Algebra & Number Theory

Volume 4
2010
No. 3

mathematical sciences publishers

Algebra & Number Theory
www.jant.org

See inside back cover or www.jant.org for submission instructions.

Regular subscription rate for 2010: $200.00 a year ($140.00 electronic only).
Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory, ISSN 1937-0652, at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

PUBLISHED BY
mathematical sciences publishers
http://www.mathscipub.org
A NON-PROFIT CORPORATION
Typeset in LaTeX

ALGEBRA AND NUMBER THEORY 4:3(2010)

A new approach to Kostant's problem

Johan Kåhrström and Volodymyr Mazorchuk

For every involution $\boldsymbol{w}$ of the symmetric group S_n we establish, in terms of a special canonical quotient of the dominant Verma module associated with $\boldsymbol{w}$, an effective criterion to verify whether the universal enveloping algebra $U(\mathfrak{sl}_n)$ surjects onto the space of all ad-finite linear transformations of the simple highest weight module $L(\boldsymbol{w})$. An easy sufficient condition derived from this criterion admits a straightforward computational check (using a computer, for example). All this is applied to get some old and many new results, which answer the classical question of Kostant in special cases; in particular we give a complete answer for simple highest weight modules in the regular block of $\mathfrak{sl}_n$, $n \leq 5$.

1. Introduction

Let $\mathfrak{g}$ be a complex semisimple finite-dimensional Lie algebra with a fixed triangular decomposition,

$$\mathfrak{g} = \mathfrak{n}_- \oplus \mathfrak{h} \oplus \mathfrak{n}_+,$$

and $U(\mathfrak{g})$ be its universal enveloping algebra. Then for every two $\mathfrak{g}$-modules M and N the space $\mathrm{Hom}_{\mathbb{C}}(M, N)$ may be viewed as a $U(\mathfrak{g})$-bimodule in the natural way, and, furthermore, also as a $\mathfrak{g}$-module under the adjoint action of $\mathfrak{g}$. The bimodule $\mathrm{Hom}_{\mathbb{C}}(M, N)$ has a sub-bimodule, usually denoted by $\mathcal{L}(M, N)$, which consists of all elements on which the adjoint action of $U(\mathfrak{g})$ is locally finite (see for example [Jantzen 1983, Kapitel 6]). Since $U(\mathfrak{g})$ itself consists of locally finite elements under the adjoint action, it naturally maps to $\mathcal{L}(M, M)$ for every $\mathfrak{g}$-module M, and the kernel of this map is obviously the annihilator $\mathrm{Ann}(M)$ of M in $U(\mathfrak{g})$. The classical problem of Kostant (see for example [Joseph 1980]) is formulated in the following way:

For which $\mathfrak{g}$-modules M is the natural injection $U(\mathfrak{g})/\mathrm{Ann}(M) \hookrightarrow \mathcal{L}(M, M)$ surjective?

MSC2000: primary 17B10; secondary 17B35, 16E30.
Keywords: universal enveloping algebra, Kostant's problem, Kazhdan–Lusztig combinatorics.

A (positive) answer to Kostant's problem is an important tool in the study of Goldie rank ratios [Joseph 1980] and in the study of induced modules, particularly generalized Verma modules, [Borho and Brylinski 1982; Miličić and Soergel 1997; Khomenko and Mazorchuk 2004; Mazorchuk and Stroppel 2008a].[1] A positive answer to Kostant's problem for certain highest weight modules allows one, for example, to give a unified irreducibility criterion for the structure of generalized Verma modules [Miličić and Soergel 1997; Khomenko and Mazorchuk 2004; MS 2008a]. A negative answer to Kostant's problem in the situation of [Borho and Brylinski 1982] results in the filtration of the appropriate quotient of the universal enveloping algebra not coinciding with that given by its embedding into differential operators.

Unfortunately, the complete answer to this problem is not even known for (simple) highest weight modules. The answer is known to be positive for Verma modules [Joseph 1980, Corollary 6.4] and for certain classes of simple highest weight modules [Gabber and Joseph 1981a, Theorem 4.4; Conze-Berline and Duflo 1977; McGovern 1994; Mazorchuk 2005, Theorem 1]. For simple highest weight modules in type A the answer is even known to be an invariant of a left cell; see [MS 2008a, Theorem 60]. However, already in [Joseph 1980, 9.5] it was shown that for some simple highest weight modules in type B the answer is negative (another example can be found in [Conze-Berline and Duflo 1977, 6.5]). Contrary to the popular belief that the answer is positive for simple highest weight modules in type A, it was recently shown in [MS 2008b, Theorem 13] that for the simple highest weight $\mathfrak{sl}_4$-module $L(rt)$, where r and t are two commuting simple reflections, the answer is negative.

The present paper is strongly inspired by this counterexample and is an attempt to analyze and generalize it. As for highest weight modules in type A the answer to Kostant's problem is an invariant of a left cell, and since every left cell of the symmetric group S_n contains a unique involution [Sagan 2001, Chapter III], it is enough to solve Kostant's problem for all modules of the form $L(w)$, where $w \in S_n$ is an involution. The counterexample in [MS 2008b, Theorem 13] was constructed relating the module $L(w)$ to a special quotient of the dominant Verma module, which in the following will be denoted by $D^{\hat{R}}$. This module is a canonical object of the category $\mathcal{O}_0^{\hat{R}}$, which was used in [MS 2008a] to categorify Kazhdan–Lusztig cell modules. Furthermore, it is the unique quotient of the dominant Verma module, whose annihilator (in $U(\mathfrak{g})$) coincides with the annihilator of $L(w)$. The module $L(w)$ is the simple socle of $D^{\hat{R}}$ and thus both $L(w)$ and $D^{\hat{R}}$ are submodules of the indecomposable injective module $P^{\hat{R}}(w)$ in $\mathcal{O}_0^{\hat{R}}$, which also turns out to be projective.

[1] Henceforth we will abreviate "Mazorchuk and Stroppel" by MS.

The main result of the present paper relates the solution of Kostant's problem for $L(\boldsymbol{w})$ to the structure of $D^{\hat{\boldsymbol{R}}}$ as follows:

Theorem 1. *Kostant's problem has a positive answer for $L(\boldsymbol{w})$ if and only if every simple submodule of the cokernel of the canonical inclusion $D^{\hat{\boldsymbol{R}}} \subset P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})$ has the form $L(x)$, where x is some element from the right cell of $\boldsymbol{w}$.*

We will show that Theorem 1 can be used to answer Kostant's problem in many cases, in particular, to obtain many new results and reprove some old results. To prove this result we further develop the functorial approach to Kostant's problem from [Mazorchuk 2005; MS 2008a; 2008b]. The most interesting application of this theorem seems to be that it implies a sufficient condition for a *negative* answer to Kostant's problem, which is purely computational and can be realized as a relatively short and efficient program on a computer. Some further progress on Kostant's problem was recently made in [Mazorchuk 2009].

In Section 2 we collect all necessary preliminaries. The main results, including Theorem 1, are formulated in detail and proved in Section 3. In Section 4 we collect many applications, both theoretical and computational.

2. Notation and preliminaries

From now on we assume that $\mathfrak{g} = \mathfrak{sl}_n$ and the triangular decomposition is just the usual decomposition into the upper triangular, diagonal and lower triangular matrices. The symmetric group S_n is the Weyl group W for $\mathfrak{g}$ and hence S_n acts on $\mathfrak{h}^*$ in the usual way $w\lambda$, and via the dot action $w \cdot \lambda = w(\lambda + \rho) - \rho$, where ρ is half the sum of all positive (with respect to the above triangular decomposition) roots of the algebra $\mathfrak{g}$.

Let $\mathbb{O}$ denote the BGG category $\mathcal{O}$ [Bernstein et al. 1976] associated with the triangular decomposition above. For $w \in W$ we let $\Delta(w)$ denote the Verma module with highest weight $w \cdot 0$, $L(w)$ denote the simple head of $\Delta(w)$, and $P(w)$ denote the indecomposable projective cover of $L(w)$. The *principal block* $\mathbb{O}_0$ is the indecomposable direct summand of $\mathbb{O}$, which contains all $L(w)$, $w \in S_n$.

For $w \in W$ we denote by θ_w the indecomposable *projective functor* on $\mathbb{O}_0$ associated with w. This functor is the unique (up to isomorphism) indecomposable direct summand of all possible functors that have the form $V \otimes_{\mathbb{C}} - : \mathbb{O} \to \mathbb{O}$, where V is a finite-dimensional $\mathfrak{g}$-module that satisfies $\theta_w \Delta(e) = P(w)$, where e is the identity element of W [Bernstein and Gel'fand 1980, Section 3].

Denote by $\leq_{\mathsf{L}}$ and $\leq_{\mathsf{R}}$ the left and the right (pre)orders on W respectively [Björner and Brenti 2005, Section 3]. For $x, y \in W$ we will write $x <_{\mathsf{L}} y$ provided that $x \leq_{\mathsf{L}} y$ and $y \not\leq_{\mathsf{L}} x$. We will use similar notation for $\leq_{\mathsf{R}}$. The left preorder coincides with the natural inclusion order on the set of annihilators of $L(w)$, $w \in S_n$ [Jantzen 1983, 14.15]. The right one is obtained applying the involution $x \mapsto x^{-1}$.

For a fixed right cell $\boldsymbol{R}$ set

$$\hat{\boldsymbol{R}} = \{x \in W \,:\, x \leq_{\mathsf{R}} w \text{ for some } w \in \boldsymbol{R}\}$$

(this is simply the principal ideal (or cone) of $(S_n, \leq_{\mathsf{R}})$, generated by the equivalence class $\boldsymbol{R}$), and denote by $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$ the smallest full subcategory of $\mathbb{O}_0$ that contains all $L(w)$, $w \in \hat{\boldsymbol{R}}$, and is closed under isomorphisms and extensions. The natural inclusion functor $\mathbb{O}_0^{\hat{\boldsymbol{R}}} \to \mathbb{O}_0$ is obviously exact and hence has both a left adjoint $\mathrm{Z}_0^{\hat{\boldsymbol{R}}} : \mathbb{O}_0 \to \mathbb{O}_0^{\hat{\boldsymbol{R}}}$ and a right adjoint $\hat{\mathrm{Z}}_0^{\hat{\boldsymbol{R}}} : \mathbb{O}_0 \to \mathbb{O}_0^{\hat{\boldsymbol{R}}}$ [MS 2008a, 5.1]. The functor $\mathrm{Z}_0^{\hat{\boldsymbol{R}}}$ is just the functor of taking the maximal possible quotient that lies in $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$; and the functor $\hat{\mathrm{Z}}_0^{\hat{\boldsymbol{R}}}$ is just the functor of taking the maximal possible submodule that lies in $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$. All projective functors on $\mathbb{O}_0$ preserve $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$, and both $\mathrm{Z}_0^{\hat{\boldsymbol{R}}}$ and $\hat{\mathrm{Z}}_0^{\hat{\boldsymbol{R}}}$ commute with θ_w for all $w \in W$ [MS 2008a, Lemma 19].

For $w \in \hat{\boldsymbol{R}}$ set $P^{\hat{\boldsymbol{R}}}(w) = \mathrm{Z}_0^{\hat{\boldsymbol{R}}} P(w)$ and $\Delta^{\hat{\boldsymbol{R}}}(w) = \mathrm{Z}_0^{\hat{\boldsymbol{R}}} \Delta(w)$. Then the modules $P^{\hat{\boldsymbol{R}}}(w)$, $w \in \hat{\boldsymbol{R}}$, are exactly the indecomposable projective modules in $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$. The module $P^{\hat{\boldsymbol{R}}}(w)$ is injective if and only if $w \in \boldsymbol{R}$ [MS 2008a, Section 5]. Let $\boldsymbol{w} \in \boldsymbol{R}$ be the unique involution in $\boldsymbol{R}$. Then $P^{\hat{\boldsymbol{R}}}(w) = \theta_w L(\boldsymbol{w})$ for any $w \in \boldsymbol{R}$; see [MS 2008b, Key statement]. By [MS 2008b, Lemma 8] we have the equality $\dim \mathrm{Hom}_{\mathfrak{g}}(P^{\hat{\boldsymbol{R}}}(e), P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})) = 1$. Denote by $D^{\hat{\boldsymbol{R}}}$ the image of the unique (up to a scalar) nonzero homomorphism from $P^{\hat{\boldsymbol{R}}}(e)$ to $P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})$.

Conjecture 2. $D^{\hat{\boldsymbol{R}}} = P^{\hat{\boldsymbol{R}}}(e)$.

Define the following full subcategories in $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$:

$$\mathscr{C}_1 = \{M \in \mathbb{O}_0^{\hat{\boldsymbol{R}}} \,:\, [M : L(x)] > 0 \text{ implies } x <_{\mathsf{R}} \boldsymbol{w}\},$$
$$\mathscr{C}_2 = \{M \in \mathbb{O}_0^{\hat{\boldsymbol{R}}} \,:\, \mathrm{Hom}_{\mathfrak{g}}(L(x), M) \neq 0 \text{ implies } x \in \boldsymbol{R}\},$$
$$\mathscr{C}_3 = \{M \in \mathbb{O}_0^{\hat{\boldsymbol{R}}} \,:\, \mathrm{Hom}_{\mathfrak{g}}(M, L(x)) \neq 0 \text{ implies } x \in \boldsymbol{R}\}.$$

Let $M \in \mathscr{C}_1$, $N \in \mathscr{C}_2$ and $K \in \mathscr{C}_3$. Then none of the composition subquotients of M occurs in the socle of N. Hence $\mathrm{Hom}_{\mathfrak{g}}(M, N) = 0$. Similarly, none of the composition subquotients of M occurs in the top of K. Hence $\mathrm{Hom}_{\mathfrak{g}}(K, M) = 0$. The following result is based on a statement from [Joseph 1979].

Lemma 3. *For all $w \in W$ and $i = 1, 2, 3$, the functor θ_w preserves the category $\mathscr{C}_i$.*

Proof. Let $x <_{\mathsf{R}} \boldsymbol{w}$ and $\boldsymbol{X}$ be the right cell of x. Then $L(x) \in \mathbb{O}_0^{\hat{\boldsymbol{X}}}$ and hence $\theta_w L(x) \in \mathbb{O}_0^{\hat{\boldsymbol{X}}}$ (because, as mentioned above, θ_w preserves $\mathbb{O}_0^{\hat{\boldsymbol{X}}}$). Now for the category $\mathscr{C}_1$, the statement follows from the exactness of the functor θ_w.

As noted before, in [MS 2008a, 5.1] it is shown that $P^{\hat{\boldsymbol{R}}}(w)$ is injective for any $w \in \boldsymbol{R}$. Since the socle of every $X \in \mathscr{C}_2$ consists, by definition, of $L(w)$, $w \in \boldsymbol{R}$, it follows that the injective envelope of X is projective. Since θ_w is both left and right adjoint to $\theta_{w^{-1}}$, it preserves the category of projective-injective modules in $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$.

This and exactness of θ_w imply the statement for the category $\mathscr{C}_2$. For the category $\mathscr{C}_3$ the statement follows by duality. □

Let $\mathscr{P} = \bigoplus_{w \in \boldsymbol{R}} P^{\hat{\boldsymbol{R}}}(w)$. For every $M \in \mathbb{O}_0^{\hat{\boldsymbol{R}}}$ let I_M be some (minimal) injective envelope of M and set

$$M_1 = \bigcap_{\substack{f \in \mathrm{Hom}_{\mathfrak{g}}(I_M, \mathscr{P}) \\ f(M)=0}} \mathrm{Ker}(f), \qquad M_1' = \bigcap_{f \in \mathrm{Hom}_{\mathfrak{g}}(M_1, \mathscr{P})} \mathrm{Ker}(f),$$

and $M_2 = M_1/M_1'$. Thus the module M_1 is the "maximal possible" nonsplit extension from a module from $\mathscr{C}_1$ to M, which does not affect the socle of M. The module M_1' is the maximal submodule of M_1 that belongs to $\mathscr{C}_1$. The correspondence $M \mapsto M_2$ is functorial and M_2 is called the *partial approximation* of M with respect to the injective module $\mathscr{P}$ [Khomenko and Mazorchuk 2005, 2.5]. We denote by $\mathrm{A} : \mathbb{O}_0^{\hat{\boldsymbol{R}}} \to \mathbb{O}_0^{\hat{\boldsymbol{R}}}$ the corresponding functor of partial approximation. This functor is inspired by the realization of (Joseph's version of) Enright's functor obtained in [Khomenko and Mazorchuk 2005, Section 4]. However, one should mention that Enright's functor does not preserve $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$ and hence is not suitable for our purposes. The functor A has the following properties:

Proposition 4. (i) A *is left exact.*

(ii) $\mathrm{A}M = 0$ *for any* $M \in \mathscr{C}_1$.

(iii) A *maps* $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$ *to* $\mathscr{C}_2$; *in particular*, A *preserves the category* $\mathscr{C}_2$.

(iv) *The quotient map from* M *to* $M/(M \cap M_1')$ *gives the natural transformation* nat *from the identity functor to* A.

(v) *The kernel of* nat *coincides with the maximal submodule of* M *that belongs to* $\mathscr{C}_1$.

(vi) *If* $M \in \mathscr{C}_2$ *and* I_M *is the injective envelope of* M, *then* $\mathrm{A}M$ *is the maximal submodule of* I_M *that contains* M *and such that* $\mathrm{A}M/M \in \mathscr{C}_1$.

(vii) *If* $M \in \mathscr{C}_2$, *then* $\mathrm{A}M \cong \mathrm{A}\mathrm{A}M$.

Proof. Statement (i) is a part of [Khomenko and Mazorchuk 2005, Corollary 2]. If $M \in \mathscr{C}_1$, then $M_1' = M$ and hence $\mathrm{A}M = 0$, proving (ii). As the module M_1' is the largest submodule of M_1 that belongs to $\mathscr{C}_1$, we get $M_1/M_1' \in \mathscr{C}_2$, which proves (iii). For statement (iv) we refer to [Khomenko and Mazorchuk 2005, 2.5] and statement (v) follows from the definition of nat and the fact that M_1' is the largest submodule of M_1, which belongs to $\mathscr{C}_1$. If $M \in \mathscr{C}_2$, then $M_1' = 0$ and (vi) follows directly from the definition of A. Finally, (vii) follows from (vi). □

3. The main results

3.1. ***A criterion for testing Kostant's problem.*** According to Theorem 60 of [MS 2008a], the answer to Kostant's problem for $L(w)$, $w \in W$, is an invariant of a left cell. Since every left cell has a unique involution, it is thus enough to study Kostant's problem for involutions in W. The main result of the paper is this:

Theorem 5. *Let $\boldsymbol{w} \in W$ be an involution and $\boldsymbol{R}$ be the right cell of W, containing $\boldsymbol{w}$. Then the following conditions are equivalent*:

(a) *Kostant's problem has a positive solution for $L(\boldsymbol{w})$, that is, the inclusion*

$$U(\mathfrak{g})/\mathrm{Ann}(M) \hookrightarrow \mathscr{L}(M, M)$$

is surjective for $\mathfrak{g} = \mathfrak{sl}_n$ and $M = L(\boldsymbol{w})$.

(b) *Every simple module occurring in the socle of the cokernel* Coker *of the natural inclusion $D^{\hat{\boldsymbol{R}}} \hookrightarrow P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})$, has the form $L(x)$, where $x \in \boldsymbol{R}$ (that is,* Coker *belongs to $\mathscr{C}_2$).*

The idea of the proof is to compare Kostant's problem for the modules $L(\boldsymbol{w})$ and $D^{\hat{\boldsymbol{R}}}$. The former is exactly the module for which we would like to solve Kostant's problem, while the latter is, by definition, a quotient of $\Delta(e)$, and hence Kostant's problem for it has a positive solution by [Jantzen 1983, 6.9(10)]. The relation between these two modules is again given by definition: $L(\boldsymbol{w})$ is the simple socle of $D^{\hat{\boldsymbol{R}}}$. So, to compare $\mathscr{L}(L(\boldsymbol{w}), L(\boldsymbol{w}))$ and $\mathscr{L}(D^{\hat{\boldsymbol{R}}}, D^{\hat{\boldsymbol{R}}})$ one might first try to show that the modules $L(\boldsymbol{w})$ and $D^{\hat{\boldsymbol{R}}}$ have the same annihilators, and then try to show that

$$\mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}), \theta_w L(\boldsymbol{w})) = \mathrm{Hom}_{\mathfrak{g}}(D^{\hat{\boldsymbol{R}}}, \theta_w D^{\hat{\boldsymbol{R}}}) \tag{1}$$

for all $w \in W$. This would be enough to conclude that

$$\mathscr{L}(L(\boldsymbol{w}), L(\boldsymbol{w})) = \mathscr{L}(D^{\hat{\boldsymbol{R}}}, D^{\hat{\boldsymbol{R}}})$$

by [Jantzen 1983, 6.8(3)], thus solving positively Kostant's problem for $L(\boldsymbol{w})$. The first step can be easily found in the literature.

Lemma 6. *We have* $\mathrm{Ann}_{U(\mathfrak{g})}(L(\boldsymbol{w})) = \mathrm{Ann}_{U(\mathfrak{g})}(D^{\hat{\boldsymbol{R}}})$.

Proof. By [MS 2008b, Lemmata 6 and 8] and definitions, the module $L(\boldsymbol{w})$ is the simple socle of $D^{\hat{\boldsymbol{R}}}$, and all other simple subquotients of $D^{\hat{\boldsymbol{R}}}$ have the form $L(x)$ for some $x <_{\mathrm{R}} \boldsymbol{w}$; in particular, they all have Gel'fand–Kirillov dimension which is strictly smaller than that of $L(\boldsymbol{w})$ [Jantzen 1983, 10.11]. Hence $D^{\hat{\boldsymbol{R}}}$ is *quasisimple* in the sense of [Joseph 1980, 6.2], and thus the claim follows from [Joseph 1980, Proposition 6.2]. □

The best way to prove (1) would be to construct a functor that commutes with all θ_w and sends $L(\boldsymbol{w})$ to $D^{\hat{\boldsymbol{R}}}$. It turns out that the functor A defined above is the best possible candidate. We will now show that A commutes with θ_w, and later on we will see that the answer to Kostant's problem is positive if and only if $\mathrm{A}L(\boldsymbol{w}) \cong D^{\hat{\boldsymbol{R}}}$. So now let's do the work.

Lemma 7. *For all $w \in W$ there is an isomorphism of functors*

$$\mathrm{A}\theta_w \cong \theta_w \mathrm{A}.$$

Proof. As A is left exact and θ_w is exact, both $\mathrm{A}\theta_w$ and $\theta_w\mathrm{A}$ are left exact.

Let $I \in \mathbb{O}_0^{\hat{\boldsymbol{R}}}$ be injective. Consider the short exact sequence

$$0 \to K \to I \xrightarrow{\mathrm{nat}_I} \mathrm{A}I \to 0, \tag{2}$$

where K is just the kernel of nat_I. Since the socle of $\mathcal{P}$ coincides with $\bigoplus_{w\in\boldsymbol{R}} L(w)$, from the definition of A we have that $K \in \mathscr{C}_1$, while $\mathrm{A}I \in \mathscr{C}_2$.

Applying θ_w to (2) and using Lemma 3, we obtain that $\theta_w K \in \mathscr{C}_1$ and $\theta_w \mathrm{A}I \in \mathscr{C}_2$. In particular, $\theta_w K$ is the maximal submodule of $\theta_w I$ that belongs to $\mathscr{C}_1$. Furthermore, the morphism $\theta_w(\mathrm{nat}_I)$ is surjective.

At the same time, the module $\theta_w I$ is injective as θ_w is right adjoint to the exact functor $\theta_{w^{-1}}$. From the definition of A we have that the morphism $\mathrm{nat}_{\theta_w I}$ is surjective and that its kernel coincides with the maximal submodule of $\theta_w I$ that belongs to $\mathscr{C}_1$. In other words, the kernels of $\mathrm{nat}_{\theta_w I}$ and $\theta_w(\mathrm{nat}_I)$ coincide.

Now the statement of the lemma follows from [Khomenko and Mazorchuk 2005, Lemma 1], applied to the situation $\mathrm{F} = \mathrm{A}\theta_w$, $\mathrm{G} = \theta_w\mathrm{A}$ and $\mathrm{H} = \theta_w$. □

Set $\overline{D}^{\hat{\boldsymbol{R}}} = \mathrm{A}L(\boldsymbol{w})$.

Lemma 8. (i) *$\overline{D}^{\hat{\boldsymbol{R}}}$ is isomorphic to the maximal submodule of the module $P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})$ that contains the socle of $P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})$ and such that all other composition subquotients of $\overline{D}^{\hat{\boldsymbol{R}}}$ have the form $L(x)$, where $x <_{\mathrm{R}} \boldsymbol{w}$.*

(ii) *We have $D^{\hat{\boldsymbol{R}}} \subset \overline{D}^{\hat{\boldsymbol{R}}}$, and the condition (b) of Theorem 5 is equivalent to the equality $D^{\hat{\boldsymbol{R}}} = \overline{D}^{\hat{\boldsymbol{R}}}$.*

Proof. As $P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})$ is the injective envelope of $L(\boldsymbol{w})$, statement (i) follows from Proposition 4(vi). Claim (ii) follows from (i) and [MS 2008b, Lemmata 5 and 7]. □

To proceed we will need the following standard lemma:

Lemma 9. *Let $X, Y \in \mathbb{O}$ be such that $\mathscr{L}(X, X) \subset \mathscr{L}(Y, Y)$ and*

$$\dim \mathrm{Hom}_{\mathfrak{g}}(X, \theta X) = \dim \mathrm{Hom}_{\mathfrak{g}}(Y, \theta Y)$$

for any (indecomposable) projective functor θ. Then $\mathscr{L}(X, X) \cong \mathscr{L}(Y, Y)$.

Proof. Both $\mathscr{L}(X, X)$ and $\mathscr{L}(Y, Y)$ are Harish-Chandra bimodules for $\mathfrak{g}$ in the sense of [Jantzen 1983, Kapitel 6]. In particular, with respect to the adjoint action of $\mathfrak{g}$, these modules are direct sums of simple finite-dimensional $\mathfrak{g}$-modules, each occurring with a finite multiplicity [Jantzen 1983, Kapitel 6]. For every simple finite-dimensional module V we compare the multiplicities of V in $\mathscr{L}(X, X)$ and $\mathscr{L}(Y, Y)$ considered as $\mathfrak{g}$-modules with the adjoint action of $\mathfrak{g}$. By [Jantzen 1983, 6.8(3)] we have

$$\mathrm{Hom}_{\mathfrak{g}}(V, \mathscr{L}(X, X)) \cong \mathrm{Hom}_{\mathfrak{g}}(X \otimes V, X)) \cong \mathrm{Hom}_{\mathfrak{g}}(X, X \otimes V^*). \tag{3}$$

First note that $\mathrm{Hom}_{\mathfrak{g}}(X, X \otimes V^*)$ is finite-dimensional for $X \in \mathbb{O}$. Since $V^* \otimes \_$ is a projective functor and any projective functor is a unique direct sum of indecomposable projective functors, the claim follows from (3) and the assumptions. □

We now state and show the key property of the functor A.

Lemma 10. *For any $w \in W$ we have*

$$\dim \mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}), \theta_w L(\boldsymbol{w})) = \dim \mathrm{Hom}_{\mathfrak{g}}(\overline{D}^{\hat{\boldsymbol{R}}}, \theta_w \overline{D}^{\hat{\boldsymbol{R}}}).$$

Proof. Since $L(\boldsymbol{w}) \in \mathscr{C}_2$, we have $\theta_w L(\boldsymbol{w}) \in \mathscr{C}_2$ by Lemma 3. Hence, by Proposition 4(v), we have that A does not annihilate $L(\boldsymbol{w})$, that A does not annihilate any simple submodule of $\theta_w L(\boldsymbol{w})$, and that A does not annihilate any homomorphism $\varphi : L(\boldsymbol{w}) \to \theta_w L(\boldsymbol{w})$. Therefore, applying A we obtain an inclusion

$$\mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}), \theta_w L(\boldsymbol{w})) \subset \mathrm{Hom}_{\mathfrak{g}}(\mathrm{A}L(\boldsymbol{w}), \mathrm{A}\theta_w L(\boldsymbol{w})).$$

Using Lemma 7 and the definition of $\overline{D}^{\hat{\boldsymbol{R}}}$ we thus get the inclusion

$$\mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}), \theta_w L(\boldsymbol{w})) \subset \mathrm{Hom}_{\mathfrak{g}}(\overline{D}^{\hat{\boldsymbol{R}}}, \theta_w \overline{D}^{\hat{\boldsymbol{R}}}). \tag{4}$$

On the other hand, consider the short exact sequence

$$0 \to L(\boldsymbol{w}) \to \overline{D}^{\hat{\boldsymbol{R}}} \to C \to 0, \tag{5}$$

where C is the cokernel. Applying the exact functor θ_w yields the short exact sequence

$$0 \to \theta_w L(\boldsymbol{w}) \to \theta_w \overline{D}^{\hat{\boldsymbol{R}}} \to \theta_w C \to 0. \tag{6}$$

Applying the bifunctor $\mathrm{Hom}_{\mathfrak{g}}(\_, \_)$ from sequence (5) to sequence (6) yields the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathfrak{g}}(C,\theta_w L(\boldsymbol{w})) & \hookrightarrow & \mathrm{Hom}_{\mathfrak{g}}(C,\theta_w \bar{D}^{\hat{\boldsymbol{R}}}) & \longrightarrow & \mathrm{Hom}_{\mathfrak{g}}(C,\theta_w C) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}_{\mathfrak{g}}(\bar{D}^{\hat{\boldsymbol{R}}},\theta_w L(\boldsymbol{w})) & \hookrightarrow & \mathrm{Hom}_{\mathfrak{g}}(\bar{D}^{\hat{\boldsymbol{R}}},\theta_w \bar{D}^{\hat{\boldsymbol{R}}}) & \longrightarrow & \mathrm{Hom}_{\mathfrak{g}}(\bar{D}^{\hat{\boldsymbol{R}}},\theta_w C) \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}),\theta_w L(\boldsymbol{w})) & \hookrightarrow & \mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}),\theta_w \bar{D}^{\hat{\boldsymbol{R}}}) & \longrightarrow & \mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}),\theta_w C).
\end{array}$$

We have $C, \theta_w C \in \mathscr{C}_1$ by definitions and Lemmata 3 and 8. We also have $L(\boldsymbol{w}) \in \mathscr{C}_3$. This yields $\mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}), \theta_w C) = 0$, which implies

$$\mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}), \theta_w L(\boldsymbol{w})) = \mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}), \theta_w \bar{D}^{\hat{\boldsymbol{R}}}).$$

Since $C \in \mathscr{C}_1$ while $\bar{D}^{\hat{\boldsymbol{R}}}, \theta_w \bar{D}^{\hat{\boldsymbol{R}}} \in \mathscr{C}_2$ by definitions and Lemma 3, we have $\mathrm{Hom}_{\mathfrak{g}}(C, \theta_w \bar{D}^{\hat{\boldsymbol{R}}}) = 0$, which yields the inclusion

$$\mathrm{Hom}_{\mathfrak{g}}(\bar{D}^{\hat{\boldsymbol{R}}}, \theta_w \bar{D}^{\hat{\boldsymbol{R}}}) \subset \mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}), \theta_w \bar{D}^{\hat{\boldsymbol{R}}}).$$

This, together with the equality obtained in the previous paragraph, implies the opposite inclusion to (4); that is,

$$\mathrm{Hom}_{\mathfrak{g}}(\bar{D}^{\hat{\boldsymbol{R}}}, \theta_w \bar{D}^{\hat{\boldsymbol{R}}}) \subset \mathrm{Hom}_{\mathfrak{g}}(L(\boldsymbol{w}), \theta_w L(\boldsymbol{w})).$$

The statement of the lemma follows. □

Lemma 11. *The inclusion $L(\boldsymbol{w}) \subset \bar{D}^{\hat{\boldsymbol{R}}}$ induces an isomorphism of $\mathfrak{g}$-bimodules as follows*: $\mathscr{L}(L(\boldsymbol{w}), L(\boldsymbol{w})) \cong \mathscr{L}(\bar{D}^{\hat{\boldsymbol{R}}}, \bar{D}^{\hat{\boldsymbol{R}}})$.

Proof. Applying the bifunctor $\mathscr{L}(\_\,,\_\,)$ to (5), we get the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccc}
\mathscr{L}(C, L(\boldsymbol{w})) & \hookrightarrow & \mathscr{L}(C, \bar{D}^{\hat{\boldsymbol{R}}}) & \longrightarrow & \mathscr{L}(C, C) \\
\downarrow & & \downarrow & & \downarrow \\
\mathscr{L}(\bar{D}^{\hat{\boldsymbol{R}}}, L(\boldsymbol{w})) & \hookrightarrow & \mathscr{L}(\bar{D}^{\hat{\boldsymbol{R}}}, \bar{D}^{\hat{\boldsymbol{R}}}) & \longrightarrow & \mathscr{L}(\bar{D}^{\hat{\boldsymbol{R}}}, C) \\
\downarrow & & \downarrow & & \downarrow \\
\mathscr{L}(L(\boldsymbol{w}), L(\boldsymbol{w})) & \hookrightarrow & \mathscr{L}(L(\boldsymbol{w}), \bar{D}^{\hat{\boldsymbol{R}}}) & \longrightarrow & \mathscr{L}(L(\boldsymbol{w}), C).
\end{array} \tag{7}$$

Note that for any $w \in W$ we have $C, \theta_w C \in \mathscr{C}_1$ by definitions and Lemma 3, while $L(\boldsymbol{w}) \in \mathscr{C}_3$. Hence from [Jantzen 1983, 6.8(3)], as in the proof of Lemma 9 we have $\mathscr{L}(L(\boldsymbol{w}), C) = 0$ implying $\mathscr{L}(L(\boldsymbol{w}), L(\boldsymbol{w})) \cong \mathscr{L}(L(\boldsymbol{w}), \bar{D}^{\hat{\boldsymbol{R}}})$.

Since for any $w \in W$ we have $\overline{D}^{\hat{R}}, \theta_w \overline{D}^{\hat{R}} \in \mathscr{C}_2$ by the definitions and Lemma 3, while $C \in \mathscr{C}_1$, from [Jantzen 1983, 6.8(3)] it follows that $\mathscr{L}(C, \overline{D}^{\hat{R}}) = 0$, implying $\mathscr{L}(\overline{D}^{\hat{R}}, \overline{D}^{\hat{R}}) \subset \mathscr{L}(L(\boldsymbol{w}), \overline{D}^{\hat{R}})$.

Hence $\mathscr{L}(\overline{D}^{\hat{R}}, \overline{D}^{\hat{R}}) \subset \mathscr{L}(L(\boldsymbol{w}), L(\boldsymbol{w}))$ and the proof is completed by applying Lemmata 9 and 10. □

Proof of implication (b)⇒(a) in Theorem 5. When (b) of Theorem 5 holds, then from Lemma 8(ii) we have $\overline{D}^{\hat{R}} = D^{\hat{R}}$. The module $D^{\hat{R}}$ is a quotient of the dominant Verma module $\Delta(e)$, and hence $U(\mathfrak{g})$ surjects onto $\mathscr{L}(D^{\hat{R}}, D^{\hat{R}})$ by [Jantzen 1983, 6.9(10)]. Lemma 11 and diagram (7) now give the induced surjection of $U(\mathfrak{g})$ onto $\mathscr{L}(L(\boldsymbol{w}), L(\boldsymbol{w}))$. This completes the proof. □

To prove the reverse implication, we will need some more properties of the functor A.

Lemma 12. (i) $\mathrm{A}\overline{D}^{\hat{R}} \cong \overline{D}^{\hat{R}}$.

(ii) $\mathrm{A}D^{\hat{R}} \cong \overline{D}^{\hat{R}}$.

(iii) *For any $w \in W$ there is an isomorphism*

$$\mathrm{Hom}_{\mathfrak{g}}(D^{\hat{R}}, \theta_w \overline{D}^{\hat{R}}) \cong \mathrm{Hom}_{\mathfrak{g}}(\overline{D}^{\hat{R}}, \theta_w \overline{D}^{\hat{R}}).$$

Proof. We have $L(\boldsymbol{w}) \in \mathscr{C}_2$ and hence $\overline{D}^{\hat{R}} = \mathrm{A}L(\boldsymbol{w}) \in \mathscr{C}_2$ by Proposition 4(iii). Therefore (i) follows from Proposition 4(vii).

Consider the short exact sequence

$$0 \to D^{\hat{R}} \to \overline{D}^{\hat{R}} \to C \to 0, \tag{8}$$

where $C \in \mathscr{C}_1$ is the cokernel. We have $\mathrm{A}C = 0$ by Proposition 4(ii). Now applying A to (8) and using (i) and the left exactness of A, we see that Proposition 4(i) yields statement (ii).

Since $C \in \mathscr{C}_1$ and $\overline{D}^{\hat{R}}, \theta_w \overline{D}^{\hat{R}} \in \mathscr{C}_2$, applying $\mathrm{Hom}_{\mathfrak{g}}(\_, \theta_w \overline{D}^{\hat{R}})$ to (8) yields the inclusion

$$\mathrm{Hom}_{\mathfrak{g}}(\overline{D}^{\hat{R}}, \theta_w \overline{D}^{\hat{R}}) \subset \mathrm{Hom}_{\mathfrak{g}}(D^{\hat{R}}, \theta_w \overline{D}^{\hat{R}}). \tag{9}$$

On the other hand, both $D^{\hat{R}}$ and $\theta_w \overline{D}^{\hat{R}}$ belong to $\mathscr{C}_2$. Thus the functor A does not annihilate $D^{\hat{R}}$, does not annihilate any submodule of $\theta_w \overline{D}^{\hat{R}}$, and does not annihilate any morphism between these two modules (Proposition 4(v)). Hence, we have the inclusion

$$\mathrm{Hom}_{\mathfrak{g}}(D^{\hat{R}}, \theta_w \overline{D}^{\hat{R}}) \subset \mathrm{Hom}_{\mathfrak{g}}(\mathrm{A}D^{\hat{R}}, \mathrm{A}\theta_w \overline{D}^{\hat{R}}).$$

Using (ii), Lemma 7 and (i) we obtain

$$\mathrm{Hom}_{\mathfrak{g}}(\mathrm{A}D^{\hat{R}}, \mathrm{A}\theta_w \overline{D}^{\hat{R}}) = \mathrm{Hom}_{\mathfrak{g}}(\overline{D}^{\hat{R}}, \theta_w \mathrm{A}\overline{D}^{\hat{R}}) = \mathrm{Hom}_{\mathfrak{g}}(\overline{D}^{\hat{R}}, \theta_w \overline{D}^{\hat{R}}),$$

which implies that inclusion (9) is in fact an isomorphism. This completes the proof. □

Proof of implication (a)⇒(b) in Theorem 5. The inclusion $L(\boldsymbol{w}) \subset D^{\hat{\boldsymbol{R}}}$ induces the inclusion $\mathrm{Ann}_{U(\mathfrak{g})}(D^{\hat{\boldsymbol{R}}}) \subset \mathrm{Ann}_{U(\mathfrak{g})}(L(\boldsymbol{w}))$, which, in turn, induces the surjection

$$U(\mathfrak{g})/\mathrm{Ann}_{U(\mathfrak{g})}(D^{\hat{\boldsymbol{R}}}) \twoheadrightarrow U(\mathfrak{g})/\mathrm{Ann}_{U(\mathfrak{g})}(L(\boldsymbol{w})). \tag{10}$$

Assume that (b) of Theorem 5 does not hold. As we have $\mathscr{L}(D^{\hat{\boldsymbol{R}}}, D^{\hat{\boldsymbol{R}}}) \cong U(\mathfrak{g})/\mathrm{Ann}_{U(\mathfrak{g})}(D^{\hat{\boldsymbol{R}}})$ by [Jantzen 1983, 6.9(10)], from the latter formula and (10) it follows that the inequality

$$\mathscr{L}(D^{\hat{\boldsymbol{R}}}, D^{\hat{\boldsymbol{R}}}) \subsetneq \mathscr{L}(L(\boldsymbol{w}), L(\boldsymbol{w})) \cong \mathscr{L}(\overline{D}^{\hat{\boldsymbol{R}}}, \overline{D}^{\hat{\boldsymbol{R}}}) \tag{11}$$

would imply that the algebra $U(\mathfrak{g})$ does not surject onto $\mathscr{L}(L(\boldsymbol{w}), L(\boldsymbol{w}))$ (since the image of $U(\mathfrak{g})$ coincides with $\mathscr{L}(D^{\hat{\boldsymbol{R}}}, D^{\hat{\boldsymbol{R}}})$). Hence, what's left is to prove inequality (11).

We apply the bifunctor $\mathscr{L}(\_\,, \_\,)$ to short exact sequence (8), where the cokernel $C \neq 0$ by Lemma 8(ii). Since $C \in \mathscr{C}_1$ and $D^{\hat{\boldsymbol{R}}}$, $\theta_w D^{\hat{\boldsymbol{R}}}$, $\overline{D}^{\hat{\boldsymbol{R}}}$ and $\theta_w \overline{D}^{\hat{\boldsymbol{R}}}$ are in $\mathscr{C}_2$ for all $w \in W$, by [Jantzen 1983, 6.8(3)] we obtain the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccc}
0 & \longrightarrow & 0 & \longrightarrow & \mathscr{L}(C, C) \\
\downarrow & & \downarrow & & \uparrow \\
\mathscr{L}(\overline{D}^{\hat{\boldsymbol{R}}}, D^{\hat{\boldsymbol{R}}}) & \hookrightarrow & \mathscr{L}(\overline{D}^{\hat{\boldsymbol{R}}}, \overline{D}^{\hat{\boldsymbol{R}}}) & \longrightarrow & \mathscr{L}(\overline{D}^{\hat{\boldsymbol{R}}}, C) \\
\uparrow & & \downarrow \wr & & \downarrow \\
\mathscr{L}(D^{\hat{\boldsymbol{R}}}, D^{\hat{\boldsymbol{R}}}) & \hookrightarrow & \mathscr{L}(D^{\hat{\boldsymbol{R}}}, \overline{D}^{\hat{\boldsymbol{R}}}) & \xrightarrow{\alpha} & \mathscr{L}(D^{\hat{\boldsymbol{R}}}, C),
\end{array} \tag{12}$$

where the isomorphism in the second column follows from Lemma 12(iii). To complete the proof it is thus enough to show that the map α on diagram (12) is nonzero.

Pick some simple submodule $L(x) \subset C$ (recall once more that $C \neq 0$ by Lemma 8(ii)). Using the adjointness and defining properties of projective functors, we have

$$\begin{aligned}
\mathbb{C} &= \mathrm{Hom}_{\mathfrak{g}}(P^{\hat{\boldsymbol{R}}}(x), L(x)) \\
&= \mathrm{Hom}_{\mathfrak{g}}(\theta_x P^{\hat{\boldsymbol{R}}}(e), L(x)) \\
&= \mathrm{Hom}_{\mathfrak{g}}(P^{\hat{\boldsymbol{R}}}(e), \theta_{x^{-1}} L(x)) \\
&\subset \mathrm{Hom}_{\mathfrak{g}}(P^{\hat{\boldsymbol{R}}}(e), \theta_{x^{-1}} C).
\end{aligned} \tag{13}$$

Let K be the kernel of the natural projection $P^{\hat{\boldsymbol{R}}}(e) \twoheadrightarrow D^{\hat{\boldsymbol{R}}}$ (note that $K \in \mathscr{C}_1$ by [MS 2008b, Lemmata 5 and 7]). Applying the bifunctor $\mathrm{Hom}_{\mathfrak{g}}(\_\,, \_\,)$ from the

short exact sequence

$$0 \to K \to P^{\hat{\boldsymbol{R}}}(e) \to D^{\hat{\boldsymbol{R}}} \to 0$$

to the short exact sequence

$$0 \to \theta_{x^{-1}} D^{\hat{\boldsymbol{R}}} \to \theta_{x^{-1}} \bar{D}^{\hat{\boldsymbol{R}}} \to \theta_{x^{-1}} C \to 0,$$

we obtain the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccc}
\mathrm{Hom}_{\mathfrak{g}}(D^{\hat{\boldsymbol{R}}}, \theta_{x^{-1}} D^{\hat{\boldsymbol{R}}}) & \hookrightarrow & \mathrm{Hom}_{\mathfrak{g}}(D^{\hat{\boldsymbol{R}}}, \theta_{x^{-1}} \bar{D}^{\hat{\boldsymbol{R}}}) & \twoheadrightarrow & \mathrm{Hom}_{\mathfrak{g}}(D^{\hat{\boldsymbol{R}}}, \theta_{x^{-1}} C) \\
\downarrow \wr & & \downarrow \wr & \overset{\beta}{\searrow} & \downarrow \\
\mathrm{Hom}_{\mathfrak{g}}(P^{\hat{\boldsymbol{R}}}(e), \theta_{x^{-1}} D^{\hat{\boldsymbol{R}}}) & \hookrightarrow & \mathrm{Hom}_{\mathfrak{g}}(P^{\hat{\boldsymbol{R}}}(e), \theta_{x^{-1}} \bar{D}^{\hat{\boldsymbol{R}}}) & \twoheadrightarrow & \mathrm{Hom}_{\mathfrak{g}}(P^{\hat{\boldsymbol{R}}}(e), \theta_{x^{-1}} C) \\
\downarrow & & \downarrow & & \downarrow \\
0 & \to & 0 & \to & \mathrm{Hom}_{\mathfrak{g}}(K, \theta_{x^{-1}} C),
\end{array}$$

where the second row is exact as $P^{\hat{\boldsymbol{R}}}(e)$ is projective in $\mathbb{O}_0^{\hat{\boldsymbol{R}}}$, and the zeros in the third row follow from the fact that $K \in \mathscr{C}_1$ while $\theta_{x^{-1}} \bar{D}^{\hat{\boldsymbol{R}}} \in \mathscr{C}_2$. From (13) it follows that the composition β is a surjection onto a nonzero vector space, hence is a nonzero map. The map α contains, as a direct summand, the image of the map β under the canonical isomorphism of [Jantzen 1983, 6.8]. Hence $\alpha \neq 0$. This completes the proof. □

3.2. ***A sufficient condition for a negative answer.*** Let Λ be the basic (that is, with one-dimensional simple modules) finite-dimensional associative algebra, whose module category is equivalent to $\mathbb{O}_0$. The algebra Λ is Koszul [Soergel 1990], so we can fix the positive Koszul $\mathbb{Z}$-grading on Λ. Let Λ-gmod denote the category of finite-dimensional graded Λ-modules. For $w \in W$ let e_w be the primitive idempotent of Λ, corresponding to w. Then we have the corresponding graded indecomposable projective module Λe_w (where the grading is induced from that on Λ). For $x \in \hat{\boldsymbol{R}}$, let $\mathsf{P}^{\hat{\boldsymbol{R}}}(x)$ denote the maximal quotient of Λe_x that belongs to $\mathbb{O}^{\hat{\boldsymbol{R}}}$ after forgetting the grading. The module $\mathsf{P}^{\hat{\boldsymbol{R}}}(x)$ is the standard graded lift of $P^{\hat{\boldsymbol{R}}}(x)$ with head concentrated in degree zero (see [MS 2008a, 4.3]). Let $\mathsf{L}(x)$ denote the simple quotient of $\mathsf{P}^{\hat{\boldsymbol{R}}}(x)$. Then $\mathsf{L}(x)$ is the standard graded lift of the corresponding simple quotient (concentrated in degree zero). For $w \in W$ we denote by $\hat{\theta}_w$ the standard graded lift of the functors θ_w [Stroppel 2003, Section 8]. Finally, let $\boldsymbol{a} : W \to \mathbb{Z}$ denote Lusztig's $\boldsymbol{a}$-function [1985], which is uniquely determined by the properties that it is constant on the two-sided cells of W and equals the length of the longest element w_0' (which belongs to this two-sided cell) of a parabolic subgroup of W.

If M is a graded module, then $\mathsf{M} = \bigoplus_{i\in\mathbb{Z}} \mathsf{M}_i$ is the decomposition of M into a direct sum of graded components. As usual, for $k \in \mathbb{Z}$ we denote by $\langle k\rangle : \Lambda\text{-gmod} \to \Lambda\text{-gmod}$ the functor that shifts the grading such that $\mathsf{M}\langle k\rangle_i = \mathsf{M}_{i+k}$.

Lemma 13. *Let $\boldsymbol{w} \in W$ be an involution and $\mathsf{M} = \hat{\theta}_{\boldsymbol{w}}\mathsf{L}(\boldsymbol{w})$. Then*:

(i) $\mathsf{M}_i = 0$ *for all i such that $|i| > \boldsymbol{a}(\boldsymbol{w})$.*

(ii) $\mathsf{M}_{\boldsymbol{a}(\boldsymbol{w})}$ *is the simple socle of* M *and is isomorphic to the module* $\mathsf{L}(\boldsymbol{w})\langle -\boldsymbol{a}(\boldsymbol{w})\rangle$.

Proof. Since $\boldsymbol{a}$ is an invariant of two-sided cells, by [MS 2008a, Theorem 18] we may without loss of generality assume that $\boldsymbol{w}$ is the maximal element of some parabolic subgroup. For such a $\boldsymbol{w}$, statement (i) follows immediately from [Stroppel 2003, Theorem 8.2]. Moreover, the same argument implies $\mathsf{M}_{\boldsymbol{a}(\boldsymbol{w})} \neq 0$.

As Λ is positively graded and M is injective (the latter follows from [MS 2008a, Section 5] and [MS 2008b, Key statement]), $\mathsf{M}_{\boldsymbol{a}(\boldsymbol{w})} \neq 0$ must be the simple socle of M. On the other hand, we know that $\theta_{\boldsymbol{w}} L(\boldsymbol{w}) = P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})$. Hence the simple socle of M is isomorphic (up to a shift of grading) to $\mathsf{L}(\boldsymbol{w})$. Claim (ii) follows and the proof is complete. □

Theorem 14. *Let $\boldsymbol{w} \in W$ be an involution and $\mathsf{M} = \hat{\theta}_{\boldsymbol{w}}\mathsf{L}(\boldsymbol{w})$. Assume that there exists $x \in W$ such that $x <_{\mathsf{R}} \boldsymbol{w}$ and*

$$[\mathsf{M} : \mathsf{L}(x)\langle 1 - \boldsymbol{a}(\boldsymbol{w})\rangle] > [\mathsf{P}^{\hat{\boldsymbol{R}}}(e) : \mathsf{L}(x)\langle 1 - \boldsymbol{a}(\boldsymbol{w})\rangle].$$

Then Kostant's problem has a negative answer for $L(\boldsymbol{w})$.

Proof. Let N be the quotient of M modulo $D^{\hat{\boldsymbol{R}}}$. As $D^{\hat{\boldsymbol{R}}}$ is nonzero, it must contain the socle of M. Hence $\mathsf{N}_i = 0$ for all $i \geq \boldsymbol{a}(\boldsymbol{w})$ by Lemma 13. By our assumption, $\mathsf{N}_{\boldsymbol{a}(\boldsymbol{w})-1}$ contains at least one copy of $\mathsf{L}(x)\langle 1 - \boldsymbol{a}(\boldsymbol{w})\rangle$.

Since Λ is positively graded and $\mathsf{N}_i = 0$ for all $i \geq \boldsymbol{a}(\boldsymbol{w})$, the space $\mathsf{N}_{\boldsymbol{a}(\boldsymbol{w})-1}$ belongs to the socle of N. Thus the condition (b) of Theorem 5 is not satisfied and the answer to Kostant's problem for $L(\boldsymbol{w})$ is negative by Theorem 5. □

Remark 15. As $\mathsf{P}^{\hat{\boldsymbol{R}}}(e)$ is a quotient of the graded dominant Verma module $\Delta(e)$, in Theorem 14 one could use a stronger assumption

$$[\mathsf{M} : \mathsf{L}(x)\langle 1 - \boldsymbol{a}(\boldsymbol{w})\rangle] > [\Delta(e) : \mathsf{L}(x)\langle 1 - \boldsymbol{a}(\boldsymbol{w})\rangle]$$

with the same result.

