Exponential sums, hypersurfaces with many symmetries and Galois representations

Gabriel Chênevert

McGill University Ph.D. thesis

Exponential sums, hypersurfaces with many symmetries and Galois representations

Gabriel Chênevert

Department of Mathematics and Statistics
McGill University, Montreal

September 2008

A thesis submitted to McGill University in partial fulfilment
of the requirements of the degree of Doctor of Philosophy

Contents

Abstract

The main theme of this thesis is the study of compatible systems of ℓ-adic Galois representations provided by the étale cohomology of arithmetic varieties with a large group of symmetries. A canonical decomposition of these systems into isotypic components is proven (Section 3.1). The isotypic components are realized as the cohomology of the quotient with values in a certain sheaf, thus providing a geometrical interpretation for the rationality of the corresponding L-functions.

A particular family of singular hypersurfaces $W_\ell^{m,n}$ of degree ℓ and dimension $m+n-3$, admitting an action by a product of symmetric groups $S_m \times S_n$, arises naturally when considering the average moments of certain exponential sums (Chapter 4); asymptotics for these moments are obtained by relating them to the trace of the Frobenius morphism on the cohomology of the desingularization of the corresponding varieties, following the approach of [39].

Two other closely related classes of smooth hypersurfaces admitting an S_n-action are introduced in Chapter 3, and the character of the representation of the symmetric group on their primitive cohomology is computed. In particular, a certain smooth cubic hypersurface of dimension 4 is shown to carry a compatible system of 2-dimensional Galois representations. A variant of the Faltings-Serre method is developed in Chapter 5 in order to explicitly determine the corresponding modular form, whose existence is predicted by Serre's conjecture. We provide a systematic treatment of the Faltings-Serre method in a form amenable to generalization to Galois representations of other fields and to other groups besides GL_2.

Résumé

Le thème principal de cette thèse est l'étude des systèmes compatibles de représentations galoisiennes ℓ-adiques provenant de la cohomologie étale de variétés arithmétiques admettant beaucoup de symétries. Une décomposition canonique de ces systèmes en composantes isotypiques est obtenue (section 3.1). Les composantes isotypiques sont décrites comme la cohomologie du quotient à valeurs dans un certain faisceau, fournissant ainsi une interprétation géométrique de la rationalité des fonctions L correspondantes.

Une famille spécifique d'hypersurfaces $W_\ell^{m,n}$ de degré ℓ et dimension $m+n-3$, admettant une action du produit de groupes symétriques $S_m \times S_n$, apparaît naturellement en lien avec les moments moyens de certaines sommes exponentielles (chapitre 4); le comportement limite de ces moments est obtenu en considérant la trace du morphisme de Frobenius sur la cohomologie de la désingularisation des variétés correspondantes, suivant l'approche développée dans [39].

Deux autres classes apparentées d'hypersurfaces lisses admettant une action du groupe symétrique sont introduites au chapitre 3, et le caractère de la représentation de S_n sur leur cohomologie primitive est calculé. En particulier, dans le cas d'une certaine hypersurface cubique de dimension 4, un système compatible de représentations galoisiennes de dimension 2 est obtenu. Une variante de la méthode de Faltings-Serre est développée dans le chapitre 5 afin de déterminer explicitement la forme modulaire correspondante, dont l'existence est prédite par la conjecture de Serre. Nous proposons un traitement systématique de la méthode de Faltings-Serre d'un point de vue qui se prête à la généralisation à d'autres corps ainsi que d'autres groupes que GL_2.

Acknowledgments

First and foremost, I want to thank my supervisor Eyal Goren for his constant dedication and support throughout the last few years. It was he who introduced me to the beauty of zeta functions when I took his algebraic geometry class as a Masters student, and through his guidance I have learned a lot both as a mathematical and human being. For some reason he always seemed to believe in my potential, and without his tacit encouragements and efforts to make me concretize it this thesis would almost certainly never have seen the light of the day.

Thanks as well to all the other professors from whom I learned, both inside and outside the classroom. Henri Darmon, Adrian Iovita, Hershy Kisilevsky, François Bergeron and Pierre Colmez come to mind. Special thanks to Jean-Pierre Serre who had the kindness of taking the time on two occasions to discuss some of his old work with me, and for being an overall awesome and inspiring person on so many levels.

Let's not forget everybody else, fellow students and post-docs, as well as support staff, which helped make my years in McGill be a pleasant and fruitful experience. A special mention goes to Carmen Baldonado, who with constant kindness always managed to keep me afloat among the many pitfalls of the McGill administration, despite me often not doing much to facilitate her task. Thanks also to Jan Nekovář and the people at Chevaleret for welcoming me there for a few months in 2006.

I also have the chance of knowing a certain number of people with whom I spent a lot of time talking about mathematical things, not necessarily directly related to this thesis, and who double as dear friends: Rémi Leclercq and Éveline Legendre, my surrogate family for a year; Baptiste Chantraine, the one and only; Étienne Ayotte-Sauvé, the hipster bureaucrat; Alexandre Girouard, the small red guy; and Clément Hyvrier, the articulate clumsy absurdist.

Thanks to those who read parts of this thesis and provided me with some helpful comments about my mathematical statements or prose, notably Filippo Nuccio who caught all sorts of small things in the first chapter.

Thanks to the Fab Four, both those from Liverpool and those from Verdun, for making my world a wonderful place to live in. And the late Elliott Smith, for bringing me solace in times when it was most direly needed.

Thanks to those who sustained me financially during these years and made it possible for me not to worry much about the many vicissitudes of material life, namely NSERC, FQRNT, ISM, the McGill math department, and of course my parents.

Thanks to anybody else who might happen to be presently reading these acknowledgements.

And to Kristel *ma belle*, without whom all of this would be utterly meaningless.

Introduction

It is a natural and pervasive approach in science in general, and mathematics in particular, to try to comprehend a complex object via its representations (in the broad sense) in a simpler setting sharing some of the same features. For example, one can try to understand a 3-dimensional geometrical object by projecting it onto various 2-dimensional planes and assemble these projections to form a coherent image of the initial object. In mathematics, much information about a complicated algebraic structure can be gained by studying its homomorphisms into more concrete or well-understood structures. Here, the complicated structure we have in mind is the Galois group

$$\mathrm{Gal}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$$

of all field automorphisms of the algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$, and understanding its structure is arguably the ultimate goal of algebraic number theory.

In general, given a group G, we can consider its actions on objects X belonging to a certain category $\mathcal{C}$, i.e. homomorphisms

$$G \longrightarrow \mathrm{Aut}_{\mathcal{C}}\, X.$$

For example, when the objects X are finite sets, we are led to consider homomorphisms from G to symmetric groups, i.e. (homomorphic) realizations of G as groups of permutations. In this thesis we will mainly be considering *linear* representations over a field E, which can be considered concretely as homomorphisms from G to a group of matrices $\mathrm{GL}_n(E)$.

In the case of $\mathrm{Gal}_{\mathbf{Q}}$, this approach has been very fruitful to date. Witness class field theory (a standard reference is [46]), which essentially gives a description of all the 1-dimensional representations of $\mathrm{Gal}_{\mathbf{Q}}$. The case of 2-dimensional representations have been a subject of active research during the last decades, and have seen a number of spectacular achievements. The most famous is certainly the proof by Wiles *et al.*

[67, 65, 6] of the Shimura-Taniyama conjecture, which states that the 2-dimensional representations coming from elliptic curves defined over $\mathbf{Q}$ arise from modular forms. More recently a full proof of Serre's conjecture [55] was announced (completing [32] which proves it for odd conductors), so that the same can be considered to be true for all odd, absolutely irreducible representations over finite fields. These are only the first steps in the far-reaching web of conjectures that encompasses the Langlands program, according to which all Galois representations arising from geometry should be automorphic.

If X is an algebraic variety defined over a number field K, the set $X(\overline{K})$ of points of X with coordinates in $\overline{K}$ carries a natural action of the absolute Galois group Gal_K of K. This action, however, does not propagates to an action on any of the invariants provided by algebraic topology since it is not continuous with respect to the topology inherited by an embedding $\overline{K} \hookrightarrow \mathbf{C}$ – never mind the fact that $X(\overline{K})$, with the topology induced from $X(\mathbf{C})$, is totally disconnected – let alone algebraic morphisms. This was one of the impetuses for Grothendieck and his coworkers to develop in the 1960's the theory of schemes to supply an appropriate category, and then to develop the machinery of *étale cohomology*, associating to X a compatible system of ℓ-adic representations

$$H^\bullet(X, \mathbf{Q}_\ell)$$

for the absolute Galois group Gal_K. Keeping in mind that representations into structures which share a certain likeness with the original one are bound to yield interesting information, it is no surprise that these ℓ-adic representations carry non-trivial arithmetic information.

Let X be a smooth and proper variety defined over a finite field $\mathbf{F}_q$ with q elements. Weil [66] had the initial insight that the conjectures he formulated about the behavior of the number of points $|X(\mathbf{F}_{q^r})|$ as r varies would follow formally from the existence of a "good" cohomology theory in this context, what is nowadays called a *Weil cohomology theory*. Among the various requirements that such a theory would have to satisfy in order to parallel the properties of Betti cohomology, one of the foremost is the analogue of the Lefschetz fixed point formula for the Frobenius morphism Frob_q of X. Weil's insight was that the set $X(\mathbf{F}_{q^r})$ of $\mathbf{F}_{q^r}$-rational points of X can be interpreted as the fixed locus of the r^{th} iterate of Frob_q on $X(\overline{\mathbf{F}}_q)$, and thus could be studied via such a suitable cohomology theory. As a consequence, if X is an arithmetic variety defined over a number field K, understanding its étale cohomology (as a compatible system of ℓ-adic representations of Gal_K) is essentially the same thing

as understanding how many points it has over all finite fields for which this question makes sense.

The starting point for this thesis was the pair of papers [39, 40] published by Livné in the 1980's. In the first one, he settles a conjecture of Birch [4] about the average distribution of exponential sums of the form

$$\sum_{x \in \mathbf{F}_q} \exp\left(\frac{2\pi i}{p}(ax^3 + bx)\right), \qquad a, b \in \mathbf{F}_p,\ a \neq 0,$$

as $p \to \infty$. Here "average limit distribution" means that for each p, we consider all the values of the parameters a and b at the same time, then look at how this set behaves as p grows. The average distribution of these exponential sums was studied in [39] via its moments, and the key fact is that these moments can be expressed in terms of the number of points on the projective varieties $W_n \subseteq \mathbf{P}^{n-1}$ defined by the pair of homogeneous equations

$$\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} x_i^3 = 0.$$

These varieties are smooth when n is odd, but acquire singularities when n is even. These singularities turn out to be ordinary double points, so the results of Schoen [50] can be applied to describe the cohomology of the desingularization of $\widetilde{W_n}$ of W_n, thus yielding asymptotics for the average moments of the exponential sums. In Chapter 4 we lay out a framework which allows to treat more general exponential sums, obtained by specifying a certain set of weights for the monomials that appear, and relate their average moments to the number of points on certain more general varieties depending on these weights. One major difference is that the cubic exponential sums above are real-valued, hence their distribution can be understood by considering a single sequence of moments; the exponential sum we consider are complex-valued in general, so that a 2-parameter family of moments is needed. For example, to study the distribution of the exponential sums

$$\sum_{x \in \mathbf{F}_p} \exp\left(\frac{2\pi i}{p}(ax^{\ell+1} + bx)\right), \qquad a, b \in \mathbf{F}_p,\ a \neq 0,$$

where ℓ is a fixed prime, we are led to study the projective varieties $W_\ell^{m,n} \subseteq \mathbf{P}^{m+n-1}$

defined by the homogeneous equations

$$\sum_{i=1}^{m} x_i - \sum_{j=1}^{n} y_j = \sum_{i=1}^{m} x_i^{\ell+1} - \sum_{j=1}^{n} y_j^{\ell+1} = 0.$$

In the second paper [40], Livné singled out the variety W_{10} (or $W_2^{0,10}$ in our notation) he considered in relation with the 10^{th} moment of cubic exponential sums and remarked that the middle-degree cohomology of its desingularization $\widetilde{W}_{10}$ has dimension 2, hence carries a compatible system of ℓ-adic representations of $\mathrm{Gal}_{\mathbf{Q}}$. He then took an educated guess at what should be the corresponding modular form, and proceeded to show it was indeed the case. This is really a statement about equivalence of two ℓ-adic Galois representations, one associated to the modular form and the other on the cohomology of $\widetilde{W}_{10}$, and he proved that the two representations were equivalent by using a criterion suggested by Serre, building on a previous remark of Faltings, which allows to decide whether two continuous 2-adic Galois representations *with even trace* and dimension 2 are equivalent or not by computing a finite number of traces.

At the time when work on this thesis started, the Serre conjecture was not expected to yield anytime soon (at least by the author of this thesis), hence it seemed desirable to come up with other such sporadic examples of modularity. The first task was to find other 2-dimensional compatible systems of Galois representations "in nature" (i.e., in the étale cohomology of some arithmetic variety) for which modularity was not known. Since varieties having a cohomology group of dimension exactly 2 are relatively few (for example, the only smooth irreducible hypersurfaces having this property are curves of genus 1), it was natural to look for varieties with possibly large cohomology, but which could be broken up in smaller pieces. It is a general phenomenon that this is the case for objects having extra symmetries (e.g. elliptic curves with complex multiplication, for which modularity was known [17] much before the 1990's).

However, even if (or rather, when) the full Serre conjecture is proven, such explicit examples of modularity for 2-dimensional "motives" over $\mathbf{Q}$ are still of interest. For one, to be able to compute the level of the modular form corresponding to a 2-dimensional compatible system of representations arising from the cohomology of a variety, one would need very precise information about the ramification of the representation, and this information is often not readily available. As a consequence, one would often have to settle for a crude upper bound on the level of the modular form. In addition, being able to perform explicit proofs of modularity for dimension 2

representations of $\mathrm{Gal}_{\mathbf{Q}}$ is certainly a good starting point in our ambition to do just the same over other number fields, or for representations into other groups, such as $\mathrm{GL}_3, \mathrm{Sp}_4, \ldots$, for which no general modularity result is currently known.

This thesis deals with several topics that are interwoven by connections such as mentioned above. We consider certain exponential sums and their moments; cohomology of certain varieties with large automorphism group and their motivic decomposition; generalization of the Faltings-Serre criterion and tests for modularity. Throughout we put emphasis on explicit methods.

The first chapter starts with a discussion of linear group representations, both of finite groups in characteristic 0, and of Galois groups over ℓ-adic fields. Its goal is mainly to set up the notation and lay down the basic concepts which will appear throughout. The distinction between isomorphism and semisimple equivalence is discussed (Section 1.1) as most Galois representations coming from geometry are not yet known to be semisimple. The isotypic decomposition of representations of finite groups in characteristic 0 is then stated in a functorial way (Section 1.2) as we will need it to prove the analogous statement in the category of compatible systems of ℓ-adic representations in Chapter 3. The representation theory of the symmetric group is then briefly described (Section 1.3), before describing some of the features of Galois representations (Section 1.4) such as ramification, Artin L-functions and Hodge-Tate weights. In the last section we describe compatible systems of ℓ-adic representations (Section 1.5).

Chapter 2 is devoted to étale cohomology, with some of its formal properties described in Section 2.1. The Grothendieck trace formula, which implies that the étale cohomology groups of with values in $\mathbf{Q}_\ell$ (or more generally in a compatible family of λ-adic constructible sheaves) form a compatible system, is discussed together with purity in Section 2.2. We then describe more concretely the cohomology of smooth hypersurfaces (Section 2.3) and in particular of smooth quadric (Section 2.4), as well as that of hypersurfaces with ordinary double points (Section 2.5), following [50].

The last three chapters contain the original contributions of this thesis. In Chapter 3 we consider the linear representations on cohomology of a finite group which acts on a variety. The main theoretical result, probably known to the experts, is the isotypic decomposition of Theorem 3.1.4 for the compatible systems of Galois representations arising in such a context, i.e. that the Galois representations on the isotypic components are themselves compatible systems. This will be needed in order to perform some of the explicit computations in Chapter 5. In Section 3.2 we define

two classes of hypersurfaces admitting an action by the symmetric group S_n by permutation of the homogeneous coordinates. For a certain subclass of these hypersurfaces, which we call *special*, we obtain a general formula for the character of the representation of S_n on primitive cohomology (Theorem 3.2.14). We discuss in Section 3.3 the existence of such special hypersurfaces by providing some examples and describing obstructions to their existence coming from the representation theory of S_n. We then introduce in Section 3.4 the hypersurfaces $W_\ell^{m,n}$ alluded to above, related to the average moments of exponential sums appearing in Chapter 4. When smooth, $W_\ell^{m,n}$ is a special hypersurface in the sense of Section 3.2; when singular, its only singularities are ordinary double points (Proposition 3.4.4). In the last section we compute decompositions into irreducibles of the primitive cohomology of special hypersurfaces of low dimension; in particular, the variety $W_2^{0,7}$ is seen to carry a 2-dimensional compatible system, for which the corresponding modular form in computed in Chapter 5.

Chapter 4 carries out the discussion of moments of exponential sums mentioned above. After a short motivating introduction (Section 4.1) and review of the needed notions from measure theory (Section 4.2), the family of exponential sums under consideration is defined in Section 4.3 and their moments are related to the number of points on varieties closely related to the $W_\ell^{m,n}$ (Theorem 4.3.2). In Section 4.4 we put the machinery to work, the main result being an expression for the limits of the average moments for exponential sums of weights $\{1, \ell+1\}$, with ℓ a prime, generalizing the results and method of proof from [39] in the case $\ell = 2$.

Finally, the last chapter is devoted to the topic of algorithmically deciding whether two ℓ-adic Galois representations are semisimply equivalent or not. In the first section we explain why even for 2-dimensional systems over $\mathbf{Q}$ such methods can still be useful even if we admit the Serre conjecture. The basic object in the Faltings-Serre method, the *deviation group* of two ℓ-adic representations, is introduced in Section 5.2, following [58], and its basic properties are discussed. In the next section we discuss a more concrete homomorphic image of the deviation group, which can sometimes be substituted for the deviation group, in particular for the application to the modularity of $W_2^{0,7}$ we had in mind (see the remark there). In any case, we proceed to discuss in Section 5.4 the Faltings-Serre-Livné criterion, which is used as a model for our generalization in the next section (Theorem 5.5.13, using the group-theoretic classification result of Theorem 5.5.11). We then write down some general facts about quadratic extensions in Section 5.6 before proceeding with the explicit determination of the modular form corresponding to $W_2^{0,7}$ (Theorem 5.7.7).

