebraically independent but not geometrically algebraically independent. In fact, after restriction to the subgroup of index two of G_k their classes become algebraically dependent and in fact equal. We also see that $x := [A_1] - [A_2] \in K_0(\mathrm{Var}_k)$ generates a polynomial ring over $\mathbb{Z}$ inside $K_0(\mathrm{Var}_k)$ even though x lies in the kernel of the base change homomorphism $K_0(\mathrm{Var}_k) \longrightarrow K_0(\mathrm{Var}_L)$. This shows that $K_0(\mathrm{Var}_k)$ encodes fine arithmetic invariants of varieties over k.

One can produce many algebraically independent varieties.

Theorem 5. *Let k be a finite field. Then there is a sequence of proper, smooth and geometrically connected curves X_i/k ($i \geq 1$) such that the classes $[X_i] \in K_0(\mathrm{Var}_k)$ are algebraically independent.*

These curves are constructed explicitely in [**Nau**] and the representation theory above reduces the proof of this theorem to a (lengthy) argument about Weil-numbers.

There is a similar result over number fields.

Theorem 6. *Let k be a number field and $\{E_i\}_{i\in I}$ a set of elliptic curves over k such that the E_i are pairwise non-isogeneous and satisfy $\mathrm{End}_{\overline{k}}(E_i) = \mathbb{Z}$. Then the classes $[E_i] \in K_0(\mathrm{Var}_k)$ are algebraically independent.*

The proof of this uses the Mumford-Tate conjecture for a finite product of elliptic curves as in the theorem (known by work of J-P. Serre and K. Ribet) and J-P. Serre's theory of Frobenius tori.

References

[And] Y. André – Motifs de dimension finie, Séminaire Bourbaki, 56ème année, 2003-2004, no 929.

[Bit04] F. Bittner – The universal Euler characteristic for varieties of characteristic zero, *Compos. Math.* **140** (2004), no. 4, p. 1011–1032.

[Gro01] A. Grothendieck – Letter to J.-P. Serre (dated 16.8.1964), 2001, in Correspondance Grothendieck-Serre, P. Colmez, J-P. Serre (eds.), Documents Mathématiques, Soc. Math. France.

[Kap] M. Kapranov – The elliptic curve in the S-duality theory and Eisenstein-series for Kac–Moody groups, `math.AG/0001005`.

[Kol] J. Kollár – Conics in the Grothendieck ring, `math.AG/0305302`.

[LL] M. Larsen & V. Lunts – Rationality criteria for motivic zeta-functions, `math.AG/0212158`.

[Loo02] E. Looijenga – Motivic measures, *Astérisque* (2002), no. 276, p. 267–297, Séminaire Bourbaki, Vol. 1999/2000.

[Nau] N. Naumann – Algebraic independence in the Grothendieck ring of varieties, `math.AG/0403075`.

[Poo02] B. Poonen – The Grothendieck ring of varieties is not a domain, *Math. Res. Lett.* **9** (2002), no. 4, p. 493–497.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 95–102
Universität Göttingen, 2004

TWO DESCENT FROM FERMAT TO NOW

Sir P. Swinnerton-Dyer
DPMMS, Centre for Mathematical Sciences, University of Cambridge,
Wilberforce Road, Cambridge, CB3 0WB, UK
E-mail : H.P.F.Swinnerton-Dyer@dpmms.cam.ac.uk

Abstract. I discuss descent on elliptic curves.

I shall describe the process of 2-descent on elliptic curves defined over $\mathbf{Q}$ which have the form

$$\Gamma : y^2 = (x - c_1)(x - c_2)(x - c_3)$$

— that is, elliptic curves all of whose 2-division points are rational. The statements of the theory over an arbitrary algebraic number field are not very different, except that the analogues of certain explicit results relating to the prime 2 are not known. We can clearly take the c_i to be integers. Let $\mathscr{B}$, the set of bad primes, be any finite set of primes containing 2, ∞ and all the odd primes dividing $(c_1-c_2)(c_1-c_3)(c_2-c_3)$; thus $\mathscr{B}$ contains the primes of bad reduction for Γ. If $\mathscr{B}$ also contains some primes of good reduction, that is harmless.

The basic version of 2-descent, which goes back to Fermat, is as follows. To any rational point (x, y) on Γ there correspond rational m_1, m_2, m_3 with

June 2, 2004.

$m_1m_2m_3 = m^2 \neq 0$ such that the three equations

$$(1) \qquad m_iy_i^2 = x - c_i \quad \text{for} \quad i = 1, 2, 3$$

are simultaneously soluble. We can multiply the m_i by non-zero squares, so that for example we can require them to be square-free integers; indeed one should really think of them as elements of $\mathbf{Q}^*/\mathbf{Q}^{*2}$, with a suitable interpretation of the equations which involve them. Denote by $\mathscr{C}(\mathbf{m})$ the curve given by the three equations (1), where $\mathbf{m} = (m_1, m_2, m_3)$. Looking for solutions of Γ is the same as looking for quadruples x, y_1, y_2, y_3 which satisfy (1) for some $\mathbf{m}$. For this purpose we need only consider the finitely many $\mathbf{m}$ for which the m_i are units at all primes outside $\mathscr{B}$; for if any m_i is divisible to an odd power by some prime p not in $\mathscr{B}$ then Γ is already insoluble in $\mathbf{Q}_p$.

One question of interest is the effect of *twisting* on the arithmetic properties of the curve Γ. If b is a nonzero rational, the twist of Γ by b is defined to be the curve

$$\Gamma_b : y^2 = (x - bc_1)(x - bc_2)(x - bc_3),$$

where we can regard b as an element of $\mathbf{Q}^*/\mathbf{Q}^{*2}$. The curve Γ_b is often written in the alternative form

$$v^2 = b(u - c_1)(u - c_2)(u - c_3).$$

The analogue of (1) for Γ_b is

$$m_iy_i^2 = x - bc_i \quad \text{for} \quad i = 1, 2, 3;$$

we shall call the curve given by these three equations $\mathscr{C}_b(\mathbf{m})$. It is often natural to compare $\mathscr{C}(\mathbf{m})$ and $\mathscr{C}_b(\mathbf{m})$ for the same $\mathbf{m}$.

There is a natural law of composition on $\Gamma(\mathbf{Q})$, the set of rational points on Γ, which makes $\Gamma(\mathbf{Q})$ into a commutative group whose identity element is the point at infinity; this is called the Mordell–Weil group. Provided one treats the m_i as elements of $\mathbf{Q}^*/\mathbf{Q}^{*2}$, the triples $\mathbf{m}$ form an abelian group under componentwise multiplication:

$$\mathbf{m}' \times \mathbf{m}'' \mapsto \mathbf{m}'\mathbf{m}'' = (m_1'm_1'', m_2'm_2'', m_3'm_3'').$$

The natural set-theoretic map from $\Gamma(\mathbf{Q})$ to this group is a homomorphism, whose kernel is $2\Gamma(\mathbf{Q})$. The $\mathbf{m}$ for which $\mathscr{C}(\mathbf{m})$ is everywhere locally soluble form a finite subgroup, called the 2-*Selmer group*. This is computable, and it contains the group of those $\mathbf{m}$ for which $\mathscr{C}(\mathbf{m})$ is actually soluble in $\mathbf{Q}$. This smaller group is isomorphic to $\Gamma(\mathbf{Q})/2\Gamma(\mathbf{Q})$. The quotient of the 2-Selmer group by this smaller group is ${}_2Ш$, the group of those elements of the *Tate–Safarevic group* which are killed by 2.

The process of going from the curve Γ to the set of curves $\mathscr{C}(\mathbf{m})$, or the finite subset which is the 2-Selmer group, is called a 2-*descent*, or sometimes a *first descent*, and the curves $\mathscr{C}(\mathbf{m})$ themselves are called 2-*coverings*. The reason for this terminology is that there is a commutative diagram

$$\begin{array}{ccc} \Gamma & \longrightarrow & \Gamma \\ \| & \nearrow & \\ \mathscr{C}(\mathbf{m}) & & \end{array} \tag{2}$$

in which the left hand map is biregular (but defined over $\mathbf{C}$ rather than $\mathbf{Q}$), the top map is multiplication by 2 and the diagonal map is given by $y = my_1y_2y_3$. A 2-covering which is everywhere locally soluble, and therefore in the 2-Selmer group, can also be written in the form

$$\eta^2 = f(\xi) \quad \text{where} \quad f(\xi) = a\xi^4 + b\xi^3 + c\xi^2 + d\xi + e,$$

and many 2-coverings do arise in this way; but a 2-covering which is not in the 2-Selmer group cannot always be put into this form.

We now put this process into more modern language. In what follows, italic capitals will always denote vector spaces over $\mathbf{F}_2$, the finite field of two elements, and each of p and q will be either a finite prime or ∞. Write

$$Y_p = \mathbf{Q}_p^*/\mathbf{Q}_p^{*2}, \quad Y_{\mathscr{B}} = \oplus_{p\in\mathscr{B}} Y_p.$$

Let V_p denote the vector space of all triples (μ_1, μ_2, μ_3) with each μ_i in Y_p and $\mu_1\mu_2\mu_3 = 1$; and write $V_{\mathscr{B}} = \oplus_{p\in\mathscr{B}} V_p$. This is the best way to introduce these spaces, because it preserves symmetry; but the prevailing custom in the literature is to define V_p as $Y_p \times Y_p$, which is isomorphic to the V_p defined above but not in a canonical way. Next, write $X_{\mathscr{B}} = \mathfrak{o}_{\mathscr{B}}^*/\mathfrak{o}_{\mathscr{B}}^{*2}$ where $\mathfrak{o}_{\mathscr{B}}^*$ is the group of nonzero rationals which are units outside $\mathscr{B}$; and let $U_{\mathscr{B}}$ be the image in $V_{\mathscr{B}}$ of the group of triples (m_1, m_2, m_3) such that the m_i are in $X_{\mathscr{B}}$ and $m_1m_2m_3 = 1$. It is known that the map $X_{\mathscr{B}} \to Y_{\mathscr{B}}$ is an embedding and $\dim U_{\mathscr{B}} = \frac{1}{2}\dim V_{\mathscr{B}}$; both these depend on the requirement that $\mathscr{B}$ contains 2 and ∞. If (x, y) is a point of Γ defined over $\mathbf{Q}_p$ other than a 2-division point, then the triple $(x - c_1, x - c_2, x - c_3)$ has a natural image in V_p. We can supply the images of the 2-division points by continuity; for example the image of $(c_1, 0)$ is

$$((c_1 - c_2)(c_1 - c_3), c_1 - c_2, c_1 - c_3), \tag{3}$$

and the image of the point at infinity is the trivial triple $(1, 1, 1)$, which is also the product of the three triples like (3). Thus we obtain a map $\Gamma(\mathbf{Q}_p) \to V_p$. This map, which is called the *Kummer map*, is a homomorphism. We denote its image by W_p; clearly W_p is the set of those triples $\mathbf{m}$ for which (1) is soluble in $\mathbf{Q}_p$. The 2-Selmer group of Γ can now be identified with $U_{\mathscr{B}} \cap W_{\mathscr{B}}$ where $W_{\mathscr{B}} = \oplus_{p\in\mathscr{B}} W_p$; for as was noted above, (1) is soluble at every prime outside $\mathscr{B}$ if and only if the elements of $\mathbf{m}$ are in $X_{\mathscr{B}}$.

Over the years, many people must have noticed that

$$\dim W_{\mathscr{B}} = \dim U_{\mathscr{B}} = \tfrac{1}{2} \dim V_{\mathscr{B}}. \tag{4}$$

The next major step, which explains and may well have been inspired by this relation, was taken by Tate. He introduced the bilinear form e_p on $V_p \times V_p$, defined by

$$e_p(\mathbf{m}', \mathbf{m}'') = (m_1', m_1'')_p (m_2', m_2'')_p (m_3', m_3'')_p.$$

Here $(u, v)_p$ is the Hilbert symbol with values in $\{\pm 1\}$, defined by

$$(u, v)_p = \begin{cases} 1 & \text{if } ux^2 + vy^2 = 1 \text{ is soluble in } \mathbf{Q}_p, \\ -1 & \text{otherwise.} \end{cases}$$

The Hilbert symbol is symmetric and multiplicative in each argument:

$$(u, v)_p = (v, u)_p \quad \text{and} \quad (u_1 u_2, v)_p = (u_1, v)_p (u_2, v)_p.$$

Effectively it is a replacement for the quadratic residue symbol, with the advantage that it treats the primes 2 and ∞ in just the same way as any other prime. Its other key property is the Hilbert product formula

$$\prod\nolimits_p (u, v)_p = 1,$$

where the product is taken over all p including ∞; the left hand side is meaningful because $(u, v)_p = 1$ whenever p is an odd prime at which u and v are units.

The bilinear form e_p is non-degenerate and alternating on $V_p \times V_p$; we use it to define $e_{\mathscr{B}} = \prod_{p \in \mathscr{B}} e_p$, which is a non-degenerate alternating bilinear form on $V_{\mathscr{B}} \times V_{\mathscr{B}}$. (For a bilinear form with values in $\{\pm 1\}$, "symmetric" and "skew-symmetric" are the same and they each mean that $e(\mathbf{m}', \mathbf{m}'') = e(\mathbf{m}'', \mathbf{m}')$; "alternating" means that also $e(\mathbf{m}, \mathbf{m}) = 1$.) It is known from class field theory that $U_{\mathscr{B}}$ is a maximal isotropic subspace of $V_{\mathscr{B}}$. Tate showed that W_p is a maximal isotropic subspace of V_p, and therefore $W_{\mathscr{B}}$ is a maximal isotropic subspace of $V_{\mathscr{B}}$. This explains (4) and shows that the 2-Selmer group of Γ can be identified with both the left and the right kernel of the restriction of $e_{\mathscr{B}}$ to $U_{\mathscr{B}} \times W_{\mathscr{B}}$.

For both aesthetic and practical reasons, one would like to show that this restriction is symmetric or skew-symmetric. But to make such a statement meaningful we need an isomorphism between $U_{\mathscr{B}}$ and $W_{\mathscr{B}}$; and though they have the same structure as vector spaces it is not obvious (nor apparently even true) that there is a natural isomorphism between them. The way round this obstacle requires the construction inside each V_p of a maximal isotropic subspace K_p such that $V_{\mathscr{B}} = U_{\mathscr{B}} \oplus K_{\mathscr{B}}$ where $K_{\mathscr{B}} = \oplus_{p \in \mathscr{B}} K_p$. Assuming that such spaces K_p can be constructed, let $t_{\mathscr{B}}:\ V_{\mathscr{B}} \to U_{\mathscr{B}}$ be the projection along $K_{\mathscr{B}}$ and write

$$U'_{\mathscr{B}} = U_{\mathscr{B}} \cap (W_{\mathscr{B}} + K_{\mathscr{B}}), \quad W'_{\mathscr{B}} = W_{\mathscr{B}}/(W_{\mathscr{B}} \cap K_{\mathscr{B}}) = \bigoplus\nolimits_{p\in\mathscr{B}} W'_p$$

where $W'_p = W_p/(W_p \cap K_p)$. The map $t_{\mathscr{B}}$ induces an isomorphism

$$\tau_{\mathscr{B}}:\ W'_{\mathscr{B}} \to U'_{\mathscr{B}},$$

and the bilinear function $e_{\mathscr{B}}$ induces a bilinear function

$$e'_{\mathscr{B}}:\ U'_{\mathscr{B}} \times W'_{\mathscr{B}} \to \{\pm 1\}.$$

The bilinear functions $U'_{\mathscr{B}} \times U'_{\mathscr{B}} \to \{\pm 1\}$ and $W'_{\mathscr{B}} \times W'_{\mathscr{B}} \to \{\pm 1\}$ defined by

$$(5) \quad \theta^{\flat}_{\mathscr{B}} : u'_1 \times u'_2 \mapsto e'_{\mathscr{B}}(u'_1, \tau^{-1}_{\mathscr{B}}(u'_2)) \quad \text{and} \quad \theta^{\sharp}_{\mathscr{B}} : w'_1 \times w'_2 \mapsto e'_{\mathscr{B}}(\tau_{\mathscr{B}} w'_1, w'_2)$$

can be shown to be symmetric. (For this and most subsequent assertions we appeal to Cassels's Principle: all vector space lemmas which are true are trivial.) Here the images of $w'_1 \times w'_2$ under the second map and of $\tau_{\mathscr{B}} w'_1 \times \tau_{\mathscr{B}} w'_2$ under the first map are the same. The 2-Selmer group of Γ is isomorphic to both the left and the right kernel of $e'_{\mathscr{B}}$, and hence also to the kernels of the two maps (5).

There is considerable freedom in choosing the K_p, and this raises three obvious questions:

- Is there a canonical choice of the K_p?
- How small can we make U' and W'?
- Can we ensure that the functions (5) are not merely symmetric but alternating?

The motive for ensuring that the functions (5) are alternating is that then the ranks of these functions are even; thus their coranks, which are equal to the dimension of the 2-Selmer group, are congruent mod 2 to $\dim U'_{\mathscr{B}}$ and $\dim W'_{\mathscr{B}}$.

The answer to the first question appears to be negative, though there is little freedom in the optimum choice of the K_p — particularly if one wishes to obtain not merely Lemma 1 but Theorem 2. Since $U'_{\mathscr{B}} \supset U_{\mathscr{B}} \cap W_{\mathscr{B}}$, the best possible answer to the second question would be that we can achieve $U'_{\mathscr{B}} = U_{\mathscr{B}} \cap W_{\mathscr{B}}$; we do this by satisfying the stronger requirement

$$(6) \qquad W_{\mathscr{B}} = (U_{\mathscr{B}} \cap W_{\mathscr{B}}) \oplus (K_{\mathscr{B}} \cap W_{\mathscr{B}}).$$

For suppose that (6) holds; then $W_{\mathscr{B}} + K_{\mathscr{B}} = (U_{\mathscr{B}} \cap W_{\mathscr{B}}) + K_{\mathscr{B}}$ and it follows immediately that

$$(7) \qquad U'_{\mathscr{B}} = U_{\mathscr{B}} \cap (W_{\mathscr{B}} + K_{\mathscr{B}}) = U_{\mathscr{B}} \cap W_{\mathscr{B}}.$$

The motivation for (6) is that we want to make $W_{\mathscr{B}} \cap K_{\mathscr{B}}$ as large as possible — that is, to choose $K_{\mathscr{B}}$ so that as much of it as possible is contained in $W_{\mathscr{B}}$. But because $K_{\mathscr{B}}$ must be complementary to $U_{\mathscr{B}}$, only the part of $W_{\mathscr{B}}$ which is complementary to $W_{\mathscr{B}} \cap U_{\mathscr{B}}$ is available for this purpose.

Since the 2-Selmer group $U_{\mathscr{B}} \cap W_{\mathscr{B}}$ is identified with the left and right kernels of each of the functions (5), if (7) holds then these functions are trivial and therefore alternating. The formal statement of this is as follows.

Lemma 1. *We can choose maximal isotropic subspaces $K_p \subset V_p$ for each p in $\mathscr{B}$ so that $V_{\mathscr{B}} = U_{\mathscr{B}} \oplus K_{\mathscr{B}}$. We can further ensure that*

$$W_{\mathscr{B}} = (U_{\mathscr{B}} \cap W_{\mathscr{B}}) \oplus (K_{\mathscr{B}} \cap W_{\mathscr{B}}),$$

which implies $U'_{\mathscr{B}} = U_{\mathscr{B}} \cap W_{\mathscr{B}}$. If so, the functions $\theta^\flat_{\mathscr{B}}$ and $\theta^\sharp_{\mathscr{B}}$ defined in (5) *are trivial.*

Unfortunately the other properties of the K_p chosen in this way are not at all obvious. Hence it is advantageous to consider other recipes for choosing the K_p, for which (6) does not hold but we can still prove that the functions (5) are alternating.

For this purpose we write $\mathscr{B}$ as the disjoint union of $\mathscr{B}'$ and $\mathscr{B}''$, where we shall always suppose that 2 and ∞ are both in $\mathscr{B}'$. For any odd prime p we denote by T_p the subset of V_p consisting of those triples (μ_1, μ_2, μ_3) with $\mu_1\mu_2\mu_3 = 1$ for which each μ_i is in $\mathfrak{o}_p^*/\mathfrak{o}_p^{*2}$ — that is, each μ_i is the image of a p-adic unit. The main point of the following theorem is that for p in $\mathscr{B}''$ it enables us to replace the complicated inductive definition of K_p used in the proof of Lemma 1 by the much simpler choice $K_p = T_p$. How one chooses $\mathscr{B}''$ depends on the particular application which one has in mind.

Theorem 2. *Let $\mathscr{B}$ be the disjoint union of $\mathscr{B}' \supset \{2, \infty\}$ and $\mathscr{B}''$. We can construct maximal isotropic subspaces $K_p \subset V_p$ such that $V_{\mathscr{B}} = U_{\mathscr{B}} \oplus K_{\mathscr{B}}$,*

$$W_{\mathscr{B}'} = (U_{\mathscr{B}'} \cap W_{\mathscr{B}'}) \oplus (K_{\mathscr{B}'} \cap W_{\mathscr{B}'}) \tag{8}$$

and $K_p = T_p$ for all p in $\mathscr{B}''$; and (8) *implies that $U'_{\mathscr{B}'} = U_{\mathscr{B}'} \cap W_{\mathscr{B}'}$. Moreover*

$$U'_{\mathscr{B}} = \jmath_* U'_{\mathscr{B}'} \oplus \tau_{\mathscr{B}} W'_{\mathscr{B}''} = \jmath_* U'_{\mathscr{B}'} \oplus \left(\oplus_{p \in \mathscr{B}''} \tau_B W'_p\right), \tag{9}$$

and the restriction of $\theta^\flat_{\mathscr{B}}$ to $\jmath_* U'_{\mathscr{B}'} \times \jmath_* U'_{\mathscr{B}'}$ is trivial.

If $\mathscr{B}'$ contains all the odd primes p such that the $v_p(c_i - c_j)$ are not all congruent mod 2, *then we can choose the K_p for p in $\mathscr{B}'$ so that also $\theta^\flat_{\mathscr{B}}$ is alternating on $U'_{\mathscr{B}}$.*

The appearance of $\jmath_* U'_{\mathscr{B}'}$ in and just after (9) calls for some explanation. Let u be any element of $U'_{\mathscr{B}'}$; then u is in $U_{\mathscr{B}}$. Moreover, for p in $\mathscr{B}''$ the image of u in V_p is in $T_p = K_p$ and therefore in $K_p + W_p$; hence u is in $U'_{\mathscr{B}}$. In this way we define a map $U'_{\mathscr{B}'} \to U'_{\mathscr{B}}$ which is clearly an injection and which we denote, with some abuse of notation, by $\jmath_*$.

Lemma 1 is the special case of Theorem 2 in which $\mathscr{B}' = \mathscr{B}$ and $\mathscr{B}''$ is empty. But the proof of Lemma 1 is a necessary step (and indeed the most substantial step) in the proof of Theorem 2. One major application of Theorem 2 is to twisted curves Γ_b, where we can take b to be an integer. Let $\mathscr{S}$ denote the set of bad primes for Γ itself — that is, $2, \infty$ and the odd primes dividing $(c_1 - c_2)(c_1 - c_3)(c_2 - c_3)$; and let $\mathscr{B} \supset \mathscr{S}$ be the set of bad primes for Γ_b, which therefore contains all the odd primes dividing b. For simplicity we assume that b is a unit at every prime of $\mathscr{S}$. (We can always arrange this by treating Γ_b as the twist of Γ_c by b/c, where c is the largest divisor of b which is a unit outside $\mathscr{S}$.) To describe the effect of twisting, we denote by d_b the dimension of the 2-Selmer group of Γ_b regarded as a vector space over $\mathbf{F}_2$; and we write $d = d_1$ for the dimension of the 2-Selmer group of Γ itself. It is now possible to prove results about $d_b - d$, the change in the dimension of the 2-Selmer group as one goes from Γ to Γ_b. There is reason to expect that statements about the parities of d and d_b will be simpler and much easier to prove than statements about their actual values. The two major facts known about d_b are Lemma 3 and Theorem 5; Lemma 3 is an easy consequence of the last sentence of Theorem 2, and Theorem 5 is an easy consequence of Lemma 4 below.

Lemma 3. *If b is in $\mathfrak{o}_p^*$ for every $p \in \mathscr{S}$, then* $d_b \equiv \dim(U_{\mathscr{S}} \cap W_{\mathscr{S}}) \bmod 2$ *where $W_{\mathscr{S}} = \oplus_{p \in \mathscr{S}} W_p$ and the W_p must be defined with respect to Γ_b and not with respect to Γ. Thus* $d_b \bmod 2$ *only depends on the classes of b in the k_p^*/k_p^{*2} for p in $\mathscr{S}$.*

To prove Lemma 4 we need to take $\mathscr{B}' = \mathscr{S} \setminus \{p\}$; thus the last sentence of Theorem 2 is not applicable though the rest of that theorem is.

Lemma 4. *Let p be an odd prime in $\mathscr{S}$ such that*

$$v_p(c_1 - c_2) > 0, \quad v_p(c_1 - c_3) = v_p(c_2 - c_3) = 0.$$

Let b in k^* be such that b is in k_q^{*2} for all q in $\mathscr{S}$ other than p and b is a quadratic non-residue at p. Then d and d_b have opposite parities.

It is not hard to state and prove the analogue of Lemma 4 for the case $p = \infty$, though the proof falls outside the machinery described in this seminar. The combination of this result and Lemma 4 yields Theorem 5. (The analogue of Lemma 4 for $p = 2$ can be confidently asserted, on the basis of a large amount of numerical evidence, and the proof of it probably requires no new ideas. But even the statement involves so extensive a separation of cases that it is unlikely soon to appear in print.)