Remark 16. The numerical condition of Theorem 14 is relatively easy to check (using a computer, for example), because it can be easily formulated in terms of Kazhdan–Lusztig combinatorics [Kazhdan and Lusztig 1979; Björner and Brenti 2005]. Via the standard categorification approach to $\mathbb{C}$ (see for example [MS 2008a, 3.4]), the characters of graded Λ-modules can be considered as elements of the Hecke algebra $\mathcal{H}$ of W (such that Verma modules correspond to the standard basis

of $\mathscr{H}$, projective modules correspond to the Kazhdan–Lusztig basis, and simple modules correspond to the dual Kazhdan–Lusztig basis). There are effective algorithms that allow one to multiply elements of $\mathscr{H}$ and to transform them from one of the mentioned basis to the other. Some of the applications presented in the next section are obtained using this approach.

Remark 17. The statement of Lemma 13 has a strong resemblance with [Mazorchuk 2007, Theorem 16], and is in some sense the Koszul dual of it (see the proof there for details).

4. Applications

In this section we present several applications of our main result, which show that it can be effectively applied in various situations. Unfortunately, we are still quite far from the complete answer.

4.1. ***Kostant's problem for the socle of the dominant Verma module in a parabolic category.*** Let $\mathfrak{p} \subset \mathfrak{g}$ be a parabolic subalgebra containing $\mathfrak{h} \oplus \mathfrak{n}_+$, and let $\mathbb{O}_0^{\mathfrak{p}}$ be the corresponding parabolic subcategory of $\mathbb{O}_0$ in the sense of [Rocha-Caridi 1980]. Let $W' \subset W$ be the Weyl group of the Levi factor of $\mathfrak{p}$, w_0 be the longest element in W and w_0' be the longest element in W'. Then

$$\mathbb{O}_0^{\mathfrak{p}} = \mathbb{O}_0^{\hat{\boldsymbol{R}}},$$

where $\boldsymbol{R}$ is the right cell of the element $w_0' w_0$; see [MS 2008a, Remark 14]. Let $\boldsymbol{w}$ be the involution in $\boldsymbol{R}$. The following result is mentioned at the end of [McGovern 1994, Section 3] without proof.

Corollary 18. *Kostant's problem has a positive answer for* $L(\boldsymbol{w})$.

Proof. The category $\mathbb{O}_0^{\mathfrak{p}}$ is known to be a highest weight category in the sense of [Cline et al. 1988]. Thus any projective-injective module in $\mathbb{O}_0^{\mathfrak{p}}$ is tilting in the sense of [Ringel 1991]; in particular, it has a filtration by standard modules (that is, generalized Verma modules, induced from simple finite-dimensional $\mathfrak{p}$-modules). In particular, the dominant standard module $P^{\hat{\boldsymbol{R}}}(e)$ is a submodule of $P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})$, and the cokernel of this inclusion again has a filtration by standard modules. Since all standard modules belong to $\mathscr{C}_2$ by [Irving 1985] (see also [MS 2008c, Theorem 5.1] for a short argument), we obtain that the condition (b) of Theorem 5 is satisfied and hence Kostant's problem has a positive answer for $L(\boldsymbol{w})$ by Theorem 5. □

Remark 19. The inclusion $P^{\hat{\boldsymbol{R}}}(e) \subset P^{\hat{\boldsymbol{R}}}(\boldsymbol{w})$ implies that Conjecture 2 is true if $\boldsymbol{R}$ contains some $w_0' w_0$.

Remark 20. Corollary 18 holds for all semisimple finite-dimensional Lie algebras.

4.2. ***Kostant's problem for $L(s)$, where s is a simple reflection.***

Corollary 21 [Mazorchuk 2005]. *Let $s \in W$ be a simple reflection. Then Kostant's problem has a positive answer for $L(s)$.*

Proof. The only element of W that is strictly smaller than s with respect to the order $<_{\mathsf{R}}$ is the identity element e, as, by adjointness,

$$\dim \mathrm{Hom}_{\mathfrak{g}}(P^{\hat{\boldsymbol{R}}}(e), \theta_s L(s)) = \dim \mathrm{Hom}_{\mathfrak{g}}(P^{\hat{\boldsymbol{R}}}(s), L(s)) = 1,$$

the module $L(e)$ occurs in $\theta_s L(s)$ with multiplicity one, and hence $L(e)$ does not occur in the cokernel of the inclusion $D^{\hat{\boldsymbol{R}}} \subset \theta_s L(s)$ at all. Therefore the condition (b) of Theorem 5 is obviously satisfied and hence Kostant's problem has a positive answer for $L(s)$ by Theorem 5. □

4.3. ***Kostant's problem for $L(st)$, where s and t are commuting simple reflections.*** Here we generalize the counterexample, constructed in [MS 2008b, Section 5]. Let $s_i = (i, i+1)$, $i = 1, \dots, n-1$, be the ith simple reflection in W. We recall that for a simple reflection $s \in W$ and any $x \in W$ such that $xs < x$ with respect to the Bruhat order, we have that the module $\hat{\theta}_s \mathsf{L}(x)$ is self-dual with simple head and socle, and we moreover have the following graded picture of this module (the middle row is in degree 0, and the arrows schematically represent the action of elements from the algebra Λ):

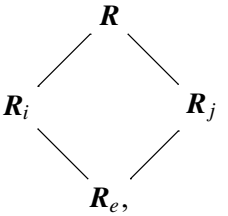
$$\begin{array}{ccc} & \mathsf{L}(x)\langle 1\rangle & \\ \swarrow & & \searrow \\ \mathsf{L}(xs) & & X \\ \searrow & & \swarrow \\ & \mathsf{L}(x)\langle -1\rangle, & \end{array} \tag{14}$$

where X is a direct sum of modules $L(y)$ such that $ys > y$, and the multiplicity of $L(y)$ in X is $\mu(x, y)$, where μ is Kazhdan and Lusztig's μ-function [1979]. The latter is a standard corollary of the now proved Kazhdan–Lusztig conjecture in the equivalent form given by Vogan (see [Kazhdan and Lusztig 1979; Gabber and Joseph 1981b; Vogan 1979]). We also refer to Remark 16 and to [Stroppel 2003, Section 8] for the appropriate graded reformulation.

Corollary 22. *Let s_i and s_j be two commuting different simple reflections in W (that is, $|i-j| > 1$). Then Kostant's problem has a positive answer for $L(s_i s_j)$ if and only if $|i-j| > 2$.*

Proof. Without loss of generality we assume $j > i$. Let $\boldsymbol{R}_e = \{e\}$, $\boldsymbol{R}_i$ denote the right cell of s_i, $\boldsymbol{R}_j$ denote the right cell of s_j, and $\boldsymbol{R}$ denote the right cell of

$s_i s_j$. Then the Hasse diagram of $<_{\mathsf{R}}$ on the set $\{\boldsymbol{R}_e, \boldsymbol{R}_i, \boldsymbol{R}_j, \boldsymbol{R}\}$, where $\boldsymbol{R}$ is the maximum element, is as follows:



and we further have

$$\boldsymbol{R}_i = \{s_i, s_i s_{i-1}, \dots, s_i s_{i-1} \dots s_1, s_i s_{i+1}, \dots, s_i s_{i+1} \dots s_{n-1}\};$$
$$\boldsymbol{R}_j = \{s_j, s_j s_{j-1}, \dots, s_j s_{j-1} \dots s_1, s_j s_{j+1}, \dots, s_j s_{j+1} \dots s_{n-1}\}.$$

A direct calculation gives $\theta_{s_i}\theta_{s_j} = \theta_{s_i s_j} = \theta_{s_j}\theta_{s_i}$.

Assume first that $j = i+2$. Since both $s_i s_{i+2}$ and $s_i s_{i+1} s_{i+2}$ are Boolean elements of W (in the sense of [Marietti 2006]), we have that the Kazhdan–Lusztig polynomial $P_{s_i s_{i+2}, s_i s_{i+1} s_{i+2}}(q) = 1$ by [Marietti 2006, Theorem 5.4] and hence $\mu(s_i s_{i+2}, s_i s_{i+1} s_{i+2}) = 1$ as well by definition. This yields

$$\mathrm{Ext}^1_{\mathbb{O}}(L(s_i s_{i+2}), L(s_i s_{i+1} s_{i+2})) \neq 0,$$

and thus $L(s_i s_{i+1} s_{i+2})$ occurs as a composition subquotient in $\theta_{s_i} L(s_i s_{i+2})$ (as a direct summand of X in (14)). Applying (14), we get that $\mathsf{L}(s_i s_{i+1} s_{i+2})\langle -1\rangle$ occurs as a composition subquotient in $\hat{\theta}_{s_i s_{i+2}} \mathsf{L}(s_i s_{i+2})$. Note that we have

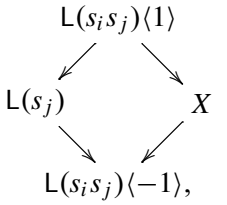
$$s_i s_{i+1} s_{i+2} <_{\mathsf{R}} s_i s_{i+2}.$$

At the same time, from [Dixmier 1996, Lemma 7.2.5], it follows that $\mathsf{P}^{\hat{\boldsymbol{R}}}(e)_1$ contains only composition subquotients of the form $\mathsf{L}(s_k)\langle -1\rangle$, $k = 1, \dots, n-1$. Hence the numerical assumption of Theorem 14 is satisfied and therefore the answer to Kostant's problem for $L(s_i s_{i+2})$ is negative by Theorem 14.

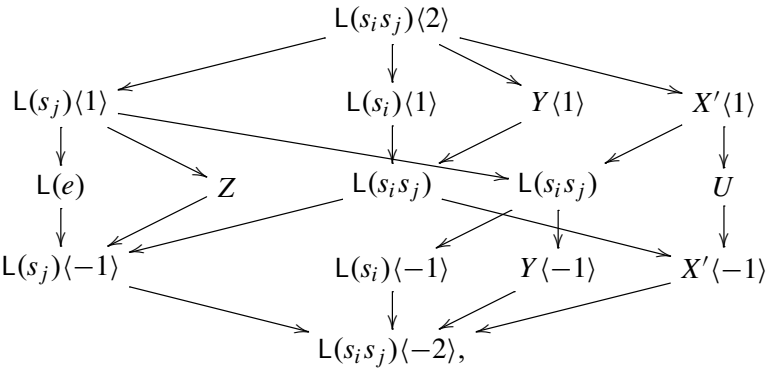
If $j > i+2$, a similar application of [Marietti 2006, Theorem 5.4] yields

$$\mu(s_i s_j, s_i s_{i+1} \dots s_{j-1} s_j) = 0 \quad \text{and} \quad \mu(s_i s_j, s_j s_{j-1} \dots s_{i+1} s_i) = 0.$$

The only other elements of $\boldsymbol{R}_i$ and $\boldsymbol{R}_j$, comparable with $s_i s_j$ with respect to the Bruhat order, are s_i and s_j respectively. Because of (14), this means that the module $\hat{\theta}_{s_i} \mathsf{L}(s_i s_j)$ looks as follows:

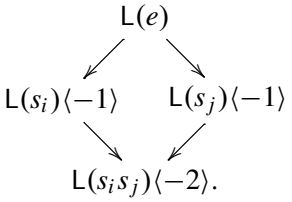


where X is a direct sum of simple modules $L(y)$, $y \in \boldsymbol{R}$. Applying now $\hat{\theta}_{s_j}$ and using (14) again we obtain the following graded filtration for the module $\hat{\theta}_{s_i s_j} \mathsf{L}(s_i s_j)$:



(15)

where Z is a direct sum of simple modules of the form $L(y)$, $y \in \boldsymbol{R}_j$; Y is a direct sum of simples modules of the form $L(y)$, $y \in \boldsymbol{R}$; and X' is a direct summand of X. Note that the arrows on (15) (which are supposed to schematically represent the action of Λ) show only the part of the action, which obviously comes from (14), but they do not show the whole action. From [Dixmier 1996, Lemma 7.2.5] it follows that the module $\mathsf{D}^{\hat{\boldsymbol{R}}}$ looks as follows:



Now we have to analyze (15) to determine the cokernel C of the inclusion $\mathsf{D}^{\hat{\boldsymbol{R}}} \subset \hat{\theta}_{s_i s_j} \mathsf{L}(s_i s_j)$. C obviously contains both $Y\langle -1\rangle$ and $X'\langle -1\rangle$, but all direct summands of these modules have the form $L(y)$, $y \in \boldsymbol{R}$, by the above. None of the simple subquotients of U can occur as a submodule in C by (14). Similarly one excludes $\mathsf{L}(s_i)\langle 1\rangle$ and $\mathsf{L}(s_i)\langle 1\rangle$. All simple submodules in Z have the form $L(y)$, $y \in \boldsymbol{R}_j$. Considering $\hat{\theta}_{s_i s_j} \mathsf{L}(s_i s_j) = \hat{\theta}_{s_i} \hat{\theta}_{s_j} \mathsf{L}(s_i s_j)$ and using the same arguments as above, one shows that none of the simple submodules of Z belongs to C. Hence C contains only simple modules of the form $L(y)$, $y \in \boldsymbol{R}$. Thus the condition (b) of Theorem 5 is satisfied and therefore Kostant's problem has a positive answer for $L(s_i s_j)$ by Theorem 5. This completes the proof. □

4.4. *Kostant's problem for $\mathfrak{sl}_n$, $n \leq 3$.*

Proposition 23. *Assume that $n \leq 3$ and $w \in W$. Then Kostant's problem has a positive answer for $L(w)$.*

Proof. The statement is trivial for $n = 1$. In the case $n = 2$ for $w = e$ the statement follows from [Jantzen 1983, 6.9(10)] (as $L(e)$ is a quotient of the dominant Verma module) and for $w = s_1$ it follows from [Joseph 1980, Corollary 6.4] (as $L(s_1)$ is a Verma module).

Finally, in the case $n = 3$ for $w = e$ the statement follows, as above, from [Jantzen 1983, 6.9(10)], for $w = s_1, s_2$ it follows from Corollary 21, for $w = s_1s_1, s_2s_1$ it follows from [Gabber and Joseph 1981a, Theorem 4.4], and, finally, for $w = s_1s_2s_1$ it follows, as above, from [Joseph 1980, Corollary 6.4]. □

4.5. *Kostant's problem for* $\mathfrak{sl}_4$.

Proposition 24. *Assume that $n = 4$ and $w \in W$. Then Kostant's problem has a positive answer for $L(w)$ if and only if $w \neq s_1s_3, s_2s_1s_3$.*

Proof. The group S_4 has 10 involutions: e, s_1, s_2, s_3, s_1s_3, $s_1s_2s_1$, $s_3s_2s_3$, $s_2s_1s_3s_2$, $s_1s_2s_3s_2s_1$, and $s_2s_1s_2s_3s_2s_1$. The module $L(e)$ is a quotient of the dominant Verma module, and hence for $L(e)$ the claim follows from [Jantzen 1983, 6.9(10)]. The module $L(s_2s_1s_2s_3s_2s_1)$ is a Verma module and hence for this module the claim follows from [Joseph 1980, Corollary 6.4]. For $L(s_1)$, $L(s_2)$, $L(s_3)$ the claim follows from Corollary 21. The left cell of each of the elements $s_1s_2s_1$, $s_3s_2s_3$, $s_2s_1s_3s_2$, $s_1s_2s_3s_2s_1$ contains an element of the form $w_0'w_0$, where w_0' is the longest element of some parabolic subgroup. Hence for $L(s_1s_2s_1)$, $L(s_3s_2s_3)$, $L(s_2s_1s_3s_2)$ and $L(s_1s_2s_3s_2s_1)$ the claim follows from [Gabber and Joseph 1981a, Theorem 4.4] and [MS 2008a, Theorem 60]. Finally, for $L(s_1s_3)$ the claim follows from Corollary 22 (or [MS 2008b, Theorem 13]). Note that the answer is negative only in the case of $L(s_1s_3)$. The left cell of s_1s_3 contains one more element, namely $s_2s_1s_3$. The statement of the proposition now follows from [MS 2008a, Theorem 60]. □

4.6. *Kostant's problem for* $\mathfrak{sl}_5$.

Proposition 25. *Assume that $n = 5$ and $w \in W$. Then Kostant's problem has a positive answer for $L(w)$ if and only if w does not belong to the left cells containing one of the following involutions*: s_1s_3, s_2s_4, $s_2s_3s_2$, $s_1s_2s_1s_4$ *or* $s_1s_3s_4s_3$.

Proof. The group S_5 has 26 involutions. As above, Kostant's problem has a positive answer for $L(e)$ since it is a quotient of the dominant Verma module. The answers for $L(s_1)$, $L(s_2)$, $L(s_3)$ and $L(s_4)$ are also positive by Corollary 21, and for $L(s_1s_2s_1s_3s_2s_1s_4s_3s_2s_1)$ the answer is positive as this module is a Verma module. The involutions

$$
\begin{array}{lll}
s_1s_2s_1, & s_1s_2s_1s_3s_2s_1, & s_1s_2s_3s_4s_3s_2s_1,\\
s_3s_4s_3, & s_2s_3s_2s_4s_3s_2, & s_2s_1s_3s_2s_1s_4s_3s_2,\\
s_3s_2s_4s_3, & s_1s_3s_2s_1s_4s_3, & s_1s_2s_3s_2s_4s_3s_2s_1,\\
s_2s_1s_3s_2, & s_2s_1s_3s_4s_3s_2, & s_1s_2s_1s_3s_4s_3s_2s_1,
\end{array}
$$

are all in left cells containing elements of the form $w_0' w_0$ where w_0' is the longest element of some parabolic subgroup of W. Hence Kostant's problem has a positive answer for the corresponding simple modules by [Gabber and Joseph 1981a, Theorem 4.4] and [MS 2008a, Theorem 60]. The involutions $s_2s_3s_4s_3s_2$ and $s_2s_4s_3s_2s_1$ are both in left cells containing elements on the form $sw_0' w_0$, where w_0' is the longest element of some parabolic subgroup, and s is a simple reflection of the same parabolic subgroup, so Kostant's problem has a positive answer for $L(s_2s_4s_3s_2s_1)$ and $L(s_2s_3s_4s_3s_2)$ by [Mazorchuk 2005, Theorem 1] and [MS 2008a, Theorem 60]. Kostant's problem has a positive answer for $L(s_1s_4)$ and a negative answer for $L(s_1s_3)$ and $L(s_2s_4)$, by Corollary 22.

Finally, the fact that Kostant's problem has a negative answer for $L(s_2s_3s_2)$, $L(s_1s_3s_4s_3)$ and $L(s_1s_2s_1s_4)$ follows from Theorem 14 by a direct computation as described in Remark 16. Consider first the involution $s_2s_3s_2$ for which we have $\mathtt{a}(s_2s_3s_2) = 3$. A direct calculation shows that the graded component $\mathsf{P}^{\hat{\boldsymbol{R}}}(s_2s_3s_2)_2$ has the following form after forgetting the grading:

$$L(s_3s_2) \oplus L(s_3s_2s_4s_3) \oplus L(s_2s_1s_3s_2s_4s_3) \oplus L(s_3s_2s_1s_4s_3s_2) \\ \oplus L(s_2s_3s_2s_1) \oplus L(s_2s_3) \oplus L(s_2s_1s_3s_2) \oplus L(s_2s_3s_2s_4).$$

Another calculation shows that the graded component $\Delta(e)_2$ has the following form after forgetting the grading:

$$L(s_3s_4) \oplus L(s_2s_4) \oplus L(s_2s_1) \oplus L(s_3s_2) \oplus L(s_1s_3) \oplus L(s_1s_4) \\ \oplus L(s_4s_3) \oplus L(s_1s_2) \oplus L(s_2s_3) \oplus L(s_2s_1s_3s_2) \oplus L(s_3s_2s_4s_3).$$

Hence the module $L(s_3s_2s_1s_4s_3s_2)$ occurs in $\mathsf{P}^{\hat{\boldsymbol{R}}}(s_2s_3s_2)_2$ but not in $\Delta(e)_2$. Note that $s_3s_2s_1s_4s_3s_2 <_{\mathsf{R}} s_2s_3s_2$. By Theorem 14 and Remark 15 this implies that Kostant's problem has a negative answer for $L(s_2s_3s_2)$.

For the involution $s_1s_2s_1s_4$ we have $\mathtt{a}(s_1s_2s_1s_4) = 4$. A direct calculation shows that the module $L(s_1s_4s_3s_2s_1)$ occurs in $\mathsf{P}^{\hat{\boldsymbol{R}}}(s_1s_2s_1s_4)_3$ but not in $\Delta(e)_3$. Again, Remark 15 implies that Kostant's problem has a negative answer for $L(s_1s_2s_1s_4)$. Applying the symmetry of the root system we obtain that the answer for $L(s_4s_3s_4s_1)$ is also negative and it remains to observe that $s_4s_3s_4s_1 = s_1s_3s_4s_3$. □

The Robinson–Schensted correspondence associates to each $w \in S_5$ a pair

$$(\alpha(x), \beta(x))$$

of standard Young tableaux of the same shape [Sagan 2001, 3.1]. The shape defines a two-sided cell. Fixing $\alpha(x)$ or $\beta(x)$ defines a right or a left cell inside the two-sided cell, respectively. We show on the next page the three two-sided cells of S_5 that contain left cells for elements of which Kostant's problem has a negative answer. The rows and columns in these figures are indexed by the corresponding $\alpha(x)$

	$\begin{array}{\|c\|c\|c\|}\hline 1&2&3\\\hline 4&5\\\cline{1-2}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&2&4\\\hline 3&5\\\cline{1-2}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&3&4\\\hline 2&5\\\cline{1-2}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&3&5\\\hline 2&4\\\cline{1-2}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&2&5\\\hline 3&4\\\cline{1-2}\end{array}$
$\begin{array}{\|c\|c\|c\|}\hline 1&2&3\\\hline 4&5\\\cline{1-2}\end{array}$	3243	324	3214	32143	321432
$\begin{array}{\|c\|c\|c\|}\hline 1&2&4\\\hline 3&5\\\cline{1-2}\end{array}$	243	24	214	2143	21432
$\begin{array}{\|c\|c\|c\|}\hline 1&3&4\\\hline 2&5\\\cline{1-2}\end{array}$	1321	124	14	143	1432
$\begin{array}{\|c\|c\|c\|}\hline 1&3&5\\\hline 2&4\\\cline{1-2}\end{array}$	13243	1324	134	13	132
$\begin{array}{\|c\|c\|c\|}\hline 1&2&5\\\hline 3&4\\\cline{1-2}\end{array}$	213243	21324	2134	213	2132

↑ ↑

	$\begin{array}{\|c\|c\|c\|}\hline 1&2&3\\\hline 4\\\cline{1-1}5\\\cline{1-1}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&2&4\\\hline 3\\\cline{1-1}5\\\cline{1-1}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&2&5\\\hline 3\\\cline{1-1}4\\\cline{1-1}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&3&4\\\hline 2\\\cline{1-1}5\\\cline{1-1}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&3&5\\\hline 2\\\cline{1-1}4\\\cline{1-1}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&4&5\\\hline 2\\\cline{1-1}3\\\cline{1-1}\end{array}$
$\begin{array}{\|c\|c\|c\|}\hline 1&2&3\\\hline 4\\\cline{1-1}5\\\cline{1-1}\end{array}$	343	3432	32432	34321	324321	3214321
$\begin{array}{\|c\|c\|c\|}\hline 1&2&4\\\hline 3\\\cline{1-1}5\\\cline{1-1}\end{array}$	2343	23432	2432	234321	24321	214321
$\begin{array}{\|c\|c\|c\|}\hline 1&2&5\\\hline 3\\\cline{1-1}4\\\cline{1-1}\end{array}$	23243	2324	232	23214	2321	21321
$\begin{array}{\|c\|c\|c\|}\hline 1&3&4\\\hline 2\\\cline{1-1}5\\\cline{1-1}\end{array}$	12343	123432	12432	1234321	124321	14321
$\begin{array}{\|c\|c\|c\|}\hline 1&3&5\\\hline 2\\\cline{1-1}4\\\cline{1-1}\end{array}$	123243	12324	1232	123214	12321	1321
$\begin{array}{\|c\|c\|c\|}\hline 1&4&5\\\hline 2\\\cline{1-1}3\\\cline{1-1}\end{array}$	1213243	121324	12132	12134	1213	121

↑

	$\begin{array}{\|c\|c\|c\|}\hline 1&2\\\hline 3&4\\\cline{1-2}5\\\cline{1-1}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&2\\\hline 3&5\\\cline{1-2}4\\\cline{1-1}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&3\\\hline 2&4\\\cline{1-2}5\\\cline{1-1}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&3\\\hline 2&5\\\cline{1-2}4\\\cline{1-1}\end{array}$	$\begin{array}{\|c\|c\|c\|}\hline 1&4\\\hline 2&5\\\cline{1-2}3\\\cline{1-1}\end{array}$
$\begin{array}{\|c\|c\|c\|}\hline 1&2\\\hline 3&4\\\cline{1-2}5\\\cline{1-1}\end{array}$	213432	2132432	21343	21324321	2134321
$\begin{array}{\|c\|c\|c\|}\hline 1&2\\\hline 3&5\\\cline{1-2}4\\\cline{1-1}\end{array}$	2321432	21321432	232143	2132143	213214
$\begin{array}{\|c\|c\|c\|}\hline 1&3\\\hline 2&4\\\cline{1-2}5\\\cline{1-1}\end{array}$	13432	132432	1343	1324321	134321
$\begin{array}{\|c\|c\|c\|}\hline 1&3\\\hline 2&5\\\cline{1-2}3\\\cline{1-1}\end{array}$	12321432	1321432	1232143	132143	13214
$\begin{array}{\|c\|c\|c\|}\hline 1&4\\\hline 2&5\\\cline{1-2}3\\\cline{1-1}\end{array}$	1213432	121432	121343	12143	1214

↑ ↑

and $\beta(x)$, respectively. The left cells for which Kostant's problem has a negative answer are marked by arrows. Each element is denoted simply by the sequence of indices in some reduced expression, that is, $s_1s_3s_2$ is denoted by 132. There seems to exist some hidden symmetry in these pictures, but we do not understand it yet.

4.7. ***Kostant's problem for*** $\mathfrak{sl}_6$**.** We are not able yet to give a complete answer to Kostant's problem in the case $\mathfrak{g} = \mathfrak{sl}_6$. The group S_6 has 76 involutions. For 45 involutions one can use arguments analogous to the arguments above to show that Kostant's problem has a positive answer; for 20 involutions one can analogously show that Kostant's problem has a negative answer. This leaves 11 involutions for which the answer is still unclear.

There are 39 involutions that lie in left cells containing an element of the form $w_0'w_0$ or $sw_0'w_0$, and hence Kostant's problem has a positive answer for these involutions. From Corollary 22 it follows that Kostant's problem has a positive answer for $L(s_1s_4)$, $L(s_1s_5)$ and $L(s_2s_5)$.

The module $\theta_{\boldsymbol{w}}L(\boldsymbol{w})$ is a quotient of an indecomposable projective module from $\mathbb{O}$. The latter module has a Verma filtration. Classical results on inclusions of Verma modules [Dixmier 1996, Chapter 7] may be used in some cases to analyze the socle of the cokernel of $D^{\hat{\boldsymbol{R}}} \hookrightarrow \theta_{\boldsymbol{w}}L(\boldsymbol{w})$. Combined with Theorem 14, these arguments imply that Kostant's problem has a positive answer for $L(s_2s_1s_3s_2)$, $L(s_3s_2s_4s_3)$ and $L(s_4s_3s_5s_4)$. We omit the details.

By Corollary 22, Kostant's problem has a negative answer for $L(s_1s_2)$, $L(s_2s_4)$ and $L(s_3s_5)$. This, and computations as described in Remark 16, show that Kostant's problem has a negative answer for the following 17 involutions:

$$
\begin{array}{llll}
s_1s_3, & s_1s_3s_5, & s_1s_4s_3s_5s_4, & s_1s_2s_1s_4s_5s_4,\\
s_3s_5, & s_1s_2s_1s_4 & s_2s_1s_3s_2s_5, & s_1s_2s_1s_3s_2s_1s_5,\\
s_2s_4, & s_1s_3s_4s_3, & s_1s_2s_3s_2s_1s_5, & s_1s_3s_4s_3s_5s_4s_3,\\
s_2s_3s_2, & s_2s_4s_5s_4, & s_1s_3s_4s_5s_4s_3, & s_1s_3s_2s_1s_4s_5s_4s_3,\\
s_3s_4s_3, & s_2s_3s_2s_5, & s_2s_3s_2s_4s_3s_2, & s_1s_2s_1s_3s_4s_3s_5s_4s_3s_2s_1.
\end{array}
$$

The remaining 11 involutions, which are not covered by Theorem 14, are:

$$
\begin{array}{lll}
s_1s_2s_1s_5, & s_2s_4s_3s_2s_5s_4, & s_1s_3s_2s_4s_3s_2s_1s_5s_4s_3,\\
s_1s_4s_5s_4, & s_2s_1s_4s_3s_2s_5s_4, & s_2s_1s_3s_2s_1s_4s_5s_4s_3s_2,\\
s_2s_3s_4s_3s_2, & s_1s_2s_3s_2s_4s_3s_2s_1, & s_2s_1s_3s_2s_4s_3s_2s_1s_5s_4s_3s_2.\\
s_2s_1s_3s_4s_3s_2, & s_2s_3s_2s_4s_5s_4s_3s_2. &
\end{array}
$$

For these involutions the answer is still unclear. Some further progress in this case was recently made in [Kåhrström 2010].

Acknowledgments

Mazorchuk's research was partially supported by the Swedish Research Council. The authors thank the referee for very useful comments.

References

[Bernstein and Gel'fand 1980] J. N. Bernstein and S. I. Gel'fand, "Tensor products of finite- and infinite-dimensional representations of semisimple Lie algebras", *Compositio Math.* **41**:2 (1980), 245–285. MR 82c:17003

[Bernstein et al. 1976] I. N. Bernstein, I. M. Gel'fand, and S. I. Gel'fand, "A certain category of $\mathfrak{g}$-modules", *Funkcional. Anal. i Priložen.* **10**:2 (1976), 1–8. In Russian; translated in *Funct. Anal. Appl.* **10** (1976), 87–92. MR 53 #10880

[Björner and Brenti 2005] A. Björner and F. Brenti, *Combinatorics of Coxeter groups*, Grad. Texts in Math. **231**, Springer, New York, 2005. MR 2006d:05001 Zbl 1110.05001

[Borho and Brylinski 1982] W. Borho and J.-L. Brylinski, "Differential operators on homogeneous spaces, I: Irreducibility of the associated variety for annihilators of induced modules", *Invent. Math.* **69**:3 (1982), 437–476. MR 84b:17007

[Cline et al. 1988] E. Cline, B. Parshall, and L. Scott, "Finite dimensional algebras and highest weight categories", *J. Reine Angew. Math.* **391** (1988), 85–99. MR 90d:18005 Zbl 0657.18005

[Conze-Berline and Duflo 1977] N. Conze-Berline and M. Duflo, "Sur les représentations induites des groupes semi-simples complexes", *Compositio Math.* **34**:3 (1977), 307–336. MR 55 #12872 Zbl 0389.22016

[Dixmier 1996] J. Dixmier, *Enveloping algebras*, Grad. Studies in Math. **11**, American Mathematical Society, Providence, RI, 1996. MR 97c:17010 Zbl 0867.17001

[Gabber and Joseph 1981a] O. Gabber and A. Joseph, "On the Bernšteĭn–Gel'fand–Gel'fand resolution and the Duflo sum formula", *Compositio Math.* **43**:1 (1981), 107–131. MR 82k:17009

[Gabber and Joseph 1981b] O. Gabber and A. Joseph, "Towards the Kazhdan–Lusztig conjecture", *Ann. Sci. École Norm. Sup.* (4) **14**:3 (1981), 261–302. MR 83e:17009 Zbl 0476.17005

[Irving 1985] R. S. Irving, "Projective modules in the category $\mathcal{O}_S$: self-duality", *Trans. Amer. Math. Soc.* **291**:2 (1985), 701–732. MR 87i:17005 Zbl 0594.17005

[Jantzen 1983] J. C. Jantzen, *Einhüllende Algebren halbeinfacher Lie-Algebren*, Ergebnisse der Mathematik **3**, Springer, Berlin, 1983. MR 86c:17011

[Joseph 1979] A. Joseph, "W-module structure in the primitive spectrum of the enveloping algebra of a semisimple Lie algebra", pp. 116–135 in *Noncommutative harmonic analysis* (Marseille, 1978), edited by J. Carmona and M. Vergne, Lecture Notes in Math. **728**, Springer, Berlin, 1979. MR 80k:17007 Zbl 0422.17004

[Joseph 1980] A. Joseph, "Kostant's problem, Goldie rank and the Gel'fand–Kirillov conjecture", *Invent. Math.* **56**:3 (1980), 191–213. MR 82f:17008

[Kåhrström 2010] J. Kåhrström, "Kostant's problem and parabolic subgroups", *Glasgow Math. J.* **52**:1 (2010), 19–32. Zbl 05656554

[Kazhdan and Lusztig 1979] D. Kazhdan and G. Lusztig, "Representations of Coxeter groups and Hecke algebras", *Invent. Math.* **53**:2 (1979), 165–184. MR 81j:20066 Zbl 0499.20035

[Khomenko and Mazorchuk 2004] O. Khomenko and V. Mazorchuk, "Structure of modules induced from simple modules with minimal annihilator", *Canad. J. Math.* **56**:2 (2004), 293–309. MR 2005b:17012 Zbl 1071.17004

[Khomenko and Mazorchuk 2005] O. Khomenko and V. Mazorchuk, "On Arkhipov's and Enright's functors", *Math. Z.* **249**:2 (2005), 357–386. MR 2005k:17004 Zbl 1103.17002

[Lusztig 1985] G. Lusztig, "Cells in affine Weyl groups", pp. 255–287 in *Algebraic groups and related topics* (Kyoto/Nagoya, 1983), edited by R. Hotta, Adv. Stud. Pure Math. **6**, North-Holland, Amsterdam, 1985. MR 87h:20074 Zbl 0569.20032

[Marietti 2006] M. Marietti, "Boolean elements in Kazhdan–Lusztig theory", *J. Algebra* **295**:1 (2006), 1–26. MR 2006i:20004 Zbl 1097.20035

[Mazorchuk 2005] V. Mazorchuk, "A twisted approach to Kostant's problem", *Glasg. Math. J.* **47**:3 (2005), 549–561. MR 2007a:17018 Zbl 1081.17007

[Mazorchuk 2007] V. Mazorchuk, "Some homological properties of the category $\mathcal{O}$", *Pacific J. Math.* **232**:2 (2007), 313–341. MR 2008m:17013 Zbl 05366268

[Mazorchuk 2009] V. Mazorchuk, "Some homological properties of the category $\mathcal{O}$, II", preprint, 2009. To appear in *Rep. Theory*. arXiv 0909.2729

[MS 2008a] V. Mazorchuk and C. Stroppel, "Categorification of (induced) cell modules and the rough structure of generalised Verma modules", *Adv. Math.* **219**:4 (2008), 1363–1426. MR 2010a:20014 Zbl 05355944

[MS 2008b] V. Mazorchuk and C. Stroppel, "Categorification of Wedderburn's basis for $\mathbb{C}[S_n]$", *Arch. Math.* (*Basel*) **91**:1 (2008), 1–11. MR 2009g:17006 Zbl 05323275

[MS 2008c] V. Mazorchuk and C. Stroppel, "Projective-injective modules, Serre functors and symmetric algebras", *J. Reine Angew. Math.* **616** (2008), 131–165. MR 2009e:16027 Zbl 05344019

[McGovern 1994] W. M. McGovern, "A remark on differential operator algebras and an equivalence of categories", *Compositio Math.* **90**:3 (1994), 305–313. MR 95a:17013 Zbl 0842.17009

[Miličić and Soergel 1997] D. Miličić and W. Soergel, "The composition series of modules induced from Whittaker modules", *Comment. Math. Helv.* **72**:4 (1997), 503–520. MR 99e:17010 Zbl 0956.17004

[Ringel 1991] C. M. Ringel, "The category of modules with good filtrations over a quasi-hereditary algebra has almost split sequences", *Math. Z.* **208**:2 (1991), 209–223. MR 93c:16010 Zbl 0725.16011

[Rocha-Caridi 1980] A. Rocha-Caridi, "Splitting criteria for $\mathfrak{g}$-modules induced from a parabolic and the Berňsteĭn–Gel'fand–Gel'fand resolution of a finite-dimensional, irreducible $\mathfrak{g}$-module", *Trans. Amer. Math. Soc.* **262**:2 (1980), 335–366. MR 82f:17006 Zbl 0449.17008

[Sagan 2001] B. E. Sagan, *The symmetric group: representations, combinatorial algorithms, and symmetric functions*, 2nd ed., Grad. Texts in Math. **203**, Springer, New York, 2001. MR 2001m:05261 Zbl 0964.05070

[Soergel 1990] W. Soergel, "Kategorie $\mathcal{O}$, perverse Garben und Moduln über den Koinvarianten zur Weylgruppe", *J. Amer. Math. Soc.* **3**:2 (1990), 421–445. MR 91e:17007

[Stroppel 2003] C. Stroppel, "Category $\mathcal{O}$: gradings and translation functors", *J. Algebra* **268**:1 (2003), 301–326. MR 2004i:17007 Zbl 1040.17002

[Vogan 1979] D. A. Vogan, Jr., "Irreducible characters of semisimple Lie groups, II: The Kazhdan–Lusztig conjectures", *Duke Math. J.* **46**:4 (1979), 805–859. MR 81f:22024

Communicated by Georgia Benkart
Received 2008-06-18 Revised 2009-10-17 Accepted 2009-12-31

Johan.Karstrom@gmail.com *Department of Mathematics, Uppsala University, 75106 Uppsala, Sweden*

mazor@math.uu.se *Department of Mathematics, Uppsala University, 75106 Uppsala, Sweden*
http://www.math.uu.se/~mazor/

ALGEBRA AND NUMBER THEORY 4:3(2010)

Twisted root numbers of elliptic curves semistable at primes above 2 and 3

Ryota Matsuura

Let E be an elliptic curve over a number field F, and fix a rational prime p. Put $F^\infty = F(E[p^\infty])$, where $E[p^\infty]$ is the group of p-power torsion points of E. Let τ be an irreducible self-dual complex representation of $\mathrm{Gal}(F^\infty/F)$. With certain assumptions on E and p, we give explicit formulas for the root number $W(E, \tau)$. We use these root numbers to study the growth of the rank of E in its own division tower and also to count the trivial zeros of the L-function of E. Moreover, our assumptions ensure that the p-division tower of E is nonabelian.

In the process of computing the root number, we also study the irreducible self-dual complex representations of $\mathrm{GL}(2, \mathcal{O})$, where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$, for p an odd prime. Among all such representations, those that factor through $\mathrm{PGL}(2, \mathcal{O})$ have been analyzed in detail in existing literature. We give a complete description of those irreducible self-dual complex representations of $\mathrm{GL}(2, \mathcal{O})$ that do not factor through $\mathrm{PGL}(2, \mathcal{O})$.

1. Introduction

We study the growth of the Mordell–Weil rank of an elliptic curve in its own division tower. Our approach will be based on root number calculation. Let E an elliptic curve over a number field F, and p a rational prime. Put $F^\infty = F(E[p^\infty])$, where $E[p^\infty]$ is the group of p-power torsion points of E. Given an irreducible self-dual complex representation τ of $\mathrm{Gal}(F^\infty/F)$, we define the associated root number $W(E, \tau)$ [Rohrlich 1996, pp. 329 and 336] and the L-function $L(s, E, \tau)$ [Rohrlich 1994, pp. 151 and 156]. Since τ is self-dual, the conjectural functional equation of $L(s, E, \tau)$ relates this function to itself and therefore we obtain

$$W(E, \tau) = (-1)^{\mathrm{ord}_{s=1} L(s,E,\tau)}.$$

The conjectures of Birch–Swinnerton-Dyer and Deligne–Gross [Rohrlich 1990, p. 127], moreover, imply that $\mathrm{ord}_{s=1} L(s, E, \tau)$ is equal to the multiplicity of τ in $\mathbb{C} \otimes_{\mathbb{Z}} E(F^\infty)$. Thus if we assume the standard conjectures, then $W(E, \tau) = -1$

MSC2000: primary 11G05; secondary 11F80, 11G40.

Keywords: elliptic curves, root number, Mordell–Weil rank.

The author gratefully acknowledges the support of NSF grant EHR 0314692.

lets us conclude that τ occurs in $\mathbb{C} \otimes_{\mathbb{Z}} E(F^\infty)$. Using this observation, we prove, for example, that if E is an elliptic curve over $\mathbb{Q}$ which is semistable at primes 2 and 3, and if p is a sufficiently large prime with $p \equiv 3 \pmod 4$, then the rank of E is unbounded in its p-division tower, provided that the standard conjectures hold.

The goal of this paper is to give explicit formulas for $W(E, \tau)$ under some simplifying assumptions on E and p. These assumptions are the same as in [Rohrlich 2006], except we relax the semistability condition by requiring E to be semistable over F only at primes of F above 2 and 3. In most cases, our formulas are identical to or differ only slightly from those of Rohrlich. However, despite the similarity in the final results, the calculations behind them are quite different, because if an elliptic curve is not semistable at a prime then the twisted local root number depends crucially on the way in which τ decomposes into irreducibles when restricted to the local Galois group. The "semistable part" of our calculation will simply be quoted from Rohrlich's paper, and most of our effort will go into the group theory needed to handle the nonsemistable case. Moreover, we remark that our assumptions ensure that the p-division tower of E is nonabelian.

As another application, we use our root number formulas to count the trivial zeros of the L-function of E over $F(E[p^n])$, where $E[p^n]$ denotes the group of p^n-torsion points of E. By *trivial zeros*, we mean the zeros at $s = 1$ which arise from the functional equation of the L-function. As remarked in [Rohrlich 2008], these trivial zeros are "virtual" in the sense that the functional equations in question are still mostly conjectural.

In the process of computing the root number, we also study the irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$, where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$, for p an odd prime. (In this paper, as was the case in [Rohrlich 2006], a *representation* of a topological group is always meant to be continuous, finite-dimensional, and defined over the complex numbers.) Among all such representations, those that factor through $\mathrm{PGL}(2, \mathcal{O})$ have been analyzed in detail by Silberger [1970]. In the present paper, we will give a complete description of those irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$ that do not factor through $\mathrm{PGL}(2, \mathcal{O})$.

2. Statement of the main theorem

As in the introduction, let F be a number field, E an elliptic curve over F, p a rational prime, and $F^\infty = F(E[p^\infty])$. Let τ be an irreducible self-dual representation of $\mathrm{Gal}(F^\infty/F)$. We will compute the root number $W(E, \tau)$ under the following assumptions:

- E is semistable over F at the primes of F above 2 and 3.
- p is odd.

- The natural embedding of $\mathrm{Gal}(F^\infty/F)$ into $\mathrm{Aut}(T_p(E))$ is an isomorphism.
- If v is a finite place of F, where E has bad reduction, then $v \nmid p$. Furthermore, if $v(j(E)) < 0$, then $p \nmid v(j(E))$.

The third condition allows us to identify $\mathrm{Gal}(F^\infty/F)$ with $\mathrm{GL}(2, \mathbb{Z}_p)$. Since the choice of basis for $T_p(E)$ over $\mathbb{Z}_p$ implicit in such an identification does not affect the resulting correspondence between isomorphism classes of representations, we may view τ as an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$.

2A. ***List of representations.*** In this section (and in Section 3), we consider representations of a slightly more general group. Let p be an odd prime and F_v a finite extension of $\mathbb{Q}_p$. Let $\mathcal{O}$ and $\mathfrak{p}$ denote the ring of integers and the maximal ideal of F_v, respectively. Let q be the order of the residue class field $\mathcal{O}/\mathfrak{p}$, and put $\mathcal{O}^n = \mathcal{O}/\mathfrak{p}^n$ for $n \geq 1$.

Given an irreducible representation τ of $\mathrm{GL}(2, \mathcal{O})$, we define its *central character*

$$\omega_\tau : \mathcal{O}^\times \to \mathbb{C}^\times$$

as follows. Take $a \in \mathcal{O}^\times$ and let I be the 2×2 identity matrix. Schur's Lemma implies that $\tau(a \cdot I)$ is multiplication by $\omega_\tau(a)$. We remark that ω_τ is trivial if and only if τ factors through $\mathrm{PGL}(2, \mathcal{O})$.

We say that τ is *reducible* modulo $\mathfrak{p}^n$ if it factors through $\mathrm{GL}(2, \mathcal{O}^n)$. And we say τ is *primitive* modulo $\mathfrak{p}^n$ if n is the smallest such integer. For $n \geq 1$, let $\mathfrak{T}_n$ be the set of isomorphism classes of irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$ with nontrivial central character that are primitive modulo $\mathfrak{p}^n$. The set $\mathfrak{T}'_n$ is defined in the same way except that the central character is assumed to be trivial. By convention, the characters 1 and λ of $\mathrm{PGL}(2, \mathcal{O})$ defined in the next paragraph are primitive modulo $\mathfrak{p}^0$. Thus we put $\mathfrak{T}'_0 = \{1, \lambda\}$.

2A.1. *Representations of* $\mathrm{PGL}(2, \mathcal{O})$. We begin by giving a complete list, up to isomorphism, of the irreducible representations of $\mathrm{GL}(2, \mathcal{O})$ that factor through $\mathrm{PGL}(2, \mathcal{O})$ [Silberger 1970, pp. 96–100]. Such representations are necessarily self-dual. We let 1 denote the trivial character of $\mathrm{GL}(2, \mathcal{O})$, or of any group. Also, we let λ denote the Legendre symbol on $\mathcal{O}^\times$ or $\mathrm{GL}(2, \mathcal{O})$, that is, the unique quadratic character of these groups. Note that the Legendre symbol on $\mathrm{GL}(2, \mathcal{O})$ is the Legendre symbol on $\mathcal{O}^\times$ composed with the determinant $\mathrm{GL}(2, \mathcal{O}) \to \mathcal{O}^\times$.

Put $G = \mathrm{GL}(2, \mathcal{O})$ and let B be the upper triangular subgroup of G. For an integer $n \geq 1$, let $K(n)$ denote the kernel of reduction modulo $\mathfrak{p}^n$ on G. Given a subgroup H of G, we set $H(n) = HK(n)$; we also set $H(0) = G$. Then we can define a representation σ_n up to isomorphism by writing

$$\mathrm{ind}_{B(n)}^G 1 = \sigma_n \oplus \mathrm{ind}_{B(n-1)}^G 1.$$

Here, note that $\mathrm{ind}_{B(n-1)}^{G} 1$ is a subrepresentation of $\mathrm{ind}_{B(n)}^{G} 1$ because $B(n)$ is a subgroup of $B(n-1)$. We remark that $\sigma_1 = \sigma$, the q-dimensional *Steinberg representation* of $\mathrm{GL}(2, \mathcal{O})$, and σ_n has dimension $q^n - q^{n-2}$ for $n \geq 2$. And using σ and λ, we obtain another q-dimensional representation, namely $\sigma \otimes \lambda$.

We introduce a general notation for characters of B. Given characters μ and ν of $\mathcal{O}^\times$, we define a character $\xi_{\mu,\nu}$ of B by

$$\xi_{\mu,\nu}(b) = \mu(b_{11})\nu(b_{22}) \qquad (b \in B), \tag{1}$$

where b_{ij} is the ij-entry of b. If the conductors of μ and ν both divide $\mathfrak{p}^n$, then $\xi_{\mu,\nu}$ extends uniquely to a character of $B(n)$ trivial on $K(n)$, and we also denote this extension by $\xi_{\mu,\nu}$.

Let α be a character of $\mathcal{O}^\times$ of conductor $\mathfrak{p}^n$ and order $|\alpha| > 2$. By a *primitive principal series representation with trivial central character*, we mean a representation of the form $u_\alpha = \mathrm{ind}_{B(n)}^{G} \xi_{\alpha,\alpha^{-1}}$. Such a representation has dimension $q^n + q^{n-1}$. For $m > n$, we define a representation $u_{\alpha,m}$ up to isomorphism by writing

$$\mathrm{ind}_{B(m)}^{G} \xi_{\alpha,\alpha^{-1}} = u_{\alpha,m} \oplus \mathrm{ind}_{B(m-1)}^{G} \xi_{\alpha,\alpha^{-1}}.$$

Then $u_{\alpha,m}$ has dimension $q^m - q^{m-2}$. Also, since $u_{\alpha,m} \cong \sigma_m$ when $m \geq 2n$ [Silberger 1970, p. 59], we will assume that $n < m < 2n$. Thus, in particular, $m \geq 3$.

Let K be the unramified quadratic extension of F_v, and $\mathcal{O}_K$ and $\mathfrak{p}_K$ its ring of integers and the maximal ideal, respectively. Let π be a character of $\mathcal{O}_K^\times$ of order $|\pi| > 2$ such that $\pi|\mathcal{O}^\times = 1$. Furthermore, suppose π has conductor $\mathfrak{p}_K^n$. Then u_π^{unr} and $u_{\pi,i}^{\mathrm{unr}}$ $(n < i < 2n)$ will refer to the unramified discrete series representations of $\mathrm{PGL}(2, \mathcal{O})$ as described by Silberger [1970, p. 80]. We remark that $\dim u_\pi^{\mathrm{unr}} = q^n - q^{n-1}$ and $\dim u_{\pi,i}^{\mathrm{unr}} = q^i - q^{i-2}$.

Now let K be a ramified quadratic extension of F_v and π a character of $\mathcal{O}_K^\times$ such that $\pi|\mathcal{O}^\times = \lambda$. Also suppose π has conductor $\mathfrak{p}_K^{2n-1}$ for some $n \geq 2$ so that $|\pi| > 2$. Then u_π^{ram} and $u_{\pi,i}^{\mathrm{ram}}$ $(n < i < 2n-1)$ will refer to the ramified discrete series representations of $\mathrm{PGL}(2, \mathcal{O})$ as described by Silberger [1970, p. 80]. Note that $\dim u_\pi^{\mathrm{ram}} = q^n - q^{n-2}$ and $\dim u_{\pi,i}^{\mathrm{ram}} = q^i - q^{i-2}$.

2A.2. *Representations of* $\mathrm{GL}(2, \mathcal{O})$ *with* $\omega_\tau \neq 1$. We now consider the irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$ that do not factor through $\mathrm{PGL}(2, \mathcal{O})$. We remark that if τ is such a representation, then ω_τ is a quadratic character on $\mathcal{O}^\times$. Therefore $\omega_\tau = \lambda$, and τ factors through $\mathrm{GL}(2, \mathcal{O})/(\mathcal{O}^\times)^2$, where we identify $(\mathcal{O}^\times)^2$ with the subgroup

$$\{a^2 \cdot I : a \in \mathcal{O}^\times\} \subset \mathrm{GL}(2, \mathcal{O}).$$

In Section 3, we will define a map $\varphi_n : [\tau'] \mapsto [\tau]$, where $[\tau'] \in \mathfrak{T}'_n$ and $[\tau] \in \mathfrak{T}_n$. Then we will use our knowledge of $\mathfrak{T}'_n$ to characterize the elements of $\mathfrak{T}_n$.

Before proceeding, we mention one family of irreducible self-dual representations of $\mathrm{GL}(2,\mathcal{O})$ with $\omega_\tau \neq 1$ that play a special role in our calculations. With the notations as in (1), let $\mu = 1$ and $\nu = \lambda$, and put

$$\theta_1 = \mathrm{ind}_{B(1)}^{G} \xi_{1,\lambda}.$$

For $n \geq 2$, define a representation θ_n up to isomorphism by writing

$$\mathrm{ind}_{B(n)}^{G} \xi_{1,\lambda} = \theta_n \oplus \mathrm{ind}_{B(n-1)}^{G} \xi_{1,\lambda}.$$

We remark that $\dim \theta_1 = q+1$ and $\dim \theta_n = q^n - q^{n-2}$ for $n \geq 2$.

2B. ***The main theorem.*** For each finite place v of F, let m_v denote the order of the residue class field of v. If E has bad reduction at v, we have $p \nmid m_v$, so we can classify m_v as either a quadratic residue or a quadratic nonresidue modulo p. Let s denote the number of places v where E has split multiplicative reduction, and s_{qr} and s_{nr} the number of such places at which m_v modulo p is a quadratic residue or a quadratic nonresidue, respectively. Moreover, let u be the number of places v where E has nonsplit multiplicative reduction and m_v is a quadratic nonresidue modulo p. And as usual, let r_1 and $2r_2$ denote the number of real and complex embeddings of F.