Notation

The use of certain symbols is hopefully mostly consistent in this thesis.

The semi-ring of natural integers (including 0) is denoted $\mathbf{N}$, the ring of relative integers $\mathbf{Z}$, and the fields of rational, real and complex numbers $\mathbf{Q}$, $\mathbf{R}$ and $\mathbf{C}$, respectively. Rational prime numbers are usually denoted by p or ℓ. The field of ℓ-adic numbers is $\mathbf{Q}_\ell$, while the ring of ℓ-adic integers is $\mathbf{Z}_\ell$. An abstract finite field with $q = p^r$ elements is written $\mathbf{F}_q$.

Number fields are usually denoted K or L or variations on these. If L/K is a Galois extension of number fields, its Galois group is denoted $\mathrm{Gal}(L/K)$. The absolute Galois group of K with respect to an implicitly fixed algebraic closure $\overline{K}$ will be referred to as Gal_K. A Gothic $\mathfrak{p}$ is usually used to denote a finite place in a number field K, i.e. a nonzero prime ideal in its ring of integers $\mathcal{O}_K$, and its norm $N(\mathfrak{p})$ is the cardinality of the residual field $k_p = \mathcal{O}_K/\mathfrak{p}$. The notation $\mathrm{Frob}_\mathfrak{p}$ *always* refers to the geometric Frobenius at $\mathfrak{p}$; the arithmetic Frobenius substitution, should it be needed, will be referred to as $\mathrm{Frob}_\mathfrak{p}^{-1}$. The cyclotomic character is denoted χ_{cycl}.

The letter E is mostly reserved for fields of characteristic 0 which serve as coefficients for representations and such. The trace of a linear operator σ on a finite dimensional vector space V over E will be denoted $\mathrm{tr}\,\sigma$ or $\mathrm{tr}(\sigma \mid V)$ if needed. Similarly, its determinant is written $\det\sigma$ or $\det(\sigma \mid V)$. A graded vector space $V^\bullet = \bigoplus_i V^i$ is denoted with the use of a bullet, the grading being often implicit. If σ is an graded endomorphism of V , it is understood that the trace and determinant of σ are to be taken in the graded sense, i.e.

$$\mathrm{tr}(\sigma \mid V^\bullet) = \sum_i (-1)^i \,\mathrm{tr}(\sigma \mid V^i), \qquad \det(\sigma \mid V) = \prod_i \det(\sigma \mid V^i)^{(-1)^i}.$$

If E is a local number field, i.e. a finite extension of $\mathbf{Q}_\ell$, with maximal ideal λ, the notation E_λ will be used for psychological clarity, and its ring of integers will be called $\mathcal{O}_\lambda$.

Notation

The letters G and H are used for groups. The symmetric group on n symbols is denoted S_n, while C_n refers to the cyclic group of order n. The symbol 1 will be used liberally to denote the neutral element in a group written multiplicatively. The identity function of a set is written Id, while $\mathbf{1}$ usually refers to the trivial linear character.

Abstract isomorphisms are written $\simeq$, while canonical isomorphisms are usually written as $=$. The symbol $\sim$ is reserved for semisimple equivalence.

Chapter 1

Linear representations

This chapter aims to establish notation and to provide appropriate background on both "ordinary" representations of finite groups and ℓ-adic Galois representations (or rather λ-adic, where λ is the maximal ideal in some local number field E_λ). Nothing here can be considered new, but some aspects are treated with more care than they usually receive in textbooks, notably a precise, functorial statement of the isotypic decomposition of a semisimple representation (Corollary 1.2.2). We also try to put emphasis on the distinction between semisimple equivalence, which can be detected by the traces of the representations, and isomorphism, which is in general much subtler for non-semisimple representations. The reason for this is that the Galois representations arising from étale cohomology (described in Chapter 2) are not yet known to be semisimple, except in some special cases (e.g., abelian varieties [18]).

We start in Section 1.1 with a discussion of the relation of semisimple equivalence between representations of a group G over a field E of characteristic 0. Section 1.2 concentrates on semisimple representations (over non-necessarily algebraically closed fields), stating carefully their isotypic decomposition in a functorial way, and explaining how the multiplicities of the irreducible constituents can be computed using the theory of characters in the case of representations of finite groups in characteristic 0. This will be needed later to establish that the isotypic components (or rather, the multiplicity spaces) of the étale cohomology of varieties with respect with rational automorphisms form compatible systems of λ-adic representations (Section 3.1). We then give in Section 1.3 an overview of the representation theory of the symmetric group S_n, as developed by Frobenius, Schur and Young at the beginning of the previous century. The irreducible representations of S_n can all be realized over $\mathbf{Q}$, and can moreover be explicitly parametrized by the conjugacy classes in a way which is uni-

form in n. These facts will be used in Chapter 3 when we compute the decomposition into irreducibles of the cohomology of varieties admitting an action by S_n.

After recalling basic facts about Galois groups of number fields, we then turn our attention to Galois representations in Section 1.4. In particular, ramification, Artin L-functions and Hodge-Tate weights of λ-adic Galois representations are briefly discussed. The apparatus of étale cohomology for a variety X defined over a number field K yields for every choice of ℓ (or more generally, of a λ-adic constructible sheaf) a graded ℓ-adic representation $H^\bullet(X, \mathbf{Q}_\ell)$ for the absolute Galois group Gal_K. These representations in some sense *look like* they come from a single representation over $\mathbf{Q}$, although this is certainly not the case in general since they tend to have large image [53]. This notion is captured by the concept of compatible systems introduced in Section 1.5, following mainly [57]. The compatible systems of representations attached to modular forms by Deligne [11] are also briefly described.

1.1 Generalities on representations

We first review basic facts about the representations of a group G over a field E of characteristic 0 at the level of generality we will need. By an *E-valued representation* of G, we shall always mean a finite dimensional vector space V over E endowed with a linear action $\rho : G \to \mathrm{GL}(V)$. Equivalently, we may think of V as an $E[G]$-module of finite dimension over E, and we will move freely between the two points of view. Note however that if G is not finite, not all $E[G]$-modules of finite type are E-valued representations of G according to our definition; in particular, $E[G]$ itself does not have finite dimension.

In the above definition, there is no harm in requiring that G, E and V are endowed with a topology compatible with their algebraic structure, and that the homomorphism $\rho : G \to \mathrm{GL}(V)$ is continuous, since we could always equip everything with the discrete topology if needed. Henceforth, all representations in this thesis will tacitly be assumed to be continuous.

The usual notion of homomorphisms between representations (continuous linear maps commuting with the action of G) yields the concept of two representations ρ_1 and ρ_2 being *isomorphic*, in which case we shall write $\rho_1 \simeq \rho_2$. But this turns out to be too fine an equivalence relation on the category of representations for our purposes, because the Galois representations coming from étale cohomology are not yet known to be semisimple in general (although they are conjectured to be). Recall that a

simple representation is one which does not admit any non-trivial subrepresentation; a *semisimple* representation is one which can be written as a direct sum of simple subrepresentations.

Every representation $\rho : G \to \mathrm{GL}(V)$ admits a *Jordan-Hölder composition series*, i.e. a decreasing filtration

$$V = V_0 \supsetneqq V_1 \supsetneqq \cdots \supsetneqq V_m = 0$$

in which each V_{i+1} is a maximal proper G-stable subspace of V_i (the existence of such a series follows from dimension arguments). Let us write $\mathrm{JH}(\rho)$ for the set of isomorphism classes of the simple quotients V_i/V_{i+1}, with multiplicities. The following fact is standard in this context.

Lemma 1.1.1. *The multiset* $\mathrm{JH}(\rho)$ *does not depend on the choice of a Jordan-Hölder composition series for* ρ*.*

This allows us to define an equivalence relation on the set of representations which is coarser than being isomorphic.

Definition 1.1.2. We say that two E-valued representations ρ_1 and ρ_2 of a group G are *(semisimply) equivalent*, and write $\rho_1 \sim \rho_2$, if $\mathrm{JH}(\rho_1) = \mathrm{JH}(\rho_2)$.

Here we list the elementary properties of this equivalence relation.

Proposition 1.1.3. *Let* ρ_1 *and* ρ_2 *be* E*-valued representations of a group* G*.*

1. *If* $\rho_1 \simeq \rho_2$*, then* $\rho_1 \sim \rho_2$*.*

2. *If* ρ_1 *and* ρ_2 *are semisimple, then* $\rho_1 \simeq \rho_2 \iff \rho_1 \sim \rho_2$*, i.e. a semisimple representation is determined up to isomorphism by the multiplicities of its simple constituents.*

3. *For every representation* ρ*, there exists a unique (up to isomorphism) semisimple representation* ρ^{ss} *such that* $\rho \sim \rho^{\mathrm{ss}}$*. Concretely, if*

$$\mathrm{JH}(\rho) = \{(W_1, m_1), \ldots, (W_k, m_k)\},$$

then ρ^{ss} *is the action of* G *on* $W_1^{m_1} \oplus \cdots \oplus W_k^{m_k}$*.*

The (isomorphism class) of the semisimple representation ρ^{ss} appearing above is called the *semisimplification* of ρ. From 2 and 3, we see that for two representations ρ_1 and ρ_2,

$$\rho_1 \sim \rho_2 \iff \rho_1^{\mathrm{ss}} \simeq \rho_2^{\mathrm{ss}},$$

i.e., two representations are equivalent if and only if they have isomorphic semisimplifications.

The problem of deciding when two semisimple representations in characteristic 0 are isomorphic is completely controlled by the "theory of characters," i.e. by their trace. Given an E-valued representation ρ of a group G, its *trace* is the continuous function given by the composition

$$\operatorname{tr}\rho : G \xrightarrow{\rho} \mathrm{GL}(V) \xrightarrow{\mathrm{tr}} E.$$

Proposition 1.1.4. *Let ρ_1 and ρ_2 be two semisimple representations of a group G with values in a field E of characteristic 0. Then*

$$\rho_1 \simeq \rho_2 \iff \operatorname{tr}\rho_1 = \operatorname{tr}\rho_2.$$

Proof. This is basically the proof one finds in [5, §12]. The first implication ($\Rightarrow$) is clear. Now for ($\Leftarrow$), let V be a semisimple E-valued representation of G and write

$$V \simeq \bigoplus_i W_i^{m_i}, \qquad m_i \geq 0,$$

where the W_i's are the pairwise non-isomorphic simple constituents of V. Letting I_i be the annihilator of W_i in $E[G]$, we have $W_i \simeq E[G]/I_i$ as $E[G]$-modules. By the Jacobson density theorem, for each i there exists an element $e_i \in E[G]$ such that

$$e_i \equiv \begin{cases} 1 & \bmod I_i, \\ 0 & \bmod I_j,\ j \neq i. \end{cases}$$

We see that, as an E-linear endomorphism of V, we have

$$\operatorname{tr}(e_i \mid V) = m_i \dim W_i \in E,$$

so that we can recover the multiplicities of the simple constituents of V from the trace function on the group algebra $E[G]$ (this is where we use the fact that the

characteristic of E is 0). But since the trace function on $E[G]$ is determined by its restriction to G, the conclusion follows using part 2 of Proposition 1.1.3. □

Note that the trace does not distinguish a representation ρ from its semisimplification ρ^{ss}, since it is additive on short exact sequences whether they are split or not. It follows that for any two representations ρ_1 and ρ_2,

$$\rho_1 \sim \rho_2 \iff \rho_1^{\mathrm{ss}} \simeq \rho_2^{\mathrm{ss}} \iff \operatorname{tr}\rho_1 = \operatorname{tr}\rho_2.$$

Remark. The notions of isomorphism and equivalence of representations over E are invariant under extensions of the field E.

One might be tempted to consider not only the trace of a representation but its whole characteristic polynomial in order to salvage more information, but this is naive as the trace and characteristic polynomial functions determine each other as follows. First, to fix notation, let us stress that in this thesis, the *characteristic polynomial* of a linear operator $\sigma \in \mathrm{End}(V)$ shall always refer to the determinant

$$\det(1 - \sigma t) \in E[t].$$

When σ is invertible, this is easily related to the perhaps more familiar $\det(t - \sigma)$. Now since

$$\det(1 - \sigma t) = 1 - (\operatorname{tr}\sigma)t + \cdots + (-1)^n(\det\sigma)t^n,$$

it is clear that one can recover the trace from the characteristic polynomial. That the trace of a representation of a group G determines its characteristic polynomial is the content of the following lemma, which is pervasive in the theory of zeta functions. Recall that, for a field E of characteristic 0, we have a pair of mutually inverse group isomorphisms

$$(tE[[t]], +) \underset{\log}{\overset{\exp}{\simeq}} (1 + tE[[t]], \times)$$

given by the usual formulas

$$\exp f = \sum_{n=0}^{\infty} \frac{f^n}{n!}, \qquad \log(1+f) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{f^n}{n}.$$

Lemma 1.1.5. *Let V be a finite-dimensional vector space over a field E of charac-*

teristic 0 and $\sigma \in \mathrm{End}(V)$. In the formal series ring $E[[t]]$, we have the identity

$$\exp\left\{\sum_{r=1}^{\infty}(\mathrm{tr}\,\sigma^r)\frac{t^r}{r}\right\} = \frac{1}{\det(1-\sigma t)}.$$

Proof. If E is algebraically closed, and $\lambda_1, \ldots, \lambda_n$ are the (non-necessarily distinct) eigenvalues of σ in E, then $\lambda_1^r, \ldots, \lambda_n^r$ are the eigenvalues of σ^r, so that

$$\begin{aligned}\exp\left\{\sum_{r=1}^{\infty}(\mathrm{tr}\,\sigma^r)\frac{t^r}{r}\right\} &= \exp\left\{\sum_{r=1}^{\infty}\left(\sum_{i=1}^{n}\lambda_i^r\right)\frac{t^r}{r}\right\} = \exp\left(-\sum_{i=1}^{n}\log(1-\lambda_i t)\right)\\ &= \prod_{i=1}^{n}\frac{1}{1-\lambda_i t} = \frac{1}{\det(1-\sigma t)}.\end{aligned}$$

In the general case, the equality holds in $\overline{E}[[t]]$ by the above argument, hence the result follows since both sides actually have coefficients in E. □

1.2 Isotypic decomposition and multiplicities

Let G be a group and E a field such that $E[G]$ is semisimple (e.g. G is a finite group and $|G| \neq 0$ in E), so that all representations of G over E are semisimple. Let $\mathrm{Irr}_E(G)$ denote the set of isomorphism classes of irreducible (i.e. simple) representations of G over E, and for every $\phi \in \mathrm{Irr}_E(G)$, choose a representative W_ϕ of ϕ. By the semisimplicity assumption, we know that every representation V can be written as

$$V \simeq \bigoplus_{\phi \in \mathrm{Irr}_E(G)} W_\phi^{m_\phi(V)}, \tag{1.1}$$

and that the multiplicities $m_\phi(V) \geq 0$ completely characterize the isomorphism class of V. However, there is in general no canonical choice of the isomorphism (1.1). To get a canonical decomposition, define the *ϕ-isotypic component V_ϕ of V* by

$$V_\phi := \bigcup_f f(W_\phi),$$

where f ranges over the set $\mathrm{Hom}_G(W_\phi, V)$. Using the simplicity of W_ϕ, V_ϕ is easily checked to be a G-stable subspace of V, which corresponds to $W_\phi^{m_\phi(V)}$ under the non-canonical isomorphism (1.1). It follows that we obtain this time an internal, canonical

decomposition,

$$V = \bigoplus_{\phi \in \mathrm{Irr}_E(G)} V_\phi,$$

into isotypic components (note in particular that V_ϕ does not depend on the choice of W_ϕ in its isomorphism class).

For $\phi \in \mathrm{Irr}_E(G)$, let $E_\phi := \mathrm{End}_G(W_\phi)$ be its ring of endomorphisms, which is a division ring by Schur's lemma, and let d_ϕ be its dimension over E. If $E_\phi = E$, or equivalently $d_\phi = 1$, for all $\phi \in \mathrm{Irr}_E(G)$, we say that G is *E-split*. For example, if G is any finite group and E is an algebraically closed field such that $\mathrm{char}\, E \nmid |G|$, then G is E-split. It is also true that S_n is $\mathbf{Q}$-split for all $n \geq 1$ (see Section 1.3).

Furthermore, call

$$M_\phi(V) := \mathrm{Hom}_G(W_\phi, V)$$

the *multiplicity space* of ϕ in V. Strictly speaking, $M_\phi(V)$ depends on the choice of the representative W_ϕ; however, a different choice yields an isomorphic multiplicity space.

As a G-module, the multiplicity space $M_\phi(V)$ naturally carries a trivial G-action, for it can be thought of as the set of fixed points for G for its natural action by conjugation on $\mathrm{Hom}(W_\phi, V)$.

Proposition 1.2.1. *For $\phi \in \mathrm{Irr}_E(G)$, the evaluation map*

$$\mathrm{ev} : M_\phi(V) \otimes_{E_\phi} W_\phi \longrightarrow V_\phi, \qquad f \otimes w \mapsto f(w),$$

is a G-equivariant natural isomorphism.

This is essentially the content of [54, §2.6] in the case where G is E-split. We provide a proof in the general case for the sake of completeness.

Proof. For $g \in G$, $f \in M_\phi(V)$, and $w \in W_\phi$, we have

$$\mathrm{ev}(g \cdot (f \otimes w)) = \mathrm{ev}(f \otimes (g \cdot w)) = f(g \cdot w) = g \cdot f(w) = g \cdot \mathrm{ev}(f \otimes w),$$

hence the evaluation map is G-equivariant.