Theorem 5. *Let b', b'' in k^* be such that b'/b'' is a unit at all $p \in \mathscr{S}$ and $b'/b'' \equiv 1 \bmod 8$. Let $\mathscr{S}^*$ be the set of $p \in \mathscr{S}$ for which b'/b'' is not in k_p^{*2}. Let $\mathscr{S}^{**}$ consist of the finite odd p in $\mathscr{S}^*$ for which the $v_p(c_i - c_j)$ are not all equal and the smallest two of them are even, together with ∞ if $b'/b'' < 0$. Then*

$$d_{b'} - d_{b''} \equiv \#\mathscr{S}^{**} \bmod 2.$$

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 103–109
Universität Göttingen, 2004

RATIONAL POINTS ON FIBERED SURFACES

Sir P. Swinnerton-Dyer
DPMMS, Centre for Mathematical Sciences, University of Cambridge,
Wilberforce Road, Cambridge, CB3 0WB, UK
E-mail : H.P.F.Swinnerton-Dyer@dpmms.cam.ac.uk

Abstract. I discuss the arithmetic of rational surfaces.

There are still important unsolved problems about rational points on curves, but it does not appear that they can be attacked by elementary methods. On the other hand, the geometric classification of varieties, which must be a prerequisite for studying the associated number theory, is only reasonably complete in dimensions 1 and 2. This suggests that one should concentrate on the study of rational points on surfaces. The simplest sort of surfaces are those described by the geometers as rational surfaces — that is, those which are birationally equivalent to a plane after an extension of the ground field. If we do not allow a field extension, rational surfaces fall into two families:

– Pencils of conics, given by an equation of the form

$$a_0(U,V)X_0^2 + a_1(U,V)X_1^2 + a_2(U,V)X_2^2 = 0 \tag{1}$$

where the $a_i(U,V)$ are homogeneous polynomials of the same degree.

June 2, 2004.

– Del Pezzo surfaces of degree d, where $0 \leqslant d \leqslant 9$, obtained over $\mathbf{C}$ by blowing up $9-d$ points of $\mathbf{P}^2$ in general position. Their theory becomes more complicated the smaller d is. For $d \geqslant 5$ the major number-theoretic problems have been solved, and for $d=4$ considerable progress has recently been made; but the surfaces with $d \leqslant 3$ still pose major problems. Del Pezzo surfaces of degree 4 are the non-singular intersections of two quadrics in $\mathbf{P}^4$. Those of degree 3 are the non-singular cubic surfaces, which have an enormous but largely irrelevent literature. In contrast, those of degree $d < 3$ are not ones which the number-theorist would naturally think of as priority targets.

In both these cases the main conjecture, due to Colliot-Thélène and Sansuc, is that the only obstruction to either the Hasse principle or weak approximation is the Brauer–Manin obstruction. But to work on these problems one hardly needs to know what the Brauer–Manin obstruction is. In my view, the right way to study the obstruction to the Hasse principle (for example) for any particular family of rational varieties is to find a sufficient condition for solubility everywhere locally to imply solubility globally, and only then to see how this condition compares with the Brauer–Manin condition.

For the methods which I am about to describe, it is necessary to introduce Schinzel's Hypothesis. Suppose we are given finitely many polynomials $F_1(X), \dots, F_n(X)$ in $\mathbf{Z}[X]$ with positive leading coefficients; is there an arbitrarily large positive integer x such that all the $F_i(x)$ are primes? There are two obvious obstructions to this: one or more of the $F_i(X)$ may factorize in $\mathbf{Z}[X]$, or there may be a prime p such that for any value of $x \mod p$ at least one of the $F_i(x)$ is divisible by p. (For an example of the second obstruction, consider X and X^2+2 with $p=3$.) The second obstruction can only happen without the first if $p \leqslant \sum \deg F_i$, so the second obstruction is easy to test for. Schinzel's Hypothesis is that these are the only obstructions: in other words, if neither of them happens we can choose an arbitrarily large x so that every $F_i(x)$ is a prime. There seems to be no hope of proving this in the foreseeable future; but to prove results subject to Schinzel's Hypothesis should at least shed light on the underlying number theory. Moreover, there is an associated result which can be proved. With the same set-up, choose an $N \geqslant \sum \deg F_i$; then there is an algebraic integer ξ with $[\mathbf{Q}(\xi) : \mathbf{Q}] = N$ such that each $(F_i(\xi))$ is a prime ideal in $\mathbf{Q}(\xi)$. Using this, if we can deduce from Schinzel's Hypothesis sufficient conditions for the Hasse Principle to hold for a certain family of varieties, then we can prove the corresponding result for the existence of rational 0-cycles of degree 1 without any analogous hypothesis. This is particularly valuable for Del Pezzo surfaces of degree 4, for which Coray has shown that the existence of rational 0-cycles of degree 1 implies the existence of rational points. The corresponding question for cubic surfaces is still open, and for pencils of conics such an assertion is definitely false.

For applications one needs to modify Schinzel's Hypothesis in three ways:

- **(i) :** One needs to be able to impose local conditions on x at each prime in a given finite set $\mathscr{B}$; but in compensation one then only requires that the $F_i(x)$ are each equal to the product of powers of primes in $\mathscr{B}$ and one prime outside $\mathscr{B}$.
- **(ii) :** One needs to work over an arbitrary algebraic number field.
- **(iii) :** It suffices to know the corresponding result for homogeneous polynomials $G_i(Y, Z)$ in two variables.

The hypothesis modified as in (i) and (ii) can easily be deduced from Schinzel's original hypothesis. To vary it as in (iii) can only make it more likely to be true, and perhaps also easier to prove; indeed Heath-Brown has shown that $Y^3 + 2Z^3$ takes infinitely many prime values.

We also need to define the Legendre function $L(\mathscr{B}; F, G; \alpha, \beta)$. Let $\mathscr{B}$ be a finite set of places of $\mathbf{Q}$ and let α, β be integers coprime outside $\mathscr{B}$. Let $F(U, V), G(U, V)$ be homogeneous coprime polynomials in $\mathbf{Z}[U, V]$, and assume that $\mathscr{B}$ contains ∞ and all the primes p at which the reduction of $FG \mod p$ has a repeated factor. Then we write

$$L(\mathscr{B}; F, G; \alpha, \beta) = \prod\nolimits_p (F(\alpha, \beta), G(\alpha, \beta))_p$$

where the outer bracket is the Hilbert symbol, the product is taken over all primes p outside $\mathscr{B}$ which divide $G(\alpha, \beta)$, and the function is defined for those $\alpha \times \beta$ in $\mathbf{Z} \times \mathbf{Z}$ such that α, β are coprime outside $\mathscr{B}$ and $F(\alpha, \beta), G(\alpha, \beta)$ are both nonzero. For any p in the product, $F(\alpha, \beta)$ must be a p-adic unit; so L can also be regarded as the value of a certain quadratic residue symbol.

Lemma 1. *Suppose that* $(\deg F)(\deg G)$ *is even; then* $L(\alpha, \beta)$ *is continuous in the topology induced by* $\mathscr{B}$.

This at first sight surprising result is easy to prove by induction, using the facts that

$$L(F, G) = L(F - GH, G)$$

for any homogeneous polynomial H in $\mathbf{Z}[U, V]$ of appropriate degree, and

$$L(F, G)L(G, F) = \prod\nolimits_{v \in \mathscr{B}} (F(\alpha, \beta), G(\alpha, \beta))_v$$

by the Hilbert product formula. Here the right hand side is continuous in the topology induced by $\mathscr{B}$. We shall describe the condition $L(\mathscr{B}; F, G; \alpha, \beta) = 1$ as the Legendre condition associated with F and G.

Now consider the pencil of conics (1), where without loss of generality we can assume that the $a_i(U,V)$ are in $\mathbf{Z}[U,V]$. By an obvious transformation we can make the $a_i(U,V)$ square-free and coprime in pairs; the $\deg a_i$ will no longer be all equal, but they will all still have the same parity. Let $c(U,V)$ be an irreducible factor of one of the $a_i(U,V)$, where to fix ideas we assume $i=0$. If (1) is soluble at $U=\alpha, V=\beta$ then

$$(-a_1(\alpha,\beta)a_2(\alpha,\beta), c(\alpha,\beta))_p = 1$$

for all primes p which divide $c(\alpha,\beta)$ but not $-a_1(\alpha,\beta)a_2(\alpha,\beta)$. With an obvious definition of $\mathscr{B}$, this implies the Legendre condition

$$L(\mathscr{B}; -a_1a_2, c; \alpha, \beta) = 1.$$

Hence the set of all Legendre conditions associated with (1) is a necessary condition for solubility. What is remarkable is that, subject to Schinzel's Hypothesis, this set of conditions is also sufficient.

Theorem 2. *Assume Schinzel's Hypothesis. Let $\mathscr{A}$ be the subset of $\mathbf{Z}\times\mathbf{Z}$ on which all the Legendre conditions are well-defined and hold, and on which* (1) *is locally soluble at each place in $\mathscr{B}$. Then the points (α,β) in $\mathbf{P}^1$ at which this conic is soluble form a dense subset of $\mathscr{A}$ in the topology induced by $\mathscr{B}$.*

For the proof, we apply Schinzel's Hypothesis to the irreducible factors c of $a_0a_1a_2$. If p is the prime associated with the c in the argument above, then

$$(-a_1(\alpha,\beta)a_2(\alpha,\beta), c(\alpha,\beta))_p = L(\mathscr{B}; -a_1a_2, c; \alpha, \beta) = 1. \tag{2}$$

For the values of α,β chosen, necessary and sufficient conditions for the solubility of (1) are just the conditions (2) together with solubility at the places in $\mathscr{B}$, and these we have now ensured.

For pencils of conics, the Brauer–Manin conditions were determined by Iskovskii. In view of the conjecture of Colliot-Thélène and Sansuc, it is no surprise that they can be shown to be equivalent to the Legendre conditions.

Can we apply these ideas to Del Pezzo surfaces? The first difficulty is that although a Del Pezzo surface contains an infinity of curves of genus 0 whenever it contains rational points, one cannot write down any such curves until one knows some rational points. This appears to block any approach to the Hasse Principle, though it does not necessarily block an approach to weak approximation. (In this seminar I use weak approximation on a variety V to mean that if $V(\mathbf{Q})$ is not empty then $V(\mathbf{Q})$ is dense in $\prod V(\mathbf{Q}_v)$ where v runs through all the places of $\mathbf{Q}$.) Indeed, one can use this methodology to give a proof of weak approximation on Del Pezzo surfaces of degree 4, quite different from the one which has been given by Salberger and Skorobogatov.

Can we do better by using pencils of curves of genus 1? There are many such curves on Del Pezzo surfaces, but a new obstacle appears: crucial to the previous argument was the fact that the Hasse Principle holds for conics, but it notoriously does not hold for curves of genus 1. However, there is a way round this provided we assume that the Tate–Shafarevich group of an elliptic curve defined over an algebraic number field is finite. This is still unproved, but is a much more respectable thing to assume than Schinzel's Hypothesis. We actually only need this for elliptic curves with finite Mordell–Weil group, and this may be easier to prove than the general case.

Lemma 3. *Let* Γ*, defined over* $\mathbf{Q}$*, be an everywhere locally soluble* 2*-covering of an elliptic curve* E*. If half the elements of the* 2*-Selmer group come from the* 2*-division points of* E*, then* $\Gamma(\mathbf{Q})$ *is not empty.*

For if $\Gamma(\mathbf{Q})$ were empty it would induce an element of the Tate–Shafarevich group, and this would be the only element of order 2 in this group. But since by hypothesis the Tate–Shafarevich group is finite, this contradicts the properties of the Cassels skew-symmetric bilinear form.

In view of Lemma 3, if we are looking for rational points on a pencil of 2-coverings, we should try to carry out a 2-descent on the curves of the underlying pencil of Jacobians. To do this in a uniform manner appears to require that the 2-division points are defined without a field extension; so we need the Jacobian to have the form

$$Y^2 = (X - a_1(U,V))(X - a_2(U,V))(X - a_3(U,V)) \tag{3}$$

where the $a_i(U,V)$ are polynomials of the same even degree. Now the tactic is to impose on the values of U and V local conditions at finitely many carefully chosen primes, all of which will be adjoined to the set of bad primes. We then use Schinzel's Hypothesis to make the value of each irreducible factor of an $a_i(U,V)$ equal to the product of one further prime with powers of bad primes. The 2-descent on such a curve can be carried out explicitly, and the conditions at the bad primes can be chosen so that the 2-Selmer group has order 8 and Γ, the 2-covering that interests us, is everywhere locally soluble. There may be an obstruction to carrying out this process, and the absence of such an obstruction is a sufficient condition for the Hasse Principle to hold for the original pencil. In contrast with what happened for Theorem 2, it is not obvious that this condition is also necessary; but it turns out that it is closely related to the algebraic part of the Brauer–Manin obstruction. The condition must also imply that the transcendental part of the Brauer–Manin obstruction is trivial, but we know too little about the latter to be able to say any more than this.

This method was first devised to obtain solubility conditions for diagonal Del Pezzo surfaces of degree 4, given by equations of the form

$$\sum_{i=0}^{4} a_i X_i^2 = 0, \quad \sum_{i=0}^{4} b_i X_i^2 = 0;$$

for such a surface every nonsingular hyperplane section has a Jacobian of the form (3). My student Bender and I have extended this to arbitrary Del Pezzo surfaces of degree 4, and removed the appeal to Schinzel's Hypothesis. The process involves

- going over to an extension k of degree 5, in order to diagonalize one variable;
- obtaining a pencil of curves of genus 1 whose Jacobians have the form

$$Y^2 = (X - c_0(U, V))(X^2 - c_1(U, V)),$$

  and carrying out a 2-descent on such a pencil;
- using the substitute for Schinzel's Hypothesis which yields a point on the Del Pezzo surface defined over a field k_1 with $[k_1 : k]$ odd;
- Using Coray's argument first to obtain a point defined over k on the surface, and thence to obtain a point defined over $\mathbf{Q}$.

The sufficient conditions for solubility which we obtain are ugly, though they are probably not much stronger than the Brauer–Manin conditions. However Olivier Wittenberg, building on work of Colliot-Thélène, is currently engaged in translating these conditions into sensible form. When he has done so, it will be possible to describe the number-theoretic problems of Del Pezzo surfaces of degree 4 as largely solved.

In general, it does not seem possible to tackle Del Pezzo surfaces of degree 3 without radically new ideas. The most interesting results currently known relate to diagonal cubic surfaces

$$a_0 X_0^3 + a_1 X_1^3 + a_2 X_2^3 + a_3 X_3^3 = 0$$

defined over an algebraic number field k. One writes this as a pair of cubic curves

$$a_0 X_0^3 + a_1 X_1^3 = cY^3, \quad a_2 X_2^3 + a_3 X_3^3 = -cZ^3$$

with a parameter c; and one has to choose a value of c for which (using the analogue of Lemma 3) one can show that both these equations are soluble. The need to control two Selmer groups simultaneously, and the need to take into account the interaction between k and $k(\sqrt{-3})$ because of the presence of complex multiplication on the underlying Jacobians, make the argument much more complicated. The good news is that one does not need Schinzel's

Hypothesis, because the expression whose value must eventually be made equal to the product of an unspecified prime and powers of bad primes is just c; so we can appeal to Dirichlet's theorem on primes in arithmetic progressions. The bad news is that, as well as the Brauer–Manin-like conditions which one expects, we have to impose the condition that c does not contain $\sqrt{-3}$. This condition is certainly an artefact of the method, and has nothing to do with the actual problem; it comes from the fact that we do not know how to take account of complex multiplication in Lemma 3 and its analogue.

So far we have considered only rational surfaces; but there are plenty of surfaces which are fibred by pencils of curves of genus 1 but are not rational. A good example is the family of K3 surfaces

$$V : a_0X_0^4 + a_1X_1^4 + a_2X_2^4 + a_3X_3^4 = 0 \tag{4}$$

over $\mathbf{Q}$, subject to the condition

$$a_0a_1a_2a_3 \text{ is a square.} \tag{5}$$

There is an obvious map from V to the quadric

$$W : a_0Y_0^2 + a_1Y_1^2 + a_2Y_2^2 + a_3Y_3^3 = 0,$$

and the condition (5) implies that each of the two pencils of lines on W is defined over $\mathbf{Q}$. These pencils pull back to two pencils of curves of genus 1 on V, and it turns out that the Jacobians of the curves in either pencil have the form (3). We can therefore apply the machinery above, and obtain sufficient conditions for the Hasse Principle to hold on surfaces (4) which satisfy the condition (5). These conditions are not much stronger than the algebraic Brauer–Manin conditions, and may well actually be equivalent to the full Brauer-Manin conditions; as usual, we do not yet know enough about the transcendental Brauer–Manin conditions to be able to plug this gap.

My student Bright has produced a comprehensive table of the algebraic Brauer groups for surfaces (4), whether or not they satisfy (5). If we drop the condition (5) there is no known way of addressing the solubility of (4); but numerical experimentation suggests that a substantial proportion of those surfaces which satisfy the algebraic Brauer–Manin conditions are nevertheless not soluble in $\mathbf{Q}$. In other words, it is the ability to fibre (or perhaps merely the fact that the Nèron-Severi group is not too small) that ensures that the Brauer–Manin conditions are close to being sufficient as well as necessary for the Hasse Principle to hold.

One particularly interesting surface (4) which does not satisfy (5) is

$$X_0^4 + 2X_1^4 = X_2^4 + 4X_3^4.$$

It has two obvious rational points; I conjecture that it has no others.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 111–117
Universität Göttingen, 2004

ON THE MOD p REDUCTIONS OF AN ELLIPTIC CURVE

W. Duke
UCLA Mathematics Department Box 951555, Los Angeles, CA 90095-1555, U.S.A. • *E-mail :* duke@math.ucla.edu

Abstract. A fixed elliptic curve defined over the rational numbers gives rise, through reduction modulo primes of good reduction, to infinitely many elliptic curves (the *reductions*) defined over finite fields. In this note I discuss the Tate–Shafarevich groups of these reductions considered as being defined over their function fields. Assuming the Generalized Riemann Hypothesis when the curve has no complex multiplications, it is shown that these groups are trivial for a positive proportion of primes, provided the elliptic curve has an irrational point of order two. This is joint work with A.C. Cojocaru.

1. Background

Let E be an elliptic curve defined over $\mathbb{Q}$ and of conductor N. For a prime $p \nmid N$, the reduction of E modulo p is an elliptic curve E_p defined over the finite field k with p elements. There is great interest in the behavior of these

---

June 8th, 2004.
Supported in part by NSF grant DMS-0355564.

reductions as p varies. The most basic questions concern the size of $E_p(k)$, the finite abelian group of k rational points of E_p. Define a_p as usual by

$$|E_p(k)| = p + 1 - a_p \tag{1}$$

where, for a set S, we write $|S|$ or $\#S$ for its cardinality. The Riemann hypothesis for E_p, proven by Hasse, states that

$$|a_p| \leqslant 2\sqrt{p}$$

Still unproven are the Sato–Tate conjecture in the case of a curve without complex multiplication (CM) counting primes p where $a_p/\sqrt{p}$ lies in a given subinterval of $(-2, 2)$ and the Lang–Trotter conjecture counting primes p with a given value of a_p.

Also of interest is the structure of $E_p(k)$ as an abelian group, in particular its cyclicity. It is easy to see that $E_p(k)$ may be cyclic only if E has an irrational point of order two, that is, a point of order two not in $E(\mathbb{Q})$. Assuming this and the Generalized Riemann Hypothesis (GRH) for Dedekind zeta functions, Serre [**Ser85**] (see [**Mur83**] for the proof) showed that $E_p(k)$ is cyclic for a positive proportion of primes:

$$\#\{p \leqslant x : p \nmid N \text{ and } E_p(k) \text{ is cyclic}\} \sim c_E\, \pi(x)$$

as $x \to \infty$, where c_E is a positive constant depending only on E and $\pi(x)$ is the number of primes $\leqslant x$. Without assuming GRH, R. Murty [**Mur83**] showed this holds for CM elliptic curves. In general, R. Gupta and R. Murty [**GM90**] showed that there are infinitely many, in fact $\gg x/\log^2 \mathrm{x}$, such primes.

2. Definition of the local Tate–Shafarevich group

A new aspect emerges when one considers the mod p reduction E_p as being defined over its function field. If $K = K(E_p)$ is the function field of E_p/k, then E_p naturally defines a constant elliptic curve over K. The resulting elliptic curve has a number of nice features; the group $E_p(k)$ may be identified with the torsion points $E_p(K)_{\mathrm{tor}}$ of the finitely generated Mordell–Weil group $E_p(K)$ and the k-endomorphisms of E_p may be identified with the Mordell–Weil lattice $E_p(K)/E_p(K)_{\mathrm{tor}}$. In view of these features, one is naturally led to consider the Tate–Shafarevich group of E_p/K. Recall that a principal homogeneous space over E/F, where for now E is any elliptic curve over an arbitrary field F, is a smooth curve C/F together with a simply transitive algebraic group action of E on C defined over F. The isomorphism classes of principal homogeneous spaces for E/F form an abelian group, the Weil–Châtelet group $WC(E/F)$, whose identity class consists of those homogeneous spaces whose curves have an

F-rational point. The group operation comes from a natural identification of $WC(E/F)$ with the cohomology group $H^1(G,E)$, where $G = \mathrm{Gal}(\bar{\mathrm{F}}/\mathrm{F})$ with $\bar{F}$ the separable closure of F. Since K is a global field we may define the Tate–Shafarevich group

$$Ш_p = Ш(E_p/K)$$

to be those elements of $WC(E_p/K)$ which, for all primes ν of K, are in the kernel of the canonical map

$$WC(E_p/K) \to WC(E_p/K_\nu),$$

where K_ν is the completion of K at the prime ν. We call $Ш_p$ the Tate–Shafarevich group of E_p and are interested in its behavior as p varies over primes of good reduction for E.

3. Results

It is known that $|Ш_p|$ is finite, hence a square. In fact, there is an explicit formula for it coming from the Hasse–Weil L-function for E_p/K, since the Birch/Swinnerton-Dyer conjecture is a theorem in this case due to Milne [**Mil68**]. This formula allows us to detect when $|Ш_p|$ is divisible by a fixed square. More precisely, there is a Galois extension J_n of $\mathbb{Q}$ so that n^2 divides $|Ш_p|$ if and only if p splits in J_n and $p \nmid n$. This field is closely related to the modular curve $X_0(n)$. An application of the Chebotarev theorem yields the following result which implies, in particular, that $|Ш_p|$ may be arbitrarily large.

Theorem 3.1. *The group $Ш_p$ contains elements of any fixed prime order ℓ for a positive proportion of primes p.*

Our principal interest is to count primes for which $Ш_p$ is trivial. This happens if and only if for any principal homogeneous space over E_p/K the curve C has a point over K if it does over K_ν for all ν. Our main result shows when this local-global principle holds for many reductions.

Theorem 3.2. *Suppose that E has an irrational point of order two. If E does not have CM assume GRH. Then $Ш_p$ is trivial for a positive proportion of primes p.*

Actually, we give an asymptotic formula for the number of such primes with a power savings in the remainder term, at least under GRH. Furthermore, since $E_p(k)$ can be shown to be cyclic whenever $Ш_p$ is trivial, the first assumption of Theorem 3.2 is necessary and its conclusion may be viewed as a refinement of the existence aspect of Serre's result about cyclicity of $E_p(k)$.

4. Outline of the proof

I give here only a very brief sketch of the proof of Theorem 3.2. For details see [**CD04**]. In the CM case it is proven using the Chebotarev Theorem for a fixed finite extension and the proof does not require GRH. In the non-CM case, Theorem 3.2 is proven using a variant of Serre's sieve method. The strong uniformity needed in the non-CM case is obtained by assuming GRH. A serious new difficulty is caused by the fact that the field J_n does not contain the full nth cyclotomic field. Thus the Brun–Titchmarsh theorem, which is used in Serre's argument to estimate the terms with large n, must be replaced. This is possible and essential use is made of the fact that $|\,Ш_p|$ *is a square*. This allows us to employ a second sieving device, a "square sieve", to estimate the remainder term.

We obtain an asymptotic formula for

$$\pi_{\mathrm{sha}}(x) = \#\left\{p \leqslant x : p \nmid N \text{ and } Ш_p \text{ is trivial}\right\}.$$

Here we assume GRH for the Dedekind zeta functions of the division fields of E. We are able to use directly the inclusion-exclusion principle in its most basic form beginning with the expansion of the delta symbol for $m \in \mathbb{Z}^+$:

$$\sum_{n|m} \mu(n) = \delta(m) = \begin{cases} 1, & \text{if } m = 1 \\ 0, & \text{if } m \neq 1, \end{cases}$$

where $\mu(\cdot\,)$ denotes the Möbius function. This yields immediately the starting formula

$$\pi_{\mathrm{sha}}(x) = \sum_{\substack{p \leqslant x \\ p \nmid N}} \delta(b_p) = \sum_{\substack{p \leqslant x \\ p \nmid N}} \sum_{n|b_p} \mu(n),$$

where we have written $|\,Ш_p| = b_p^2$. It is shown that $b_p \leqslant 2\sqrt{p/3}$ and so in this summation $n < 2\sqrt{x}$. After rearrangement, the sum can thus be written

$$\pi_{\mathrm{sha}}(x) = \sum_{n < 2\sqrt{x}} \mu(n) \#\{p \leqslant x : p \nmid N \text{ and } n | b_p\}.$$

This gives

$$\pi_{\mathrm{sha}}(x) = \sum_{n \leqslant y} \mu(n)\pi_n(x) + \sum_{y<n<2\sqrt{x}} \mu(n)\pi_n(x),$$

where $\pi_n(x)$ is defined by

$$\pi_n(x) = \#\{p \leqslant x : p \nmid N \text{ and } n^2 \text{ divides } |\text{Ш}_p|\}$$

and $y = y(x)$ is a parameter chosen later.

We show that for a certain Galois extension J_n of $\mathbb{Q}$ that n^2 divides $|\text{Ш}_p|$ if and only if p splits in J_n and $p \nmid n$. Then we can apply a conditional Chebotarev Theorem as in [**Ser81**] to the first term giving

$$\pi_{\mathrm{sha}}(x) = \left(\sum_{n \leqslant y} \mu(n)c_n\right)\pi(x) + \sum_{y<n<2\sqrt{x}} \mu(n)\pi_n(x) + O(yx^{1/2}\log xyN), \tag{2}$$

where $c_n = [J_n : \mathbb{Q}]^{-1}$. In this way we are led to seek an asymptotic evaluation in y of

$$C(y) = \sum_{n \leqslant y} \mu(n)c_n$$

and an upper bound in x and y for

$$D(x, y) = \sum_{y<n<2\sqrt{x}} \pi_n(x).$$

We establish the following two results about $C(y)$ and $D(x, y)$. Define

$$c = \left(\sum_{n \mid B} \mu(n)c_n\right) \prod_{\substack{\ell \nmid B \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right),$$

where $c_n = [J_n : \mathbb{Q}]^{-1}$ and $B = 2A_E N$, where A_E is the product of the exceptional primes for E.