Let T^- denote the set of finite places v of F where E has additive reduction and $v(j(E)) < 0$. Define the set T^+ in the same way except with $v(j(E)) \geq 0$. Let t_3^- and t_{nr}^- denote the number of places $v \in T^-$ such that $m_v \equiv 3 \pmod 4$ and m_v is a quadratic nonresidue modulo p, respectively.

Now let $v \in T^+$, that is, E has bad but potentially good reduction at v. Let Δ_v denote the discriminant associated to a minimal Weierstrass equation for E at v, and put

$$e_v = \frac{12}{\gcd(v(\Delta_v), 12)} \ (= 2, 3, 4, \text{or } 6). \tag{2}$$

Define the following subsets of T^+:

$$\begin{aligned}
T_2^+ &= \{v \in T^+ : e_v = 2 \text{ or } 6, \text{ and } m_v \equiv -1 \pmod 4\},\\
T_3^+ &= \{v \in T^+ : e_v = 3 \text{ and } m_v \equiv -1 \pmod 3\},\\
T_4^+ &= \{v \in T^+ : e_v = 4, \text{ and } m_v \equiv 5 \text{ or } 7 \pmod 8\},\\
T_6^+ &= \{v \in T^+ : e_v = 6 \text{ and } m_v \equiv -1 \pmod 6\}.
\end{aligned}$$

Let $t_{2,4}^+$, t_3^+, and t_6^+ denote the cardinalities of $T_2^+ \cup T_4^+$, T_3^+, and T_6^+, respectively.

Theorem 2.1. *Let τ be an irreducible self-dual representation of* $\mathrm{Gal}(F^\infty/F)$ *and let w be the integer modulo* 2 *such that $W(E,\tau) = (-1)^w$.*

- *If $\tau = 1$, then $w = r_1 + r_2 + s + t_3^- + t_{2,4}^+ + t_3^+ \pmod 2$.*
- *If $\tau = \lambda$, then $w = r_1(p+1)/2 + r_2 + s_{\mathrm{qr}} + u + t_3^- + t_{2,4}^+ + t_3^+ \pmod 2$.*

- *If* $\tau \cong \sigma$, *then*

$$w = \begin{cases} r_1(p+1)/2 + r_2 + s + t_3^- + t_{2,4}^+ + t_3^+ \pmod 2 & \text{if } p > 3, \\ r_2 + s + t_3^- + t_{2,4}^+ \pmod 2 & \text{if } p = 3. \end{cases}$$

- *If* $\tau \cong \sigma \otimes \lambda$, *then*

$$w = \begin{cases} r_1 + r_2 + s_{\mathrm{qr}} + u + t_3^- + t_{2,4}^+ + t_3^+ \pmod 2 & \text{if } p > 3, \\ r_1 + r_2 + s_{\mathrm{qr}} + u + t_3^- + t_{2,4}^+ \pmod 2 & \text{if } p = 3. \end{cases}$$

- *If* $\tau \cong \sigma_n$ *with* $n \geq 2$, *then*

$$w = \begin{cases} s_{\mathrm{nr}} + u + t_3^+ \pmod 2 & \text{if } p = 3 \text{ and } n = 2, \\ s_{\mathrm{nr}} + u \pmod 2 & \text{otherwise}. \end{cases}$$

- *If* $\tau \cong u_\alpha$, *where* α *is primitive modulo* p^n $(n \geq 1)$, *then*

$$w = \begin{cases} r_1(p-1)/2 + t_3^+ \pmod 2 & \text{if } p \equiv 1 \pmod 3 \text{ and } 3|\alpha| \nmid p^{n-1}(p-1), \\ r_1(p-1)/2 \pmod 2 & \text{otherwise}. \end{cases}$$

- *If* $\tau \cong u_\pi^{\mathrm{unr}}$, *where* π *is primitive modulo* $\mathfrak{p}_K^n$ $(n \geq 1)$, *then*

$$w = \begin{cases} r_1(p-1)/2 + t_3^+ \pmod 2 & \text{if } p \equiv -1 \pmod 3 \text{ and } \pi(1+\sqrt{-3}) \neq 1, \\ r_1(p-1)/2 + t_3^+ \pmod 2 & \text{if } p = 3 \text{ and } n = 1, \\ r_1(p-1)/2 \pmod 2 & \text{otherwise}. \end{cases}$$

- *If* $\tau \cong u_\pi^{\mathrm{ram}}$, *where* π *is primitive modulo* $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, *then*

$$w = \begin{cases} t_3^+ \pmod 2 & \text{if } p = 3 \text{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \text{otherwise}. \end{cases}$$

- *If* $[\tau] = \varphi_n([u_\pi^{\mathrm{ram}}])$, *where* π *is primitive modulo* $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, *then*

$$w = \begin{cases} t_3^+ + t_6^+ \pmod 2 & \text{if } p = 3 \text{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \text{otherwise}. \end{cases}$$

- *If* $\tau \cong \theta_n$ *with* $n \geq 1$, *then*

$$w = \begin{cases} s_{\mathrm{nr}} + u + t_{\mathrm{nr}}^- + t_3^+ + t_6^+ \pmod 2 & \text{if } p = 3 \text{ and } 1 \leq n \leq 2, \\ s_{\mathrm{nr}} + u + t_{\mathrm{nr}}^-(p-1)/2 \pmod 2 & \text{otherwise}. \end{cases}$$

In all other cases, $w = 0 \pmod 2$ *so that* $W(E, \tau) = 1$.

Remark. The criterion

$$\pi(1+\sqrt{-3}) \neq 1 \quad \text{when } \tau \cong u_\pi^{\mathrm{unr}}$$

does not depend on the choice of $\sqrt{-3}$, because $\pi(1+\sqrt{-3})\pi(1-\sqrt{-3}) = \pi(4) = 1$ (since $\pi|\mathbb{Z}_p^\times = 1$).

The following proposition serves as an illustrative example. Here we assume the standard conjectures discussed in the introduction.

Proposition 2.2. *Let E be an elliptic curve over $\mathbb{Q}$ which is semistable at 2 and 3. Choose $p \equiv 3 \pmod 4$ sufficiently large so that our assumptions on E and p are satisfied. Then, assuming the standard conjectures, the rank of E is unbounded in its p-division tower.*

Proof. Consider an integer $n \geq 2$ and choose a character α of $\mathbb{Z}_p^\times$ of conductor p^n. Moreover if $p \equiv 1 \pmod 3$, choose α so that $3|\alpha| \,||\, p^{n-1}(p-1)$. Put $\tau = u_\alpha$. Since $r_1 = 1$ and $(p-1)/2 \equiv 1 \pmod 2$, Theorem 2.1 implies $W(E, \tau) = -1$. Viewed as a representation of $\mathrm{Gal}(\mathbb{Q}^\infty/\mathbb{Q})$, the map τ factors through $\mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q})$, where $\mathbb{Q}^{(n)} = \mathbb{Q}(E[p^n])$. Then $W(E, \tau) = -1$, in conjunction with the standard conjectures, implies that the multiplicity of τ in $\mathbb{C} \otimes_{\mathbb{Z}} E(\mathbb{Q}^{(n)})$ is odd, and hence positive. Therefore, we have

$$\mathrm{rank}_{\mathbb{Z}}\, E(\mathbb{Q}^{(n)}) \geq \dim \tau = p^n + p^{n-1}$$

whence the result follows. □

2C. ***Trivial zeros of L-functions.*** For $n \geq 1$, put $F^{(n)} = F(E[p^n])$ so that we can identify $\mathrm{Gal}(F^{(n)}/F)$ with $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. As in [Rohrlich 2008], we let $\mathcal{T}_n$ denote the set of isomorphism classes of irreducible self-dual representations of $\mathrm{Gal}(F^\infty/F)$ which factor through $\mathrm{Gal}(F^{(n)}/F)$. In particular, $\mathcal{T}_n$ is the disjoint union of the sets $\mathfrak{T}_i'$ $(0 \leq i \leq n)$ and $\mathfrak{T}_j$ $(1 \leq j \leq n)$. To measure the "size" of $\mathcal{T}_n$, we define the quantity

$$\vartheta_n = \sum_{[\tau] \in \mathcal{T}_n} \dim \tau.$$

Silberger [1970, pp. 96–100] lists the number of isomorphism classes of each type of irreducible representations of $\mathrm{PGL}(2, \mathbb{Z}_p)$. And we can find their dimensions using his character tables (pp. 102–107). Moreover we will show in Section 3 that $\#\mathfrak{T}_n = p^{n-1}$ and that for $[\tau] \in \mathfrak{T}_n$,

$$\dim \tau = \begin{cases} p+1 & \text{if } n = 1, \\ p^{n-2}(p^2-1) & \text{if } n \geq 2. \end{cases}$$

Combining all of this, we obtain:

Theorem 2.3. $\vartheta_n = p^{2n} + p^{2n-1} + 2$.

Now let $\mathcal{T}_n^\pm$ be the subsets of $\mathcal{T}_n$ containing those isomorphism classes $[\tau]$ for which $W(E, \tau) = \pm 1$. Then define the quantities

$$\vartheta_n^\pm = \sum_{[\tau] \in \mathcal{T}_n^\pm} \dim \tau.$$

Let $\mathcal{T}_n^*$ denote the set of *all* isomorphism classes of irreducible representations of $\mathrm{Gal}(F^{(n)}/F)$ (i.e., not just the self-dual ones). Then we have

$$L(s, E/F^{(n)}) = \prod_{[\tau]\in\mathcal{T}_n^*} L(s, E/F, \tau)^{\dim\tau}$$

as a factorization of the L-function of E over $F^{(n)}$. If we assume the conjectural analytic continuation of the L-function, we obtain

$$\mathrm{ord}_{s=1}\, L(s, E/F^{(n)}) = \sum_{[\tau]\in\mathcal{T}_n^*} \dim\tau \cdot \mathrm{ord}_{s=1}\, L(s, E/F, \tau).$$

We restrict the sum on the right-hand side to $\mathcal{T}_n^-$ and note that the standard conjectures imply $\mathrm{ord}_{s=1}\, L(s, E/F, \tau) \geq 1$ for $[\tau] \in \mathcal{T}_n^-$. Therefore we obtain

$$\mathrm{ord}_{s=1}\, L(s, E/F^{(n)}) \geq \vartheta_n^- \tag{3}$$

so that the quantity ϑ_n^- gives a lower bound for the number of trivial zeros of $L(s, E/F^{(n)})$ at $s = 1$.

Theorem 2.4. *Suppose* $p \equiv 3 \pmod 4$ *and* $[F : \mathbb{Q}]$ *is odd.*

- *If* $p > 3$, *then* $\vartheta_n^- \sim a(1 - 1/p) \cdot p^{2n}$, *where*

$$a = \begin{cases} 1 & \text{if } t_3^+ \equiv 0 \pmod 2, \\ 2/3 & \text{if } t_3^+ \equiv 1 \pmod 2. \end{cases}$$

- *If* $p = 3$, *then* $\vartheta_n^- \sim a \cdot 3^{2n}$, *where*

$$a = \begin{cases} 2/3 & \text{if } t_3^+ \equiv t_6^+ \equiv 0 \pmod 2, \\ 8/9 & \text{if } t_3^+ \equiv 1 \text{ and } t_6^+ \equiv 0 \pmod 2, \\ 7/9 & \text{otherwise}. \end{cases}$$

Suppose $p \equiv 1 \pmod 4$ *or* $[F : \mathbb{Q}]$ *is even.*

- *Let* $p > 3$. *Then* $\vartheta_n^- = O(p^n)$ (*in fact*, $\vartheta_n^- \leq 4 \cdot p^n$) *when* $t_3^+ \equiv 0 \pmod 2$, *and* $\vartheta_n^- \sim (1/3)(1 - 1/p) \cdot p^{2n}$ *when* $t_3^+ \equiv 1 \pmod 2$.
- *Let* $p = 3$. *If* $t_3^+ \equiv t_6^+ \equiv 0 \pmod 2$, *then* $\vartheta_n^- = O(3^n)$ (*in fact*, $\vartheta_n^- \leq 4 \cdot 3^n$). *Otherwise*, *we have* $\vartheta_n^- \sim a \cdot 3^{2n}$, *where*

$$a = \begin{cases} 2/9 & \text{if } t_6^+ \equiv 0 \pmod 2, \\ 1/9 & \text{if } t_6^+ \equiv 1 \pmod 2. \end{cases}$$

Remark. An expression such as $\vartheta_n^- \sim a(1 - 1/p) \cdot p^{2n}$ means

$$\lim_{n\to\infty} \frac{\vartheta_n^-}{p^{2n}} = a(1 - 1/p).$$

Proof. Suppose $p \equiv 3 \pmod 4$ and $[F : \mathbb{Q}]$ is odd, or equivalently, $r_1(p-1)/2 \equiv 1 \pmod 2$. Suppose further that $p > 3$ and $t_3^+ \equiv 0 \pmod 2$. From Theorem 2.1, we see that $W(E, \tau) = -1$ for representations τ of the form $\tau = u_\alpha$ and $\tau = u_\pi^{\mathrm{unr}}$. There are $(p-3)/2$ representations (up to isomorphism) of the type $\tau = u_\alpha$ that are primitive modulo p, each with dimension $p+1$ [Silberger 1970, p. 96]. And for $i \geq 2$, there are $p^{i-2}(p-1)^2/2$ representations from this family that are primitive modulo p^i, each with dimension $p^i + p^{i-1}$ [Silberger 1970, pp. 98 and 102]. Thus the contribution to ϑ_n^- from the family of representations u_α is given by

$$\frac{1}{2}\Big((p-3)(p+1)+\sum_{i=2}^{n} p^{i-2}(p-1)^2(p^i+p^{i-1})\Big) = \tfrac{1}{2}(p^{2n}-p^{2n-1}-p-3). \quad (*)$$

Similarly, the family u_π^{unr} contributes to ϑ_n^- by the quantity

$$\tfrac{1}{2}(p^{2n} - p^{2n-1} - p + 1). \quad (**)$$

The representations $1, \lambda, \sigma, \sigma\otimes\lambda, \sigma_i$ $(i \geq 2)$, and θ_i $(i \geq 1)$ can also contribute to ϑ_n^-, but the sum of their contributions would be at most $O(p^n)$, making it negligible. Combining $(*)$ and $(**)$, we get $\vartheta_n^- \sim (1 - 1/p) \cdot p^{2n}$. All the other cases are handled analogously. □

We again assume the standard conjectures. The Birch–Swinnerton-Dyer conjecture states

$$\mathrm{rank}_{\mathbb{Z}}\, E(F^{(n)}) = \mathrm{ord}_{s=1}\, L(s, E/F^{(n)}). \quad (4)$$

Combining (3) and (4) and applying Theorem 2.4, we see that $\mathrm{rank}_{\mathbb{Z}}\, E(F^{(n)})$ is at least order p^{2n}, provided $p \equiv 3 \pmod 4$ and $[F : \mathbb{Q}]$ is odd. This is stronger than the bound

$$\mathrm{rank}_{\mathbb{Z}}\, E(F^{(n)}) \geq p^n + p^{n-1} \quad (5)$$

we found in the proof of Proposition 2.2. Note that this reflects the fact that (5) was obtained using only one irreducible self-dual representation τ of $\mathrm{Gal}(F^{(n)}/F)$ for which $W(E, \tau) = -1$, while ϑ_n^- was computed using *all* such representations up to isomorphism.

3. Characterizations of representations of GL(2, $\mathcal{O}$)

As in Section 2A, let p be an odd prime and let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$, let q denote the order of the residue class field $\mathcal{O}/\mathfrak{p}$, and put $\mathcal{O}^n = \mathcal{O}/\mathfrak{p}^n$ for $n \geq 1$. Our goal in this section is to characterize all irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$.

3A. ***Cardinalities.*** We begin by proving:

Theorem 3.1. $\#\mathfrak{T}_n = q^{n-1}$.

We introduce some definitions and notations. Let G be a group and c a conjugacy class of G. We put c^{-1} for the class consisting of elements x^{-1}, where $x \in c$. We say that c is *real* if $c = c^{-1}$. Suppose $c = [a]$, that is, the class c is represented by an element $a \in G$. Then one immediately sees that c is real if and only if a is conjugate to a^{-1}. We also remark that if G is finite, then the number of real-valued irreducible characters of G is equal to the number of real conjugacy classes of G [Serre 1977, p. 109, Exercise 13.9(a)].

For $n \geq 1$, put

$$K'_n = \mathrm{PGL}(2, \mathcal{O}^n) = \mathrm{GL}(2, \mathcal{O}^n)/(\mathcal{O}^n)^\times.$$

Let α_n denote the number of irreducible (self-dual) representations of K'_n up to isomorphism, or equivalently, the number of (real) conjugacy classes of K'_n. By [Silberger 1970, p. 101], we have

$$\alpha_n = 2 + q + q^2 + \cdots + q^n.$$

For $n \geq 1$, put

$$K_n = \mathrm{GL}(2, \mathcal{O}^n)/(\mathcal{O}^n)^{\times 2}.$$

Recall that for an irreducible self-dual representation τ of $\mathrm{GL}(2, \mathcal{O})$, $\omega_\tau = 1$ or λ (see Section 2A.2). Thus there is a natural one-to-one correspondence between the isomorphism classes of irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$ that are reducible modulo $\mathfrak{p}^n$ and of irreducible self-dual representations of K_n. Let β_n denote the number of irreducible self-dual representations of K_n up to isomorphism, or equivalently, the number of real conjugacy classes of K_n. To prove Theorem 3.1, we must compute β_n.

Let $K = \mathrm{GL}(2, \mathcal{O})/(\mathcal{O}^\times)^2$ and fix a nonsquare element of $\mathcal{O}^\times$, say ζ.

Lemma 3.2. *Let $A \in \mathrm{GL}(2, \mathcal{O})$. If $\det A \in (\mathcal{O}^\times)^2$, then A is conjugate to A^{-1} in K, that is, $[A]$ is real in K. And the converse holds if $\operatorname{tr} A \neq 0$.*

Proof. A calculation shows that if $A \in \mathrm{GL}(2, \mathcal{O})$ and $\det A \in (\mathcal{O}^\times)^2$, then $sAs^{-1} \equiv (A^{-1})^{\mathrm{t}}$, where $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\equiv$ denotes equivalence in K. Since every element of $\mathrm{GL}(2, \mathcal{O})$ is conjugate to its transpose (see [Rohrlich 2006, lemma on p. 364] — the proof is valid for arbitrary $\mathcal{O}$), A is conjugate to A^{-1} in K.

Now suppose $\operatorname{tr} A \neq 0$ and that A is conjugate to A^{-1} in K. Thus, A is conjugate to x^2A^{-1} in $\mathrm{GL}(2, \mathcal{O})$ for some $x \in \mathcal{O}^\times$. Taking determinants gives $\det A = \pm x^2$. If $\det A = x^2$, we are done. So assume that $\det A = -x^2$. Then a calculation shows that $\operatorname{tr}(x^2A^{-1}) = -\operatorname{tr} A$. Thus, the fact that A and x^2A^{-1} are conjugate in $\mathrm{GL}(2, \mathcal{O})$ implies $\operatorname{tr} A = -\operatorname{tr} A$ and hence $\operatorname{tr} A = 0$, a contradiction. □

The following proposition will allow us to compute β_n when $q \equiv 1 \pmod 4$.

Proposition 3.3. *Suppose $q \equiv 1 \pmod 4$ and $A \in \mathrm{GL}(2, \mathcal{O})$.*

(1) $\det A \in (\mathcal{O}^\times)^2$ *if and only if* A *is conjugate to* A^{-1} *in* K.

(2) A *is not conjugate to* ζA *in* K.

Proof. Suppose A is conjugate to A^{-1} in K. As in the proof of Lemma 3.2, we have $\det A = \pm x^2$ for some $x \in \mathcal{O}^\times$. And since $q \equiv 1 \pmod 4$, we get $\det A \in (\mathcal{O}^\times)^2$. Combining this with Lemma 3.2 gives the proof of (1).

To prove (2), suppose that A and ζA are conjugate in K. Then

$$\det A \equiv \zeta^2 \det A \pmod{(\mathcal{O}^\times)^4}.$$

Thus $\zeta^2 = x^4$ for some $x \in \mathcal{O}^\times$ so that $\zeta = \pm x^2 \in (\mathcal{O}^\times)^2$, a contradiction. □

From Proposition 3.3(2) above, we can deduce that if

$$\{A_1, A_2, \ldots, A_r\}$$

is a set of distinct conjugacy class representatives of K_n' (with $A_i \in \mathrm{GL}(2, \mathcal{O})$), then

$$\{A_1, \zeta A_1, A_2, \zeta A_2, \ldots, A_r, \zeta A_r\}$$

is a set of distinct conjugacy class representatives of K_n. Now, Silberger's list of conjugacy class representatives of K_n' [Silberger 1970, p. 101] shows that when $q \equiv 1 \pmod 4$, exactly $(\alpha_n + (q^n - 1)/(q-1))/2$ of the A_i's have $\det A_i \in (\mathcal{O}^n)^{\times 2}$. Hence:

Proposition 3.4. *Let* $q \equiv 1 \pmod 4$. *Then*

$$\beta_n = \alpha_n + \frac{q^n - 1}{q - 1}.$$

Let us now consider the case $q \equiv 3 \pmod 4$.

Proposition 3.5. *Suppose* $q \equiv 3 \pmod 4$ *and let* $A \in \mathrm{GL}(2, \mathcal{O})$. *Then* A *is conjugate to* ζA *in* K *if and only if* $\operatorname{tr} A = 0$.

Proof. Suppose A is conjugate to ζA in K. Thus $x^2 A$ is conjugate to ζA in $\mathrm{GL}(2, \mathcal{O})$ for some $x \in \mathcal{O}^\times$. Taking determinants gives $x^4 = \zeta^2$, and since ζ is a nonsquare element of $\mathcal{O}^\times$ and $q \equiv 3 \pmod 4$, we get $x^2 = -\zeta$. Therefore $-\zeta A$ is conjugate to ζA in $\mathrm{GL}(2, \mathcal{O})$, and taking traces gives $\operatorname{tr} A = 0$.

Conversely, suppose $\operatorname{tr} A = 0$. A calculation shows that $sAs^{-1} = (-A)^{\mathrm{t}}$, where $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Recalling that every element of $\mathrm{GL}(2, \mathcal{O})$ is conjugate to its transpose, we see that A is conjugate to $-A$ in $\mathrm{GL}(2, \mathcal{O})$. And since $q \equiv 3 \pmod 4$ (i.e., -1 is a nonsquare element in $\mathcal{O}^\times$), we conclude that A is conjugate to ζA in K. □

From Proposition 3.5 above, we can deduce that if the union

$$\underbrace{\{A_1, \ldots, A_r\}}_{\operatorname{tr} A_i \neq 0} \cup \underbrace{\{B_1, \ldots, B_s\}}_{\operatorname{tr} B_i = 0}$$

is a set of distinct conjugacy class representatives of K_n', then the union

$$\{A_1, \zeta A_1, \ldots, A_r, \zeta A_r\} \cup \{B_1, \ldots, B_s\}$$

is a set of distinct conjugacy class representatives of K_n. With $q \equiv 3 \pmod 4$, Silberger's list of conjugacy class representatives of K_n' shows that exactly

$$(\alpha_n + (q^n - 1)/(q - 1))/2 - 1$$

of the A_i's with $\operatorname{tr} A_i \neq 0$ have $\det A_i \in (\mathcal{O}^n)^{\times 2}$. Also from the list, the B_i's with $\operatorname{tr} B_i = 0$ are

$$\{B_i\} = \left\{ \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \zeta \\ 1 & 0 \end{smallmatrix}\right) \right\}.$$

And each B_i is conjugate to B_i^{-1} in K_n. Therefore:

Proposition 3.6. *Let $q \equiv 3 \pmod 4$. Then*

$$\beta_n = \alpha_n + \frac{q^n - 1}{q - 1}.$$

Thus, the value of β_n is the same regardless of whether q is congruent to 1 or 3 modulo 4. Finally, we obtain

$$\#\mathfrak{T}_n = (\beta_n - \beta_{n-1}) - (\alpha_n - \alpha_{n-1}) = q^{n-1},$$

which proves Theorem 3.1. Note that in contrast, $\#\mathfrak{T}_n' = \alpha_n - \alpha_{n-1} = q^n$.

3B. ***Class functions on finite groups.*** Here we introduce some more notations. Given representations π and τ of a profinite group G, we define their inner product $\langle \pi, \tau \rangle$ by

$$\langle \pi, \tau \rangle = \sum_{[\rho] \in \operatorname{Irr}(G)} (\text{multiplicity of } \rho \text{ in } \pi)(\text{multiplicity of } \rho \text{ in } \tau),$$

where $\operatorname{Irr}(G)$ is the set of isomorphism classes of irreducible representations of G.

For a finite group G, let $\operatorname{Cl}(G)$ denote the space of complex-valued class functions on G. We also define an inner product $\langle \cdot, \cdot \rangle$ on $\operatorname{Cl}(G)$ by

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)}.$$

Note that if π and τ are representations of G so that $\operatorname{tr} \pi, \operatorname{tr} \tau \in \operatorname{Cl}(G)$, we have

$$\langle \pi, \tau \rangle = \langle \operatorname{tr} \pi, \operatorname{tr} \tau \rangle.$$

Moreover, we let $X(G)$ denote the set of those $\chi \in \operatorname{Cl}(G)$ that can be written as a linear combination of irreducible characters of G with *integer* coefficients.

Suppose further that $G = G_1 \times G_2$ is a product of subgroups, and ρ_i a representation of G_i $(i = 1, 2)$. We then define the tensor product representation $\rho_1 \otimes \rho_2$ of G by

$$(\rho_1 \otimes \rho_2)(g_1, g_2) = \rho_1(g_1) \otimes \rho_2(g_2).$$

We note that if each ρ_i is irreducible, then so is their tensor product $\rho_1 \otimes \rho_2$; moreover, every irreducible representation of $G = G_1 \times G_2$ arises in this way [Serre 1977, p. 27, Theorem 10].

Proposition 3.7. *Let G be a finite group, $\zeta \in G$ a central involution, and $S \subset G$ a set of representatives for the distinct cosets in G of the central subgroup of order two generated by ζ. Fix $\chi' \in X(G)$ satisfying two conditions*:

(i) $\chi'(\zeta x) = \chi'(x)$ *for* $x \in G$.

(ii) *If* $s \in S$ *and* $\chi'(s) \neq 0$, *then* $|s|$ *is odd.*

Define a function χ on G by

$$\chi(x) = \begin{cases} \chi'(x) & \text{if } x \in S, \\ -\chi'(x) & \text{if } x \notin S. \end{cases}$$

Then $\chi \in X(G)$.

Proof. We begin by showing that χ is a class function on G. Take $g \in G$, $s \in S$, and write $gsg^{-1} = t$ or ζt with $t \in S$. Then $\chi'(s) = \chi'(t)$ because χ' is a class function on G and $\chi'(\zeta t) = \chi'(t)$. Now if $gsg^{-1} = t$, then

$$\chi(gsg^{-1}) = \chi'(t) = \chi'(s) = \chi(s)$$

by the definition of χ. If $gsg^{-1} = \zeta t$, then

$$\chi(gsg^{-1}) = -\chi'(t) = -\chi'(s) = -\chi(s).$$

If either s or t has even order, then by (ii) we conclude that $\chi(gsg^{-1})$ and $\chi(s)$ are both 0, hence equal. If $|s|$ and $|t|$ are both odd, then the equation $gsg^{-1} = \zeta t$ is impossible. Thus in all cases, we have $\chi(gsg^{-1}) = \chi(s)$. On the other hand, the definition of χ shows that $\chi(\zeta x) = -\chi(x)$ for all $x \in G$. Hence

$$\chi(g(\zeta s)g^{-1}) = \chi(\zeta gsg^{-1}) = -\chi(gsg^{-1}) = -\chi(s) = \chi(\zeta s).$$

Thus χ is a class function on G.

Now we will show that $\chi \in X(G)$. By Brauer's characterization of characters [Lang 2002, p. 709, Corollary 10.12], it suffices to show that $\chi|_E \in X(E)$ for every elementary subgroup E of G. But first suppose E is any subgroup of G (not necessarily elementary) such that $\zeta \notin E$. Then we claim that $\chi|_E = \chi'|_E$ and so

$\chi|_E \in X(E)$. For otherwise, there exists $x \in E$ such that $\chi(x) \neq \chi'(x)$. Thus $\zeta x \in S$ and $\chi'(\zeta x) \neq 0$ so that by (ii), $m := |\zeta x|$ is odd. But then

$$\zeta x^m = (\zeta x)^m = 1 \in E$$

so that $\zeta \in E$, a contradiction. Now an elementary subgroup of any finite group can be written in the form $A \times B$, where A is a group of odd order and B is a 2-group. Hence it suffices to show that $\chi|_E \in X(E)$ for every subgroup E of the form $E = A \times B$ with $\zeta \in E$.

Let $\chi^+ = \chi'$ and $\chi^- = \chi$. Suppose $x = ab \in E$ ($a \in A$, $b \in B$) with $\chi^\pm(x) \neq 0$. Writing $x = s$ or $x = \zeta s$ with $s \in S$, we have $\chi'(s) \neq 0$. By (ii), $|s|$ is odd, so $x = a$ (i.e., $b = 1$) or $x = a\zeta$ (i.e., $b = \zeta$). Therefore, we have

$$\chi^\pm|_E(ab) = \begin{cases} \chi^\pm|_A(a) & \text{if } b = 1, \\ \pm\chi^\pm|_A(a) & \text{if } b = \zeta, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\varphi^\pm$ be a class function on B defined by

$$\varphi^\pm(b) = \begin{cases} 1 & \text{if } b = 1, \\ \pm 1 & \text{if } b = \zeta, \\ 0 & \text{otherwise.} \end{cases}$$

so that $\chi^\pm|_E(ab) = \chi^\pm|_A(a) \cdot \varphi^\pm(b)$. Writing

$$\varphi^\pm = \sum_{[\rho] \in \mathrm{Irr}(B)} c_\rho \cdot \mathrm{tr}\,\rho \qquad (c_\rho \in \mathbb{C})$$

with $c_\rho = \langle \varphi^\pm, \mathrm{tr}\,\rho \rangle$, we find

$$\varphi^\pm = \frac{2}{\#B} \sum_{[\rho]} \dim \rho \cdot \mathrm{tr}\,\rho, \tag{$*$}$$

where the sum in $(*)$ runs over all $[\rho] \in \mathrm{Irr}(B)$ such that $\rho(\zeta) = \pm\,\mathrm{id}$. Since $\#A$ is odd, the definition of χ together with (ii) imply that $\chi|_A = \chi'|_A \in X(A)$. Thus write

$$\chi^\pm|_A = \sum_{[\pi_i] \in \mathrm{Irr}(A)} n_i \cdot \mathrm{tr}\,\pi_i \qquad (n_i \in \mathbb{Z})$$

so that

$$\chi^\pm|_E = \sum_{[\pi_i] \in \mathrm{Irr}(A)} \sum_{[\rho]} \frac{2}{\#B} \dim \rho \cdot n_i \cdot \mathrm{tr}(\pi_i \otimes \rho). \tag{$**$}$$

To show that $\chi|_E \in X(E)$, we must show that the coefficient $(2/\#B) \dim \rho \cdot n_i$ in $(**)$ is an integer for each ordered pair (i, ρ) with $\rho(\zeta) = -\,\mathrm{id}$. Since $\chi'|_E \in X(E)$, we know that $(2/\#B) \dim \rho \cdot n_i$ is an integer for every ordered pair (i, ρ) with $\rho(\zeta) = \mathrm{id}$. In particular, letting ρ be the trivial character of B, we get $\dim \rho = 1$

and so $(2/\#B)n_i$ is an integer for all i. Therefore, $(2/\#B)\dim\rho\cdot n_i$ is an integer regardless of ρ. □

3C. ***The map φ_n.*** We now describe the set $\mathfrak{T}_n$ for $n\geq 1$. Since $\mathfrak{T}_1=\{[\theta_1]\}$, we may assume that $n\geq 2$. For $n\geq 2$, let $\mathfrak{S}'_n$ be the set consisting of all $[\tau']\in\mathfrak{T}'_n$ *except* for the isomorphism classes of those representations of the form u_α and u_π^{unr}. Using Silberger's classification of irreducible representations of $\mathrm{PGL}(2,\mathcal{O})$ [Silberger 1970, pp. 98–100], we see that the cardinality of $\mathfrak{S}'_n$ is q^{n-1}. In particular, $\#\mathfrak{S}'_n=\#\mathfrak{T}_n$.

Let $\mathrm{Silb}^n\subset\mathrm{GL}(2,\mathcal{O}^n)$ be a set of conjugacy class representatives of K'_n as described by [Silberger 1970, p. 101]. We remark that there are several choices to be made here, including a nonsquare element ζ of $\mathcal{O}^\times$ and a prime element $\mathfrak{s}$ of $\mathcal{O}$. In any case, fix a choice of such a set Silb^n. Also observe that ζ, when viewed as an element of K_n, is a central involution.

Lemma 3.8. *Let $G=K_n$. There exists a set S of representatives for the distinct cosets of $\{1,\zeta\}$ in G which satisfies condition (ii) of Proposition 3.7 simultaneously for all $\chi'=\operatorname{tr}\tau'\in X(G)$ with $[\tau']\in\mathfrak{S}'_n$.*

Proof. Let $\chi'=\operatorname{tr}\tau'$ with $[\tau']\in\mathfrak{S}'_n$. An inspection of Silberger's tables shows that if $x\in\mathrm{Silb}^n$ and $\chi'(x)\neq 0$, then $|x|$ is odd. (Here, x is being viewed as an element of G.) Given $y\in G$, we can write either $y=gxg^{-1}$ or $y=\zeta gxg^{-1}$ with $x\in\mathrm{Silb}^n$ and $g\in G$, and in either case $\chi'(y)=\chi'(x)$. Hence if $\chi'(y)\neq 0$ then either $|y|$ or $|\zeta y|$ is odd. Now let S_0 be any set of representatives for the distinct cosets of $\{1,\zeta\}$ in G. After replacing each $y\in S_0$ by ζy if necessary, we obtain a set S with the required properties. □

We will now construct a bijection

$$\varphi_n:\mathfrak{S}'_n\to\mathfrak{T}_n.$$

Choose a set S as in Lemma 3.8. Given $[\tau']\in\mathfrak{S}'_n$, put $\chi'=\operatorname{tr}\tau'$. Define $\chi\in X(K_n)$ as in Proposition 3.7. Since $\chi(x)=\pm\chi'(x)$ for $x\in K_n$, we have $\langle\chi,\chi\rangle=\langle\chi',\chi'\rangle=1$. Also, $1\in S$ so that $\chi(1)=\chi'(1)=\dim\tau'>0$, and thus $\chi=\operatorname{tr}\tau$, where τ is an irreducible self-dual representation of K_n. Moreover, $\chi(\zeta)=-\chi'(1)<0$ so that $\omega_\tau\neq 1$. And by induction on $n\geq 2$, τ is primitive modulo $\mathfrak{p}^n$. Thus $[\tau]\in\mathfrak{T}_n$ and so we define $\varphi_n([\tau'])=[\tau]$. The map φ_n is injective, and since $\#\mathfrak{S}'_n=\#\mathfrak{T}_n$ we conclude that φ_n is a bijection.

We make a few observations. First, with the notations as in the previous paragraph, we have $\chi(x)=\chi'(x)$ for all $x\in\mathrm{Silb}^n$. For, suppose $x\in\mathrm{Silb}^n$ and $\chi'(x)\neq 0$ so that $|x|$ is odd. Now if $x\notin S$, then $\zeta x\in S$ and $\chi'(\zeta x)\neq 0$, and thus $|\zeta x|$ is odd by condition (ii) of Proposition 3.7. But $|x|$ and $|\zeta x|$ can not be both odd, hence $x\in S$ and so $\chi(x)=\chi'(x)$. Moreover, the map φ_n is independent of the choice of Silb^n

or S. And using Silberger's character tables for $[\tau'] \in \mathfrak{S}'_n$ in conjunction with the map φ_n, we can now write down the character tables for all $[\tau] \in \mathfrak{T}_n$. In particular, we have $\dim \tau' = q^{n-2}(q^2-1)$ for all $[\tau'] \in \mathfrak{S}'_n$ so that $\dim \tau = q^{n-2}(q^2-1)$ for $[\tau] \in \mathfrak{T}_n$ with $n \geq 2$.

Example. For $n \geq 2$, the map φ_n sends $[\sigma_n] \in \mathfrak{S}'_n$ to $[\theta_n] \in \mathfrak{T}_n$. This follows from the fact that $\operatorname{tr}\sigma_n(x) = \operatorname{tr}\theta_n(x)$ for all $x \in \mathrm{Silb}^n$. Note that we can compute $\operatorname{tr}\theta_n$ directly using the formula for the trace of an induced representation.

Remark. When $q \equiv 1 \pmod 4$, the map φ_n can be defined more directly using the following fact: Let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathcal{O})$ with $\omega_\tau \neq 1$, and H the kernel of the map $\lambda \circ \det : \mathrm{GL}(2, \mathcal{O}) \to \{\pm 1\}$. Then τ is induced from H (see [Rohrlich 2006, p. 365, Proposition 1]; the proof is valid for arbitrary $\mathcal{O}$).

4. Global multiplicities

Put $G = \mathrm{GL}(2, \mathbb{Z}_p)$ and let U be the open subgroup of $\mathbb{Z}_p^\times$ topologically generated by a fixed rational integer $m \geq 2$ such that $p \nmid m$. Let J denote the subgroup of G which consists of matrices of the form

$$b(u, z) = \begin{pmatrix} u & z \\ 0 & 1 \end{pmatrix}$$

with $u \in U$ and $z \in \mathbb{Z}_p$. Put $J'' = \{\pm I\}J$, and let η'' be the quadratic character of J'' given by $\eta''(b) = b_{22}$. Extend η'' to $J''(n)$ by setting $\eta''|K(n) = 1$.

Proposition 4.1. *Let τ be an irreducible self-dual representation of G, and choose $n \geq 1$ such that $1 + p^n \in U$ and τ factors through $G/K(n)$. If $p \equiv -1 \pmod 4$, m is a quadratic nonresidue modulo p, and $\tau \cong \theta_i$ with $i \geq 1$, then $\langle \mathrm{ind}_{J''(n)}^G \eta'', \tau \rangle$ is odd. Otherwise, $\langle \mathrm{ind}_{J''(n)}^G \eta'', \tau \rangle$ is even.*

Proof. As in the proof of [Rohrlich 2006, p. 371, Proposition 7], we have

$$\langle \mathrm{ind}_{J''(n)}^G \eta'', \tau \rangle \equiv \sum_{\mu^2=\nu^2=1} \langle \mathrm{ind}_{B(n)}^G \xi_{\mu,\nu}, \tau \rangle \pmod 2, \tag{$*$}$$

where μ and ν are characters of $\mathbb{Z}_p^\times$ that are trivial on $1 + p^n\mathbb{Z}_p$ and satisfy

$$\xi_{\mu,\nu}|J'' = \eta''. \tag{$**$}$$

Thus, we must determine which of the four pairs $(\mu, \nu) = (1, 1), (\lambda, \lambda), (1, \lambda), (\lambda, 1)$ satisfy $(**)$.

Write a typical element $b \in J''$ as $b = \epsilon b(u, z)$ with $\epsilon \in \{\pm 1\}$, $u \in U$, and $z \in \mathbb{Z}_p$. Then $\eta''(b) = \epsilon$. If $\mu = \nu = 1$, then $\xi_{\mu,\nu}(b) = 1$. So, $(1, 1)$ does not satisfy $(**)$ and hence does not occur in $(*)$. If $\mu = \nu = \lambda$, then $\xi_{\mu,\nu}(b) = \lambda(u)$. So, (λ, λ)

does not occur in $(*)$ either. We now consider the pairs $(1, \lambda)$ and $(\lambda, 1)$. Note that $\xi_{1,\lambda}(b) = \lambda(\epsilon)$ and $\xi_{\lambda,1}(b) = \lambda(\epsilon)\lambda(u)$.

Suppose $p \equiv 1 \pmod 4$ so that $\lambda(\epsilon) = 1$. In this case, $\xi_{1,\lambda}(b) = 1$ and $\xi_{\lambda,1}(b) = \lambda(u)$. So neither $(1, \lambda)$ nor $(\lambda, 1)$ occurs in $(*)$ and we get

$$\langle \mathrm{ind}_{J''(n)}^{G} \eta'', \ \tau \rangle \equiv 0 \pmod 2.$$

Suppose $p \equiv -1 \pmod 4$ so that $\lambda(\epsilon) = \epsilon$. Thus $\xi_{1,\lambda}|J'' = \eta''$. Furthermore, $\xi_{\lambda,1}|J'' = \eta''$ if and only if $\lambda(m) = 1$. If $\lambda(m) = 1$, then $\langle \mathrm{ind}_{J''(n)}^{G} \eta'', \ \tau \rangle$ is even because the representations induced by $\xi_{1,\lambda}$ and $\xi_{\lambda,1}$ are equivalent [Rohrlich 2006, p. 38, Equation 3.5]. If $\lambda(m) = -1$, then $\xi_{\lambda,1}|J'' \neq \eta''$. We thus get

$$\langle \mathrm{ind}_{J''(n)}^{G} \eta'', \ \tau \rangle \equiv \langle \mathrm{ind}_{B(n)}^{G} \xi_{1,\lambda}, \ \tau \rangle \pmod 2.$$

Since

$$\mathrm{ind}_{B(n)}^{G} \xi_{1,\lambda} = \theta_1 \oplus \theta_2 \oplus \cdots \oplus \theta_n,$$

and observing that if $\tau \cong \theta_i$, we necessarily have $1 \leq i \leq n$ because τ factors through $G/K(n)$ by assumption, the proof is complete. □

5. Local multiplicities

We first describe some local identifications and introduce notations. Given a place v of F, we let F_v denote the completion of F at v and $\bar{F}_v$ an algebraic closure of F_v that contains $\bar{F}$. Put $F_v^{\infty} = F^{\infty}F_v$, with the compositum taking place inside $\bar{F}_v$. Identify $\mathrm{Gal}(F_v^{\infty}/F_v)$ with the decomposition subgroup of $\mathrm{Gal}(F^{\infty}/F)$ that corresponds to the embedding $F^{\infty} \subset F_v^{\infty}$. Suppose τ is an irreducible self-dual representation of $\mathrm{Gal}(F^{\infty}/F)$. Then for each place v of F, we let τ_v denote the restriction of τ to $\mathrm{Gal}(F_v^{\infty}/F_v)$. Hence τ_v is still self-dual but not necessarily irreducible.

For $n \geq 1$, we let μ_n denote the group of nth roots of unity (inside an algebraically closed field) with a generator ζ_n. Furthermore, any one dimensional character $\chi : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathbb{C}^{\times}$ factors through $\mathrm{Gal}(K/F_v)$ for some finite abelian subextension K/F_v of $\bar{F}_v/F_v$, allowing us to view χ as a character of $F_v^{\times}$ via

$$\chi(x) = \chi((x^{-1}, K/F_v)) \qquad (x \in F_v^{\times}), \tag{6}$$

where $(*, K/F_v)$ is the local Artin map. Moreover, if K/F_v is any finite extension, we let ind_{K/F_v} and res_{K/F_v} denote the induction and restriction functors associated with $\mathrm{Gal}(\bar{F}_v/F_v)$ and its subgroup of finite index $\mathrm{Gal}(\bar{F}_v/K)$.

For the remainder of this section, we will assume $v \in T^{+}$ so that E/F_v is an elliptic curve having bad but potentially good reduction over F_v. For ease of notation, put $q = m_v$. Also, put $e = e_v$ as defined in (2), and assume that $e = 3$, 4, or 6 and $q \equiv -1 \pmod e$ so that $H = F_v(\zeta_e)$ is the unramified quadratic extension

of F_v. Let η denote the unramified quadratic character of $\mathrm{Gal}(\bar{F}_v/F_v)$. Define a representation $\hat{\sigma}_e$ of $\mathrm{Gal}(\bar{F}_v/F_v)$ by

$$\hat{\sigma}_e = \mathrm{ind}_{H/F_v}\,\hat{\varphi}_e = \mathrm{ind}_{H/F_v}\,\hat{\varphi}_e^{-1},$$

where $\hat{\varphi}_e$ is either of the tamely ramified characters of $H^\times$ of exact order e such that $\hat{\varphi}_e|F_v^\times = 1$. Our goal in this section is to compute the parity of the integer

$$s(e, \tau_v) := \langle 1, \tau_v\rangle + \langle \eta, \tau_v\rangle + \langle \hat{\sigma}_e, \tau_v\rangle.$$

5A. *Representations η and $\hat{\sigma}_e$.*

Lemma 5.1. *Let E/F_v be an elliptic curve and suppose E has bad but potentially good reduction at v. Assume $v \mid \ell$, where $5 \le \ell < \infty$. Let Δ denote the discriminant associated to a minimal Weierstrass equation for E over F_v. Put*

$$e = \frac{12}{\gcd(v(\Delta), 12)}\ (= 2, 3, 4, \textit{or } 6).$$

Then any finite Galois extension of F_v over which E acquires good reduction contains $F_v(\zeta_e)$.

Proof. Let K/F_v be a finite Galois extension over which E acquires good reduction. We will show that $F_v(\zeta_e) \subset K$. First, we note that $e \mid e'$, where e' is the ramification index of K/F_v. Let T/F_v and V/F_v denote the maximal unramified and the maximal tamely ramified subextensions of K/F_v, respectively. Thus, we have

$$F_v \subset T \subset V \subset K.$$

Write $e' = m\ell^a$ with $\gcd(m, \ell) = 1$ and $a \ge 0$. Note that $e \mid m$ because $\gcd(e, \ell) = 1$. The extension V/T is totally and tamely ramified of degree m. Since V/T is also Galois, we have $\mu_m \subset V$ and thus $\mu_e \subset V \subset K$ as desired. □

We apply this lemma to the situation at hand. Since $p \ge 3$ and $v \nmid p$, E has good reduction over $F_v(E[p])$ [Silverman 1994, p. 383, Proposition 10.3(b)]. Thus, we have $F_v(\zeta_e) \subset F_v(E[p])$ by Lemma 5.1. Therefore, η may be viewed as a character of $\mathrm{Gal}(F_v(E[p^n])/F_v)$ for all $n \ge 1$.

We state, without proof, a standard fact from group representation theory:

Lemma 5.2. *Let G be a profinite group and $\mathcal{H}$ a normal subgroup of finite index. Let χ be a character of $\mathcal{H}$ such that every conjugate of χ is a power of χ. Put $\rho = \mathrm{ind}_{\mathcal{H}}^{G}\,\chi$. Then $\ker\rho = \ker\chi$.*

Since $\hat{\varphi}_e|F_v^\times = 1$, we have $\hat{\varphi}_e \circ \gamma = \hat{\varphi}_e^{-1}$, where γ is the nontrivial element of $\mathrm{Gal}(H/F_v)$. Hence Lemma 5.2 implies $\ker\hat{\sigma}_e = \ker\hat{\varphi}_e$. Let M' be the fixed field of $\ker\hat{\sigma}_e$.

Next, let π be a uniformizer of F_v and put $M = F_v(\zeta_e, \pi^{1/e})$. We will show that $M' = M$, which will also imply that M is independent of the choice of the uniformizer π. We begin with the following lemma:

Lemma 5.3. *Let e be an integer with $e \geq 3$. Let G be a finite group of order $2e^2$ with subgroups I and C satisfying the following conditions*:

(i) *C is cyclic of order $2e$ whose unique subgroup J of order e is normal in G.*

(ii) *I is cyclic of order e and normal in G. Moreover, if c is a generator of C, then $cic^{-1} = i^{-1}$ for all $i \in I$.*

Suppose further that $I \cap J$ is trivial and put $K = I \times J$. Then there exists a unique cyclic subgroup N of K which is normal in G and for which G/N is dihedral of order $2e$. Furthermore $N = J$.

Proof. For existence, we take $N = J$. Note that the image of c in G/J is an involution. And since $cic^{-1} = i^{-1}$ for $i \in I$, it follows that G/J is dihedral.

For uniqueness, let N be such a subgroup of K and observe that K/N is the unique cyclic subgroup of G/N of order e. Hence any element of G/N not belonging to K/N is an involution. In particular, the image of c does not belong in K/N because $c \notin K$. So $c^2 = 1$ in G/N, that is, $c^2 \in N$. Thus $J \subset N$, and since $|J| = |N| = e$, we get $N = J$ as desired. □

To apply the lemma, we let H_e^{ab} be the maximal abelian extension of H of exponent e. Write $H_e^{\mathrm{ab}} = H_1 H_2$, where H_1 is the unramified extension of H of degree e and $H_2 = H(\pi^{1/e})$ with a uniformizer π of F_v. Using the notations of Lemma 5.3, put $G = \mathrm{Gal}(H_e^{\mathrm{ab}}/F_v)$, $I = \mathrm{Gal}(H_e^{\mathrm{ab}}/H_1)$, and $C = \mathrm{Gal}(H_e^{\mathrm{ab}}/F_v(\pi^{1/e}))$ so that $J = \mathrm{Gal}(H_e^{\mathrm{ab}}/H_2)$. To see that c acts on I by inversion, it suffices to verify that cic^{-1} and i^{-1} ($i \in I$) agree on $\pi^{1/e}$. And in fact, they both send $\pi^{1/e}$ to $\omega^{-1}\pi^{1/e}$, where ω is the e-th root of unity such that $i(\pi^{1/e}) = \omega\pi^{1/e}$. Finally, recall that M' is the fixed field of $\ker\hat{\sigma}_e = \ker\hat{\varphi}_e$ and note that M'/H is a subextension of H_e^{ab}/H. Putting $N = \mathrm{Gal}(H_e^{\mathrm{ab}}/M')$, we observe that G/N is isomorphic to the image of $\hat{\sigma}_e$, hence dihedral [Rohrlich 1996, pp. 316–317, Proposition 1(ii)]. Thus we can deduce using Lemma 5.3 that $N = J$, or equivalently, $M' = H_2 = F_v(\zeta_e, \pi^{1/e})$.

5B. ***The decomposition subgroup.*** Next, we will determine the structure of the decomposition subgroup $D = \mathrm{Gal}(F_v^\infty/F_v)$. Fixing a choice of a $\mathbb{Z}_p$-basis for $T_p(E)$, we obtain an embedding

$$\rho : D \hookrightarrow \mathrm{GL}(2, \mathbb{Z}_p)$$

via the natural action of $\mathrm{Gal}(F_v^\infty/F_v)$ on $T_p(E)$. We will also determine the conjugacy class of $\rho(g) \in \mathrm{GL}(2, \mathbb{Z}_p)$ for certain representative elements $g \in D$.

We begin by letting $V_p(E) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(E)$ and $\sigma'_{E/F_v,p}$ the contragradient of the natural action of $\mathrm{Gal}(\bar{F}_v/F_v)$ on $V_p(E)$. Hence $\sigma'_{E/F_v,p}$ is the map

$$\sigma'_{E/F_v,p} : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathrm{GL}(V_p(E)^*),$$

where $V_p(E)^*$ is the dual of $V_p(E)$. Let $\sigma_{E/F_v,p}$ be the restriction of $\sigma'_{E/F_v,p}$ to the Weil group $\mathcal{W}(\bar{F}_v/F_v)$. Fix an embedding $\iota : \mathbb{Q}_p \hookrightarrow \mathbb{C}$, and compose $\sigma_{E/F_v,p}$ with the extension-of-scalars map $\mathrm{GL}(V_p(E)^*) \hookrightarrow \mathrm{GL}(\mathbb{C} \otimes_\iota V_p(E)^*)$ to obtain a homomorphism

$$\sigma_{E/F_v,p,\iota} : \mathcal{W}(\bar{F}_v/F_v) \to \mathrm{GL}(V),$$

where, for ease of notation, we put $V = \mathbb{C} \otimes_\iota V_p(E)^*$. Since E has potential good reduction over F_v, $\sigma_{E/F_v,p,\iota}$ is continuous [Rohrlich 1994, pp. 131 and 148], and hence is a two-dimensional complex representation. Note also that $\sigma_{E/F_v,p,\iota}$ is semisimple and so its isomorphism class is independent of p and ι [Rohrlich 1994, p. 148]. Thus we will simply write σ_{E/F_v} instead of $\sigma_{E/F_v,p,\iota}$.