For naturality, let V and V' be two E-valued representations of G and consider $\varphi \in \mathrm{Hom}_G(V, V')$ a G-equivariant linear map. The following diagram is easily seen to

be commutative.

$$\begin{array}{ccc} M_\phi(V) \otimes_{E_\phi} W_\phi & \xrightarrow{\text{ev}} & V_\phi \\ {\scriptstyle \varphi_* \otimes \mathrm{Id}} \downarrow & & \downarrow {\scriptstyle \varphi} \\ M_\phi(V') \otimes_{E_\phi} W_\phi & \xrightarrow{\text{ev}} & V'_\phi \end{array}$$

Moreover, by the definition of V_ϕ, the evaluation map is clearly surjective, so that the only thing left to check is that the dimensions (as vector spaces over E) of $M_\phi(V) \otimes_{E_\phi} W_\phi$ and V_ϕ agree. As mentioned above, any isomorphism (1.1) restricts to an isomorphism $V_\phi \simeq W_\phi^{m_\phi(V)}$, so that

$$\dim V_\phi = m_\phi(V) \dim W_\phi.$$

On the other hand, using the properties of Hom we also get

$$M_\phi(V) \simeq M_\phi\Big(\bigoplus_\psi W_\psi^{m_\psi(V)} \Big) = \bigoplus_\psi M_\phi(W_\psi)^{m_\psi(V)} = E_\phi^{m_\phi(V)},$$

since $M_\phi(W_\psi) = 0$ when $\phi \neq \psi$ by Schur's lemma, and $M_\phi(W_\phi) = E_\phi$. It follows that

$$\dim \big(M_\phi(V) \otimes_{E_\phi} W_\phi \big) = \frac{\dim M_\phi(V) \dim W_\phi}{\dim E_\phi} = \frac{m_\phi(V)\, d_\phi \dim W_\phi}{d_\phi} = \dim V_\phi,$$

which concludes the proof. □

From the proof, we see that $\dim_{E_\phi} M_\phi(V) = m_\phi(V)$; the choice of an E_ϕ-basis of $M_\phi(V)$ is equivalent to the choice of an isomorphism $V_\phi \simeq m_\phi(V)\, W_\phi$. The interest of replacing the abstract multiplicity space $E_\phi^{m_\phi(V)}$ with its concrete realization $M_\phi(V) = \mathrm{Hom}_G(W_\phi, V)$ is paramount when other structures are involved, because of the functorial nature of M_ϕ.

Corollary 1.2.2. *On the category of E-valued representations of G, we have a natural isomorphism of endofunctors*

$$\mathrm{Id} = \bigoplus_{\phi \in \mathrm{Irr}_E(G)} M_\phi(-) \otimes W_\phi.$$

For example, suppose that in addition to its action by G, V is endowed with a linear action of another group H which commutes with that of G (or, equivalently, that V is a linear representation for $G \times H$). If V is semisimple as an $E[G]$-module,

then one may consider its G-isotypic decomposition

$$V = \bigoplus_{\phi \in \mathrm{Irr}_E(G)} M_\phi(V) \otimes_{E_\phi} W_\phi.$$

By naturality, this decomposition is actually $(G \times H)$-equivariant, with G acting solely on the simple modules W_ϕ and H only on the multiplicity spaces $M_\phi(V)$. Note that this holds without any semi-simplicity assumption for H.

Remark. If, in addition, $E[H]$ is semisimple, then one can decompose each multiplicity space appearing above into isotypic components for H,

$$M_\phi(V) = \bigoplus_{\psi \in \mathrm{Irr}_E(H)} M_\psi(M_\phi(V)) \otimes_{E_\psi} W_\psi,$$

and the resulting decomposition for V is naturally equivalent to its isotypic decomposition as a representation for $G \times H$, since

$$\mathrm{Irr}_E(G \times H) = \{W_\phi \boxtimes W_\psi \mid \phi \in \mathrm{Irr}_E(G), \psi \in \mathrm{Irr}_E(H)\}.$$

Moreover, if we insist that G is finite and that E has characteristic 0, then the dimension

$$\dim_E M_\phi(V) = d_\phi \dim_{E_\phi} M_\phi(V) = d_\phi \, m_\phi(V)$$

of the multiplicity space can be explicitly computed using the theory of characters. Recall that the inner product of two class functions $\chi, \psi : G \to E$ on G is defined by

$$\langle \chi, \psi \rangle := \frac{1}{|G|} \sum_{g \in G} \chi(g)\psi(g^{-1}),$$

and that if χ denotes the character of a linear representation of $G \to \mathrm{GL}(V)$, the dimension of the space of invariants is given by

$$\dim V^G = \langle \chi, \mathbf{1} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g),$$

where $\mathbf{1}$ is the trivial character. It follows that, for any irreducible representation W_ϕ,

$$\dim M_\phi(V) = \dim \mathrm{Hom}_G(W_\phi, V) = \dim \mathrm{Hom}(W_\phi, V)^G = \langle \phi^* \otimes \chi, \mathbf{1} \rangle = \langle \chi, \phi \rangle.$$

This can be viewed of as a concrete instance of the fact that characters determine semisimple representations up to isomorphism (Proposition 1.1.4).

1.3 Representations of the symmetric group

The number of irreducible representations of a finite group G over an algebraically closed field of characteristic 0 is equal to the number of conjugacy classes in G. However, there does not seem to exist a general and natural way of setting up a bijection between the conjugacy classes and the irreducible characters. The symmetric groups S_n are exceptional in this regard, because they constitute a family for which we have an explicit parametrization of the irreducible representations by the conjugacy classes. We explain this succinctly here; the reader is referred to [21, §4] or [49] for more details.

Definition 1.3.1. A *partition* of n is a multiset $\lambda = \{\lambda_1, \ldots, \lambda_m\}$, where $\lambda_1, \ldots, \lambda_m$ are positive integers such that $n = \sum_i \lambda_i$. If λ is a partition of n, we write $\lambda \vdash n$. The integers λ_i are called the *parts* of λ.

Many authors choose to standardize the notation by requiring that the parts be in decreasing order, i.e. a partition $\lambda \vdash n$ is then thought of as a sequence of integers $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m > 0$ such that $\sum_i \lambda_i = n$.

Another useful way of representing a partition is by giving the multiplicity of each part. For a partition $\lambda \vdash n$, let $d_i(\lambda)$ denote the number of times that i occurs as a part in λ. We thus obtain a *multiplicity sequence*

$$d(\lambda) = (d_1(\lambda), d_2(\lambda), \ldots)$$

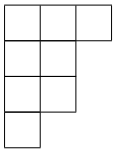
of non-negative integers with finite support. Note that $n = \sum_i i\, d_i(\lambda)$.

Any permutation $\sigma \in S_n$ partitions (in the set-theoretic sense) the set $\{1, \ldots, n\}$ into disjoint orbits $A_1, \ldots, A_m$ whose cardinalities $\lambda_i := |A_i|$ add up to n. We shall refer to

$$\lambda(\sigma) := \{\lambda_1, \ldots, \lambda_m\}$$

as the *partition associated to* σ. We also have a factorization of σ into disjoint cycles $\sigma_1, \ldots, \sigma_m$, one for each orbit, whose lengths are precisely the parts λ_i in $\lambda(\sigma)$, and it is an easy exercise to show that these lengths completely characterize the conjugacy class of σ. That is, two permutations $\sigma, \tau \in S_n$ are conjugated if and only if $\lambda(\sigma) = \lambda(\tau)$.

A partition $\lambda = \{\lambda_1 \geq \cdots \geq \lambda_m\}$ can be graphically represented by a *Young diagram* consisting of m lines, the i^{th} line being composed of λ_i left-aligned boxes. For example, the Young diagram associated to $\lambda = \{3, 2, 2, 1\}$ is the following.



A *Young tableau of shape* λ, where $\lambda \vdash n$, is obtained by numbering the boxes of the Young diagram associated to λ with the integers $1, \ldots, n$. For example,

1	2	3
4	5	
6	7	
8		

1	6	3
2	5	
8	4	
7		

3	1	4
2	8	
6	5	
7		

are 3 Young tableaux of shape $\lambda = \{3, 2, 2, 1\}$. The first one, in which the boxes are labeled in increasing order from left to right and then up to down, is the *canonical Young tableau* of shape λ. If $\mathcal{T}_\lambda$ denotes the set of Young tableaux of shape $\lambda \vdash n$, then clearly S_n acts simply transitively on $\mathcal{T}_\lambda$ by permutation of the labels. To a tableau $t \in \mathcal{T}_\lambda$, we can associate two subgroups of S_n, the stabilizer R_t of all the rows of t, and the stabilizer C_t of all the columns of t. Note that

$$R_{\sigma \cdot t} = \sigma \, R_t \, \sigma^{-1}, \qquad C_{\sigma \cdot t} = \sigma \, C_t \, \sigma^{-1}, \qquad \forall \sigma \in S_n.$$

Therefore, up to conjugation, R_t and C_t only depend on the shape λ of t. Moreover, define for every tableau t two elements r_t, c_t of the group algebra $\mathbf{Q}[S_n]$ by

$$r_t := \sum_{\sigma \in R_t} \sigma \quad \text{and} \quad c_t := \sum_{\sigma \in C_t} \mathrm{sg}(\sigma) \, \sigma,$$

and define the *Specht module associated to* t by

$$S^t := \mathbf{C}[S_n] \cdot (r_t \cdot c_t),$$

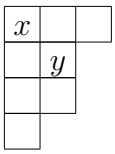
together with its linear action by S_n on the left. By previous remarks, it is easy to see that $S^t \simeq S^{t'}$ as representations of S_n if the shapes of the tableaux t and t' represent the same partition λ; we will thus refer to (the isomorphism class of) S^t by S^λ. We

have the following fundamental result.

Proposition 1.3.2. *The Specht modules S^λ, $\lambda \vdash n$, are pairwise non-isomorphic, absolutely irreducible, and form a complete set of representatives for the irreducible representations of $\mathbf{Q}[S_n]$.*

In particular, we see that S_n is $\mathbf{Q}$-split, as claimed in the previous section.

There is a combinatorial formula for the dimension of the Specht module S^λ, expressed in terms of hook lengths. The *hook length* h_x of a box x in a Young diagram is the number of boxes below it, plus the number of boxes on the right of it, plus one (for the box x itself), i.e. the total number of boxes in the "hook" pointing downward and right having its right angle at x. For example, in



we have $h_x = 3 + 2 + 1 = 6$ and $h_y = 1 + 0 + 1 = 2$.

Proposition 1.3.3 (Hook length formula)**.** *We have*

$$\dim S^\lambda = \frac{n!}{\prod_{x \in \lambda} h_x}.$$

There is another natural representation of S_n that one can associate to a partition $\mu \vdash n$. In addition to its left-action of S_n by permutation of the labels, the set $\mathcal{T}_\mu$ of Young tableaux of shape μ affords a right-action by permutation of the boxes (as they are labeled in the canonical tableau t_μ of shape μ). The stabilizer of the rows of any tableau $t \in \mathcal{T}_\mu$ is seen to be the *Young subgroup*

$$S_\mu := R_{t_\mu} \simeq S_{\mu_1} \times \cdots \times S_{\mu_m}.$$

Define the corresponding *permutation module* by

$$M^\mu := \mathbf{Q}[\mathcal{T}_\mu / S_\mu] \simeq \mathbf{Q}[S_n / S_\mu] = \mathrm{Ind}_{S_\mu}^{S_n} \mathbf{1}.$$

The multiplicities $K_{\lambda\mu}$ of the Specht modules S^λ in the decomposition of M^μ into irreducibles,

$$M^\mu \simeq \bigoplus_{\lambda \vdash n} K_{\mu\lambda}\, S^\lambda,$$

are called the *Kostka numbers*. It is possible to work out an explicitly basis of $\mathrm{Hom}_{S_n}(S^\lambda, M^\mu)$ in terms of semistandard tableaux. Given two partitions λ and μ of n, a *Young tableau of shape* λ *and content* μ is a tableau of shape λ in which the boxes have been labeled with μ_i times the integer i. For example,

$$\begin{array}{|c|c|c|}\hline 4&1&2\\\hline 5&1\\\cline{1-2} 3&2\\\cline{1-2} 1\\\cline{1-1}\end{array}\qquad\begin{array}{|c|c|c|}\hline 1&3&5\\\hline 1&2\\\cline{1-2} 2&4\\\cline{1-2} 1\\\cline{1-1}\end{array}\qquad\begin{array}{|c|c|c|}\hline 1&1&1\\\hline 2&2\\\cline{1-2} 3&5\\\cline{1-2} 4\\\cline{1-1}\end{array}$$

are 3 tableaux of shape $\lambda = \{3,2,2,1\}$ and content $\mu = \{3,2,1,1,1\}$. We say that such a tableau is *semistandard* if its entries are non-decreasing along each row, and strictly increasing along each column. In the examples above, only the third one is semistandard.

Proposition 1.3.4. *The Kostka number* $K_{\lambda\mu}$ *is the number of* semistandard Young tableaux of shape λ and content μ.

In particular, we find that $K_{\lambda\lambda} = 1$, since the only semistandard Young tableau of shape and content λ is the one in which the i^{th} line is filled with the integer i. A necessary and sufficient condition for S^λ to appear in M^μ, i.e. to have $K_{\lambda\mu} > 0$, is that λ *dominates* μ, that is,

$$\lambda_1 + \cdots + \lambda_i \geq \mu_1 + \cdots + \mu_i \qquad \text{for all } i \geq 1.$$

If λ dominates μ, we write $\lambda \trianglerighteq \mu$, and $\lambda \triangleright \mu$ if in addition $\lambda \neq \mu$. It can be seen that dominance is a partial ordering on the set of partitions. Moreover, it follows that the permutation module M^μ decomposes as

$$M^\mu \simeq S^\mu \oplus \bigoplus_{\lambda \triangleright \mu} K_{\lambda\mu}\, S^\lambda.$$

1.4 Galois representations

Of particular interest to us are linear representations of Galois groups of a number field. Let K be a number field, i.e. a finite extension of $\mathbf{Q}$. Recall that the *Galois group* of a Galois extension L/K is the group $\mathrm{Gal}(L/K)$ of all field automorphisms of

L which fix K. In particular, the *absolute Galois group* of K is

$$\mathrm{Gal}_K := \mathrm{Gal}(\overline{K}/K),$$

where $\overline{K}$ is an implicitly fixed algebraic closure of K.

For any Galois extension L/K, when have an identification as groups,

$$\mathrm{Gal}(L/K) = \varprojlim_{L'/K} \mathrm{Gal}(L'/K),$$

where L' ranges over all *finite* Galois subextensions of L/K. If we consider that all the finite groups $\mathrm{Gal}(L'/K)$ on the right-hand side carry the discrete topology, this identification defines a topology on $\mathrm{Gal}(L/K)$, the *Krull topology*, giving it the structure of a profinite group. (Of course, if L/K is finite, the resulting topology on $\mathrm{Gal}(L/K)$ is discrete.) The basic feature of this topology is the *Galois correspondence*, according to which the closed subgroups of $\mathrm{Gal}(L/K)$ are precisely the subgroups of the form $\mathrm{Gal}(L/L')$, where L' is a subextension of L/K. In particular, the continuous quotients of $\mathrm{Gal}(L/K)$ are exactly the Galois groups $\mathrm{Gal}(L'/K)$ of the Galois subextensions L' of L/K.

We have the following crucial fact, which allows one to think of any λ-adic Galois representation as being integer-valued (remember that all our representations are required to be continuous).

Proposition 1.4.1. *Let E_λ be a finite extension of $\mathbf{Q}_\ell$ with ring of integers $\mathcal{O}_\lambda$, endowed with the λ-adic topology. Any linear representation of $\mathrm{Gal}(L/K)$ on a finite-dimensional vector space V over E_λ stabilizes a full $\mathcal{O}_\lambda$-lattice.*

Proof. The Galois group $\mathrm{Gal}(K/L)$, being profinite, is compact, hence so is its image under a continuous homomorphism $\rho : \mathrm{Gal}_K \to \mathrm{GL}(V)$. The result follows from the fact that all maximal compact subgroups of $\mathrm{GL}(V) \simeq \mathrm{GL}_n(E_\lambda)$ are conjugated to $\mathrm{GL}_n(\mathcal{O}_\lambda)$. □

Given a nonzero prime ideal $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ of K, the Galois group $\mathrm{Gal}(L/K)$ acts transitively on the prime ideals $\mathfrak{P}$ of the ring of integers $\mathcal{O}_L$ of L which lie above $\mathfrak{p}$, i.e., such that $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}_L$. For such a prime $\mathfrak{P}$, let

$$D(\mathfrak{P}/\mathfrak{p}) := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

be its stabilizer, called the *decomposition group* at $\mathfrak{P}/\mathfrak{p}$. It can be identified with the Galois group of the local extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$.

Writing $k_{\mathfrak{p}}$ for the finite field $\mathcal{O}_K/\mathfrak{p}$ and $k_{\mathfrak{P}}$ for $\mathcal{O}_L/\mathfrak{P}$, one has a short exact sequence

$$1 \longrightarrow I(\mathfrak{P}/\mathfrak{p}) \longrightarrow D(\mathfrak{P}/\mathfrak{p}) \longrightarrow \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}) \longrightarrow 1, \tag{1.2}$$

which defines the *inertia group* at $\mathfrak{P}/\mathfrak{p}$ as

$$I(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}/\mathfrak{p}) \mid \sigma(x) \equiv x \bmod \mathfrak{P},\ \forall x \in \mathcal{O}_L\}.$$

Note that for $\sigma \in \mathrm{Gal}(L/K)$,

$$D(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma D(\mathfrak{P}/\mathfrak{p})\sigma^{-1} \qquad \text{and} \qquad I(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma I(\mathfrak{P}/\mathfrak{p})\sigma^{-1}. \tag{1.3}$$

Definition 1.4.2. A homomorphism $\rho : \mathrm{Gal}(L/K) \to H$ is *unramified* at $\mathfrak{p}$ if

$$I(\mathfrak{P}/\mathfrak{p}) \subseteq \mathrm{Ker}\,\rho.$$

In particular, we say that the extension L/K is unramified at $\mathfrak{p}$ if the identity homomorphism $\mathrm{Id} : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/K)$ is unramified at $\mathfrak{p}$, i.e. if $I(\mathfrak{P}/\mathfrak{p}) = 1$.

Note that, by (1.3), the definition does not depend on the choice of a prime $\mathfrak{P}$ above $\mathfrak{p}$.

Going back to the short exact sequence (1.2), we know that, since $k_{\mathfrak{p}}$ is a finite field, the residual Galois group $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is topologically generated by the *arithmetic Frobenius substitution*

$$x \mapsto x^{|k_{\mathfrak{p}}|},$$

or by its inverse, the *geometric Frobenius substitution*, which we denote $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$. Now, if we assume that $\mathfrak{p}$ is unramified in L, i.e. that $I(\mathfrak{P}/\mathfrak{p}) = 1$, then (1.2) becomes just

$$D(\mathfrak{P}/\mathfrak{p}) \simeq \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}}),$$

and we may think of $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ as an element in the decomposition group $D(\mathfrak{P}/\mathfrak{p})$. The Frobenius substitutions $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ may change when the prime $\mathfrak{P}$ above $\mathfrak{p}$ varies, but since $\mathrm{Gal}(L/K)$ acts transitively on these primes, and

$$\mathrm{Frob}(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma\,\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})\sigma^{-1} \qquad \text{for } \sigma \in \mathrm{Gal}(L/K),$$

we get a well-defined *(geometric) Frobenius conjugacy class* in $\mathrm{Gal}(L/K)$,

$$\mathrm{Frob}_{\mathfrak{p}} := \{\mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \mid \mathfrak{P} \text{ divides } \mathfrak{p}\mathcal{O}_L\}.$$

Theorem 1.4.3 (Weak Chebotarev)**.** *For a Galois extension L/K of a number field K which is unramified outside a finite set of primes S, the Frobenius conjugacy classes*

$$\mathrm{Frob}_{\mathfrak{p}}, \quad \mathfrak{p} \notin S,$$

are dense in $\mathrm{Gal}(L/K)$.