Proposition 4.1. *Suppose that E does not have CM. Then*

$$C(y) = \sum_{n \leqslant y} \mu(n)c_n = c + O(y^{-2}B^2)$$

with an absolute implied constant. Furthermore, $c > 0$ if and only if $c_2 \neq 1$. In fact,

$$c \geqslant (1 - c_2) \prod_{\substack{\ell \nmid B \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell(\ell^2-1)}\right).$$

The second result is more difficult and uses a sieve that detects squares in conjunction with a certain estimate for a character sum involving a_p from (1) that is itself conditional upon GRH.

Proposition 4.2. *Suppose that E does not have CM and let $\varepsilon > 0$ be given. Assume GRH. Then, for $1 \leqslant y \leqslant 2\sqrt{x}$ and $x \geqslant 1$, we have the uniform bound*

$$D(x,y) \ll y^{-2} x^{\frac{35}{18}+\varepsilon},$$

where the implied constant depends only on ε and E.

Theorem 3.2 in the non-CM case is a consequence the a more precise result, which follows from the previous two propositions and (2) after taking $y = x^{\frac{13}{27}}$.

Proposition 4.3. *Suppose E does not have CM and assume GRH. Then, for any $\varepsilon > 0$ we have*

$$\#\{p \leqslant x : p \nmid N \text{ and } Ш_p \text{ is trivial}\} = c\,\pi(x) + O(x^{\frac{53}{54}+\varepsilon}),$$

where the implied constant depends only on ε and E. Here c is positive if and only if E has an irrational point of order two and is given by

$$c = \left(\sum_{n|B} \mu(n) c_n\right) \prod_{\ell \nmid B} \left(1 - \frac{1}{\ell(\ell^2-1)}\right),$$

where $c_n = [J_n : \mathbb{Q}]^{-1}$ and $B = 2A_E N$, with A_E being the product of the exceptional primes for E.

5. Some problems

One open problem is to prove unconditionally the existence of infinitely many primes p for which $Ш_p$ is trivial for any non-CM curve E with an irrational point of order 2. The method used in the cyclicity problem [**GM90**], which relies on sieve arguments for primes in arithmetic progressions, is not directly applicable since the field J_n does not contain the nth cyclotomic field.

It follows from [**Mil68**] that, under the same conditions as in Theorem 2, the Brauer groups of the reductions of $E \times E$ are trivial for a positive proportion of primes. It seems interesting to consider similar questions for the reductions of more general elliptic surfaces.

References

[CD04] A. C. Cojocaru & W. Duke – Reductions of an elliptic curve and their Tate–Shafarevich groups, *Math. Annalen* **329** (2004), p. 513–534.

[GM90] R. Gupta & M. R. Murty – Cyclicity and generation of points mod p on elliptic curves, *Invent. Math.* **101** (1990), no. 1, p. 225–235.

[Mil68] J. S. Milne – The Tate-Šafarevič group of a constant abelian variety, *Invent. Math.* **6** (1968), p. 91–105.

[Mur83] M. R. Murty – On Artin's conjecture, *J. Number Theory* **16** (1983), no. 2, p. 147–168.

[Ser81] J.-P. Serre – Quelques applications du théorème de densité de Chebotarev, *Inst. Hautes Études Sci. Publ. Math.* (1981), no. 54, p. 323–401.

[Ser85] J.-P. Serre – Résumé des cours de 1977-1978, 1985, Annuaire du Collège de France 1978, in Collected papers, volume III, Springer-Verlag, p. 67–70.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 119–127
Universität Göttingen, 2004

TWISTED THOM ISOMORPHISMS IN BALMER-WITT THEORY

A. Nenashev
Department of Mathematics and Statistics, University of Regina, Regina, SK, Canada S4S 0A2 • *E-mail :* nenashev@math.uregina.ca

Abstract. Twisted Thom isomorphisms are introduced in Balmer–Witt theory. They are used to calculate the Witt groups of projective bundles and to approach the construction of push-forwards in this theory.

1. Introduction

These are notes from a lecture given in the Summer 2004 on the following occasions:

1. Seminar on algebraic geometry at the University of Göttingen, June 9
2. Topological seminar, University of Bonn, June 15
3. Summer School & Workshop on Motives, K-Theory, and Arithmetical Geometry in Sestri Levante (Italy), June 28 - July 2

I will show that though Balmer–Witt theory is not an oriented theory in the sense of Panin and Smirnov, some of [**Pan03**]-technology can be applied to it. The main tool making this at all possible is a twisted form of Thom

June 9th, 2004.

isomorphisms. Existence of such isomorphisms in BW-theory enables us to achieve the following goals.

I. We reprove the formulas for the *Witt groups of projective bundles* obtained recently by Charles Walter [**Wal03**]. As opposed to the methods of [**Wal03**], we do not make any use of triangulated/derived categories. Instead, we provide a geometric proof [**Nen04b**], resembling somehow and inspired by the proof of the projective bundle theorem in [**Pan03**], by using some basic (but important and nontrivial) properties of the theory obtained by Balmer and Gille. The same approach allows to compute some of the Witt groups of completely split projective quadrics.

II. We define *Gysin maps*, i.e., push-forwards along closed embeddings, for Witt groups exactly the same way it was done in [**Pan03**] for oriented theories, necessarily taking the twisting into account [**Nen**]. Among other properties required of Gysin maps, we prove that they are compatible with compositions of closed embeddings. Observe that it is this property that proved to be a most delicate in [**Pan03**]; its proof there required the whole machinery of the paper. Observe further that we cannot rewrite the proof given in [**Pan03**] for Witt groups as it is based on the use of Chern classes, which we do not have in Balmer–Witt theory. For this reason we had to provide first a completely different proof in the case of oriented theories [**Nen04a**]; it is based on the properties of Thom isomorphisms and the deformation to the normal cone isomorphisms, does not appeal to Chern classes and can be extended to Witt groups.

III. The final goal in this direction would be to introduce *push-forwards along arbitrary projective morphisms*. They must have the form

$$f_* : W^i(Y; f^*L \otimes \omega_{Y/X}) \to W^{i+d}(X; L) \tag{1}$$

where $f : Y \to X$ is a projective morphism of codimension $d = \dim X - \dim Y$, L is a linear bundle on X, and $\omega_{Y/X} = \omega_Y \otimes (f^*\omega_X)^{-1}$. Taking $L = \omega_X$, we get maps

$$f_* : W^i(Y; \omega_Y) \to W^{i+d}(X; \omega_X)\,.$$

These maps must be also compatible with compositions, which makes the assignment

$$X \mapsto W^*(X; \omega_X) \tag{2}$$

a covariant functor with respect to projective morphisms. (Note that there is actually no linear bundle variable in (2), the right hand side depends on X

only.) This functor can be considered then as a theory of Borel-Moore type associated to Balmer–Witt theory.

It is now time to say that *we work with smooth quasi-projective varieties* over a field k of *char* $\neq 2$. All the results/ideas could be possibly extended to regular noetherian schemes of finite Krull dimension or whatever larger class of schemes, but we won't discuss this.

According to [**Pan03**], transfers for projective morphisms should be introduced along the following guidelines.

1. Decompose a projective $f : Y \to X$ as $Y \xhookrightarrow{j} X \times \mathbb{P}^n \xrightarrow{p} X$, where j is a closed embedding.

2. Define a transfer $p_* : W^i(X \times \mathbb{P}^n; p^*L \otimes \omega_X^n) \to W^{i-n}(X; L)$ for any such projection $p : X \times \mathbb{P}^n \to X$, where $\omega_X^n = \omega_{X\times\mathbb{P}^n/X} = p_n^*\omega_{\mathbb{P}^n}$, with $p_n : X \times \mathbb{P}^n \to \mathbb{P}^n$.

3. Define f_* as p_*j_*, where j_* is the corresponding Gysin map, and prove that this does not depend on the choice of a decomposition $f = pj$.

4. Prove that $(fg)_* = f_*g_*$ for any composable projective f and g, as well as other standard properties of push-forwards, e.g., compatibility with pull-backs, projection formula, etc. (see [**Pan03**], 4.1.2]).

Concerning 2., observe that $\omega_X^n \cong \mathscr{O}_{X\times\mathbb{P}^n}(-n-1)$, i.e., the twist is odd when n is even and vise versa. According to [**Wal03**], [**Nen04b**] (also see Section 2 below), $W^i(X \times \mathbb{P}^n; p^*L \otimes \omega_X^n)$ is isomorphic to $W^{i-n}(X; L)$ in the first case and contains it as a direct summand in the second case. Thus in either case we naturally get a definition of p_*.

Concerning 3. and 4., some assertions are to be verified yet, and some could turn out to be technically complicated. However, it is overall clear what to prove and how to do it. In the rest of this note we will comment on the definition of Thom isomorphisms and their applications mentioned in I and II above.

2. Twisted Thom isomorphisms

For a vector bundle $p : E \to X$ of rank n over a smooth X consider the associated Koszul complex (of vector bundles over E):

$$K(E) = (0 \to \wedge^n p^*E^\vee \to \wedge^{n-1} p^*E^\vee \to \ldots \to \wedge^1 p^*E^\vee \to \wedge^0 p^*E^\vee \to 0)$$

It is known that it is exact off X, i.e., its cohomology sheaves are located on X ([**BFM79**], [**Ful84**], App. B). As $(\wedge^i p^*E^\vee)^\vee \cong \wedge^{n-i} p^*E^\vee \otimes \det p^*E$ (canonically), the terms of $K(E)$ can be canonically identified with the terms of $K(E)^{\vee}[n] \otimes \det p^* E^{\vee}$ degreewise; here we assume that $K(E)$ is located in degrees n through 0. Taking into account the sign conventions involved in the definition of a dual complex and the translation functor, we get an isomorphism of complexes

$$\Theta(E) : K(E) \to K(E)^{\vee}[n] \otimes \det p^* E^{\vee} .$$

It can be checked that $(K(E), \Theta(E))$ is a symmetric n-space in the sense adopted for derived Witt groups [**Bal00**], [**Bal01**].

This gives an element $\kappa(E) \in W^n_X(E; \det p^* E^{\vee})$. Adopting the terminology used in [**BFM79**] for K_0, we will call $\kappa(E)$ the Koszul-Thom class. In case of a trivial bundle $E = X \times \mathbb{A}^n$, $K(E)$ becomes the Koszul complex considered by Balmer and Gille [**BG04**], Sections 3 and 5 in terms of (regular) sequences in a (polynomial) ring.

If L is a linear bundle over X, consider the pairing [**GN03**]:

$$W^n_X(E; \det p^* E^{\vee}) \times W^i(E; p^* L) \to W^{i+n}_X(E; (\det p^* E^{\vee}) \otimes p^* L).$$

Multiplication by $\kappa(E)$ yields a map

$$\kappa(E) \star - : W^i(E; p^* L) \to W^{i+n}_X(E; (\det p^* E^{\vee}) \otimes p^* L). \tag{3}$$

We denote by $th(E)$ the composition of (3) with $W^i(X; L) \xrightarrow{\cong} W^i(E; p^* L)$ (homotopy invariance).

Localizing, we can assume that both E and L are trivial bundles, in which case (3) is an isomorphism by a result of S. Gille [**Gil03**], Theorem 9.3 (see also [**BG04**], Theorem 8.2). By Mayer-Vietoris argument we now get

Theorem 1. *The map $th(E) : W^i(X; L \otimes \det E) \to W^{i+n}_X(E; p^* L)$ is an isomorphism for any linear bundle L over X.*

Following [**BFM79**] and [**Pan03**], we call $th(E)$ a Thom isomorphism rather than calling it a dévissage isomorphism as in [**Gil03**].

3. Witt groups of projective bundles

The theorems proved in [**Nen04b**] with the help of Thom isomorphisms assert that for a vector bundle E over X of rank $r+1$ and a linear bundle L/X we have for all i

(a) $W^i(\mathbb{P}(E); p^* L) \cong W^i(X; L)$ if r is even;
(b) $W^i(\mathbb{P}(E); p^* L \otimes \mathscr{O}(2l+1)) = 0$ if r is odd;
(c) $W^i(\mathbb{P}(E); p^* L \otimes \mathscr{O}(2l+1)) \cong W^{i-r}(X; L \otimes det\, E)$ if r is even;

(d) $W^i(\mathbb{P}(E); p^*L) \cong W^i(X; L) \oplus W^{i-r}(X; L \otimes det\, E)$ if r is odd and E can be represented as an extension $0 \to E' \to E \to E'' \to 0$ with E' and E'' of odd rank.

To illustrate our methods, we will sketch (a) by proving that

$$p^* : W^i(X; L) \to W^i(\mathbb{P}(E); p^*L)$$

is an isomorphism. By Mayer-Vietoris, this localizes to the case of trivial E and L. It therefore suffices to show that $p^* : W^i(X) \to W^i(X \times \mathbb{P}^r)$ is an isomorphism if $r \equiv 0 \mod 2$. Next we reduce this to the case $X = pt$; we will prove that $p^* : W^i(pt) \to W^i(\mathbb{P}^r)$ is an isomorphism, and the reader is suggested to insert $X \times -$ throughout the proof and check that it works. The only reference we need is to the following simply looking fact.

Claim 1. (Gille) Let $j : \mathbb{A}^1 - 0 \to \mathbb{A}^1$ denote the natural embedding and let t denote the coordinate on $\mathbb{A}^1 - 0$ (i.e., $\mathbb{A}^1 - 0 \cong spec\, k[t, t^{-1}]$). Then the map $(j^*, t^*j^*) : W^i(\mathbb{A}^1) \oplus W^i(\mathbb{A}^1) \to W^i(\mathbb{A}^1 - 0)$ is an isomorphism for all i, where t^* is the involution on $W^i(\mathbb{A}^1 - 0)$ given by the multiplication of a symmetric form by t.

Claim 2. $W^i(\mathbb{P}^1; \mathscr{O}(2l+1)) = 0$ for any i (which is the simplest case of formula (b)).

Proof. By 2-periodicity in twisting, it suffices to prove $W^i(\mathbb{P}^1; \mathscr{O}(1)) = 0$ for all i. Consider the Mayer-Vietoris sequence for $\mathbb{P}^1 = \mathbb{A}^1_0 \cup \mathbb{A}^1_\infty$ with $\mathscr{O}(1)$ twisting:

$$\begin{aligned} \ldots \to W^i(\mathbb{P}^1; \mathscr{O}(1)) &\to W^i(\mathbb{A}^1_0; \mathscr{O}(1)|_{\mathbb{A}^1_0}) \oplus W^i(\mathbb{A}^1_\infty; \mathscr{O}(1)|_{\mathbb{A}^1_\infty}) \to \\ &\to W^i(\mathbb{A}^1_0 \cap \mathbb{A}^1_\infty; \mathscr{O}(1)|_{\mathbb{A}^1_0 \cap \mathbb{A}^1_\infty}) \to \ldots . \end{aligned}$$

Trivializing $\mathscr{O}(1)$ on $\mathbb{A}^1_0$, $\mathbb{A}^1_\infty$ and $\mathbb{A}^1_0 \cap \mathbb{A}^1_\infty = \mathbb{A}^1 - 0$, we get an isomorphic sequence of the form

$$\ldots \to W^i(\mathbb{P}^1; \mathscr{O}(1)) \to W^i(\mathbb{A}^1) \oplus W^i(\mathbb{A}^1) \xrightarrow{(j^*, -t^*j^*)} W^i(\mathbb{A}^1 - 0) \to \ldots .$$

The assertion follows by Claim 1. $\square$

Claim 3. Let $\mathbb{P}^n \subset \mathbb{P}^{n+2}$ be a linear embedding. If n is even, then the pull-back $W^i(\mathbb{P}^{n+2}) \to W^i(\mathbb{P}^n)$ is an isomorphism for all i.

Proof. Consider the localization sequence

$$(4) \qquad \ldots \to W^i(\mathbb{P}^{n+2}) \to W^i(\mathbb{P}^{n+2} - \mathbb{P}^1) \to W^{i+1}_{\mathbb{P}^1}(\mathbb{P}^{n+2}) \to \ldots ,$$

where $\mathbb{P}^1 \subset \mathbb{P}^{n+2}$ is a complementary projective line. By excision,

$$W^{i+1}_{\mathbb{P}^1}(\mathbb{P}^{n+2}) \cong W^{i+1}_{\mathbb{P}^1}(\mathbb{P}^{n+2} - \mathbb{P}^n).$$

The variety $\mathbb{P}^{n+2} - \mathbb{P}^n$ can be naturally considered as a $(n+1)$-dimensional vector bundle over $\mathbb{P}^1$, which we will denote by V_{n+1}. It can be easily seen that $\det V_{n+1} \cong \mathcal{O}_{\mathbb{P}^1}(n+1)$.

By Theorem 1.1,

$$W^{i+1}_{\mathbb{P}^1}(\mathbb{P}^{n+2} - \mathbb{P}^n) = W^{i+1}_{\mathbb{P}^1}(V_{n+1}) \cong W^{i-n}(\mathbb{P}^1; \det V_{n+1}) \cong W^{i-n}(\mathbb{P}^1; \mathcal{O}_{\mathbb{P}^1}(n+1)).$$

The last group vanishes by Claim 2 as $n+1$ is odd, hence $W^{i+1}_{\mathbb{P}^1}(\mathbb{P}^{n+2}) = 0$ for any i. It follows from (4) that $W^i(\mathbb{P}^{n+2}) \to W^i(\mathbb{P}^{n+2} - \mathbb{P}^1)$ is an isomorphism for any i. But $\mathbb{P}^{n+2} - \mathbb{P}^1$ can be considered as a vector bundle over $\mathbb{P}^n$. By homotopy invariance we are done. □

Thus for an even r we have a sequence of isomorphisms

$$W^i(\mathbb{P}^r) \to W^i(\mathbb{P}^{r-2}) \to \ldots \to W^i(\mathbb{P}^2) \to W^i(pt).$$

The pull-back $p^* : W^i(pt) \to W^i(\mathbb{P}^r)$ splits the composition and must be an isomorphism too. Formula (a) is proved.

To prove (b) for $r \equiv 1 \mod 2$, we get isomorphisms

$$W^i(\mathbb{P}^r; \mathcal{O}(2l+1)) \to W^i(\mathbb{P}^{r-2}; \mathcal{O}(2l+1)) \to \ldots \to W^i(\mathbb{P}^1; \mathcal{O}(2l+1)) = 0$$

by exactly the same reasoning. For the proof of (c) and (d) the reader is referred to [**Nen04b**]. The term of degree $i-d$ in (c) and (d) appears when we apply a Thom isomorphism, of course.

4. Witt groups of completely split quadrics

In [**Nen04b**], a formula is also deduced for the Witt groups of a completely split quadric $Q = Q((d+1)\mathbb{H})$ in certain cases, by using the same methods. Such a quadric can be defined by $x_0y_0 + x_1y_1 + \ldots + x_dy_d = 0$ in $\mathbb{P}^{2d+1}$. Here we consider everything over $pt = spec\, k$, but the same can be done over a base X. We were able to get formulas in the following cases in which the respective localization sequence splits for simple reasons.

(e) If d is even, then $W^i(Q) \cong W^i(pt) \oplus W^{i-2d}(pt)$ for all i.
(f) If d is odd, then $W^i(Q; \mathcal{O}(2l+1)) = 0$ for all i.

These formulas are obtained with the help of a *cell decomposition* of Q. Define $\mathbb{P}^d_x, \mathbb{P}^d_y \subset \mathbb{P}^{2d+1}$ by the equations $y_0 = y_1 = \ldots = y_d = 0$ and $x_0 = x_1 = \ldots = x_d = 0$ respectively. Then $\mathbb{P}^d_x, \mathbb{P}^d_y \subset Q$ and it turns out that

$Q - \mathbb{P}^d_x$ naturally has a vector bundle structure over $\mathbb{P}^d_y$, with the projection $(x_0 : y_0 : \ldots : x_d : y_d) \mapsto (y_0 : \ldots : y_d)$, and vise versa. This makes Q a *relative cellular space* with a 1-step *smooth* filtration. It was used in [**NZ04**] to compute an arbitrary oriented theory of such a quadric, as well as its motivic decomposition. In Witt theory we consider the localization sequence

$$\ldots \to W^i_{\mathbb{P}^d_x}(Q) \to W^i(Q) \to W^i(Q - \mathbb{P}^d_x) \to \ldots \tag{5}$$

in which $W^i(Q - \mathbb{P}^d_x) \cong W^i(\mathbb{P}^d_y)$ by homotopy invariance. If d is even, then $W^i(\mathbb{P}^d_y) \cong W^i(pt)$ (case (a) in Section 2), the pull-back $W^i(pt) \to W^i(Q)$ splits therefore (5), and we get

$$W^i(Q) \cong W^i(pt) \oplus W^i_{\mathbb{P}^d_x}(Q)\,.$$

Next we compute the determinant of the vector bundle $(Q - \mathbb{P}^d_y) \to \mathbb{P}^d_x$, apply a Thom isomorphism and formula (c) of Section 2, and get $W^i_{\mathbb{P}^d_x}(Q) \cong W^{i-2d}(pt)$, which proves (e).

To prove (f), we consider (4) with an odd twist. Then $W^i(Q - \mathbb{P}^d_x; \mathscr{O}(2l+1))$ vanishes by (b), whence $W^i(Q; \mathscr{O}(2l+1)) \cong W^i_{\mathbb{P}^d_x}(Q; \mathscr{O}(2l+1))$. By the same reasoning as above and applying (b) again we show that $W^i_{\mathbb{P}^d_x}(Q; \mathscr{O}(2l+1)) = 0$, which proves (f).

Remark 2. We cannot yet apply the methods of [**NZ04**] to Witt groups of arbitrary cellular varieties as push-forwards are still lacking in this theory.

5. Gysin maps for Witt groups

Recall first how Gysin maps are defined in [**Pan03**] for oriented theories. Let $j : Y \hookrightarrow X$ be a closed embedding of smooth varieties of codimension $d = \dim X - \dim Y$, and let $N_{X/Y}$ denote the normal bundle to Y in X. Then $j_* : A^i(Y) \to A^{i+d}(X)$ is defined as the composition

$$A^i(Y) \xrightarrow{th(N_{X/Y})} A^{i+d}_Y(N_{X/Y}) \xrightarrow[\cong]{d(X,Y)} A^{i+d}_Y(X) \longrightarrow A^{i+d}(X)\,,$$

where

(i) $th(N_{X/Y})$ is the Thom isomorphism associated to the vector bundle $N_{X/Y}$;

(ii) $d(X, Y)$ is the *deformation to the normal cone isomorphisms* for the embedding $Y \hookrightarrow X$;

(iii) the last (trivial) arrow is an extension of support, which is an attribute of any cohomology theory, not necessarily orientable.

Ingredient (i), i.e., Thom isomorphisms, was introduced for Balmer–Witt theory in Section 1. Concerning (ii), we only comment that the deformation isomorphisms $d(X,Y)$ also exist in any, not necessarily orientable cohomology theory and that their existence is not an easy fact [**Pan03**], 2.2.8. However, this can be modified to Witt groups almost straightforward. Taking into account the linear bundle variable, we get deformation isomorphisms of the form

$$W_Y^*(N_{X/Y};p^*L_Y) \cong W_Y^*(X;L)\,,$$

where L is a linear bundle over X, $L_Y = j^*L$ is its restriction to Y, and $p : N_{X/Y} \to Y$ is the projection. Note that there is no degree indexation in [**Pan03**], but in many examples th raises the degree by the rank of the vector bundle, which is the case for W^*, while $d(X,Y)$ always preserves it.

Now we are prepared to define Gysin maps for Witt groups. With the same notation, j_* will denote the composition

$$\begin{tikzcd} W^i(Y;L_Y\otimes\det N_{X/Y}) \arrow[r, "th(N_{X/Y})"] & W_Y^{i+d}(N_{X/Y};p^*L_Y) \arrow[r, "d(X,Y)", "\cong"'] & W_Y^{i+d}(X;L) \arrow[d] \\ & & A^{i+d}(X;L)\,. \end{tikzcd}$$

As $\det N_{X/Y} \cong \omega_{Y/X}$ canonically, we get $j_* : W^i(Y;j^*L\otimes\omega_{Y/X}) \to W^{i+d}(X;L)$, which agrees with (1).

A proof of $(jj')_* = j_*j'_*$ for composable embeddings $Z \overset{j'}{\hookrightarrow} Y \overset{j}{\hookrightarrow} X$ is given in [**Nen04a**] in the case of oriented theories. (Observe that this property is far from being obvious with the definition of j_* that we use.) This proof can be easily modified to Witt groups. This will be done in [**Nen**], as well as a proof of other properties of Gysin maps, including their compatibility with pull-backs in transversal squares, the smooth divisor case, etc. will be given there.

References

[Bal00] P. Balmer – Triangular Witt groups. I. The 12-term localization exact sequence, *K-Theory* **19** (2000), no. 4, p. 311–363.

[Bal01] ______, Triangular Witt groups. II. From usual to derived, *Math. Z.* **236** (2001), no. 2, p. 351–382.

[BFM79] P. Baum, W. Fulton & R. MacPherson – Riemann-Roch and topological K theory for singular varieties, *Acta Math.* **143** (1979), no. 3-4, p. 155–192.

[BG04] P. Balmer & S. Gille – Koszul complexes and symmetric forms over the punctured affine space, 2004, `www.math.uiuc.edu/K-theory`.

[Ful84] W. Fulton – *Intersection theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 2, Springer-Verlag, Berlin, 1984.

[Gil03] S. Gille – A transfer morphism for Witt groups, *J. Reine Angew. Math.* **564** (2003), p. 215–233.

[GN03] S. Gille & A. Nenashev – Pairings in triangular Witt theory, *J. Algebra* **261** (2003), no. 2, p. 292–309.

[Nen] A. Nenashev – Gysin maps in Balmer–Witt theory, in preparation.

[Nen04a] ———, Gysin maps in oriented theories, 2004, www.math.uiuc.edu/K-theory/0695/.

[Nen04b] ———, On the Witt groups of projective bundles and split quadrics, 2004, preprint.