Let $F_v^{\mathrm{unr}} \subset \bar{F}_v$ denote the maximal unramified extension of F_v and $R \subset \bar{F}_v$ the minimal extension of F_v^{unr} over which E acquires good reduction. Then $\ker \sigma_{E/F_v} = \mathrm{Gal}(\bar{F}_v/R)$ and we may view σ_{E/F_v} as a faithful representation of

$$\mathcal{W}(R/F_v) = \mathcal{W}(\bar{F}_v/F_v)/\mathrm{Gal}(\bar{F}_v/R).$$

Letting $\Phi \in \mathrm{Gal}(\bar{F}_v/F_v)$ denote an inverse Frobenius element, we have

$$\mathcal{W}(R/F_v) = \mathrm{Gal}(R/F_v^{\mathrm{unr}}) \rtimes \langle \Phi | R \rangle. \tag{7}$$

By [Serre 1972, p. 312], we have $\mathrm{Gal}(R/F_v^{\mathrm{unr}}) \cong \mathbb{Z}/e\mathbb{Z}$. And since $e = 3$, 4, or 6, and $q \equiv -1 \pmod{e}$, $\mathcal{W}(R/F_v)$ is nonabelian [Rohrlich 1996, pp. 331–332]. Thus, letting h be a generator of $\mathrm{Gal}(R/F_v^{\mathrm{unr}})$, we have $\Phi h \Phi^{-1} = h^{-1}$.

Since $\mathcal{W}(R/F_v)$ is a dense subgroup of $\mathrm{Gal}(R/F_v)$, (7) implies

$$\mathrm{Gal}(R/F_v) = \mathrm{Gal}(R/F_v^{\mathrm{unr}}) \rtimes \overline{\langle \Phi | R \rangle} = \langle h \rangle \rtimes \overline{\langle \Phi | R \rangle},$$

where the closure is taken in $\mathrm{Gal}(R/F_v)$. Observe that $R = F_v^\infty F_v^{\mathrm{unr}}$. (In fact, since E has good reduction over $F_v(E[p])$, we have $R = F_v(E[p])F_v^{\mathrm{unr}}$.) Therefore we have

$$D = \mathrm{Gal}(F_v^\infty/F_v) = \langle h | F_v^\infty \rangle \rtimes \overline{\langle \Phi | F_v^\infty \rangle},$$

with the closure now taken in D. We still have $\langle h | F_v^\infty \rangle = \mathbb{Z}/e\mathbb{Z}$ because $R = F_v^\infty F_v^{\mathrm{unr}}$. Now our task is to determine the conjugacy classes of $\rho(\Phi)$ and $\rho(h)$ in $\mathrm{GL}(2, \mathbb{Z}_p)$.

The element $(\Phi|R)^2 \in \mathcal{W}(R/F_v)$ is central. And since σ_{E/F_v} is irreducible (because $\mathcal{W}(R/F_v)$ is nonabelian and σ_{E/F_v} is semisimple), Schur's Lemma implies that $\sigma_{E/F_v}((\Phi|R)^2)$ is multiplication by c for some $c \in \mathbb{C}^\times$. Let

$$T = \sigma_{E/F_v}(\Phi|R) \in \mathrm{GL}(V)$$

so that $T^2 = c \cdot \mathrm{id}_V$. We will show that T has distinct eigenvalues $\sqrt{c}$ and $-\sqrt{c}$. Suppose on the contrary that T has a single repeated eigenvalue $\lambda = \sqrt{c}$ or $-\sqrt{c}$. Then the Jordan canonical form of T is either $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}\lambda & 1\\ 0 & \lambda\end{smallmatrix}\right)$. The latter possibility contradicts $T^2 = c \cdot \mathrm{id}_V$, while the former implies that T is scalar and hence $\Phi|R$ acts trivially on $\mathrm{Gal}(R/F_v^{\mathrm{unr}})$. We conclude that the Jordan canonical form of T is

$$\begin{pmatrix}\sqrt{c} & 0\\ 0 & -\sqrt{c}\end{pmatrix},$$

as desired. This also means that $\det T = -c$, and since

$$\det T = \det \sigma_{E/F_v}(\Phi|R) = \omega^{-1}(\Phi|R) = q,$$

where ω denotes the p-adic cyclotomic character of $\mathcal{W}(\bar{F}_v/F_v)$ [Rohrlich 1994, p. 150], we get $c = -q$. Therefore, the characteristic polynomial of T is $x^2 + q$. Moreover, since $q \in \mathbb{Q}$ and thus is fixed by the embedding $\iota : \mathbb{Q}_p \hookrightarrow \mathbb{C}$, we conclude that the characteristic polynomial of $\sigma'_{E/F_v,p}(\Phi)$ is also $x^2 + q$.

Recall that h is a generator of $\mathrm{Gal}(R/F_v^{\mathrm{unr}}) \cong \mathbb{Z}/e\mathbb{Z}$. Then

$$\det \sigma_{E/F_v}(h) = \omega^{-1}(h) = 1$$

because ω is trivial on the inertia subgroup $I_v = \mathrm{Gal}(\bar{F}_v/F_v^{\mathrm{unr}})$. One then easily shows that the eigenvalues of $\sigma_{E/F_v}(h)$ are ζ_e and ζ_e^{-1}, so its characteristic polynomial is $x^2 - z_e x + 1$, where

$$z_e = \zeta_e + \zeta_e^{-1} = \begin{cases} -1 & \text{if } e = 3,\\ 0 & \text{if } e = 4,\\ 1 & \text{if } e = 6.\end{cases}$$

And since $z_e \in \mathbb{Q}$, the characteristic polynomial of $\sigma'_{E/F_v,p}(h)$ is also $x^2 - z_e x + 1$.

To summarize, we have the following. For a fixed choice of a $\mathbb{Z}_p$-basis for $T_p(E)$, we have a map

$$\sigma'_{E/F_v,p} : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathrm{GL}(2, \mathbb{Q}_p)$$

whose image is in $\mathrm{GL}(2, \mathbb{Z}_p)$. We have shown that

$$\sigma'_{E/F_v,p}(\Phi) \sim \begin{pmatrix}0 & -q\\ 1 & 0\end{pmatrix} \quad \text{and} \quad \sigma'_{E/F_v,p}(h) \sim \begin{pmatrix}0 & -1\\ 1 & z_e\end{pmatrix}, \tag{8}$$

where $\sim$ denotes conjugacy over $\mathbb{Q}_p$.

Lemma 5.4. *Consider $A \in \mathrm{GL}(2, \mathbb{Z}_p)$ whose reduction $\bar{A} \in \mathrm{GL}(2, \mathbb{F}_p)$ is nonscalar. Then A is conjugate in $\mathrm{GL}(2, \mathbb{Z}_p)$ to its rational canonical form.*

Proof. Since $\bar{A}$ is nonscalar, there exists

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}_p)$$

such that

$$(\bar{B})^{-1}\bar{A}\,\bar{B} = \begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix} \text{ in } \mathrm{GL}(2, \mathbb{F}_p).$$

Let v denote the column vector $v = (a, c)^{\mathrm{t}}$ so that $\bar{A}\bar{v} = (\bar{b}, \bar{d})^{\mathrm{t}}$. Thus, the matrix $U = (v, Av)$ is in $\mathrm{GL}(2, \mathbb{Z}_p)$ because $\bar{U} = \bar{B} \in \mathrm{GL}(2, \mathbb{F}_p)$. Now, $U^{-1}AU$ is the matrix of A with respect to the basis $\{v, Av\}$ so that

$$U^{-1}AU = \begin{pmatrix} 0 & -\det A \\ 1 & \operatorname{tr} A \end{pmatrix},$$

as desired. □

Applying Lemma 5.4, we see that the conjugations in (8) actually occur over $\mathbb{Z}_p$. We summarize the results of this section with the following proposition.

Proposition 5.5. *Let $D = \mathrm{Gal}(F_v^\infty/F_v)$ be the decomposition subgroup and let $\rho : D \hookrightarrow \mathrm{GL}(2, \mathbb{Z}_p)$ be an embedding induced by the natural action of $\mathrm{Gal}(F_v^\infty/F_v)$ on $T_p(E)$. Then*

$$D = \langle h | F_v^\infty \rangle \rtimes \overline{\langle \Phi | F_v^\infty \rangle}$$

with $\langle h | F_v^\infty \rangle \cong \mathbb{Z}/e\mathbb{Z}$ and $\Phi h \Phi^{-1} = h^{-1}$. Moreover,

$$\rho(\Phi) \sim \begin{pmatrix} 0 & (-q)^{-1} \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \rho(h) \sim \begin{pmatrix} z_e & -1 \\ 1 & 0 \end{pmatrix}, \tag{9}$$

where $\sim$ denotes conjugation over $\mathbb{Z}_p$.

Proof. The conjugacy classes of $\rho(\Phi)$ and $\rho(h)$ require some explanation. If we use the same $\mathbb{Z}_p$-basis for $T_p(E)$ in ρ and in $\sigma'_{E/F_v,p}$, we obtain

$$\rho(\Phi) = \sigma'_{E/F_v,p}(\Phi)^{-\mathrm{t}} \sim \begin{pmatrix} 0 & -q \\ 1 & 0 \end{pmatrix}^{-\mathrm{t}} = \begin{pmatrix} 0 & (-q)^{-1} \\ 1 & 0 \end{pmatrix},$$

where the superscript $-\mathrm{t}$ denotes the inverse transpose. Note that $\sigma'_{E/F_v,p}$ is the contragradient of the natural action, and thus we must take the inverse transpose here. The conjugacy class of $\rho(h)$ is obtained analogously. □

5C. ***Images of D.*** We will find the image of D in $K'_n = \mathrm{PGL}(2, \mathbb{Z}/p^n\mathbb{Z})$ and in $K_n = \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})/(\mathbb{Z}/p^n\mathbb{Z})^{\times 2}$. Put $F_v^{(n)} = F_v(E[p^n])$ and $D^n = \mathrm{Gal}(F_v^{(n)}/F_v)$ for $n \geq 1$. Since $\rho(\mathrm{Gal}(F_v^\infty/F_v^{(n)})) \subset K(n)$, ρ induces an embedding (which we also denote by ρ)

$$\rho : D^n \hookrightarrow \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}).$$

The group D^n is generated by the elements $h|F_v^{(n)}$ and $\Phi|F_v^{(n)}$ with relations $h^e = 1$, $\Phi h \Phi^{-1} = h^{-1}$, and possibly more. We can obtain further information about D^n by studying its embedded image in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. For example, the rational canonical form of $\rho(\Phi)$ given in (9) implies that $\Phi|F_v^{(n)}$ has order $2d_n$ in D^n, where d_n is the order of $-q$ modulo p^n.

We will also determine whether or not the unramified quadratic character η and the representation $\hat{\sigma}_e$ of $\mathrm{Gal}(\bar{F}_v/F_v)$ factor through the image of D in K_n' and in K_n. Recall from Section 5A that η factors through D^n for all $n \geq 1$ and that $\ker \hat{\sigma}_e = \mathrm{Gal}(\bar{F}_v/M)$, where $M = F_v(\zeta_e, \pi^{1/e})$ for any uniformizer π of F_v. Consequently, the image of $\hat{\sigma}_e$ is isomorphic to $\mathrm{Gal}(M/F_v) \cong \mathbb{Z}/e\mathbb{Z} \rtimes \{\pm 1\}$. Moreover, noting that Φ is an (inverse) Frobenius element of $\mathrm{Gal}(\bar{F}_v/F_v)$ and that $q \equiv -1 \pmod{e}$, we get $\Phi^2|M = \mathrm{id}_M$ so that $\Phi^2 \in \mathrm{Gal}(\bar{F}_v/M)$. We now consider the three cases, $e = 3$, 4, and 6.

Remark. In the discussions to follow, we will often commit a slight abuse of notation (for the sake of brevity) and write Φ to denote both an element of D^n and its image $\rho(\Phi)$ in $\rho(D^n)$. We will do likewise with h. Their meaning should be clear from the context in which they are used.

The case $e = 3$. Let $e = 3$ (that is, $z_e = -1$). Then D^n is a semidirect product

$$D^n = \langle h \rangle \rtimes \langle \Phi \rangle. \tag{10}$$

Let L be the fixed field of $\langle \Phi|F_v^{(1)} \rangle \subset \mathrm{Gal}(F_v^{(1)}/F_v)$ so that L/F_v is totally ramified. In fact, since $\mathrm{Gal}(F_v^{(1)}/F_v) = \mathbb{Z}/3\mathbb{Z} \rtimes \langle \Phi \rangle$ by (10), we see that L/F_v is totally and tamely ramified of degree 3. (Note: The residue characteristic of v is $\ell \geq 5$.) Thus, we may write $L = F_v(\pi^{1/3})$ for some uniformizer π of F_v so that $F_v^{(1)}$ contains $M = F_v(\zeta_3, \pi^{1/3})$. Therefore $\hat{\sigma}_3$ factors through $\mathrm{Gal}(F_v^{(1)}/F_v)$ and so $\hat{\sigma}_3$ may be viewed as a representation of $D^n = \mathrm{Gal}(F_v^{(n)}/F_v)$ for all $n \geq 1$.

Let Z denote the subgroup of all scalar matrices in $\rho(D^n)$. Then $Z = \langle \Phi^2 \rangle$ so that the image of D in K_n' is given by

$$G_3' := \frac{\rho(D^n)}{Z} = \langle h \rangle \rtimes \langle \Phi \rangle \cong \mathbb{Z}/3\mathbb{Z} \rtimes \{\pm 1\}$$

for all $n \geq 1$. Moreover, η and $\hat{\sigma}_3$ may both be viewed as representations of G_3' because they are trivial on Z. The character table of G_3' is shown in Table 1.

Let $Z^{(2)}$ be the subgroup of $\rho(D^n)$ defined as

$$Z^{(2)} = \left\{ a^2 \cdot I \in \rho(D^n) : a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\} \tag{11}$$

so that the image of D in K_n is given by $G_3 := \rho(D^n)/Z^{(2)}$. We remark that the structure of G_3 depends only on the Legendre symbol of $-q$ modulo p. In particular, it is independent of n.

	1	η	$\operatorname{tr}\hat{\sigma}_3$
$\{1\}$	1	1	2
$\{h, h^2\}$	1	1	-1
$\{\Phi, h\Phi, h^2\Phi\}$	1	-1	0

Table 1. Character table of G_3'.

(a) Suppose $\lambda(-q) = 1$. Then $Z^{(2)} = Z$ so that $G_3 = G_3'$. Hence, the character table of G_3 is given by Table 1.

(b) Suppose $\lambda(-q) = -1$. Then $Z^{(2)} = \langle\Phi^4\rangle$, so $G_3 = \langle h\rangle \rtimes \langle\Phi\rangle \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$. Table 2 shows the character table of G_3 ($\psi \cong \chi_i \otimes \hat{\sigma}_3$, where $i = 1$ or 2).

	1	η	χ_1	χ_2	$\operatorname{tr}\hat{\sigma}_3$	$\operatorname{tr}\psi$
$\{1\}$	1	1	1	1	2	2
$\{\Phi^2\}$	1	1	-1	-1	2	-2
$\{h, h^2\}$	1	1	1	1	-1	-1
$\{h\Phi^2, h^2\Phi^2\}$	1	1	-1	-1	-1	1
$\{\Phi, h\Phi, h^2\Phi\}$	1	-1	$\sqrt{-1}$	$-\sqrt{-1}$	0	0
$\{\Phi^3, h\Phi^3, h^2\Phi^3\}$	1	-1	$-\sqrt{-1}$	$\sqrt{-1}$	0	0

Table 2. Character table of G_3 when $\lambda(-q) = -1$.

The case $e = 4$. Let $e = 4$ (i.e., $z_e = 0$). Recall that d_n is the order of $-q$ modulo p^n. The structure of D^n varies according to the parity of d_n. But note that the parity of d_n is independent of n.

If d_n is odd, then D^n is a semidirect product $D^n = \langle h\rangle \rtimes \langle\Phi\rangle$. Moreover, the representation $\hat{\sigma}_4$ factors through D^n for all $n \geq 1$ when d_n is odd, since the same argument from the case $e = 3$ applies here as well.

If $d = d_n$ is even, we have $\rho(\Phi^d) = \rho(h^2) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Thus, D^n is generated by h and Φ with relations $h^4 = 1$, $\Phi^d = h^2$, and $\Phi h \Phi^{-1} = h^{-1}$.

Let Z denote the subgroup of all scalar matrices in $\rho(D^n)$. Then

$$Z = \{h^i \Phi^j : i, j \text{ are even}\}.$$

Thus, regardless of the parity of d_n, the image of D in K_n' is given by

$$G_4' := \frac{\rho(D^n)}{Z} = \langle h\rangle \times \langle\Phi\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

for all $n \geq 1$. Since η is trivial on Z, it may be viewed as a character of G_4'. Table 3 shows the character table of G_4'.

	1	η	χ_1	χ_2
1	1	1	1	1
h	1	1	−1	−1
Φ	1	−1	1	−1
$h\Phi$	1	−1	−1	1

Table 3. Character table of G_4'.

Define the subgroup $Z^{(2)}$ of $\rho(D^n)$ as in (11) so that the image of D in K_n is given by $G_4 := \rho(D^n)/Z^{(2)}$. Then the structure of the group G_4 depends only on the Legendre symbols of -1 and $-q$ modulo p.

(a) Suppose $p \equiv 1 \pmod 4$ and $\lambda(-q) = 1$. Then $Z^{(2)} = Z$, so $G_4 = G_4'$, and the character table of G_4 is given by Table 3.

(b) Suppose $p \equiv 1 \pmod 4$ and $\lambda(-q) = -1$. Then $d_n \equiv 0 \pmod 4$ and $Z^{(2)} = \{h^i\Phi^j : 2 \mid i,\ 4 \mid j\}$, so

$$G_4 = \langle h\rangle \times \langle \Phi\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

The character table of G_4 is shown in Table 4.

(c) Suppose $p \equiv -1 \pmod 4$ and $\lambda(-q) = 1$. Then d_n is odd and $Z^{(2)} = \langle \Phi^2\rangle$, so

$$G_4 = \langle h\rangle \rtimes \langle \Phi\rangle \cong \mathbb{Z}/4\mathbb{Z} \rtimes \{\pm 1\}.$$

The character table of G_4 is given by Table 5. Because d_n is odd, $\hat{\sigma}_4$ factors through D^n. And since $\hat{\sigma}_4$ is trivial on $Z^{(2)}$, it factors through G_4 as well.

	1	η	χ_1	χ_2	χ_3	χ_4	χ_5	χ_6
1	1	1	1	1	1	1	1	1
h	1	1	1	1	−1	−1	−1	−1
Φ	1	−1	i	$-i$	1	−1	i	$-i$
$h\Phi$	1	−1	i	$-i$	−1	1	$-i$	i
Φ^2	1	1	−1	−1	1	1	−1	−1
$h\Phi^2$	1	1	−1	−1	−1	−1	1	1
Φ^3	1	−1	$-i$	i	1	−1	$-i$	i
$h\Phi^3$	1	−1	$-i$	i	−1	1	i	$-i$

Table 4. Character table of G_4 when $p \equiv 1 \pmod 4$, $\lambda(-q) = -1$. Here $i = \sqrt{-1}$.

	1	η	χ_1	χ_2	$\operatorname{tr}\hat{\sigma}_4$
$\{1\}$	1	1	1	1	2
$\{h^2\}$	1	1	1	1	−2
$\{h, h^3\}$	1	1	−1	−1	0
$\{\Phi, h^2\Phi\}$	1	−1	1	−1	0
$\{h\Phi, h^3\Phi\}$	1	−1	−1	1	0

Table 5. Character table of G_4 when $p \equiv -1 \pmod 4$, $\lambda(-q) = 1$.

(d) Suppose $p \equiv -1 \pmod 4$ and $\lambda(-q) = -1$. Then $d_n \equiv 2 \pmod 4$ and $Z^{(2)} = \langle h^2\Phi^2 \rangle$ so that G_4 is generated by h and Φ with relations $h^4 = 1$, $\Phi^2 = h^2$, and $\Phi h \Phi^{-1} = h^{-1}$. In other words, G_4 is the quaternion group of order 8 and its character table is given by Table 6. Note here that $\psi \ncong \hat{\sigma}_4$, that is, the representation $\hat{\sigma}_4$ does not factor through G_4 because its image is the dihedral group of order 8 which is not a quotient of G_4.

	1	η	χ_1	χ_2	$\operatorname{tr}\psi$
$\{1\}$	1	1	1	1	2
$\{h^2\}$	1	1	1	1	−2
$\{h, h^3\}$	1	1	−1	−1	0
$\{\Phi, h^2\Phi\}$	1	−1	1	−1	0
$\{h\Phi, h^3\Phi\}$	1	−1	−1	1	0

Table 6. Character table of G_4 when $p \equiv -1 \pmod 4$, $\lambda(-q) = -1$.

The case $e = 6$. Let $e = 6$ (i.e., $z_e = 1$). The analysis is very similar to that of the case $e = 4$. Thus, we will omit details and merely present the results.

Let G_6' denote the image of D in K_n'. Then $G_6' = \langle h \rangle \rtimes \langle \Phi \rangle \cong \mathbb{Z}/3\mathbb{Z} \rtimes \{\pm 1\}$, and its character table is shown in Table 7. Note that $\psi \ncong \hat{\sigma}_6$, that is, $\hat{\sigma}_6$ does not factor through G_6' since its image has order 12 and hence is not a quotient of G_6'.

Now let G_6 be the image of D in K_n. As with the case $e = 4$, the group G_6 depends only on the Legendre symbols of -1 and $-q$ modulo p.

	1	η	$\operatorname{tr}\psi$
$\{1\}$	1	1	2
$\{h, h^2\}$	1	1	−1
$\{\Phi, h\Phi, h^2\Phi\}$	1	−1	0

Table 7. Character table of G_6'.

	1	η	χ_1	χ_2	tr ψ_1	tr ψ_2
$\{1\}$	1	1	1	1	2	2
$\{\Phi^2\}$	1	1	−1	−1	2	−2
$\{h, h^2\}$	1	1	1	1	−1	−1
$\{h\Phi^2, h^2\Phi^2\}$	1	1	−1	−1	−1	1
$\{\Phi, h\Phi, h^2\Phi\}$	1	−1	$\sqrt{-1}$	$-\sqrt{-1}$	0	0
$\{\Phi^3, h\Phi^3, h^2\Phi^3\}$	1	−1	$-\sqrt{-1}$	$\sqrt{-1}$	0	0

Table 8. Character table of G_6 when $p \equiv 1 \pmod 4$, $\lambda(-q) = -1$.

(a) Suppose $p \equiv 1 \pmod 4$ and $\lambda(-q) = 1$. Then $G_6 = G_6'$ and the character table of G_6 is given by Table 7.

(b) Suppose $p \equiv 1 \pmod 4$ and $\lambda(-q) = -1$. Then

$$G_6 = \langle h \rangle \rtimes \langle \Phi \rangle \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}.$$

The character table of G_6 is shown in Table 8. Note that $\psi_i \ncong \hat{\sigma}_6$ $(i = 1, 2)$ because the image of $\hat{\sigma}_6$ is a dihedral group of order 12 and hence is not a quotient of G_6.

(c) Suppose $p \equiv -1 \pmod 4$ and $\lambda(-q) = 1$. Then

$$G_6 = \langle h \rangle \rtimes \langle \Phi \rangle \cong \mathbb{Z}/6\mathbb{Z} \rtimes \{\pm 1\}.$$

The character table of G_6 is shown in Table 9.

(d) Suppose $p \equiv -1 \pmod 4$ and $\lambda(-q) = -1$. Then G_6 is generated by h and Φ with relations

$$h^6 = 1, \ \Phi^2 = h^3, \text{ and } \Phi h \Phi^{-1} = h^{-1}.$$

The character table of G_6 is shown in Table 10. Note that $\psi_i \ncong \hat{\sigma}_6$ $(i = 1, 2)$.

	1	η	χ_1	χ_2	tr ψ	tr $\hat{\sigma}_6$
$\{1\}$	1	1	1	1	2	2
$\{h^3\}$	1	1	−1	−1	2	−2
$\{h, h^5\}$	1	1	−1	−1	−1	1
$\{h^2, h^4\}$	1	1	1	1	−1	−1
$\{\Phi, h^2\Phi, h^4\Phi\}$	1	−1	1	−1	0	0
$\{h\Phi, h^3\Phi, h^5\Phi\}$	1	−1	−1	1	0	0

Table 9. Character table of G_6 when $p \equiv -1 \pmod 4$, $\lambda(-q) = 1$.

	1	η	χ_1	χ_2	tr ψ_1	tr ψ_2
$\{1\}$	1	1	1	1	2	2
$\{h^3\}$	1	1	−1	−1	2	−2
$\{h, h^5\}$	1	1	−1	−1	−1	1
$\{h^2, h^4\}$	1	1	1	1	−1	−1
$\{\Phi, h^2\Phi, h^4\Phi\}$	1	−1	$\sqrt{-1}$	$-\sqrt{-1}$	0	0
$\{h\Phi, h^3\Phi, h^5\Phi\}$	1	−1	$-\sqrt{-1}$	$\sqrt{-1}$	0	0

Table 10. Character table of G_6 when $p \equiv -1 \pmod 4$, $\lambda(-q) = -1$.

5D. ***Computing $s(e, \tau_v)$ when $\omega_\tau = 1$.*** We are now ready to compute the sum

$$s(e, \tau_v) = \langle 1, \tau_v\rangle + \langle \eta, \tau_v\rangle + \langle \hat{\sigma}_e, \tau_v\rangle \pmod 2$$

for representations τ of $G = \mathrm{GL}(2, \mathbb{Z}_p)$ with $\omega_\tau = 1$. Let us consider the individual cases $e = 3$, 4, and 6.

The case $e = 3$. Let $e = 3$ so that $\rho(h) \in \mathrm{GL}(2, \mathbb{Z}_p)$ is conjugate to the matrix $M_h = M_{h,3} = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Let τ be an irreducible representation of $\mathrm{PGL}(2, \mathbb{Z}_p)$ (which, we recall, is necessarily self-dual) so that τ_v may be viewed as a representation of G_3'. Using Table 1, we may write

$$\tau_v \cong 1^{\oplus m_1} \oplus \eta^{\oplus m_2} \oplus \hat{\sigma}_3^{\oplus m_3} \qquad (m_i \geq 0)$$

and obtain the equations $\dim \tau = m_1 + m_2 + 2m_3$ and $\operatorname{tr} \tau(M_h) = m_1 + m_2 - m_3$, so

$$s(3, \tau_v) = m_1 + m_2 + m_3 = \tfrac{1}{3}\big(2 \dim \tau + \operatorname{tr} \tau(M_h)\big). \tag{12}$$

Thus it suffices to compute the trace $\operatorname{tr} \tau(M_h)$, for which we will rely on Silberger's character tables [Silberger 1970, pp. 102 and 107]. Silberger [p. 101] also lists representatives for the conjugacy classes of $\mathrm{PGL}(2, \mathbb{Z}/p^i\mathbb{Z})$. And in order to use his character tables, we must first find the matrix on this list to which M_h is conjugate.

Fix a prime element $\mathfrak{s}$ of $\mathbb{Q}_p$ and a nonsquare element ζ of $\mathbb{Z}_p^\times$. We note that $\mathfrak{s}$ is the same as Silberger's τ.

Proposition 5.6. *Let $M_h = M_{h,3} = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $M_h \sim \alpha A$ in $\mathrm{GL}(2, \mathbb{Z}/p^i\mathbb{Z})$ $(i > 0)$, where $\alpha \in \mathbb{Z}_p^\times$ and $A \in \mathrm{GL}(2, \mathbb{Z}_p)$ are given as follows*:

- *If $p \equiv 1 \pmod 3$, then $\alpha = t$ and $A = \left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $t^2 + t + 1 = 0$. Moreover, $A = \beta B$, where $\beta = (1 - b)^{-1}$ and*

$$B = \begin{pmatrix} 1 + b & 0 \\ 0 & 1 - b \end{pmatrix}$$

with $b = 1 + 2t^{-2}$. In particular, $\operatorname{ord}_p(b) = 0$.

- *If* $p \equiv -1 \pmod 3$, *then* $\alpha = -\frac{1}{2}$ *and*

$$A = \begin{pmatrix} 1 & b\zeta \\ b & 1 \end{pmatrix}$$

with $b^2 = -3/\zeta$. *In particular*, $\operatorname{ord}_p(b) = 0$.

- *Suppose* $p = 3$. *Then*

$$\begin{cases} A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \text{ and } \alpha = 1 & \text{if } i = 1, \\ A = \left(\begin{smallmatrix} 1 & b\mu\mathfrak{s} \\ b & 1 \end{smallmatrix}\right) \text{ and } \alpha = -\frac{1}{2} & \text{if } i \geq 2, \end{cases}$$

where $\mu \in \{1, \zeta\}$ *and* $b^2\mu\mathfrak{s} = -3$ *so that* $\operatorname{ord}_3(b) = 0$.

In particular, the classes of M_h *and* A (*and* B *when* $p \equiv 1 \pmod 3$) *are conjugate in* $\mathrm{PGL}(2, \mathbb{Z}/p^i\mathbb{Z})$.

Proof. By Lemma 5.4, it suffices to observe that the reduction $\bar{A} \in \mathrm{GL}(2, \mathbb{F}_p)$ is nonscalar and that $\operatorname{tr}(\alpha A) = \operatorname{tr}(M_h) = -1$ and $\det(\alpha A) = \det(M_h) = 1$. In the case $p \equiv 1 \pmod 3$, direct calculation shows $A = \beta B$. □

In view of Proposition 5.6, the following can be read from Silberger's tables.

Proposition 5.7. *Suppose* $e = 3$ *and* τ *an irreducible representation of* $\mathrm{PGL}(2, \mathbb{Z}_p)$.

- *If* $\tau = 1$ *or* λ, *then* $\operatorname{tr}\tau(M_h) = 1$.
- *If* $\tau \cong \sigma$ *or* $\sigma \otimes \lambda$, *then*

$$\operatorname{tr}\tau(M_h) = \begin{cases} 1 & \text{if } p \equiv \ \ 1 \pmod 3, \\ -1 & \text{if } p \equiv -1 \pmod 3, \\ 0 & \text{if } p = \ \ 3. \end{cases}$$

- *If* $\tau \cong \sigma_n$ *with* $n \geq 2$, *then*

$$\operatorname{tr}\tau(M_h) = \begin{cases} -1 & \text{if } p = 3 \text{ and } n = 2, \\ 0 & \text{otherwise}. \end{cases}$$

- *If* $\tau \cong u_\alpha$, *where* α *is a character of* $\mathbb{Z}_p^\times$ *of conductor* p^n *and order* $|\alpha| > 2$, *then*

$$\operatorname{tr}\tau(M_h) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 3 \text{ and } 3|\alpha| \mid p^{n-1}(p-1), \\ -1 & \text{if } p \equiv 1 \pmod 3 \text{ and } 3|\alpha| \nmid p^{n-1}(p-1), \\ 0 & \text{otherwise}. \end{cases}$$

- *Let* K *be the unramified quadratic extension of* $\mathbb{Q}_p$, *and let* π *be a character of* $\mathcal{O}_K^\times$ *of order* > 2 *such that* $\pi|\mathbb{Z}_p^\times = 1$. *Furthermore, suppose* π *is primitive*

modulo $\mathfrak{p}_K^n$ $(n \geq 1)$. *If* $\tau \cong u_\pi^{\mathrm{unr}}$, *then*

$$\operatorname{tr}\tau(M_h) = \begin{cases} 2(-1)^n & \text{if } p \equiv -1 \pmod 3 \text{ and } \pi(1+\sqrt{-3}) = 1, \\ (-1)^{n+1} & \text{if } p \equiv -1 \pmod 3 \text{ and } \pi(1+\sqrt{-3}) \neq 1, \\ -1 & \text{if } p = 3 \text{ and } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

- *Let* K *be a ramified quadratic extension of* $\mathbb{Q}_p$. *Let* π *be a character of* $\mathcal{O}_K^\times$, *primitive modulo* $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, *such that* $\pi|\mathbb{Z}_p^\times = \lambda$. *Suppose* $\tau \cong u_\pi^{\mathrm{ram}}$.
  - *If* $p > 3$, *then* $\operatorname{tr}\tau(M_h) = 0$.
  - *If* $p = 3$, *then*

$$\operatorname{tr}\tau(M_h) = \begin{cases} 2 & \text{if } K = \mathbb{Q}_3(\sqrt{3}) \text{ and } n = 2, \\ 0 & \text{if } K = \mathbb{Q}_3(\sqrt{3}) \text{ and } n > 2, \\ -1 & \text{if } K = \mathbb{Q}_3(\sqrt{-3}) \text{ and } n = 2, \\ \pm 3 & \text{if } K = \mathbb{Q}_3(\sqrt{-3}) \text{ and } n > 2. \end{cases}$$

- *If* $\tau \cong u_{\alpha,m}, u_{\pi,i}^{\mathrm{unr}}$, *or* $u_{\pi,i}^{\mathrm{ram}}$, *then* $\operatorname{tr}\tau(M_h) = 0$.

Remark. The character table for the representation u_α is the second table on [Silberger 1970, p. 102]. There is an error in the second row of the table, namely $|t - t^{-1}|$ must be replaced by $|t - 1|$.

The case $e = 4$. Let $e = 4$ so that $\rho(h) \in \mathrm{GL}(2, \mathbb{Z}_p)$ is conjugate to the matrix $M_h = M_{h,4} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Let τ be an irreducible (self-dual) representation of $\mathrm{PGL}(2, \mathbb{Z}_p)$ so that τ_v may be viewed as a representation of G_4'. By Table 3, we can write

$$\tau_v \cong 1^{\oplus m_1} \oplus \eta^{\oplus m_2} \oplus \chi_1^{\oplus m_3} \oplus \chi_2^{\oplus m_4} \qquad (m_i \geq 0)$$

and obtain the equations

$$\dim\tau = m_1 + m_2 + m_3 + m_4 \quad \text{and} \quad \operatorname{tr}\tau(M_h) = m_1 + m_2 - m_3 - m_4$$

so that

$$s(4, \tau_v) = m_1 + m_2 = \tfrac{1}{2}\big(\dim\tau + \operatorname{tr}\tau(M_h)\big). \tag{13}$$

Thus, it again suffices to compute the trace $\operatorname{tr}\tau(M_h)$. As with the case $e = 3$, we will rely on Silberger's character tables so that we must first determine the conjugacy class of M_h. The proof of the following proposition is similar to that of Proposition 5.6. Recall that ζ denotes a nonsquare element of $\mathbb{Z}_p^\times$.

Proposition 5.8. *Let* $M_h = M_{h,4} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. *Then* $M_h \sim \alpha A$ *in* $\mathrm{GL}(2, \mathbb{Z}/p^i\mathbb{Z})$ $(i > 0)$, *where* $\alpha \in \mathbb{Z}_p^\times$ *and* $A \in \mathrm{GL}(2, \mathbb{Z}_p)$ *are given as follows*:

- *If* $p \equiv 1 \pmod 4$, *then* $\alpha^2 = -1$ *and* $A = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
- *If* $p \equiv -1 \pmod 4$, *then* $\alpha^2 = (-\zeta)^{-1}$ *and* $A = \left(\begin{smallmatrix} 0 & \zeta \\ 1 & 0 \end{smallmatrix}\right)$.

In particular, the classes of M_h and A are conjugate in $\mathrm{PGL}(2, \mathbb{Z}/p^i\mathbb{Z})$.

Proposition 5.9. *Suppose $e=4$ and τ an irreducible representation of* $\mathrm{PGL}(2, \mathbb{Z}_p)$.

- *If $\tau = 1$ or λ, then* $\operatorname{tr}\tau(M_h) = 1$.
- *If $\tau \cong \sigma$ or $\sigma \otimes \lambda$, then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} 1 & \text{if } p \equiv \ \ 1 \pmod 4, \\ -1 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$
- *If $\tau \cong u_\alpha$, then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} \pm 2 & \text{if } p \equiv \ \ 1 \pmod 4, \\ 0 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$
- *If $\tau \cong u_\pi^{\mathrm{unr}}$, then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} 0 & \text{if } p \equiv \ \ 1 \pmod 4, \\ \pm 2 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$
- *If $\tau \cong \sigma_n$ with $n \geq 2$, $u_{\alpha,m}$, $u_{\pi,i}^{\mathrm{unr}}$, u_π^{ram}, or $u_{\pi,i}^{\mathrm{ram}}$, then* $\operatorname{tr}\tau(M_h) = 0$.

The case $e=6$. Let $e=6$ so that $\rho(h) \in \mathrm{GL}(2, \mathbb{Z}_p)$ is conjugate to the matrix $M_h = M_{h,6} = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Let τ be an irreducible (self-dual) representation of $\mathrm{PGL}(2, \mathbb{Z}_p)$ so that τ_v may be viewed as a representation of G_6'. Thus by Table 7, we may write

$$\tau_v \cong 1^{\oplus m_1} \oplus \eta^{\oplus m_2} \oplus \psi^{\oplus m_3} \qquad (m_i \geq 0)$$

and obtain the equations $\dim\tau = m_1 + m_2 + 2m_3$ and $\operatorname{tr}\tau(M_h) = m_1 + m_2 - m_3$, so

$$s(6, \tau_v) = m_1 + m_2 = \tfrac{1}{3}\big(\dim\tau + 2\operatorname{tr}\tau(M_h)\big). \tag{14}$$

So as before, it suffices to compute the trace $\operatorname{tr}\tau(M_h)$. Moreover, with

$$M_{h,3} = \begin{pmatrix} z_3 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad M_{h,6} = \begin{pmatrix} z_6 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},$$

we have $M_{h,3} = -(M_{h,6})^{\mathrm{t}}$. And since every element of $\mathrm{GL}(2, \mathbb{Z}_p)$ is conjugate to its transpose, we conclude that $M_{h,3}$ and $M_{h,6}$ are in the same conjugacy class of $\mathrm{PGL}(2, \mathbb{Z}_p)$. Thus for a representation τ of $\mathrm{PGL}(2, \mathbb{Z}_p)$, the value of $\operatorname{tr}\tau(M_h)$ is the same for the cases $e=3$ and $e=6$.

5E. ***Computing $s(e, \tau_v)$ when $\omega_\tau \neq 1$.*** Let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$ with nontrivial central character ω_τ. We recall that $\omega_\tau = \lambda$, the Legendre symbol on $\mathbb{Z}_p^\times$. By Proposition 5.5, we have $\rho(\Phi^2) = (-q)^{-1} \cdot I$ so that

$$\operatorname{tr}\tau(x\Phi^2) = \lambda(-q)\operatorname{tr}\tau(x) \tag{15}$$

for $x \in \mathrm{GL}(2, \mathbb{Z}_p)$.

In the next three propositions, we derive formulas for $s(e, \tau_v)$ when $\omega_\tau \neq 1$ for the individual cases $e = 3$, 4, and 6.

Proposition 5.10. *Suppose $e = 3$, and let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$ with nontrivial central character.*

- *If $\lambda(-q) = 1$, then $s(3, \tau_v) = \frac{1}{3}\big(2 \dim \tau + \operatorname{tr} \tau(M_h)\big)$.*
- *If $\lambda(-q) = -1$, then $s(3, \tau_v) = 0$.*

Proof. If τ is such a representation, then τ_v may be viewed as a representation of G_3. Suppose $\lambda(-q) = 1$. Then $G_3 = G_3'$ so we may proceed as we did when deriving the formula (12) for the case $\omega_\tau = 1$.

Next suppose $\lambda(-q) = -1$. Then using Table 2, we may write

$$\tau_v \cong 1^{\oplus m_1} \oplus \eta^{\oplus m_2} \oplus \chi_1^{\oplus m_3} \oplus \chi_2^{\oplus m_4} \oplus \hat{\sigma}_3^{\oplus m_5} \oplus \psi^{\oplus m_6} \qquad (m_i \geq 0),$$

and thus we get

$$s(3, \tau_v) = m_1 + m_2 + m_5 = \tfrac{1}{6}\big(2 \dim \tau + 2 \operatorname{tr} \tau(\Phi^2) + \operatorname{tr} \tau(h) + \operatorname{tr} \tau(h\Phi^2)\big). \quad (*)$$

Also, (15) gives $\operatorname{tr} \tau(\Phi^2) = -\dim \tau$ and $\operatorname{tr} \tau(h\Phi^2) = -\operatorname{tr} \tau(h)$, since $\lambda(-q) = -1$. Thus $(*)$ becomes $s(3, \tau_v) = 0$ as desired. □

Similarly, the formulas for $s(4, \tau_v)$ and $s(6, \tau_v)$ are obtained using Tables 3–6 and Tables 7–10, respectively, in conjunction with (15).

Proposition 5.11. *Suppose $e = 4$, and let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$ with nontrivial central character.*

- *If $\lambda(-q) = 1$, then $s(4, \tau_v) = \frac{1}{2}\big(\dim \tau + \operatorname{tr} \tau(M_h)\big)$.*
- *If $\lambda(-q) = -1$, then $s(4, \tau_v) = 0$.*

Proposition 5.12. *Suppose $e = 6$, and let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$ with nontrivial central character.*

- *If $\lambda(-q) = 1$, then*

$$s(6, \tau_v) = \begin{cases} \frac{1}{3}\big(\dim \tau + 2 \operatorname{tr} \tau(M_h)\big) & \text{if } p \equiv \ \ 1 \pmod 4, \\ \frac{1}{3}\big(\dim \tau + \operatorname{tr} \tau(M_h)\big) & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

- *If $\lambda(-q) = -1$, then $s(6, \tau_v) = 0$.*

Now we compute the trace values $\operatorname{tr} \tau(M_h)$ for $[\tau] \in \mathfrak{T}_n$. First, recall that $\mathfrak{T}_1 = \{[\theta_1]\}$. And note that if $\tau \cong \theta_1$, $\operatorname{tr} \tau(M_h)$ can be computed directly using the formula for the trace of an induced representation.

Proposition 5.13. *Suppose $\tau \cong \theta_1$.*

- *If* $e = 3$, *then*

$$\operatorname{tr}\tau(M_{h,3}) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 3, \\ 0 & \text{if } p \equiv -1 \pmod 3, \\ 1 & \text{if } p = 3. \end{cases}$$

- *If* $e = 4$, *then*

$$\operatorname{tr}\tau(M_{h,4}) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod 8, \\ -2 & \text{if } p \equiv 5 \pmod 8, \\ 0 & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

- *If* $e = 6$, *then*

$$\operatorname{tr}\tau(M_{h,6}) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod{12}, \\ -2 & \text{if } p \equiv 7 \pmod{12}, \\ 0 & \text{if } p \equiv -1 \pmod 3, \\ -1 & \text{if } p = 3. \end{cases}$$

For $n \geq 2$, we use the bijection $\varphi_n : \mathfrak{S}'_n \to \mathfrak{T}_n$ from Section 3C in conjunction with the trace values $\operatorname{tr}\tau'(M_h)$ for $[\tau'] \in \mathfrak{S}'_n$, which we have already computed.

Proposition 5.14. *For* $n \geq 2$, *let* $[\tau'] \in \mathfrak{S}'_n$ *and* $[\tau] = \varphi_n([\tau']) \in \mathfrak{T}_n$. *If* $e = 4$ *or* $p > 3$, *then* $\operatorname{tr}\tau(M_{h,e}) = 0$. *If* $p = 3$, *then*

- $\operatorname{tr}\tau(M_{h,3}) = \operatorname{tr}\tau'(M_{h,3})$;
- $\operatorname{tr}\tau(M_{h,6}) = -\operatorname{tr}\tau(M_{h,3})$.

Proof. If $e = 4$ or $p > 3$, then Propositions 5.7 and 5.9 show that $\operatorname{tr}\tau'(M_{h,e}) = 0$ and hence $\operatorname{tr}\tau(M_{h,e}) = 0$, also. Now suppose $p = 3$. Then by Proposition 5.6,

$$M_{h,3} \sim \alpha A \quad \text{in } \mathrm{GL}(2, \mathbb{Z}/3^n\mathbb{Z})$$

with $\alpha = -\frac{1}{2}$ and $A \in \mathrm{Silb}^n$. And since $-\frac{1}{2}$ is a square in $(\mathbb{Z}/3^n\mathbb{Z})^\times$, we get $M_{h,3} \sim A$ in K_n and hence $\operatorname{tr}\tau(M_{h,3}) = \operatorname{tr}\tau'(M_{h,3})$. Finally, we have seen that $M_{h,6} \sim -1 \cdot M_{h,3}$, where the conjugation occurs in $\mathrm{GL}(2, \mathbb{Z}_p)$. And since -1 is a nonsquare element of $\mathbb{Z}_p^\times$ when $p = 3$, we have $\operatorname{tr}\tau(M_{h,6}) = -\operatorname{tr}\tau(M_{h,3})$ as desired. □

5F. ***Summary of results.*** In the following theorem, we combine the results of the previous sections to compute $s(e, \tau_v)$ in the cases $e = 3$, 4, and 6.

Theorem 5.15. *Let* τ *be an irreducible self-dual representation of* $\mathrm{GL}(2, \mathbb{Z}_p)$.

- *If* $\tau = 1$ *or* $\tau = \lambda$, *then* $s(e, \tau_v) = 1$.
- *If* $\tau \cong \sigma$ *or* $\tau \cong \sigma \otimes \lambda$, *then*

$$s(e, \tau_v) \equiv \begin{cases} 0 \pmod 2 & \text{if } e = 3 \text{ and } p = 3, \\ 1 \pmod 2 & \text{otherwise.} \end{cases}$$

- *If* $\tau \cong \sigma_n$ *with* $n \geq 2$, *then*

$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \text{if } e = 3,\ p = 3, \text{ and } n = 2, \\ 0 \pmod 2 & \text{otherwise.} \end{cases}$$

- *If* $\tau \cong u_\alpha$, *where* α *is primitive modulo* p^n $(n \geq 1)$, *then*

$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \text{if } e = 3,\ p \equiv 1 \pmod 3, \text{ and } 3|\alpha| \nmid p^{n-1}(p-1), \\ 0 \pmod 2 & \text{otherwise.} \end{cases}$$

- *If* $\tau \cong u_\pi^{\mathrm{unr}}$, *where* π *is primitive modulo* $\mathfrak{p}_K^n$ $(n \geq 1)$, *then*

$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \text{if } e = 3,\ p \equiv -1 \pmod 3, \text{ and } \pi(1+\sqrt{-3}) \neq 1, \\ 1 \pmod 2 & \text{if } e = 3,\ p = 3, \text{ and } n = 1, \\ 0 \pmod 2 & \text{otherwise.} \end{cases}$$

- *If* $\tau \cong u_\pi^{\mathrm{ram}}$, *where* π *is primitive modulo* $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, *then*

$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \text{if } e = 3,\ p = 3, \text{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \text{otherwise.} \end{cases}$$

- *If* $[\tau] = \varphi_n([u_\pi^{\mathrm{ram}}])$, *where* π *is primitive modulo* $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, *then*

$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \text{if } 3 \mid e,\ p = 3, \text{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \text{otherwise.} \end{cases}$$

- *If* $\tau \cong \theta_n$ *with* $n \geq 1$, *then*

$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \text{if } 3 \mid e,\ p = 3, \text{ and } 1 \leq n \leq 2, \\ 0 \pmod 2 & \text{otherwise.} \end{cases}$$

In all other cases, $s(e, \tau_v) \equiv 0 \pmod 2$.

Proof. If $[\tau] \in \mathfrak{T}'_n$, we compute $s(e, \tau_v)$ by substituting the trace $\operatorname{tr} \tau(M_h)$ from Propositions 5.7 and 5.9 and the dimension $\dim \tau$ from Silberger's tables into Equations (12)–(14). For $[\tau] \in \mathfrak{T}_n$, we substitute $\operatorname{tr} \tau(M_h)$ from Propositions 5.13 and 5.14 and $\dim \tau$ into the formulas for $s(e, \tau_v)$ given in Propositions 5.10–5.12. Note that $\dim \theta_1 = p+1$ and $\dim \tau = p^{n-2}(p^2-1)$ for all $[\tau] \in \mathfrak{T}_n$ with $n \geq 2$. □

6. Proof of the main theorem

We now return to our initial setting. Hence F is a number field and E/F is an elliptic curve semistable at primes of F above 2 and 3. If v is a finite place of F, where E has bad reduction, then $v \nmid p$. If $v(j(E)) < 0$, then $p \nmid v(j(E))$. We also assume that the natural embedding $\mathrm{Gal}(F^\infty/F) \hookrightarrow \mathrm{Aut}(T_p(E))$ is surjective, which allows us to identify $\mathrm{Gal}(F^\infty/F)$ with $\mathrm{GL}(2, \mathbb{Z}_p)$.

Given a finite place v of F such that $v(j(E)) < 0$, let $\mathcal{E}_v$ denote the Tate curve over F_v with $j(\mathcal{E}_v) = j(E)$. Then there exists a unique real-valued character

χ_v of $\mathrm{Gal}(\overline{F}_v/F_v)$ such that E is isomorphic over F_v to the twist of $\mathcal{E}_v$ by χ_v. Furthermore, $\chi_v = 1$, χ_v is the unramified quadratic character of $\mathrm{Gal}(\overline{F}_v/F_v)$, or χ_v is a ramified quadratic character of $\mathrm{Gal}(\overline{F}_v/F_v)$ according as E/F_v has split multiplicative reduction, nonsplit multiplicative reduction, or additive reduction, respectively. In all cases, χ_v factors through $\mathrm{Gal}(F_v^{\infty}/F_v)$.

Recall that τ is an irreducible self-dual representation of $\mathrm{Gal}(F^{\infty}/F)$, and for each place v of F, we let τ_v be the restriction of τ to the decomposition subgroup $\mathrm{Gal}(F_v^{\infty}/F_v)$. Given a finite place v such that $v(j(E)) \geq 0$, we define the local factor $\gamma(E/F_v, \tau_v)$ as follows. If E has good reduction at v, put $\gamma(E/F_v, \tau_v) = 1$. Otherwise, E has bad but potentially good reduction at v (i.e., $v \in T^+$), and $v \mid \ell$, where $5 \leq \ell < \infty$ and $\ell \neq p$. Let Δ_v denote the discriminant associated to a minimal Weierstrass equation for E over F_v, and as in (2) put

$$e_v = \frac{12}{\gcd(v(\Delta_v), 12)} \ (= 2, 3, 4, \text{or } 6).$$

Let

$$\epsilon_v = \begin{cases} 1 & \text{if } f(F_v/\mathbb{Q}_\ell) \text{ is even,} \\ -1/\ell & \text{if } f(F_v/\mathbb{Q}_\ell) \text{ is odd and } e_v = 2 \text{ or } 6, \\ -3/\ell & \text{if } f(F_v/\mathbb{Q}_\ell) \text{ is odd and } e_v = 3, \\ -2/\ell & \text{if } f(F_v/\mathbb{Q}_\ell) \text{ is odd and } e_v = 4. \end{cases}$$

We then define

$$\gamma(E/F_v, \tau_v) = \begin{cases} \epsilon_v^{\dim \tau} & \text{if } m_v \equiv 1 \pmod{e_v}, \\ (-\epsilon_v)^{\dim \tau}(-1)^{s(e_v, \tau_v)} & \text{if } e_v = 3, 4, \text{ or } 6 \text{ and } m_v \equiv -1 \pmod{e_v}, \end{cases} \tag{16}$$

where we recall that m_v denotes the order of the residue class field of v and that

$$s(e_v, \tau_v) = \langle 1, \tau_v \rangle + \langle \eta, \tau_v \rangle + \langle \hat{\sigma}_{e_v}, \tau_v \rangle.$$

Remark. Recall the following subsets of T^+:

$$T_2^+ = \{v \in T^+ : e_v = 2 \text{ or } 6, \text{ and } m_v \equiv -1 \pmod 4\},$$
$$T_3^+ = \{v \in T^+ : e_v = 3 \text{ and } m_v \equiv -1 \pmod 3\},$$
$$T_4^+ = \{v \in T^+ : e_v = 4, \text{ and } m_v \equiv 5 \text{ or } 7 \pmod 8\}.$$

Their union constitutes the set of elements $v \in T^+$ for which $\epsilon_v = -1$. We also recall that $t_{2,4}^+$ and t_3^+ denote the cardinalities of $T_2^+ \cup T_4^+$ and T_3^+, respectively.