Given a finite set of primes S of K, let I_S be the closed normal subgroup of $\mathrm{Gal}(L/K)$ generated by all inertia subgroups $I(\mathfrak{P}/\mathfrak{p})$ for $\mathfrak{p} \notin S$; then the quotient

$$\mathrm{Gal}(L/K)_S := \mathrm{Gal}(L/K)/I_S$$

is the largest continuous quotient of $\mathrm{Gal}(L/K)$ which is unramified outside S. By the Galois correspondence, there exists a subextension L_S of L/K such that

$$I_S = \mathrm{Gal}(L/L_S);$$

it is the maximal subextension of L which is unramified outside S. More generally, for any topological group H, the continuous homomorphisms $\rho : \mathrm{Gal}(L/K) \to H$ that are unramified outside S are precisely those that factor through the quotient

$$\mathrm{Gal}(L/K)_S \simeq \mathrm{Gal}(L_S/K).$$

Proposition 1.4.4. *Let E be a topological field and V a finite-dimensional vector space over E, endowed with the product topology. Let ρ_1 and ρ_2 be two representations of* Gal_K *into* $\mathrm{GL}(V)$ *which are unramified outside S. Then*

$$\rho_1 \sim \rho_2 \iff \mathrm{tr}\,\rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{tr}\,\rho_2(\mathrm{Frob}_{\mathfrak{p}}) \text{ for all } \mathfrak{p} \notin S.$$

Note that since the trace is constant on conjugacy classes, the right-hand statement makes sense.

Proof. The equivalence class of a continuous representation of $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}(V)$ unramified outside S is determined by its trace, which we may view as a continuous

function on $\mathrm{Gal}(L_S/K)$, and the trace is itself determined by its restriction to a dense subset. □

Definition 1.4.5. The *Artin L-series* of a Galois representation $\rho : \mathrm{Gal}_K \to \mathrm{GL}(V)$ is the formal Dirichlet series on the monoid of non-zero ideals of $\mathcal{O}_K$ given by the formal Euler product

$$L(\rho, s) := \prod_{\mathfrak{p}} \det(1 - N(\mathfrak{p})^s \rho(\mathrm{Frob}_p) \mid V^{I_\mathfrak{p}})^{-1}.$$

Even though this Dirichlet series converges for $\mathrm{Re}\, s > \dim V$ when $E = \mathbf{C}$, it is important that we will always consider it here *formally*, in order to be able to remember the individual Euler factors at the primes of K. In particular, if ρ_1 and ρ_2 are Galois representations with finite ramification, we have

$$\rho_1 \sim \rho_2 \iff L(\rho_1) = L(\rho_2) \text{ up to finitely many Euler factors.}$$

The following is a crucially important example of ℓ-adic Galois representation.

Example 1.4.6. For any prime integer ℓ, Gal_K permutes the ℓ^{th} roots of unity $\mu_\ell(\overline{K})$ in the algebraic closure $\overline{K}$, hence acts on

$$\mu_{\ell^\infty}(\overline{K}) := \varprojlim_n \mu_{\ell^n}(\overline{K}) \simeq \varprojlim_n \mathbf{Z}/\ell^n\mathbf{Z} = \mathbf{Z}_\ell.$$

Let ψ_ℓ denote the corresponding homomorphism

$$\mathrm{Gal}_K \longrightarrow \mathrm{Aut}\, \mu_{\ell^\infty}(\overline{K}) \simeq \mathbf{Z}_\ell^\times.$$

In other words, Gal_K acts on a root of unity $\zeta \in \mu_{\ell^\infty}(\overline{K})$ by

$$\sigma \cdot \zeta = \zeta^{\psi_\ell(\sigma)}.$$

In particular, for any prime $\mathfrak{p}$ of K away from ℓ, the *arithmetic* Frobenius $\mathrm{Frob}_\mathfrak{p}^{-1}$ acts on ℓ-power roots of unity by raising to the $N(\mathfrak{p})$, so that

$$\psi_\ell(\mathrm{Frob}_\mathfrak{p}^{-1}) = N(\mathfrak{p}), \qquad (\mathfrak{p}, \ell) = 1.$$

The character ψ_ℓ could be called the *arithmetic* ℓ-adic cyclotomic character of Gal_K;

we will prefer to work instead with the *geometric ℓ-adic cyclotomic character*

$$\chi_\ell := \psi_\ell^{-1},$$

so that we have

$$\chi_\ell(\mathrm{Frob}_\mathfrak{p}) = N(\mathfrak{p}), \qquad (\mathfrak{p}, \ell) = 1.$$

It is an ℓ-adic 1-dimensional representation of Gal_K which is unramified away from ℓ. Note that its Artin L-function $L(\chi_\ell, s)$ equals the Dirichlet zeta-function $\zeta_K(s)$ of K up to the Euler factors corresponding to primes above ℓ.

For $i \in \mathbf{Z}$, and V an ℓ-adic Galois representation, we will denote by $V(i)$ the Galois module structure on V obtained by tensoring (over $\mathbf{Z}_\ell$) by the i^{th} power of the ℓ-adic cyclotomic character. This is called the i^{th} *Tate twist* of V.

Another concept we will need to use (albeit somewhat informally) for ℓ-adic representations is that of Hodge-Tate weights (see e.g. [64] or [19, ch. 5]). Let $\mathbf{C}_\ell$ denote the ℓ-adic completion of the algebraic closure of $\mathbf{Q}_\ell$, equipped with its natural Galois action by $\mathrm{Gal}_{\mathbf{Q}_\ell}$.

Definition 1.4.7. An n-dimensional ℓ-adic Galois representation V is called *Hodge-Tate* if we have a $\mathrm{Gal}_{\mathbf{Q}_\ell}$-equivariant decomposition

$$\mathbf{C}_\ell \otimes_{\mathbf{Q}_\ell} V \simeq \mathbf{C}_\ell(i_1) \oplus \cdots \oplus \mathbf{C}_\ell(i_n).$$

The integers $\mathrm{HT}(V) = \{i_1, \ldots, i_n\}$, with multiplicities, are then called the *Hodge-Tate weights* of V.

In the language of Fontaine's theory, Hodge-Tate representations are those which are B_{HT}-admissible, where B_{HT} is the graded ring

$$B_{\mathrm{HT}} = \mathbf{C}_\ell[t, t^{-1}] = \bigoplus_{i \in \mathbf{Z}} \mathbf{C}_\ell\, t^i = \bigoplus_{i \in \mathbf{Z}} \mathbf{C}_\ell(i),$$

with $\mathrm{Gal}_{\mathbf{Q}_\ell}$ acting on t via the cyclotomic character.

We will content ourselves of noting the following facts from the "yoga of weights".

- The cyclotomic character χ_ℓ is Hodge-Tate with weight 1.

- If ρ_1 and ρ_2 are Hodge-Tate, then $\rho_1 \oplus \rho_2$ and $\rho_1 \otimes \rho_2$ also are, with

$$\mathrm{HT}(\rho_1 \oplus \rho_2) = \mathrm{HT}(\rho_1) \cup \mathrm{HT}(\rho_2),$$
$$\mathrm{HT}(\rho_1 \otimes \rho_2) = \mathrm{HT}(\rho_1) + \mathrm{HT}(\rho_2).$$

- If ρ is Hodge-Tate, then $\det \rho$ also is with single weight $\sum \mathrm{HT}(\rho)$.

1.5 Compatible systems

In addition to considering a single λ-adic Galois representation, it will be needed to vary λ and consider families of representations satisfying a compatibility condition, since this is how they arise "in nature" (i.e. from étale cohomology). One should think of these different ℓ-adic incarnations of a single, "motivic" object. We now formulate a precise definition, which corresponds to what Serre calls "strictly compatible systems" in [57]. Given K and E two number fields and λ a prime of E, let S_λ denote the set of primes of K which divide $N(\lambda)$.

Definition 1.5.1. An *E-rational compatible system of λ-adic representations of degree n* of Gal_K is a family indexed by the finite places λ of E,

$$\rho = \{\rho_\lambda : \mathrm{Gal}_K \longrightarrow \mathrm{GL}_n(E_\lambda)\}_\lambda ,$$

for which there exists a finite set S of primes of K such that for every λ:

- ρ_λ is unramified outside $S \cup S_\lambda$;
- for every prime $\mathfrak{p} \notin S \cup S_\lambda$ of K, the characteristic polynomial

$$\det(1 - t\,\rho_\lambda(\mathrm{Frob}_\mathfrak{p})) \in E_\lambda[t]$$

  has coefficients in E, and does not depend on λ.

The minimal set S satisfying these two conditions, the "exceptional set" of [57], will be denoted $\mathrm{Ram}\,\rho$.

Example 1.5.2. To any representation $\rho : \mathrm{Gal}_K \to \mathrm{GL}_n(E)$ with finite ramification, one can trivially associate a compatible system by putting

$$\rho_\lambda := \rho \otimes E_\lambda.$$

This defines a canonical inclusion of the category of finitely ramified E-representations of degree n into the category of E-rational compatible systems of degree n.

This example, although seemingly innocent, is psychologically important because compatible systems are precisely the families of λ-adic representations over the completions of E which *look like* they come from a single representation over E. Note that here we think about the category of E-rational compatible systems as a full subcategory of the product of the categories of E_λ-representations. We can thus make sense in a natural way of all the operations on representations by performing them component-wise.

Example 1.5.3. If ρ is an E-rational compatible system with finite ramification, then $\det\rho$ is a 1-dimensional E-rational compatible system with $\mathrm{Ram}(\det\rho) \subseteq \mathrm{Ram}\,\rho$.

Example 1.5.4. The *cyclotomic character* $\chi_{\mathrm{cycl}} := (\chi_\ell)_\ell$ is a $\mathbf{Q}$-rational compatible system of ℓ-adic representations of Gal_K with $\mathrm{Ram}\,\chi_{\mathrm{cycl}} = \varnothing$.

If $\rho = (\rho_\lambda)_\lambda$ is an E-rational compatible system of λ-adic representations, then all the individual representations share the same Artin L-function at all unramified primes, i.e. up to finitely many Euler factors, and we can consider this to be the L-function attached to ρ. To be precise, we let

$$L(\rho, s) := \prod_{\mathfrak{p}\notin\mathrm{Ram}\,\rho} \det(1 - N(\mathfrak{p})^s\,\rho_\lambda(\mathrm{Frob}_\mathfrak{p}))^{-1},$$

where the choice of λ away from $\mathfrak{p}$ in the Euler factor at $\mathfrak{p}$ is immaterial. If ρ is a compatible system of *continuous* λ-adic representations, $L(\rho, s)$ completely characterizes ρ^{ss}, the semisimple compatible system associated to ρ.

Example 1.5.5. For the trivial representation $\mathbf{1}$ of Gal_K, considered as a compatible system, we have

$$L(\mathbf{1}, s) = \prod_\mathfrak{p} \frac{1}{1 - N(\mathfrak{p})^s} = \zeta_K(s),$$

the Dedekind zeta function of K.

Example 1.5.6. For the r^{th} power of the cyclotomic character of K, we have

$$L(\chi_{\mathrm{cycl}}^r, s) = \prod_\mathfrak{p} \frac{1}{1 - N(\mathfrak{p})^{s+r}} = \zeta_K(s + r).$$

More generally, if ρ is any compatible system of representations of Gal_K, then for its r^{th} Tate twist $\rho \otimes \chi_{\text{cycl}}^r$ we have

$$L(\rho \otimes \chi_{\text{cycl}}^r, s) = L(\rho, s + r).$$

A very important family of 2-dimensional compatible systems are those attached to modular forms by Deligne (see [47] for an exposition). A compatible system of representations $\rho = (\rho_\lambda)_\lambda$ is said to have *Hodge-Tate weights* $\mathrm{HT}(\rho)$ if all the individual λ-adic representations are Hodge-Tate with the same weights $\mathrm{HT}(\rho_\lambda) = \mathrm{HT}(\rho)$.

Proposition 1.5.7. *Let f be a Hecke newform of weight k, level N and Nebentypus ε, i.e. $f \in S_k^{\text{new}}(N, \varepsilon)$, and let $E = \mathbf{Q}(f)$ be the number field generated by its Fourier coefficients. There exists a 2-dimensional E-rational compatible system of representations ρ_f of $\mathrm{Gal}_{\mathbf{Q}}$, with $\mathrm{HT}(\rho_f) = \{0, k-1\}$, unramified away from N, such that*

$$\det \rho_f = \varepsilon \otimes \chi_{\text{cycl}}^{k-1}$$

and

$$\operatorname{tr} \rho_f(\mathrm{Frob}_p) = a_p(f), \qquad \text{for all } p \nmid N.$$

In particular, the L-function $L(\rho_f, s)$ is equal to the Mellin transform of f up to Euler factors for $p \mid N$. Note that these factors are completely determined by those for $p \mid N$ by "multiplicity 1" for newforms.

Chapter 2

Étale cohomology

We will want to study in Chapter 4 the distribution of certain exponential sums via their moments, which can in turn be expressed in terms of the number of points on projective hypersurfaces defined by equations of the form

$$\sum_{i=1}^{m} x_i = \sum_{j=1}^{n} y_j, \quad \sum_{i=1}^{m} x_i^k = \sum_{j=1}^{n} y_j^k. \tag{2.1}$$

As is often the case, this counting problem can be conveniently treated using étale cohomology, and this chapter lays down the relevant facts to be used in the sequel. We first describe in Section 2.1 the construction and some of the properties of the λ-adic cohomology groups

$$H^\bullet(X, \mathcal{F}_\lambda)$$

of a variety defined over a number field K with values in a λ-adic constructible sheaf $\mathcal{F}_\lambda$. If we let $\mathcal{F}_\lambda$ vary along a compatible system of λ-adic sheaves, the graded Galois representations afforded by the cohomology groups form a compatible system thanks to the Grothendieck trace formula (Section 2.2). In particular, if we take sheaves with trivial Galois action by Gal_K, such as the various λ-adic completions of a number field E, we recover the number of points of the reductions of X over finite fields as the alternating trace of Frobenius morphisms on the cohomology.

The varieties defined by the equations (2.1) above are often smooth, but may be singular in general. The singularities will be seen in the next chapter (Section 3.4) to consist of isolated ordinary double points, i.e. points which become smooth quadrics when blown-up. Accordingly, we proceed to discuss the cohomology of smooth hypersurfaces in Section 2.3, which is particularly simple since the Lefschetz hyperplane

theorem implies that only the middle-degree cohomology carries non-trivial information. The special case of smooth quadrics in then described in some more details in Section 2.4. In the last pages (Section 2.5), we describe the results of Schoen [50] about the cohomology of singular hypersurfaces of odd dimension whose only singularities are ordinary double points, and treat as well the case of even dimension.

2.1 Basic properties

In this section, we roughly describe how étale cohomology is defined, and then state without any attempt of proof some of its formal properties. The reader is referred to [24] for a quick overview, to [42] for a readable account, to [62, 20] for more details, and of course to the SGA for the source, in particular [14].

Let $\mathbf{F}$ be an separably closed field, and X a scheme over $\mathbf{F}$. As well as the category X_{Zar} of Zariski open sets of X, one may consider with Grothendieck *et al.* the larger category $X_{\text{ét}}$ of étale open sets of X, together with the natural "continuous" map

$$\iota : X_{\text{ét}} \longrightarrow X_{\mathrm{Zar}}.$$

At the level of sheaves, ι induces an *etalization map* $\iota^* : \mathcal{S}\mathrm{h}(X_{\mathrm{Zar}}) \to \mathcal{S}\mathrm{h}(X_{\text{ét}})$. Since the category $\mathcal{S}\mathrm{h}(X_{\text{ét}})$ of étale sheaves has enough injectives, sheaf cohomology, as the right derived functor to the global sections, is defined. Hence, for any Zariski sheaf $\mathcal{F} \in \mathcal{S}\mathrm{h}(X_{\mathrm{Zar}})$, we can define the *étale cohomology groups of X with values in $\mathcal{F}$* as

$$H^\bullet_{\text{ét}}(X, \mathcal{F}) := H^\bullet(X_{\text{ét}}, \iota^*\mathcal{F}).$$

Definition 2.1.1. Let E_λ be a local number field with ring of integers $\mathcal{O}_\lambda$. A *λ-adic constructible sheaf* on a topological space X is a constructible sheaf $\mathcal{F}_\lambda$ of E_λ-vector spaces together with a co-filtration $(\mathcal{F}_{\lambda,n})_{n\geq 1}$, where $\mathcal{F}_{\lambda,n}$ is a sheaf of $\mathcal{O}_\lambda/\lambda^n$-modules and

$$\mathcal{F}_\lambda = \big(\varprojlim_n \mathcal{F}_{\lambda,n}\big) \otimes_{\mathcal{O}_\lambda} E_\lambda.$$

We define the i^{th} *étale cohomology group of X with coefficients in $\mathcal{F}_\lambda$* as

$$H^i(X, \mathcal{F}_\lambda) := \big(\varprojlim_n H^i_{\text{ét}}(X, \mathcal{F}_{\lambda,n})\big) \otimes_{\mathcal{O}_\lambda} E_\lambda,$$

and write $H^\bullet(X, \mathcal{F}_\lambda)$ for the graded vector space

$$H^\bullet(X, \mathcal{F}_\lambda) = \bigoplus_i H^i(X, \mathcal{F}_\lambda).$$

In the case where X is defined over a perfect field K, we define

$$H^\bullet(X, \mathcal{F}_\lambda) := H^\bullet(X_{\overline{K}}, \mathcal{F}_\lambda|_{X_{\overline{K}}}),$$

where $X_{\overline{K}} = X \otimes \overline{K}$ denotes the base-change of X to $\overline{K}$. When $\mathcal{F}_\lambda$ is the constant sheaf E_λ, we will refer to $H^\bullet(X, E_\lambda)$ as *the* λ-adic cohomology of X.

Proposition 2.1.2 (Functoriality)**.** *A morphism $f : X \to Y$ of K-schemes induces a natural map*

$$f^* : H^\bullet(Y, \mathcal{F}_\lambda) \longrightarrow H^\bullet(X, f^*\mathcal{F}_\lambda)$$

for any λ-adic constructible sheaf $\mathcal{F}_\lambda$ on Y.