[NZ04] A. Nenashev & K. Zainoulline – Oriented theories of relative cellular spaces, 2004, preprint.

[Pan03] I. Panin – Push-forwards in oriented cohomology theories of algebraic varieties: II, 2003, www.math.uiuc.edu/K-theory/0619/, after I. Panin and A. Smirnov.

[Wal03] C. Walter – Grothendieck–Witt groups of projective bundles, 2003, www.math.uiuc.edu/K-theory/0645/.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 129–134
Universität Göttingen, 2004

BETHE ANSATZ, FUCHSIAN EQUATIONS AND SCHUBERT CALCULUS

E. Mukhin
Department of Mathematics, IUPUI, Science Building, LD 270, 402 N. Blackford Str., Indianapolis, IN 46202-3216, U.S.A. • *E-mail :* mukhin@math.iupui.edu

Abstract. We consider the Bethe Ansatz Equation (BAE) related to the Gaudin model associated to a semisimple Lie group G. Given a solution of the BAE we construct a family of new solutions called a population. The populations are isomorphic to the flag variety associated to the Langlands dual Lie group $G^{\vee}$. The sl_N populations are in one-to-one correspondence with intersection points of appropriate Schubert cycles in the Grassmannian of N planes in the space of polynomials. Thus we relate the subjects of Bethe Ansatz and of Schubert Calculus.

1. A story from 19-th century.

In 1878 Heinrich Eduard Heine, motivated by the developments in the theory of orthogonal polynomials, posed the following question.

Given polynomials $A(x), B(x)$ of degrees n and $n-1$ respectively, what is the number of polynomials $C(x)$ of degree $n-2$ such that the differential equation

$$A(x)y'' - B(x)y' + C(x)y = 0$$

has a polynomial solution $y(x)$ of degree l?

June 15th, 2004.

H.E. Heine proved [**Hei78**] that the number of such $C(x)$ is at most $\binom{n+l-2}{l}$.

An important contribution came from Thomas Jan Stieltjes in 1885 who considered the case

$$A(x) = \prod_{i=1}^{n}(x - z_i), \qquad B(x) = A(x)\sum_{i=1}^{n}\frac{m_i}{x - z_i},$$

where all z_i are distinct (and real) and m_i are negative. T.J. Stieltjes proved [**Sti85**] that in this case the answer to the question of Heine is exactly $\binom{n+l-2}{l}$.

The proof is based on the following simple but very important observation: a polynomial $y(x) = \prod_{i=1}^{l}(x - t_i)$ with distinct roots t_i satisfies (1) if and only if t_i satisfy the following system of algebraic equations:

$$-\sum_{j=1}^{n}\frac{m_j}{t_i - z_j} + \sum_{j=1, j\neq i}^{l}\frac{2}{t_i - t_j} = 0.$$

for all $i = 1, \ldots, l$.

This equation has a meaning in electrostatics. Imagine magnets of charge m_i located at points z_i. Place l identical electrons at points t_i. Then equation (1) can be viewed as the equation of equilibrium meaning that the sum of all forces acting on each electron is zero.

At the same time another German mathematician Hermann Schubert was working on a problem of enumerative geometry. In the modern language, he was studying the integral homology of the Grassmannian variety of s-dimensional planes in a p-dimensional space. The Grassmannian is a smooth projective variety and the additive basis in homology is given by some explicit cycles, called Schubert cycles. Then the ring structure (intersection constants) is described via some combinatorial rule, known today as the Littlewood–Richardson rule.

The work of H. Schubert was awarded a prize in 1874 though it became rigorous only after contributions of D. Hilbert and F. Salveri in 1912.

Now a century later we came to the realization that the two classical subjects described above are actually two facets of the same story. The purpose of this lecture is to explain this fact.

2. The Bethe equations

With the 20th century there come a generalization of equation (1)

Let $\mathfrak{g}$ be a semisimple Lie algebra with simple roots $\alpha_1, \ldots, \alpha_r$, coroots $\alpha_1^\vee, \ldots, \alpha_r^\vee$, let $z_1, ..., z_n$ be distinct complex numbers, $\Lambda_1, \ldots, \Lambda_n$ $\mathfrak{g}$-weights, $l_1, \ldots, l_r$ non-negative integers.

The Bethe Ansatz equation is the following algebraic equation for variables $t_i^{(j)}$, $j = 1, \ldots, r$, $i = 1, \ldots, l_j$:

$$\sum_{s=1}^{n} \frac{-(\Lambda_s, \alpha_i)}{t_j^{(i)} - z_s} \; + \; \sum_{s,\ s\neq i} \sum_{k=1}^{l_s} \frac{(\alpha_s, \alpha_i)}{t_j^{(i)} - t_k^{(s)}} \; + \; \sum_{s,\ s\neq j} \frac{(\alpha_i, \alpha_i)}{t_j^{(i)} - t_s^{(i)}} \; = \; 0.$$

The equation (1) is the case of $\mathfrak{g} = sl_2$ and $\Lambda_i = m_i$.

Note that equation (1) is symmetric with respect to permutations of variables with the same upper index. In what follows we do not distinguish solutions which differ by such permutations.

The Bethe equation (1) appeared in the Bethe Ansatz method of diagonalizing a certain set of commuting matrices, called Hamiltonians of Gaudin model. Each solution of Bethe equation produces an eigenvector. We expect that all eigenvectors are obtained this way and this leads us to the following conjecture (we skip some technical conditions which assure that the number of solutions is indeed finite and that the situation is generic):

The number of solutions of (1) equals the multiplicity of L_{Λ_∞} in

$$L_{\Lambda_1} \otimes \cdots \otimes L_{\Lambda_n}.$$

Here L_Λ denotes the irreducible $\mathfrak{g}$-module with highest weights Λ and the weight Λ_∞ is explicitly given by

$$\Lambda_\infty = \sum_{i=1}^{n} \Lambda_i - \sum_{i=1}^{r} l_i \alpha_i.$$

The Heine-Stieltjes theorem verifies the conjecture in the case of sl_2 when all the weights are negative (and L_{m_i} are Verma modules).

3. Populations

From now on we will deal with the case when all weight Λ_i are integral dominant.

Let $y_i = \prod_{j=1}^{l_i} (x - t_j^{(i)})$. We say that the r-tuple of polynomials $\boldsymbol{y} = \{y_i\}$ represents $t_i^{(j)}$. We call an r-tuple of polynomials $\boldsymbol{y}$ generic if y_i has no multiple roots, does not vanish at z_i and does not have common roots with y_j whenever $(\alpha_i, \alpha_j) < 0$.

We also set

$$T_i(x) = \prod_{s=1}^{n} (x - z_s)^{\langle \Lambda_s, \alpha_i^\vee \rangle}.$$

The following lemma is an adaptation of the Stieltjes observation to the case of integral weights and general Lie algebra.

Lemma 3.1. [**MV02**] *The tuple $\boldsymbol{y}$ represents a Bethe solution if and only if it is generic and there exist polynomials $\tilde{y}_i$ satisfying*

$$W(y_i, \tilde{y}_i) = T_i \prod_{j,\ a_{ij}<0} y_j^{-\langle \alpha_j, \alpha_i^\vee \rangle},$$

where $W(u,v) = u'v - uv'$ denotes the Wronskian of two functions.

Proof. One can treat (1) as an equation of the first order for the unknown function $\tilde{y}_i$. The solution is an integral which becomes a polynomial if and only if some residues vanish. Equation (1) is exactly the vanishing condition for these residues. $\square$

Note that if the polynomial $\tilde{y}_i$ exists then it is not unique, it is parameterized by the choice of the integration constant.

Lemma 3.2. [**MV02**] *If $\boldsymbol{y}$ represents a Bethe solution and the vector $\boldsymbol{y}^{(i)} := (y_1, \dots, \tilde{y}_i, \dots, y_r)$ is generic then $\boldsymbol{y}^{(i)}$ also represents a Bethe solution.*

Proof. The proof is done via comparison of Bethe equations for zeroes of $\boldsymbol{y}$ and $\boldsymbol{y}^{(i)}$ using the Wronskian identity (1). $\square$

Thus starting from a solution of Bethe equation (1), we obtain a family of new solutions $\boldsymbol{y}^{(i)}$ and we can repeat the procedure which we call the reproduction procedure once again. The closure of the family of Bethe solutions obtained from a given one via successive application of the reproduction procedure is called a population.

It is easy to see that a population is an irreducible finite-dimensional variety.

Theorem 3.3. [**MV03**], [**Fre03**] *Any population is isomorphic to the full flag variety G^t/B^t of the Langlands dual of $\mathfrak{g}$. Moreover the decomposition of the population with respect to the degrees of polynomials coincides with the Bruhat decomposition. In particular each population contains a unique Bethe solution which corresponds to a dominant integral weight at infinity.* $\square$

4. Fuchsian equations

The proof of Theorem 3.3 is based on the connection of the Bethe Equation to the some objects called Miura opers. For the purposes of this lecture we restrict our consideration to the case of sl_{r+1} when the Miura oper is equivalent to a scalar differential operator.

Given an r-tuple of polynomials $\boldsymbol{y}$, define a scalar differential operator of order $r+1$ by the formula:

$$\begin{aligned} D(\boldsymbol{y}) &= (\partial - \ln'(\frac{\prod_{s=1}^{r} T_s}{y_r}))\,(\partial - \ln'(\frac{y_r \prod_{s=1}^{r-1} T_s}{y_{r-1}}))\ldots(\partial - \ln'(\frac{y_2 T_1}{y_1}))\,(\partial - \ln'(y_1)) \\ &= \prod_{i}^{0 \,\to\, r} (\,\partial \,-\, \ln'\,(\,\frac{y_{r+1-i}\prod_{s=1}^{r-i} T_s}{y_{r-i}}\,)\,)\,. \end{aligned}$$

Let now $\boldsymbol{y}$ represent an sl_{r+1} Bethe solution and let P be the corresponding population of Bethe solutions.

Theorem 4.1. [**MV02**]

- *If $\boldsymbol{y}_1 \in P$ then $D(\boldsymbol{y}_1) = D(\boldsymbol{y})$.*
- *All solutions of $D(\boldsymbol{y})u = 0$ are polynomials. Moreover these polynomials are relatively prime.*
- *The operator $D(\boldsymbol{y})$ is Fuchsian with singular points $z_1, \ldots, z_n$ and ∞ with exponents given by*

$$z_i \quad : \qquad 0, (\Lambda_i, \alpha_1) + 1, (\Lambda_i, \alpha_1 + \alpha_2) + 2, \ldots, (\Lambda_i, \sum_{j=1}^{r} \alpha_j) + r$$

$$\infty \quad : \qquad l, l + (\Lambda_\infty, \alpha_1) + 1, l + (\Lambda_\infty, \alpha_1 + \alpha_2) + 2, \ldots, l + (\Lambda_\infty, \sum_{j=1}^{r} \alpha_j) + r,$$

where l is some nonnegative integer and Λ_∞ is the unique integer dominant weight occuring in P. □

We call $D(\boldsymbol{y}) = D(P)$ the fundamental operator of the population P.

Theorem 4.2. [**MV02**] *Let D be a Fuchsian differential operator of order $r+1$ with polynomial kernel and exponents as in Theorem 4.1. Assume in addition that the polynomials in kernel are relatively prime. Then D is a fundamental operator of some population P of sl_{r+1} Bethe solutions.*

Therefore we have a one-to-one correspondence between population and differential operators with polynomial solutions.

5. Schubert calculus

Let D be the fundamental operator of the sl_{r+1} population of Bethe solutions and let V be its kernel. Then V is a point on the Grassmannian of $r+1$ dimensional planes in the space of polynomials $\mathbb{C}_d[x]$ of degree at most d for sufficiently large d.

The description of the singular points and exponents given in Theorem 4.1 immediately implies that in fact V belongs to a certain intersection of Schubert cycles related to flags at z_i given by the order of vanishing at z_i and the flag to infinity given by degree.

Thus we have a one-to-one correspondence between points of intersection of certain Schubert cycles and populations of Bethe solutions. The Schubert calculus asserts that the algebraic index of the intersection of the corresponding Schubert cycles equals the multiplicity of L_{Λ_∞} in $L_{\Lambda_1} \otimes \cdots \otimes L_{\Lambda_n}$. The Bethe Ansatz conjecture claims that the number of solutions of Bethe equations corresponding to dominant integral weight at infinity $\Lambda - \infty$ for generic z, properly counted, also equals the multiplicity of L_{Λ_∞} in $L_{\Lambda_1} \otimes \cdots \otimes L_{\Lambda_n}$.

Therefore the Bethe Ansatz conjecture is related to the question of transversality of Schubert cycles for generic z_i.

6. Conclusion

At present, the problem of counting solutions of Bethe equation and the problem of transversality of Schubert cycles are both open. However we hope that the described connection between the two problems will help in the search of the solution.

References

[Fre03] E. Frenkel – Opers on the projective line, flag manifolds and Bethe ansatz, 2003, `math.QA/0308269`.

[Hei78] E. Heine – *Handbuch der Kugelfunctionen*, vol. 1, Berlin, 1878.

[MV02] E. Mukhin & A. Varchenko – Critical Points of Master Functions and Flag Varieties, 2002, `math.QA/0209017`.

[MV03] ———, Miura Opers and Critical Points of Master Functions, 2003, `math.QA/0312`.

[Sti85] T. Stieltjes – Sur certains polynomes qui verifient une equation differentielle lineaire du second ordre et sur la theorie des fonctions de Lame, *Acta Mathematica* **6** (1885), p. 321–326.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 135–143
Universität Göttingen, 2004

EQUATIONS OF UNIVERSAL TORSORS AND COX RINGS

B. Hassett

Department of Mathematics, Rice University, MS 136, Houston, TX 77251-1892, U.S.A. • *E-mail :* hassett@math.rice.edu

Abstract. We discuss several constructions of universal torsors over rational surfaces.

1. Universal torsors and Cox rings

1.1. Motivating Example. All fields are supposed to be of characteristic 0.

Let X/K be a quintic Del Pezzo surface over a number field K. We have $\overline{X} = X_{\overline{K}} = \mathrm{Bl}_{P_1,P_2,P_3,P_4}\,\mathbb{P}^2$, i.e. geometrically, X is the blow-up of $\mathbb{P}^2$ in four points in general position. Without loss of generality, we may assume that

$$P_1 = [1,0,0], P_2 = [0,1,0], P_3 = [0,0,1], P_4 = [1,1,1].$$

***Theorem 1* (Enriques, Swinnerton-Dyer).** *Even in the non-split case,*

$$X(K) \neq \emptyset.$$

Proof. See [**Sko93**]. □

Notes by Ulrich Derenthal, June 18th and 19th, 2004.

Since there is a unique projectivity taking arbitrary generic points P_1, P_2, P_3, P_4 (i.e., distinct and no three of them collinear) to $[1,0,0], \ldots, [1,1,1]$ as above, the geometry behind this over $\overline{K}$ is (where $P_5 \in \overline{X}$ is the point we want to describe):

$$\begin{aligned} \overline{X} &= \mathrm{SL}_3 \backslash\backslash \{(P_1, \ldots, P_5) \in \mathbb{P}^2\} \\ &= \mathrm{SL}_3 \backslash\backslash \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ y_1 & y_2 & y_3 & y_4 & y_5 \\ z_1 & z_2 & z_3 & z_4 & z_5 \end{pmatrix} //\mathbb{G}_m^5 . \end{aligned}$$

Consider the Grassmannian of 3-dimensional subspaces of 5-dimensional space $\mathrm{Gr}(3,5)$. Since such a subspace is described by a basis which is unique only up to an action of GL_3, we have $\mathrm{GL}_3 \backslash\backslash M(3 \times 5) \cong \mathrm{Gr}(3,5)$, where we interpret the three rows of a 3×5 matrix as a basis. This implies that $\mathrm{SL}_3 \backslash\backslash M(3 \times 5)$ is the cone over this Grassmannian.

Therefore, $\overline{X} \cong \mathrm{Cone}(\mathrm{Gr}(3,5))//\mathbb{G}_m^5$. Here, $\mathrm{Gr}(3,5)$ is embedded into $\mathbb{P}^9$ by the Plücker embedding.

The "miracle" is that this generalizes to non-closed fields.

Remark 2. The permutation group S_5 of the five points acts on the situation, and actually $\mathrm{Aut}(\overline{X}) = S_5$.

Descent data for X is given by representations $\rho : \mathrm{Gal}(\overline{K}/K) \to S_5$. Let T_ρ be the nonsplit form of $\mathbb{G}_m^5$ corresponding to ρ. In fact, X is $\mathrm{Cone}(\mathrm{Gr}(3,5))//T_\rho$.

1.2. Universal torsors. Let X be a smooth projective variety over $\overline{K}$. Assume $\mathrm{Pic}(X)$ is free of rank r. Let T_X be the Néron-Severi torus, i.e., its character group is $\chi^*(T_X) = \mathrm{Pic}(X)$.

Definition 3. A *universal torsor* $\mathscr{U}$ is a T_X-principal homogeneous space

$$\begin{tikzcd} T_x \arrow[r] & \mathscr{U} \arrow[d] \\ & X \end{tikzcd}$$

so that given an element $\lambda \in \chi^*(T_X)$ (i.e., $\lambda : T_X \to \mathbb{G}_m$), then $\mathscr{M}_\lambda^\times \cong \mathscr{L}_\lambda - \{0\text{-section}\}$ as $\mathbb{G}_m$-bundles over X. Here, $\mathscr{L}_\lambda \in \mathrm{Pic}(X)$ is the line bundle associated to λ by $\chi^*(T_X) \cong \mathrm{Pic}(X)$, and $\mathscr{M}_\lambda$ is the associated bundle to the principal bundle $\mathscr{U} \to X$ induced by the representation λ.

Example 4. 1. Let $X = \mathbb{P}^n$. Then $\mathscr{U} = \mathbb{A}^{n+1} - \{0\}$ is the corresponding universal torsor with the torus acting diagonally. We have $\mathscr{U}/\mathbb{G}_m \cong X = \mathbb{P}^n$.

2. Let X be the quintic Del Pezzo surface as above with the action of T_X on $\mathrm{Cone}(\mathrm{Gr}(3,5))$. Then the universal torsor $\mathscr{U}$ is the open subset of $\mathrm{Cone}(\mathrm{Gr}(3,5))$ on which T_X acts freely.

The abstract approach to universal torsors is as follows: Choose a minimal set $\mathscr{L}_1, \ldots, \mathscr{L}_r$ generating $\mathrm{Pic}(X)$ over $\mathbb{Z}$. Denote $\mathscr{L}_j - \{0\text{-section}\}$ by $\mathscr{L}_j^\times$. Let $\mathscr{U} = \mathscr{L}_1^\times \times \cdots \times \mathscr{L}_r^\times$. Then $T_X \to \mathscr{U} \to X$ is a T_X-principal bundle defining the universal torsor.

However, this abstract definition is not very useful, e.g., for number theoretic applications.

Remark 5. Over non-closed fields, we may not be able to descend the universal torsor $\mathscr{U}$.

For example, consider a non-split conic X. It is geometrically isomorphic to $\mathbb{P}^1$, but it has no line bundle isomorphic to $\mathscr{O}_{\mathbb{P}^1}(1)$ over the ground field. It only has line bundles of even degree, so there cannot exist a universal torsor over the ground field.

1.3. Total coordinate rings / Cox rings.

Definition 6. Let X be a projective variety with properties as above. Let $\mathscr{L}_1, \ldots, \mathscr{L}_r$ be a basis of $\mathrm{Pic}(X)$. Then the Cox ring of X is defined as

$$\mathrm{Cox}(X) = \bigoplus_{(v_1,\ldots,v_r)\in\mathbb{Z}^r} \Gamma(X, \mathscr{L}_1^{v_1} \otimes \cdots \otimes \mathscr{L}_r^{v_r}).$$

Properties of $\mathrm{Cox}(X)$ are:

1. It is graded by $\mathrm{Pic}(X)$: for $\lambda \in \chi^*(T_X) \cong \mathrm{Pic}(X)$, the part of degree λ is given by $\mathrm{Cox}(X)_\lambda = \Gamma(X, \mathscr{L}_\lambda)$.
2. The torus T_X acts naturally on $\mathrm{Cox}(X)$: For $t \in T_X$, $s \in \mathrm{Cox}(X)_\lambda$, this action is given by $t(s) := \lambda(t) \cdot s$.
3. $\mathrm{Cox}(X)$ is independent of the choice of generators $\mathscr{L}_i$ of the Picard group. Given two sets of generators $\mathscr{L}_i$ and $\mathscr{M}_j$, the induced isomorphism of rings is canonical only up to the action of the torus T_X. The reason is that the isomorphism depens on a choice of isomorphisms

$$L_j \cong \mathscr{M}_1^{n_1} \otimes \cdots \otimes \mathscr{M}_r^{n_r}, j \in \{1, \ldots, r\}.$$

However, such an isomorphism is not canonical: $\mathscr{L}_j$ has automorphisms given by scalar multiplication. For details, see **[HT04]**.

The existence of non-trivial automorphisms makes the descent of universal torsors an interesting question.

4. The graded pieces of $\mathrm{Cox}(X)$ which are non-zero correspond to effective divisors on X.

The Cox ring does not need to be finitely generated:

Example 7 **(Mukai).** Let $X = \mathrm{Bl}_{P_1,\ldots,P_n}\mathbb{P}^{r-1}$ be the blowup of projective space in n points in general position. If $\frac{1}{2}+\frac{1}{r}+\frac{1}{n-r}\geq 1$, then $\mathrm{Cox}(X)$ is not finitely generated (i.e., for $\mathbb{P}^2$: $n\geq 9$; for $\mathbb{P}^3$: $n\geq 8$). Details can be found in [**Muk01**].

However, it is finitely generated if one of the following conditions is true:

1. The cone of effective divisors $\mathrm{NE}(X)$ is generated by a finite collection of semi-ample line bundles (e.g., $X = G/P$ where P is parabolic subgroup of an algebraic group G).
2. X is (log) Fano of dimension ≤ 3.
3. X is toric. In this case, for $X - \mathbb{G}_m^{\dim X} = \bigcup_{j=1}^{N} D_j$ where the D_j are subvarieties of codimension 1, and $s_j \in \Gamma(\mathscr{O}_X(D_j))$ is non-zero, then $\mathrm{Cox}(X)\cong K[s_1,\ldots,s_N]$.

1.4. Relations between universal torsors and Cox rings. From now on, assume that $\mathrm{Cox}(X)$ is finitely generated. Let $\mathscr{V} = \mathrm{Spec}(\mathrm{Cox}(X))$. It is affine with T_X-action $T_X\times\mathscr{V}\to\mathscr{V}$. Fix an open subset $\mathscr{U}$ on which T_X acts freely. The basic fact is that $\mathscr{U}$ is a T_X-principal bundle over X:

$$\begin{tikzcd} T_X \arrow[r] & \mathscr{U} \arrow[d] \\ & X \end{tikzcd}$$

and $\mathscr{U}$ is a universal torsor.

The punchline is that this way, the universal torsor $\mathscr{U}$ is naturally a quasi-affine variety. Therefore, giving equations for $\mathscr{U}$ is equivalent to giving generators and relations for $\mathrm{Cox}(X)$. This can be done by algebro-geometric methods, which may be seen as an improvement to the existing number theoretic method to calculate universal torsors.

To sketch a proof of these results, observe that X is naturally a Geometric Invariant Theory quotient $(\mathscr{V}//T_X)_\lambda$ (by Keel–Hu, [**HK00**]) after specifying a linearization $\lambda\in\chi^*(T_X)$ so that $\mathscr{L}_\lambda$ is an ample line bundle on X.

Note that we need to mix affine invariant theory and the usual projective Geometric Invariant Theory to interpret $(\mathscr{V}//T_X)_\lambda$: First take the affine quotient under the action of $\ker(\lambda)$, which gives an affine variety. Then take Proj using the grading coming from the character λ.

Then $\mathrm{Proj}(\bigoplus_{n\geq 0}\mathrm{Cox}(X)_{n\lambda}) = (\mathscr{V}//T_X)_\lambda$ by Geometric Invariant Theory. The left hand side is $\mathrm{Proj}(\bigoplus_{n\geq 0}\Gamma(X,\mathscr{L}_\lambda^{\otimes n}))$, which is just X since $\mathscr{L}_\lambda$ is ample.

A second observation is that given $\lambda\in\chi^*(T_X)$, i.e., $\lambda : T_X\to\mathbb{G}_m$, the associated bundle induces $\mathscr{L}_\lambda^{-1}$. Therefore, it suffices to check the claim for ample λ.

We have an inclusion $\bigoplus_{n\geq 0}\mathrm{Cox}(X)_{n\lambda}\to\mathrm{Cox}(X)$ which induces a dominant map $\mathscr{V}\to\mathrm{Cone}(X\subset\mathbb{P}^N,\mathscr{L}_\lambda)$. Therefore, we have

$$\begin{array}{ccc}
\mathscr{V} & \longrightarrow & \mathrm{Cone}(X\subset\mathbb{P}^N) \\
\uparrow & & \uparrow \\
\mathscr{U} & \longrightarrow & (\mathrm{Cone}(X\subset\mathbb{P}^N)-\{0\})\cong(\mathscr{L}_\lambda^{-1})^\times
\end{array}$$

The point is: One gets hold of the universal torsor by embedding it into the affine variety $\mathrm{Spec}(\mathrm{Cox}(X))$.

2. Equations of universal torsors

From now on, let X be a smooth projective variety over on algebraically closed field K of characteristic 0 with $\mathrm{Pic}(X)\cong\mathbb{Z}^r$ whose Cox ring is finitely generated. Therefore, the cone of effective divisors $\mathrm{NE}(X)$ is finitely generated.

2.1. The method of Colliot-Thélène and Sansuc.

This approach to the calculation of Cox rings can be found in [**CTS87**].

On X, choose effective divisors $D_1,\dots,D_N$ generating $\mathrm{Pic}(X)$. Let $W = X\backslash(D_1\cup\cdots\cup D_N$. Since removing these generators kills the Picard group, $\mathrm{Pic}(W)=0$.

We have an exact sequence

$$0\to K[W]^*/K^*\to\bigoplus_{j=1}^N\mathbb{Z}D_j\to\mathrm{Pic}(X)\to 0$$

where $K[W]^*/K^*$ describes the linear equivalences among $\{D_1,\dots,D_N\}$.