Given the above notations, we define the root number $W(E, \tau)$ by

$$W(E, \tau) = \prod_v W(E/F_v, \tau_v),$$

where the local factors are given by the following [Rohrlich 1996, pp. 329–330, Theorem 2; p. 332, Proposition 8]:

- If $v \mid \infty$ (that is, if v is an infinite place), then
$$W(E/F_v, \tau_v) = (-1)^{\dim \tau}.$$
- Suppose $v \mid \ell$ with $\ell = 2$ or 3.
  (a) If $v(j(E)) \geq 0$ (good reduction), then
  $$W(E/F_v, \tau_v) = \det \tau_v(-1).$$
  Here, we view the one dimensional character $\det \tau_v$ of $\mathrm{Gal}(F_v^{\infty}/F_v)$ as a character of $F_v^{\times}$ via the Artin map (6).
  (b) If $v(j(E)) < 0$ (i.e., multiplicative reduction), then
  $$W(E/F_v, \tau_v) = \det \tau_v(-1) \cdot (-1)^{\langle \chi_v, \tau_v \rangle}.$$
- Suppose $v \mid \ell$ with $5 \leq \ell < \infty$.
  (a) If $v(j(E)) \geq 0$, then
  $$W(E/F_v, \tau_v) = \det \tau_v(-1) \cdot \gamma(E/F_v, \tau_v).$$
  Note that $\gamma(E/F_v, \tau_v) = 1$ if E has good reduction at v.
  (b) If $v(j(E)) < 0$, then
  $$W(E/F_v, \tau_v) = \det \tau_v(-1) \cdot (-1)^{\langle \chi_v, \tau_v \rangle} \cdot \chi_v(-1)^{\dim \tau}.$$
  Note that $\chi_v(-1) = 1$ if E has multiplicative reduction at v.

Therefore, we obtain

$$W(E, \tau) = (-1)^{(r_1+r_2)\dim \tau} \cdot \prod_{v \nmid \infty} \det \tau_v(-1) \cdot \prod_{\substack{v \nmid \infty \\ v(j(E))<0}} (-1)^{\langle \chi_v, \tau_v \rangle} \cdot \prod_{v \in T^+} \gamma(E/F_v, \tau_v) \cdot \prod_{v \in T^-} \chi_v(-1)^{\dim \tau}. \quad (17)$$

As in [Rohrlich 2006, pp. 372–373], we can replace the second factor by $\det \tau(c)^{r_1}$, where c is any element of $\mathrm{GL}(2, \mathbb{Z}_p)$ satisfying $c^2 = 1$ and $\det(c) = -1$. Moreover, we have

$$\prod_{\substack{v \nmid \infty \\ v(j(E))<0}} (-1)^{\langle \chi_v, \tau_v \rangle} = (-1)^{\Sigma + \Sigma' + \Sigma''} \cdot \prod_{v \in T^-} (-1)^{\langle \chi_v, \tau_v \rangle},$$

where Σ, Σ', and Σ'' are as defined in [Rohrlich 2006, p. 375]. Therefore, (17) becomes

$$W(E, \tau) = W_1(E, \tau) \cdot W_2(E, \tau), \quad (18)$$

where

$$W_1(E,\tau) = (-1)^{(r_1+r_2)\dim\tau} \cdot \det\tau(c)^{r_1} \cdot (-1)^{\Sigma+\Sigma'+\Sigma''}$$

and

$$W_2(E,\tau) = \prod_{v\in T^-} (-1)^{\langle\chi_v,\tau_v\rangle} \cdot \prod_{v\in T^-} \chi_v(-1)^{\dim\tau} \cdot \prod_{v\in T^+} \gamma\,(E/F_v,\tau_v). \tag{19}$$

The term $W_1(E,\tau)$ was computed by [Rohrlich 2006, p. 362, Theorem 1]. We recall his result in the following theorem.

Theorem 6.1 (Rohrlich). *Let τ be an irreducible self-dual representation of*

$$\mathrm{Gal}(F^\infty/F)$$

and let w_1 be the integer modulo 2 such that

$$W_1(E,\tau) = (-1)^{w_1}. \tag{20}$$

- *If $\tau = 1$, then $w_1 = r_1 + r_2 + s \pmod 2$.*
- *If $\tau = \lambda$, then $w_1 = r_1(p+1)/2 + r_2 + s_{\mathrm{qr}} + u \pmod 2$.*
- *If $\tau \cong \sigma$, then $w_1 = r_1(p+1)/2 + r_2 + s \pmod 2$.*
- *If $\tau \cong \sigma\otimes\lambda$, then $w_1 = r_1 + r_2 + s_{\mathrm{qr}} + u \pmod 2$.*
- *If $\tau \cong \sigma_n$ with $n \geq 2$ or $\tau \cong \theta_n$ with $n \geq 1$, then $w_1 = s_{\mathrm{nr}} + u \pmod 2$.*
- *If $\tau \cong u_\alpha$ or $\tau \cong u_\pi^{\mathrm{unr}}$, then $w_1 = r_1(p-1)/2 \pmod 2$.*

In all other cases, $w_1 = 0 \pmod 2$ so that $W_1(E,\tau) = 1$.

In the next two propositions, we recall that t_3^- and t_{nr}^- denote the number of places $v \in T^-$ such that $m_v \equiv 3 \pmod 4$ and m_v is a quadratic nonresidue modulo p, respectively.

Proposition 6.2. *Let τ be an irreducible self-dual representation of* $\mathrm{Gal}(F^\infty/F)$ *and let w_2 be the integer modulo 2 such that*

$$\prod_{v\in T^-} (-1)^{\langle\chi_v,\tau_v\rangle} = (-1)^{w_2}. \tag{21}$$

Then

$$w_2 = \begin{cases} t_{\mathrm{nr}}^-(p-1)/2 \pmod 2 & \text{if } \tau \cong \theta_n \text{ with } n \geq 1, \\ 0 \pmod 2 & \text{otherwise.} \end{cases}$$

Proof. We adapt the approach taken in [Rohrlich 2006, pp. 373–375] to the case $v \in T^-$. Thus let $v \in T^-$ and consider the action of $\mathrm{Gal}(\bar{F}_v/F_v)$ on $T_p(E)$ and $T_p(\mathcal{E}_v)$. We shall regard this action as given by maps

$$\alpha_v : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathrm{GL}(2,\mathbb{Z}_p) \quad \text{and} \quad \beta_v : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathrm{GL}(2,\mathbb{Z}_p),$$

respectively, where the implicit choice of bases for the two Tate modules is made as follows. For α_v, we will use the composition of the restriction $\mathrm{Gal}(\bar{F}_v/F_v) \to \mathrm{Gal}(F_v^\infty/F_v)$, the inclusion $\mathrm{Gal}(F_v^\infty/F_v) \subset \mathrm{Gal}(F^\infty/F)$, and the isomorphism $\mathrm{Gal}(F^\infty/F) \cong \mathrm{GL}(2, \mathbb{Z}_p)$. And by the theory of Tate curves, we may choose β_v to have the form

$$\beta_v(x) = \begin{pmatrix} \kappa_v(x) & z_v(x) \\ 0 & 1 \end{pmatrix} \qquad (x \in \mathrm{Gal}(\bar{F}_v/F_v)),$$

where $\kappa_v : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character.

Since $v \nmid p$, the image of κ_v is the open subgroup $U_v \subset \mathbb{Z}_p^\times$ topologically generated by m_v. Furthermore, the assumption $p \nmid v(j(E))$ implies that the image of β_v is

$$J_v = \left\{ b(u, z) = \begin{pmatrix} u & z \\ 0 & 1 \end{pmatrix} : u \in U_v, z \in \mathbb{Z}_p \right\}.$$

Observe that the fixed fields of the kernels of χ_v and κ_v are linearly disjoint over F_v, because one is totally ramified over F_v while the other is unramified. Thus the image of $\chi_v\beta_v$ is $J_v'' = \{\pm I\}J_v$. And since the maps α_v and $\chi_v\beta_v$ are conjugate, we get

$$\mathrm{Gal}(F_v^\infty/F_v) = g J_v'' g^{-1}$$

for some $g \in \mathrm{GL}(2, \mathbb{Z}_p)$.

Put $G = \mathrm{GL}(2, \mathbb{Z}_p)$ and choose $n \geq 1$ such that $1 + p^n \in U_v$ and τ factors through $G/K(n)$. Arguing as in [Rohrlich 2006, pp. 374–375], we get

$$\langle \chi_v, \tau_v \rangle = \langle \mathrm{ind}_{J_v''(n)}^G \eta_v'', \tau \rangle, \tag{$*$}$$

where η_v'' is the quadratic character of Proposition 4.1 with $m = m_v$.

Using $(*)$, Proposition 4.1, and the definition of t_{nr}^-, we obtain the desired result. □

Proposition 6.3. *Let τ be an irreducible self-dual representation of* $\mathrm{Gal}(F^\infty/F)$ *and let w_2' be the integer modulo* 2 *such that*

$$\prod_{v \in T^-} \chi_v(-1)^{\dim \tau} = (-1)^{w_2'}. \tag{22}$$

Then

$$w_2' = \begin{cases} t_3^- \pmod 2 & \text{if } \dim \tau \text{ is odd}, \\ 0 \pmod 2 & \text{if } \dim \tau \text{ is even}. \end{cases}$$

Proof. Let $v \in T^-$ so that χ_v is a ramified quadratic character of $\mathrm{Gal}(\bar{F}_v/F_v)$. We have

$$\chi_v(-1) = \begin{cases} 1 & \text{if } m_v \equiv 1 \pmod 4, \\ -1 & \text{if } m_v \equiv 3 \pmod 4, \end{cases}$$

and thus the result follows. □

Remark. Up to isomorphism, the only irreducible self-dual representations of $\mathrm{GL}(2, \mathbb{Z}_p)$ with odd dimension are 1, λ, σ, and $\sigma \otimes \lambda$ [Rohrlich 2006, p. 366, Proposition 3].

Theorem 6.4. *Let τ be an irreducible self-dual representation of $\mathrm{Gal}(F^\infty/F)$ and let w_2'' be the integer modulo 2 such that*

$$\prod_{v \in T^+} \gamma\,(E/F_v, \tau_v) = (-1)^{w_2''}. \tag{23}$$

- *If $\tau = 1$ or $\tau = \lambda$, then $w_2'' = t_{2,4}^+ + t_3^+ \pmod 2$.*
- *If $\tau \cong \sigma$ or $\tau \cong \sigma \otimes \lambda$, then*

$$w_2'' = \begin{cases} t_{2,4}^+ + t_3^+ \pmod 2 & \text{if } p > 3, \\ t_{2,4}^+ \pmod 2 & \text{if } p = 3. \end{cases}$$

- *If $\tau \cong \sigma_n$ with $n \geq 2$, then*

$$w_2'' = \begin{cases} t_3^+ \pmod 2 & \text{if } p = 3 \text{ and } n = 2, \\ 0 \pmod 2 & \text{otherwise}. \end{cases}$$

- *If $\tau \cong u_\alpha$, where α is primitive modulo p^n $(n \geq 1)$, then*

$$w_2'' = \begin{cases} t_3^+ \pmod 2 & \text{if } p \equiv 1 \pmod 3 \text{ and } 3|\alpha| \nmid p^{n-1}(p-1), \\ 0 \pmod 2 & \text{otherwise}. \end{cases}$$

- *If $\tau \cong u_\pi^{\mathrm{unr}}$, where π is primitive modulo $\mathfrak{p}_K^n$ $(n \geq 1)$, then*

$$w_2'' = \begin{cases} t_3^+ \pmod 2 & \text{if } p \equiv -1 \pmod 3 \text{ and } \pi(1+\sqrt{-3}) \neq 1, \\ t_3^+ \pmod 2 & \text{if } p = 3 \text{ and } n = 1, \\ 0 \pmod 2 & \text{otherwise}. \end{cases}$$

- *If $\tau \cong u_\pi^{\mathrm{ram}}$, where π is primitive modulo $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, then*

$$w_2'' = \begin{cases} t_3^+ \pmod 2 & \text{if } p = 3 \text{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \text{otherwise}. \end{cases}$$

- *If $[\tau] = \varphi_n([u_\pi^{\mathrm{ram}}])$, where π is primitive modulo $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, then*

$$w_2'' = \begin{cases} t_3^+ + t_6^+ \pmod 2 & \text{if } p = 3 \text{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \text{otherwise}. \end{cases}$$

- *If $\tau \cong \theta_n$ with $n \geq 1$, then*

$$w_2'' = \begin{cases} t_3^+ + t_6^+ \pmod 2 & \text{if } p = 3 \text{ and } 1 \leq n \leq 2, \\ 0 \pmod 2 & \text{otherwise}. \end{cases}$$

In all other cases, $w_2'' = 0 \pmod 2$.

Proof. Throughout the proof, we assume $v \in T^+$. And whenever $s(e_v, \tau_v)$ is mentioned, we implicitly assume that $e_v = 3$, 4, or 6 and $m_v \equiv -1 \pmod{e_v}$.

Suppose $\tau = 1$, $\tau = \lambda$, $\tau \cong \sigma$ with $p > 3$, or $\tau \cong \sigma \otimes \lambda$ with $p > 3$. Then Theorem 5.15 shows that $s(e_v, \tau_v) \equiv 1 \pmod 2$. Thus, (16) gives $\gamma(E/F_v, \tau_v) = \epsilon_v$ in both cases: (i) $m_v \equiv 1 \pmod{e_v}$ and (ii) $e_v = 3$, 4, or 6 and $m_v \equiv -1 \pmod{e_v}$. And therefore $w_2'' = t_{2,4}^+ + t_3^+ \pmod 2$.

Now suppose $\tau \cong \sigma$ or $\sigma \otimes \lambda$ with $p = 3$. Then Theorem 5.15 shows

$$s(e_v, \tau_v) \equiv \begin{cases} 0 \pmod 2 & \text{if } e_v = 3, \\ 1 \pmod 2 & \text{if } e_v = 4 \text{ or } 6. \end{cases}$$

Therefore, (16) implies

$$\gamma(E/F_v, \tau_v) = \begin{cases} -\epsilon_v & \text{if } v \in T_3^+, \\ \epsilon_v & \text{otherwise,} \end{cases}$$

and thus we get $w_2'' = t_{2,4}^+ \pmod 2$.

Before proceeding, we remark that the remaining representations all have even dimension. And for such representations, (16) simplifies to

$$\gamma(E/F_v, \tau_v) = \begin{cases} 1 & \text{if } m_v \equiv 1 \pmod{e_v}, \\ (-1)^{s(e_v, \tau_v)} & \text{if } e_v = 3, 4, \text{ or } 6 \text{ and } m_v \equiv -1 \pmod{e_v}. \end{cases} \quad (*)$$

Suppose $\tau \cong \sigma_n$ with $n \geq 2$. We have by Theorem 5.15

$$s(e_v, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \text{if } e_v = 3,\ p = 3, \text{ and } n = 2, \\ 0 \pmod 2 & \text{otherwise,} \end{cases}$$

so that $(*)$ gives the following:

- If $p = 3$ and $n = 2$, then

$$\gamma(E/F_v, \tau_v) = \begin{cases} -1 & \text{if } v \in T_3^+, \\ 1 & \text{otherwise} \end{cases}$$

  so that $w_2'' = t_3^+ \pmod 2$.
- Otherwise, $\gamma(E/F_v, \tau_v) = 1$ and so $w_2'' = 0 \pmod 2$.

The cases $\tau \cong u_\alpha$, $\tau \cong u_\pi^{\mathrm{unr}}$, $\tau \cong u_\pi^{\mathrm{ram}}$, $[\tau] = \varphi_n([u_\pi^{\mathrm{ram}}])$, and $\tau \cong \theta_n$ follow similarly. And in all other cases, Theorem 5.15 gives $s(e_v, \tau_v) \equiv 0 \pmod 2$ so that $(*)$ implies $\gamma(E/F_v, \tau_v) = 1$ and hence $w_2'' = 0 \pmod 2$. □

Substituting (21), (22), and (23) into (19) yields

$$W_2(E, \tau) = (-1)^{w_2 + w_2' + w_2''}, \quad (24)$$

and then substituting (20) and (24) into (18) gives

$$W(E, \tau) = (-1)^{w_1 + w_2 + w_2' + w_2''}.$$

Theorem 2.1 now follows from combining the values of w_1 (Theorem 6.1), w_2 (Proposition 6.2), w_2' (Proposition 6.3), and w_2'' (Theorem 6.4).

Acknowledgments

This paper is based on the author's Ph.D. thesis at Boston University. He thanks his advisor, David E. Rohrlich, for his generous mentoring, guidance, and support over the years.

References

[Lang 2002] S. Lang, *Algebra*, 3rd ed., Grad. Texts in Math. **211**, Springer, New York, 2002. MR 2003e:00003 Zbl 0984.00001

[Rohrlich 1990] D. E. Rohrlich, "The vanishing of certain Rankin–Selberg convolutions", pp. 123–133 in *Automorphic forms and analytic number theory* (Montréal, 1989), edited by M. Ram Murty, Univ. Montréal, Montreal, QC, 1990. MR 92d:11051 Zbl 0737.11014

[Rohrlich 1994] D. E. Rohrlich, "Elliptic curves and the Weil–Deligne group", pp. 125–157 in *Elliptic curves and related topics*, edited by H. Kisilevsky and M. Ram Murty, CRM Proc. Lecture Notes **4**, Amer. Math. Soc., Providence, RI, 1994. MR 95a:11054 Zbl 0852.14008

[Rohrlich 1996] D. E. Rohrlich, "Galois theory, elliptic curves, and root numbers", *Compositio Math.* **100**:3 (1996), 311–349. MR 97m:11075 Zbl 0860.11033

[Rohrlich 2006] D. E. Rohrlich, "Root numbers of semistable elliptic curves in division towers", *Math. Res. Lett.* **13**:2-3 (2006), 359–376. MR 2007c:11072 Zbl 1124.11026

[Rohrlich 2008] D. E. Rohrlich, "Scarcity and abundance of trivial zeros in division towers", *J. Algebraic Geom.* **17**:4 (2008), 643–675. MR 2009e:14039 Zbl 05352807

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[Serre 1977] J.-P. Serre, *Linear representations of finite groups*, Grad. Texts in Math. **42**, Springer, New York, 1977. MR 56 #8675 Zbl 0355.20006

[Silberger 1970] A. J. Silberger, PGL_2 *over the p-adics: its representations, spherical functions, and Fourier analysis*, Lecture Notes in Math. **166**, Springer, Berlin, 1970. MR 44 #2891 Zbl 0204.44102

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

Communicated by Karl Rubin
Received 2009-01-15 Revised 2009-11-28 Accepted 2009-11-29

matsuura@math.bu.edu *School of Education, Boston University, Two Silber Way, Boston, MA 02215, United States*

ALGEBRA AND NUMBER THEORY 4:3(2010)

Raccord sur les espaces de Berkovich

Jérôme Poineau

Nous présentons ici quelques résultats autour du problème inverse de Galois. Nous commençons par rappeler la stratégie géométrique classique permettant de démontrer que tout groupe fini est groupe de Galois sur $\mathbf{C}(T)$. Nous l'appliquons dans une autre situation afin de démontrer que, si $\mathcal{M}(B)$ désigne le corps des fonctions méromorphes sur une partie B, d'un certain type, d'un espace de Berkovich sur un corps, alors l'énoncé précédent reste valable lorsque l'on remplace $\mathbf{C}$ par $\mathcal{M}(B)$. On retrouve, en particulier, le fait que tout groupe fini est groupe de Galois sur $K(T)$, lorsque K est un corps valué complet dont la valuation n'est pas triviale.

Dans un second temps, en utilisant une méthode similaire, nous proposons une nouvelle preuve, purement géométrique, dans le langage des espaces de Berkovich sur un anneau d'entiers de corps de nombres, d'un résultat de D. Harbater assurant que tout groupe fini est groupe de Galois sur un corps de séries arithmétiques convergentes, ainsi que quelques généralisations.

Patching on Berkovich spaces. We present a few results related to the inverse Galois problem. First we recall the geometric patching strategy that is used to handle the problem in the complex case. We use it in a different situation to prove that if $\mathcal{M}(B)$ is the field of meromorphic functions over a part B, satisfying some conditions, of a Berkovich space over a valued field, then every finite group is a Galois group over $\mathcal{M}(B)(T)$. From this we derive a new proof of the fact that any finite group is a Galois group over $K(T)$, where K is a complete valued field with nontrivial valuation.

In a second part, we deal with the following theorem by D. Harbater: every finite group is a Galois group over a field of convergent arithmetic power series. We switch to Berkovich spaces over the ring of integers of a number field and use a similar strategy to give a new and purely geometric proof of this theorem, as well as some generalizations.

MSC2000: primary 12F12; secondary 14G22, 14G20, 14G25.

Mots-clefs: problème inverse de Galois, espaces de Berkovich, géométrie analytique p-adique, géométrie analytique globale, séries arithmétiques convergentes, inverse Galois problem, Berkovich spaces, p-adic analytic geometry, global analytic geometry, convergent arithmetic power series.

L'auteur est membre du projet jeunes chercheurs « Espaces de Berkovich » de l'agence nationale de la recherche.

Introduction

Le problème inverse de Galois consiste à montrer que tout groupe fini peut être réalisé comme groupe de Galois sur le corps des nombres rationnels $\mathbf{Q}$. La simplicité de l'énoncé n'augure en rien de la difficulté de la question et sa réponse nous échappe encore à ce jour.

Une stratégie due à D. Hilbert consiste à chercher à réaliser, tout d'abord, un groupe fini G donné comme groupe de Galois sur le corps $\mathbf{Q}(T)$. Ce second problème se prête à une approche géométrique. En effet, supposons que l'on sache construire un revêtement galoisien (ramifié) X de la droite projective $\mathbf{P}^1_{\mathbf{Q}}$ de groupe de Galois G. L'extension

$$\mathcal{M}(\mathbf{P}^1_{\mathbf{Q}}) = \mathbf{Q}(T) \to \mathcal{M}(X)$$

induite entre les corps de fonctions fournirait alors une solution. Le théorème d'irréductibilité de Hilbert permet ensuite de revenir au problème initial : il assure qu'il est toujours possible de spécialiser une telle extension de façon à obtenir une extension du corps $\mathbf{Q}$ dont le groupe de Galois est encore G.

Dans ce texte, nous nous intéressons à des variantes du second problème. Nous commençons par rappeler, dans la section 1, une stratégie classique pour obtenir des revêtements galoisiens : construire localement des revêtements analytiques cycliques, puis raccorder ces revêtements, et enfin montrer que le revêtement obtenu est algébrique.

Dans la deuxième section, nous nous plaçons dans le cadre des espaces analytiques au sens de Berkovich et appliquons la stratégie indiquée. Nous parvenons à démontrer que, lorsque K est un corps ultramétrique complet dont la valuation n'est pas triviale, tout groupe fini est groupe de Galois sur le corps $K(T)$. En particulier, pour tout nombre premier p, tout groupe fini est groupe de Galois sur le corps $\mathbf{Q}_p(T)$, un corps qui contient $\mathbf{Q}(T)$. La démonstration originale de ce résultat est due à D. Harbater [1987, Corollary 2.4] ; elle est écrite dans le cadre de

la géométrie formelle. Il existe également une preuve dans le cadre de la géométrie rigide, rédigée par Q. Liu [1995] en suivant une idée de J.-P. Serre. Signalons que l'absence, en général, de racines primitives de l'unité de tout ordre complique la première étape. Aussi les deux démonstrations citées font-elles appel aux constructions décrites par D. Saltman [1982]. Dans la preuve que nous proposons ici, en revanche, nous en faisons l'économie : un choix judicieux des lieux où nous construisons les revêtements cycliques nous permet d'avoir recours uniquement à des extensions de Kummer lorsque le corps K est de caractéristique nulle, ou de Kummer et d'Artin–Schreier–Witt lorsqu'il est de caractéristique strictement positive. En toute logique, la simplification de l'arithmétique du problème a un coût et nous utilisons un résultat de géométrie plus compliqué, mais fort naturel : un théorème de type GAGA relatif au-dessus d'un espace affinoïde (*cf.* annexe A).

La dernière section du texte est consacrée à la construction d'extensions galoisiennes d'un sur-corps de $\mathbf{Q}(T)$ d'un type différent : le corps des fractions de l'anneau $\mathbf{Z}_{1-}[\![T]\!]$ formé des séries en une variable à coefficients entiers qui convergent sur le disque unité ouvert complexe. Nous en déduisons une nouvelle preuve du résultat de D. Harbater [1988, Corollary 3.8] qui assure que tout groupe fini est groupe de Galois sur ce corps, et l'étendons à tout corps de nombres. La démonstration originale de ce résultat, aboutissement de la série d'articles [Harbater 1984a ; 1984b; 1984c; 1988], est ardue et technique ; elle est basée sur des manipulations algébriques des anneaux de séries du même type que $\mathbf{Z}_{1-}[\![T]\!]$. Celle que nous proposons est, en revanche, purement géométrique. La seule difficulté réside dans le fait que le cadre adapté à ce problème est celui, fort naturel mais sans doute encore un peu exotique, de la droite de Berkovich sur un anneau d'entiers de corps de nombres (la construction et les propriétés de cet espace font l'objet de l'annexe B).

Signalons, pour finir, que, contrairement à l'habitude, nous construisons un revêtement d'un ouvert d'un espace affine ; les résultats de type GAGA y tombent donc en défaut et nous utiliserons, pour pallier ce manque, le fait que l'ouvert en question soit un espace de Stein.

Notations. Nous désignerons par $\mathbf{N}$ l'ensemble des nombres entiers positifs et par $\mathbf{N}^*$ le sous-ensemble formé de ceux qui ne sont pas nuls.

1. Stratégie de raccord

Nous rappelons ici une démonstration classique du fait que tout groupe fini est groupe de Galois d'un revêtement de la variété algébrique $\mathbf{P}^1_{\mathbf{C}}$. Ce n'est qu'un prétexte pour présenter la stratégie de raccord que nous utiliserons constamment par la suite.

Considérons tout d'abord le cas des groupes cycliques. Pour disposer de plus de souplesse, nous allons commencer par construire des revêtements de la variété analytique $\mathbf{P}^1(\mathbf{C})$, et même des revêtements de petits ouverts de cette variété. Soit $m \in \mathbf{N}^*$. Choisissons un point P de $\mathbf{P}^1(\mathbf{C})$, une coordonnée locale z au voisinage de ce point, un disque ouvert D_P sur lequel elle est définie et un disque fermé E_P de rayon strictement positif contenu dans D_P. Soient a et b deux points distincts de E_P. Considérons le revêtement connexe et lisse X_P du disque D_P donné par l'équation

$$u^m = (z-a)(z-b)^{m-1}.$$

C'est un revêtement galoisien de groupe $\mathbf{Z}/m\mathbf{Z}$. En outre, il est trivial au-dessus du complémentaire du disque E_P. Remarquons que pour déterminer le groupe de Galois nous avons utilisé le fait que le corps $\mathbf{C}$ contienne une racine primitive $m^{\text{ème}}$ de l'unité.

Nous allons maintenant recoller des revêtements du type précédent afin d'en construire qui possèdent des groupes de Galois finis arbitraires. Fixons un groupe fini G. Notons n son ordre et choisissons-en des générateurs $g_1, \ldots, g_t$, avec $t \in \mathbf{N}^*$. Soit $i \in [\![1, t]\!]$. Notons n_i l'ordre de l'élément g_i dans le groupe G et posons $d_i = n/n_i$. Choisissons un point P_i de $\mathbf{P}^1(\mathbf{C})$ et construisons, par la méthode du paragraphe précédent, un $\mathbf{Z}/n_i\mathbf{Z}$-revêtement X_{P_i} au-dessus d'un disque ouvert D_{P_i} et trivial hors d'un disque fermé $E_{P_i} \subset D_{P_i}$. Indexons les feuillets de ce revêtement par les entiers compris entre 0 et $n_i - 1$ de façon compatible avec l'action du groupe $\mathbf{Z}/n_i\mathbf{Z} \simeq \langle g_i \rangle$. Considérons maintenant $\mathrm{Ind}_{\langle g_i \rangle}^G(X_{P_i})$, le G-revêtement induit par le $\langle g_i \rangle$-revêtement X_{P_i}. Rappelons qu'il est constitué topologiquement de d_i copies de X_{P_i}. Nous pouvons envoyer, de façon bijective, les feuillets de ce revêtement sur les éléments du groupe. Pour ce faire, choisissons, dans G, des représentants $a_{i,0}, \ldots, a_{i,d_i-1}$ des éléments du quotient $G/\langle g_i \rangle$. L'application qui envoie le feuillet indexé par k de la copie indexée par l de X_{P_i} sur l'élément $a_{i,l}g_i^k$ de G est bijective. Nous pouvons alors décrire l'action du groupe G sur le revêtement $\mathrm{Ind}_{\langle g_i \rangle}^G(X_{P_i})$ de la façon suivante : l'élément g de G envoie le feuillet associé à l'élément h de G sur le feuillet associé à l'élément hg.

Notons D' le complémentaire de la réunion des disques $E_{P_1}, \ldots, E_{P_t}$ dans $\mathbf{P}^1(\mathbf{C})$. Considérons le G-revêtement $\mathrm{Ind}_{\langle e \rangle}^G(D')$ induit par le revêtement trivial de D' et indexons ses feuillets par les éléments de G de façon compatible avec l'action de ce groupe.

Raccordons, maintenant, les revêtements que nous venons de construire. Nous supposerons que les disques D_{P_i}, avec $i \in [\![1, t]\!]$, sont deux à deux disjoints. Nous pouvons facilement nous ramener à ce cas en les réduisant, si besoin est. Pour tout élément i de $[\![1, t]\!]$, nous recollons alors, au-dessus de l'intersection $D_{P_i} \cap D'$, les feuillets associés aux mêmes éléments du groupe G (*cf.* figure 1). Nous obtenons

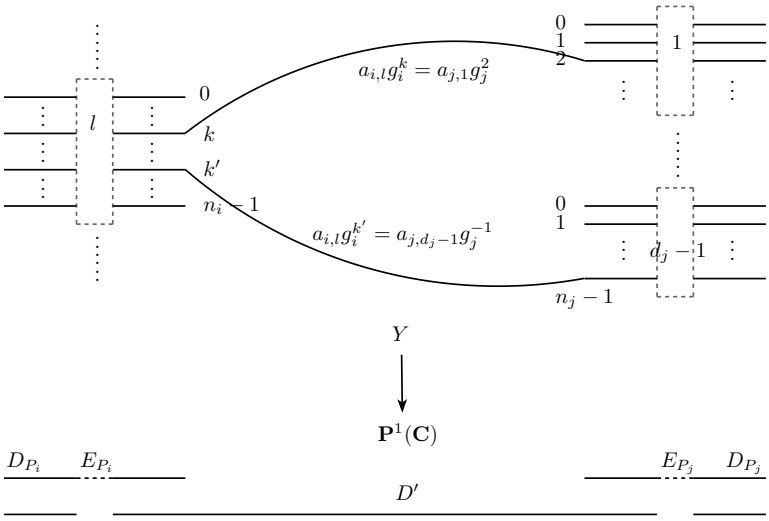


FIGURE 1. Raccord de revêtements cycliques.

ainsi un revêtement Y de $\mathbf{P}^1(\mathbf{C})$ dont on vérifie facilement qu'il est connexe, lisse et galoisien de groupe G.

Ainsi avons-nous obtenu une variété analytique complexe Y vérifiant les propriétés requises. Il nous reste à montrer que c'est, en réalité, une variété algébrique. Ce résultat découle du théorème d'existence de Riemann ou, si l'on veut, des théorèmes GAGA de Serre. Nous avons finalement obtenu le résultat suivant :

Théorème 1.1. *Tout groupe fini est groupe de Galois d'une extension du corps* $\mathbf{C}(T)$.

Pour résumer, rappelons en quelques mots la stratégie de la preuve :

(1) Construire des revêtements cycliques sur de petits ouverts, triviaux au voisinage du bord.

(2) Raccorder ces revêtements.

(3) Montrer que le revêtement obtenu est algébrique.

Harbater l'a développée dans plusieurs contextes et utilisée pour démontrer de nombreux résultats. Nous renvoyons le lecteur désireux d'en savoir plus au texte [Harbater 2003].

La simplicité de cette stratégie de raccord (« patching » chez Harbater) invite à l'appliquer dans de nombreux contextes géométriques, pour peu que l'on dispose d'une bonne notion de « petits ouverts » et de théorèmes d'algébricité. Ce n'est pas le cas de la géométrie algébrique, où deux ouverts non vides de la droite projective se coupent toujours, mais ce devrait l'être pour toute géométrie analytique. Dans

la suite de ce texte, nous illustrerons cette idée en appliquant la stratégie indiquée dans le cadre des espaces de Berkovich sur un corps ultramétrique complet, à la section 2, puis sur un anneau d'entiers de corps de nombres, à la section 3.

2. Problème inverse de Galois sur une droite relative

Soient k un corps muni d'une valeur absolue ultramétrique pour laquelle il est complet et X un espace k-analytique géométriquement irréductible. Nous noterons $\mathcal{O}$ le faisceau structural sur cet espace. Soit B une partie de l'espace X.

Notons Y le produit fibré $X \times_k \mathbf{P}_k^{1,\mathrm{an}}$, $\pi : Y \to X$ et $\lambda : Y \to \mathbf{P}_k^{1,\mathrm{an}}$ les morphismes naturels de projection. Signalons que, d'après [Ducros 2009, théorèmes 7.16 et 8.4], l'espace Y est géométriquement irréductible. Notons $Y(B)$ l'image réciproque de B par le morphisme π.

Dans les numéros 2A, 2B et 2C, nous supposerons que la partie B est compacte (pour les applications, dans la preuve des corollaires 2.13 et 2.14, elle sera même réduite à un point). Nous la munirons alors du faisceau des fonctions surconvergentes, c'est-à-dire du faisceau $j^{-1}\mathcal{O}$, où $j : B \hookrightarrow X$ désigne l'inclusion. De façon générale, nous utiliserons, sans plus le préciser, le faisceau des fonctions surconvergentes pour toute partie compacte. En particulier, l'espace localement annelé associé à l'espace $Y(B)$ que nous obtiendrons ainsi ne sera autre que le germe $(Y, \pi^{-1}(B))$ au sens de Berkovich [1993, §3.4 ; 1996, §2].

2A. ***Construction locale de revêtements cycliques.*** Dans le cas complexe, la construction locale était particulièrement simple, car nous disposions de racines primitives de l'unité de tout ordre. Lorsque nous cherchons à construire un revêtement cyclique dont l'ordre n est premier à l'exposant caractéristique du corps de base, la situation n'est guère plus compliquée, car nous disposons encore de racines primitives $n^{\text{èmes}}$ de l'unité sur certains ouverts. Nous utiliserons alors une extension de Kummer bien choisie. Dans les autres cas, nous ferons appel à la théorie d'Artin–Schreier–Witt. Nous noterons p l'exposant caractéristique du corps k.

Fixons une extension finie et séparable K de k. Soit $P \in k[T]$ le polynôme minimal unitaire d'un élément primitif de cette extension. Notons t le point de $\mathbf{P}_k^{1,\mathrm{an}}$ défini par l'annulation de ce polynôme.

2A1. *Extensions de Kummer.* Soit n un entier supérieur ou égal à 2 et premier à p. Supposons que le corps K contient une racine primitive $n^{\text{ème}}$ de l'unité.

Puisque l'anneau local au point t est hensélien, il contient une racine primitive $n^{\text{ème}}$ de l'unité, que nous noterons ζ. Cette racine est définie sur un voisinage du point t, que nous pouvons supposer de la forme

$$V_u = \left\{ y \in \mathbf{P}_k^{1,\mathrm{an}} \;\middle|\; |P(y)| \leq u \right\},$$

avec $u > 0$.

Posons $V = \lambda^{-1}(V_u)$. Nous noterons encore P et ζ les rétrotirettes des éléments P et ζ par le morphisme λ. Remarquons que l'élément ζ de $\mathbb{O}(V)$ est encore une racine primitive $n^{\text{ème}}$ de l'unité.

Soient U un voisinage de B dans X et α un élément de $\mathbb{O}(U)$ nul en tout point de B. Posons

$$Q(S) = S^n - P^n - \alpha \in \mathbb{O}(\pi^{-1}(U))[S].$$

Définissons un préfaisceau $\mathscr{F}$ sur $\pi^{-1}(U)$ en posant, pour toute partie ouverte W de $\pi^{-1}(U)$,

$$\mathscr{F}(W) = \mathbb{O}(W)[S]/(Q(S)),$$

et en utilisant les morphismes de restriction induits par ceux du faisceau $\mathbb{O}$. Le caractère unitaire du polynôme Q assure que $\mathscr{F}$ est un faisceau de $\mathbb{O}_{\pi^{-1}(U)}$-algèbres cohérent.

Remarque 2.1. Le faisceau $\mathscr{F}$ est l'image directe du faisceau structural d'une courbe analytique sur Y. Celle-ci nous est donnée comme un revêtement ramifié de degré n de $\pi^{-1}(U)$.

Soit $v \in]0, u]$. Posons

$$V(B) = \{y \in Y(B) \,\big|\, |P(y)| \leq v\} \quad \text{et} \quad V'(B) = \{y \in V(B) \mid P(y) \neq 0\}.$$

Remarquons que le complémentaire de $V'(B)$ dans $V(B)$ est fermé dans $Y(B)$.

Proposition 2.2. *Il existe un isomorphisme de $\mathbb{O}_{V'(B)}$-algèbres*

$$\varphi : \mathscr{F} \to \mathbb{O}^n$$

tel que, pour tout ouvert W de $V'(B)$ et tout élément s de $\mathscr{F}(W)$, nous ayons

$$\varphi(\zeta s) = \tau(\varphi(s)),$$

où τ désigne l'automorphisme du faisceau $\mathbb{O}^n$ qui consiste à faire agir la permutation cyclique $(1\ 2\ \ldots\ n)$ sur les coordonnées.

Démonstration. Le rayon de convergence de la série

$$(1+T)^{1/n} = \sum_{i=0}^{+\infty} C_{1/n}^i\, T^i \in k[\![T]\!]$$

est strictement positif. La série

$$P \sum_{i=0}^{+\infty} C_{1/n}^i \left(\frac{\alpha}{P^n}\right)^i$$

définit donc un élément ω de $\mathcal{O}(V'(B))$, qui est une racine du polynôme Q. Nous avons alors l'égalité

$$Q(S) = S^n - P^n - \alpha = \prod_{j=0}^{n} (S - \zeta^j \omega) \quad \text{dans } \mathcal{O}(V'(B)).$$

Par conséquent, le morphisme

$$\mathscr{F} \to \mathcal{O}^n, \quad R(S) \mapsto \big(R(\omega), R(\zeta^{-1}\omega), \dots, R(\zeta^{-(n-1)}\omega)\big)$$

est un isomorphisme. On vérifie immédiatement qu'il satisfait la condition requise. □

Remarque 2.3. La première partie du résultat signifie que le revêtement associé au faisceau $\mathscr{F}$ est trivial au-dessus de $V'(B)$. La seconde assure que le groupe $\langle \zeta \rangle \simeq \mathbf{Z}/n\mathbf{Z}$ agit sur le revêtement par une permutation cyclique des feuillets du lieu trivial.

Nous allons maintenant imposer des conditions sur les données B et α de façon que le faisceau $\mathscr{F}$ soit associé à un revêtement irréductible.

Définition 2.4. Nous dirons que la partie B de X satisfait la condition CGI si elle est compacte et possède un système fondamental de voisinages affinoïdes géométriquement intègres.

Sous les conditions de cette définition, l'anneau $\mathcal{O}(B)$ est intègre et la partie B connexe. En particulier, le principe du prolongement analytique vaut sur B et les anneaux locaux en tous les points de B sont intègres.

Lemme 2.5. *Supposons que la partie B de X satisfait la condition CGI. Alors, la partie $V(B)$ de Y possède un système fondamental de voisinages affinoïdes irréductibles.*

En particulier, pour tout point z de $V(B)$, le morphisme naturel

$$\mathcal{O}(V(B)) \to \mathcal{O}_z$$

est injectif.

Démonstration. Soient U' un voisinage affinoïde géométriquement irréductible de B dans U et v' un nombre réel strictement supérieur à v. La partie de Y définie par

$$\big\{ z \in \pi^{-1}(U') \,\big|\, |P(z)| \leq v' \big\}$$

est alors irréductible, d'après [Ducros 2009, théorème 8.4]. En effet, ce n'est autre que le produit, au-dessus de k, de l'espace géométriquement irréductible U' par l'espace

$$\big\{ x \in \mathbf{P}_k^{1,\mathrm{an}} \,\big|\, |P(x)| \leq v' \big\},$$

qui est irréductible, car le polynôme P est irréductible sur k.

La condition CGI assure que l'ensemble des parties de la forme précédente est un système fondamental de voisinages de $V(B)$ dans Y. □

Nous supposerons désormais que la partie compacte B de X satisfait la condition CGI.

Définition 2.6. Nous dirons que l'élément α de $\mathcal{O}(B)$ satisfait la condition $\mathrm{I}_{n,K}$ s'il existe un point x de B qui vérifie les deux conditions suivantes :

(i) les corps K et $\mathrm{Frac}(\mathcal{O}_x)$ sont linéairement disjoints sur k ;

(ii) le polynôme $S^n - \alpha$ est irréductible sur le corps $\mathrm{Frac}(\mathcal{O}_x) \otimes_k K$.

Lemme 2.7. *Supposons que l'élément α de $\mathcal{O}(B)$ satisfait la condition $\mathrm{I}_{n,K}$. Alors, le polynôme $Q(S) = S^n - P^n - \alpha$ est irréductible sur le corps $\mathrm{Frac}(\mathcal{O}(V(B)))$. En particulier, l'anneau $\mathcal{F}(V(B))$ est intègre.*

Démonstration. Soit x un point de B satisfaisant les propriétés énoncées dans la définition de la condition $\mathrm{I}_{n,K}$. Puisque les corps K et $\mathrm{Frac}(\mathcal{O}_x)$ sont linéairement disjoints sur k, le polynôme P est irréductible sur $\mathcal{O}_x$. Il l'est donc encore dans $\mathcal{H}(x)[T]$, puisque le corps $\kappa(x)$ et l'anneau local $\mathcal{O}_x$ sont henséliens.

Notons $Z(B)$ l'ensemble des points de $Y(B)$ en lesquels la fonction P est nulle. D'après le raisonnement précédent, la trace de la fibre $\pi^{-1}(x)$ sur Z comporte un seul point, que nous noterons z. Notons $\mathcal{O}_Z$ le faisceau structural sur Z. Nous avons alors un isomorphisme

$$\mathcal{O}_x[T]/(P(T)) \xrightarrow{\sim} \mathcal{O}_{Z,z}.$$

Le polynôme $S^n - \alpha$ est donc irréductible sur le corps $\mathrm{Frac}(\mathcal{O}_{Z,z})$, isomorphe à $\mathrm{Frac}(\mathcal{O}_x) \otimes_k K$. Par conséquent, le polynôme $Q(S)$ est irréductible sur le corps $\mathrm{Frac}(\mathcal{O}_z)$.

D'après le lemme 2.5, le morphisme naturel $\mathcal{O}(V(B)) \to \mathcal{O}_z$ est injectif. Par conséquent, le corps $\mathrm{Frac}(\mathcal{O}(V(B)))$ est un sous-corps de $\mathrm{Frac}(\mathcal{O}_z)$. On en déduit que le polynôme $Q(S)$ est irréductible sur le corps $\mathrm{Frac}(\mathcal{O}(V(B)))$.

Le polynôme $Q(S)$ étant unitaire, l'unicité de la division euclidienne assure que le morphisme

$$\mathcal{O}(V(B))[S]/(Q(S)) \to \mathrm{Frac}(\mathcal{O}(V(B)))[S]/(Q(S))$$

est injectif. Puisque l'anneau au but est intègre, celui à la source, qui n'est autre que l'anneau $\mathcal{F}(V(B))$, l'est également. □

Remarque 2.8. Ce résultat signifie que la courbe associée au faisceau $\mathcal{F}$ est intègre, c'est-à-dire réduite et irréductible.

2A2. *Extensions d'Artin–Schreier–Witt.* Il nous reste à traiter le cas des groupes cycliques dont l'ordre n'est pas premier à l'exposant caractéristique p du corps k. Nous supposons désormais que p est un nombre premier et chercherons à construire un revêtement cyclique d'ordre $n = p^r$, où r est un entier supérieur à 1. Il s'agit essentiellement de remplacer, dans le numéro précédent, la théorie de Kummer par celle d'Artin–Schreier–Witt. Nous nous contenterons d'indiquer les grandes lignes de la preuve.

Dans ce numéro, comme dans le précédent, *nous supposerons que la partie compacte B de X satisfait la condition CGI.*

Soit α un élément de $\mathscr{O}(B)$ nul en tout point de B.

Définition 2.9. Nous dirons que l'élément α de $\mathscr{O}(B)$ satisfait la condition $\mathrm{I}_{p,K}$ s'il existe un point x de B qui vérifie les deux conditions suivantes :

(i) les corps K et $\mathrm{Frac}(\mathscr{O}_x)$ sont linéairement disjoints sur k ;

(ii) le polynôme $S^p - \alpha$ est irréductible sur le corps $\mathrm{Frac}(\mathscr{O}_x) \otimes_k K$.

Soit $v > 0$. Posons

$$V(B) = \{y \in Y(B) \,\big|\, |P(y)| \leq v\} \quad \text{et} \quad V'(B) = \{y \in V(B) \mid P(y) \neq 0\}.$$

Soit W_r l'anneau des vecteurs de Witt de longueur r sur $\mathscr{O}(V(B))[S_0, \ldots, S_{r-1}]$. Posons

$$S = (S_0, \ldots, S_{r-1}) \in W_r$$

et, pour tout élément a de $\mathscr{O}(V(B))[S_0, \ldots, S_{r-1}]$,

$$\{a\} = (a, 0, \ldots, 0) \in W_r.$$

Pour tout $i \in [\![0, r-1]\!]$, définissons un polynôme $Q_i(S_0, \ldots, S_{r-1})$ à coefficients dans $\mathscr{O}(V(B))$ par la formule

$$(Q_0, \ldots, Q_{r-1}) = F(S) - \{P\}^{p-1} S - \{\alpha\} \text{ dans } W_r.$$

Le groupe $\mathbf{Z}/p^r\mathbf{Z}$ agit sur l'anneau $\mathscr{O}(V(B))[S_0, \ldots, S_{r-1}]/(Q_0, \ldots, Q_{r-1})$ en laissant stable $\mathscr{O}(V(B))$ et en envoyant S_i, pour $i \in [\![0, r-1]\!]$, sur la $(i+1)^{\text{ème}}$ coordonnée du vecteur $S + \{P\}$ dans W_r. Par analogie avec la construction précédente, nous définissons un faisceau sur $V(B)$ par

$$\mathscr{F} = \mathscr{O}[S_0, \ldots, S_{r-1}]/(Q_0, \ldots, Q_{r-1}).$$

Les propriétés des vecteurs de Witt montrent que, pour tout $i \in [\![0, r-1]\!]$, nous avons

$$Q_i = S_i^p - P^{(p-1)p^i} S_i \mod (\alpha, Q_0, \ldots, Q_{i-1}).$$

Soit $y \in V'(B)$. L'image $S_0^p - P^{p-1} S_0$ du polynôme $Q_0(S_0)$ dans le corps résiduel $\kappa(y)$ de l'anneau local $\mathscr{O}_y$ est scindé à racines simples. Puisque cet anneau

local est hensélien, le polynôme $P_0(S_0)$ possède p racines simples dans $\mathbb{O}_y$. En raisonnant par récurrence sur le nombre de variables, on montre ainsi que le système d'équations polynomiales donné par $Q_0, \ldots, Q_{r-1}$ possède exactement p^r racines $\omega_1, \ldots, \omega_{p^r}$ dans $\mathbb{O}_y^r$ et que le morphisme

$$\psi : \mathbb{O}_y[S_0, \ldots, S_{r-1}]/(Q_0, \ldots, Q_{r-1}) \to \mathbb{O}_y^{p^r}, \quad R(S_0, \ldots, S_{r-1}) \mapsto (R(\omega_i))_{1 \leq i \leq p^r}$$

est un isomorphisme. On en déduit que le revêtement est trivial sur $V'(B)$, comme à la proposition 2.2.

Supposons que l'élément α de $\mathbb{O}(B)$ satisfait la condition $\mathrm{I}_{p,K}$. L'énoncé du lemme 2.7 vaut alors encore. Pour le démontrer, l'on remplace simplement les arguments de la théorie de Kummer par ceux de la théorie d'Artin–Schreier–Witt. L'argument-clé consiste à utiliser le fait que le polynôme $S^p - \alpha$ est irréductible sur $\mathbb{O}_x$, où x est un point de B satisfaisant les propriétés énoncées dans la définition de la condition $\mathrm{I}_{p,K}$, et à en déduire que le polynôme $S^p - P^{p-1}S - \alpha$ est irréductible sur $\mathbb{O}_z$, où z désigne l'unique point de la fibre $\pi^{-1}(x)$ en lequel P s'annule.

2B. ***Raccord et retour à l'algèbre.*** Soit G un groupe fini. Soient $g_1, \ldots, g_t$, avec $t \in \mathbf{N}^*$, des générateurs du groupe G. Nous pouvons les choisir de façon que, pour tout élément i de $[\![1, t]\!]$, il existe un nombre premier p_i et un entier $r_i \geq 1$ tels que le sous-groupe de G engendré par g_i soit cyclique d'ordre $p_i^{r_i}$. Nous supposerons qu'il existe $s \in [\![1, t]\!]$ tel que $p_i \neq p$ pour tout $i \leq s$ et $p_i = p$ pour tout $i \geq s+1$.

Nous nous plaçons sous les hypothèses suivantes :

- la partie B de X satisfait la condition CGI ;
- pour tout élément i de $[\![1, s]\!]$, il existe une extension séparable K_i de k contenant une racine primitive $(p_i^{r_i})^{\text{ème}}$ de l'unité et un élément α_i de $\mathbb{O}(B)$ qui satisfait la condition $\mathrm{I}_{p_i^{r_i}, K_i}$;
- pour tout élément i de $[\![s+1, t]\!]$, il existe une extension séparable K_i de k et un élément α_i de $\mathbb{O}(B)$ qui satisfait la condition I_{p,K_i} ;
- les corps $K_1, \ldots, K_t$ sont deux à deux non isomorphes.

Supposons que les éléments $\alpha_1, \ldots, \alpha_t$ sont nuls en tout point de B. Soit i un élément de $[\![1, t]\!]$. Construisons par la méthode du numéro 2A1 ou 2A2 un revêtement galoisien de groupe $\mathbf{Z}/p_i^{r_i}\mathbf{Z}$. Il est défini au-dessus d'une partie V_i et trivial au-dessus d'une partie V_i'. Notons $\mathrm{Ind}_{\langle g_i \rangle}^G(V_i)$ le G-revêtement induit.

Puisque les corps $K_1, \ldots, K_t$ sont deux à deux non isomorphes, nous pouvons choisir les parties $V_1, \ldots, V_t$ de façon qu'elles soient deux à deux disjointes (il suffit de choisir des éléments v assez petits). Pour $i \in [\![1, t]\!]$, posons $V_i'' = V_i \setminus V_i'$. C'est une partie fermée de $Y(B)$. Posons

$$Y'(B) = Y(B) \setminus \bigcup_{1 \leq i \leq t} V_i''$$

et considérons le G-revêtement $\mathrm{Ind}_{\langle e\rangle}^{G}(Y'(B))$ induit par le revêtement trivial au-dessus de $Y'(B)$.

Raccordons, à présent, les différents revêtements selon les relations entre les éléments du groupe G, par la méthode décrite à la section 1. Nous obtenons un revêtement de $Y(B)$, galoisien de groupe G. On montre à l'aide du lemme 2.7 et de son analogue dans le cas des revêtements d'Artin–Schreier–Witt, qu'il est intègre. Un théorème du type GAGA (corollaire A.6) assure qu'il est algébrique. En passant aux corps de fonctions, nous obtenons donc finalement une extension finie et galoisienne de groupe G

$$\mathscr{M}(Y(B)) = \mathrm{Frac}(\mathscr{O}(B))(T) \to L,$$

où $\mathscr{M}$ désigne le faisceau des fonctions méromorphes. La construction que nous avons menée étant purement géométrique, on se convainc aisément que cette extension est régulière, c'est-à-dire que le corps $\mathrm{Frac}(\mathscr{O}(B))$ est algébriquement fermé dans le corps L.