In particular, if G is any group of scheme automorphisms of X and $\mathcal{F}_\lambda$ a G-equivariant constructible sheaf on X (in the sense that $g^*\mathcal{F}_\lambda = \mathcal{F}_\lambda$ for all $g \in G$), then $H^\bullet(X, \mathcal{F}_\lambda)$ is naturally endowed with a linear action from G.

Note that when $\mathcal{F}$ is a sheaf on X, then $\mathcal{F}|_{X_{\overline{K}}}$ is a Gal_K-equivariant sheaf on $X_{\overline{K}}$, so that

$$H^\bullet(X, \mathcal{F}) = H^\bullet(X \otimes \overline{K}, \mathcal{F} \otimes \overline{K})$$

inherits a Galois action from Gal_K to which we will return in Section 2.2 below.

In addition to being well-behaved on the category of schemes, étale cohomology shares a lot of formal properties with Betti cohomology.

Proposition 2.1.3 (Finiteness)**.** *If X is a scheme of finite type over a perfect field and $\mathcal{F}_\lambda$ a λ-adic constructible sheaf on X, the étale cohomology groups*

$$H^i(X, \mathcal{F}_\lambda)$$

vanish unless $0 \leq i \leq 2 \dim X$. If in addition X is proper, they all have finite dimension as vector spaces over E_λ.

Proposition 2.1.4 (Poincaré duality)**.** *If X is smooth and separated, there exists a natural cup-product pairing*

$$\cup : H^i(X, E_\lambda) \otimes H^j(X, E_\lambda) \longrightarrow H^{i+j}(X, E_\lambda),$$

which is non-degenerate when $i + j = 2 \dim X$.

It is also true that étale cohomology agrees with Betti cohomology "as much as it possibly could".

Proposition 2.1.5 (Comparison theorem)**.** *If X is a smooth variety over a number field, the choice of an embedding $E_\lambda \hookrightarrow \mathbf{C}$ induces an isomorphism*

$$H^\bullet(X, E_\lambda) \otimes_{E_\lambda} \mathbf{C} \simeq H^\bullet_{\mathrm{Bet}}(X(\mathbf{C}), \mathbf{C}).$$

Recall that as a complex variety, we have a Hodge decomposition

$$H^i_{\mathrm{Bet}}(X(\mathbf{C}), \mathbf{C}) = H^i_{\mathrm{dR}}(X(\mathbf{C}), \mathbf{C}) = \bigoplus_{p+q=i} H^{p,q}(X(\mathbf{C}), \mathbf{C}).$$

The comparison isomorphism also preserves the Hodge structures on both sides, in the following sense. If we set

$$h^{p,q} := \dim H^{p,q}(X(\mathbf{C}), \mathbf{C}) = \dim H^q(X(\mathbf{C}), \Omega^p),$$

then $h^{p,q}$ is the multiplicity of p in $\mathrm{HT}(H^i(X, E_\lambda))$. In particular, since $h^{p,q} = h^{q,p}$, we see that the multiset of Hodge-Tate weights of $H^i(X, E_\lambda)$ is invariant under the involution $p \mapsto i - p$.

The following fact is also crucial to describe the residual Galois representations on étale cohomology at primes of good reduction. Recall that the spectrum of a Henselian discrete valuation ring (such as the ring of integers in a local number field) is called a *Henselian trait*.

Proposition 2.1.6 (Smooth base change)**.** *Let $\mathcal{X}$ be a smooth proper scheme over a Henselian trait with generic fiber X and special fiber $X_\mathfrak{p}$, and $\mathcal{F}_\lambda$ a λ-adic constructible locally constant sheaf on $\mathcal{X}$ where λ is coprime with the characteristic of the base field. Then the natural maps*

$$H^\bullet(X, \mathcal{F}_\lambda|_X) \longleftarrow H^\bullet(\mathcal{X}, \mathcal{F}_\lambda) \longrightarrow H^\bullet(X_\mathfrak{p}, \mathcal{F}_\lambda|_{X_\mathfrak{p}})$$

are isomorphisms.

In particular, let X be a smooth proper variety defined over a number field K and $\mathfrak{p}$ a prime of good reduction for X. This means that there exists a smooth proper model

$\mathcal{X}$ of X over $\operatorname{Spec} K_{\mathfrak{p}}$, which carries an action of the decomposition group $D_{\mathfrak{p}} \subseteq \mathrm{Gal}_K$. The functorial isomorphism given by smooth base change tells us that

$$H^\bullet(X, \mathcal{F}_\lambda|_X) \simeq H^\bullet(X_{\mathfrak{p}}, \mathcal{F}_\lambda|_{X_{\mathfrak{p}}})$$

as representations for $D_{\mathfrak{p}}$. But the action on the right-hand side factors through the residual Galois group $\mathrm{Gal}_{k_{\mathfrak{p}}}$, so we conclude that the inertia group $I_{\mathfrak{p}}$ acts trivially on the left-hand side as well. We conclude the following.

Corollary 2.1.7. *If X is a smooth proper variety defined over a number field K, the Galois representation of Gal_K on $H^\bullet(X, E_\lambda)$ is unramified outside the primes of bad reduction of X. In particular, it has finite ramification.*

2.2 The trace formula and purity

Weil [66] remarked early on that an analogue of the Lefschetz trace formula for the Frobenius automorphism of a variety defined over a finite field would be highly desirable, since it would allow to study the number of points of that variety using cohomological methods. Such a formula was proved first by Grothendieck in the version that we state here, then later generalized by Verdier.

Theorem 2.2.1 (Trace formula)**.** *Let X be a smooth, proper variety over $\mathbf{F}_q$ and $\mathcal{F}_\lambda$ a λ-adic constructible sheaf on X with λ away from q. For the geometric Frobenius morphism Frob_q, we have*

$$\sum_{x \in X(\mathbf{F}_{q^r})} \operatorname{tr}(\mathrm{Frob}_q \mid \mathcal{F}_{\lambda,x}) = \sum_{i=0}^{2\dim X} (-1)^i \operatorname{tr}(\mathrm{Frob}_q \mid H^i(X, \mathcal{F}_\lambda)),$$

or, more concisely, considering the right-hand side as a trace in the graded sense:

$$\operatorname{tr}(\mathrm{Frob}_q \mid \mathcal{F}_{\lambda, X(\mathbf{F}_{q^r})}) = \operatorname{tr}(\mathrm{Frob}_q \mid H^\bullet(X, \mathcal{F}_\lambda)).$$

Definition 2.2.2. Let X be a smooth, proper variety defined over $\mathbf{F}_q$ and $\mathcal{F}_\lambda$ a constructible λ-adic sheaf. The *zeta function of X with coefficients in $\mathcal{F}_\lambda$* is the formal series

$$Z(X, \mathcal{F}_\lambda; t) := \exp\left\{ \sum_{r=1}^{\infty} \operatorname{tr}(\mathrm{Frob}_q^r \mid \mathcal{F}_{\lambda, X^F}) \frac{t^r}{r} \right\} \in E_\lambda[[t]].$$

In particular, when $\mathcal{F}_\lambda = E_\lambda$, as Frobenius acts trivially on the stalks, we have

$$\mathrm{tr}(\mathrm{Frob}_q^r \mid \mathcal{F}_{\lambda, X(\mathbf{F}_{q^r})}) = |X(\mathbf{F}_{q^r})|,$$

and the zeta function $Z(X, E_\lambda; t)$ is just a generating series for the number of points of X over all finite extensions $\mathbf{F}_{q^r}$ of $\mathbf{F}_q$.

Corollary 2.2.3. *The zeta function of a smooth, proper variety X defined over $\mathbf{F}_q$ with coefficients in $\mathcal{F}_\lambda$ can be written as*

$$Z(X, \mathcal{F}_\lambda; t) = \det(1 - t\,\mathrm{Frob}_q \mid H^\bullet(X, \mathcal{F}_\lambda))^{-1}.$$

In particular, it is a rational function of t with coefficients in E_λ.

Proof. If X is defined over $\mathbf{F}_q$, then for any $r \geq 1$ we may consider X as defined over $\mathbf{F}_{q^r}$, and since $\mathrm{Frob}_{q^r} = \mathrm{Frob}_q^r$, the trace formula implies that

$$\mathrm{tr}(\mathrm{Frob}_q^r \mid \mathcal{F}_{\lambda, X^F}) = \mathrm{tr}(\mathrm{Frob}_q^r \mid H^\bullet(X, \mathcal{F}_\lambda)), \qquad r \geq 1.$$

The conclusion follows by taking the exponential on both sides of the definition of the zeta function and using Lemma 1.1.5. □

Now suppose that X is a global variety defined over a number field K. By smooth base change, for every prime $\mathfrak{p}$ of good reduction for X, if $\mathcal{F}_\lambda$ is a λ-adic constructible sheaf on X which extends to a smooth model $\mathcal{X}$, we have

$$H^\bullet(X, \mathcal{F}_\lambda) \simeq H^\bullet(X_\mathfrak{p}, \mathcal{F}_\lambda|_{X_\mathfrak{p}})$$

as representations for the decomposition group $D_\mathfrak{p}$ at $\mathfrak{p}$, so that

$$\det(1 - t\,\mathrm{Frob}_\mathfrak{p} \mid H^\bullet(X, \mathcal{F}_\lambda)) = \det(1 - t\,\mathrm{Frob}_\mathfrak{p} \mid H^\bullet(X_\mathfrak{p}, \mathcal{F}_\lambda)).$$

It follows that the *(global) zeta function of X*,

$$\zeta(X, \mathcal{F}_\lambda; s) := L(H^\bullet(X, \mathcal{F}_\lambda), s),$$

defined as the Artin L-function (in the graded sense) of its étale cohomology viewed

as a representation for Gal_K, factors up to finitely many Euler factors as

$$\zeta(X, \mathcal{F}_\lambda, s) = \prod_{\text{good } \mathfrak{p}} Z(X_\mathfrak{p}, \mathcal{F}_\lambda|_{X_\mathfrak{p}}; N(\mathfrak{p})^{-s}).$$

It is then natural to consider compatible families of λ-adic sheaves in order to obtain a compatible system of λ-adic representations from étale cohomology.

Definition 2.2.4. A family $\mathcal{F} = (\mathcal{F}_\lambda)_\lambda$ of λ-adic constructible sheaves on X will be called *compatible* if for all primes $\mathfrak{p}$ of good reduction for X, the number

$$\mathrm{tr}(\mathrm{Frob}_\mathfrak{p}^r \mid \mathcal{F}_{\lambda, X_\mathfrak{p}(\mathbf{F}_{q^r})}) \in E_\lambda$$

actually lies in E and is independent on the choice of λ away from $\mathfrak{p}$.

In particular, if $\mathcal{F}$ is a constructible sheaf of E-vector spaces on X, then $(\mathcal{F} \otimes E_\lambda)_\lambda$ is a compatible family of λ-adic sheaves on X which could still be denoted $\mathcal{F}$ by abuse of notation. The following follows at once from the trace formula.

Corollary 2.2.5. *Let X be a scheme of finite type over a perfect field K, E a number field and $\mathcal{F}$ a compatible system of λ-adic constructible sheaves on X. Then*

$$H^\bullet(X, \mathcal{F}) := \left(H^\bullet(X \otimes \overline{K}, \mathcal{F}_\lambda)\right)_\lambda$$

is a compatible system of graded λ-adic representations of Gal_K.

It should also be mentioned that Deligne, in his celebrated paper [13], completed the proof of the Weil conjectures by proving the Riemann hypothesis for varieties over finite fields.

Theorem 2.2.6 (Purity)**.** *Let X be a smooth proper variety over $\mathbf{F}_q$ and $\mathcal{F}_\lambda$ a λ-adic constructible sheaf on X. If all the eigenvalues of* Frob_q *on the stalks $\mathcal{F}_{\lambda,x}$ are* pure of weight *a, i.e. have absolute value $q^{a/2}$ under every embedding $E_\lambda \hookrightarrow \mathbf{C}$, then all the eigenvalues of* Frob_q *on $H^i(X, \mathcal{F}_\lambda)$ are pure of weight $a + i$.*

In particular, if we take $\mathcal{F}_\lambda$ to be the constant sheaf E_λ, on which Frobenius acts trivially hence purely of weight 0, then all the eigenvalues of Frob_q on $H^i(X, E_\lambda)$ are pure of weight i. One of the striking applications of purity is giving bounds on certain exponential sums; more on this in Chapter 4.

2.3 Smooth hypersurfaces

This section is devoted to the cohomology of smooth projective hypersurfaces, both from the geometric and Galois points of view. We start by describing the cohomology of projective space, since the Lefschetz hyperplane theorem states that the cohomology of a smooth hypersurface is *almost* the same as that of the ambient projective space.

Let X be a variety defined over a perfect field K and let $\mathrm{CH}^\bullet(X)$ denote its Chow ring, i.e. $\mathrm{CH}^i(X)$ is the free abelian group on the subvarieties (defined over K) of X of codimension i, modulo linear equivalence, the product on the graded module $\mathrm{CH}^\bullet(X)$ being given by

$$\cap : \mathrm{CH}^i(X) \otimes \mathrm{CH}^j(X) \longrightarrow \mathrm{CH}^{i+j}(X), \qquad [Z_1] \cap [Z_2] = [Z_1 \cap Z_2],$$

when Z_1 and Z_2 meet transversally.

Proposition 2.3.1 (Cycle class map)**.** *There exists a functorial homomorphism of graded compatible systems of algebras given by*

$$\gamma : \mathrm{CH}^i(X)(i) \longrightarrow H^{2i}(X, E_\lambda).$$

Recall that the notation $M(i)$ refers to the i^{th} Tate twist of M (cf. Example 1.5.6).

In the case of projective space $\mathbf{P}^n$, it is well known that

$$\mathrm{CH}^i(\mathbf{P}^n) = \langle \gamma[H]^i \rangle,$$

where $H \simeq \mathbf{P}^{n-1}$ is any hyperplane, and that the cycle class map is actually a bijection onto $H^\bullet(\mathbf{P}^n)$. Thus, as a graded compatible system,

$$H^\bullet(\mathbf{P}^n) = \{\chi_{\mathrm{cycl}}^0 \;\; 0 \;\; \chi_{\mathrm{cycl}}^1 \;\; 0 \;\; \chi_{\mathrm{cycl}}^2 \;\; \cdots \;\; 0 \;\; \chi_{\mathrm{cycl}}^n\},$$

where χ_{cycl}^i is the action on $H^{2i}(\mathbf{P}^n)$. This could also have been deduced from the fact that over every finite field $\mathbf{F}_q$,

$$|\mathbf{P}^n(\mathbf{F}_q)| = \frac{q^{n+1}-1}{q-1} = 1 + q + q^2 + \cdots + q^n,$$

together with the trace formula.

Now suppose that X is a smooth hypersurface in $\mathbf{P}^{n+1}$. The following result states that the only interesting cohomology of X occurs in the middle degree n.

Proposition 2.3.2 (Lefschetz hyperplane theorem)**.** *If j denotes the inclusion of a smooth hypersurface X in $\mathbf{P}^{n+1}$, then*

$$j^* : H^i(\mathbf{P}^{n+1}) \longrightarrow H^i(X)$$

is an isomorphism for $i < n$, and is injective for $i = n$.

Remark. From Poincaré duality, it follows that j^* is also an isomorphism above the middle degree. Indeed, for $n < i \leq 2n$, consider the following commutative diagram.

$$\begin{array}{ccccc} H^i(\mathbf{P}^{n+1}) & \otimes & H^{2n-i}(\mathbf{P}^{n+1}) & \xrightarrow{\cup} & H^{2n}(\mathbf{P}^{n+1}) \\ \downarrow{\scriptstyle j^*} & & \simeq\downarrow{\scriptstyle j^*} & & \simeq\downarrow{\scriptstyle j^*} \\ H^i(X) & \otimes & H^{2n-i}(X) & \xrightarrow{\cup} & H^{2n}(X) \end{array}$$

The Lefschetz hyperplane theorem guarantees that j^* is an isomorphism in degree $2n - i < n$. Note that j^* is known to be an isomorphism in degree $2n$, since it maps the generator $\gamma[H]^n$ of $H^{2n}(\mathbf{P}^{n+1})$, the class of a line, to $\deg X$ points in $H^{2n}(X)$. It then follows by taking duals that j^* is an isomorphism in degree i as well.

In degree n, it is actually possible to define a canonical complement to $j^*H^n(\mathbf{P}^{n+1})$, the *primitive cohomology* $H^n_{\mathrm{pr}}(X)$ of X, using the hard Lefschetz theorem. Of course, if n is odd, there is nothing to do as $H^n(\mathbf{P}^{n+1}) = 0$.

Corollary 2.3.3. *If X is a smooth hypersurface of dimension n, we have*

$$H^\bullet(X) \simeq H^\bullet(\mathbf{P}^n) \oplus H^n_{\mathrm{pr}}(X)$$

as graded compatible systems.

Proof. For $i < n$, by the Lefschetz hyperplane theorem, we have

$$H^i(X) \simeq H^i(\mathbf{P}^{n+1}) \simeq H^i(\mathbf{P}^n),$$

i.e. 0 if i is odd and $\chi_{\mathrm{cycl}}^{i/2}$ if i is even. For $i = n$, we similarly have

$$H^n(X) = H^n(\mathbf{P}^{n+1}) \oplus H^n_{\mathrm{pr}}(X) \simeq H^n(\mathbf{P}^n) \oplus H^n_{\mathrm{pr}}(X).$$

For $i > n$, by Poincaré duality it follows that

$$H^i(X) \simeq H^{2n-i}(X)^\vee(n) = H^{2n-i}(X)^\vee \otimes \chi_{\mathrm{cycl}}^n,$$

from which the conclusion follows. □

It is possible, using the Riemann-Roch-Hirzebruch formula, to give a general formula for the Hodge numbers of the primitive cohomology of a smooth complete intersection over $\mathbf{C}$ ([25, app. 1] and [12]). In the case of smooth hypersurfaces, we have the following. For $p+q=n$, let $h_d^{p,q}$ denote the Hodge numbers of the primitive cohomology of a smooth hypersurface of degree d and dimension n, and let

$$\mathcal{H}_d(x,y) := \sum_{p,q\geq 0} h_d^{p,q} x^p y^q.$$

Proposition 2.3.4. *The generating series $\mathcal{H}_d(x,y)$ for the primitive Hodge numbers of smooth hypersurfaces of degree d is*

$$\mathcal{H}_d(x,y) = \frac{(1+x)^{d-1} - (1+y)^{d-1}}{x(1+y)^d - y(1+x)^d}.$$

In particular, evaluating this expression at $x=y$ (and using the formal L'Hôpital rule for the right-hand side) yields the following formula for the dimension of the primitive cohomology of smooth hypersurfaces.