Dualizing this sequence by applying $\mathrm{Hom}(\cdot,\mathbb{G}_m)$, we obtain

$$1\to T_X\to\mathbb{G}_m^N\xrightarrow{q}R_W\to 1.$$

Remark 8. A morphism $\varphi : Z \to R_W$ gives a T_X-torsor:

$$\begin{tikzcd} T_X \arrow[r] & \mathbb{G}_m^N \times_{R_W} Z \arrow[d] & \supset & q^{-1}(\varphi(z)) \arrow[d] \\ & Z & \ni & z \end{tikzcd}$$

The strategy is to construct a T_X-torsor $\mathcal{U}_W$ over W which extend to a universal torsor over X. This strategy works well in many cases, but not in general.

The morphism $\varphi : W \to R_W$ is constructed by constructing a splitting σ to the quotient

$$\begin{tikzcd} K[W]^* \arrow[r, shift right] & K[W]^*/K^* : \arrow[l, shift right, "\sigma"'] \end{tikzcd}$$

Note that σ induces a K-algebra homomorphism

$$K[R_W] = K[t_1, t_1^{-1}, \dots, t_{N-r}, t_{N-r}^{-1}] \to K[W], \quad t_j \mapsto \sigma(t_j),$$

where the t_j form a basis for $\chi^*(R_W)$ and $r = \mathrm{Rank}(\mathrm{Pic}(X))$. Since R_W is affine, such a homomorphism corresponds to a K-morphism $W \to R_W$, which defines φ.

The key fact is that the morphism φ extracted from σ gives a torsor $T_X \to \mathcal{U}_W \to W$ on W admitting an extension to a universal torsor $T_X \to \mathcal{U} \to X$ over X.

$$\begin{tikzcd} T_X \arrow[r] & \mathcal{U}_W \arrow[d] & \rightsquigarrow & T_X \arrow[r] & \mathcal{U} \arrow[d] \\ & W & & & X \end{tikzcd}$$

An explicit method for constructing such an extension is not known. Only the existence is proven in [**CTS87**].

Remark 9 **(Batyrev).** Given a point $P \in W$, we get a natural splitting σ_P : $K[W]^*/K^* \to K[W]^*$: for every element of $K[W]^*/K^*$, choose a representing f satisfying $f(P) = 1$.

2.2. The example of the quintic Del Pezzo surface. Let $X = \mathrm{Bl}_{P_1,\dots,P_4}\mathbb{P}^2$ be again the blow-up of $\mathbb{P}^2$ in

$$P_1 = [1,0,0], P_2 = [0,1,0], P_3 = [0,0,1], P_4 = [1,1,1].$$

We will see how to obtain the Plücker equations defining the universal torsor by this method.

Consider the exceptional divisors E_i and the transforms l_{ij} of the lines through P_i and P_j ($i \neq j \in \{1, \ldots, 4\}$). Choose coordinates $[x, y, z]$ and let $u = \frac{x}{z}$, $v = \frac{y}{z}$.

Consider

$$\begin{aligned}
\operatorname{div}(u = x/z) &= l_{23} + E_3 - l_{12} - E_1 \\
\operatorname{div}(v = y/z) &= l_{13} + E_3 - l_{12} - E_2 \\
\operatorname{div}(u - 1) &= l_{24} + E_4 - l_{12} - E_1 \\
\operatorname{div}(v - 1) &= l_{14} + E_4 - l_{12} - E_2 \\
\operatorname{div}(u - v) &= l_{34} + E_3 + E_4 - l_{12} - E_1 - E_2
\end{aligned}$$

Next, we normalize these functions by constructing a section σ_P from a chosen point, say $P = [3, 2, 1]$. This gives a morphism $\varphi : W \to R_W$ as above.

Consider the sections λ_{ij} corresponding to l_{ij} and η_i to E_i. Using the normalization, we obtain:

$$\frac{u}{3} = \frac{\lambda_{23}\eta_3}{\lambda_{12}\eta_1}, \quad \frac{v}{2} = \frac{\lambda_{13}\eta_3}{\lambda_{12}\eta_2}, \quad \frac{u-1}{2} = \frac{\lambda_{24}\eta_4}{\lambda_{12}\eta_1}, \quad v-1 = \frac{\lambda_{14}\eta_4}{\lambda_{12}\eta_2}, \quad u-v = \frac{\lambda_{34}\eta_3\eta_4}{\lambda_{12}\eta_1\eta_2}.$$

Then the relations between the sections $u, v, u-1, v-1, u-v$ give relations between the sections λ_{ij}, η_i:

$$\begin{aligned}
3\frac{u}{3} - 2\frac{v}{2} = u - v \quad &\rightsquigarrow \quad -(3\lambda_{23})\eta_2 + (2\lambda_{13})\eta_1 + \lambda_{34}\eta_4 = 0 \\
2\frac{v}{2} = (v-1) + 1 \quad &\rightsquigarrow \quad \lambda_{14}\eta_4 - (2\lambda_{13})\eta_3 + \lambda_{12}\eta_2 = 0 \\
2\frac{u-1}{2} - (v-1) = u - v \quad &\rightsquigarrow \quad \lambda_{34}\eta_3 - (2\lambda_{24})\eta_4 + \lambda_{14}\eta_1 = 0 \\
3\frac{u}{3} = 2\frac{u-1}{2} + 1 \quad &\rightsquigarrow \quad (2\lambda_{24})\eta_4 - (3\lambda_{23})\eta_3 + \lambda_{12}\eta_1 = 0 \\
-(u-v) + v(u-1) - (v-1)u = 0 \quad &\rightsquigarrow \quad \lambda_{12}\lambda_{34} - (2\lambda_{13})(2\lambda_{24}) + (3\lambda_{23})\lambda_{14} = 0
\end{aligned}$$

Replacing $3\lambda_{23}, 2\lambda_{13}, 2\lambda_{24}$ by new variables exactly gives the Plücker relations.

2.3. The Cox ring approach. Consider a different example:

$$X = \mathrm{Bl}_{P_1,P_2,P_3}\,\mathbb{P}^2 \text{ where } P_1 = [1, 0, 0], P_2 = [1, 1, 0], P_3 = [0, 1, 0],$$

i.e., X is the blow-up of $\mathbb{P}^2$ in three points lying on a line. Let l_{123} be the transform of this line.

Basic facts on X are:

1. $\mathrm{NE}(X) = \langle l_{123}, E_1, E_2, E_3 \rangle$ is a simplicial cone, i.e., there are no relations between its generators. Therefore, the previous method does not work.

We have $W = X - \{E_1, E_2, E_3, l_{123}\} \cong \mathbb{A}^2$, and X is an equivariant compactification of $\mathbb{G}_a^2$, acting on $\mathbb{A}^2$ by translation.

2. The ample cone, which is the dual of the effective cone, is generated by

$$\{l_{123} + E_1 + E_2 + E_3, l_{123} + E_1 + E_2, l_{123} + E_1 + E_3, l_{123} + E_2 + E_3\}.$$

3. The anticanonical divisor $-K_X$ is nef and big. Therefore, X is (log) Del Pezzo.

Next, we are looking for generators and relations of $\mathrm{Cox}(X)$. Generators are $\lambda_{123} \in \Gamma(\mathscr{O}_X(l_{123})) \subset \mathrm{Cox}(X)_{l_{123}}$ which is vanishing exactly along l_{123}, and $\eta_j \in \Gamma(\mathscr{O}_X(E_j)) \subset \mathrm{Cox}(X)_{E_j}$ for $j \in \{1, 2, 3\}$.

These sections do not generate the Cox ring – in cases where they generate it, the method of Colliot-Thélène works well, but not here. We must choose additional generators: $\Gamma(\mathscr{O}_X(l_{123} + E_1 + E_2))$ corresponds to linear forms in x, y, z vanishing at P_3, i.e., it is $K^2 \cong \langle x, z\rangle$. Besides $\lambda_{123}\eta_1\eta_2$, which can be identified as z, we can choose another section ξ_3 such that $\xi_3\eta_3 = -x$.

Similarly, we have $\xi_1 \in \Gamma(\mathscr{O}_X(l_{123} + E_2 + E_3))$ such that $y = \xi_1\eta_1$ and $\xi_2 \in \Gamma(\mathscr{O}_X(l_{123} + E_1 + E_3))$ such that $x - y = \xi_2\eta_2$.

This gives a homomorphism

$$\psi : K[\lambda_{123}, \eta_1, \eta_2, \eta_3, \xi_1, \xi_2, \xi_3]/\langle \eta_1\xi_1 + \eta_2\xi_2 + \eta_3\xi_3\rangle \to \mathrm{Cox}(X),$$

and since the dimension of both of these is 6 ($\dim(X) = 2$ and $\mathrm{Rank}(\mathrm{Pic}(X)) = 4$), it is reasonable to hope that this is an isomorphism.

Remark 10. Then $\eta_1\xi_1 + \eta_2\xi_2 + \eta_3\xi_3$ is the equation of the universal torsor $T_X \to \mathscr{U} \to X$ in the sense that

$$\mathscr{U} \subset \mathscr{V} := \operatorname{Spec} K[\lambda_{123}, \eta_1, \eta_2, \eta_3, \xi_1, \xi_2, \xi_3]/\langle \eta_1\xi_1 + \eta_2\xi_2 + \eta_3\xi_3\rangle.$$

Strategy of the proof. First, consider ψ in degrees ν corresponding to a nef line bundles on X. Such line bundles are semi-ample and in this case even globally generated. By induction on the effective monoid or by application of a vanishing theorem, we can prove that ψ is surjective in these nef degrees.

In degrees ν corresponding to not necessarily nef divisors ν, we reduce to the nef case the following way: Given $s \in \mathrm{Cox}(X)_\nu = \Gamma(X, \mathscr{L}_\nu)$, there exists a nef line bundle m, a section $\mu \in \mathrm{Cox}(X)_m$ and $a, b_1, b_2, b_3 \in \mathbb{Z}_{\geq 0}$ so that $s = \mu\lambda_{123}^a\eta_1^{b_1}\eta_2^{b_2}\eta_3^{b_3}$. This follows from the geometric fact that, given effective D on X, we can write $D = M + F$ for a base point free divisor M and a fixed divisor F supported in $\{l_{123}, E_1, E_2, E_3\}$. □

References

[CTS87] J.-L. Colliot-Thélène & J.-J. Sansuc – La descente sur les variétés rationnelles. II, *Duke Math. J.* **54** (1987), no. 2, p. 375–492.

[HK00] Y. Hu & S. Keel – Mori dream spaces and GIT, *Michigan Math. J.* **48** (2000), p. 331–348, Dedicated to William Fulton on the occasion of his 60th birthday.

[HT04] B. Hassett & Y. Tschinkel – Universal torsors and Cox rings, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), Progr. Math., vol. 226, Birkhäuser Boston, Boston, MA, 2004, p. 149–173.

[Muk01] S. Mukai – Counterexample to Hilbert's Fourteenth Problem for the 3-dimensional additive group, RIMS preprint 1343, 2001.

[Sko93] A. N. Skorobogatov – On a theorem of Enriques-Swinnerton-Dyer, *Ann. Fac. Sci. Toulouse Math. (6)* **2** (1993), no. 3, p. 429–440.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 145–158
Universität Göttingen, 2004

QUELQUES BORDS IRRATIONNELS DE VARIÉTÉS DE SHIMURA

F. Paugam
NWF I - Mathematik, Universität Regensburg, 93040 Regensburg, Germany
E-mail : `frederic.paugam@mathematik.uni-regensburg.de`

Abstract. We are looking for a formulation of Manin's real multiplication question in higher rank. This question has at least two parts:

1. formalization of the linear algebra side of the story in terms of morphisms of algebraic groups analogous to Shimura and Deligne's point of view on the theory of complex multiplication.
2. noncommutative algebraic geometry.

Here we are interested mostly in the first part. We also recall some known results concerning the second part.

1. Introduction

Ce document contient essentiellement les notes d'un exposé fait à Goettingen pour la conférence "Géométrie diophantienne" organisée par Yuri Tschinkel. Cet exposé a aussi été fait dans plusieurs autres endroit d'avril à juin 2004: les séminaires de géométrie algébrique de Rennes, K-théorie et géométrie non

---

June 22nd, 2004.

commutative à l'IHP, mathématiques pures de l'ENS Lyon, géométrie non commutative et théorie des nombres II à Bonn. Je remercie mes hôtes mathématiques (Pierre Berthelot, Max Karoubi, Etienne Ghys, Matilde Marcolli et Yuri Tschinkel) de m'avoir offert l'opportunité d'exposer ces travaux, qui consistent essentiellement en un effort de compréhension de l'aspect algèbre linéaire du problème de multiplication réelle de Manin en rang supérieur du point de vue des groupes algébriques. J'espère que ce point de vue sera utile aux géomètres non commutatifs désireux d'aborder cette question. Ce travail porte l'empreinte des discussions éclairantes que j'ai eues avec Matilde Marcolli, et pour lesquelles je la remercie. Je remercie aussi Gabor Wiese pour son aide sur la multiplication complexe. Ce travail à été fait sur les fonds du réseau RTN "K-theory and algebraic groups", à Regensburg.

Le théorème de Kronecker-Weber nous dit que l'extension abélienne maximale de $\mathbb{Q}$ est engendrée par l'image de l'application

$$e^{2i\pi\bullet} : \mathbb{Q} \to \mathbb{C}.$$

Soit $F/\mathbb{Q}$ un corps de nombres. Le douzième problème de Hilbert est de trouver des fonctions analytiques remplaçant la fonction exponentielle et dont les valeurs spéciales engendrent l'extension abélienne maximale de F. Ceci peut-être considéré comme une explicitation de la théorie du corps de classe qui permet, elle, de décrire cette extension en termes de classes d'idéaux généralisés.

Soit $F/\mathbb{Q}$ un corps quadratique imaginaire. Alors $\mathbb{C}/\mathscr{O}_F$ est une courbe elliptique dite à multiplication complexe par F et on peut montrer qu'elle est définie sur un corps de nombres, extension abélienne de F. La théorie de la multiplication complexe ("Jugendtraum" de Kronecker) dit que toutes les extension abéliennes de F peuvent être décrites grâce à des courbes elliptiques de ce genre et à leurs points de torsion.

Shimura et Taniyama ont montré que le même genre de chose marchait pour des extensions quadratiques totalement imaginaires de corps totalement réels en utilisant des variétés abéliennes.

Ce que Manin appelle son "Alterstraum" (voir [**Man**]) est que si $F/\mathbb{Q}$ est quadratique réel, on peut utiliser des "quotients" du type $\mathbb{C}/\mathscr{O}_F$ pour faire une théorie de la multiplication réelle analogue à ce qui se fait avec les courbes elliptiques. On remarque que dans ce cas, $\mathscr{O}_F$ est dense dans une droite réelle et la notion habituelle de quotient ne suffit pas. Il faut remarquer que Gauss, Shimura, Stark et bien d'autres ont aussi étudié ce genre de rêve, sans le formuler sous cette forme.

J'ai cherché à mieux comprendre ce rêve de Manin, en prenant un point de vue à la Deligne sur les variétés de Shimura qui permet plus facilement de voir ce dont on a besoin en dimension supérieure.

Regardons maintenant le point de vue modulaire sur la multiplication complexe. L'espace des modules des courbes elliptiques sur $\mathbb{C}$ à structure de niveau infinie est une variété de Shimura qui à un modèle sur $\mathbb{Q}$ (l'espace de module des courbe elliptiques sur $\mathbb{Q}$) noté

$$S = \mathrm{Sh}(\mathrm{GL}_2, \mathbb{H}^{\pm}).$$

Si $x \in S(\mathbb{C})$ est un point spécial correspondant à une courbe elliptique à multiplication complexe par un corps quadratique totalement imaginaire $F/\mathbb{Q}$, on lui associe une sous-variété de Shimura profinie définie sur F

$$\mathrm{Sh}(T, \{x\}) \subset S_F$$

avec $T = \mathrm{Res}_{F/\mathbb{Q}} \mathbb{G}_m$.

On a une action naturelle $\mathfrak{nat}$ de $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ sur $\mathrm{Sh}(T, \{x\})(\overline{\mathbb{Q}})$ donnée par la restriction de l'action naturelle sur $S(\overline{\mathbb{Q}})$. On a aussi une action naturelle de $T(\mathbb{A}_f)/T(\mathbb{Q})$ sur $\mathrm{Sh}(T, \{x\})(\overline{\mathbb{Q}})$. Ce groupe étant le groupe des composantes connexes du groupe de classes d'idèles de F, on a un morphisme de réciprocité du corps de classe

$$\mathfrak{artin}^{-1} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to T(\mathbb{A}_f)/T(\mathbb{Q})$$

et donc une nouvelle action de Galois sur $\mathrm{Sh}(T, \{x\})(\overline{\mathbb{Q}})$ notée $\mathfrak{rec}$ (donnée par l'inverse de l'action $\mathfrak{artin}^{-1}$).

Le théorème principal de la multiplication complexe implique que ces deux actions sont les mêmes, i.e.

$$\mathfrak{nat} = \mathfrak{rec}.$$

On peut montrer que ce résultat, bien que visuellement loin du problème de Hilbert, en donne la réponse pour les corps quadratiques (la fonction j et les fonctions elliptiques sont les fonctions dont on prend des valeurs spéciales car elles permettent de calculer les corps de définition des classes d'isomorphismes de courbes elliptiques et de leurs points de torsion).

En rang supérieur, la théorie de la multiplication complexe se formule de la même manière en regardant les points spéciaux dans les espaces de modules de variétés abéliennes principalement polarisées

$$\mathrm{Sh}(\mathrm{GSp}_{2n}, \mathscr{S}^{\pm}),$$

qui sont aussi munis de deux actions, l'une naturelle et l'autre donnée par le corps de classe. Le théorème principal de la multiplication complexe donne l'égalité de ces deux actions.

Les variétés de Shimura (connexes) finies sont des (limites projectives de) quotients du type

$$\Gamma \backslash G(\mathbb{R})/K$$

avec $G/\mathbb{Q}$ groupe réductif connexe, $\Gamma \subset G(\mathbb{Q})$ sous-groupe arithmétique et $K \subset G(\mathbb{R})$ sous-groupe compact maximal dans $G^{ad}(\mathbb{R})$.

Pour les compactifier, on rajoute des composantes de bords rationnelles correspondant à des sous-groupes paraboliques rationnels $P \subset G$.

On peut aussi compactifier l'espace symétrique $G(\mathbb{R})/K$ en rajoutant des composantes du type $G(\mathbb{R})/P(K)$ où $P(K) = M(K)AN$ est un parabolique réel (voir [**BL01**]). On va s'intéresser aux telles composantes qui viennent d'un parabolique rationnel P. On peut voir les quotients

$$\Gamma\backslash G(\mathbb{R})/P(K)$$

comme des épaississements du bord rationnel, décrivant certaines dégénérescences irrationnelles des structures de Hodge paramétrées par la variété de Shimura de départ. On va montrer (sur des exemples) que les ensembles $\Gamma\backslash G(\mathbb{R})/P(K)$ et surtout leurs revêtements

$$\mathrm{Sh}^{\pm} = \Gamma\backslash G(\mathbb{R})/M(K)A^{+}$$

et leur interprétation modulaire en termes d'algèbre linéaire ont un intérêt pour la généralisation du rêve de Manin en rang supérieur.

Plus précisément, on définira des ensembles de Shimura

$$\mathrm{Sh}(\mathrm{GSp}_{2n}, \mathscr{R}^{\pm})$$

et des points spéciaux dans ces ensembles et on munira les sous-ensembles spéciaux correspondants d'une action de Galois $\mathfrak{rec}$ donnée par la théorie du corps de classe.

Le rêve de Manin en rang supérieur peut alors (en première approche naïve) se formuler en disant qu'il existe une bonne notion de variété abélienne non commutative sur un corps de nombres, à multiplication par un corps quadratique F/E (avec $E/\mathbb{Q}$ un corps totalement réel) telle que

1. les périodes (K-theorie, cohomologie cyclique,...) soient les objets d'algèbre linéaire décrits dans ce document,
2. les modules algébriques soient fortement liés aux nombres de Stark,
3. les sous-espaces spéciaux soient naturellement munis d'une action de Galois $\mathfrak{nat}$,

et qu'on ait en plus

$$\mathfrak{rec} = \mathfrak{nat}.$$

On peut appeler ce rêve en rang supérieur le rêve de multiplication quadratique car les corps quadratiques y apparaîssant ne sont pas nécessairement totalement imaginaires ni totalement réels.

Bien que ce rêve soit pure spéculation, il pose quelques questions préliminaires, qui ont un intérêt indépendant et dont voici quelques exemples:

– Est-il possible de donner une définition adélique des nombres de Stark pour les corps quadratiques réels?
– Est-ce que les (générateurs des) sous-catégories stables par extensions des catégories dérivées de faisceaux cohérents sur une courbe elliptique définie sur $\mathbb{Q}$ (obtenues en généralisant légèrement la construction de Polishchuk/Schwarz [**Pol03**]) données par nos analogues réels de structures complexes sont définies sur le corps de classe du corps de multiplication réelle?

2. Rappels: corps de classe et variétés de Shimura

2.1. Corps de classe. On note $\hat{\mathbb{Z}} = \prod \mathbb{Z}_p$, $\mathbb{A}_f \cong \hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ et $\mathbb{A} = \mathbb{R} \times \mathbb{A}_f$ (1). Si $F/\mathbb{Q}$ est un corps de nombres, on note $\mathbb{A}_{f,F} = \mathbb{A}_f \otimes_{\mathbb{Q}} F$ et $\mathbb{A}_F = \mathbb{A} \otimes_{\mathbb{Q}} F$.

Si C est un groupe topologique commutatif, on note

$$\pi_0(C) := \lim_{\leftarrow} C/K$$

où la limite projective est prise sur les sous-groupes $K \subset C$ fermés d'indice fini (2).

Soit $C_F := \mathbb{A}_F^\times / F^\times$ (3). La théorie du corps de classe nous dit qu'il existe un morphisme naturel

$$\mathfrak{artin} : C_F \to \mathrm{Gal}(F^{ab}/F),$$

qui induit un isomorphisme $\mathfrak{artin} : \pi_0(C_F) \to \pi_0(\mathrm{Gal}(F^{ab}/F)) = \mathrm{Gal}(F^{ab}/F)$ et que ce morphisme permet de décrire toutes les extensions abéliennes de F. On note $\mathfrak{rec} : \mathrm{Gal}(F^{ab}/F) \to \pi_0(C_F)$ son inverse.

Soit $T = \mathrm{Res}_{F/\mathbb{Q}} \mathbb{G}_m$ le groupe $F^\times$ vu comme groupe algébrique sur $\mathbb{Q}$. Alors on a $C_F = T(\mathbb{Q}) \backslash T(\mathbb{A})$ et $\pi_0(T(\mathbb{Q}) \backslash T(\mathbb{A}))$ est un groupe profini qui peut s'écrire comme

$$\lim_{\leftarrow}{}_K T(\mathbb{Q}) \backslash T(\mathbb{A}) / T(\mathbb{R})^+ \times K$$

où K parcourt les sous-groupes compacts ouverts de $T(\mathbb{A}_f)$ (Voir Deligne, Variétés de Shimura, [**Del79**]).

(1) On peut aussi décrire les adèles comme la réunion des $\mathbb{A}_S := \mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p \times \times \prod_{p \notin S} \mathbb{Z}_p$ avec S fini. Les ouverts de $\mathbb{A}_S$ sont les $U \times \prod_{p \notin S} \mathbb{Z}_p$ avec U ouvert de $\mathbb{R} \times \prod_{p \in S} \mathbb{Q}_p$.

(2) Cette définition un peu tordue s'identifie dans le cas qu'on regarde d'après Deligne au π_0 muni de la topologie quotient. En effet, ce groupe de composantes connexes des classes d'idèles est profini car compact et totalement discontinu. Il est compact car quotient d'un groupe compact: $\pi_0(\mathbb{I}^1/\mathbb{Q}^\times)$

(3) La topologie induite par la topologie adélique sur les points d'une variété affine est bonne si cette variété est fermée. On prend donc la topologie induite par $\mathbb{A}^\times \mapsto \mathbb{A} \times \mathbb{A}, x \mapsto (x, x^{-1})$ car $\mathbb{G}_{m,\mathbb{Q}} \to \mathbb{A}^1_{\mathbb{Q}}$ (espace affine) n'est pas fermée.

Un théorème de Chevalet nous dit que

$$\varprojlim T(\mathbb{Q})\backslash T(\mathbb{A}_f)/K \cong \overline{T(\mathbb{Q})}\backslash T(\mathbb{A}_f).$$

Supposons que F est une extension quadratique de $\mathbb{Q}$. Si F est un corps totalement imaginaire, $T(\mathbb{R})^+ = T(\mathbb{R}) = \mathbb{C}^\times$ et de plus $T(\mathbb{Q})$ est fermé dans $T(\mathbb{A}_f)$ d'où on déduit

$$\pi_0(T(\mathbb{Q})\backslash T(\mathbb{A})) = T(\mathbb{Q})\backslash T(\mathbb{A}_f).$$

Si $F/\mathbb{Q}$ est une extension quadratique réelle, la composante $T(\mathbb{R})/T(\mathbb{R})^+$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ et il ne faut pas l'oublier.

L'espace topologique naturel dans lequel on peu plonger $T(\mathbb{R})/T(\mathbb{R})^+$ est l'espace

$$\mathscr{R}^\pm := \mathrm{GL}_2(\mathbb{R})/T(\mathbb{R})^+$$

des géodésiques orientées sur le demi-plan de poincaré.

2.2. Variété de Shimura. Une *pré-donnée de Shimura* est un couple (G, X) avec G un groupe algébrique réductif sur $\mathbb{Q}$ et X un $G(\mathbb{R})$-espace topologique (ou lisse) à gauche.