Théorème 2.10. *Il existe une extension finie du corps* $\mathrm{Frac}(\mathscr{O}(B))(T)$ *qui est régulière et galoisienne de groupe de Galois* G.

2C. ***Conclusion.*** Regroupons les résultats que nous avons obtenus jusqu'ici.

Théorème 2.11. *Soient k un corps muni d'une valeur absolue ultramétrique pour laquelle il est complet. Soient X un espace k-analytique et B une partie compacte de X qui possède un système fondamental de voisinages affinoïdes géométriquement intègres. Supposons que pour tout nombre premier q différent de la caractéristique du corps k et tout entier $r \in \mathbf{N}^*$, il existe une famille infinie $\mathscr{H}_{q^r}$ de corps deux à deux non isomorphes satisfaisant les propriétés suivantes* :

(i) *tout élément de $\mathscr{H}_{q^r}$ est une extension finie et séparable de k contenant une racine primitive $(q^r)^{\text{ème}}$ de l'unité* ;

(ii) *pour tout élément K de $\mathscr{H}_{q^r}$, il existe un élément x de B et un élément α de $\mathscr{O}(B)$ nul en tout point de B tels que les corps K et $\mathrm{Frac}(\mathscr{O}_x)$ soient linéairement disjoints et le polynôme $S^{q^r} - \alpha$ soit irréductible sur leur compositum.*

Si la caractéristique du corps k est un nombre premier p, supposons en outre qu'il existe une famille infinie $\mathscr{H}_p$ de corps deux à deux non isomorphes satisfaisant les propriétés suivantes :

(i) *tout élément de $\mathscr{H}_p$ est une extension finie et séparable de k* ;

(ii) *pour tout élément K de $\mathscr{H}_p$, il existe un élément x de B et un élément α de $\mathscr{O}(B)$ nul en tout point de B tels que les corps K et $\mathrm{Frac}(\mathscr{O}_x)$ soient linéairement disjoints et le polynôme $S^p - \alpha$ soit irréductible sur leur compositum.*

Alors, tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $\mathrm{Frac}(\mathscr{O}(B))(T)$.

Remarque 2.12. Ce théorème ne contient malheureusement aucun résultat qui ne soit déjà connu. En effet, le corps $\mathrm{Frac}(\mathcal{O}(B))$ contient toujours un corps complet pour une valeur absolue non triviale (un corps de séries de Laurent engendré par l'un des éléments α lorsque k est trivialement valué) et, sur un tel corps, le résultat est dû à Harbater [1987, Corollary 2.4].

Nous allons, à présent, appliquer ce résultat général dans des cas particuliers.

Corollaire 2.13. *Soit k un corps muni d'une valeur absolue ultramétrique non triviale pour laquelle il est complet. Alors, tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $k(T)$.*

Démonstration. Appliquons le théorème 2.11 en choisissant pour espace X la droite analytique $\mathbf{A}_k^{1,\mathrm{an}}$, dont nous noterons U la variable, et pour partie B le point 0. Soit K une extension finie du corps k. Choisissons pour point x le point 0 : l'anneau local $\mathcal{O}_0$ est l'anneau des séries en une variable à coefficients dans k de rayon de convergence strictement positif. Par conséquent, les corps K et $\mathrm{Frac}(\mathcal{O}_0)$ sont linéairement disjoints sur k. Choisissons pour fonction α la fonction U : pour tout entier $n \geq 1$, le polynôme $S^n - U$ est irréductible sur le corps $\mathrm{Frac}(\mathcal{O}_0) \otimes_k K$, qui est un sous-corps de $K((U))$, par le théorème d'Eisenstein. Les hypothèses du théorème 2.11 sont donc satisfaites.

Soit G un groupe fini. Il existe une extension finie et régulière du corps

$$\mathrm{Frac}(\mathcal{O}(B))(T) = \mathrm{Frac}(\mathcal{O}_0)(T),$$

qui est galoisienne de groupe G. Puisque l'anneau local $\mathcal{O}_0$ est composé de séries convergentes et que le corps k n'est pas trivialement valué, toute variété qui possède un point sur $\mathrm{Frac}(\mathcal{O}_0)$ en possède un sur k. En utilisant le théorème de Bertini–Noether [Fried et Jarden 2008, Proposition 10.4.2], on montre alors que l'on peut spécialiser l'extension précédente en une extension finie et régulière du corps $k(T)$ qui est galoisienne de groupe G. □

Rappelons qu'un corps k est dit fertile [1] si tout k-schéma de type fini qui possède un point sur $k((U))$ en possède un sur k (l'on peut démontrer que cela équivaut à demander que toute k-courbe lisse qui possède un point sur k en possède une infinité). F. Pop a démontré que, si k est un corps fertile, tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $k(T)$ [Pop 1996, Main Theorem A].

Corollaire 2.14. *Soit k un corps. Alors, tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $k((U))(T)$. En particulier, si le corps k est fertile ou contient un corps fertile, tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $k(T)$.*

1. Nous empruntons ce terme à L. Moret-Bailly [2001]. Les corps fertiles sont connus sous beaucoup d'autres noms. Ils ont été introduits par F. Pop [1996] sous l'appellation de « large fields ».

Démonstration. Munissons le corps k de la valuation triviale et considérons la même situation que dans la preuve précédente. Nous avons alors $\mathcal{O}(B) = \mathcal{O}_0 = k[\![U]\!]$ et le théorème 2.11 fournit le résultat annoncé.

Lorsque le corps k est fertile, le théorème de Bertini–Noether permet de spécialiser l'extension précédente en une extension de $k(T)$ possédant les mêmes propriétés. La régularité de l'extension de $k(T)$ permet d'obtenir, par produit tensoriel, pour tout corps L contenant k, une extension de $L(T)$ possédant encore les propriétés requises. □

Remarque 2.15. Le résultat du second corollaire contient le résultat du premier, puisque tout corps complet pour une valeur absolue ultramétrique non triviale est fertile. Cependant, la preuve de ce dernier énoncé étant assez difficile (on peut, par exemple, le démontrer en utilisant l'approximation d'Artin), nous avons choisi de proposer une preuve directe du corollaire 2.13.

2D. ***Cas de la valuation triviale.*** Lorsque le corps k est trivialement valué, nous pouvons obtenir des résultats plus généraux. Nous indiquons simplement ici les modifications à apporter au raisonnement qui précède.

Supposons que le corps k est muni de la valeur absolue triviale. Pour tout $n \in \mathbf{N}$, nous pouvons alors définir une application, appelée flot [Poineau 2008, 1.3], de $\mathbf{A}_k^{n,\mathrm{an}} \times \mathbf{R}_+^*$ dans $\mathbf{A}_k^{n,\mathrm{an}}$ de la façon suivante. Soient x un point de $\mathbf{A}_k^{n,\mathrm{an}}$ — il est associé à une semi-norme multiplicative $|.|_x$ sur $k[T_1, \ldots, T_n]$ qui induit la valeur absolue triviale sur k — et ε un nombre réel strictement positif. L'image du couple (x, ε) est le point de $\mathbf{A}_k^{n,\mathrm{an}}$ associée à la semi-norme multiplicative $|.|_x^\varepsilon$. Par restriction à la source et au but, nous pouvons encore définir le flot sur tout fermé de Zariski d'un espace affine analytique. Signalons qu'une fonction définie au voisinage d'un point se prolonge, et ce de façon unique, à un voisinage de sa trajectoire sous le flot (*ibid.*, proposition 1.3.10).

Nous considérerons désormais un espace analytique X qui est un fermé de Zariski d'un espace affine analytique et une partie ouverte B de X. Nous définissons comme précédemment Y, π et λ.

Expliquons comment adapter les constructions locales du numéro 2A. Comme alors, choisissons une extension finie et séparable K de k. Soit $P \in k[T]$ le polynôme minimal unitaire d'un élément primitif de cette extension et notons t le point de $\mathbf{P}_k^{1,\mathrm{an}}$ défini par l'annulation de ce polynôme.

Reprenons, à présent, le raisonnement du numéro 2A1. À cet effet, choisissons un entier n supérieur ou égal à 2 et premier à p et supposons que le corps K contient une racine primitive $n^{\text{ème}}$ de l'unité. Par hensélianité, elle se relève, dans l'anneau local au point t, en une racine primitive $n^{\text{ème}}$ de l'unité, que nous noterons ζ. Les propriétés du flot assurent qu'elle est définie sur l'ouvert

$$\left\{ y \in \mathbf{P}_k^{1,\mathrm{an}} \;\middle|\; |P(y)| < 1 \right\}.$$

Soit α un élément de $\mathcal{O}(B)$. Insistons sur le fait que nous ne supposons plus qu'il soit nul en tout point de B. Nous définissons alors un faisceau $\mathcal{F}$, comme précédemment, au-dessus de l'ouvert

$$V_t(B) = \left\{ y \in Y(B) \,\middle|\, |P(y)| < 1 \right\}.$$

Puisque le corps k est trivialement valué, le rayon de convergence de la série $(1+T)^{1/n}$ est égal à 1 et le revêtement associé à $\mathcal{F}$ est trivial au-dessus de l'ouvert

$$V_t'(B) = \left\{ y \in V(B) \,\middle|\, |\alpha(y)| < |P(y)|^n \right\}.$$

Supposons, en outre, que l'élément α est de valeur absolue strictement inférieure à 1 en tout point de B. Alors, le complémentaire de la partie $V_t'(B)$ dans $V_t(B)$ est fermé dans $Y(B)$.

Pour assurer l'irréductibilité du revêtement associé au faisceau $\mathcal{F}$, nous remplaçons la condition CGI par la condition suivante : l'ouvert B est limite inductive d'espaces affinoïdes géométriquement intègres. Le résultat du lemme 2.7 vaut alors encore.

Passons aux résultats du numéro 2A2. Supposons donc que p est un nombre premier et considérons un entier n de la forme p^r, avec $r \in \mathbf{N}^*$. Soit α un élément de $\mathcal{O}(B)$ et posons, de nouveau,

$$V_t(B) = \left\{ y \in Y(B) \,\middle|\, |P(y)| < 1 \right\}.$$

Les propriétés du flot permettent de préciser le domaine de définition des racines du polynôme $P_0(S_0)$. Notons B_0 le lieu d'annulation de α dans B. Supposons qu'il ne soit pas vide et que pour tout point b de B vérifiant $|\alpha(b)| < 1$ et tout voisinage B_+ de B_0, le flot joigne le point b à un point de B_+ (c'est en particulier le cas dès que la partie B est stable par le flot, que l'élément α est de valeur absolue strictement inférieure à 1 en tout point de B et s'annule sur B). Posons

$$V_t'(B) = \left\{ y \in V(B) \,\middle|\, |\alpha(y)| < 1 \text{ et } |P(y)| < 1 \right\}.$$

Les propriétés du flot assurent que le revêtement associé à $\mathcal{F}$ est encore trivial sur une partie $V_t'(B)$ de $V_t(B)$ dont le complémentaire dans $V_t(B)$ est fermé. Si l'élément α est de valeur absolue strictement inférieure à 1 en tout point de B, nous pouvons même choisir la partie $V_t'(B)$ de façon que son complémentaire dans $V_t(B)$ soit fermé dans $Y(B)$.

Dans la preuve du théorème 2.10, il faut finalement remplacer le résultat de type GAGA du corollaire A.6 par celui du corollaire A.7.

Nous obtenons finalement le résultat suivant :

Théorème 2.16. *Soient k un corps. Munissons-le de la valeur absolue triviale. Soient X un espace de Zariski d'un espace affine k-analytique et B une partie*

ouverte de X stable par le flot qui soit limite inductive d'espaces affinoïdes géométriquement intègres. Supposons que pour tout nombre premier q différent de la caractéristique du corps k et tout entier $r \in \mathbf{N}^*$, il existe une famille infinie $\mathcal{H}_{q^r}$ de corps deux à deux non isomorphes satisfaisant les propriétés suivantes :

(i) *tout élément de $\mathcal{H}_{q^r}$ est une extension finie et séparable de k contenant une racine primitive $(q^r)^{ème}$ de l'unité* ;

(ii) *pour tout élément K de $\mathcal{H}_{q^r}$, il existe un élément x de B et un élément α de $\mathbb{O}(B)$ de valeur absolue strictement inférieure à 1 en tout point de B et qui s'annule sur B tels que les corps K et $\mathrm{Frac}(\mathbb{O}_x)$ soient linéairement disjoints et le polynôme $S^{q^r} - \alpha$ soit irréductible sur leur compositum.*

Si la caractéristique du corps k est un nombre premier p, supposons en outre qu'il existe une famille infinie $\mathcal{H}_p$ de corps deux à deux non isomorphes satisfaisant les propriétés suivantes :

(i) *tout élément de $\mathcal{H}_p$ est une extension finie et séparable de k* ;

(ii) *pour tout élément K de $\mathcal{H}_p$, il existe un élément x de B et un élément α de $\mathbb{O}(B)$ de valeur absolue strictement inférieure à 1 en tout point de B et qui s'annule sur B tels que les corps K et $\mathrm{Frac}(\mathbb{O}_x)$ soient linéairement disjoints et le polynôme $S^p - \alpha$ soit irréductible sur leur compositum.*

Alors, tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $\mathrm{Frac}(\mathbb{O}(B))(T)$.

Remarque 2.17. De nouveau, le résultat de ce théorème est connu, puisque le corps $\mathrm{Frac}(\mathbb{O}(B))$ contient un corps de séries de Laurent sur k (engendré par l'un des éléments α).

Corollaire 2.18. *Soit k un corps. Notons*

$$k_{+\infty,1^-}[\![U_1, U_2]\!]$$

le sous-anneau de $k[U_1][\![U_2]\!]$ composé des séries de la forme

$$\sum_{n\geq 0} a_n(U_1)U_2^n$$

qui vérifient la condition

$$\forall r > 0, \forall s \in [0, 1[, \lim_{n\to+\infty} (r^{\deg(a_n)} s^n) = 0.$$

Alors, tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $\mathrm{Frac}(k_{+\infty,1^-}[\![U_1, U_2]\!])(T)$.

Démonstration. Appliquons le théorème 2.11 en choisissant pour espace X l'espace analytique de dimension deux $\mathbf{A}_k^{2,\mathrm{an}}$, dont nous noterons U_1 et U_2 les variables, et pour partie B le disque ouvert relatif de rayon 1 au-dessus de $\mathbf{A}_k^{1,\mathrm{an}}$:

$$B = \left\{ x \in \mathbf{A}_k^{2,\mathrm{an}} \;\middle|\; |U_2(x)| < 1 \right\}.$$

Cette partie est stable par le flot et nous avons $\mathcal{O}(B) = k_{+\infty,1^-}[\![U_1, U_2]\!]$.

Soit K une extension finie du corps k. Choisissons pour point x le point de coordonnées $(0, 0)$: l'anneau local $\mathcal{O}_x$ est isomorphe à $k[\![U_1, U_2]\!]$. Par conséquent, les corps K et $\mathrm{Frac}(\mathcal{O}_x)$ sont linéairement disjoints sur k. Choisissons pour fonction α la fonction U_2 : pour tout entier $n \geq 1$, le polynôme $S^n - U_2$ est irréductible sur le corps $\mathrm{Frac}(\mathcal{O}_x) \otimes_k K \simeq K[\![U_1, U_2]\!]$. Les hypothèses du théorème 2.11 sont donc satisfaites. On en déduit le résultat attendu. □

Ce dernier énoncé peut surprendre, puisqu'il découle directement du corollaire 2.14. En effet, le corps $\mathrm{Frac}(k_{r^-,1^-}[\![U_1, U_2]\!])$ contient le corps $k(\!(U_2)\!)$. Il présente cependant un intérêt dans le cadre de l'analogie entre corps de fonctions et corps de nombres. La droite analytique sur un corps trivialement valué est proche, à bien des égards, du spectre analytique — espace analytique de dimension 0 — d'un anneau d'entiers de corps de nombres (voir annexe B). Il semble donc raisonnable d'envisager que le résultat du corollaire précédent reste vrai en remplaçant l'anneau $k_{r^-,1^-}[\![U_1, U_2]\!]$ par l'anneau du disque ouvert de rayon 1 au-dessus du spectre d'un anneau d'entiers de corps de nombres. Signalons que les constructions effectuées peuvent effectivement être menées dans ce cadre. Pour conclure, seuls manquent encore les théorèmes du type GAGA sur les espaces de Berkovich au-dessus des anneaux d'entiers de corps de nombres.

Conjecture 2.19. *Soient K un corps de nombres, A l'anneau de ses entiers et Σ_∞ l'ensemble des plongements de K dans $\mathbf{C}$. Notons $A_{1^-}[\![X]\!]$ le sous-anneau de $A[\![X]\!]$ composé des séries f telles que, pour tout $\sigma \in \Sigma_\infty$, la série à coefficients complexes $\sigma(f)$ a un rayon de convergence supérieur ou égal à 1. Alors, tout groupe fini est groupe de Galois d'une extension finie et régulière du corps* $\mathrm{Frac}(A_{1^-}[\![X]\!])(T)$.

Remarque 2.20. Nous ignorons si le corps $\mathrm{Frac}(A_{1^-}[\![X]\!])$ est fertile, même lorsque l'anneau A est l'anneau $\mathbf{Z}$ des entiers.

3. Problème inverse de Galois sur un disque relatif

Soit A un anneau d'entiers de corps de nombres. Nous allons maintenant appliquer la stratégie de raccord décrite à la section 1 dans le cadre des espaces de Berkovich sur A (voir annexe B). Plus précisément, un groupe fini G étant donné,

nous allons construire un revêtement galoisien de groupe G du disque

$$\mathbf{D} = \left\{ x \in \mathbf{A}_A^{1,\mathrm{an}} \,\middle|\, |T(x)| < 1 \right\}.$$

Cela indique que la troisième étape de notre démonstration différera fondamentalement de la troisième étape de la démonstration du cas complexe. En effet, le disque $\mathbf{D}$ est un espace affine et non plus projectif comme l'était $\mathbf{P}^1(\mathbf{C})$. En particulier, les théorèmes GAGA n'y sont pas valables. Nous utiliserons, pour les remplacer, le caractère Stein du disque $\mathbf{D}$.

Nous noterons $X = \mathbf{A}_A^{1,\mathrm{an}}$ et, pour tout idéal maximal $\mathfrak{m}$ de A,

$$\mathbf{D}_{\mathfrak{m}} = \mathbf{D} \cap \pi^{-1}([a_0, \tilde{a}_{\mathfrak{m}}]) \quad \text{et} \quad \mathbf{D}'_{\mathfrak{m}} = \mathbf{D} \cap \pi^{-1}(]a_0, \tilde{a}_{\mathfrak{m}}]).$$

Ces deux parties sont connexes.

3A. ***Construction locale de revêtements cycliques.*** Dans le cas complexe, la construction locale était particulièrement simple car nous disposions de racines primitives de l'unité de tout ordre. Elle ne sera guère plus difficile ici puisque, comme nous allons l'expliquer, un entier $n \geq 1$ étant donné, il existe toujours une branche de $\mathcal{M}(A)$, et même une infinité, dont l'anneau des fonctions contient une racine primitive $n^{\text{ème}}$ de l'unité.

Soient $n \geq 1$ un entier, p un nombre premier congru à 1 modulo n et $\mathfrak{m}$ un idéal maximal de A contenant p. Notons $\hat{A}_{\mathfrak{m}}$ le complété de l'anneau A pour la topologie $\mathfrak{m}$-adique. Soit $\pi_{\mathfrak{m}}$ une uniformisante de l'anneau $\hat{A}_{\mathfrak{m}}$. Posons

$$Q(S) = S^n - \pi_{\mathfrak{m}}^n - T \in \mathcal{O}(\mathbf{D}'_{\mathfrak{m}})[S].$$

Définissons un préfaisceau $\mathcal{F}$ sur $D'_{\mathfrak{m}}$ en posant, pour toute partie ouverte W de $D'_{\mathfrak{m}}$,

$$\mathcal{F}(W) = \mathcal{O}(W)[S]/(Q(S)),$$

et en utilisant les morphismes de restriction induits par ceux du faisceau $\mathcal{O}$. Le caractère unitaire du polynôme Q assure que $\mathcal{F}$ est un faisceau de $\mathcal{O}_{D'_{\mathfrak{m}}}$-algèbres cohérent. Nous considérons ce faisceau comme l'image directe du faisceau d'un revêtement fini de $\mathbf{D}'_{\mathfrak{m}}$.

Le résultat classique qui suit explique le choix des entiers n et p.

Lemme 3.1. *L'anneau $\mathbf{Z}_p$ contient une racine primitive $n^{ème}$ de l'unité et, pour tout $i \in \mathbf{N}$, nous avons $C_{1/n}^i \in \mathbf{Z}_p$.*

Soit $\zeta \in \hat{A}_{\mathfrak{m}}$ une racine primitive $n^{\text{ème}}$ de l'unité. Posons

$$U = \left\{ x \in \mathbf{D}'_{\mathfrak{m}} \,\middle|\, |T(x)| < |\pi_{\mathfrak{m}}(x)|^n \right\}.$$

Le résultat suivant affirme que le revêtement de $\mathbf{D}'_{\mathfrak{m}}$ associé au faiseau $\mathcal{F}$ est trivial au-dessus de l'ouvert U.

Proposition 3.2. *Il existe un isomorphisme de $\mathcal{O}_U$-algèbres*

$$\varphi : \mathscr{F} \to \mathcal{O}^n$$

tel que, pour tout ouvert V de U et tout élément s de $\mathscr{F}(V)$, nous ayons

$$\varphi(\zeta s) = \tau(\varphi(s)),$$

où τ désigne l'automorphisme du faisceau $\mathcal{O}^n$ qui consiste à faire agir la permutation cyclique $(1\ 2\ \ldots\ n)$ sur les coordonnées.

Démonstration. En utilisant le lemme précédent, on montre que la fonction $\pi_{\mathrm{m}}^{-n} T$ possède une racine $n^{\text{ème}}$ dans $\mathcal{O}(U)$. Nous la noterons ω. On en déduit l'égalité

$$Q(S) = S^n - \pi_{\mathrm{m}}^n - T = \prod_{j=0}^{n} (S - \pi_{\mathrm{m}} \zeta^j \omega) \quad \text{dans } \mathcal{O}(U)[S].$$

Par conséquent, le morphisme

$$\mathscr{F} \to \mathcal{O}^n, \quad R(S) \mapsto \big(R(\pi_{\mathrm{m}} \omega), R(\pi_{\mathrm{m}} \zeta^{-1} \omega), \ldots, R(\pi_{\mathrm{m}} \zeta^{-(n-1)} \omega)\big)$$

est un isomorphisme. On vérifie immédiatement qu'il satisfait la condition requise. □

Démontrons, à présent, que le revêtement est irréductible.

Lemme 3.3. *Le polynôme $Q(S) = S^n - \pi_{\mathrm{m}}^n - T$ est irréductible sur le corps* $\mathrm{Frac}(\mathcal{O}(\mathbf{D}'_{\mathrm{m}}))$. *En particulier, l'anneau $\mathscr{F}(\mathbf{D}'_{\mathrm{m}})$ est intègre.*

Démonstration. Notons z_{m} le point 0 de la fibre $\pi^{-1}(\tilde{a}_{\mathrm{m}})$. D'après la discussion menée à la fin de l'annexe B, l'anneau local en ce point est isomorphe à l'anneau $\hat{A}_{\mathrm{m}}[\![T]\!]$. Commençons par montrer que le polynôme $Q(S)$ est irréductible sur le corps $\mathrm{Frac}(\mathcal{O}_{z_{\mathrm{m}}})$. Pour des raisons de valuation T-adique, l'élément $\pi_{\mathrm{m}}^n + T$ de $\hat{A}_{\mathrm{m}}[\![T]\!]$ n'est racine $d^{\text{ème}}$ dans $\hat{A}_{\mathrm{m}}[\![T]\!]$ pour aucun diviseur $d \geq 2$ de n. D'après la théorie de Kummer, cela impose au polynôme $Q(S)$ d'être irréductible sur $\mathrm{Frac}(\mathcal{O}_{z_{\mathrm{m}}})$. Les mêmes arguments que dans la preuve du lemme 2.7 permettent alors de conclure. □

Nous pouvons même être plus précis et démontrer un principe du prolongement analytique.

Lemme 3.4. *Soient x un point de U et i un élément de $[\![1, n]\!]$. Le morphisme*

$$\rho_{i,x} : \mathscr{F}(\mathbf{D}'_{\mathrm{m}}) \longrightarrow \mathscr{F}_x \xrightarrow[\sim]{\varphi_x} \mathcal{O}_x^n \xrightarrow{p_i} \mathcal{O}_x,$$

où p_i est la projection sur le $i^{ème}$ facteur, est injectif.

Démonstration. Soit s un élément de l'anneau $\mathscr{F}(\mathbf{D}'_{\mathfrak{m}}) = \mathscr{O}(\mathbf{D}'_{\mathfrak{m}})[S]/(Q(S))$ dont l'image par le morphisme $\rho_{i,x}$ est nulle. Choisissons un élément $R(S)$ de $\mathscr{O}(\mathbf{D}'_{\mathfrak{m}})[S]$ qui représente la section s. Reprenons les notations de la preuve de la proposition 3.2. Par hypothèse, nous avons

$$R(\pi_{\mathfrak{m}}\,\zeta^{-i}\,\omega) = 0 \text{ dans } \mathscr{O}_x.$$

Pour montrer que l'élément s est nul, il suffit de montrer que le polynôme $Q(S)$ est le polynôme minimal de l'élément $\pi_{\mathfrak{m}}\,\zeta^{-i}\,\omega$ sur le corps $\mathrm{Frac}(\mathscr{O}(\mathbf{D}'_{\mathfrak{m}}))$. C'est bien le cas, puisque le lemme précédent assure que le polynôme Q est irréductible sur le corps $\mathrm{Frac}(\mathscr{O}(\mathbf{D}'_{\mathfrak{m}}))$. □

Terminons par un résultat topologique.

Lemme 3.5. *La partie*

$$F = \mathbf{D}'_{\mathfrak{m}} \setminus U = \left\{x \in \mathbf{D}'_{\mathfrak{m}} \;\middle|\; |T(x)| \geq |\pi_{\mathfrak{m}}(x)|^n\right\}$$

est fermée dans le disque $\mathbf{D}$.

Démonstration. Il suffit de montrer que F est fermée dans $\mathbf{D}_{\mathfrak{m}}$ puisque cette dernière partie est elle-même fermée dans $\mathbf{D}$. En d'autres termes, nous souhaitons montrer que la partie

$$V = U \cup (\mathbf{D} \cap \pi^{-1}(a_0))$$

est ouverte dans $\mathbf{D}_{\mathfrak{m}}$. Puisque U est une partie ouverte de $\mathbf{D}_{\mathfrak{m}}$, il suffit de montrer que V est voisinage dans $\mathbf{D}_{\mathfrak{m}}$ de chacun des points de $\mathbf{D} \cap \pi^{-1}(a_0)$.

Soit x un point de $\mathbf{D} \cap \pi^{-1}(a_0)$. Posons $r = |T(x)|$. C'est un élément de l'intervalle $]0, 1[$. Soient s un élément de $]r, 1[$ et ε un élément de $]0, 1[$ tels que l'on ait $|\pi_{\mathfrak{m}}|_{\mathfrak{m}}^{n\varepsilon} > s$. La partie

$$\left\{y \in \pi^{-1}([a_0, a_{\mathfrak{m}}^{\varepsilon}[) \;\middle|\; |T(y)| < s\right\}$$

est un voisinage ouvert du point x dans $\mathbf{D}_{\mathfrak{m}}$ qui est contenu dans V. □

3B. ***Raccord et retour à l'algèbre.*** Soit G un groupe fini. Notons $n \in \mathbf{N}^*$ son ordre. Soient $g_1, \ldots, g_t$, avec $t \in \mathbf{N}^*$, des générateurs du groupe G. Pour tout élément i de $[\![1, t]\!]$, notons n_i l'ordre de l'élément g_i, choisissons un nombre premier p_i congru à 1 modulo n_i et un idéal maximal $\mathfrak{m}_i$ de A contenant p_i. Nous pouvons supposer que les $\mathfrak{m}_i$ sont distincts.

Soit i un élément de $[\![1, t]\!]$. Construisons par la méthode du numéro 3A un revêtement galoisien de groupe $\mathbf{Z}/n_i\mathbf{Z}$. Il est défini au-dessus de $\mathbf{D}'_{\mathfrak{m}_i}$ et trivial au-dessus de

$$U_i = \left\{x \in \mathbf{D}'_{\mathfrak{m}_i} \;\middle|\; |T(x)| < |\pi_{\mathfrak{m}_i}(x)|^{n_i}\right\}.$$

Notons $\mathrm{Ind}_{\langle g_i\rangle}^{G}(\mathbf{D}'_{\mathfrak{m}_i})$ le G-revêtement induit (*cf.* section 1).

D'après le lemme 3.5, pour tout élément i de $[\![1, t]\!]$, la partie $F_i = \mathbf{D}'_{\mathfrak{m}_i} \setminus U_i$ est fermée dans $\mathbf{D}$. Définissons une partie ouverte de $\mathbf{D}$ par

$$U_0 = \mathbf{D} \setminus \bigcup_{1 \leq i \leq t} F_i.$$

On se convainc aisément que cet ensemble est connexe. Considérons le G-revêtement $\mathrm{Ind}_{\langle e \rangle}^{G}(U_0)$ induit par le revêtement trivial au-dessus de U_0. Recollons ces différents revêtements par la méthode décrite à la section 1. Nous obtenons un revêtement de $\mathbf{D}$, galoisien de groupe G, associé à un faisceau $\mathcal{G}$. On montre à l'aide du lemme 3.4 qu'il est intègre, c'est-à-dire que l'anneau $\mathcal{G}(\mathbf{D})$ est intègre.

Nous disposons, à présent, d'un revêtement du disque $\mathbf{D}$ possédant le groupe de Galois désiré G. Il nous reste à montrer que l'extension induite entre les corps de fonctions est galoisienne de même groupe. Nous utiliserons, pour ce faire, le caractère Stein du disque $\mathbf{D}$ (*cf.* théorème B.4).

Proposition 3.6. *Le groupe des automorphismes de $\mathcal{O}(\mathbf{D})$-algèbres du faisceau $\mathcal{G}(\mathbf{D})$ est isomorphe à G.*

Démonstration. Soient $\mathcal{A}$ et $\mathcal{B}$ deux faisceaux de $\mathcal{O}_{\mathbf{D}}$-algèbres cohérents. Considérons l'application

$$\mathrm{Mor}_{\mathcal{O}}(\mathcal{A}, \mathcal{B}) \to \mathrm{Mor}_{\mathcal{O}(\mathbf{D})}(\mathcal{A}(\mathbf{D}), \mathcal{B}(\mathbf{D})).$$

Elle est bijective car les faisceaux $\mathcal{A}$ et $\mathcal{B}$ satisfont le théorème A sur $\mathbf{D}$.

Par construction, le groupe des automorphismes de $\mathcal{O}_{\mathbf{D}}$-algèbres du faisceau $\mathcal{G}$ est isomorphe à G. On en déduit le résultat attendu. □

Il reste à montrer que l'extension $\mathcal{O}(\mathbf{D}) \to \mathcal{G}(\mathbf{D})$ est entière. Puisque les théorèmes du type GAGA ne sont pas valables dans ce cadre, nous utiliserons un raisonnement direct.

Lemme 3.7. *Tout élément de $\mathcal{G}(\mathbf{D})$ annule un polynôme unitaire à coefficients dans $\mathcal{O}(\mathbf{D})$ de degré inférieur à n.*

Démonstration. Soit s un élément de $\mathcal{G}(\mathbf{D})$. Nous supposerons, tout d'abord, qu'il existe un point x_0 de U_0 tel que toutes les coordonnées de son image s_{x_0} dans $\mathcal{G}_{x_0} = \mathcal{O}_{X,x_0}^n$ soient distinctes. Puisque l'ouvert U_0 est connexe, le principe du prolongement analytique (*cf.* théorème B.3) assure qu'en tout point x de U_0, toutes les coordonnées du germe s_x sont distinctes. Notons $a_1, \ldots, a_n$ les coordonnées de l'image de s dans $\mathcal{G}(U_0) = \mathcal{O}(U_0)^n$. Posons

$$M(Z) = \prod_{l=1}^{n} (Z - a_l) \in \mathcal{O}(U_0)[Z].$$

En tout point x de U_0, l'image du polynôme M est l'unique polynôme unitaire de degré inférieur à n à coefficients dans $\mathcal{O}_x$ qui annule le germe s_x.

Pour tout élément j de $[\![0,t]\!]$, posons $V_j = U_0 \cup \bigcup_{1\leq i\leq j} \mathbf{D}'_{\mathfrak{m}_i}$. Montrons, par récurrence, que pour tout élément j de $[\![0,t]\!]$, il existe un polynôme unitaire N_j de degré n à coefficients dans $\mathcal{O}(V_j)$ qui annule l'élément $s_{|V_j}$ de $\mathcal{G}(V_j)$. Nous avons déjà traité le cas $j=0$. Soit maintenant un élément j de $[\![0,t-1]\!]$ pour lequel l'hypothèse de récurrence est vérifiée. L'élément $s_{|\mathbf{D}'_{\mathfrak{m}_{j+1}}}$ de l'anneau $\mathcal{G}(\mathbf{D}'_{\mathfrak{m}_{j+1}}) = \mathcal{O}(\mathbf{D}'_{\mathfrak{m}_{j+1}})[S]/(S^{n_{j+1}} - p_{j+1}^{n_{j+1}} - T)$ est annulé par un polynôme unitaire M_{j+1} de degré inférieur à n à coefficients dans le corps $\mathcal{O}(\mathbf{D}'_{\mathfrak{m}_{j+1}})$. Soit x un élément de $U_{j+1} = \mathbf{D}'_{\mathfrak{m}_{j+1}} \cap U_0$. Nous avons démontré qu'il existe un unique polynôme unitaire de degré inférieur à n à coefficients dans $\mathcal{O}_x$ qui annule le germe s_x. On en déduit que les images des polynômes N_j et M_{j+1} dans $\mathcal{O}_x[Z]$ coïncident. L'ouvert U_{j+1} étant connexe, d'après le théorème B.3, les images de ces polynômes dans $\mathcal{O}(U_{j+1})[Z]$ coïncident. On en déduit que le polynôme N_j se prolonge en un polynôme unitaire N_{j+1} de degré inférieur à n à coefficients dans $\mathcal{O}(V_{j+1})$ qui annule l'élément $s_{|V_{j+1}}$ de $\mathcal{G}(V_{j+1})$.

On déduit finalement le résultat attendu du cas $j=t$.

Soit x_0 un point de l'ouvert U_0. La fibre du faisceau $\mathcal{G}$ au point x_0 est isomorphe à l'algèbre $\mathcal{O}_{x_0}^n$. D'après le théorème B.4, le faisceau $\mathcal{G}$ vérifie le théorème A de Cartan sur le disque $\mathbf{D}$. On en déduit qu'il existe un élément s_0 de $\mathcal{G}(\mathbf{D})$ dont toutes les coordonnées de l'image dans la fibre $\mathcal{G}_{x_0} = \mathcal{O}_{x_0}^n$ sont distinctes.

Soit s un élément de $\mathcal{G}(\mathbf{D})$. Il existe un élément λ de $\mathcal{O}(\mathbf{D})$ tel que toutes les coordonnées du germe de la section $s_1 = s + \lambda s_0$ au point x_0 soient distinctes. Le raisonnement qui précède montre qu'il existe deux polynômes unitaires P_0 et P_1 de degré inférieur à n à coefficients dans $\mathcal{O}(\mathbf{D})$ qui annulent respectivement les sections s_0 et s_1. On en déduit qu'il existe un polynôme unitaire P de degré inférieur à n à coefficients dans $\mathcal{O}(\mathbf{D})$ qui annule la section s. □

Lemme 3.8. *L'anneau A est intégralement fermé dans l'anneau $\mathcal{G}(\mathbf{D})$.*

Démonstration. Soit P un polynôme unitaire à coefficients dans A sans racines dans A. Supposons, par l'absurde, qu'il existe une section s de $\mathcal{G}(\mathbf{D})$ qui est racine du polynôme P. Notons z_0 le point 0 de la fibre $\pi^{-1}(a_0)$ de l'espace X. C'est un point de l'ouvert U_0. Notons a la première coordonnée de l'image du germe s_{z_0} par l'isomorphisme $\mathcal{G}_{z_0} \simeq \mathcal{O}_{z_0}^t$. C'est un élément de $\mathcal{O}_{z_0}$ qui vérifie l'égalité $P(a)=0$. D'après la discussion menée à la fin de l'annexe B, l'anneau local $\mathcal{O}_{z_0}$ se plonge dans l'anneau $K[\![T]\!]$. On en déduit que le polynôme P possède une racine dans l'anneau $K[\![T]\!]$ et donc dans le corps K. Puisque l'anneau A est algébriquement fermé dans le corps K, cette racine doit appartenir à A. Nous avons abouti à une contradiction. On en déduit le résultat annoncé. □

Introduisons une définition correspondant à cette propriété.

Définition 3.9. Une extension L du corps $\mathrm{Frac}(\mathcal{O}(\mathbf{D}))$ est dite régulière si le corps K est algébriquement fermé dans L.

Regroupons, à présent, les résultats obtenus.

Proposition 3.10. *L'extension de corps*

$$\mathrm{Frac}(\mathcal{O}(\mathbf{D})) \to \mathrm{Frac}(\mathcal{G}(\mathbf{D}))$$

est finie de degré n, régulière et galoisienne de groupe G.

Démonstration. L'extension $\mathrm{Frac}(\mathcal{O}(\mathbf{D})) \to \mathrm{Frac}(\mathcal{G}(\mathbf{D}))$ est finie et de degré inférieur à n d'après le lemme 3.7. Elle est régulière d'après le lemme 3.8. On déduit de la proposition 3.6 qu'il existe un morphisme injectif du groupe G dans le groupe des $\mathrm{Frac}(\mathcal{O}(\mathbf{D}))$-automorphismes du corps $\mathrm{Frac}(\mathcal{G}(\mathbf{D}))$. Or le groupe G a pour cardinal n. On en déduit que l'extension $\mathrm{Frac}(\mathcal{O}(\mathbf{D})) \to \mathrm{Frac}(\mathcal{G}(\mathbf{D}))$ est exactement de degré n, qu'elle est galoisienne et que son groupe de Galois est isomorphe au groupe G. □

Remarque 3.11. Puisque le disque $\mathbf{D}$ est connexe, les théorèmes B.3 et B.4 assurent que l'anneau des sections méromorphes globales $\mathcal{M}(\mathbf{D})$ est un corps isomorphe à $\mathrm{Frac}(\mathcal{O}(\mathbf{D}))$. L'extension $\mathrm{Frac}(\mathcal{O}(\mathbf{D})) \to \mathrm{Frac}(\mathcal{G}(\mathbf{D}))$ est donc bien l'extension obtenue à partir du revêtement du disque $\mathbf{D}$ associé au faisceau $\mathcal{G}$ en passant aux corps de fonctions.

3C. ***Conclusion et généralisations.*** Regroupons, à présent, les résultats que nous avons obtenus. Puisque nous sommes partis d'un groupe fini G arbitraire, nous avons finalement démontré que tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $\mathrm{Frac}(\mathcal{O}(\mathbf{D}))$. D'après la description de l'anneau $\mathcal{O}(\mathbf{D})$ donnée à la fin de l'annexe B, ce dernier est isomorphe au corps $\mathrm{Frac}(A_1\text{-}[\![T]\!])$, où $A_1\text{-}[\![T]\!]$ désigne l'anneau des séries en une variable à coefficients dans A de rayon de convergence complexe supérieur ou égal à 1 en toute place infinie. Lorsque $A = \mathbf{Z}$, nous retrouvons bien ainsi le résultat de Harbater [1988, Corollary 3.8] énoncé en introduction.

Théorème 3.12. *Soit A un anneau d'entiers de corps de nombres. Tout groupe fini est groupe de Galois d'une extension finie et régulière du corps* $\mathrm{Frac}(A_1\text{-}[\![T]\!])$.

Remarque 3.13. Pour tout $r > 1$, l'anneau $A_r\text{-}[\![T]\!]$ des séries en une variable à coefficients dans A de rayon de convergence complexe supérieur ou égal à r en toute place infinie (une seule suffirait) est réduit à l'anneau de polynômes $A[T]$. Si nous disposions du théorème précédent pour un certain nombre réel $r > 1$, nous aurions donc résolu le problème inverse de Galois géométrique sur K.

Pour finir, nous regroupons plusieurs résultats proches de celui du théorème 3.12. Les démonstrations en sont fort similaires et nous n'indiquerons que les modifications à effectuer.

Ainsi que nous l'avons déjà signalé, le spectre analytique d'un anneau d'entiers de corps de nombres présente de nombreuses similitudes avec la droite analytique

sur un corps trivialement valué. C'est donc, tout d'abord, dans ce cadre que nous allons nous placer. Soit k un corps. Munissons-le de la valeur absolue triviale afin d'en faire un corps ultramétrique complet. Considérons, maintenant, l'espace $\mathbf{A}_k^{2,\mathrm{an}}$, analogue de $\mathbf{A}_A^{1,\mathrm{an}}$. Nous noterons U et T les coordonnées sur cet espace.

Lorsque la caractéristique du corps k est nulle, pour tout entier $n \geq 1$, il existe une infinité de branches de la droite $\mathbf{A}_k^{1,\mathrm{an}}$ dont l'anneau des fonctions contient une racine primitive $n^{\text{ème}}$ de l'unité. Posons

$$\mathbf{D}_k = \left\{ x \in \mathbf{A}_k^{2,\mathrm{an}} \;\middle|\; |T(x)| < 1 \right\}.$$

En appliquant le raisonnement de cette section, nous démontrons que tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $\mathrm{Frac}(\mathscr{O}(\mathbf{D}_k))$. Par régulière, nous entendons ici que le corps $k(U)$ est algébriquement fermé dans l'extension en question.

Supposons, à présent, que le corps k est de caractéristique p, où p est un nombre premier. Dans ce cas, la construction des revêtements cycliques locaux est plus complexe. Cependant, il est possible de la mener à bien en faisant appel aux extensions d'Artin–Schreier–Witt, comme nous l'avons déjà fait au numéro 2A. Il est plus difficile de montrer qu'un tel revêtement est trivial sur une partie dont le complémentaire est fermé dans $\mathbf{D}_k$, mais les propriétés du flot nous permettent d'y parvenir.

En utilisant une description explicite de l'anneau $\mathscr{O}(\mathbf{D}_k)$, nous obtenons finalement le résultat suivant :

Théorème 3.14. *Soit k un corps. Notons*

$$k_{+\infty,1^-}[\![U, T]\!]$$

le sous-anneau de $k[U][\![T]\!]$ composé des séries de la forme

$$\sum_{n\geq 0} a_n(U)T^n$$

qui vérifient la condition

$$\forall r > 0, \forall s \in [0, 1[, \ \lim_{n\to+\infty} (r^{\deg(a_n)}\, s^n) = 0.$$

Tout groupe fini est groupe de Galois d'une extension finie et régulière du corps $\mathrm{Frac}(k_{+\infty,1^-}[\![U, T]\!])$.

Remarque 3.15. Le théorème précédent nous permet, en particulier, de réaliser, pour tout corps k, tout groupe fini comme groupe de Galois sur le corps des fractions de $k[U][\![T]\!]$. Nous étendons ainsi les corollaires 1.4 et 1.5 de [Harbater 1984b].

Annexe A. Théorèmes GAGA relatifs sur un affinoïde

Soit k un corps muni d'une valeur absolue ultramétrique pour laquelle il est complet, $\mathscr{A}$ une algèbre k-affinoïde et X un schéma localement de type fini sur $\mathscr{A}$. Berkovich [1993, 2.6] a défini, de manière fonctorielle, l'analytifié X^{an} du schéma X. Il vient avec un morphisme d'espaces localement annelés $X^{\mathrm{an}} \to X$, qui est plat et surjectif (cette dernière propriété tombe évidemment en défaut dans le cas complexe). À tout faisceau de $\mathscr{O}_X$-modules $\mathscr{F}$, nous pouvons associer, par rétrotirette, un faisceau de $\mathscr{O}_{X^{\mathrm{an}}}$-modules, que nous noterons $\mathscr{F}^{\mathrm{an}}$. Remarquons que l'analytifié d'un faisceau cohérent est encore cohérent.

Dans la lignée des théorèmes GAGA [Serre 1955–1956 ; SGA1 1971, exposé XII] nous allons nous intéresser aux propriétés du foncteur d'analytification lorsque l'espace X est propre. Précisément, nous allons démontrer le théorème suivant :

Théorème A.1. *Soit k un corps muni d'une valeur absolue ultramétrique pour laquelle il est complet, $\mathscr{A}$ une algèbre k-affinoïde et X un $\mathscr{A}$-schéma propre.*

(i) *Pour tout faisceau de $\mathscr{O}_X$-modules cohérent $\mathscr{F}$ et tout entier $q \in \mathbf{N}$, le morphisme $H^q(X, \mathscr{F}) \to H^q(X^{\mathrm{an}}, \mathscr{F}^{\mathrm{an}})$ est un isomorphisme.*

(ii) *Le foncteur d'analytification $\mathscr{F} \to \mathscr{F}^{\mathrm{an}}$ induit une équivalence entre la catégorie des $\mathscr{O}_X$-modules cohérents et celle des $\mathscr{O}_{X^{\mathrm{an}}}$-modules cohérents.*

La preuve originale de Serre, qui concerne l'analytification complexe, peut être adaptée à notre contexte sans difficultés majeures. Signalons que le théorème précédent a d'ailleurs déjà été obtenu par U. Köpf [1974] dans le cadre de la géométrie rigide et par A. Ducros en général, dans un texte inédit. Nous en rédigeons cependant une démonstration pour la commodité du lecteur, sans prétendre aucunement à l'originalité.

Comme dans le cas complexe, on se ramène à démontrer le théorème pour un espace X de la forme $\mathbf{P}^r_{\mathscr{A}}$ et on utilise les résultats classiques concernant les faisceaux cohérents sur un tel espace. Deux propriétés joueront un rôle essentiel dans la preuve : la platitude du morphisme $X^{\mathrm{an}} \to X$ et la finitude cohomologique des morphismes propres. Ce dernier point prend la forme du théorème suivant :

Théorème A.2. *Soit k un corps muni d'une valeur absolue ultramétrique pour laquelle il est complet, $\mathscr{A}$ une algèbre k-affinoïde et X un $\mathscr{A}$-espace analytique propre. Pour tout faisceau de $\mathscr{O}_X$-modules cohérent et tout entier naturel q, le $\mathscr{A}$-module $H^q(X, \mathscr{F})$ est un $\mathscr{A}$-module de Banach de type fini.*

Ce résultat a été démontré par R. Kiehl [1967, Theorem 3.3] dans le cas d'un corps de valuation non triviale et d'objets strictement affinoïdes. Il a été étendu au cas général par Berkovich [1990, Proposition 3.3.5].

Indiquons pour finir le seul véritable ajout que nous avons dû faire à la preuve de Serre (et qui figure chez Ducros) : il s'agit du lemme A.4, un résultat de changement de base, utilisé pour pallier le fait qu'un point de l'espace k-analytique $\mathbf{P}_k^{r,\mathrm{an}}$ n'est pas toujours situé sur un hyperplan.

Démonstration du théorème A.1. Commençons par quelques réductions classiques. En utilisant le lemme de Chow [EGA II 1961, théorème 5.6.1], on montre qu'il suffit de prouver le théorème dans le cas où X est un schéma projectif sur $\mathscr{A}$. Dans le cas complexe, les détails de l'argument figurent dans [SGA1 1971, exposé XII] ; un raisonnement en tout point semblable vaut ici.

Si X est un schéma projectif sur $\mathscr{A}$, il existe une immersion fermée $\varphi : X \to \mathbf{P}^r_{\mathscr{A}}$, pour un certain entier naturel r. Pour tout faisceau de $\mathcal{O}_X$-modules cohérent $\mathscr{F}$, le faisceau de $\mathcal{O}_{\mathbf{P}^r_{\mathscr{A}}}$-modules $\varphi_*(\mathscr{F})$, qui n'est autre que le prolongement de $\mathscr{F}$ par zéro, est encore cohérent. On vérifie que cette opération de prolongement commute à l'analytification et préserve la cohomologie. En outre, elle possède un inverse à gauche : la restriction à Y. En utilisant ces propriétés, on montre qu'il suffit de prouver le théorème dans le cas où X est un espace projectif sur $\mathscr{A}$. C'est ce que nous supposerons désormais.

Assertion (i) *lorsque* $\mathscr{F} = \mathcal{O}(n)$. Nous allons démontrer, par récurrence sur r, que, pour tout entier naturel r et tout entier relatif n, l'assertion (i) du théorème est vraie lorsque $X = \mathbf{P}^r_{\mathscr{A}}$ et $\mathscr{F} = \mathcal{O}_X(n)$.

Pour $r = 0$, le résultat découle du théorème d'acyclicité de Tate.

Soit $r \in \mathbf{N}$ tel que le résultat soit vrai pour $\mathbf{P}^r_{\mathscr{A}}$. Posons $X = \mathbf{P}^{r+1}_{\mathscr{A}}$. Soit t une section non nulle du fibré $\mathcal{O}_X(1)$ et Y l'hyperplan de X (isomorphe à $\mathbf{P}^r_{\mathscr{A}}$) qu'elle définit. Nous noterons $\mathcal{O}_Y$ à la fois le faisceau structural sur Y et son prolongement par zéro à X. D'après l'hypothèse de récurrence, pour tout entier $q \in \mathbf{N}$, le morphisme

$$H^q(X, \mathcal{O}_Y(n)) = H^q(Y, \mathcal{O}_Y(n)) \to H^q(Y^{\mathrm{an}}, \mathcal{O}_{Y^{\mathrm{an}}}(n)) = H^q(X^{\mathrm{an}}, \mathcal{O}_{Y^{\mathrm{an}}}(n))$$

est un isomorphisme.

Pour tout $n \in \mathbf{Z}$, la multiplication par t définit une suite exacte courte

$$0 \to \mathcal{O}_X(n-1) \to \mathcal{O}_X(n) \to \mathcal{O}_Y(n) \to 0.$$

En écrivant la suite exacte longue associée et en utilisant le lemme des cinq, on montre que l'on a un isomorphisme

$$H^q(X, \mathcal{O}_X(n)) \simeq H^q(X^{\mathrm{an}}, \mathcal{O}_{X^{\mathrm{an}}}(n))$$

pour tout $q \in \mathbf{N}$ si, et seulement si, on a un isomorphisme

$$H^q(X, \mathcal{O}_X(n-1)) \simeq H^q(X^{\mathrm{an}}, \mathcal{O}_{X^{\mathrm{an}}}(n-1))$$

pour tout $q \in \mathbf{N}$.

Un calcul explicite montre que l'on a $H^q(X, \mathcal{O}_X) \simeq H^q(X^{\mathrm{an}}, \mathcal{O}_{X^{\mathrm{an}}})$ pour tout $q \in \mathbf{N}$. On en déduit le résultat annoncé.

Assertion (i) *en général.* Soit $r \in \mathbf{N}$. Posons $X = \mathbf{P}^r_{\mathcal{A}}$. Nous allons démontrer, par une récurrence descendante sur q, que, pour tout entier naturel q, l'assertion (i) du théorème est vraie pour H^q.

Si $q > r$, pour tout faisceau de $\mathcal{O}_X$-modules cohérent $\mathcal{F}$, les groupes $H^q(X, \mathcal{F})$ et $H^q(X^{\mathrm{an}}, \mathcal{F}^{\mathrm{an}})$ sont tous deux nuls, et le résultat est vrai.