Corollary 2.3.5. *If X is a smooth hypersurface of degree d and dimension n, t hen*

$$\dim H^n_{\mathrm{pr}}(X) = \frac{(d-1)^{n+2} + (-1)^n(d-1)}{d}.$$

For example, if $n=0$, we find $\dim H^0_{\mathrm{pr}}(X) = d-1$, as it should. Similarly, when X is a smooth curve, we recover the classical degree-genus formula

$$\dim H^1(X) = 2\binom{d-1}{2}.$$

Moreover, if $d=1$, so that $X \simeq \mathbf{P}^n$ is an hyperplane in $\mathbf{P}^{n+1}$, the primitive cohomology of X vanishes.

Recall that the *Euler characteristic* of X is defined in general by

$$\chi(X) := \mathrm{tr}(\mathrm{Id} \mid H^\bullet(X)) = \sum_{i=0}^{2\dim X} (-1)^i \dim H^i(X).$$

Corollary 2.3.6. *The Euler characteristic of a smooth projective hypersurface X of*

degree d and dimension n is given by

$$\chi(X) = n + 2 + \frac{(1-d)^{n+2} - 1}{d}.$$

Proof. This follows at once from Corollary 2.3.3, which implies that

$$\chi(X) = \chi(\mathbf{P}^n) + (-1)^n \dim H_{\mathrm{pr}}(X) = n + 1 + (-1)^n \dim H_{\mathrm{pr}}(X),$$

together with the formula of Corollary 2.3.5. □

We now turn to a description of structure of Galois module afforded by the primitive cohomology of a smooth hypersurface, which can in some situations be studied by elementary means, *à la* Weil, using Gauss and Jacobi sums to count points on the hypersurface. Recall that the *Gauss sum* associated to a multiplicative character $\chi : \mathbf{F}_q^\times \to \mathbf{C}^\times$ of the finite field $\mathbf{F}_q$ of characteristic p is defined by

$$g(\chi) := \sum_{x \in \mathbf{F}_q^\times} \chi(x) \exp\left(\frac{2\pi i}{p} \operatorname{tr}_{\mathbf{F}_q/\mathbf{F}_p}(x)\right).$$

For the rest of this section, let X be the *diagonal hypersurface* in $\mathbf{P}^{n-1}$ defined by

$$\sum_{i=1}^{n} a_i x_i^k = 0. \tag{2.2}$$

Provided k is invertible in the base field, X is smooth if and only if $a_i \neq 0$ for all i.

Proposition 2.3.7 ([27, §11.3, th. 2])**.** *Let X be the diagonal hypersurface (2.2) of dimension $n-2$ over the field $\mathbf{F}_q$, with $a_i \neq 0$, $q \equiv 1 \bmod k$. The zeta function of X is given by*

$$Z(X/\mathbf{F}_q; t) = \frac{P(t)^{(-1)^{n+1}}}{(1-t)(1-qt)\cdots(1-q^{n-2}t)},$$

where $P(t)$ is the polynomial

$$\prod \left(1 - \frac{(-1)^n}{q} \prod_{i=1}^{n} \chi_i(a_i^{-1}) g(\chi_i) t\right),$$

the product ranging over all n-tuples $(\chi_1, \ldots, \chi_n)$ of multiplicative characters of $\mathbf{F}_q$ such that $\chi_i^k = \mathbf{1}$, $\chi_i \neq \mathbf{1}$ and $\chi_1 \cdots \chi_n = \mathbf{1}$.

From Corollary 2.3.3, the polynomial $P(t)$ appearing above is nothing but the characteristic polynomial of Frob_q on $H^{n-2}_{\mathrm{pr}}(X)$. In particular, using the fact that $|g(\chi)| = \sqrt{q}$ for any Gauss sum over $\mathbf{F}_q$, we find that the eigenvalues of Frobenius on the primitive cohomology have absolute value

$$\left| \frac{(-1)^n}{q} \prod_{i=1}^{n} \chi_i(a_i^{-1}) g(\chi_i) \right| = \frac{1}{q} \prod_{i=1}^{n} |\chi_i(a_i^{-1})||g(\chi_i)| = \frac{1}{q} \prod_{i=1}^{n} q^{1/2} = q^{(n-2)/2},$$

in accordance with purity. (This was actually one of the examples which led Weil to formulate his conjectures.)

The degree of $P(t)$ is the number of n-tuples of characters $(\chi_1, \ldots, \chi_n)$ appearing in Proposition 2.3.7. For fixed number of variables n and degree k, let

$$\begin{aligned} \Omega_{n,k} &:= \{(\chi_1, \ldots, \chi_n) \mid \chi_i \in \widehat{\mathbf{F}_q^\times}, \chi_i^k = \mathbf{1}, \chi_i \neq \mathbf{1}\} \quad \text{and} \\ D_{n,k} &:= \{(\chi_1, \ldots, \chi_n) \in \Omega_{n,k} \mid \chi_1 \cdots \chi_n = \mathbf{1}\}. \end{aligned}$$

As $\Omega_{n,k} \setminus D_{n,k}$ is in bijection with $D_{n+1,k}$ via $(\chi_1, \ldots, \chi_n) \mapsto (\chi_1, \ldots, \chi_n, (\chi_1 \cdots \chi_n)^{-1})$, we have

$$|\Omega_{n,k}| = |D_{n,k}| + |\Omega_{n,k} \setminus D_{n,k}| = |D_{n,k}| + |D_{n+1,k}|.$$

Since by assumption k divides the order of the cyclic group $\widehat{\mathbf{F}_q^\times}$, $|\Omega_{n,k}| = (k-1)^n$. It follows that $|D_{n,k}|$ satisfies the recurrence equation

$$|D_{n+1,k}| = (k-1)^n - |D_{n,k}|, \quad n \geq 1,$$

with initial condition $|D_{1,k}| = 0$. By an easy induction argument, one finds that

$$|D_{n,k}| = \frac{(k-1)^n + (-1)^n(k-1)}{k},$$

which is precisely the dimension of the primitive cohomology of X according to Proposition 2.3.5.

2.4 Smooth quadrics

We now specialize the discussion of the previous section to smooth quadrics over perfect fields. A projective quadric Q of dimension n in $\mathbf{P}^{n+1}$ is defined by the vanishing of a homogeneous quadratic polynomial $f(\mathbf{x})$, which over a perfect field $\mathbf{F}$

of characteristic different than 2 can be written as

$$f(\mathbf{x}) = \mathbf{x}^t A\mathbf{x},$$

where A is a symmetric matrix with coefficients in $\mathbf{F}$. Using Gauss-Lagrange reduction on the matrix A, we can find an invertible matrix B such that

$$B^t AB = \operatorname{diag}(a_1, \ldots, a_{n+2}),$$

hence the quadric Q is projectively equivalent to the diagonal quadric

$$\sum_{i=1}^{n+2} a_i x_i^2 = 0.$$

Since diagonal hypersurfaces are smooth if and only if none of their coefficients vanish, it follows that Q is smooth if and only if

$$\det A = (\det B)^2 \prod_{i=1}^{n+2} a_i \neq 0.$$

Now, if Q is smooth, by Corollary 2.3.5, we have

$$\dim H^n_{\mathrm{pr}}(Q) = \frac{1 + (-1)^n}{2} = \begin{cases} 0 & \text{for } n \text{ odd}, \\ 1 & \text{for } n \text{ even}. \end{cases}$$

Hence, when n is odd, from Corollary 2.3.3 we have the following.

Proposition 2.4.1. *If Q is a smooth quadric of odd dimension n, then*

$$H^\bullet(Q) \simeq H^\bullet(\mathbf{P}^n).$$

Now, if Q is a smooth quadric of even dimension, its primitive cohomology is 1-dimensional and we will now determine explicitly the Galois representation it carries. We first make a definition.

Definition 2.4.2. Let Q be a smooth quadric over $\mathbf{F}$ of dimension $n = 2r$ defined by the homogeneous equation $\mathbf{x}^t A\mathbf{x}$, where A is a symmetric $(n+2) \times (n+2)$ matrix.

The *signed discriminant* of Q is defined to be

$$\Delta(Q) := (-1)^{r+1} \det A \in \mathbf{F}^\times/(\mathbf{F}^\times)^2.$$

Note that since the signed discriminant $\Delta(Q)$ is only considered modulo squares, it does not depend on the choice of a matrix A and thus only depends on the projective quadric Q.

Proposition 2.4.3. *Let Q be a smooth quadric of even dimension $n = 2r$ defined over a finite field $\mathbf{F}_q$ of characteristic different from 2. Then Frob_q acts on the primitive cohomology $H^n_{\mathrm{pr}}(Q)$ by multiplication by $\varepsilon_q(\Delta)\, q^r$, where ε_q is the (unique) multiplicative character of $\mathbf{F}_q$ of order 2, and $\Delta = \Delta(Q)$ is the signed discriminant of Q.*

Proof. Without loss of generality, we can assume that Q is a diagonal quadric

$$\sum_{i=1}^{n+2} a_i x_i^2 = 0.$$

By Proposition 2.3.7, Frob_q acts on $H^n_{\mathrm{pr}}(Q)$ by multiplication by

$$\frac{1}{q} \prod_{i=1}^{n+2} \chi_i(a_i^{-1}) g(\chi_i),$$

where the sum is over all $(n+2)$-tuples of characters χ_i such that $\chi_i^2 = \mathbf{1}$, $\chi_i \neq \mathbf{1}$ and $\chi_1 \cdots \chi_{n+2} = \mathbf{1}$. It turns out that the only possibility is to have $\chi_i = \varepsilon_q$ for all i, where ε_q is the unique multiplicative character of $\mathbf{F}_q$ of order 2. Hence the action of Frobenius is via multiplication by

$$\frac{1}{q} \prod_{i=1}^{n+2} \varepsilon_q(a_i^{-1}) g(\varepsilon_q) = \frac{1}{q} \varepsilon_q(a_1 \cdots a_{n+2}) g(\varepsilon_q)^{n+2},$$

since

$$a_1^{-1} \cdots a_{n+2}^{-1} \equiv a_1 \cdots a_{n+2} \text{ modulo squares.}$$

But here $g(\varepsilon_q)^2 = g(\varepsilon_q) g(\overline{\varepsilon}_q) = \varepsilon_q(-1) q$, so that the above expression equals

$$\frac{1}{q} \varepsilon_q(a_1 \cdots a_{n+2}) \varepsilon_q(-1)^{r+1} q^{r+1} = \varepsilon_q(\Delta) q^r,$$

as announced. □

Corollary 2.4.4. *If Q is a smooth quadric of dimension $n = 2r$ defined over a number field K, the compatible system of ℓ-adic Galois representations on $H^n_{\mathrm{pr}}(Q)$ is*

$$\chi_{\mathrm{cycl}}^r \otimes \varepsilon_\Delta,$$

where Δ is the signed discriminant of Q and $\varepsilon_\Delta : \mathrm{Gal}_K \twoheadrightarrow \mathrm{Gal}(K(\sqrt{\Delta})/K) \to \{\pm 1\}$ is the corresponding quadratic character.

Proof. According to Proposition 2.4.3, the action of $\mathrm{Frob}_\mathfrak{p}$ agrees for all finite places $\mathfrak{p}$ of K away from 2. The conclusion follows by continuity. □

We could also have obtained the same result by a more geometric method, using the fact that in this situation, the cycle class map

$$\chi : \mathrm{CH}^r(Q)(r) \longrightarrow H^n(Q)$$

is actually surjective, and that two r-planes R and R' in Q are rationally equivalent if and only if

$$\dim R \cap R' \equiv r \bmod 2,$$

where we convene that $\dim \varnothing = -1$ (see [22]).

By standard manipulations on quadratic forms, a defining equation for Q can be brought into diagonal form and the variables arbitrarily paired to get an equation of the form

$$\sum_{i=1}^{r+1} \alpha_i (x_i^2 - \beta_i y_i^2) = 0.$$

The two r-planes defined over $L := K(\sqrt{\beta_0}, \ldots, \sqrt{\beta_r})$,

$$R_\pm : x_i + \sqrt{\beta_i} y_i = 0, \quad i = 0, \ldots, r, \quad x_{r+1} \pm \sqrt{\beta_i} y_i = 0,$$

yield different cohomology classes, and we have

$$H^n(Q) = \langle \gamma[R_+], \gamma[R_-] \rangle.$$

Now if $\sqrt{\beta_i} \notin K$, the Galois involution $\sqrt{\beta_i} \mapsto -\sqrt{\beta_i}$ interchanges $[R_+]$ and $[R_-]$, so that $\mathrm{Gal}(L/K)$ acts on $[R_+] + [R_-]$ trivially and on $[R_+] - [R_-]$ as $\mathrm{Gal}(K(\sqrt{\Delta})/K)$ because

$$\det Q = \prod_{i=0}^{r} \alpha_i \cdot (-\alpha_i \beta_i) \equiv (-1)^{r+1} \prod_{i=0}^{r} \beta_i \bmod (K^\times)^2.$$

It follows after twisting by χ_{cycl}^r that Gal_K acts via $\chi_{\mathrm{cycl}}^r(\mathbf{1} \oplus \varepsilon_\Delta)$ on

$$H^n(Q) = \langle \gamma[R_+] + \gamma[R_-] \rangle \oplus \langle \gamma[R_+] - \gamma[R_-] \rangle,$$

hence the action on $H^n_{\mathrm{pr}}(Q) = \langle \gamma[R_+] - \gamma[R_-] \rangle$ is via $\chi_{\mathrm{cycl}}^r \otimes \varepsilon_\Delta$.

2.5 Hypersurfaces with ordinary double points

In this section we describe the cohomology of the desingularizations of hypersurfaces whose singular locus consists only of ordinary double points, following and expanding on Schoen's treatment [50], where only hypersurfaces of odd dimension are considered.

Definition 2.5.1. A singular point x on a projective hypersurface X is an *ordinary double point* if the tangent cone $C_x(X)$ at x is a smooth quadric.

Let X a projective hypersurface of dimension m sitting inside $\mathbf{P} := \mathbf{P}^{m+1}$. We suppose that the singular locus S of X consists entirely of ordinary double points. Consider $\widetilde{X} \to X$ (resp. $\widetilde{\mathbf{P}} \to \mathbf{P}$) the blow-up of X (resp. $\mathbf{P}$) along S.

The following is an analogue of the Lefschetz hyperplane theorem for the inclusion

$$j : \widetilde{X} \hookrightarrow \widetilde{\mathbf{P}}.$$

Proposition 2.5.2. *The induced homomorphism in cohomology $j^* : H^i(\widetilde{\mathbf{P}}) \to H^i(\widetilde{X})$ is an isomorphism for $i \leq m-2$, and injective for $i \leq m$.*

For convenient reference, we first state a standard fact from commutative algebra that will be used in the proof.

Lemma 2.5.3 (Five lemma)**.** *Consider the following commutative diagram, in which the rows are exact.*

$$\begin{array}{ccccccccc} A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & D_1 & \longrightarrow & E_1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \varepsilon} \\ A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & D_2 & \longrightarrow & E_2 \end{array}$$

1. *If α is surjective, β and δ injective, then γ is injective.*
2. *If ε is injective, β and δ surjective, then γ is surjective.*

In particular, if α, β, δ and ε are isomorphisms, then γ also is.

Proof of proposition. Let Q (resp. E) be the exceptional fiber in $\widetilde{X}$ (resp. $\widetilde{\mathbf{P}}$). By the assumption that S consists only of ordinary double points, we have decompositions $Q = \sqcup_{s\in S} Q_s$, $E = \sqcup_{s\in S} E_s$, where Q_s is a smooth quadric in $E_s \simeq \mathbf{P}^m$. By the Lefschetz hyperplane theorem applied to the fibers Q_s, the map

$$H^i(E) = \bigoplus_{s\in S} H^i(E_s) \longrightarrow \bigoplus_{s\in S} H^i(Q_s) = H^i(Q)$$

is an isomorphism for $i \neq \dim Q = m-1$, and injective when $i = m-1$.

Now consider the long exact sequences for the couples (X, S) and $(\mathbf{P}, S)$.

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & H^{i-1}(\mathbf{P}) & \longrightarrow & H^{i-1}(S) & \longrightarrow & H^i(\mathbf{P}, S) & \longrightarrow & H^i(\mathbf{P}) & \longrightarrow & H^i(S) & \longrightarrow \cdots \\
 & & \downarrow & & \| & & \downarrow & & \downarrow & & \| & \\
\cdots & \longrightarrow & H^{i-1}(X) & \longrightarrow & H^{i-1}(S) & \longrightarrow & H^i(X, S) & \longrightarrow & H^i(X) & \longrightarrow & H^i(S) & \longrightarrow \cdots
\end{array}$$

Together with the Lefschetz hyperplane theorem for $X \hookrightarrow \mathbf{P}$, the five lemma implies that $H^i(\mathbf{P}, S) \to H^i(X, S)$ is bijective for $i < m$ and injective when $i = m$. The same statement holds for $H^i(\widetilde{\mathbf{P}}, E) \to H^i(\widetilde{X}, Q)$ since the blow-ups induce isomorphisms

$$\begin{array}{ccc}
H^i(\widetilde{\mathbf{P}}, E) & \longrightarrow & H^i(\widetilde{X}, Q) \\
\uparrow \simeq & & \uparrow \simeq \\
H^i(P, S) & \longrightarrow & H^i(X, S).
\end{array}$$

Now we may consider the long exact sequences associated to the couples $(\widetilde{X}, Q)$ and $(\widetilde{\mathbf{P}}, E)$.