Si (G, X) est une pré-donnée de Shimura et $K \subset G(\mathbb{A}_f)$ est un sous-groupe compact ouvert, on peut lui associer l'*espace de Shimura fini*

$$\mathrm{Sh}_K(G, X) := G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K.$$

On appelle *espace de Shimura* la limite projective ensembliste

$$\mathrm{Sh}(G, X) := \varprojlim{}_K \mathrm{Sh}_K(G, X).$$

Soit $\mathbb{S} := \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m$. Une donnée de Shimura est un couple (G, X) avec G réductif connexe sur $\mathbb{Q}$ et $X \subset \mathrm{Hom}(\mathbb{S}, G_{\mathbb{R}})$ une $G(\mathbb{R})$-classe de conjugaison vérifiant quelques axiomes fondamentaux supplémentaires (voir Deligne [**Del79**]) qui impliquent notamment que $\mathrm{Sh}(G, X)$ est une variété algébrique quasi-projective (théorème de Bailly-Borel) qui admet un modèle canonique sur un corps de nombres (Travaux de Shimura, Deligne, Milne, Shi). Ces deux théorèmes a eux seuls montrent toute la puissance des axiomes de base des variétés de Shimura.

Par exemple, si $h_0 : \mathbb{S} \to \mathrm{GL}_{2,\mathbb{R}}$ est le morphisme donné sur les points réels par $z = a + ib \mapsto \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ et $\mathbb{H}^\pm$ est la classe de $\mathrm{GL}_2(\mathbb{R})$-conjugaison de h_0 alors $(\mathrm{GL}_2, \mathbb{H}^\pm)$ est la donnée de Shimura modulaire dont on a parlé dans l'introduction.

Nous allons maintenant nous intéresser à des pré-données de Shimura qui ne vérifient pas les axiomes de données de Shimura.

3. Géodésiques orientées et corps quadratiques réels

Rappelons par un tableau une analogie entre la courbe modulaire et l'espace des géodésiques sur icèle, essentiellement due à Gauss.

Définition 3.1. Soit M un $\mathbb{Z}$-module libre de rang 2, pour lequel on ne choisit pas à priori de base. Une *structure complexe* sur M est une décomposition $M_{\mathbb{C}} = F \oplus \bar{F}$ de $M_{\mathbb{C}}$ en deux sous-espaces complexes conjugués. Un *lilas* sur M est la donnée d'une décomposition $M_{\mathbb{R}} = F \oplus \tilde{F}$ de $M_{\mathbb{R}}$ en somme directe de deux droites et d'orientations sur ces deux droites données par le choix de deux demi-droites F^+ et $\tilde{F}^+$ sur ces dernières.

L'analogie qui nous intéresse se fait entre les espaces de modules de ces deux types d'objets d'algèbre linéaire. Elle comporte trois volets: *algèbre linéaire*, *géométrie analytique* et *géométrie algébrique*.

Algèbre linéaire

	structures complexes	lilas
en général	$M_{\mathbb{C}} = F \oplus \bar{F}$	$M_{\mathbb{R}} = F \oplus \tilde{F}$ et $F^+ \subset F, \tilde{F}^+ \subset \tilde{F}$
un exemple spécial	$M = \mathbb{Z}[\sqrt{-2}]$	$M = \mathbb{Z}[\sqrt{2}]$
isomorphismes d'algèbres	$\mathbb{Z}[\sqrt{-2}] \otimes_{\mathbb{Z}} \mathbb{C} \underset{alg}{\cong} \mathbb{C}_{\iota_1} \times \mathbb{C}_{\iota_2}$	$\mathbb{Z}[\sqrt{2}] \otimes_{\mathbb{Z}} \mathbb{R} \underset{alg}{\cong} \mathbb{R}_{\iota_1} \times \mathbb{R}_{\iota_2}$, $\mathbb{R}^+_{\iota_1}, \mathbb{R}^+_{\iota_2}$

Dans la dernière ligne du tableau, ι_1 et ι_2 sont les deux plongements de l'algèbre considérée, complexes pour la colonne de gauche et réels pour la colonne de droite. L'orientation sur les droites réelles est obtenue en prenant la composante connexe de l'identité dans le groupe des inversibles $\mathbb{R}^*$.

Définition 3.2. Un *morphisme* entre deux structures complexes (resp. lilas) est la donnée d'un morphisme $f : M_1 \to M_2$ entre les réseaux sous-jacents tel que $f_{\mathbb{C}}(F_1) \subset F_2$ (resp. $f_{\mathbb{R}}(F_1^+) \subset F_2^+$ et $f_{\mathbb{R}}(\tilde{F}_1^+) \subset \tilde{F}_2^+$).

Définition 3.3. Une *structure de niveau* N sur une structure complexe (resp. un lilas) de réseau sous-jacent M est un isomorphisme $M \otimes_{\mathbb{Z}} \mathbb{Z}/N\mathbb{Z} \xrightarrow{i} (\mathbb{Z}/N\mathbb{Z})^2$.

Nous nous intéressons maintenant à la géométrie des espaces de modules de ces objects d'algèbre linéaire.

Géomètrie analytique

	classique	dynamique
espace de modules	$\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})/\mathbb{C}^\times$	$\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})/(\mathbb{R}^{+\times})^2$
géométriquement	$X = \mathrm{PGL}_2(\mathbb{Z})\backslash\mathbb{H}$	{géodésiques sur X}
tour modulaire (tous niveaux)	$\varprojlim \Gamma(N)\backslash\mathrm{GL}_2(\mathbb{R})/\mathbb{C}^\times$	$\varprojlim \Gamma(N)\backslash\mathrm{GL}_2(\mathbb{R})/(\mathbb{R}^{+\times})^2$

Les groupes $\Gamma(N)$ considérés dans la limite projective sont les usuels groupes de congruence de niveau N, donnés par la suite exacte

$$1 \to \Gamma(N) \to \mathrm{GL}_2(\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to 1.$$

Cet aspect géométrique est celui qui semble bien connu par Gauss. Une des manières d'aborder la question de multiplication réelle de Manin est de chercher à remplir le tableau à trous suivant.

Géomètrie algébrique

	classique	quantique
structures linéaires	$M_{\mathbb{C}} = F \oplus \bar{F}$	$M_{\mathbb{R}} = F \oplus \bar{F}$ et $F^+ \subset F, \bar{F}^+ \subset \bar{F}$
réalisation géométrique	$E = M\backslash M_{\mathbb{C}}/\bar{F} \subset \mathbb{P}^2(\mathbb{C})$	?
par exemple	$E = \mathbb{C}/\mathbb{Z}[\sqrt{-2}] \subset \mathbb{P}^2(\mathbb{C})$	$? \sim \mathbb{R}/\mathbb{Z}[\sqrt{2}]$

On va maintenant expliquer plus en détails la deuxième colonne de nos tableaux *algèbre linéaire* et *géométrie analytique* en gardant cette analogie en tête.

Soit $h_1 : \mathbb{G}_{m,\mathbb{R}}^2 \to \mathrm{GL}_{2,\mathbb{R}}$ le morphisme donné par $(x, y) \mapsto \mathrm{diag}(x, y)$ et $\mathscr{R} \subset \mathrm{Hom}(\mathbb{G}_{m,\mathbb{R}}^2, \mathrm{GL}_{2,\mathbb{R}})$ sa $\mathrm{GL}_2(\mathbb{R})$-classe de conjugaison. Le stabilisateur de h_1 est le tore diagonal $T(\mathbb{R})$ de $\mathrm{GL}_2(\mathbb{R})$ donc

$$\mathscr{R} \cong \mathrm{GL}_2(\mathbb{R})/T(\mathbb{R}).$$

Les points de $\mathscr{R}$ correspondent aux couples de deux droites propres pour x et y. On peut les dessiner comme des points sur le bord $\mathbb{P}^1(\mathbb{R})$ du disque de poincaré. On munit maintenant ces points d'un sens (arrivée ou départ).

Soit $\mathscr{R}^\pm$ l'espace des couples (h, c) avec $h \in \mathscr{R}$ et $c \in \pi_0(\mathrm{im}(h(\mathbb{R})))$. On a alors

$$\mathscr{R}^\pm \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathscr{R}$$

et l'action de $\mathrm{GL}_2(\mathbb{R})$ par conjugaison agit seulement sur le deuxième facteur.

Définition 3.4. Le couple $(\mathrm{GL}_2, \mathscr{R}^\pm)$ est appelé la *donnée de rivage modulaire.*

Définition 3.5. Si $h \in \mathscr{R}$, on appelle *mauvais* [4] *groupe de Mumford-Tate de* h le plus petit sous-$\mathbb{Q}$-groupe algébrique $\mathrm{BMT}(h) \subset \mathrm{GL}_2$ contenant sur $\mathbb{R}$ l'image de h. Un point $h \in \mathscr{R}$ est dit *spécial* si $\mathrm{BMT}(h)$ est un tore non scindé.

On montre facilement que si h est spécial, $\mathrm{BMT}(h)$ peut s'écrire $\mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_m$ avec $E/\mathbb{Q}$ quadratique totalement réel [5].

On peut ainsi compléter notre analogie par un tableau intitulé *structure spéciales* qui donne les idées clefs de la question de multiplication réelle.

Structures spéciales

	multiplication complexe	multiplication réelle
structures linéaires	$M_{\mathbb{C}} = F \oplus \bar{F}$ $\mathrm{End}(M, F, \bar{F}) \otimes_{\mathbb{Z}} \mathbb{Q}$ quadratique imaginaire	$M_{\mathbb{R}} = F \oplus \tilde{F}$ et $F^+ \subset F, \tilde{F}^+ \subset F$ $\mathrm{End}(M, F, \tilde{F}) \otimes_{\mathbb{Z}} \mathbb{Q}$ quadratique réel
par exemple	$M = \mathbb{Z}[\sqrt{-2}]$	$M = \mathbb{Z}[\sqrt{2}]$
géométrie algébrique	courbes elliptiques à multiplication complexe	?
structures de niveau	points de torsion	?
modules algébriques	valeurs de fonction j et fonctions elliptiques	? $\sim$ nombres de stark

On peut dessiner sur le disque de Poincaré la géodésique liant $\sqrt{2}$ et $-\sqrt{2}$ qui est une géodésique spéciale.

Si $h \in \mathscr{R}$ est un tel point spécial de groupe de Mumford–Tate $T = \mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_m$, on lui associe la sous-donnée

$$s : (T, Z = \pi_0(T(\mathbb{R}))) \to (\mathrm{GL}_2, \mathscr{R}^{\pm}).$$

Comme vu précédemment, on a

$$\mathrm{Sh}(T, Z) = \pi_0(T(\mathbb{Q})\backslash T(\mathbb{A}))$$

s'identifie au groupe des composantes connexes du groupe de classes d'idèles.

On munit donc l'image de $\mathrm{Sh}(s)$ d'une action notée $\mathfrak{rec}$ de $\mathrm{Gal}(E^{ab}/E)$ donnée par l'inverse de l'isomorphisme du corps de classe.

---

(4) Les bons groupes de Mumford-Tate sont donnés par les enveloppes réductives et ont un intérêt indépendant pour des questions de dynamique.

(5) Par exemple: considérons $d > 1$ un entier positif sans facteur carré. Soit $g := \left(\begin{smallmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{smallmatrix}\right)$. En conjuguant h_0 par g, on obtient la matrice $h' = \left(\begin{smallmatrix} a & b \\ db & a \end{smallmatrix}\right)$ avec $a = \frac{x+y}{2}$ et $b = \frac{x-y}{2\sqrt{d}}$. Le groupe des matrices de la forme $\left(\begin{smallmatrix} a & b \\ db & a \end{smallmatrix}\right)$ avec a et b rationnels est un groupe algébrique sur $\mathbb{Q}$ qui est le groupe de Mumford-Tate de h'. C'est en fait $\mathrm{Res}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}\mathbb{G}_m$.

Rêve 3.6 **("Alterstraum" de Manin: multiplication réelle)**
On espère que cette action peut-être décrite de manière plus naturelle grâce à une interprétation modulaire de $\mathrm{Sh}(T, Z)$ *en termes de géométrie algébrique non commutative, liée aux nombres de Stark pour ce corps quadratique.*

4. Dans les espaces de modules de variétés abéliennes

On souhaite comprendre ce que le rêve de Manin signifie pour un corps comme $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$. On remarque qu'on a

$$\mathbb{Q}(\sqrt[4]{2}) \otimes_{\mathbb{Q}} \mathbb{R} \underset{\mathbb{R}-alg}{\cong} \mathbb{C} \times \mathbb{R} \times \mathbb{R}$$

et ce corps quadratique n'est ni totalement réel, ni totalement imaginaire.

Soit $\mathbb{D}_k \subset (\mathbb{G}_{m,\mathbb{R}}^2)^k$ le sous-groupe des $(x_i, y_i)_{i=1,\ldots,k}$ tels que $x_i y_i = x_j y_j$ pour tout $i, j \in \{1, \ldots, k\}$. On remarque que $\mathbb{D}_k$ peut être vu comme le tore maximal de $\mathrm{GSp}_{2k,\mathbb{R}}$. Soit $\mathbb{T}_k \subset \mathbb{S} \times \mathbb{D}_k$ le sous-groupe des $(z, (x_i, y_i))$ tels que $z\bar{z} = x_i y_i$ pour tout $i \in \{1, \ldots, k\}$. Soit $\mathbb{T} := \varprojlim \mathbb{T}_k$ où les projections $\mathbb{T}_{k+1} \to \mathbb{T}_k$ sont données par oubli du dernier facteur $\mathbb{G}_{m,\mathbb{R}}^2$. On note $\pi_k : \mathbb{T} \to \mathbb{T}_k$ la projection naturelle.

On a un morphisme diagonal $w : \mathbb{G}_m \to \mathbb{T}$ dit de poids et un autre morphisme $\mu : \mathbb{G}_{m,\mathbb{C}} \to \mathbb{T}_{\mathbb{C}}$ dit de Hodge donné par $x \mapsto ((x, 1), \ldots, (x, 1))$.

Soit $G_n \subset \mathrm{GL}_2^n$ le sous-groupe des matrices (g_i) telles que $\det(g_i) = \det(g_j)$ pour tout i, j.

Soit

$$f_n : G_n \to \mathrm{GSp}_{2n}$$

le morphisme donné pour $(g_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right))$ par la matrice

$$\begin{pmatrix} \mathrm{diag}(a_i) & \mathrm{diag}(b_i) \\ \mathrm{diag}(c_i) & \mathrm{diag}(d_i) \end{pmatrix}$$

On note $h_0 : \mathbb{S} \to \mathrm{GL}_{2,\mathbb{R}}$ le morphisme standard donné sur les points réels par $z = a + ib \mapsto \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ et $h_1 : \mathbb{G}_{m,\mathbb{R}}^2 \to \mathrm{GL}_{2,\mathbb{R}}$ le morphisme diagonal donné par $(x, y) \mapsto \mathrm{diag}(x, y)$.

Soit $k_0 + k_1 = n$ une partition de n. On note $h_{k_0,k_1} : \mathbb{T}_{k_1} \to G_n \subset \mathrm{GL}_{2,\mathbb{R}}^n$ le morphisme donné par

$$h_{k_0,k_1} := (\underbrace{h_0, \ldots, h_0}_{k_0}, \underbrace{h_1, \ldots, h_1}_{k_1}).$$

Soit $h_{S,k_0,k_1} : \mathbb{T} \to \mathrm{GSp}_{2n}$ le morphisme donné par $h_{S,k_0,k_1} = f_n \circ h_{k_0,k_1} \circ \pi_{k_1}$ et $\mathscr{R}_{k_0,k_1}$ la $\mathrm{GSp}_{2n}(\mathbb{R})$-classe de conjugaison de ce morphisme dans $\mathrm{Hom}(\mathbb{T}, \mathrm{GSp}_{2n})$.

On remarque que pour $h \in \mathscr{R}_{k_0,k_1}$, le morphisme $h \circ w : \mathbb{G}_{m,\mathbb{R}} \to \mathrm{GSp}_{2n}$ est simplement le plongement diagonal et est donc indépendant de h.

Dans le cas $k_1 = 0$, on retrouve l'espace de Siegel classique $\mathscr{S}^{\pm}$ et dans le cas $k_0 = 0$, on trouve

$$\mathscr{R}_{0,n} \cong \mathrm{GSp}_{2n}(\mathbb{R})/\mathbb{D}_n(\mathbb{R}).$$

Rappelons que le couple $(\mathrm{GSp}_{2n}, \mathscr{S}^{\pm})$ est appelée *donnée de Shimura de Siegel*. La variété de Shimura correspondante est l'espace de module des variétés abéliennes à structure de niveau infinie.

On note $\mathscr{R}^{\pm}_{k_0,k_1}$ l'espace des morphismes h munis d'une composante connexe $c \in \pi_0(\mathrm{im}(h(\mathbb{T}(\mathbb{R}))))$.

Définition 4.1. Le couple $(\mathrm{GSp}_{2n}, \mathscr{R}^{\pm}_{k_0,k_1})$ est appelé *donnée de rivage de type* (k_0, k_1) de la donnée de Siegel $(\mathrm{GSp}_{2n}, \mathscr{S}^{\pm})$.

Définition 4.2. Si $h \in \mathscr{R}_{k_0,k_1}$, on appelle *mauvais* [(6)] *groupe de Mumford–Tate de h* le plus petit sous-$\mathbb{Q}$-groupe algébrique $\mathrm{BMT}(h) \subset \mathrm{GSp}_{2n}$ contenant sur $\mathbb{R}$ l'image de h. Un point $h \in \mathscr{R}_{k_0,k_1}$ est dit *spécial* si son groupe de Mumford–Tate est un tore T tel que $T/w(\mathbb{G}_m)$ soit anisotrope sur $\mathbb{Q}$ [(7)].

Si h est un point spécial, on a

$$T(\mathbb{R})/T(\mathbb{R})^+ = h(\mathbb{T}(\mathbb{R}))/h(\mathbb{T}(\mathbb{R}))^+$$

d'où un plongement

$$T(\mathbb{R})/T(\mathbb{R})^+ \subset \mathscr{R}^{\pm}_{k_0,k_1}$$

donné par $c \mapsto (h, c)$.

On peut maintenant refaire la construction de Deligne dans ce cadre. On a un morphisme $\mu_h := h_{\mathbb{C}} \circ \mu : \mathbb{G}_{m,\mathbb{C}} \to T_{\mathbb{C}}$ dit de Hodge et le corps reflex $E(h)$ de h est le corps de définition de ce morphisme. Si $F = E(h)$, on a

$$\mu_h : \mathbb{G}_{m,F} \to T_F$$

et on construit

$$\mathrm{NR}(\mu_h) : \mathrm{Res}_{F/\mathbb{Q}}\mathbb{G}_m \to \mathrm{Res}_{F/\mathbb{Q}}T_F \overset{\mathrm{Nm}}{\to} T.$$

On a

$$\pi_0(\mathrm{NR}(\mu_h)) : \pi_0(C_F) \to \pi_0(T(\mathbb{Q})\backslash T(\mathbb{A})).$$

---

(6) Les bons groupes de Mumford–Tate sont donnés par les enveloppes réductives. Il semble plausible que ces groupes soient définis de manière unique (c'est le cas si $k_0 = 0$ ou $k_1 = 0$). Il serait intéressant de connaître leur signification pour des questions de dynamique.

(7) Cette condition est automatiquement vérifiée sur $\mathbb{R}$ dans le cas des variétés abéliennes car $h(i)$ est une involution de Cartan de $(T/w(\mathbb{G}_m))_{\mathbb{R}}$.

Soit h un point spécial de groupe de Mumford–Tate T, on munit canoniquement le sous-espace

$$\mathrm{Sh}(T, Z) \subset \mathrm{Sh}(\mathrm{GSp}_{2n}, \mathscr{R}^{\pm}_{k_0,k_1})$$

avec $Z = \pi_0(T(\mathbb{R}))$ d'une action de Galois notée $\mathfrak{rec}$ donnée par

$$g : x \mapsto (\pi_0(\mathrm{NR}(\mu_h)) \circ \mathfrak{rec}(g)) \cdot x.$$

***Rêve 4.3* (de multiplication quadratique).** *On espère que cette action de Galois peut-être construite de manière plus naturelle en interprétant* $\mathrm{Sh}(T, Z)$ *comme un espace de modules défini sur un corps de nombres d'analogues non commutatifs des variétés abéliennes dont les modules algébriques seraient liés aux nombres de Stark pour* F.

Regardons notre exemple de départ de ce point de vue. Notons $F' = \mathbb{Q}(\sqrt[4]{2})$ et $E = \mathbb{Q}(\sqrt{2})$. Le choix d'une E-base de F' nous donne un plongement $\mathrm{Res}_{F'/\mathbb{Q}}\mathbb{G}_m \subset \mathrm{Res}_{E/\mathbb{Q}}\mathrm{GL}_2$. On note $T \subset G$ l'inclusion correspondante des sous-groupes donnés par les matrices de déterminant dans $\mathbb{G}_{m,\mathbb{Q}}$. On remarque que $T \cong \mathrm{Res}_{F'/\mathbb{Q}}\mathbb{G}_m/(\mathrm{Res}_{E/\mathbb{Q}}\mathbb{G}_m)^{(1)}$. On peut plonger G dans $\mathrm{GSp}_{4,\mathbb{Q}}$. On a $T_{\mathbb{R}} \cong \mathbb{T}_1$ et on note $h : \mathbb{T} \to \mathrm{GSp}_{4,\mathbb{R}}$ le morphisme correspondant. Alors $h \in \mathscr{R}_{1,1}$ et T est clairement le groupe de Mumford–Tate de h. Le morphisme $\mu_h : \mathbb{G}_{m,\mathbb{C}} \to T_{\mathbb{C}}$ est défini sur le corps $F = \mathbb{Q}(i\sqrt[4]{2}, \sqrt[4]{2})$.

5. Littérature

La littérature regarde essentiellement des cas de rang 1. Les gens s'intéressent au bord irrationnel

$$\mathrm{PGL}_2(\mathbb{Z})\backslash\mathbb{P}^1(\mathbb{R})$$

qui a l'air d'être un espace moins naturel que le rivage

$$\mathrm{GL}_2(\mathbb{Z})\backslash\mathrm{GL}_2(\mathbb{R})/\mathbb{R}^{+\times 2}$$

de notre point de vue de la théorie du corps de classe et des groupes algébriques.

On découpe la littérature en deux approches:

- l'approche *périodes* qui part des objets d'algèbre linéaire et construit des objets de géométrie non commutative correspondants,
- l'approche *nombres de Stark* qui part des nombres de Stark et construit des objets de géométrie non commutative correspondants.

Le rêve est qu'il existe un bon point de rencontre entre ces deux approches. La littérature s'énumère ainsi.

1. Connes, Manin, Marcolli [**Con85, Man, MM02**]: approche *periodes*: les aspects analytiques peuvent être donnés par les tores non commutatifs (K-theorie, HC).
2. Polishchuk [**Pol02**]: approche *periodes*: les tores non commutatifs analytiques sont des “variétés projectives”. Annonce en rang supérieur.
3. Manin [**Man**]: approche *nombres de Stark*: fonctions theta non commutatives et nombres de Stark.
4. Darmon: autre approche: points de Hegner-Stark sur les courbes elliptiques sur $\mathbb{Q}$ conjecturalement définis sur des corps de classe.
5. Connes-Marcolli-Ramachandran (non publié): états KMS et multiplication complexe.

Appendix A
Rappels sur la multiplication complexe

Ce paragraphe est essentiellement le résultat de mes discussions avec Gabor Wiese que je remercie pour son aide. Soit F un corps de nombres. Soit $\mathscr{E}\ell\ell(F)_{\mathbb{Q}}$ la catégorie dont les objets sont les courbes elliptiques sur F et les morphismes sont donnés par $\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Q}$. On note une courbe elliptique E vue comme objet de $\mathscr{E}\ell\ell(F)_{\mathbb{Q}}$ comme $E \otimes \mathbb{Q}$.

Pour E/F une courbe elliptique, on note

$$T(E) := \lim_{\leftarrow}{}_n E[n](\bar{F}) \text{ et } V(E) := T(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

avec $E[n]$ le noyau de la multiplication par n dans E.

On note $\mathbb{A}_f := \hat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ avec $\hat{\mathbb{Z}}$ le complété de $\mathbb{Z}$ pour les sous-groupes d'indice fini. On sait que $T(E) \cong \hat{\mathbb{Z}}^2$ et donc

$$V(E) \cong \mathbb{A}_f^2.$$

Soit $F/\mathbb{Q}$ un corps quadratique totalement imaginaire. Une courbe elliptique est dite à multiplication complexe par F si on se fixe un morphisme injectif $F \to \mathrm{End}(E \otimes \mathbb{Q})$. Si on note $\mathbb{A}_{f,F} := \mathbb{A}_f \otimes_{\mathbb{Q}} F$, on peut montrer que $V(E)$ est un $\mathbb{A}_{f,F}$-module de rang 1.

On note $S_F(\overline{\mathbb{Q}})$ l'espace des classes d'isomorphismes de triplets

$$(E \otimes \mathbb{Q}, \alpha : F \to \mathrm{End}(E \otimes \mathbb{Q}), \psi : \mathbb{A}_{f,F} \to V(E))$$

avec ψ un isomorphisme de $\mathbb{A}_{f,F}$-modules et α une injection.

On a une action naturelle de $\mathbb{A}_{f,F}^{\times}$ sur $S_F(\overline{\mathbb{Q}})$ et on peut montrer que le stabilisateur d'un points est $F^{\times}$, ce qui fait de $S_F(\overline{\mathbb{Q}})$ un $C_F := \mathbb{A}_{f,F}^{\times}/F^{\times}$-torseur.

D'autre part, $S_F(\overline{\mathbb{Q}})$ est muni d'une <u>action naturelle</u> de $\mathscr{G}_F^{ab} := \mathrm{Gal}(F^{ab}/F)$ et ces deux actions commutent, i.e. $(\sigma \cdot x) \times y = \sigma \cdot (x \times y)$.

Fixons un point $x \in S_F(\overline{\mathbb{Q}})$, donc un isomorphisme $C_F \cong S_F(\overline{\mathbb{Q}})$. Ceci nous permet de définir un morphisme [8]

$$\Phi : \mathscr{G}_F^{ab} \to C_F$$

par $\Phi(\sigma) = \sigma \cdot 1$.

On a d'autre part l'application d'artin donnée par le corps de classe $\mathfrak{artin}$: $C_F \to \mathscr{G}_F^{ab}$.

Théorème A.1 **(Principal: Multiplication complexe)**
La composition

$$C_F \xrightarrow{\mathfrak{artin}} \mathscr{G}_F^{ab} \xrightarrow{\Phi} C_F$$

envoie $x \in C_F$ *sur* x^{-1}.