Soit $q \in \mathbf{N}^*$ tel que le résultat soit vrai pour H^q. Soit $\mathcal{F}$ un faisceau de $\mathcal{O}_X$-modules cohérent. Nous pouvons l'insérer dans une suite exacte de faisceaux de $\mathcal{O}_X$-modules cohérents

$$0 \to \mathcal{R} \to \mathcal{L} \to \mathcal{F} \to 0,$$

où $\mathcal{L}$ est somme directe de faisceaux isomorphes à $\mathcal{O}(n)$, avec $n \in \mathbf{Z}$.

Insérons le faisceau $\mathcal{R}$ dans une suite exacte courte du même type

$$0 \to \mathcal{R}' \to \mathcal{L}' \to \mathcal{R} \to 0.$$

D'après l'hypothèse de récurrence et le cas $\mathcal{F} = \mathcal{O}(n)$ déjà démontré, le résultat vaut pour le faisceau $\mathcal{R}'$ en rang q et pour le faisceau $\mathcal{L}'$ en rangs q et $q-1$. Le lemme des cinq assure alors que le morphisme

$$H^{q-1}(X, \mathcal{R}) \to H^{q-1}(X^{\mathrm{an}}, \mathcal{R}^{\mathrm{an}})$$

est surjectif.

Pour les mêmes raisons que précédemment, nous savons en outre que le résultat vaut pour le faisceau $\mathcal{R}$ en rang q et pour le faisceau $\mathcal{L}$ en rangs q et $q-1$. Une nouvelle application du lemme des cinq assure alors que le morphisme

$$H^{q-1}(X, \mathcal{F}) \to H^{q-1}(X^{\mathrm{an}}, \mathcal{F}^{\mathrm{an}})$$

est bijectif.

Pleine fidélité du foncteur $\mathcal{F} \to \mathcal{F}^{\mathrm{an}}$. Soit X un espace projectif sur $\mathcal{A}$. Soient $\mathcal{F}$ et $\mathcal{G}$ deux faisceaux de $\mathcal{O}_X$-modules cohérents. Soit x^{an} un point de X^{an}. Notons x son image dans X.

Nous disposons des isomorphismes

$$\mathcal{H}om(\mathcal{F}, \mathcal{G})^{\mathrm{an}}_{x^{\mathrm{an}}} \simeq \mathrm{Hom}(\mathcal{F}, \mathcal{G})_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X^{\mathrm{an}}, x^{\mathrm{an}}}$$

et

$$\mathcal{H}om(\mathcal{F}^{\mathrm{an}}, \mathcal{G}^{\mathrm{an}})_{x^{\mathrm{an}}} \simeq \mathrm{Hom}(\mathcal{F}_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X^{\mathrm{an}}, x^{\mathrm{an}}}, \mathcal{G}_x \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X^{\mathrm{an}}, x^{\mathrm{an}}}).$$

La platitude du morphisme naturel $X^{\mathrm{an}} \to X$ entraîne que le morphisme

$$\mathcal{H}om(\mathcal{F}, \mathcal{G})^{\mathrm{an}} \to \mathcal{H}om(\mathcal{F}^{\mathrm{an}}, \mathcal{G}^{\mathrm{an}})$$

est un isomorphisme.

On conclut en appliquant le résultat de l'assertion (i) du théorème au faisceau cohérent $\mathscr{H}om(\mathscr{F}, \mathscr{G})$ et à l'entier $q = 0$.

Surjectivité essentielle du foncteur $\mathscr{F} \to \mathscr{F}^{\mathrm{an}}$. Nous allons démontrer, par récurrence sur r, que, pour tout entier naturel r, le foncteur $\mathscr{F} \to \mathscr{F}^{\mathrm{an}}$ est essentiellement surjectif lorsque $X = \mathbf{P}^r_{\mathscr{A}}$.

Lorsque $r = 0$, le résultat est classique [Berkovich 1990, Proposition 2.3.1].

Soit $r \in \mathbf{N}$ tel que le résultat soit vrai pour le schéma $\mathbf{P}^r_{\mathscr{A}}$. Posons $X = \mathbf{P}^{r+1}_{\mathscr{A}}$. Commençons par une série de lemmes.

Lemme A.3. *Pour chaque hyperplan projectif Y de X et chaque faisceau de $\mathscr{O}_{X^{\mathrm{an}}}$-modules cohérent $\mathscr{N}$, il existe un entier n_0 tel que*

$$\forall n \geq n_0,\ \forall q \geq 1,\ H^q(Y^{\mathrm{an}}, \mathscr{N}_{|Y^{\mathrm{an}}}(n)) = 0.$$

Démonstration. On démontre ce résultat en appliquant l'hypothèse de récurrence au faisceau $\mathscr{N}_{|Y^{\mathrm{an}}}$, puis en utilisant le résultat analogue pour les schémas projectifs et les isomorphismes fournis par l'assertion (i) du théorème. □

Lemme A.4. *Soit L une extension valuée complète de k. Notons $\pi : X_L^{\mathrm{an}} \to X^{\mathrm{an}}$ le morphisme de projection. Soient x un point de X^{an} et x_L l'un de ses antécédents par le morphisme π. Soit $\mathscr{F}$ un faisceau de $\mathscr{O}_{X^{\mathrm{an}}}$-modules cohérent. Supposons que la fibre $\pi^*(\mathscr{F})_{x_L}$ soit engendrée par l'ensemble des sections globales de $\pi^*(\mathscr{F})$. Alors, la fibre $\mathscr{F}_x$ est engendrée par l'ensemble des sections globales de $\mathscr{F}$.*

Démonstration. D'après le théorème A.2, $\mathscr{F}(X^{\mathrm{an}})$ est un $\mathscr{A}$-module de Banach fini. Considérons une famille $(f_1, \ldots, f_r)$, avec $r \in \mathbf{N}$, qui l'engendre. Notons $\mathscr{G}$ le conoyau du morphisme $\mathscr{O}^r_{X^{\mathrm{an}}} \to \mathscr{F}$ défini par cette famille. Puisque le produit tensoriel est exact à droite, le faisceau $\pi^*(\mathscr{G})$ est le conoyau du morphisme $\mathscr{O}^r_{X_L^{\mathrm{an}}} \to \pi^*(\mathscr{F})$ défini par la famille $(\pi^*(f_1), \ldots, \pi^*(f_r))$.

L'exactitude du foncteur $\cdot\, \hat{\otimes}_k L$ assure que les $(\mathscr{A}\hat{\otimes}_k L)$-modules $\pi^*(\mathscr{F})(X_L^{\mathrm{an}})$ et $\mathscr{F}(X^{\mathrm{an}})\hat{\otimes}_k L$ sont isomorphes. En particulier, la famille $(\pi^*(f_1), \ldots, \pi^*(f_r))$ engendre $\pi^*(\mathscr{F})(X_L^{\mathrm{an}})$. Puisque, par hypothèse, cet ensemble engendre $\pi^*(\mathscr{F})_{x_L}$, la fibre $\pi^*(\mathscr{G})_{x_L} \simeq \mathscr{G}_x \otimes_{\mathscr{O}_{X^{\mathrm{an}},x}} \mathscr{O}_{X_L^{\mathrm{an}},x_L}$ est nulle. *A fortiori*, nous avons $\mathscr{G}_x \otimes_{\mathscr{O}_{X^{\mathrm{an}},x}} \kappa(x_L) = 0$. Puisque $\mathscr{G}_x \otimes_{\mathscr{O}_{X^{\mathrm{an}},x}} \kappa(x_L) \simeq \mathscr{G}_x \otimes_{\mathscr{O}_{X^{\mathrm{an}},x}} \kappa(x) \otimes_{\kappa(x)} \kappa(x_L)$, nous avons même $\mathscr{G}_x \otimes_{\mathscr{O}_{X^{\mathrm{an}},x}} \kappa(x) = 0$, d'où l'on déduit que $\mathscr{G}_x = 0$, par le lemme de Nakayama. □

Lemme A.5. *Soient $\mathscr{N}$ un faisceau de $\mathscr{O}_{X^{\mathrm{an}}}$-modules cohérent et x un point de X^{an}. Il existe un entier naturel n_0 tel que, pour tout $n \geq n_0$, la fibre $\mathscr{N}(n)_x$ soit engendrée par l'ensemble des sections globales de $\mathscr{N}(n)$.*

Démonstration. D'après le lemme A.4, quitte à effectuer un changement de corps de base de k à $\mathscr{H}(x)$ (et à modifier les autres données en conséquence), nous pouvons supposer que le point x est k-rationnel. Il est alors situé sur l'analytifié Y^{an} d'un certain hyperplan projectif Y de X.

Soit t une section de $\mathcal{O}_X(1)$ de lieu des zéros Y. La multiplication par t définit une suite exacte

$$0 \to \mathcal{N}' \to \mathcal{N}(-1) \to \mathcal{N} \to \mathcal{N}_{|Y^{\mathrm{an}}} \to 0,$$

où $\mathcal{N}'$ est un faisceau de $\mathcal{O}_{X^{\mathrm{an}}}$-modules cohérent supporté par Y^{an}.

Soit $n \in \mathbf{Z}$. En tensorisant la suite précédente par $\mathcal{O}_{X^{\mathrm{an}}}(n)$ puis en la scindant, nous obtenons les deux suites exactes courtes

$$0 \to \mathcal{N}'(n) \to \mathcal{N}(n-1) \to \mathcal{P}_n \to 0$$

et

$$0 \to \mathcal{P}_n \to \mathcal{N}(n) \to \mathcal{N}_{|Y^{\mathrm{an}}}(n) \to 0,$$

qui donnent naissance aux deux suites exactes de cohomologie

$$H^1(X^{\mathrm{an}}, \mathcal{N}(n-1)) \to H^1(X^{\mathrm{an}}, \mathcal{P}(n)) \to H^2(X^{\mathrm{an}}, \mathcal{N}'(n))$$

et

$$H^1(X^{\mathrm{an}}, \mathcal{P}_n) \to H^1(X^{\mathrm{an}}, \mathcal{N}(n)) \to H^1(X^{\mathrm{an}}, \mathcal{N}_{|Y^{\mathrm{an}}}(n)).$$

D'après le lemme A.3, il existe un entier n_1 tel que, pour tout $n \geq n_1$, les groupes de cohomologie

$$H^2(X^{\mathrm{an}}, \mathcal{N}'(n)) \text{ et } H^1(X^{\mathrm{an}}, \mathcal{N}_{|Y^{\mathrm{an}}}(n))$$

soient nuls et, par conséquent, le morphisme composé

$$H^1(X^{\mathrm{an}}, \mathcal{N}(n-1)) \to H^1(X^{\mathrm{an}}, \mathcal{P}_n) \to H^1(X^{\mathrm{an}}, \mathcal{N}(n))$$

soit surjectif.

Le morphisme $X^{\mathrm{an}} \to \mathcal{M}(\mathcal{A})$ étant propre, le théorème A.2, assure que le $\mathcal{A}$-module $H^1(X^{\mathrm{an}}, \mathcal{N}(n_1-1))$ est de type fini, et donc noethérien. On en déduit qu'il existe un entier $n_2 \geq n_1$ tel que, pour tout $n \geq n_2$, le morphisme

$$H^1(X^{\mathrm{an}}, \mathcal{N}(n-1)) \to H^1(X^{\mathrm{an}}, \mathcal{N}(n))$$

soit un isomorphisme. Par conséquent, pour tout $n \geq n_2$, le morphisme surjectif

$$H^1(X^{\mathrm{an}}, \mathcal{P}_n) \to H^1(X^{\mathrm{an}}, \mathcal{N}(n))$$

est bijectif, d'où l'on déduit, en considérant la suite exacte longue associé à la seconde suite exacte courte, que le morphisme

$$H^0(X^{\mathrm{an}}, \mathcal{N}(n)) \to H^0(X^{\mathrm{an}}, \mathcal{N}_{|Y^{\mathrm{an}}}(n))$$

est surjectif.

D'après l'hypothèse de récurrence, le faisceau de $\mathcal{O}_{Y^{\mathrm{an}}}$-modules cohérent $\mathcal{N}_{|Y^{\mathrm{an}}}$ est l'analytifié d'un faisceau de $\mathcal{O}_Y$-modules cohérent $\mathcal{G}$. Notons x^{alg} l'image du point x dans Y. Les résultats classiques sur les schémas projectifs assurent qu'il existe un entier $n_0 \geq n_2$ tel que, pour tout $n \geq n_0$, la fibre $\mathcal{G}(n)_{x^{\mathrm{alg}}}$ soit engendrée,

en tant que $\mathcal{O}_{Y,x^{\mathrm{alg}}}$-module, par l'ensemble des sections globales $H^0(Y, \mathcal{G}(n))$. En utilisant l'assertion (i) du théorème, on en déduit que le résultat vaut encore en remplaçant respectivement Y par Y^{an}, $\mathcal{G}$ par $\mathcal{N}_{|Y^{\mathrm{an}}}$ et x^{alg} par x.

Notons $\mathcal{I}$ le faisceau d'idéaux qui définit Y^{an} dans X^{an}. Remarquons que sa fibre $\mathcal{I}_x$ est contenue dans l'idéal maximal $\mathfrak{m}_x$ de $\mathcal{O}_{X^{\mathrm{an}},x}$. Soit $n \geq n_0$. Nous venons de montrer que $\mathcal{N}(n)_x \otimes_{\mathcal{O}_{X^{\mathrm{an}},x}} (\mathcal{O}_{X^{\mathrm{an}},x}/\mathcal{I}_x)$ est engendré par $H^0(X^{\mathrm{an}}, \mathcal{N}_{|Y^{\mathrm{an}}}(n))$. On en déduit que $\mathcal{N}(n)_x \otimes_{\mathcal{O}_{X^{\mathrm{an}},x}} (\mathcal{O}_{X^{\mathrm{an}},x}/\mathfrak{m}_x)$ est engendré par $H^0(X^{\mathrm{an}}, \mathcal{N}_{|Y^{\mathrm{an}}}(n))$, et donc par $H^0(X^{\mathrm{an}}, \mathcal{N}(n))$. On conclut par le lemme de Nakayama. □

Terminons, à présent, la démonstration du théorème A.1. Soit $\mathcal{N}$ un faisceau de $\mathcal{O}_{X^{\mathrm{an}}}$-modules cohérent. En utilisant le résultat du lemme précédent et la compacité de X^{an}, on montre qu'il existe un entier n tel qu'en tout point x de X^{an}, la fibre $\mathcal{N}(n)_x$ soit engendrée par $H^0(X^{\mathrm{an}}, \mathcal{N}(n))$. On en déduit l'existence d'un entier naturel p, d'un faisceau de $\mathcal{O}_{X^{\mathrm{an}}}$-modules cohérent $\mathcal{R}$ et d'une suite exacte $0 \to \mathcal{R} \to \mathcal{O}_{X^{\mathrm{an}}}(-n)^p \to \mathcal{N} \to 0$. En appliquant le même raisonnement au faisceau $\mathcal{R}$, nous parvenons finalement à écrire le faisceau $\mathcal{N}$ comme le conoyau d'un morphisme $\varphi : \mathcal{O}_{X^{\mathrm{an}}}(-m)^q \to \mathcal{O}_{X^{\mathrm{an}}}(-n)^p$, avec $m \in \mathbf{Z}$ et $q \in \mathbf{N}$. Puisque le foncteur d'analytification est pleinement fidèle, le morphisme φ est l'analytifié d'un morphisme $\varphi^{\mathrm{alg}} : \mathcal{O}_X(-m)^q \to \mathcal{O}_X(-n)^p$. L'exactitude à droite du foncteur d'analytification assure alors que le faisceau $\mathcal{N}$ est isomorphe à l'analytifié du conoyau du morphisme φ^{alg}, qui est un faisceau de $\mathcal{O}_X$-modules cohérent. □

Corollaires. Nous énonçons ici deux corollaires du théorème A.1. Ils ont également pour objet des résultats de type GAGA, mais sur des bases qui ne sont plus nécessairement affinoïdes. Nous sommes convaincu qu'il est possible de les étendre à une base quelconque, de façon à obtenir un analogue parfait des théorèmes obtenus par M. Hakim [1972, chapitre VIII, théorèmes 3.2 et 3.5] dans le cadre de la géométrie analytique complexe. Cependant, pour éviter d'avoir à utiliser le formalisme un peu lourd des schémas relatifs sur un espace analytique, nous nous contenterons d'énoncer les deux cas particuliers que nous utilisons dans cet article.

Soit k un corps muni d'une valeur absolue ultramétrique pour laquelle il est complet, $\mathcal{A}$ une algèbre k-affinoïde et X un $\mathcal{A}$-schéma propre. Soit B une partie compacte de $\mathcal{M}(\mathcal{A})$ possédant un système fondamental de voisinages affinoïdes. Rappelons que la notation $\mathcal{O}(B)$ désigne l'anneau des germes de fonctions analytiques au voisinage de B. Notons $Y = X \times_{\mathrm{Spec}(\mathcal{A})} \mathrm{Spec}(\mathcal{O}(B))$ et désignons par Y^{an} l'image réciproque de B dans X^{an}. Munissons Y^{an} du faisceau des fonctions surconvergentes. En utilisant le morphisme d'analytification au-dessus d'un espace affinoïde défini par V. Berkovich, on montre qu'il existe un morphisme d'espaces localement annelés $Y^{\mathrm{an}} \to Y$. La rétrotirette d'un faisceau de $\mathcal{O}_Y$-modules cohérent $\mathcal{F}$ est un faisceau de $\mathcal{O}_{Y^{\mathrm{an}}}$-modules cohérent, que nous noterons $\mathcal{F}^{\mathrm{an}}$.

Corollaire A.6. *Supposons que nous nous trouvons dans la situation décrite ci-dessus.*

(i) *Pour tout faisceau de $\mathcal{O}_Y$-modules cohérent $\mathcal{F}$ et tout entier $q \in \mathbf{N}$, le morphisme $H^q(Y, \mathcal{F}) \to H^q(Y^{\mathrm{an}}, \mathcal{F}^{\mathrm{an}})$ est un isomorphisme.*

(ii) *Le foncteur d'analytification $\mathcal{F} \to \mathcal{F}^{\mathrm{an}}$ induit une équivalence entre la catégorie des $\mathcal{O}_Y$-modules cohérents et celle des $\mathcal{O}_{Y^{\mathrm{an}}}$-modules cohérents.*

Démonstration. Il faut tout d'abord remarquer que l'espace Y^{an} est compact. En reprenant le raisonnement de la preuve de la proposition 1 de [Cartan 1951], on en déduit que tout faisceau cohérent sur Y^{an} se prolonge en un faisceau cohérent sur un voisinage de Y^{an}, et donc sur une partie de la forme $Y^{\mathrm{an}} \times_{\mathcal{M}(\mathcal{A})} V$, où V est un voisinage affinoïde de B. En utilisant ce raisonnement et le théorème A.1, on obtient le résultat attendu. □

Soit k un corps muni d'une valeur absolue ultramétrique pour laquelle il est complet, $\mathcal{A}$ une algèbre k-affinoïde et X un $\mathcal{A}$-schéma propre. Soit B un espace $\mathcal{A}$-analytique qui soit limite inductive d'espaces affinoïdes. Notons $Z = X \times_{\mathrm{Spec}(\mathcal{A})} \mathrm{Spec}(\mathcal{O}(B))$. En utilisant le morphisme d'analytification au-dessus d'un espace affinoïde défini par Berkovich, on construit, par limite inductive, un espace analytique Z^{an} et un morphisme d'espaces localement annelés $Z^{\mathrm{an}} \to Z$. Comme précédemment, la rétrotirette d'un faisceau de $\mathcal{O}_Z$-modules cohérent $\mathcal{F}$ est un faisceau de $\mathcal{O}_{Z^{\mathrm{an}}}$-modules cohérent, que nous noterons $\mathcal{F}^{\mathrm{an}}$. Le résultat suivant se déduit alors aisément du théorème A.1.

Corollaire A.7. *Supposons que nous nous trouvons dans la situation décrite ci-dessus.*

(i) *Pour tout faisceau de $\mathcal{O}_Z$-modules cohérent $\mathcal{F}$ et tout entier $q \in \mathbf{N}$, le morphisme $H^q(Z, \mathcal{F}) \to H^q(Z^{\mathrm{an}}, \mathcal{F}^{\mathrm{an}})$ est un isomorphisme.*

(ii) *Le foncteur d'analytification $\mathcal{F} \to \mathcal{F}^{\mathrm{an}}$ induit une équivalence entre la catégorie des $\mathcal{O}_Z$-modules cohérents et celle des $\mathcal{O}_{Z^{\mathrm{an}}}$-modules cohérents.*

Annexe B. La droite de Berkovich sur un anneau d'entiers de corps de nombres

Dans cette annexe, nous présentons succintement la droite de Berkovich sur un anneau d'entiers de corps de nombres. Nous invitons le lecteur dont ces prémices auront éveillé la curiosité à parcourir l'ouvrage [Poineau 2008] pour approfondir ce sujet.

Définitions. Soit K un corps de nombres. Notons A l'anneau de ses entiers. Commençons par rappeler la définition d'espace affine analytique sur A. Elle est due à Berkovich [1990, §1.5]. Soit $n \in \mathbf{N}$. L'espace affine analytique de dimension n

sur A, noté $\mathbf{A}_A^{n,\mathrm{an}}$, est l'ensemble des semi-normes multiplicatives sur $A[T_1, \dots, T_n]$, c'est-à-dire l'ensemble des applications

$$|\,.\,| : A[T_1, \dots, T_n] \to \mathbf{R}_+$$

qui vérifient les propriétés suivantes :

(i) $|0| = 0$ et $|1| = 1$;

(ii) $\forall P, Q \in A[T_1, \dots, T_n],\ |P + Q| \leq |P| + |Q|$;

(iii) $\forall P, Q \in A[T_1, \dots, T_n],\ |PQ| = |P|\,|Q|$.

Remarque B.1. Dans la définition proposée par Berkovich figure une condition supplémentaire qui fait intervenir une norme sur l'anneau A. Pour $a \in A$, posons

$$\|a\| = \max_{\sigma \in \Sigma_\infty} (|\sigma(a)|_\infty),$$

où Σ_∞ désigne l'ensemble des plongements complexes du corps K et $|\,.\,|_\infty$ la valeur absolue usuelle sur $\mathbf{C}$. La fonction $\|.\| : A \to \mathbf{R}_+$ définit une norme sur A et, lorsque l'on munit l'anneau A de cette norme, la définition de Berkovich coïncide avec la nôtre. Signalons que, quelle que soit la norme dont on munit A (sous réserve tout de même qu'elle soit sous-multiplicative et fasse de A un espace complet), on obtient un espace contenu dans celui que nous avons défini.

Soit x un point de $\mathbf{A}_A^{n,\mathrm{an}}$. Il lui est associé une semi-norme multiplicative $|\,.\,|_x$ sur $A[T_1, \dots, T_n]$. L'ensemble $\mathfrak{p}_x$ des éléments sur lesquels elle s'annule est un idéal premier de $A[T_1, \dots, T_n]$. Le quotient est un anneau intègre sur lequel la semi-norme $|\,.\,|_x$ induit une valeur absolue. Nous noterons $\mathscr{H}(x)$ le complété du corps des fractions de cet anneau pour cette valeur absolue. Nous noterons simplement $|\,.\,|$ la valeur absolue sur le corps $\mathscr{H}(x)$, cela n'entraînant pas de confusion. La construction fournit un morphisme

$$A[T_1, \dots, T_n] \to \mathscr{H}(x).$$

L'image d'un élément P de $A[T_1, \dots, T_n]$ par ce morphisme sera notée $P(x)$. Avec ces notations, nous avons donc $|P(x)| = |P|_x$.

Munissons, à présent, l'espace analytique $\mathbf{A}_A^{n,\mathrm{an}}$ d'une topologie : celle engendrée par les ensembles de la forme

$$\{x \in \mathbf{A}_A^{n,\mathrm{an}} \mid r < |P(x)| < s\},$$

pour $P \in A[T_1, \dots, T_n]$ et $r, s \in \mathbf{R}$.

Pour finir, nous définissons un faisceau d'anneaux $\mathscr{O}$ sur $\mathbf{A}_A^{n,\mathrm{an}}$ de la façon suivante : pour tout ouvert U de $\mathbf{A}_A^{n,\mathrm{an}}$, l'anneau $\mathscr{O}(U)$ est constitué des applications

$$f : U \to \bigsqcup_{x \in U} \mathscr{H}(x)$$

qui vérifient les deux conditions suivantes :

(i) $\forall x \in U,\ f(x) \in \mathscr{H}(x)$;

(ii) f est localement limite uniforme de fractions rationnelles sans pôles.

***Dimension* 0.** Afin de rendre plus palpables les définitions précédentes, nous allons décrire explicitement $\mathbf{A}_A^{0,\mathrm{an}}$, l'espace affine analytique de dimension 0 sur A, que nous noterons plus volontiers $\mathscr{M}(A)$. Nous noterons $|\,.\,|_\infty$ la valeur absolue usuelle sur $\mathbf{C}$ et, pour tout idéal maximal $\mathfrak{m}$ de A, nous noterons $|\,.\,|_\mathfrak{m}$ la valeur absolue $\mathfrak{m}$-adique normalisée. Du théorème d'Ostrowski, l'on déduit que les points de $\mathscr{M}(A)$ sont exactement

(i) la valeur absolue triviale $|\,.\,|_0$ (nous noterons a_0 le point associé) ;

(ii) la valeur absolue archimédienne $|\sigma(\,.\,)|_\infty^\varepsilon$ (nous noterons a_σ^ε le point associé) pour tout toute classe de conjugaison de plongements complexes σ de K et tout élément ε de $]0, 1]$;

(iii) la valeur absolue $\mathfrak{m}$-adique $|\,.\,|_\mathfrak{m}^\varepsilon$ (nous noterons $a_\mathfrak{m}^\varepsilon$ le point associé) pour tout idéal maximal $\mathfrak{m}$ de A et tout élément ε de $]0, +\infty[$;

(iv) la semi-norme $|\,.\,|_\mathfrak{m}^{+\infty}$ (nous noterons $\tilde{a}_\mathfrak{m}$ le point associé) induite par la valeur absolue triviale sur le corps fini $A/\mathfrak{m}$ pour tout idéal maximal $\mathfrak{m}$ de A.

Nous pouvons également décrire la topologie de l'espace $\mathscr{M}(A)$ (*cf.* figure 2, tracée dans le cas où $K = \mathbf{Q}$ pour simplifier les notations, mais aisément généralisable). Pour cela, il suffit d'indiquer que chacune des branches tracée sur la figure est homéomorphe à un segment réel et qu'un voisinage du point central a_0 est une

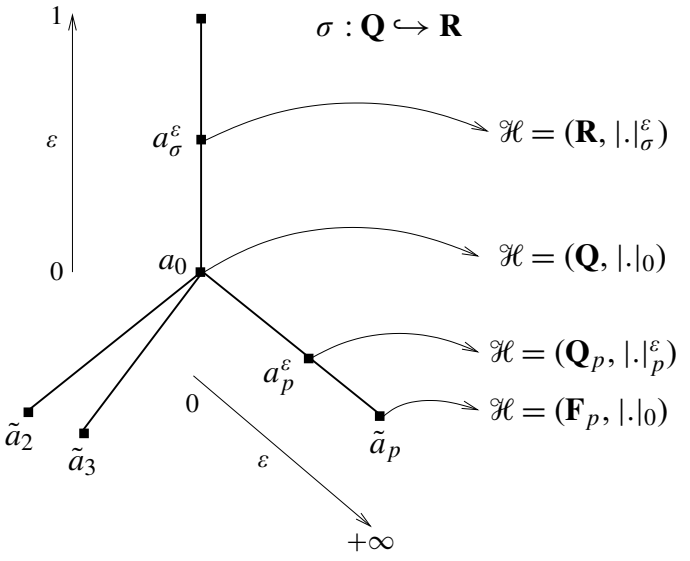


FIGURE 2. L'espace $\mathscr{M}(\mathbf{Z})$.

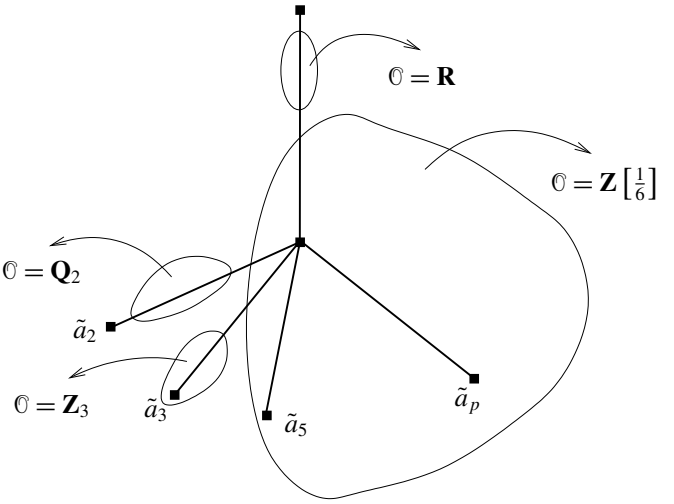


FIGURE 3. Le faisceau structural sur $\mathcal{M}(\mathbf{Z})$.

partie qui contient entièrement toutes les branches à l'exception d'un nombre fini, et qui contient un voisinage de a_0 dans chacune des branches restantes. Si l'on préfère, l'espace $\mathcal{M}(A)$ possède la topologie du compactifié d'Alexandrov de la réunion disjointe de ses branches privées de a_0, le point a_0 jouant le rôle du point à l'infini.

Nous pouvons également décrire explicitement les sections du faisceau structural sur les ouverts de $\mathcal{M}(A)$. Nous avons représenté les différents cas à la figure 3, de nouveau dans le cas où $K = \mathbf{Q}$.

***Dimension* 1.** Venons-en, à présent, à l'espace affine analytique de dimension 1 sur A. Nous noterons T la coordonnée sur cet espace. Remarquons, tout d'abord, que le morphisme $A \to A[T]$ induit un morphisme de projection

$$\pi : \mathbf{A}_A^{1,\mathrm{an}} \to \mathcal{M}(A).$$

Cela permet d'obtenir une description topologique de la droite de Berkovich sur A : la fibre de π au-dessus d'un point x de $\mathcal{M}(A)$ est isomorphe à la droite de Berkovich sur le corps $\mathcal{H}(x)$. Si $\mathcal{H}(x) = \mathbf{C}$, cette droite est isomorphe à l'espace $\mathbf{C}$ et, si $\mathcal{H}(x) = \mathbf{R}$, elle est isomorphe à son quotient par la conjugaison complexe. Nous ne chercherons pas à obtenir de description plus précise et nous contenterons d'indiquer quelques propriétés [Poineau 2008, théorèmes 4.4.1 et 4.5.5].

Théorème B.2. (i) *L'espace* $\mathbf{A}_A^{1,\mathrm{an}}$ *est localement compact, métrisable et de dimension topologique* 3.

(ii) *L'espace* $\mathbf{A}_A^{1,\mathrm{an}}$ *est localement connexe par arcs.*

(iii) *Le morphisme de projection* $\pi : \mathbf{A}_A^{1,\mathrm{an}} \to \mathcal{M}(A)$ *est ouvert.*

(iv) *En tout point x de $\mathbf{A}_A^{1,\mathrm{an}}$, l'anneau local $\mathcal{O}_x$ est hensélien, noethérien, régulier, de dimension inférieure à 2 et le corps résiduel $\kappa(x)$ est hensélien.*

(v) *Le faisceau structural $\mathcal{O}$ est cohérent.*

Signalons encore que la droite de Berkovich sur A satisfait au principe du prolongement analytique (*ibid.*, théorèmes 4.4.2 et 7.1.9, corollaire 4.4.5).

Théorème B.3. *Soit U une partie connexe de $\mathbf{A}_A^{1,\mathrm{an}}$.*

(i) *Le principe du prolongement analytique vaut sur U. En particulier, l'anneau $\mathcal{O}(U)$ est intègre.*

(ii) *L'anneau des sections méromorphes $\mathcal{M}(U)$ est un corps.*

(iii) *Si U est de Stein, le morphisme naturel* $\mathrm{Frac}(\mathcal{O}(U)) \to \mathcal{M}(U)$ *est un isomorphisme.*

Rappelons ici ce que nous entendons par espace de Stein. Nous dirons qu'un espace localement annelé $(X, \mathcal{O}_X)$ est de Stein s'il satisfait les conclusions des théorèmes A et B de H. Cartan :

(A) pour tout faisceau de $\mathcal{O}_X$-modules cohérent $\mathcal{F}$ et tout point x de X, la fibre $\mathcal{F}_x$ est engendrée par l'ensemble des sections globales $\mathcal{F}(X)$;

(B) pour tout faisceau de $\mathcal{O}_X$-modules cohérent $\mathcal{F}$ et tout entier $q \in \mathbf{N}^*$, nous avons $H^q(X, \mathcal{F}) = 0$.

Donnons quelques exemples de sous-espaces de la droite analytique $\mathbf{A}_{\mathbf{Z}}^{1,\mathrm{an}}$ qui sont des espaces de Stein (*ibid.*, théorème 6.6.29).

Théorème B.4. *Soient V une partie ouverte et connexe de l'espace $\mathcal{M}(A)$ et $s, t \in \mathbf{R}$. Soit $P(T)$ un polynôme unitaire à coefficients dans $\mathcal{O}(V)$. Les parties suivantes de la droite analytique $\mathbf{A}_A^{1,\mathrm{an}}$ sont des espaces de Stein :*

(i) $\big\{x \in \pi^{-1}(V) \,\big|\, s < |P(T)(x)| < t\big\}$;

(ii) $\big\{x \in \pi^{-1}(V) \,\big|\, |P(T)(x)| > s\big\}$.

Pour terminer, disons quelques mots des sections globales sur les parties de la droite analytique $\mathbf{A}_A^{1,\mathrm{an}}$. Sur les disques, elles s'expriment essentiellement en termes de séries dont les coefficients sont des fonctions sur $\mathcal{M}(A)$. Considérons, par exemple, le disque ouvert relatif de rayon 1 :

$$\mathbf{D} = \big\{x \in \mathbf{A}_A^{1,\mathrm{an}} \,\big|\, |T(x)| < 1\big\}.$$

Le morphisme naturel $A[T] \to \mathcal{O}(\mathbf{D})$ induit un isomorphisme

$$A_{1^-}[\![T]\!] \xrightarrow{\sim} \mathcal{O}(\mathbf{D}),$$

où $A_1\text{-}[\![T]\!]$ désigne l'anneau constitué des séries de la forme

$$\sum_{n\geq 0} a_n\, T^n \in A[\![T]\!]$$

telles que le rayon de convergence de la série à coefficients complexes

$$\sum_{n\geq 0} \sigma(a_n)\, T^n$$

soit supérieur ou égal à 1, pour tout plongement complexe σ de K. On déduit cette description du théorème 3.2.16 de *ibid.*

À partir de la description des anneaux de sections sur les disques, nous pouvons déduire celle des anneaux locaux en certains points. Nous nous contenterons de deux exemples. Soit $\mathfrak{m}$ un idéal maximal de A. Notons $z_{\mathfrak{m}}$ le point 0 de la fibre de π au-dessus du point $\tilde{a}_{\mathfrak{m}}$. D'après le corollaire 3.2.5 de *ibid.*, le morphisme naturel $A[T] \to \mathscr{O}_{z_p}$ induit un isomorphisme

$$\hat{A}_{\mathfrak{m}}[\![T]\!] \xrightarrow{\sim} \mathscr{O}_{z_p}.$$

Notons z_0 le point 0 de la fibre de π au-dessus du point a_0. D'après le corollaire 3.2.8 de *ibid.*, le morphisme naturel $A[T] \to \mathscr{O}_{z_0}$ induit un isomorphisme

$$E \xrightarrow{\sim} \mathscr{O}_{z_0},$$

où E désigne l'anneau constitué des éléments f de $K[\![T]\!]$ qui vérifient les propriétés suivantes :

(i) $\exists a \in A \setminus \{0\},\ f(aT) \in A[\![T]\!]$;

(ii) pour tout plongement complexe σ de K, le rayon de convergence complexe de la série $\sigma(f)$ est strictement positif ;

(iii) pour tout idéal maximal $\mathfrak{m}$ de A, le rayon de convergence $\mathfrak{m}$-adique de la série f est strictement positif (il suffit d'imposer cette condition pour les idéaux maximaux qui contiennent un élément a possédant les propriétés décrites en (i).

Remerciements

La dernière partie de cet article a été rédigée au cours de l'année que j'ai passée à l'université de Ratisbonne. Je souhaite remercier Klaus Künnemann, qui m'a permis d'y séjourner, pour son accueil et ses encouragements. Ma gratitude va également à Antoine Chambert-Loir dont les conseils concernant la structure de cet texte m'ont permis, je l'espère, d'en accroître l'intérêt et la clarté. Merci également à Antoine Ducros de m'avoir communiqué ses notes sur les théorèmes GAGA.

Bibliographie

[Berkovich 1990] V. G. Berkovich, *Spectral theory and analytic geometry over non-Archimedean fields*, Mathematical Surveys and Monographs **33**, American Mathematical Society, Providence, RI, 1990. MR 91k :32038 Zbl 0715.14013

[Berkovich 1993] V. G. Berkovich, "Étale cohomology for non-Archimedean analytic spaces", *Inst. Hautes Études Sci. Publ. Math.* 78 (1993), 5–161 (1994). MR 95c :14017 Zbl 0804.32019

[Berkovich 1996] V. G. Berkovich, "Vanishing cycles for non-Archimedean analytic spaces", *J. Amer. Math. Soc.* **9** :4 (1996), 1187–1209. MR 97e :32037 Zbl 0988.14004

[Cartan 1951] H. Cartan, "Faisceaux analytiques sur les variétés de Stein : démonstration des théorèmes fondamentaux", dans *Séminaire Henri Cartan* 1951/52 (Exposé 19), vol. 4, 1951. Republié en 1955 par le département de mathématiques de MIT.

[Ducros 2009] A. Ducros, "Les espaces de Berkovich sont excellents", *Ann. Inst. Fourier* (*Grenoble*) **59** :4 (2009), 1443–1552.

[EGA II 1961] A. Grothendieck, "Éléments de géométrie algébrique, II : Étude globale élémentaire de quelques classes de morphismes", *Inst. Hautes Études Sci. Publ. Math.* **8** (1961).

[Fried et Jarden 2008] M. D. Fried et M. Jarden, *Field arithmetic*, 3rd éd., Ergebnisse der Mathematik (3) **11**, Springer, Berlin, 2008. MR 2009j :12007 Zbl 1145.12001

[Hakim 1972] M. Hakim, *Topos annelés et schémas relatifs*, Ergebnisse der Math. **64**, Springer, Berlin, 1972. MR 51 #500 Zbl 0246.14004

[Harbater 1984a] D. Harbater, "Convergent arithmetic power series", *Amer. J. Math.* **106** :4 (1984), 801–846. MR 85j :13036 Zbl 0577.13017

[Harbater 1984b] D. Harbater, "Mock covers and Galois extensions", *J. Algebra* **91** :2 (1984), 281–293. MR 86c :13004 Zbl 0559.14021

[Harbater 1984c] D. Harbater, "Algebraic rings of arithmetic power series", *J. Algebra* **91** :2 (1984), 294–319. MR 86i :13007 Zbl 0578.13013

[Harbater 1987] D. Harbater, "Galois coverings of the arithmetic line", pp. 165–195 dans *Number theory* (New York, 1984–1985), édité par D. V. Chudnovsky et al., Lecture Notes in Math. **1240**, Springer, Berlin, 1987. MR 88h :14020 Zbl 0627.12015

[Harbater 1988] D. Harbater, "Galois covers of an arithmetic surface", *Amer. J. Math.* **110** :5 (1988), 849–885. MR 90e :14013 Zbl 0683.14004

[Harbater 2003] D. Harbater, "Patching and Galois theory", pp. 313–424 dans *Galois groups and fundamental groups*, édité par L. Schneps, Math. Sci. Res. Inst. Publ. **41**, Cambridge Univ. Press, 2003. MR 2004j :14030 Zbl 1071.14029

[Kiehl 1967] R. Kiehl, "Der Endlichkeitssatz für eigentliche Abbildungen in der nichtarchimedischen Funktionentheorie", *Invent. Math.* **2** (1967), 191–214. MR 35 #1833 Zbl 0202.20101

[Köpf 1974] U. Köpf, "Über eigentliche Familien algebraischer Varietäten über affinoiden Räumen", *Schr. Math. Inst. Univ. Münster* (2) Heft 7 (1974), iv+72. MR 54 #10657 Zbl 0275.14006

[Liu 1995] Q. Liu, "Tout groupe fini est un groupe de Galois sur $\mathbf{Q}_p(T)$, d'après Harbater", pp. 261–265 dans *Recent developments in the inverse Galois problem* (Seattle, 1993), édité par M. D. Fried et al., Contemp. Math. **186**, Amer. Math. Soc., Providence, RI, 1995. MR 96h :12006 Zbl 0834.12004

[Moret-Bailly 2001] L. Moret-Bailly, "Construction de revêtements de courbes pointées", *J. Algebra* **240** :2 (2001), 505–534. MR 2003a :14042 Zbl 1047.14013

[Poineau 2008] J. Poineau, "La droite de Berkovich sur **Z**", preprint, 2008. À paraître dans *Astérisque* (2010). arXiv 0809.2880

[Pop 1996] F. Pop, "Embedding problems over large fields", *Ann. of Math.* (2) **144** :1 (1996), 1–34. MR 97h :12013 Zbl 0862.12003

[Saltman 1982] D. J. Saltman, "Generic Galois extensions and problems in field theory", *Adv. in Math.* **43** :3 (1982), 250–283. MR 84a :13007 Zbl 0484.12004

[Serre 1955–1956] J.-P. Serre, "Géométrie algébrique et géométrie analytique", *Ann. Inst. Fourier, Grenoble* **6** (1955–1956), 1–42. MR 18,511a Zbl 0075.30401

[SGA1 1971] A. Grothendieck (éditeur), *Revêtements étales et groupe fondamental*, Lecture Notes in Mathematics **224**, Springer, Berlin, 1971. MR 50 #7129

Communicated by Jean-Louis Colliot-Thélène
Received 2009-05-29 Revised 2009-08-31 Accepted 2009-09-30

jerome.poineau@math.unistra.fr *Institut de recherche mathématique avancée, 7, rue René Descartes, 67084 Strasbourg, France*
http://www-irma.u-strasbg.fr/~poineau/

ALGEBRA AND NUMBER THEORY 4:3(2010)

K3 surfaces with Picard rank 20

Matthias Schütt

We determine all complex K3 surfaces with Picard rank 20 over $\mathbb{Q}$. Here the Néron–Severi group has rank 20 and is generated by divisors which are defined over $\mathbb{Q}$. Our proof uses modularity, the Artin–Tate conjecture and class group theory. With different techniques, the result has been established by Elkies to show that Mordell–Weil rank 18 over $\mathbb{Q}$ is impossible for an elliptic K3 surface. We apply our methods to general singular K3 surfaces, that is, those with Néron–Severi group of rank 20, but not necessarily generated by divisors over $\mathbb{Q}$.

1. Introduction

Complex K3 surfaces of geometric Picard number 20 are called *singular* since they involve no moduli. They share many properties with elliptic curves with complex multiplication (CM). For instance, they can always be defined over some number field. Moreover, over some finite extension of the number field, the L-series is given in terms of Hecke characters (see Theorem 29).

For singular K3 surfaces over $\mathbb{Q}$, Livné [1995] proved motivic modularity. However, this definition does not require that the Néron–Severi group be generated by divisors which are defined over $\mathbb{Q}$. We refer to this particular property as "Picard rank 20 over $\mathbb{Q}$".

The motivation to study such K3 surfaces was the following: Shioda [1994] raised the question whether it was possible for an elliptic K3 surface to have Mordell–Weil rank 18 over $\mathbb{Q}$. One way to disprove this would have been to show that in general, K3 surfaces with Picard rank 20 over $\mathbb{Q}$ do not exist.

However, it turned out that there are such examples (see Examples 8, 9). Recently Elkies determined all these surfaces in terms of their transcendental lattices:

Theorem 1 [Elkies 2007]. *Let X be a K3 surface with Picard rank* 20 *over* $\mathbb{Q}$. *Then the transcendental lattice $T(X)$ is primitive of class number one.*

MSC2000: primary 14J28; secondary 11F11, 11G15, 11G25, 11R29.

Keywords: singular K3 surface, Artin–Tate conjecture, complex multiplication, modular form, class group.

Using sphere packings and gluing up to a Niemeier lattice, Elkies concluded that Mordell–Weil rank 18 over $\mathbb{Q}$ is impossible for an elliptic K3 surface.

Conversely, let $T(X)$ be primitive of class number one. Then the singular K3 surface X with transcendental lattice $T(X)$ has a model with Picard rank 20 over $\mathbb{Q}$ (see Section 10).

In this paper, we present an alternative proof of Theorem 1 that we hope will be of independent interest. Our proof uses the following ingredients: modularity plus the classification of CM-forms in [Schütt 2009]; reduction and the Artin–Tate conjecture at split primes; and class group theory.

We then generalise our techniques to all singular K3 surfaces. We deduce the following obstruction to the field of definition:

Theorem 2. *Let L be a number field and X a K3 surface of Picard rank 20 over L. Denote the discriminant of X by $d < 0$. Then $L(\sqrt{d})$ contains the ring class field $H(d)$.*

This result enables us to give a direct proof of Shafarevich's finiteness theorem for singular K3 surfaces (Theorem 35). It is the only known obstruction for the field of definition of a singular K3 surface other than the result on the genus of $T(X)$ in [Schütt 2007b] (see (1) on next page and Lemma 34). In private correspondence, Elkies has informed me that his proof for Theorem 1 also generalises to Theorem 2.

The paper is organised as follows: The next two sections recall the relevant facts about singular K3 surfaces and modularity. In Section 4 we give two explicit examples of K3 surfaces of Picard rank 20 over $\mathbb{Q}$. Section 5 introduces the main techniques to be used, particularly the Artin–Tate conjecture. The proof of Theorem 1 is presented in Sections 6 through 9. The converse statement of Theorem 1 is covered in Section 10. We continue with the classification of K3 surfaces of Picard rank 20 over $\mathbb{Q}$ up to $\mathbb{Q}$-isomorphism. Section 12 generalises Theorem 1 to K3 surfaces with Picard rank 20 over a quadratic extension of $\mathbb{Q}$. The paper concludes with the proof of the general case of Theorem 2.

2. Singular K3 surfaces

The main invariant of a singular K3 surface X is its *transcendental lattice* $T(X)$. Here we consider the Néron–Severi group $\mathrm{NS}(X)$ of divisors up to algebraic equivalence as a lattice in $H^2(X, \mathbb{Z})$ with cup-product. Then the transcendental lattice is the orthogonal complement

$$T(X) = \mathrm{NS}(X)^{\perp} \subset H^2(X, \mathbb{Z}).$$

The following classification was first stated by Pjateckiĭ–Šapiro and Shafarevich [1971]. The proof was completed by Shioda and Inose [1977]:

Theorem 3 [Piatetskiĭ-Shapiro and Shafarevich 1971; Shioda and Inose 1977]. *The map $X \mapsto T(X)$ gives a bijection*

$$\{\textit{Singular K3 surfaces}\}_{/\cong} \overset{1:1}{\longleftrightarrow} \begin{Bmatrix}\textit{positive-definite oriented}\\ \textit{even lattices of rank two}\end{Bmatrix}_{/\cong}.$$

The injectivity of this map follows from the Torelli theorem for singular K3 surfaces [Piatetskiĭ-Shapiro and Shafarevich 1971]. For the surjectivity, Shioda and Inose [1977] exhibited an explicit construction involving isogenous CM-elliptic curves E, E'. This is often referred to as Shioda–Inose structure:

$$\begin{array}{ccc} E \times E' & & X \\ & \searrow \quad \swarrow & \\ & \mathrm{Km}(E \times E') & \end{array}$$

Here both rational maps are 2:1, and $T(X) \cong T(E \times E')$. Shioda and Inose exhibited the rational map $X \dashrightarrow \mathrm{Km}(E \times E')$ through base change of elliptic fibrations. Explicit equations were subsequently given by Inose [1978]. In [Schütt 2007b], Inose's results were improved to derive a model over the ring class field $H(d)$ associated to the discriminant $d = \mathrm{disc}(T(X))$ of the transcendental lattice (Lemma 33). Over some extension, one can moreover determine the ζ-function of X (Theorem 29).

The set of singular K3 surfaces over $\mathbb{Q}$ (up to $\mathbb{C}$-isomorphism) is finite by a result of Shafarevich [1996], quoted in Theorem 35. However, there is only one effective obstruction known for a singular K3 surface X to be defined over $\mathbb{Q}$: By [Schütt 2007b], the genus of $T(X)$ has to consist of a single class. (Shimada [2009] proved this first for the case of the fundamental discriminant d.) In other words, we require that its class group be only two-torsion:

$$\mathrm{Cl}(T(X)) \cong (\mathbb{Z}/2)^g. \tag{1}$$

The general case will be treated in Section 13. There we will also provide a formulation in terms of fields of definition (Lemma 34).

The only drawback of relation (1) is that the class group $\mathrm{Cl}(T(X))$ does not recognise whether $T(X)$ is primitive. We know 101 discriminants $d < 0$ such that the class group $\mathrm{Cl}(d)$ is only two-torsion. By a result of Weinberger [1973] there is at most one more such d, and in fact none under some condition on Siegel–Landau zeroes (which would follow from GRH). However, so far we lacked bounds for the degree of primitivity of $T(X)$. For Picard rank 20 over $\mathbb{Q}$, primitivity is part of Theorem 1. For the general case, bounds for the degree of primitivity follow from Theorem 2 (see Section 13).

3. Modularity of singular K3 surfaces over $\mathbb{Q}$

We shall now see that condition (1) can also be understood in terms of modularity. Here the modular motive is the compatible system of Galois representations attached to the transcendental lattice. Over some extension, this motive is related to Hecke characters by Theorem 29.

Throughout the paper, we fix the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ where $d < 0$ is the discriminant of X. Write d_K for the discriminant of K. Hence $d = N^2 d_K$.

Theorem 4 [Livné 1995]. *Every singular K3 surface X over $\mathbb{Q}$ is modular. The L-series of the transcendental lattice $T(X)$ is the Mellin transform of a Hecke eigenform of weight 3 with CM by K.*

By a result of Ribet [1977], CM-newforms are associated to Hecke characters. Essentially, a Hecke character ψ of K is given by its conductor $\mathfrak{m}$, an ideal in the ring of integers $\mathbb{O}_K$, and by its ∞-type l. Then ψ satisfies

$$\psi(\alpha\mathbb{O}_K) = \alpha^l \quad \text{for all } \alpha \equiv 1 \bmod \mathfrak{m}.$$

Let $\mathrm{N}_{K/\mathbb{Q}}$ denote the norm of $K/\mathbb{Q}$. The sum over all ideals $\mathfrak{a}$ of $\mathbb{O}_K$ that are relatively prime to $\mathfrak{m}$ gives the L-function of ψ:

$$L(\psi, s) = \sum_{\mathfrak{a}} \psi(\mathfrak{a})\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})^s.$$

Through the inverse Mellin transform, $L(\psi, s)$ defines a newform of weight $k = l+1$ and level $|\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{m})d_K|$. For the weight of the corresponding newform to be 3, the Hecke character thus has to have ∞-type 2. Moreover, we require the newform to have Fourier coefficients in $\mathbb{Z}$. This is possible if and only if the class group of K consists only of two-torsion (see Theorem 6). This condition is necessarily satisfied if (1) holds.

Example 5. Let K be such that $\mathrm{Cl}(K) \cong (\mathbb{Z}/2)^g$ with $d_K \neq -3, -4$. Then we can define a Hecke character ψ of K with trivial conductor and ∞-type 2 by setting

$$\psi(\alpha\mathbb{O}_K) = \alpha^2$$

for every principal ideal in $\mathbb{O}_K$ and choosing suitable values for a set of generators of $\mathrm{Cl}(K)$. Explicitly, throughout this paper let

$$D = \begin{cases} -d_K, & \text{if } 4 \nmid d_K, \\ -d_K/4, & \text{if } 4 \mid d_K. \end{cases}$$

Assume that $p = \mathfrak{p}\bar{\mathfrak{p}}$ splits in K. Since $d_K \neq -3, -4$, we can write p^2 uniquely as

$$p^2 = x^2 + Dy^2, \quad x, y \in \tfrac{1}{2}\mathbb{N}.$$

(Here $x, y \in \mathbb{N}$ unless $D = -d_K$.) Then $\psi(\mathfrak{p}) = \pm(x \pm \sqrt{-D}y)$. For the corresponding newform $f = \sum a_n q^n$, we obtain

$$a_p = \pm 2x.$$

Once a normalisation is fixed, f has level $|d_K|$ and Fourier coefficients in $\mathbb{Z}$.