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & H^{i-1}(E) & \longrightarrow & H^i(\widetilde{\mathbf{P}}, E) & \longrightarrow & H^i(\widetilde{\mathbf{P}}) & \longrightarrow & H^i(E) & \longrightarrow & H^{i+1}(\widetilde{\mathbf{P}}, E) & \longrightarrow \cdots \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle j^*} & & \downarrow & & \downarrow & \\
\cdots & \longrightarrow & H^{i-1}(Q) & \longrightarrow & H^i(\widetilde{X}, Q) & \longrightarrow & H^i(\widetilde{X}) & \longrightarrow & H^i(Q) & \longrightarrow & H^{i+1}(\widetilde{X}, Q) & \longrightarrow \cdots
\end{array}$$

For $i \leq m-2$, all vertical arrows besides j^* are isomorphisms, hence by the five lemma j^* is an isomorphism as well. When $i = m-1$, $H^{i-1}(E) \to H^{i-1}(Q)$ is an isomorphism and $H^i(\widetilde{\mathbf{P}}, E) \to H^i(\widetilde{X}, Q)$, $H^i(E) \to H^i(Q)$ are isomorphisms, which is enough to apply the first part of the five lemma to conclude that j^* is injective. For $i = m$, we know that $H^i(\widetilde{\mathbf{P}}, E) \to H^i(\widetilde{X}, Q)$ is injective and $H^i(E) \to H^i(Q)$ is an isomorphism. However, in order to apply the five lemma to show that j^* is injective, we need to

know that $H^{i-1}(E) \to H^{i-1}(Q)$ is surjective, and this is the case only when m is even, so that Q has no primitive cohomology (and actually $H^{i-1}(E) = H^{i-1}(Q) = 0$). For m odd, one needs a slightly different argument as in [50] – again using the fact that the connected components of Q are smooth quadrics.

□

Definition 2.5.4. Let us call

$$H_{\mathrm{pr}}(\widetilde{X}) := H^m(\widetilde{X})/H^m(\widetilde{\mathbf{P}}) \quad \text{and} \quad H_{\mathrm{sub}}(\widetilde{X}) := H^{m-1}(\widetilde{X})/H^{m-1}(\widetilde{\mathbf{P}})$$

the *primitive* and *subprimitive cohomology groups* of $\widetilde{X}$, respectively.

The following tells us that the subprimitive cohomology of $\widetilde{X}$ comes from the primitive cohomology of the fibers of Q.

Proposition 2.5.5 ([50])**.** *When $m = \dim X$ is even, $H_{\mathrm{sub}}(\widetilde{X}) = 0$. For m odd, let $k = \frac{m-1}{2}$ and for every $s \in S$ let R_s and R'_s be two k-planes in Q_s belonging to different rulings, so that $H^{m-1}_{\mathrm{pr}}(Q_s) = \langle [R_s] - [R'_s] \rangle$. The cup-product induces an isomorphism*

$$H_{\mathrm{sub}}(\widetilde{X}) \xrightarrow{\sim} H_0^{m+1}(\widetilde{X}),$$

where $H_0^{m+1}(\widetilde{X})$ denotes the subspace of $H^{m+1}(\widetilde{X})$ spanned by the classes $[R_s] - [R'_s]$, for $s \in S$. Moreover, there is a natural isomorphism

$$H_0^{m+1}(\widetilde{X}) \otimes \mathbf{C} \xrightarrow{\sim} H^1(\mathbf{P}, \mathcal{I}_S \otimes K \otimes \mathcal{O}(kX)).$$

We also need to understand the cohomology of $\widetilde{\mathbf{P}}$.

Proposition 2.5.6. *Let $\widetilde{\mathbf{P}}$ be the blow-up of $\mathbf{P} = \mathbf{P}^{m+1}$ along a finite set of points S, and let E be the exceptional fiber. Then $H^i(\widetilde{\mathbf{P}}) = 0$ when i is odd, and for $0 < i < m+1$ we have a natural short exact sequence*

$$0 \longrightarrow H^{2i}(\mathbf{P}) \longrightarrow H^{2i}(\widetilde{\mathbf{P}}) \longrightarrow H^{2i}(E) \longrightarrow 0.$$

Proof. Consider the long exact sequences associated to the couples $(\widetilde{\mathbf{P}}, E)$ and $(\mathbf{P}, S)$.

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & H^{i-1}(E) & \longrightarrow & H^i(\widetilde{\mathbf{P}}, E) & \longrightarrow & H^i(\widetilde{\mathbf{P}}) & \longrightarrow & H^i(E) & \longrightarrow & H^{i+1}(\widetilde{\mathbf{P}}, E) & \longrightarrow \cdots \\
& \uparrow & & \uparrow \simeq & & \uparrow & & \uparrow & & \uparrow \simeq & \\
\cdots \longrightarrow & H^{i-1}(S) & \longrightarrow & H^i(\mathbf{P}, S) & \longrightarrow & H^i(\mathbf{P}) & \longrightarrow & H^i(S) & \longrightarrow & H^{i+1}(\mathbf{P}, S) & \longrightarrow \cdots
\end{array}$$

Since S has dimension 0, from the lower line we see that $H^i(\mathbf{P}, S) \simeq H^i(\mathbf{P})$ for all i. Hence, for i odd, since $H^i(\widetilde{\mathbf{P}}, E) \simeq H^i(\mathbf{P}) = 0$ and $H^i(E) = 0$, from the upper line we conclude that $H^i(\widetilde{\mathbf{P}}) = 0$. Similarly, when $i > 0$ is even, since $H^{i-1}(E)$ and $H^{i+1}(\mathbf{P}, E) \simeq H^{i+1}(\mathbf{P})$ vanish, we get a short exact sequence

$$0 \longrightarrow H^i(\widetilde{\mathbf{P}}, E) \longrightarrow H^i(\widetilde{\mathbf{P}}) \longrightarrow H^i(E) \longrightarrow 0,$$

in which we can replace $H^i(\widetilde{\mathbf{P}}, E)$ by $H^i(\mathbf{P})$. □

We can get some information about the dimensions of the primitive and subprimitive cohomology using the Euler characteristic of $\widetilde{X}$.

Proposition 2.5.7.

$$\dim H_{\mathrm{pr}}(\widetilde{X}) = \begin{cases} \frac{(d-1)^{m+2}-1}{d} - |S| & \textit{when } m \textit{ is even,} \\ 2\dim H_{\mathrm{sub}}(\widetilde{X}) + \frac{(d-1)^{m+2}+1}{d} - 2|S| & \textit{when } m \textit{ is odd.} \end{cases}$$

Proof. By Proposition 2.5.2 and Poincaré duality,

$$\chi(\widetilde{X}) = \chi(\widetilde{\mathbf{P}}) + 2(-1)^{m-1}\dim H_{\mathrm{sub}}(\widetilde{X}) + (-1)^m \dim H_{\mathrm{pr}}(\widetilde{X}).$$

From Proposition 2.5.6, we see that

$$\chi(\widetilde{\mathbf{P}}) = \chi(\mathbf{P}) + \chi(E) - \dim H^0(E) = m + 2 + |S|m - |S|,$$

since $E \simeq \sqcup_{s\in S}\mathbf{P}^{m-1}$. But the Euler characteristic of X (see [39, Prop. 3.1], generalizing Corollary 2.3.6) can be expressed as

$$\chi(\widetilde{X}) = m + 2 + \frac{(1-d)^{m+2} - 1}{d} + |S|(m + \delta_m),$$

where $\delta_m = 1$ when m is odd, and $\delta_m = -2$ when m is even. Comparing the two expressions for $\chi(\widetilde{X})$ yields

$$\dim H_{\mathrm{pr}}(\widetilde{X}) - 2\dim H_{\mathrm{sub}}(\widetilde{X}) = \frac{(d-1)^{m+2} - (-1)^m}{d} + (-1)^m|S|(\delta_m + 1),$$

from which the conclusion follows according to the parity of m. □

Galois representations. Suppose now that our base algebraically closed field $\mathbf{F}$ is separably closed and that the variety X is defined over a subfield K of which $\mathbf{F}$

is the algebraic closure, so that $H^\bullet(\widetilde{X})$ admits a natural action by Gal_K. Since all the homomorphisms considered above are natural, they are Galois-equivariant when it makes sense, so that they provide some information on $H^\bullet(\widetilde{X})$ as a Galois module as well.

By the Jacobian criterion, the singular locus S of X is defined over K, even though the individual singular points need not. For a singular point $s \in S$, let $K(s)$ be the normal closure of the field of definition of s. Furthermore, let $K(S)$ be the compositum of all the extensions $K(s)$, $s \in S$, so that S becomes isomorphic to $|S|$ points over $K(S)$. The smooth quadric Q_s above $s \in S$ is easily seen to be defined over $K(s)$ as well.

The action of Gal_K on $H^\bullet(Q)$ can be described as follows. Over $K(S)$, Q is isomorphic to $\sqcup_{s\in S} Q_s$, so that

$$H^\bullet(Q) = \bigoplus_{s\in S} H^\bullet(Q_s)$$

as $\mathrm{Gal}_{K(S)}$-modules, while $\mathrm{Gal}(K(S)/K)$ permutes the fibers among themselves. More precisely, if we decompose $S = \sqcup S_i$ into disjoint Gal_K-orbits, each orbit S_i is defined over K, hence a corresponding decomposition $Q = \sqcup Q_i$ over K. Choosing some point $s_i \in S_i$, we see that

$$H^\bullet(Q_i) \simeq H^0(S_i) \otimes H^\bullet(Q_{s_i}),$$

where $\mathrm{Gal}(K(s_i)/K)$ acts on $H^0(S_i)$ by permuting the points and $G_{K(s_i)}$ acts on $H^\bullet(Q_{s_i})$ as described in Section 2.4.

Chapter 3

Hypersurfaces with symmetries

When X is a variety defined over a number field K admitting an action by a finite group G of K-automorphisms, its étale cohomology inherits an action of G commuting with the Galois structure. The G-isotypic components of $H^\bullet(X)$ are thus preserved by the Galois action, and we prove in Section 3.1 that these isotypic components form compatible systems of Galois representations. This fact could have been deduced by suitably interpreting the work of Grothendieck [23] on the G-equivariant L-functions defined in [52]. There, rationality results where obtained by interpreting every individual element $g \in G$ as a Frobenius morphism with respect to some twisted Galois structure on X. The approach used here however is novel in that it gives a geometrical (and, in this writer's opinion, more natural) "motivic" explanation for rationality by interpreting the multiplicity spaces of Section 1.2 as the étale cohomology groups of the quotient X/G with coefficients in a suitable sheaf. Decomposing the trace of Frobenius according to isotypic components (as will be done on certain examples in Section 5.7) could not be carried out without the previous knowledge that these systems of isotypic Galois representations are actually compatible.

The remainder of the chapter is devoted to the study of certain families of hypersurfaces admitting an action by the symmetric group S_n and for which the character of the representation on primitive cohomology can be computed in a general fashion. In Section 3.2 we define two such families, *S_n-hypersurfaces of type I or II*, and the notion of a *special* S_n-hypersurface for which we can give a general formula for the character of the representation of S_n on primitive cohomology (Theorem 3.2.14) by using the Lefschetz fixed point theorem to relate the value of this character to the Euler-Poincaré characteristic of the fixed loci. We then discuss in Section 3.3 the existence of these special S_n-hypersurfaces, by providing some examples as well as certain

obstructions coming from the representation theory of S_n. A precise conjecture is formulated about the existence of special hypersurfaces of type II.

In Section 3.4, we introduce and discuss the varieties $W_\ell^{m,n}$, which arise naturally when considering the moments of the exponential sums of Chapter 4 (the case $\ell = 2$, $m = 0$ was previously considered by Livné [39]). These varieties admit an action by $S_m \times S_n$; in particular, when m = 0, they are examples of S_n-hypersurfaces of type II *provided they are smooth*. We thus discuss for which values of the parameters ℓ, m, n they are smooth, and prove that in any case their singularities are ordinary double points, so that the cohomology of their desingularization can be studied via the results of Section 2.5.

Finally, we perform in Section 3.5 some explicit computations of decomposition into irreducibles of the corresponding representations for small values of the parameters. In particular, we observe that the primitive cohomology of $W_2^{0,7}$ admits an isotypic component of dimension 2; the modular form corresponding to this 2-dimensional compatible system will be explicitly determined in Chapter 5. We also provided a description of the action of $S_m \times S_n$ on the subprimitive cohomology of the desingularization of $W_\ell^{m,n}$ which will be needed to compute the moments of the corresponding exponential sums in Chapter 4.

3.1 Isotypic decomposition

Let X be a smooth, proper variety defined over a number field K, on which a finite group G acts by automorphisms defined over K. The goal of this section is to show that the étale cohomology of X admits a G-isotypic decomposition

$$H^\bullet(X) = \bigoplus_\phi M_\phi(H^\bullet(X)) \otimes W_\phi, \qquad M_\phi(H^\bullet(X)) = \mathrm{Hom}_G(W_\phi, H^\bullet(X)),$$

in the category of compatible systems. Recalling how étale cohomology is defined (Section 2.1), we first prove the corresponding statement for sheaf cohomology, allowing general sheaves of coefficients.

Suppose that X is a topological space on which a group G acts continuously *on the right*.

Definition 3.1.1. A G-sheaf on X is a sheaf of finite dimensional vector spaces over a field E of characteristic 0, endowed with a lift of the action of G on X, i.e. a couple

$(\mathcal{F}, \theta)$, where $\mathcal{F}$ is a sheaf of E-vector spaces on X, and $\theta = (\theta_g)_{g\in G}$ is a collection of isomorphisms $\theta_g : \mathcal{F} \to g^*\mathcal{F}$ satisfying the cocycle relation

$$\theta_{gh} = g^*\theta_h \circ \theta_g, \qquad g, h \in G.$$

In particular, if G acts trivially on X, then a G-sheaf $\mathcal{F}$ on X is a "sheaf-valued representation of G", i.e. G acts on $\mathcal{F}$ by sheaf automorphisms. Using the notation of Section 1.2, we can prove an isotypic decomposition for such sheaf-valued representations.

Lemma 3.1.2. *Let $\mathcal{F}$ be a G-sheaf on X, where G is a finite group acting trivially on X. There is a natural isomorphism*

$$\mathcal{F} = \bigoplus_{\phi\in \mathrm{Irr}_E(G)} \mathcal{M}_\phi(\mathcal{F}) \otimes_{E_\phi} W_\phi,$$

where $\mathcal{M}_\phi(\mathcal{F}) := \mathcal{H}\mathrm{om}_G(W_\phi, \mathcal{F})$ is the multiplicity sheaf *of ϕ in $\mathcal{F}$, and W_ϕ is considered as a constant sheaf.*

Proof. As in the proof of Corollary 1.2.2, we have a natural homomorphism

$$\bigoplus_{\phi\in \mathrm{Irr}_E(G)} \mathcal{M}_\phi(\mathcal{F}) \otimes_{E_\phi} W_\phi \longrightarrow \mathcal{F}$$

induced by the evaluation maps. To prove that it is an isomorphism of sheaves, it suffices to check that it induces isomorphisms at the level of stalks. But for $x \in X$, since

$$\mathcal{M}_\phi(\mathcal{F})_x = \mathcal{H}\mathrm{om}_G(W_\phi, \mathcal{F})_x = \mathrm{Hom}_G(W_\phi, \mathcal{F}_x),$$

the induced map on the stalks at x is precisely the isotypic decomposition of $\mathcal{F}_x$. □

In general, if F is a G-sheaf on X, the sheaf cohomology $H^\bullet(X, \mathcal{F})$ with coefficients in $\mathcal{F}$ inherits by functoriality the structure of a graded E-valued representation for G. As such, we can consider its isotypic decomposition

$$H^\bullet(X, \mathcal{F}) = \bigoplus_{\phi\in \mathrm{Irr}_E(G)} M_\phi(H^\bullet(X, \mathcal{F})) \otimes_{E_\phi} W_\phi. \tag{3.1}$$

The following theorem says that the multiplicity spaces $M_\phi(H^\bullet(X, \mathcal{F}))$ can be interpreted as the sheaf cohomology of the *quotient* X/G with values in the multiplicity sheaves of the push-forward of $\mathcal{F}$ on X/G.

Theorem 3.1.3. *Let G be a finite group acting on X and $\pi : X \twoheadrightarrow X/G$ denote the projection on the quotient. For any G-sheaf $\mathcal{F}$ on X, there is canonical isomorphism*

$$M_\phi(H^\bullet(X, \mathcal{F})) = H^\bullet(X/G, \mathcal{M}_\phi(\pi_*\mathcal{F})).$$

Proof. Since G is a finite group, π is a proper, finite map and thus induces an isomorphism

$$\pi_* : H^\bullet(X/G, \pi_*\mathcal{F}) \xrightarrow{\sim} H^\bullet(X, \mathcal{F}). \tag{3.2}$$

Now $\pi_*\mathcal{F}$ is a G-sheaf on X/G, with G acting trivially on X/G, hence using Lemma 3.1.2 we can write

$$\pi_*\mathcal{F} = \bigoplus_{\phi \in \mathrm{Irr}_E(G)} \mathcal{M}_\phi(\pi_*\mathcal{F}) \otimes_{E_\phi} W_\phi.$$

Taking sheaf cohomology on both sides we obtain

$$H^\bullet(X/G, \pi_*\mathcal{F}) = \bigoplus_{\phi \in \mathrm{Irr}_E(G)} H^\bullet(X/G, \mathcal{M}_\phi(\pi_*\mathcal{F})) \otimes_{E_\phi} W_\phi.$$

Comparing this expression with the isotypic decomposition (3.1) of $H^\bullet(X, \mathcal{F})$ via the isomorphism (3.2), we see that the assertion of the theorem would follow automatically from the existence of a natural map

$$H^\bullet(X/G, \mathcal{M}_\phi(\pi_*\mathcal{F})) \longrightarrow M_\phi(H^\bullet(X, \mathcal{F})) \tag{3.3}$$

since it would then automatically be an isomorphism. Now remark that

$$\mathcal{M}_\phi(\pi_*\mathcal{F})) = \mathcal{H}\mathrm{om}_G(W_\phi, \pi_*\mathcal{F}) = \mathcal{H}\mathrm{om}(W_\phi, \pi_*\mathcal{F})^G$$

naturally injects into $\mathcal{H}\mathrm{om}(W_\phi, \pi_*\mathcal{F})$, hence the existence of a natural map

$$H^\bullet(X/G, \mathcal{M}_\phi(\pi_*\mathcal{F}) \longrightarrow H^\bullet(X/G, \mathcal{H}\mathrm{om}(W_\phi, \pi_*\mathcal{F})),$$

which actually restricts, since G acts trivially on the left-hand side, to a map

$$H^\bullet(X/G, \mathcal{M}_\phi(\pi_*\mathcal{F})) \longrightarrow H^\bullet(X/G, \mathcal{H}\mathrm{om}(W_\phi, \pi_*\mathcal{F}))^G. \tag{3.4}$$

Since W_ϕ is a constant sheaf, the functor $\mathcal{H}\mathrm{om}(W_\phi, -)$ is exact, hence

$$\begin{aligned} H^\bullet(X/G, \mathcal{H}\mathrm{om}(W_\phi, \pi_*\mathcal{F}))^G &= \mathrm{Hom}(W_\phi, H^\bullet(X/G, \pi_*\mathcal{F}))^G \\ &= \mathrm{Hom}_G(W_\phi, H^\bullet(X/G, \pi_*\mathcal{F})) \\ &= M_\phi(H^\bullet(X/G, \pi_*\mathcal{F})) \\ &= M_\phi(H^\bullet(X, \mathcal{F})), \end{aligned}$$

where we have used the isomorphism (3.2) again in the last step. It follows that (3.4) gives the natural map (3.3) we were looking for, hence completing the proof. □

It is reasonable to expect that such a result still holds in ℓ-adic cohomology (at least when the order of G is prime to ℓ). Some details need to be supplied, since the definition of ℓ-adic cohomology is more involved than sheaf cohomology on ordinary topological spaces; however, we will take this for granted here.