References

[BL01] A. Borel & J. Lizhen – *Compactifications of locally symmetric spaces*, IAS/Michigan, 2001, Prepublication, june 2001.

[Con85] A. Connes – Noncommutative differential geometry, *Inst. Hautes Études Sci. Publ. Math.* (1985), no. 62, p. 257–360.

[Del79] P. Deligne – Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Amer. Math. Soc., Providence, R.I., 1979, p. 247–289.

[Man] Y. I. Manin – Real Multiplication and noncommutative geometry, `arXiv:math.AG/0202109`.

[MM02] Y. I. Manin & M. Marcolli – Continued fractions, modular symbols, and noncommutative geometry, *Selecta Math. (N.S.)* **8** (2002), no. 3, p. 475–521.

[Pol02] A. Polishchuk – Noncommutative 2-tori with real multiplication as noncommutative projective varieties, *arXiv* (2002), no. http://fr.arXiv.org/abs/math.AG/0212306.

[Pol03] ______, Classification of holomorphic vector bundles on noncommutative two-tori, *arXiv* (2003), no. http://fr.arXiv.org/abs/math.QA/0308136.

[8] On a $\Phi(\sigma) \times \Phi(\tau) = (\sigma \cdot 1) \times (\tau \cdot 1) = \sigma \cdot (1 \times (\tau \cdot 1))) = \sigma \cdot (\tau \cdot 1) = (\sigma\tau) \cdot 1$.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 159–163
Universität Göttingen, 2004

CONSTRUCTION OF CURVES WITH A JACOBIAN OF GIVEN CM-TYPE

A. Weng
Johannes Gutenberg Universität Mainz Staudingerweg 9, D-55128 Mainz, Germany • *E-mail :* weng@mathematik.uni-mainz.de

Abstract. We discuss an algorithm for the construction of low genus curves whose Jacobians have complex multiplication by a given CM-field K. We present examples for genus 2 and 3.

1. Introduction

Let C be a smooth projective curve of genus $g \geq 1$ over a field κ and let J_C be the Jacobian of C. Recall that the Jacobian J_C is an abelian variety of dimension g whose group of λ-rational points for every field extension λ/κ is isomorphic to the group of λ-rational divisor classes of degree 0 of the curve C. In our talk, the ground field κ will either be finite, a number field or the field of complex numbers.

Suppose that J_C has a commutative endomorphism algebra over $\overline{\kappa}$ (where $\overline{\kappa}$ denotes the algebraic closure of κ) whose degree over $\mathbb{Q}$ is as large as possible. In this case, $\mathrm{End}(J_C) \otimes \mathbb{Q}$ is a CM field K (i.e., an imaginary quadratic extension of a totally real field) of degree $2g$ where g is the genus of the curve C and

June 24th, 2004.

$\mathrm{End}(J_C)$ itself is an order in K.

In this talk, we describe an algorithm for the construction of curves of genus $g \leq 3$ whose Jacobian has complex multiplication by the maximal order $\mathcal{O}_K$ where K is a CM field of degree $2g$.
Before going into the details of the algorithm, we mention an application to cryptography:
Let $\kappa = \mathbb{F}_q$ be a finite field. In this case, the group of $\mathbb{F}_q$-rational points, $J_C(\mathbb{F}_q)$, is a *finite* abelian group and we can consider the discrete logarithm problem in this group, i.e., given two elements P, $Q \in J_C(\kappa)$ with $Q \in \langle P \rangle$, find an integer r such that $rP = Q$. There are many cryptosystems based on the difficulty of the discrete logarithm problem such as Diffie-Hellmann key exchange or El-Gamal encryption. To ensure the security of a cryptosystem based on the discrete logarithm problem in a finite abelian group we have to be aware that the group order contains a large prime factor [**PH78**]. More precisely, the group order should either be prime or a product of a prime and a small number. For curves of genus $g \geq 2$, finding the group order seems to be a non-trivial task. Note that we need to find the number of elements in a group which has around 2^{160} elements since this is the size which is commonly accepted to be secure.
If we know the endomorphism ring of the Jacobian, counting the elements becomes easy. For simplicity, we restrict to a finite prime field $\kappa = \mathbb{F}_p$.
Consider the Frobenius endomorphism π_p on the Jacobian. If J_C has endomorphism ring $\mathrm{End}(J_C) \simeq \mathcal{O}_K$, there exists $w \in \mathcal{O}_K$ which corresponds to $\pi \in \mathrm{End}(J_C)$. It is well-known that w is an element whose absolute value is equal to $\sqrt{p}$, hence

$$w\overline{w} = p. \tag{1}$$

If J_C is simple, then $\mathbb{Q}(w) = K$.
We easily see that we have only finitely many choices for $w \in \mathcal{O}_K$ satisfying (1).
The group order of $J_C(\mathbb{F}_p)$ is now given by

$$\#\ker(\pi - \mathrm{id}) = \mathrm{Norm}_{K/\mathbb{Q}}(w-1).$$

Since we have only finitely many possibilities for w, we get only finitely many possibilities for the group order of $J_C(\mathbb{F}_p)$. We choose random elements in $J_C(\mathbb{F}_p)$ and test whether they have the right order. In most cases, this will be enough to determine the order of the Jacobian.

2. The algorithm

We describe the rough scheme of an algorithm which, given a CM field K, computes a curve whose Jacobian has complex multiplication by $\mathcal{O}_K$.

1. Compute a complete set (up to isomorphism) of isomorphism classes of all simple principally polarized abelian varieties over $\mathbb{C}$ having complex multiplication by $\mathcal{O}_K$. We represent each isomorphism class by an element $\Omega_i \in \mathbb{H}_g$, the Siegel upper half plane. The abelian variety is then given by $\mathbb{C}^g/\Lambda$.
   Let s be the number of isomorphism classes.
   The next steps are done for all s isomorphism classes.
2. Compute numerical approximations of a *certain* set of values of theta functions with characteristics
   $$\theta \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix} (\Omega, 0) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i (n+\delta)^t \Omega (n+\delta) + 2(n+\delta)^t(\varepsilon)).$$
   where $\delta, \varepsilon \in (\mathbb{Q}/\mathbb{Z})^g$.
3. Using the values of theta functions compute absolute invariants which classify the isomorphism class of the curve uniquely. Let (K, Φ) be the CM-type. The absolute invariants lie in a number field k_0^* which is a class field over the reflex field K^* of (K, Φ). If the precision is chosen high enough, we recover the invariants from their numerical approximations.
   If we want to compute a curve over a finite field, we can now reduce the invariants modulo a prime ideal $\mathfrak{P}$ in k_0^* to obtain invariants in the finite field isomorphic to $\mathcal{O}_{k_0^*}/\mathfrak{P}$.
4. Compute the curve with the given invariants.

Remark 1.

1. In the case of elliptic curves, the algorithm is well-known (cf. [**AM93**]).
2. The complexity of the algorithm depends on the discriminant and the class number of the CM field K.
3. If p satisfies a relative norm equation, i.e., $p = w\overline{w}$, using class field theory we can show that there exists a prime $\mathfrak{P} \in k_0^*$ of degree 1 over p. If the set of simple principally polarized abelian varieties is non-empty, we find a curve whose field of moduli is $\mathbb{F}_p$ and whose Jacobian has complex multiplication by $\mathcal{O}_K$.
4. The set of simple principally polarized abelian varieties with complex multiplication by $\mathcal{O}_K$ might be empty. For instance, if K is a quartic CM field whose Galois group is the Kleinian 4-group there does not exist a primitive CM type. In this case, every principally polarized abelian

variety is isogenous to the product of two elliptic curve with complex multiplication. We can still try to use the algorithm to construct Jacobians with complex multiplication by $\mathcal{O}_K$, but in some cases there does not exist a Jacobian, e.g., for $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$.

3. An example: curves of genus 2

We give some details of the algorithm in the case $g = 2$ (cf. [**Wen03**]). In our talk we also discussed two special cases with $g = 3$: hyperelliptic curves and Picard curves (cf. [**Wen01, KW03**]).
For the first step we need to implement the construction of complex tori with complex multiplication by $\mathcal{O}_K$ given in [**Shi98**]. This is theoretically well-understood, the subtleties lie in the implementation and we will not give the details here.
In the second step, we compute all 10 even theta characteristics, i.e.,

$$\theta \begin{bmatrix} \delta \\ \varepsilon \end{bmatrix} (\Omega, 0) \text{ with } \delta, \varepsilon \in \left(\frac{1}{2}\mathbb{Z}/\mathbb{Z}\right)$$

and $\delta^t \varepsilon \equiv 0 \mod 2$. From the values of the theta functions we can compute the values of the generating functions j_1, j_2 and j_3 of the field of modular functions of degree 2 at Ω. They are absolute invariants of the isomorphism class, i.e., two principally polarized abelian varieties $A \simeq \mathbb{C}/\Omega$, $A' \simeq \mathbb{C}/\Omega'$ are isomorphic if and only if $j_k(\Omega) = j_k(\Omega')$ for $k = 1, 2, 3$. are isomorphic if and only if they have the same invariants [**Igu60**].
If we compute $j_k^{(i)}$ for all isomorphism classes $i = 1, \ldots, s$, we can construct the class polynomials

$$H_k(X) = \prod_{i=1}^{s} (X - j_k^{(i)}), k = 1, 2, 3.$$

These polynomials have rational coefficients. Contrarily to the elliptic curve case, the coefficients are in general not integers. The size of the denominator and the size of the primes dividing the denominator depend on the discriminant of the CM field K. If K has a small discriminant (in practice this is always true), the denominator can be recovered using the continued fraction algorithm.
The last step can now be solved using an algorithm due to Mestre (if $\mathrm{Aut}(C) \simeq \mathbb{Z}/2\mathbb{Z}$, [**Mes91**]), and its modification by Cardona (for larger automorphism groups, [**Car03**]). Note that a primitive CM field (i.e., a CM field which is either non-normal or has a cyclic Galois group) usually has trivial automorphism group except for the case $K = \mathbb{Q}(\zeta_5)$ which is well-known.

In our talk we also gave examples of curves of genus 2 and 3 over large finite fields which were constructed using the algorithm above and its modification for genus 3.

References

[AM93] A. O. L. Atkin & F. Morain – Elliptic curves and primality proving, *Math. Comp.* **61** (1993), no. 203, p. 29–68.

[Car03] G. Cardona – On the number of curves of genus 2 over a finite field, *Finite Fields Appl.* **9** (2003), no. 4, p. 505–526.

[Igu60] J.-i. Igusa – Arithmetic variety of moduli for genus two, *Ann. of Math. (2)* **72** (1960), p. 612–649.

[KW03] K. Koike & A. Weng – Construction of CM-Picard curves, 2003, to appear in *Math. Comp.*

[Mes91] J.-F. Mestre – Construction de courbes de genre 2 à partir de leurs modules, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, p. 313–334.

[PH78] S. C. Pohlig & M. E. Hellman – An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, *IEEE Trans. Information Theory* **IT-24** (1978), no. 1, p. 106–110.

[Shi98] G. Shimura – *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1998.

[Wen01] A. Weng – A class of hyperelliptic CM-curves of genus three, *J. Ramanujan Math. Soc.* **16** (2001), no. 4, p. 339–372.

[Wen03] ———, Constructing hyperelliptic curves of genus 2 suitable for cryptography, *Math. Comp.* **72** (2003), no. 241, p. 435–458.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 165–173
Universität Göttingen, 2004

A GALOIS CODE FOR VALUATIONS

J. Königsmann
Mathematisches Institut, Eckerstr. 1, D-79104 Freiburg, Germany
E-mail : Jochen.Koenigsmann@unibas.ch

Abstract. Valuations on a field K are encoded in the absolute Galois group G_K of K: They are in one-to-one correspondence with the conjugacy classes of decomposition subgroups of G_K which (apart from few exceptions) can be characterized in group theoretic terms. Roughly speaking, decomposition subgroups of G_K are maximal subgroups of G_K with a Sylow-subgroup containing a non-trivial abelian normal subgroup. We sketch the main ideas of the proof.

1. Introduction

By Artin-Schreier theory, orderings are encoded in the absolute Galois group $G_K := Gal(K^{sep}/K)$ of a field K: they are in one-to-one correspondence with conjugacy classes of involutions (elements of order 2) in G_K.

The goal of this note is to show how one can draw a similar picture w.r.t. (general Krull) valuations. (For details see [K4]).

Unfortunately, this cannot always be achieved. For example, the field $\mathbf{C}((t))$ of formal power series over $\mathbf{C}$ has the same absolute Galois group as any finite

June 29th, 2004.

field $\mathbf{F}_q$, so the t-adic valuation on $\mathbf{C}((t))$ is not reflected in $G_{\mathbf{C}((t))} \cong G_{\mathbf{F}_q} \cong \hat{\mathbf{Z}}$, because $\mathbf{F}_q$ has no non-trivial valuation at all.

To exclude this and a few other exceptional cases we have to restrict ourselves to tamely branching valuations. Denoting for a valued field (K, v) the value group (written additively), the valuation ring, the maximal ideal, and the residue field by Γ_v, $\mathscr{O}_v$, $\mathscr{M}_v$ and $Kv := \mathscr{O}_v/\mathscr{M}_v$, this is defined as follows:

Definition 1.1. *A valuation v on K is called* **tamely branching** *(***at** *p) if there is a prime $p \neq char\, Kv$ with $d_p(v) := \dim_{\mathbf{F}_p} \Gamma_v/p\Gamma_v \geqslant 1$, and, if $d_p(v) = 1$ then $p^2 \mid \sharp G_{Kv}$ (equivalently, $d_p(v) \geqslant 1 < d_p(v) + vcd_p(G_{Kv})$).*

For the characterization of valuations in group theoretic terms we will work with the

Definition 1.2. *A profinite group is called a* **Hensel group** *if it has a non-procyclic Sylow subgroup $P \not\cong \mathbf{Z}_2 \rtimes (\mathbf{Z}/2\mathbf{Z})$ with a non-trivial abelian normal subgroup $N \triangleleft P$.*

The main result is the following

Theorem 1.3. *(Theorem 1 in [K4]) A field K is henselian w.r.t. a tamely branching valuation iff G_K is a Hensel group.*

Note that decomposition subgroups of G_K are just the absolute Galois groups of henselisations of K, that henselisations w.r.t. tamely branching valuations are tamely branching, that the henselisations of K are the minimal henselian extensions of K, and that for a fixed valuation on K, all henselisations are conjugate. Together with the theorem above, this leads to the rough picture that valuations on K are in one-to-one correspondence with conjugacy classes of maximal hensel subgroups of G_K. This picture is correct if, e.g., all tamely branching valuations on G_K are rank-1 valuations (i.e., valuations with archimedean value group). In general it may happen that two distinct valuations have the same henselisations, and then G_K does not see the difference. So the general picture is a bit more complicated (see Theorem 2 and 3 of [K4]).

Let us also remark that one direction in the theorem is an easy application of general ramification theory. If (K, v) is henselian valued and if V and T are the ramification resp. inertia subgroup of G_K (w.r.t. the unique prolongation of v to K^{sep}) then V and T are normal subgroups of G_K, V is the unique Sylow-l subgroup of T, where $l = char\, Kv$ (and $V = 1$ for $l = 0$), T/V is torsion-free abelian with Sylow-p subgroups of the form $\mathbf{Z}_p^{d_p(v)}$ and $G_K/T \cong G_{Kv}$. So if v is a henselian valuation on K, tamely branching at p, then the unique prolongation w of v to the fixed field of a Sylow-p subgroup P of G_K remains henselian and $d_p(w) = d_p(v)$. The inertia subgroup N of P is then a normal subgroup of the form $\mathbf{Z}_p^{d_p(v)}$, i.e., non-trivial and abelian. Hence G_K is a hensel group.

2. Tools

When one looks at the theorem it may seem surprising that a Sylow subgroup of G_K already knows such a rare property like henselianity of K. We will see, however, that this is a general phenomenon (Lemma 2.1). It reduces the theorem to the case where G_K is a pro-p group.

In this special case we can construct valuations from non-trivial normal abelian subgroups because these subgroups produce via some kind of local reciprocity law (using norms) 'rigid elements' in K, i.e., elements $a \in K$ such that $\dot{K}^p + a\dot{K}^p = \dot{K}^p \cup a\dot{K}^p$. If (K, v) is henselian and tamely branching at p, then any $a \in K$ with $v(a) \notin p\Gamma_v$ is rigid in this sense. Conversely, it turns out that rigid elements are almost always of this type, that one can construct tamely branching valuations from (sufficiently many) rigid elements in K (Lemma 2.2).

2.1. Henseling down. Henselianity always goes up to algebraic extensions: If (K, v) is henselian and F/K is an algebraic extension then the unique prolongation of v to F is again henselian. In few special cases, Henselianity also goes down:

Lemma 2.1. *Let F/K be an algebraic extension with $F \neq F^{sep}$, and let v be a henselian valuation on F which is comparable to any other henselian valuation on F, and if Fv is real closed assume that no proper coarsening of v has real closed residue field. Assume that*

1. *$G_F \triangleleft G_K$, i.e., F/K is normal, or*
2. *$[F : K] < \infty$ or*
3. *G_F is a Sylow-p subgroup of G_K.*

Then $v_K := v\,|_K$ is henselian.

Proof. Recall that a field may have several henselian valuations, but most of them are comparable (i.e., there is an inclusion of valuation rings): Any two henselian valuations with residue field non-separably-closed are comparable and they are all coarser (i.e. the valuation ring is larger) than those with separably closed residue field (this generalizes an old theorem of F.K. Schmidt, cf. [**EE77**]). So the condition that v be comparable to any other henselian valuation on F is equivalent to the condition that for any proper coarsening of v the residue field is non-sepaparbly-closed.

1. If F/K is normal, then any prolongation of v_K to F is conjugate to v, i.e., of the form $v \circ \sigma$ for some $\sigma \in Aut(F/K)$. Of course, $v \circ \sigma$ is again henselian (e.g., by Hensel's lemma). But conjugate valuations are incomparable, so $v \circ \sigma = v$, because v is comparable to any other henselian valuation on K. Thus v is the unique prolongation of v_K to F, and since v extends uniquely to the algebraic closure, so does v_K.

2. If F/K is a proper finite extension then, by Artin-Schreier theory, $[F^{sep} : K] = \infty$. Hence the normal hull F' of F/K is not separably closed. The unique prolongation v' of v to F' then inherits the hypotheses on the comparability with other henselian valuations, and we may apply case 1. to (F', v').

3. Let us first assume that $Fv \neq (Fv)^{sep}$ and that Fv is not real closed. We shall assume that $char\, Fv \neq p$ (for the proof in equal characteristic $p > 0$ one has to work with Artin-Schreier- in place of Kummer-extensions, and in mixed characteristic $(0, p)$ one has to apply an easy translation from residual Artin-Schreier-extensions to Kummer extensions of K, cf. Lemma 3.2 of [**Koe03**]). Replacing K by a finite subextension of F/K we may then assume (using case 2.) that K contains a primitive p-th root ζ_p of unity and that $Kv \neq Kv^p$.

Now assume that v_K has two prolongations to F. Then there is a finite subextension L/K of F/K with two distinct prolongations $v_1 = v\mid_L \neq v_2$ of v_K. Choose $a \in \mathscr{O}_{v_2}$ with residue not a p-th power (this is possible because Lv_2/Kv is finite and $Kv \neq Kv^p$ is not real closed). Since v_1 and v_2 are incomparable, weak approximation produces an element $x \in (1 + \mathscr{M}_{v_1}) \cap (a + \mathscr{M}_{v_2})$. By Hensel's Lemma, $x \in F^p$. Hence $L(\sqrt[p]{x})/L$ is a Galois subextension of F/K of degree p which is impossible because G_F is a Sylow-p subgroup of G_K, and so also of G_L. So v_K is henselian after all.

The next case to be considered is the case that v is a rank-1 valuation and Fv is not real closed. In this case we have strong approximation for any distinct prolongations of v_K to a finite extension of K and the above proof can be adjusted to this situation using density of a rank-1 valued field in its henselisation and Krasner's Lemma in place of Hensel's Lemma.

The third case is that $Fv = Fv^{sep}$. Either there is a relative rank-1 coarsening w of v, i.e., v induces a rank-1 valuation v/w on Fw; then the first case applies to w and the second to v/w; this suffices since the 'composed' valuation v_K is henselian iff both w_K and $v_K/w_K = (v/w)\mid_{Kw_K}$ are. Or $\mathscr{O}_v$ is the intersection of the valuation rings of all proper coarsenings of v, and since they are henselian on K by the first case, so is v_K.

Finally, if Fv is real closed we can apply the previous case to $F(\sqrt{-1})/K(\sqrt{-1})$ and use 2. again. $\square$

2.2. Rigid elements induce valuations. If (K, v) is a valued field and if $x \in F^\times \setminus \mathscr{O}_v^\times$ then

$$\mathscr{O}_v^\times + x\mathscr{O}_v^\times \subseteq \mathscr{O}_v^\times \cup x\mathscr{O}_v^\times.$$

Similarly, if T is any multiplicative subgroup with $\mathscr{O}_v^\times \leqslant T \leqslant F^\times$, and if $x \in F^\times \setminus T$ then

$$T + xT \subseteq T \cup xT, \text{ i.e., } x \text{ is } T-\textbf{rigid}.$$

Conversely, T-rigid elements often give rise to valuations:

Lemma 2.2. *(Proposition 2.13 in* [**Koe03**]*) Let p be a prime > 2, let K be a field with a multiplicative subgroup T such that $(K^\times)^p \leqslant T \leqslant K^\times$ and such that every $x \in K^\times \setminus T$ is T-rigid.*

Then $\mathscr{O}(T) := \mathscr{O}_1(T) \cup \mathscr{O}_2(T)$ is a valuation ring with $\mathscr{O}(T)^\times \subseteq T$, where

$$\begin{array}{rcl} \mathscr{O}_1(T) & = & \{x \in K \setminus T \mid 1 + x \in T\} \\ \mathscr{O}_2(T) & = & \{x \in T \mid x\mathscr{O}_1(T) \subseteq \mathscr{O}_1(T)\} \end{array}$$

If $p = 2$ a similar statement is true (cf. [**AEJ87**]). And if $T = (K^\times)^p$ it is enough to have a single element in $x \in K^\times \setminus T$ whose prime-to-p powers are T-rigid in order to produce a valuation v with $v(x) \notin p\Gamma_v$ (cf. [**Koe95**]).

Proof. The proof is completely elementary. To give a flavour of the kind of arguments used we here only show that $-\mathscr{O}_1 = \mathscr{O}_1$:

$$\begin{array}{rcl} x \in \mathscr{O}_1(T) & \Rightarrow & -x \notin T = -T \;\&\; \pm x^2 \notin T \\ & \Rightarrow & 1 - x^2 = (1-x)(1+x) \in (T \cup x^2T) \cap (T \cup xT) = T \\ & \Rightarrow & 1 - x \in T \\ & \Rightarrow & -x \in \mathscr{O}_1(T) \end{array}$$

In a similar fashion one shows (in this order) $\mathscr{O} \cdot \mathscr{O} \subseteq \mathscr{O}$, $K \subseteq \mathscr{O} \cup \mathscr{O}^{-1}$, $1 + \mathscr{O}_1 \subseteq \mathscr{O}_2$, $1 + \mathscr{O}_2 \subseteq \mathscr{O}$, $\mathscr{O} + \mathscr{O} \subseteq \mathscr{O}$, and reads off from the proof that $\mathscr{O}^\times \subseteq \mathscr{O}_2 \subseteq T$. $\square$

3. Proof of the theorem

To prove the non-trivial direction of the equivalence stated in the theorem assume that K is a field such that G_K is a hensel group. We have to show that K has a tamely branching henselian valuation. By Lemma 2.1, it suffices to prove this in the case where G_K is a pro-p group. For simplicity, we will consider again only the case that p is odd.

The essential case is the **classical case** where $G_K \cong \mathbf{Z}_p \rtimes \mathbf{Z}_p$ ('classical', because the Sylow-p subgroups of $G_{\mathbf{Q}_l}$, $l \neq p$, are of this form).

Let us first show that the case that G_K is an arbitrary pro-p Hensel group follows from the classical case. Let N be a non-trivial abelian normal subgroup of G_K. Then, by Artin-Schreier (p is odd), $N \cong \mathbf{Z}_p^\alpha$ for some cardinal α.

If $\alpha > 1$ then N has a (normal) subgroup $M \cong \mathbf{Z}_p \times \mathbf{Z}_p$. By the classical case, the fixed field $Fix\,M$ of M has a tamely branching henselian valuation v. By passing to a non-trivial coarsening of v we may also assume that v is comparable to any other henselian valuation on $Fix\,M$. By applying Lemma 2.1.1 twice, we see that $v\,|_{Fix\,N}$ is again henselian, and the same holds for $v\,|_K$. And the property that v is tamely branching is, of course, inherited by the restriction of v to any algebraic subfield.

If $\alpha = 1$ and $\sigma \in G_K \setminus N$ then $H := N\langle\sigma\rangle \cong \mathbf{Z}_p \rtimes \mathbf{Z}_p$. So $Fix\,H$ has a tamely branching henselian valuation w, by the classical case. We denote its unique prolongation to $Fix\,N$ by v. If v is comparable to any other henselian valuation on $Fix\,N$, then $v\,|_K$ is again henselian, and, as restriction of w, also tamely branching. If not we replace v by the finest coarsening of v with separably closed residue field. The new v then still has non-p-divisible value group and residual characteristic $\neq p$. So the restriction to $Fix\,H$ (and hence to K) is (as coarsening of the tamely branching valuation w with non-p-divisible value group) again tamely branching. And $v\,|_K$ is henselian, once more by Lemma 2.1.1.

What remains to be done is the

*Proof of the classical case***.** So now $G_K \cong \mathbf{Z}_p \rtimes \mathbf{Z}_p$. This implies that the (p-th) cohomological dimension of G_K is 2, and so $char\,K \neq p$. In particular, as G_K is pro-p, $\zeta_p \in K$. Moreover, any open subgroup G_L of G_K is of the same form $\mathbf{Z}_p \rtimes \mathbf{Z}_p$, hence of rank 2, and so, by Kummer theory, $[L^\times : (L^\times)^p] = p^2$.