The newforms arising from different normalisations (that is, sign choices) are quadratic twists of each other. In general, consider a (quadratic) Dirichlet character χ and a newform $f = \sum a_n q^n$. Then we obtain the twisted Hecke eigenform

$$f \otimes \chi = \sum_n a_n \chi(n) q^n. \tag{2}$$

The classification in [Schütt 2009] says that the construction of Example 5 produces all Hecke characters and Hecke eigenforms with Fourier coefficients in $\mathbb{Z}$ after twisting:

Theorem 6 [Schütt 2009]. *Let K be an imaginary quadratic field. Then all Hecke characters of K with fixed ∞-type l such that the corresponding newform f has coefficients in $\mathbb{Z}$, are identified under twisting. Moreover, there is such a Hecke character if and only if* $\mathrm{Cl}(K) \subseteq (\mathbb{Z}/l)^g$ *for some* $g \in \mathbb{N}$.

Remark 7. If $d_K \neq -3, -4$, then we only have to consider quadratic twists. If χ is a quadratic Dirichlet character, then we twist the Hecke character by $\chi \circ \mathrm{N}_{\mathbb{Q}}^K$. In terms of the associated newform f, this corresponds to the quadratic twist in (2). For $d_K = -3, -4$, we also have to take cubic and biquadratic twisting into account. All these twists have geometric equivalents. For instance, any quadratic Dirichlet character can be identified with a Legendre symbol $\left(\frac{\delta}{\cdot}\right)$ for some square-free $\delta \in \mathbb{Z}$. Then consider an elliptic curve (or a general equation of this type)

$$E : y^2 = g(x) \quad \text{and twist} \quad E_\delta : \delta y^2 = g(x). \tag{3}$$

For geometric equivalents of cubic and biquadratic twists, see Remark 27.

4. K3 surfaces of Picard rank 20 over $\mathbb{Q}$: Examples

In this section, we recall two of the most elementary examples of K3 surfaces of Picard rank 20 over $\mathbb{Q}$. Both use elliptic fibrations with section. For further examples, the reader is referred to Section 10.

Example 8. There is a unique complex elliptic K3 surface X with a fibre of type I_{19}. The fibration can be defined over $\mathbb{Q}$. This follows from work of Hall [1971] and was studied in detail by Shioda [2003]. A simple explicit Weierstrass equation is derived in [Schütt and Schweizer 2007]:

$$X : \quad y^2 = x^3 + (t^4 + t^3 + 3t^2 + 1)\, x^2 + 2(t^3 + t^2 + 2t)\, x + t^2 + t + 1. \tag{4}$$

Let U denote the hyperbolic plane generated by a general fibre and the zero-section. It is immediate that the Néron–Severi lattice of X (over $\overline{\mathbb{Q}}$) can be written as

$$\mathrm{NS}(X) = U \oplus A_{18}(-1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \oplus A_{18}(-1).$$

In particular, X is a singular K3 surface. The Picard rank of X over $\mathbb{Q}$ is 20 if and only if the all components of the special fibre are defined over $\mathbb{Q}$ (that is, if the special fibre has split multiplicative reduction). This can be achieved by an appropriate twist as in (3), and was first exhibited in [Schütt and Top 2006]. The model in (4) has the fibre of type I_{19} at $t = \infty$. The fibre is split multiplicative, so the Picard rank of the surface over $\mathbb{Q}$ is already 20. The corresponding Hecke eigenform has level 19 by [Schütt and Top 2006] (see [Schütt 2009, Table 1]).

The next example goes back to [Tate 1974]. It has been studied very concretely in [Hulek and Verrill 2005].

Example 9. Let X denote the universal elliptic curve for $\Gamma_1(7)$. Since this group has genus 0, the base curve is $\mathbb{P}^1$. One the other hand, the space of cusp forms $S_3(\Gamma_1(7))$ is one-dimensional, so X has geometric genus $p_g(X) = 1$. It follows that X is a K3 surface. By general theory, the elliptic surface X has a model over $\mathbb{Q}$ with a section P of order 7 also defined over $\mathbb{Q}$. Such a model was first given by Tate [1974]:

$$X: \quad y^2 + (1 + t - t^2)xy + (t^2 - t^3)y = x^3 + (t^2 - t^3)x^2.$$

Here $P = (0, 0)$ is a point of order 7. In the following, we shall employ an abstract approach to show that X has Picard rank 20 over $\mathbb{Q}$.

The quotient of X by translation by P gives rise to another elliptic K3 surface after resolving singularities. Hence the configuration of singular fibres can only be $[1, 1, 1, 7, 7, 7]$. In particular, X is a singular K3 surface. We claim that the above model has Picard rank 20 over $\mathbb{Q}$. Equivalently, each reducible fibre is completely defined over $\mathbb{Q}$. To prove this, we show that P meets each I_7 fibre in a different nontrivial component.

We employ Shioda's theory [1990] of Mordell–Weil lattices and the height pairing. As a torsion section, P has height 0. Since P does not meet the 0-section, we can compute the height directly as

$$h(P) = 4 - (\text{correction terms for reducible fibres}).$$

Here the correction terms are $(n(7-n))/7$ according to the component Θ_n which P meets (cyclically numbered so that the zero-section meets Θ_0). The only way to obtain $h(P) = 0$ is

$$0 = h(P) = 4 - \tfrac{6}{7} - \tfrac{10}{7} - \tfrac{12}{7}.$$

Since P intersects each I_7 fibre at a nontrivial component, these special fibres are split multiplicative. Moreover, as the components differ for each I_7 fibre, their cusps cannot be conjugate. Hence all fibre components are defined over $\mathbb{Q}$, and the claim follows.

Remark 10. The same argument applies to other modular elliptic K3 surfaces, but not to all of them. For instance, the universal elliptic curve for $\Gamma(4)$ is a Kummer surface. Hence it cannot have Picard rank 20 over $\mathbb{Q}$ by the next remark. This argument will also be used in the proof of the primitivity of the transcendental lattice (Lemma 22). Alternatively, we could also argue with the Weil pairing. Since the Weil pairing has image μ_4, the fourth roots of unity, we deduce that $MW(X/\mathbb{Q}) \subset \mathbb{Z}/4 \times \mathbb{Z}/2$. Then we apply the inverse argument of Example 9 to a 4-torsion section which is not defined over $\mathbb{Q}$. This implies that there are singular fibres which are not completely defined over $\mathbb{Q}$.

Remark 11 (Singular abelian surfaces). The situation for abelian surfaces is different: Let A be a singular complex abelian surface, that is, $\rho(A) = 4$. Then $A \cong E \times E'$ for isogenous CM-elliptic curves E, E' by a result of Shioda and Mitani [1974]. However, as Shioda [2005] noted, Picard rank 4 over $\mathbb{Q}$ is impossible. This is a consequence of the cohomology structure of abelian varieties and carries over to Kummer surfaces (see also Remark 10 and Lemma 22).

5. The Artin–Tate conjecture

Let X be a K3 surface of Picard rank 20 over $\mathbb{Q}$. In order to prove Theorem 1, we will consider the reductions of X at the good primes p that split in K and apply the Artin–Tate conjecture.

Let p be a prime of good reduction of X. Then the reduction morphism induces embeddings

$$\mathrm{NS}(X/\mathbb{Q}) \hookrightarrow \mathrm{NS}(X/\mathbb{F}_p) \quad \text{and} \quad \mathrm{NS}(X/\overline{\mathbb{Q}}) \hookrightarrow \mathrm{NS}(X/\overline{\mathbb{F}}_p), \tag{5}$$

which are isometries onto the image. For almost all p, these embeddings are primitive. This follows from Shimada's argumentation [2009, §2.2], since the proof for the case of supersingular reduction can be generalised directly. For the remainder of the paper, we will only consider *good primes* where the reduction is good and the embeddings in (5) are primitive.

On $X/\mathbb{F}_p$ we have the Frobenius endomorphism Frob_p raising coordinates to their pth powers. We want to consider the induced action on cohomology. For this, we fix a prime $\ell \neq p$ and work with étale ℓ-adic cohomology of the base change $\bar{X} = X_{\overline{\mathbb{F}}_p}$ to an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. Then we consider the induced

map Frob_p^* on $H^2_{\text{ét}}(\bar{X}, \mathbb{Q}_\ell)$ and its reciprocal characteristic polynomial

$$P(X/\mathbb{F}_p, T) = \det(1 - \mathrm{Frob}_p^*\, T;\, H^2_{\text{ét}}(\bar{X}, \mathbb{Q}_\ell)).$$

Frob_p^* acts through a permutation on the algebraic cycles in $H^2_{\text{ét}}(\bar{X}, \mathbb{Q}_\ell)$. More precisely, it operates as multiplication by p on $\mathrm{NS}(X/\mathbb{F}_p)$ and in particular on the image of $\mathrm{NS}(X/\mathbb{Q})$ under the primitive embedding (5). In the present case, X has Picard rank 20 over $\mathbb{Q}$ and discriminant d. Let $f = \sum a_n q^n$ denote the associated newform by Theorem 4. Then

$$P(X/\mathbb{F}_p, T) = (1 - p\,T)^{20}\Big(1 - a_p\,T + \Big(\frac{d}{p}\Big)p^2\,T^2\Big). \tag{6}$$

The Tate conjecture [1965] relates the shape of the zeroes of $P(X/\mathbb{F}_p, T)$ to the Picard number: Conjecturally for any smooth projective surface X over $\mathbb{F}_p$, it predicts

$$\rho(X/\mathbb{F}_p) = \#\Big\{\text{zeroes } T = \frac{1}{p} \text{ of } P(X/\mathbb{F}_p, T)\Big\},$$
$$\rho(X/\bar{\mathbb{F}}_p) = \#\Big\{\text{zeroes } T = \zeta\frac{1}{p} \text{ of } P(X/\mathbb{F}_p, T) \text{ where } \zeta \text{ is a root of unity}\Big\}.$$

Here we count the zeroes with multiplicities. Since Frob_p acts as multiplication by p on $NS(X/\mathbb{F}_p)$, we always have $\leq$ in the above equations. For instance, the Tate conjecture is known for elliptic K3 surfaces [Artin and Swinnerton-Dyer 1973]. By [Milne 1975] (see the addendum cited for characteristic two), it is equivalent to the Artin–Tate conjecture:

Conjecture 12 (Artin and Tate [Tate 1966]). Let $X/\mathbb{F}_p$ be a smooth projective surface. Let $\alpha(X) = \chi(X) - 1 + \dim \mathrm{Pic\ Var}(X)$. Then

$$\frac{P(X/\mathbb{F}_p, T)}{(1 - p\,T)^{\rho(X/\mathbb{F}_p)}}\Big|_{T=\frac{1}{p}} = \frac{|\mathrm{Br}(X/\mathbb{F}_p)|\ |\mathrm{discr}(\mathrm{NS}(X/\mathbb{F}_p))|}{p^{\alpha(X)}\ |\mathrm{NS}(X/\mathbb{F}_p)_{\mathrm{tor}}|^2} \tag{7}$$

Remark 13. By [Liu et al. 2005], $|\mathrm{Br}(X/\mathbb{F}_p)|$ is always a square. For K3 surfaces, $\alpha(X) = 1$ and the Néron–Severi group is torsion-free, since numerical and algebraic equivalence coincide. Hence (7) simplifies to

$$\frac{P(X/\mathbb{F}_p, T)}{(1 - p\,T)^{\rho(X/\mathbb{F}_p)}}\Big|_{T=\frac{1}{p}} = \frac{1}{p}\ |\mathrm{Br}(X/\mathbb{F}_p)|\ |\mathrm{discr}(\mathrm{NS}(X/\mathbb{F}_p))|. \tag{8}$$

We shall now specialise to the situation where X is a K3 surface with Picard rank 20 over $\mathbb{Q}$ and p is a good split prime. The Fourier coefficient a_p can be computed in terms of Example 5. In particular, it is never a multiple of p. Hence the zero $T = (1/p)$ of $P(X/\mathbb{F}_p, T)$ has multiplicity exactly 20, and there is no further zero $T = \zeta(1/p)$. It follows that $\rho(X/\mathbb{F}_p) = \rho(X/\bar{\mathbb{F}}_p) = 20$. In particular,

the Tate conjecture holds for X over $\mathbb{F}_p$. From (5) we deduce

$$\mathrm{NS}(X/\overline{\mathbb{Q}}) = \mathrm{NS}(X/\mathbb{Q}) = \mathrm{NS}(X/\mathbb{F}_p) = \mathrm{NS}(X/\overline{\mathbb{F}}_p)$$

and thus

$$\mathrm{discr}(\mathrm{NS}(X/\mathbb{Q})) = \mathrm{discr}(\mathrm{NS}(X/\mathbb{F}_p)) = d = N^2\, d_K.$$

Hence the Artin–Tate conjecture for $X/\mathbb{F}_p$ (8) gives, with $M^2 = |\mathrm{Br}(X/\mathbb{F}_p)|$,

$$2p - a_p = M^2|d| = (MN)^2|d_K|. \tag{9}$$

The proof of Theorem 1 now proceeds in three steps:

(A) The imaginary quadratic field K has class number one (Corollary 15).

(B) The discriminant d has class number one (Corollary 20).

(C) The transcendental lattice $T(X)$ is primitive (Lemma 22).

As a by-product, we will also determine the possible shapes of the associated newform f (Lemma 17).

6. Class number of K

In this section, we will prove that K has class number one. We achieve this through the following proposition:

Proposition 14. *Let p split in K and let $a_p \in \mathbb{Z}$ be the coefficient of a newform of weight* 3 *with CM by K. Then* (9) *implies that p splits into principal ideals in K.*

Proof. By Example 5, we can write $a_p = 2z$ with $z = \pm x \in \frac{1}{2}\mathbb{Z}$. By (9), we have

$$p - z = \frac{m^2 D}{2} \tag{10}$$

for some $m \in \mathbb{N}$. On the other hand, $p^2 = z^2 + Dy^2$ for some $y \in \frac{1}{2}\mathbb{N}$ by assumption, that is,

$$p^2 - z^2 = Dy^2. \tag{11}$$

Dividing (11) by (10), we obtain

$$p + z = 2\Big(\frac{y}{m}\Big)^2. \tag{12}$$

Now we add (10) and (12) and divide by two to derive

$$p = \Big(\frac{y}{m}\Big)^2 + D\Big(\frac{m}{2}\Big)^2. \tag{13}$$

Since $m/2 \in \frac{1}{2}\mathbb{N}$, the same holds for y/m. We deduce that p splits into principal ideals in K. □

Corollary 15. *Let X be a K3 surface of Picard rank 20 over $\mathbb{Q}$. Then its CM-field K has class number one.*

Proof. By the Artin–Tate conjecture, Equation (9) holds at all but finitely many p that split in K. By Proposition 14, each of these p splits into principal ideals in K. Hence K has class number one. □

7. Shape of f

If K has class number one, we can describe the CM-newforms of K even more explicitly in terms of Example 5. Here we only have to take extra care of the special cases $d_K = -3, -4$ where $\mathbb{O}_K \neq \{\pm 1\}$. For this purpose, let

$$D' = \begin{cases} 27, & \text{if } d_K = -3, \\ 4, & \text{if } d_K = -4, \\ D, & \text{if } d_K \neq -3, -4. \end{cases}$$

Example 16 (Class number one). Let K have class number one. Let D' as above. If p splits in K, then we rewrite (13) uniquely as

$$p = x^2 + D'y^2, \qquad x, y \in \tfrac{1}{2}\mathbb{N}.$$

The corresponding Hecke character ψ of ∞-type 2 sends the prime ideal $(x + \sqrt{-D'}\, y)$ to its square. We obtain the newform f_K of weight 3 and level D' from [Schütt 2009, Table 1] with coefficients

$$a_p = 2(x^2 - D'y^2). \tag{14}$$

Lemma 17. *Let X be a K3 surface of Picard rank 20 over $\mathbb{Q}$. Let f denote the associated newform.*

(i) *If $d_K \neq -3, -4$, then $f = f_K$.*

(ii) *If $d_K = -4$, then f is a quadratic twist of f_K.*

(iii) *If $d_K = -3$, then f is a cubic twist of f_K.*

Proof. Assume that $d_K \neq -3, -4$. Let p be a split prime as in Example 16. By Theorem 6, f has the coefficient

$$a_p = \pm 2(x^2 - Dy^2). \tag{15}$$

Inserting into (9) gives

$$2(x^2 + Dy^2 \mp (x^2 - Dy^2)) = m^2 D. \tag{16}$$

Since d_K is not a square and neither is D, it follows that only the minus sign in (16) is possible. That is, in (15), only the plus sign occurs. By definition $f = f_K$.

If $d_K = -4$ and $p = x^2 + 4y^2$, then

$$a_p = \begin{cases} \pm 2(x^2 - 4y^2), \\ \pm 8xy. \end{cases}$$

The second case occurs (at some split p) if and only if f is a biquadratic twist of f_K. Only the first case is compatible with (9), since in the second case

$$2p - a_p = 2(x^2 + 4y^2 \mp 4xy) = 2(x \mp 2y)^2 \neq 4n^2.$$

Hence f is a quadratic twist of f_K.

A similar argument rules out quadratic and sextic twists of f_K for $d_K = -3$: Here we can always write the coefficients of f as

$$a_p = \pm 2(x^2 - 3y^2) \quad \text{where nonuniquely} \quad p = x^2 + 3y^2, \quad x, y \in \tfrac{1}{2}\mathbb{N}.$$

By the argument of case (i), only the plus sign occurs. This implies that f is a cubic twist of f_K. □

8. Class number of d

Let X be a K3 surface of Picard rank 20 over $\mathbb{Q}$. Denote the associated newform by $f = \sum a_n q^n$. We can rephrase Lemma 17 and its proof as follows: At every good split prime p, we can write (nonuniquely if $D \neq D'$)

$$p = x_p^2 + Dy_p^2 \quad \text{such that} \quad a_p = 2(x_p^2 - Dy_p^2) \quad \text{and} \quad 4Dy_p^2 = M_p^2 |d|. \quad (17)$$

By construction, we have either $d_K = -4D$ and $y \in \mathbb{N}$ or $d_K = -D$ and $y \in \frac{1}{2}\mathbb{N}$. Recall that $d = N^2 d_K$ and d_K has class number one by Corollary 15. We want to find all d which are compatible with Picard rank 20 over $\mathbb{Q}$. In other words, we search for all $N | M_p$ which are simultaneously possible in (17) at all good split p.

Observation 18. Let gcd denote the greatest common divisor in $\mathbb{N}$ if $d_K = -4D$, or in $\frac{1}{2}\mathbb{N}$ if $d_K = -D$. Let y_p be given by (17) at a good split prime p. Then

$$N \mid \gcd(y_p;\ p \text{ good split prime for } X).$$

Hence, if for instance there was a $y_p = 1$ (or $y_p = \frac{1}{2}$ in the case $d_K = -D$) occurring, then $d = d_K$ (and $N = M_p = 1$) would follow. However, this need not be the case in general. To see this, let the associated newform f have level 27. Then by construction $3 | y_p$ for all split p. Hence at least $d = -3$ and $d = -27$ would be possible a priori.

To bound d (or N) in general, we need information on the greatest common divisor of the y_p. This divisibility problem translates into class group theory through representations of primes by quadratic forms:

Lemma 19. *Let $d < 0$ and let $Q = \left(\begin{smallmatrix} 2 & b \\ b & 2c \end{smallmatrix}\right)$ be a quadratic form of discriminant d. For $r \in \mathbb{N}$, the following are equivalent*:

(i) *For almost every prime p represented by Q, there is a representation*

$$p = u^2 + buv + cv^2, \quad u, v \in \mathbb{Z}, \tag{18}$$

such that $r \mid v$.

(ii) $h(d) = h(dr^2)$.

Proof. Note that Q always represents the principal class in $\mathrm{Cl}(d)$. Hence, if $h(d) = h(dr^2)$, the quadratic form

$$Q_r = \begin{pmatrix} 2 & br \\ br & 2cr^2 \end{pmatrix}$$

in $\mathrm{Cl}(dr^2)$ represents the same primes as Q (the principal ones). Thus $r \mid v$ for all these p.

Conversely, assume that $r \mid v$ for almost all p represented by Q. Thus all these p are represented by Q_r as well. Since the split primes are equally distributed on the classes that represent them, we obtain $h(d) \geq h(dr^2)$. On the other hand, $h(d) \leq h(r^2 d)$ holds trivially. Hence the class numbers $h(d)$ and $h(dr^2)$ have to coincide. □

Corollary 20. *Let X be a K3 surface of Picard rank 20 over $\mathbb{Q}$. Then the transcendental lattice has discriminant d of class number one.*

Proof. By Corollary 15, d_K has class number one. Assume that $d \neq d_K$, that is, there is some r dividing all y_p in (17). To apply Lemma 19, we have to relate divisibility of y_p and v_p. We consider the following quadratic forms:

$$\left(Q = \begin{smallmatrix} 2 & 0 \\ 0 & 2D \end{smallmatrix}\right) \quad \text{if } d_K \text{ is even}, \qquad Q = \begin{pmatrix} 2 & 1 \\ 1 & (D+1)/2 \end{pmatrix} \quad \text{if } d_K \text{ is odd}.$$

If d_K is even, then $d_K = -4D$ and $v_p = y_p \in \mathbb{N}$. Hence $h(d) = h(d_K) = 1$ follows from Lemma 19. If d_K is odd, then we can rewrite (18) in half-integers:

$$p = u_p^2 + u_p v_p + \frac{D+1}{4} v_p^2 = \left(u_p + \frac{v_p}{2}\right)^2 + D\left(\frac{v_p}{2}\right)^2.$$

Hence, divisibility of y_p in $\frac{1}{2}\mathbb{N}$ translates into divisibility of $v_p \in \mathbb{N}$ and vice versa. Again we deduce $h(d) = h(d_K) = 1$ by Lemma 19. □

Remark 21. Let X be a K3 surface of Picard rank 20 over $\mathbb{Q}$. If $d \neq d_K$, it is immediate from the above argument that the associated newform f has a particular shape. For $d = -28$, this newform is uniquely determined with level 7 by Lemma 17. In the other three cases ($d = -12, -16, -27$), it is easily checked that the condition $r \mid y_p$ fixes a unique Hecke character. We find that f is the unique newform of weight 3 and level $|d|$.

9. Primitivity of $T(X)$

We have seen that a K3 surface with Picard rank 20 over $\mathbb{Q}$ has discriminant of class number one. Hence there are a priori 17 possibilities for the transcendental lattice:

- the 13 primitive lattices of class number one, corresponding to isomorphism classes of CM-elliptic curves over $\mathbb{Q}$ through the Shioda–Inose structure, and
- the 4 imprimitive lattices of discriminant $d = -12, -16, -27, -28$.

In this section, we will rule out the second case.

Lemma 22. *Let X be a K3 surface of Picard rank 20 over $\mathbb{Q}$. Then $T(X)$ is primitive.*

Proof. Assume that $T(X)$ is not primitive. By Corollary 20, we are in the second case above. We shall treat even and odd discriminants separately.

If d is even in the second case above, then the transcendental lattice $T(X)$ has intersection form $2Q$ for $Q \in \mathrm{Cl}(d')$ where $4d' = d$. It follows from [Shioda and Inose 1977] that X is the Kummer surface of an abelian surface A such that the transcendental lattice $T(A)$ has intersection form Q. By Remark 11, $\rho(A/\mathbb{Q}) < 4$ and $\rho(X/\mathbb{Q}) \le \rho(A/\mathbb{Q}) + 16 < 20$.

If d is odd, that is, $d = -27$, we consider Inose's fibration on X [Inose 1978; Shioda 2006]. In the present case, $K = \mathbb{Q}(\sqrt{-3})$, and X arises from the Shioda–Inose construction (see Section 2) for the following elliptic curves:

$$E \text{ with CM by } \mathbb{O}_K \quad \text{and} \quad E' \text{ with CM by } \mathbb{Z} + 3\mathbb{O}_K.$$

In particular, $j(E) = 0$. It follows from [Inose 1978] that X admits the isotrivial elliptic fibration

$$X: \quad y^2 = x^3 + t^5(3t^2 - 2 \cdot 11 \cdot 23\, t + 3).$$

Here the singular fibres have type II^*, II^*, II, II, and the Mordell–Weil group over $\overline{\mathbb{Q}}$ has rank two. The generic fibre has CM by $\mathbb{O}_K$. Let ω denote a primitive third root of unity acting on X via $x \mapsto \omega x$. If P is a section of the elliptic surface, then so is $\omega^* P$. Since the singular fibres admit no nontrivial torsion sections, these sections are independent. Since this argumentation applies to any twist Y of X, $\mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$ always acts nontrivially on $MW(Y)$. Hence $\mathrm{rk}\, MW(Y/\mathbb{Q}) < 2$ and in particular $\rho(Y/\mathbb{Q}) < 20$. □

10. Existence of K3 surfaces of Picard rank 20 over $\mathbb{Q}$

There are 13 primitive lattices T of class number one appearing in Theorem 1. For each of them one can ask whether there is a K3 surface with Picard rank 20 over $\mathbb{Q}$ and this transcendental lattice. Elkies [2007] announced in that this holds true

for each T. It follows that for each of these surfaces, one such model is given by Inose's fibration for the CM-elliptic curve corresponding to T, as exhibited over $\mathbb{Q}$ in [Schütt 2007b].

However, for Inose's fibration, the nontrivial sections are often not immediate. In the cases at hand, there are two fibres of type II^* plus an additional reducible fibre of type I_2. Hence the Mordell–Weil rank is one. Elkies recently computed the Mordell–Weil generator of height $|d|/2$ explicitly for all these fibrations [Elkies 2008a].

For the reader's convenience we include a list of different models of these K3 surfaces where the Picard rank 20 over $\mathbb{Q}$ becomes evident. These models are given in terms of elliptic fibrations with configuration of singular fibres and the abstract structure of the Mordell–Weil group. We also include a reference, but naturally the given models are far from unique. Other models may be found in [Elkies 2008b; Schütt 2007a; Top and Yui 2007] for instance. Explanations follow the table.

d	configuration	MW	reference
-3	$[1^3, 3, 12^*]$	$\mathbb{Z}/4$	Lemma 26
-4	$[0^*, III^*, III^*]$	$\mathbb{Z}/2$	Lemma 25
-7	$[1^3, 7^3]$	$\mathbb{Z}/7$	Example 9
-8	$[1, 4, III^*, II^*]$	$\{0\}$	[Schütt 2007a, §7]
-11	$[1^3, 11, II^*]$	$\{0\}$	[Schütt 2006, (III.2)]
-12	$[2, 3, III^*, II^*]$	$\{0\}$	[Schütt 2007a, §7]
-16	$[2, 8, 1^*, 1^*]$	$\mathbb{Z}/4$	[Schütt 2007a, §7]
-19	$[1^5, 19]$	$\{0\}$	Example 8
-27	$[1^4, 2, 9^2]$	$\mathbb{Z}+\mathbb{Z}/3$	Example 23
-28	$[1^6, 6, 12]$	$\mathbb{Z}^2$	[Elkies 2008b, §5]
-43	$[1^6, 6, 12]$	$\mathbb{Z}^2$	[Elkies 2008b, §5]
-67	$[1^3, 4, 7, II^*]$	$\mathbb{Z}$	[Elkies 2008b, §4]
-163	$[1^6, 6, 12]$	$\mathbb{Z}^2$	[Elkies 2008b, §5]

For $\boldsymbol{d=-8, -12}$, it was shown in [Schütt 2007a, §7] that the named fibrations are defined over $\mathbb{Q}$. To obtain Picard rank 20 over $\mathbb{Q}$, it suffices to apply a quadratic twist as in Example 8 such that the fibre of type I_4 or I_3, respectively, becomes split-multiplicative.

For $\boldsymbol{d=-11}$, the following Weierstrass form was derived in [Schütt 2006]:

$$y^2 = x^3 + t^2(t^2+3t+1)\,x^2 + t^4(2t+4)\,x + t^5(t+1).$$

This fibration has a II^* fibre at 0 and a split-multiplicative fibre of type I_{11} at ∞.

For $d = -16$, we realise the surface as a quadratic base change of the extremal rational elliptic surface with configuration $[1, 4, 1^*]$. It has a rational 4-torsion section P which meets the singular fibres I_4 at a near and I_1^* at a far component [Miranda and Persson 1986]. This implies that all fibre components are defined over $\mathbb{Q}$. The same argumentation applies to the base changed surface. Here we choose the base change in such a way that the I_1^* fibres sit above rational cusps.

Example 23 (Discriminant $d = -27$). For this discriminant, we searched the one-dimensional family of elliptic K3 surfaces with the given configuration $[1^4, 2, 9^2]$ and a 3-torsion section for an appropriate specialisation. Using techniques from [Elkies and Schütt 2008], we found

$$X: \quad y^2 + 3(2t^2+1)xy + (1-t^2)^3 y = x^3.$$

This elliptic surface has 3-torsion sections with zero x-coordinate and an independent section P over $\mathbb{Q}$ with x-coordinate $x(P) = (t-1)^3$ and height $h(P) = 3/2$. The I_9 fibres are located at $t = \pm 1$ and split-multiplicative. Hence X has Picard rank 20 over $\mathbb{Q}$. Using the height pairing [Shioda 1990], one can show that neither P nor its translates by the torsion sections are 3-divisible. Hence X has discriminant

$$d = -h(P)\,\frac{\operatorname{disc}(A_1)\operatorname{disc}(A_8)^2}{|MW(X)|^2} = -27.$$

11. Classification up to $\mathbb{Q}$-isomorphism

So far, we have only considered K3 surfaces up to isomorphism over $\mathbb{C}$. Then a singular K3 surface X is identified by its transcendental lattice $T(X)$ (Theorem 3). In this section, we answer the question which $\mathbb{Q}$-isomorphism classes have Picard rank 20 over $\mathbb{Q}$. This is closely related to the precise shape of the corresponding Hecke eigenform (compare Lemma 17).

We will work with Inose's elliptic fibration. In this context, one should always have quadratic twisting as in (3) in mind. This operation twists the modular forms. Notably it also twists sections and affects singular fibres of types IV, IV^*, I_m^*, $I_n (n > 2)$. Our first result concerns the case $d \neq -3, -4$:

Proposition 24. *Let $0 > d \neq -3, -4$ of class number one. Up to $\mathbb{Q}$-isomorphism, there is a unique K3 surface X of discriminant d and Picard rank 20 over $\mathbb{Q}$.*

Proof. The existence was shown in the previous section. We work with Inose's fibration with reducible singular fibres I_2, II^*, II^* and a section P of height $h(P) = |d|/2$. Over $\mathbb{C}$, such a fibration is unique [Shioda 2006]. Over $\mathbb{Q}$, this only leaves quadratic twists (for $d \neq -3, -4$). But then the condition that the section P be defined over $\mathbb{Q}$ distinguishes the unique twist with Picard rank 20 over $\mathbb{Q}$. □

Lemma 25. *Let $d = -4$. Consider the extremal elliptic K3 surface*

$$X: \quad y^2 = x^3 - t^3(t-1)^2 x, \tag{19}$$

with singular fibres III^* at 0 and ∞ and I_0^* at 1 and two-torsion section $(0,0)$. Then any K3 surface with discriminant d and Picard rank 20 over $\mathbb{Q}$ is $\mathbb{Q}$-isomorphic to a quadratic twist of X.

Proof. The configuration determines a unique elliptic fibration over $\mathbb{C}$. Over $\mathbb{Q}$, we distinguish biquadratic twists

$$X_\delta: \quad y^2 = x^3 - \delta t^3(t-1)^2 x, \quad \delta \in \mathbb{Q}^*.$$

All fibre components are defined over $\mathbb{Q}$ with the possible exception of the simple components of the I_0^* fibre which do not meet the zero section. These components are endowed with the Galois action of the extension $\mathbb{Q}(x^3 - \delta x)/\mathbb{Q}$. Hence all components are defined over $\mathbb{Q}$ if and only if δ is a square in $\mathbb{Q}^*$. This corresponds to the quadratic twist of (19) by $\sqrt{\delta}$ as in (3). □

Lemma 26. *Let $d = -3$. Consider Inose's fibration*

$$X: \quad y^2 = x^3 - t^5(t+1)^2$$

with singular fibres II^* at 0 and ∞ and IV at -1. Then any K3 surface with discriminant d and Picard rank 20 over $\mathbb{Q}$ is $\mathbb{Q}$-isomorphic to a cubic twist of X.

Different elliptic fibrations on this surface have been studied in [Schütt 2008]. We omit the proof, which is analogous to the previous one.

Remark 27. If $d = -3$ or -4, then there are infinitely many possible associated newforms by Lemma 17. By the previous two lemmata, each of these twists (quadratic and cubic) is associated to a unique K3 surface of Picard rank 20 over $\mathbb{Q}$.

12. K3 surfaces with Picard rank 20 over a quadratic extension

In the next section, we will apply our methods to fields of definition of general singular K3 surfaces and their Néron–Severi lattices. To give a flavor of the ideas involved, we first give a full treatment of K3 surfaces with Picard rank 20 over a quadratic extension of $\mathbb{Q}$. We keep the techniques and notation above.

Proposition 28. *Let L be a quadratic extension of $\mathbb{Q}$ and X be a K3 surface with Picard rank 20 over L. As before, let $T(X)$ denote the transcendental lattice, d its discriminant and $K = \mathbb{Q}(\sqrt{d})$.*

(i) *If $L = K$, then d has class number one.*

(ii) *If $L \neq K$, then d has class number one or two. In the latter case, the compositum LK agrees with the ring class field $H(d)$.*

Proof. We consider all those primes p that split in both K and L. Let $\mathfrak{p} \mid p$ in L. Then $\mathbb{F}_\mathfrak{p} = \mathbb{F}_p$ and again $\rho(X/\mathbb{F}_p) = 20$. As before we will apply the Artin–Tate conjecture to the reduction of X at $\mathfrak{p}$. For this, we need the coefficient $a_\mathfrak{p}$ of the characteristic polynomial of $\mathrm{Frob}_\mathfrak{p}$ as in (6). Even if X is not defined over $\mathbb{Q}$, there still is a modularity result over some extension:

Theorem 29 [Shioda and Inose 1977, Theorem 6]. *Upon increasing the base field, the ζ-function of a singular K3 surface X splits into one-dimensional factors. Then the L-function of the transcendental lattice factors as*

$$L(T(X), s) = L(\psi^2, s)\, L(\overline{\psi}^2, s),$$

where ψ is the Hecke character associated to an elliptic curve with CM in K. Here one can choose the elliptic curve E identified with the transcendental lattice $T(S)$ under the map

$$\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \mapsto \tau = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \mapsto E = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}).$$

Thanks to this result, we are able to derive the relevant properties of $a_\mathfrak{p}$ to apply our previous techniques. We will need the following lemma:

Lemma 30. *In the above notation, $a_\mathfrak{p} \in K$. Moreover $a_\mathfrak{p}$ takes the shape of Example 5 and p splits into primes of order two in* $\mathrm{Cl}(K)$:

$$p^2 = \alpha_\mathfrak{p} \cdot \bar{\alpha}_\mathfrak{p} = x^2 + Dy^2, \quad a_\mathfrak{p} = \pm 2x.$$

Remark 31. By inspection, Lemma 30 does not require $\mathrm{NS}(X)$ to be rational over $\mathbb{F}_\mathfrak{p}$, but only p to split in K and $\mathfrak{p} \mid p$. In our special case where $\mathrm{NS}(X)$ is fully defined over $\mathbb{F}_\mathfrak{p}$, the proof of Proposition 28 will ultimately show that p splits into principal primes in $\mathrm{Cl}(d)$.

Proof of Lemma 30. From the Weil conjectures we know that

$$a_\mathfrak{p} = \alpha_\mathfrak{p} + \bar{\alpha}_\mathfrak{p} \quad \text{with } |\alpha_\mathfrak{p}| = p. \tag{20}$$

Here $\alpha_\mathfrak{p}, \bar{\alpha}_\mathfrak{p}$ are algebraic integers, complex conjugate in an imaginary quadratic extension of $\mathbb{Q}$ since $a_\mathfrak{p} \in \mathbb{Z}$. We have to show that this quadratic field is K. In the present situation we know the ζ-function of X over some extension of L by Theorem 29. As a result of increasing the ground field, the eigenvalues $\psi(\mathfrak{P})^2$, $\overline{\psi(\mathfrak{P})}^2$ of Frobenius at a prime $\mathfrak{P}$ above $\mathfrak{p}$ agree with some power of $\alpha_\mathfrak{p}$, $\bar{\alpha}_\mathfrak{p}$. Since $\psi(\mathfrak{P}) \in K \setminus \mathbb{Q}$ and $\alpha_\mathfrak{p}$ is quadratic over $\mathbb{Q}$, this implies that $\alpha_\mathfrak{p} \in K$. It follows that $a_\mathfrak{p}$ has exactly the same shape as a_p in Example 5. In fact, we deduce from (20) that

$$p^2 = \alpha_\mathfrak{p} \cdot \bar{\alpha}_\mathfrak{p} = x^2 + Dy^2, \quad \text{where } a_\mathfrak{p} = \alpha_\mathfrak{p} + \bar{\alpha}_\mathfrak{p} = \pm 2x.$$

This is to say that the prime factors of p in K become principal upon squaring. □

Thanks to Lemma 30 we can continue exactly along the lines of the previous sections to complete the proof of Proposition 28. We distinguish two cases:

If $L = K$, then at every good split prime $\mathfrak{p}$ in K, we have $\rho(X/\mathbb{F}_\mathfrak{p}) = 20$. Hence the arguments from the previous sections carry over except for Lemma 22. That is, d has class number one, but imprimitive $T(X)$ occurs.

If $L \neq K$, then Proposition 14 tells us that all the primes that split in both K and L are principal. Hence K has class number one or two. By the argumentation of Section 8, all these p are principal in $\mathrm{Cl}(d)$ as well (as mentioned in Remark 31). Hence, d has class number one or two. In the latter case, $LK = H(d)$ by class field theory. □

Remark 32. For many K3 surfaces with Picard rank 20 over a quadratic extension, we know a model over $\mathbb{Q}$. Most of these models arise through the Shioda–Inose fibration [Inose 1978; Schütt 2007b] or through extremal elliptic surfaces [Beukers and Montanus 2008; Schütt 2007a]. It is an open question whether *all* K3 surfaces with Picard rank 20 over a quadratic extension (or more generally with discriminant d of class number two) might have a model over $\mathbb{Q}$.

13. Singular K3 surfaces over number fields

We conclude the paper with an application of our techniques to general singular K3 surfaces. We will derive an explicit obstruction for the field of definition of the surface and that of its Néron–Severi group. First we recall a possible field of definition:

Lemma 33. *Let X be a singular K3 surface of discriminant d. Then X has a model over the ring class field $H(d)$.*

A model was given in [Schütt 2007b, proof of Proposition 10], based on Inose's fibration [1978] (compare [Shioda 2006]). Elkies [2007] announced another model.

In general, the field $H(d)$ need not be the optimal field of definition. In fact, there are examples of singular K3 surfaces over $\mathbb{Q}$ where $H(d)$ has degree 16 or 24 over K. The question arises how far one can possibly descend X, starting from $H(d)$. Shimada [2009] (for fundamental d) and the author [Schütt 2007b] (in full generality) derived the following condition in terms of lattice:

$$\{T(X^\sigma);\, \sigma \in \mathrm{Aut}(\mathbb{C}/K)\} = \text{genus of } T(X). \tag{21}$$

In Section 2, we used this to the following effect: If X is defined over $\mathbb{Q}$, then the genus of $T(X)$ consists of a single class, that is, $\mathrm{Cl}(T(X)) \cong (\mathbb{Z}/2)^g$.

To rephrase (21) in terms of class field theory, denote the degree of primitivity of $T(X)$ by m. Write $d = m^2 d'$, so that we can identify

$$\mathrm{Cl}(T(X)) \cong \mathrm{Cl}(d').$$

Let $G = \mathrm{Cl}(d')[2]$, the two-torsion subgroup of $\mathrm{Cl}(d')$, and M the fixed field of G in the abelian Galois extension $H(d')/K$.

Lemma 34. *Let X be a singular K3 surface over some number field L. In the above notation,*

$$M \subset KL.$$

So far, this was the only known obstruction to fields of definition of singular K3 surfaces. The only drawback of Lemma 34 is that it fails to measure the degree of primitivity of $T(X)$. For this reason, Theorem 2 provides a major improvement: By providing bounds on the discriminant d, it also implies restrictions on the degree of primitivity. We shall now apply the techniques from the previous sections to prove Theorem 2.

Proof of Theorem 2. Without loss of generality, we can assume that L contains K. We consider all those good primes p that split completely in L. Let $\mathfrak{p} \mid p$ in L. Then $\mathbb{F}_\mathfrak{p} = \mathbb{F}_p$ and $\rho(X/\mathbb{F}_p) = 20$. Hence we can apply the Artin–Tate conjecture at $\mathfrak{p}$. As in the previous section, Lemma 30 guarantees that $a_\mathfrak{p}$ has the shape of Example 5 and p splits into prime ideals of order two in $\mathrm{Cl}(K)$. By the argumentation of Sections 6–8, p is not only represented by the principal class of $\mathrm{Cl}(K)$, but also of $\mathrm{Cl}(d)$. Hence, by class field theory, L has to contain the ring class field $H(d)$. □

Since there are only limited possibilities for the Galois action on the Néron–Severi lattice of a singular K3 surface (or on any lattice of given rank), Theorem 2 provides us with a direct proof of the following finiteness result due to Shafarevich. For best efficiency, Theorem 2 should be combined with Lemma 34.

Theorem 35 [Shafarevich 1996]. *Let $n \in \mathbb{N}$. Then*

$$\#\{\textit{singular K3 surface } X \textit{ over } L;\ [L:\mathbb{Q}] \le n\}_{/\cong} < \infty.$$

Remark 36. Similar results can be established for other modular surfaces, for instance for singular abelian surfaces [Shioda and Mitani 1974]. In that particular case, they would also follow from the cohomological structure (see Remark 11).

Acknowledgements

The author would like to thank N. Elkies, I. Shimada and T. Shioda for many stimulating discussions. Funding from DFG under research grant Schu 2266/2-2 is gratefully acknowledged.

References

[Artin and Swinnerton-Dyer 1973] M. Artin and H. P. F. Swinnerton-Dyer, "The Shafarevich–Tate conjecture for pencils of elliptic curves on $K3$ surfaces", *Invent. Math.* **20** (1973), 249–266. MR 54 #5240 Zbl 0289.14003

[Beukers and Montanus 2008] F. Beukers and H. Montanus, "Explicit calculation of elliptic fibrations of $K3$-surfaces and their Belyi-maps", pp. 33–51 in *Number theory and polynomials*, edited by J. McKee and C. Smyth, London Math. Soc. Lecture Note Ser. **352**, Cambridge Univ. Press, Cambridge, 2008. MR 2009j:14011

[Elkies 2007] N. D. Elkies, "The maximal Mordell–Weil rank of an elliptic K3 surface over $\mathbb{Q}(t)$", talk at conference on Birational Automorphisms of Compact Complex Manifolds and Dynamical Systems at Nagoya University, 28 August 2007.

[Elkies 2008a] N. D. Elkies, "Mordell–Weil generators for singular Shioda–Inose surfaces over $\mathbb{Q}$", preprint, 2008, Available at http://www.math.harvard.edu/~elkies/K3_20SI.html.

[Elkies 2008b] N. D. Elkies, "Shimura curve computations via K3 surfaces of Néron–Severi rank at least 19", pp. 196–211 in *Algorithmic number theory*, edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, Berlin, 2008. MR 2467847 Zbl 05279287

[Elkies and Schütt 2008] N. D. Elkies and M. Schütt, "K3 surfaces and modular forms", preprint, 2008. arXiv 0809.0830

[Hall 1971] M. Hall, Jr., "The Diophantine equation $x^3 - y^2 = k$", pp. 173–198 in *Computers in number theory* (Oxford, 1969), edited by A. O. L. Atkin and B. J. Birch, Proc. Sci. Res. Council Atlas Sympos. **2**, Academic Press, London, 1971. MR 48 #2061 Zbl 0225.10012

[Hulek and Verrill 2005] K. Hulek and H. A. Verrill, "On the motive of Kummer varieties associated to $\Gamma_1(7)$", *J. Math. Kyoto Univ.* **45**:4 (2005), 667–681. supplement to R. Livné and N. Yui, "The modularity of certain non-rigid Calabi–Yau threefolds", *J*. Math. Kyoto Univ. **45**:4 (2005), 645–665. MR 2007b:11092 Zbl 1106.14023

[Inose 1978] H. Inose, "Defining equations of singular $K3$ surfaces and a notion of isogeny", pp. 495–502 in *Proceedings of the International Symposium on Algebraic Geometry* (Kyoto, 1977), edited by M. Nagata, Kinokuniya Book Store, Tokyo, 1978. MR 81h:14021 Zbl 0411.14009

[Liu et al. 2005] Q. Liu, D. Lorenzini, and M. Raynaud, "On the Brauer group of a surface", *Invent. Math.* **159**:3 (2005), 673–676. MR 2005k:14036 Zbl 1077.14023

[Livné 1995] R. Livné, "Motivic orthogonal two-dimensional representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$", *Israel J. Math.* **92**:1-3 (1995), 149–156. MR 96m:11050 Zbl 0847.11035

[Milne 1975] J. S. Milne, "On a conjecture of Artin and Tate", *Ann. of Math.* (2) **102**:3 (1975), 517–533. See also his addendum to this article at http://www.jmilne.org/math/articles/add/addendaA.pdf. MR 54 #2659 Zbl 0343.14005

[Miranda and Persson 1986] R. Miranda and U. Persson, "On extremal rational elliptic surfaces", *Math. Z.* **193**:4 (1986), 537–558. MR 88a:14044 Zbl 0652.14003

[Piatetskiĭ-Shapiro and Shafarevich 1971] I. I. Piatetskiĭ-Shapiro and I. R. Shafarevich, "Torelli's theorem for algebraic surfaces of type K3", *Izv. Akad. Nauk SSSR Ser. Mat.* **35** (1971), 530–572. In Russian. MR 44 #1666 Zbl 0219.14021

[Ribet 1977] K. A. Ribet, "Galois representations attached to eigenforms with Nebentypus", pp. 17–51 in *Modular functions of one variable* (Bonn, 1976), edited by J.-P. Serre and D. B. Zagier, Lecture Notes in Math. **601**, Springer, Berlin, 1977. MR 56 #11907 Zbl 0363.10015

[Schütt 2006] M. Schütt, *Hecke eigenforms and the arithmetic of singular K3 surfaces*, dissertation, Universität Hannover, 2006.

[Schütt 2007a] M. Schütt, "Elliptic fibrations of some extremal $K3$ surfaces", *Rocky Mountain J. Math.* **37**:2 (2007), 609–652. MR 2008c:14047

[Schütt 2007b] M. Schütt, "Fields of definition of singular $K3$ surfaces", *Commun. Number Theory Phys.* **1**:2 (2007), 307–321. MR 2008g:14060 Zbl 1157.14308

[Schütt 2008] M. Schütt, "Arithmetic of a singular $K3$ surface", *Michigan Math. J.* **56**:3 (2008), 513–527. MR 2009k:11106 Zbl 1163.14022

[Schütt 2009] M. Schütt, "CM newforms with rational coefficients", *Ramanujan J.* **19**:2 (2009), 187–205. MR 2511671 Zbl 05633530

[Schütt and Schweizer 2007] M. Schütt and A. Schweizer, "On the uniqueness of elliptic K3 surfaces with maximal singular fibre", preprint, 2007. arXiv 0712.3873

[Schütt and Top 2006] M. Schütt and J. Top, "Arithmetic of the [19, 1, 1, 1, 1, 1] fibration", *Comment. Math. Univ. St. Pauli* **55**:1 (2006), 9–16. MR 2007m:14053 Zbl 1125.14022

[Shafarevich 1996] I. R. Shafarevich, "On the arithmetic of singular $K3$-surfaces", pp. 103–108 in *Algebra and analysis* (Kazan, 1994), edited by M. M. Arslanov et al., de Gruyter, Berlin, 1996. MR 98h:14041 Zbl 0947.14020

[Shimada 2009] I. Shimada, "Transcendental lattices and supersingular reduction lattices of a singular $K3$ surface", *Trans. Amer. Math. Soc.* **361**:2 (2009), 909–949. MR 2009m:14055 Zbl 05518627

[Shioda 1990] T. Shioda, "On the Mordell–Weil lattices", *Comment. Math. Univ. St. Paul.* **39**:2 (1990), 211–240. MR 91m:14056 Zbl 0725.14017

[Shioda 1994] T. Shioda, "On the rank of elliptic curves over $\mathbf{Q}(t)$ arising from $K3$ surfaces", *Comment. Math. Univ. St. Paul.* **43**:1 (1994), 117–120. MR 95c:14041 Zbl 0815.14022

[Shioda 2003] T. Shioda, "The elliptic $K3$ surfaces with with a maximal singular fibre", *C. R. Math. Acad. Sci. Paris* **337**:7 (2003), 461–466. MR 2004j:14046 Zbl 1048.14017

[Shioda 2005] T. Shioda, "On $K3$ surfaces defined over $\mathbf{Q}$", *Comment. Math. Univ. St. Pauli* **54**:1 (2005), 87–88. Correction to [Shioda 1994]. MR 2006b:14065 Zbl 0815.14022

[Shioda 2006] T. Shioda, "Kummer sandwich theorem of certain elliptic $K3$ surfaces", *Proc. Japan Acad. Ser. A Math. Sci.* **82**:8 (2006), 137–140. MR 2008b:14064 Zbl 1112.14044

[Shioda and Inose 1977] T. Shioda and H. Inose, "On singular $K3$ surfaces", pp. 119–136 in *Complex analysis and algebraic geometry*, edited by W. L. B. Jr. et al., Iwanami Shoten, Tokyo, 1977. MR 56 #371 Zbl 0374.14006

[Shioda and Mitani 1974] T. Shioda and N. Mitani, "Singular abelian surfaces and binary quadratic forms", pp. 259–287 in *Classification of algebraic varieties and compact complex manifolds*, edited by H. Popp, Lecture Notes in Math. **412**, Springer, Berlin, 1974. MR 52 #3174 Zbl 0302.14011

[Tate 1965] J. T. Tate, "Algebraic cycles and poles of zeta functions", pp. 93–110 in *Arithmetical Algebraic Geometry* (West Lafayette, IN, 1963), edited by O. F. G. Schilling, Harper & Row, New York, 1965. MR 37 #1371 Zbl 0213.22804

[Tate 1966] J. Tate, "On the conjectures of Birch and Swinnerton-Dyer and a geometric analog", pp. 415–440 in *Sém. Bourbaki* 1965/66 (Exposé 306), edited by N. H. K. A. Grothendieck, 1966. Reprinted as pages 189–214 of *Dix exposés sur la cohomologie des schemas*, North-Holland, Amsterdam, 1968. MR 1610977 Zbl 0199.55604

[Tate 1974] J. T. Tate, "The arithmetic of elliptic curves", *Invent. Math.* **23** (1974), 179–206. MR 54 #7380 Zbl 0296.14018

[Top and Yui 2007] J. Top and N. Yui, "Explicit equations of some elliptic modular surfaces", *Rocky Mountain J. Math.* **37**:2 (2007), 663–687. MR 2008c:14049 Zbl 1140.14036

[Weinberger 1973] P. J. Weinberger, "Exponents of the class groups of complex quadratic fields", *Acta Arith.* **22** (1973), 117–124. MR 47 #1776

Communicated by János Kollár
Received 2009-07-21 Revised 2009-11-14 Accepted 2009-12-31

schuett@math.uni-hannover.de *Institut für Algebraische Geometrie, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany*
http://www.iag.uni-hannover.de/~schuett/

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in ANT are usually in English, but articles written in other languages are welcome.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@mathscipub.org with details about how your graphics were generated.

White Space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 4 No. 3 2010

Algebra & Number Theory 2010 Vol. 4, No. 3

1937-0652(2010)4:3;1-G