By direct computation, this implies a **local reciprocity law**: *for each* $x \in K \setminus K^p$ *the image of the norm* $N_x : K(\sqrt[p]{x})^\times \to K^\times$ *is* $\langle x\rangle(K^\times)^p$ (thus giving rise to a bijection between abelian extensions of degree p and multiplicative subgroups of index p).

To see this, let $L = K(\sqrt[p]{x})$, and choose $y \in K^\times \setminus \langle x\rangle(K^\times)^p$. By Kummer theory, $y \notin L^p$, and, since $N_x(y) \in K^p$, even $y \notin \langle\sqrt[p]{x}\rangle(L^\times)^p$. As $N_x(\sqrt[p]{x}) = x \notin K^p$, also $\sqrt[p]{x} \notin L^p$. Thus, $L^\times = \langle\sqrt[p]{x}\rangle\langle y\rangle(L^\times)^p$, and the image of N_x is $\langle x\rangle(K^\times)^p$.

As immediate consequence of the local reciprocity law we see (computing $N_x(a + b\sqrt[p]{x}) = a^p + xb^p$) that

$$(\star) \qquad \forall x \in K \setminus K^p : (K^\times)^p + x(K^\times)^p \subseteq \bigcup_{i=0}^{p-1} x^i (K^\times)^p.$$

Now we apply a combinatorial argument which is called 'the wonderful creation of rigid elements' in Section 2.5 of [**Koe03**], because we haven't understood yet the true reason why things work as they do. The argument shows that condition $(\star)$ implies that there is a subgroup $T \leqslant K^\times$ with $(K^\times)^p \leqslant T$, $[T:(K^\times)^p] \leqslant p$ and such that all $x \in K^\times \setminus T$ are T-rigid.

This allows us to conclude from Lemma 2.2 that there is a valuation v on K with $\mathscr{O}_v = \mathscr{O}(T)$ such that $\mathscr{O}_v^\times \leqslant T$. Hence $\Gamma_v \neq p\Gamma_v$. After dividing Γ_v by its maximal convex p-divisible subgroup we may also assume that there is no such (except $\{0\}$).

We have to show that v is henselian. If not, there is some Galois extension L/K of degree p admitting several (hence exactly p) immediate prolongations $v_1, \ldots, v_p$ of v. By weak approximation we find for each i an element $x_i \in \mathscr{M}_{v_i} \cap \bigcap_{j\neq i} \mathscr{O}_{v_j}^\times$. Replacing, if necessary, x_i by $x_i + a$ for some $a \in \mathscr{M}_v$ with $v_i(x) > v(a) \notin p\Gamma_{v_i}$ (Γ_v has no non-trivial convex p-divisible subgroup), we may also assume $v_i(x_i) \notin p\Gamma_{v_i}$. But then $x_1, \ldots, x_p$ are $\mathbf{F}_p$-independent modulo $(L^\times)^p$, which is not in accord with the above observation that $[L^\times : (L^\times)^p] = p^2$ (note that $p > 2$).

Finally we have to show that $char\, Kv \neq p$. Suppose not. Then $char\, K = 0$. Since Γ_v is l-divisible for any prime $l \neq p$, it is densely ordered, but it has no non-trivial p-divisible convex subgroup. Hence we find some $\pi \in K$ with $0 < v(\pi) < v(\pi^2) \leqslant v(p)$ such that $v(\pi) \notin p\Gamma_v$. Direct computation shows that then π, $1+\pi$ and $1+\pi^2$ are $\mathbf{F}_p$-independent modulo $(K^\times)^p$, contradicting $[K^\times : (K^\times)^p] = p^2$. ☐

4. Applications

That valuations on a field K are encoded in G_K has many interesting applications. Let us just list a few of them.

A Galois characterization of p-adic fields : If $K/\mathbf{Q}_p$ is a finite extension, then any field L with $G_L \cong G_K$ is p-adically closed, i.e., L has a henselian valuation v of mixed characteristic $(0,p)$ such that $\mathscr{O}_v/p\mathscr{O}_v$ is finite (so Lv is finite and the convex hull Δ of $\mathbf{Z}\cdot v(p)$ in Γ_v is $\cong \mathbf{Z}$), and such that Γ_v/Δ is divisible [**Koe95**].

Classification of solvable absolute Galois groups : If G_K is solvable (i.e., has a finite subnormal series with abelian quotients) it is metabelian. More precisely, there is then an exact sequence

$$1 \to A \to G_K \to C_1 \times C_2 \times Z \to 1$$

with A torsion-free abelian, C_1, C_2 finite cyclic and Z torsion-free procyclic. If $G_{K(\sqrt{-1})}$ is non-projective then K has a non-trivial henselian valuation which is responsible for the structure of G_K. A complete list of solvable profinite groups occuring as absolute Galois groups is given in [**Koe01**].

Elementary characterization of fields by their Galois group : We say that K is elementarily characterized by G_K if for any field L

$$G_L \cong G_K \Leftrightarrow L \equiv K.$$

Here '$L \equiv K$' means that L is elementarily equivalent to K, i.e., L satisfies the same first-order sentences in the language of fields as K. By the work of Artin-Schreier and Tarski, we know that the field $\mathbf{R}$ of real numbers is elementarily characterized by $G_{\mathbf{R}}$: any field L with $G_L \cong G_{\mathbf{R}} \cong \mathbf{Z}/2\mathbf{Z}$ is real closed, and all real closed fields have the same first-order theory (axiomatized by saying that the squares define an ordering and that odd-degree polynomials have zeroes). The same holds if K is a finite abelian extension of $\mathbf{Q}_p$ or if K is a generalized Laurent series field $\mathbf{Q}_p((\mathbf{Z}_{(q)}))$ with coefficients in $\mathbf{Q}_p$ and exponents in the ring $\mathbf{Z}_{(q)}$ of q-adic rational integers. Conversely, it turns out that — apart from exotic cases which conjecturally don't exist — these three classes of fields cover all fields elementarily characterized by their absolute Galois group [**Koeb**].

The birational section conjecture over the p-adics : If X is a smooth projective curve over K with function field $K(X)$ then the birational section conjecture says that all sections of the canonical projection $G_{K(X)} \to$ $\to G_K$ are induced by K-rational points on X. This was conjectured by Grothendieck for fields which are finitely generated over $\mathbf{Q}$, but it is still open. What can be proved is that over $\mathbf{Q}_p$ this conjecture is true [**Koec**].

Products of absolute Galois groups : Absolute Galois groups can hardly ever be written as direct products. More precisely, if $G_K = G_1 \times G_2$ for some field K then either G_1 and G_2 are of coprime order (in the sense of supernatural numbers) or K has a henselian valuation v with $G_{Kv} \cong \overline{G_1} \times \overline{G_2}$ and $(\sharp\overline{G_1}, \sharp\overline{G_2}) = 1$. In the latter case, the Sylow-p subgroups of one of the factors are abelian for any $p \mid (\sharp G_1, \sharp G_2)$. So, for example, $G_{\mathbf{Q}} \times G_{\mathbf{Q}}$ or $G_{\mathbf{Q}_p} \times G_{\mathbf{Q}_p}$ cannot be realized as absolute Galois groups [**Koed**].

Birational anabelian geometry over almost arbitrary fields : For most constant fields K it is possible to recover function fields F/K in one variable from their absolute Galois group [**Koea**].

References

[AEJ87] J. K. Arason, R. Elman & B. Jacob – Rigid elements, valuations, and realization of Witt rings, *J. Algebra* **110** (1987), no. 2, p. 449–467.

[EE77] O. Endler & A. J. Engler – Fields with Henselian valuation rings, *Math. Z.* **152** (1977), no. 2, p. 191–193.

[Koea] J. Koenigsmann – Birational anabelian geometry over almost arbitrary fields, this volume.

[Koeb] ———, Elementary characterization of fields by their absolute Galois group, to appear in Siberian Advanc. Math., also on the Valuation Theory homepage `math.usask.ca/fvk/Valth.html`.

[Koec] ———, On the section conjecture in anabelian geometry, submitted 2003, also on `arXiv.org/math.AG/0305226`.

[Koed] ———, Products of absolute galois groups, to appear in Int. Math. Research Not., also on the Valuation Theory homepage `math.usask.ca/fvk/Valth.html`.

[Koe95] ———, From p-rigid elements to valuations (with a Galois-characterization of p-adic fields), *J. Reine Angew. Math.* **465** (1995), p. 165–182, With an appendix by Florian Pop.

[Koe01] ———, Solvable absolute Galois groups are metabelian, *Invent. Math.* **144** (2001), no. 1, p. 1–22.

[Koe03] ———, Encoding valuations in absolute Galois groups, Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999), Fields Inst. Commun., vol. 33, Amer. Math. Soc., Providence, RI, 2003, p. 107–132.

Mathematisches Institut, Seminars
(Y. Tschinkel, ed.), p. 175–181
Universität Göttingen, 2004

ANABELIAN GEOMETRY OVER ALMOST ARBITRARY FIELDS

J. Königsmann
Mathematisches Institut, Eckerstr. 1, D-79104 Freiburg, Germany
E-mail : Jochen.Koenigsmann@unibas.ch

Abstract. The paper develops the local theory of one-dimensional birational anabelian geometry over almost arbitrary fields and indicates how the global theory should work. This generalizes corresponding results of Pop and Mochizuki over finitely generated and sub-p-adic fields.

1. Anabelian geometry

We briefly recall the basic setting of Grothendieck's anabelian geometry. For more elaborate versions (higher-dimensional, pro-l, Hom-versions etc.) cf. e.g., the survey [**MNT01**].

Let K be a field, let $\hat{X}$ be a smooth projective curve of genus g over K, let $S \subseteq \hat{X}(\overline{K})$ be a finite set of points and let $X := \hat{X} \setminus S$. When considering X as a curve over the algebraic closure $\overline{K}$ of K we write $\overline{X} := X \otimes_K \overline{K}$. Let $K(X)$ be the function field of X (or, equivalently, of $\hat{X}$) over K and let $K(X)^S$ be the maximal Galois extension of $K(X)$ which is unramified on X (so only ramification above the points in S occurs). Let $\pi_1(X) := Gal(K(X)^S/K(X))$

June 30th, 2004.

be the **arithmetic fundamental group** of X/K. Denoting the absolute Galois group of a field F by $G_F := Gal(F^{sep}/F) \cong Aut(\overline{F}/F)$ one has two canonical (horizontal) exact sequences with (vertical) epimorphisms making the squares commute:

$$\begin{array}{ccccccccc} 1 & \to & G_{\overline{K}(X)} & \to & G_{K(X)} & \to & G_K & \to & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \to & \pi_1(\overline{X}) & \to & \pi_1(X) & \to & G_K & \to & 1 \end{array}$$

The **Fundamental Conjecture FC**(X/K) of anabelian geometry (for X/K) says that *for hyperbolic X, X is encoded in $\pi_1(X)$, i.e., if Y is another smooth curve over K with $\pi_1(Y) \cong_{G_K} \pi_1(X)$ then $Y \cong_K X$.* Recall that X is called hyperbolic, if $\chi(X) := 2-2g-\sharp S < 0$ which in characteristic 0 is equivalent to $\pi_1(\overline{X})$ being (highly) non-abelian. The Fundamental Conjecture was conjectured by Grothendieck for fields K which are finitely generated over $\mathbf{Q}$, and was proved in the 90's by the works of Nakamura, Tamagawa and Mochizuki more generally for sub-p-adic fields, i.e., for subfields of finitely generated extensions of $\mathbf{Q}_p$.

The **Birational Fundamental Conjecture BFC**(X/K) of anabelian geometry says that *X is encoded in $G_{K(X)}$ up to birational equivalence, i.e., if Y is another smooth curve over K with $G_{K(Y)} \cong_{G_K} G_{K(X)}$ then Y is birationally equivalent to K over K, i.e., $K(X) \cong_K K(Y)$.* This was proved by Pop for K finitely generated over its prime field [**Pop94**], and, by Mochizuki for sub-p-adic K [**Moc99**]. Bogomolov and Tschinkel [**BT**] prove the same for surfaces, i.e., in dimension 2, provided K contains all roots of unity.

In this note we indicate how to prove the (one-dimensional) birational fundamental conjecture over almost arbitrary fields. The 'local theory' (encoding rational points on X in $G_{K(X)}$) will follow from the general characterization of valuations on a field in its absolute Galois group [**Koeb**], while the 'global theory' will utilize some of the techniques developed in [**BT**].

2. The local theory

In order to apply the machinery from [**Koeb**] we need to restrict ourselves to almost arbitrary fields:

Definition 2.1. *A field K is called* **almost arbitrary** *if*

- *K is not separably closed and not real closed;*
- *K admits proper algebraic extensions of degree prime to char K;*

– *K is non-henselian or p-adic henselian, i.e., either K admits no non-trivial henselian valuation or K admits a henselian rank-1-valuation of mixed characteristic $(0,p)$ and $p \mid \sharp G_K$.*

Note that finite extensions of almost arbitrary fields are again almost arbitrary. Examples of almost arbitrary fields are all sub-p-adic fields, all finite fields, all hilbertian fields, $\mathbf{Q}^{ab}$, $\mathbf{Q}^{solv}$, $\mathbf{Q}_p^{ab}$ etc.

From now on we fix an almost arbitrary field K and a smooth projective curve X over K. Since we are only interested in the *birational* fundamental conjecture we need not distinguish between X and $\hat{X}$.

We want to characterize the K-rational points on X in group-theoretic terms. However, if we pass from K to the perfect hull K^{perf} of K, i.e., the maximal purely inseparable subextension of $\overline{K}/K$, we obtain canonical isomorphisms of Galois groups making $pr_{X/K}$ and $pr_{X/K^{perf}}$ indistinguishable:

$$\begin{array}{ccc} G_{K^{perf}(X)} & \twoheadrightarrow & G_{K^{perf}} \\ \| & & \| \\ G_{K(X)} & \twoheadrightarrow & G_K \end{array}$$

This means that we will not be able to distinguish between K-rational points and K^{perf}-rational points in a Galois-theoretic way.

For each point $P \in X(K^{perf})$ we may choose a decomposition subgroup D_P of $G_{K(X)}$ corresponding to a chosen prolongation of the valuation v_P induced by P on $K(X)$ to $\overline{K(X)}$. D_P is then uniquely determined up to conjugation in $G_{K(X)}$. By ramification theory (cf.e.g., [**KPR86**], $D_P = R_P \rtimes (C_P \rtimes G_P)$, where R_P is the ramification subgroup of D_P (a normal pro-p subgroup of D_P, where $p = char\, K$), where $I_P = R_P \rtimes C_P$ is the inertia subgroup of D_P, where $C_P \cong \hat{\mathbf{Z}}$ if $char\, K = 0$ resp. $C_P \cong \hat{\mathbf{Z}}/\mathbf{Z}_p = \prod_{q \neq p} \mathbf{Z}_q$ if $char\, K = p > 0$ and $pr_{X/K}$ maps G_P isomorphically onto G_K.

This suggests the following definition:

Definition 2.2. *We call a subgroup D of $G_{K(X)}$* **geometric** *if*

$$D \cong R \rtimes (C \rtimes G),$$

where

$$\begin{array}{llll} R = 1 & \text{and} & C \cong \hat{\mathbf{Z}} & \text{if } char\, K = 0 \\ R \text{ is pro-}p & \text{and} & C \cong \hat{\mathbf{Z}}/\mathbf{Z}_p = \prod_{q \neq p} \mathbf{Z}_q & \text{if } char\, K = p > 0 \end{array}$$

and where $pr_{X/K}|_G \colon G \to G_K$ is an isomorphism.

Note that the characteristic of K is (under our assumption that K is almost arbitrary) group-theoretically encoded:

$$\begin{array}{rcl} \mathit{char}\,K = p > 0 & \Leftrightarrow & p \text{ is a prime with } cd_p(G_K) = cd_p(G_{K(X)}) = 1 \\ \mathit{char}\,K = 0 & \Leftrightarrow & \text{no such prime exists.} \end{array}$$

Now we can present our group-theoretic characterization of rational points, similar as in Theorem 4.1 and Corollary 4.3 of [**Koeb**]:

Proposition 2.3. *Let K be an almost arbitrary field, let X be a smooth projective curve over K, and let $pr_{X/K} : G_{K(X)} \twoheadrightarrow G_K$ be the canonical projection. Then there is a bijection*

$$\begin{array}{rcl} X(K^{perf}) & \leftrightarrow & \{\textit{conjugacy classes of maximal geometric subgroups of } G_{K(X)}\} \\ P & \mapsto & [D_P] \end{array}$$

Proof. Let us assume that $D \leqslant G_{K(X)}$ is a maximal geometric subgroup of $G_{K(X)}$. We will show that $D = D_P$ for some $P \in X(K^{perf})$. Let q be a prime $\neq \mathit{char}\,K$ with $q^2 \mid \sharp G_K$ (such primes exist because K is almost arbitrary), and let G_q be a Sylow-q subgroup of G_K. Then the Sylow-q subgroups of D are of the form $\mathbf{Z}_q \rtimes G_q$. Let F be the fixed field of D. By Theorem 1.3 of [**Koeb**], this implies that F has a henselian valuation v with non-q-divisible value group and residual characteristic $\neq q$. So, in particular, v is non-trivial.

But $v_K := v\mid_K$ is trivial: K is relatively algebraically closed in F, because the restriction $pr_{X/K}$ maps D onto G_K. So v_K is again henselian. If K has no non-trivial henselian valuation, then v_K must be trivial. Otherwise K has a henselian rank-1 valuation w of mixed characteristic $(0,p)$ and $p^2 \mid \sharp G_K$. So we might as well have taken $q = p$ which implies that v_K is again trivial because any non-trivial henselian valuation on K has residual characteristic $= p$ (w has rank 1, so any other non-trivial henselian valuation must be finer).

Hence $v\mid_{K(X)}$ is a non-trivial valuation on $K(X)$ which is trivial on K, and so it is the P-adic valuation v_P for some point P on X. Choose a henselisation F_P of $K(X)$ w.r.t. v_P inside F. Then $G_{F_P} = D_P \supseteq D$. Since D is maximal and D_P is also a geometric subgroup of $G_{K(X)}$ we must have equality $D = D_P$. Moreover, by Hensel's Lemma, $P \in X(K^{perf})$, because K is relatively algebraically closed in F_P.

At the same time, this shows that the map in the proposition is well-defined, i.e., that each D_P is indeed a maximal geometric subgroup of $G_{K(X)}$. Of course, one should also mention that the set of maximal geometric subgroups like the set of decomposition subgroups is closed under conjugation.

Finally, the map is injective by the theorem of F.K. Schmidt: distinct points (i.e., rank-1-valuations on $K(X)$) have non-conjugate henselisations. $\square$

3. Global theory

Throughout this section we assume that K and L are almost arbitrary fields, that X is a smooth projective curve over K, that Y is a smooth projective curve over L and that $\varphi : G_{K(X)/K} \to G_{L(Y)/L}$ is an isomorphism, i.e., $\varphi : G_{K(X)} \to G_{L(Y)}$ is an isomorphism inducing an isomorphism $G_K \to G_L$:

$$\begin{array}{ccc} G_{K(X)} & \overset{\varphi}{\leftrightarrow} & G_{L(Y)} \\ pr_{X/K} \downarrow & & \downarrow pr_{Y/L} \\ G_K & \leftrightarrow & G_L \end{array}$$

Conjecture 3.1. *Then φ induces an isomorphism $K^{perf}(X) \cong L^{perf}(Y)$ which restricts to an isomorphism $K^{perf} \cong L^{perf}$.*

The conjecture is very close to being proved [**Koea**].

Let us first draw some consequences from the local theory.

Corollary 3.2. *φ induces a bijection $X(\overline{K}) \leftrightarrow Y(\overline{L})$ respecting the G_K- resp. G_L-action.*

Proof. Any finite separable extension K_1/K is the fixed field of an open subgroup of G_K. Let L_1 be the fixed field of the corresponding open subgroup of G_L. Then L_1/L is a finite separable extension and φ restricts to an isomorphism $G_{K_1(X)/K_1} \to G_{L_1(Y)/L_1}$ carrying maximal geometric subgroups of $G_{K_1(X)}$ to maximal geometric subgroups of $G_{L_1(Y)}$. Since K_1 and L_1 are again almost arbitrary, Proposition 2.3 gives a bijection $X(K_1^{perf}) \leftrightarrow Y(L_1^{perf})$.

If $K_1 \subseteq K_2$ are two finite separable extensions of K then these bijections respect the canonical embedding $X(K_1^{perf}) \subseteq X(K_2^{perf})$ as well as the Galois action of G_K resp. G_L. Hence the bijection passes to the inductive limit $X(\overline{K})$. □

Let $Div\,\overline{X}$ be the group of divisors of X over $\overline{K}$. Then $Div\,\overline{X}$ is a G_K-module, and, similarly, $Div\,\overline{Y}$ is a G_L-module. The following corollary is an immediate consequence of the previous one:

Corollary 3.3. *φ induces a (G_K, G_L)-module isomorphism $\varphi_{div} : Div\,\overline{X} \leftrightarrow Div\,\overline{Y}$ preserving the degree.*

If the genus of X and L is zero this implies that φ induces a (G_K, G_L)-module isomorphism between the groups $PDiv\,\overline{X} = Div^0\,\overline{X}$ and $PDiv\,\overline{Y} = Div^0\,\overline{Y}$ of principal divisors (this seems to hold for general genus as well). Moreover, if for any $D \in Div\,\overline{X}$ we write $\overline{L(D)}$ for the image of the linear function space $L(D) := \{f \in \overline{K}(X) \mid (f) + D \geqslant 0\}$ in $PDiv\,\overline{X}$, φ then also induces a bijection between the spaces $\overline{L(D)}$ and $\overline{L(\varphi_{div}(D))}$. We expect that the same holds for any finite-dimensional, and so, in particular, for any 2-dimensional space of functions. If this is true, then the above conjecture follows from [**BT**], Theorem 4.6 (details will be worked out in [**Koea**].

What we can already say for sure is that the Galois group knows the genus:

Corollary 3.4. *The genus of X and Y are the same.*

Proof. If $S \subseteq X(\overline{K})$ is a finite set of points then φ induces an isomorphism between $\pi_1(\overline{X} \setminus S)$ and $\pi_1(\overline{Y} \setminus \varphi(S))$, because

$$\pi_1(\overline{X} \setminus S) \cong G_{K(X)}/\langle I_P \mid P \in \overline{X} \setminus S\rangle,$$

where I_P runs through the inertia subgroups of all decomposition subgroups D_P of $G_{K(X)}$ w.r.t. $P \in \overline{X} \setminus S$. Note that $n := \sharp S = \sharp\varphi(S)$.

If $char\, K = 0$ then $\pi_1(\overline{X} \setminus S)$ is a free profinite group of rank $2g_X + n - 1$. Hence $g_Y = g_X$ (recall that the characteristic is also encoded in $pr_{X/K}$).

If $char\, K \neq 0$ then the maximal pro-l quotient of $\pi_1(\overline{X} \setminus S$ still is a free pro-l group of rank $2g_X + n - 1$, whenever l is a prime $\neq char\, K$. So, again, $g_Y = g_X$. □

4. Further applications of the local theory

We would like to mention two further applications of the local theory, one on the relation between the two fundamental conjectures of anabelian geometry, and one on the solvability of polynomial equations by radicals.

It seems natural that the fundamental conjecture of anabelian geometry should imply the birational fundamental conjecture, because the absolute Galois group of $K(X)$ is the inverse limit of all arithmetic fundamental groups of X'/K when X' runs through all Zariski open subvarieties of X. However, in principle, $G_{K(X)}$ may have forgotten its genealogy. If K is almost arbitrary, it has not:

Corollary 4.1. *Let K be an almost arbitrary field, let X be a smooth projective curve over K and assume that the fundamental conjecture* $\mathbf{FC}(X'/K)$ *holds for some Zariski open hyperbolic $X' \subseteq X$. Then the birational fundamental conjecture* $\mathbf{BFC}(X/K)$ *holds.*

Proof. The proof uses the same argument as in the previous corollary: the quotients of $G_{K(X)}$ which are arithmetic fundamental groups are group-theoretically encoded in $pr_{X/K}$. □

The second application goes back to the roots of Galois theory, the question which polynomials over the field $\mathbf{Q}$ of rational numbers can be solved by radicals. Galois gave a precise answer for polynomials in one variable: the group-theoretic criterion is that the Galois group of the splitting field be solvable in the group-theoretic sense. If one considers polynomials in two variables, it is easy to construct polynomial equations without radical solutions, using the one-dimensional case. However, the same question for *absolutely irreducible* polynomials over $\mathbf{Q}$ is still open: it is not known whether any curve defined over $\mathbf{Q}$ has a $\mathbf{Q}^{solv}$-rational point (Problem 10.16(a) of [**FJ86**]). Our local theory immediately gives — à la Galois — at least a group-theoretic criterion:

Corollary 4.2. *If X is a smooth projective curve over $\mathbf{Q}$ then $X(\mathbf{Q}^{solv}) \neq \emptyset$ if and only if $G_{\mathbf{Q}^{solv}(X)}$ contains a geometric subgroup.*

Note that this *is* a group-theoretic criterion since $pr_{X/\mathbf{Q}^{solv}}$ is encoded in $pr_{X/\mathbf{Q}}$.

References

[BT] F. Bogomolov & Y. Tschinkel – Reconstruction of function fields, `www.math.princeton.edu/~ytschink/papers/yuri/recon/recon32.pdf`.

[FJ86] M. D. Fried & M. Jarden – *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 11, Springer-Verlag, Berlin, 1986.

[Koea] J. Koenigsmann – Galois groups of function fields, in preparation.

[Koeb] ______, On the section conjecture in anabelian geometry, `arXiv/math.AG/0305226`.

[KPR86] F.-V. Kuhlmann, M. Pank & P. Roquette – Immediate and purely wild extensions of valued fields, *Manuscripta Math.* **55** (1986), no. 1, p. 39–67.

[MNT01] S. Mochizuki, H. Nakamura & A. Tamagawa – The Grothendieck conjecture on the fundamental groups of algebraic curves, *Sugaku Expositions* **14** (2001), no. 1, p. 31–53.

[Moc99] S. Mochizuki – The local pro-p anabelian geometry of curves, *Invent. Math.* **138** (1999), no. 2, p. 319–423.

[Pop94] F. Pop – On Grothendieck's conjecture of birational anabelian geometry, *Ann. of Math. (2)* **139** (1994), no. 1, p. 145–182.