We can now state the desired result for arithmetic varieties. Recall that for a scheme X on which a group G acts, a sufficient condition for the existence of the quotient X/G in the category of schemes is that X can be covered by G-stable affine sets [44, §7]. In such a case, writing $X = \cup_i U_i$ as a union of G-stable open affine sets, we can then construct X/G by gluing together the affine quotients U_i/G, where

$$U_i/G := \mathrm{Spec}\, A_i^G \qquad \text{if} \quad U_i = \mathrm{Spec}\, A_i.$$

Theorem 3.1.4. *Let X be a smooth, proper variety defined over a number field K and G a finite group acting on X by K-automorphisms such that the quotient X/G exists and is smooth. Let $\mathcal{F} = (\mathcal{F}_\lambda)_\lambda$ be a λ-adic compatible system of constructible G-sheaves over a number field E. The multiplicity*

$$M_\phi(H^\bullet(X, \mathcal{F}))$$

in $H^\bullet(X, \mathcal{F})$ of every irreducible representation $\phi \in \mathrm{Irr}_E(G)$ forms an E-rational compatible system of λ-adic representations of Gal_K.

Proof. For every λ, it follows from the analogue of Theorem 3.1.3 that

$$M_\phi(H^\bullet(X, \mathcal{F}_\lambda)) = H^\bullet(X/G, \mathcal{M}_\phi(\pi_*\mathcal{F}_\lambda))$$

as λ-adic representations of Gal_K. Since the quotient map $\pi : X \twoheadrightarrow X/G$ is defined

over K, the push-forward sheaves $\pi_*\mathcal{F}_\lambda$ are seen to form a compatible family, and so do the multiplicity sheaves $\mathcal{M}_\phi(\pi_*\mathcal{F}_\lambda) = \mathcal{H}\mathrm{om}_G(W_\phi, \pi_*\mathcal{F}_\lambda)$. □

Remark. The properness hypothesis on X/G, as well as on X, can be removed if one is willing to use étale cohomology with compact support since the trace formula holds in this context. Namely, it can be proven by exercising a little extra care that for any compatible system $\mathcal{F}$ of λ-adic G-sheaves,

$$M_\phi(H_c^\bullet(X, \mathcal{F})) = H_c^\bullet(X/G, \mathcal{M}_\phi(\pi_*\mathcal{F}))$$

as compatible systems of λ-adic representations.

It follows immediately from the theorem that for a compatible system $\mathcal{F}$ of E-rational λ-adic G-sheaves on X, we have an isotypic decomposition

$$H^\bullet(X, \mathcal{F}) = \bigoplus_{\phi \in \mathrm{Irr}_E(G)} M_\phi(H^\bullet(X, \mathcal{F})) \otimes_{E_\phi} W_\phi$$

as compatible systems of λ-adic Galois representations. As a result, if $\zeta(X, \mathcal{F})$ denotes the zeta function of $H^\bullet(X, \mathcal{F})$ and $\zeta_\phi(X, \mathcal{F})$ that of $M_\phi(H^\bullet(X, \mathcal{F}))$, we obtain a factorization

$$\zeta(X, \mathcal{F}) = \prod_{\phi \in \mathrm{Irr}_E(G)} \zeta_\phi(X, \mathcal{F})^{\dim_{E_\phi} W_\phi} = \prod_{\phi \in \mathrm{Irr}_E(G)} \zeta(X/G, \mathcal{M}_\phi(\pi_*\mathcal{F}))^{\dim_{E_\phi} W_\phi}.$$

3.2 Symmetric hypersurfaces

The goal of this section is to compute the character of S_n acting on the cohomology of certain kinds of symmetric projective hypersurfaces. Throughout, we fix $n \geq 1$ a positive integer and $\mathbf{F}$ an algebraically closed field in which $n! \neq 0$. We consider the projective *right* action of the symmetric group S_n on the projective space $\mathbf{P}^{n-1}$ by permutation of homogeneous coordinates, i.e.

$$\sigma \cdot [x_1 : \cdots : x_n] := [x_{\sigma(1)} : \cdots : x_{\sigma(n)}], \qquad \sigma \in S_n.$$

This is nothing but the projectivization of (the transpose of) the standard linear permutation representation, i.e. the composition

$$S_n \longrightarrow \mathrm{GL}_n(\mathbf{F}) \twoheadrightarrow \mathrm{PGL}_n(\mathbf{F}) = \mathrm{Aut}\, \mathbf{P}^{n-1}.$$

We will consider two types of symmetric hypersurfaces.

Definition 3.2.1. An *S_n-hypersurface of type I* is a smooth hypersurface $X \subseteq \mathbf{P}^{n-1}$ of dimension $n-2$ which is stable under the action of S_n by permutation of homogeneous coordinates. Let H be the hyperplane of $\mathbf{P}^{n-1}$ defined by $x_1 + \cdots + x_n = 0$.

An *S_n-hypersurface of type II* is a smooth projective hypersurface $X \subseteq H$ of dimension $n-3$ which is stable under the action of S_n.

The hyperplane $H \subseteq \mathbf{P}^{n-2}$ is itself a S_n-hypersurface of type I. Note that the action of S_n on H can be thought of as the projectivization of the irreducible representation of degree $n-1$ occurring in the permutation representation on $\mathbf{F}^n$.

We would like to compute in some generality the representation of S_n acting on the cohomology of S_n-hypersurfaces of type I or II. In both cases the only interesting part is the primitive cohomology thanks to the Lefschetz hyperplane theorem.

Proposition 3.2.2. *Let X be a smooth projective hypersurface which is stable under a group G of projective transformations. Then G acts trivially on the non-primitive part of $H^\bullet(X)$, and the character χ_{pr} of the representation on $H_{\mathrm{pr}}(X)$ is given for $g \in G$ by*

$$\chi_{\mathrm{pr}}(g) = (-1)^{\dim X}\Big(\chi(\operatorname{Fix} g|_X) - \dim X - 1\Big),$$

where $\chi(\operatorname{Fix} g|_X)$ denotes the Euler characteristic of the fixed locus of g on X.

Proof. We first remark that the induced action of G on the cohomology of the ambient projective space $\mathbf{P}$ is trivial, since $H^\bullet(\mathbf{P})$ is generated by the class of a hyperplane, and that any two hyperplanes are rationally equivalent. Hence, by the hard Lefschetz theorem, G acts trivially on the non-primitive part of $H^\bullet(X)$. Now the graded character $\chi^\bullet$ of G acting on $H^\bullet(X)$ can be written as

$$\chi^\bullet = \chi(\mathbf{P}^{\dim X}) + (-1)^{\dim X}\chi_{\mathrm{pr}},$$

so that

$$\chi_{\mathrm{pr}} = (-1)^{\dim X}\big(\chi^\bullet - \chi(\mathbf{P}^{\dim X})\big) = (-1)^{\dim X}\big(\chi^\bullet - \dim X - 1\big).$$

According to the Lefschetz fixed point formula (see [43, 34] and [16] in the algebraic setting), for every $g \in G$ we have

$$\chi^\bullet(g) = \operatorname{tr}(g^* \mid H^\bullet(X)) = \chi(\operatorname{Fix} g|_X),$$

which completes the proof. □

In order to study the fixed loci of permutations on symmetric hypersurfaces, let us first describe the fixed locus $\operatorname{Fix}\sigma$ in $\mathbf{P}^{n-1}$ of a permutation $\sigma \in S_n$. First, note that for a point $[\mathbf{x}] \in \operatorname{Fix}\sigma$, we have $\sigma \cdot \mathbf{x} = \alpha\mathbf{x}$ for some scalar $\alpha \in \mathbf{F}^\times$ which does not depend on the choice of a representative $\mathbf{x}$ for $[\mathbf{x}]$. Hence there is a partition of the fixed locus as

$$\operatorname{Fix}\sigma = \bigsqcup_{\alpha\in\mathbf{F}^\times} \operatorname{Fix}_\alpha \sigma, \quad \text{where } \operatorname{Fix}_\alpha \sigma := \{[\mathbf{x}] \in \mathbf{P}^{n-1} \mid \sigma \cdot \mathbf{x} = \alpha\mathbf{x}\}.$$

Note that a fixed point $[\mathbf{x}] \in \mathbf{P}^{n-1}$ for σ corresponds to a 1-dimensional linear representation of the cyclic group $\langle\sigma\rangle$. It follows that if $\sigma^m = 1$, then $\operatorname{Fix}_\alpha \sigma = \varnothing$ unless $\alpha^m = 1$, so that we can restrict the disjoint union above to a finite number of roots of unity in $\mathbf{F}$.

Recall that any representation $\sigma \in S_n$ can be written as a product of disjoint cycles $\sigma_1, \ldots \sigma_m$, one for each orbit of $\langle\sigma\rangle$ on the set $\{1, \ldots, n\}$, and that this decomposition is unique up to the ordering of these cycles. We shall refer to the set $\{\sigma_1, \ldots, \sigma_m\}$ as the *cycle decomposition* of σ. Associated to this cycle decomposition is a partition $\lambda(\sigma) = \{\lambda_1, \ldots, \lambda_m\}$ of n, where λ_i denotes the length of the cycle σ_i. This partition characterizes the conjugacy class of σ (cf. Section 1.3).

Definition 3.2.3. For a permutation $\sigma \in S_n$ and any integer $d \geq 1$, we define $m_d(\sigma)$ to be the number of parts in $\lambda(\sigma)$ which are divisible by d.

Example 3.2.4. If $\sigma = (12)(3456)(789) \in S_{10}$, then $m_1(\sigma) = 4$, $m_2(\sigma) = 2$, $m_3(\sigma) = m_4(\sigma) = 1$, and $m_d(\sigma) = 0$ for $d > 4$.

Remark that for any permutation $\sigma \in S_n$, $m_1(\sigma)$ is just the number of cycles in its cycle decomposition, while we necessarily have $m_d(\sigma) = 0$ for $d > n$.

Proposition 3.2.5. *For $\sigma \in S_n$ and $\alpha \in \mathbf{F}^\times$ a scalar with multiplicative order d, $\operatorname{Fix}_\alpha \sigma$ is a linear subspace of $\mathbf{P}^{n-1}$ of dimension $m_d(\sigma) - 1$.*

Proof. Write $\lambda(\sigma) = \{\lambda_1, \ldots, \lambda_m\}$. Since the statement only depends on the conjugacy class of σ, we can assume that σ lies in $S_{\lambda_1} \times \ldots \times S_{\lambda_m}$ under the standard embedding. Any point $\mathbf{x} \in \mathbf{F}^n$ can thus be written as $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_m)$, with $\mathbf{x}_i \in \mathbf{F}^{\lambda_i}$, and the condition that $\sigma \cdot \mathbf{x} = \alpha\mathbf{x}$ is equivalent to

$$\sigma_i \cdot \mathbf{x}_i = \alpha\mathbf{x}_i, \qquad i = 1, \ldots, m.$$

But as a linear transformation, σ_i has characteristic polynomial $t^{\lambda_i} - 1$, so that the above admits a non-zero solution $\mathbf{x}_i$ if and only if $\alpha^{\lambda_i} = 1$, i.e. if and only if $d \mid \lambda_i$. Since $t^{\lambda_i} - 1$ has distinct roots in $\mathbf{F}$ by our assumption on the characteristic of the field, in the case where $\alpha^{\lambda_i} = 1$, the associated eigenspace of σ_i is 1-dimensional. Let $\mathbf{z}_{\lambda_i}(\alpha)$ be an eigenvector of σ_i associated to α. Then we proved that the points in $\operatorname{Fix}_\alpha \sigma$ are those of the form

$$[x_1 \mathbf{z}_{\lambda_1}(\alpha) : \cdots : x_n \mathbf{z}_{\lambda_m}(\alpha)],$$

with $x_1, \ldots, x_m$ not all zero but $x_i = 0$ if $d \nmid \lambda_i$, which form a linear subspace of $\mathbf{P}^{n-1}$ with $m_d(\sigma)$ homogeneous coordinates. □

This means that in the decomposition

$$\operatorname{Fix} \sigma = \bigsqcup_{\alpha \in \mathbf{F}^\times} \operatorname{Fix}_\alpha \sigma, \tag{3.5}$$

we have $\operatorname{Fix}_\alpha \sigma \simeq \mathbf{P}^{m_d(\sigma)-1}$ when $O(\alpha) = d$. In particular, $\operatorname{Fix}_\alpha \sigma \neq \varnothing$ if and only if $m_d(\sigma) > 0$. Note that for composite d this is strictly stronger than the condition mentioned earlier ($\sigma^d = 1$), since the order of σ is the least common multiple of $\lambda_1, \ldots, \lambda_m$.

Lemma 3.2.6. *For $\sigma \in S_n$,*

$$\sum_{d \geq 1} \varphi(d)\, m_d(\sigma) = n,$$

where φ is the Euler totient function.

Proof. From (3.5) and the additivity of the Euler characteristic, we find

$$\chi(\operatorname{Fix} \sigma) = \sum_{d \geq 1} \varphi(d)\, \chi(\mathbf{P}^{m_d(\sigma)-1}) = \sum_{d \geq 1} \varphi(d)\, m_d(\sigma).$$

Since σ acts trivially on $H^\bullet(\mathbf{P}^{n-1})$, the Lefschetz fixed point formula for σ reads

$$\chi(\operatorname{Fix} \sigma) = \chi(\mathbf{P}^{n-1}) = n,$$

and the result follows. □

Note that this identity could also easily have been obtained by an elementary argument by writing σ as a product of disjoint cycles.

We now turn to an explicit description of the two types of symmetric hypersurfaces we are considering. We first state a standard lemma in the theory of symmetric polynomials.

Lemma 3.2.7. *Let $\Delta := \prod_{i<j}(x_i - x_j) \in \mathbf{F}[x_1, \ldots, x_n]$ be the discriminant polynomial. The vector space of polynomials where S_n acts via the alternating representation is*

$$\mathbf{F}[x_1, \ldots, x_n]_{\mathrm{sg}} = \Delta \cdot \mathbf{F}[x_1, \ldots, x_n]^{S_n}.$$

Proof. As S_n acts on Δ via sg, it is clear that $\Delta \cdot \mathbf{F}[x_1, \ldots, x_n]^{S_n}$ lies in $\mathbf{F}[x_1, \ldots, x_n]_{\mathrm{sg}}$. To prove the reverse inclusion, let f be a polynomial such that $\sigma \cdot f = \mathrm{sg}(\sigma) f$ for all $\sigma \in S_n$. In particular, for $i < j$, we have $(i\,j) \cdot f = -f$, hence

$$2f(x_1, \ldots, x_i, \ldots, x_i, \ldots, x_n) = 0.$$

If there exists such a pair $i < j$, then necessarily $n \geq 2$, so that by our hypothesis on the characteristic, 2 is invertible in $\mathbf{F}$. We conclude that f, considered as a polynomial in x_j with coefficients in the ring $\mathbf{F}[x_1, \ldots, \widehat{x_j}, \ldots, x_n]$, has a root at $x_j = x_i$, hence can be factored as $f = (x_i - x_j) f_{ij}$. If $k < \ell$ is another pair of indices, distinct (but not necessarily disjoint) from (i, j), the same argument shows that f has a root at $x_\ell = x_k$. However, since in all cases $x_i - x_j$ does not vanish at $x_\ell = x_k$, we conclude that f_{ij} has to be divisible by $x_k - x_\ell$. Continuing in this fashion, we find that f can be written as

$$f = \prod_{i<j}(x_i - x_j) \cdot g = \Delta \cdot g,$$

where g is some polynomial. But

$$\sigma \cdot g = \sigma \cdot \left(\frac{f}{\Delta}\right) = \frac{\sigma \cdot f}{\sigma \cdot \Delta} = \frac{\mathrm{sg}(\sigma) f}{\mathrm{sg}(\sigma)\Delta} = \frac{f}{\Delta} = g,$$

so that g in invariant under the action of S_n as claimed. □

Proposition 3.2.8. *For $n \geq 3$, any S_n-hypersurface of type I is of the form $Z(f)$ where f is a homogeneous symmetric polynomial. Similarly, for $n \geq 4$, any S_n-hypersurface of type II is of the form $Z(f) \cap H$, where f is a homogeneous symmetric polynomial.*

Proof. Let X be a S_n-hypersurface of type I in $\mathbf{P}^{n-1}$ and $f \in \mathbf{F}[x_1, \ldots, x_n]$ a defining polynomial for X. Since the action of S_n on $\mathbf{F}[x_1, \ldots, x_n]$ is degree-preserving and stabilizes the homogeneous ideal generated by f, we know that there exists a linear character ε of S_n such that

$$\sigma \cdot f = \varepsilon(\sigma)\, f, \qquad \sigma \in S_n.$$

If ε is trivial, then f is symmetric and we are done. The other case, $\varepsilon = \mathrm{sg}$, cannot occur, because by Lemma 3.2.7 we would conclude that $f = \Delta \cdot g$ for some symmetric polynomial g. But then

$$X = Z(g) \cup Z(\Delta) = Z(g) \cup \bigcup_{i<j} Z(x_i - x_j)$$

would be reducible, and thus singular (since smooth hypersurfaces of positive dimension are irreducible). But an S_n-hypersurface is required by definition to be smooth.

Now let X be a S_n-hypersurface of type II. As a Zariski closed subset of $\mathbf{P}^{n-1}$, we can write $X = Z(f, h)$, where $h = x_1 + \cdots + x_n$ and f is a homogeneous polynomial. The fact that X is stable under the action of S_n means that the ideal (f, h) also is, so that for every $\sigma \in S_n$ there exist polynomials $a(\sigma)$, $\varepsilon(\sigma)$ such that

$$\sigma \cdot f = a(\sigma)h + \varepsilon(\sigma)f.$$

Since f and h are homogeneous, we can require that $a(\sigma)$ be homogeneous degree $\deg f - 1$ and $\varepsilon(\sigma)$ of degree 0; with these assumptions, the polynomials $a(\sigma)$ and $\varepsilon(\sigma)$ become unique. Indeed, if $\sigma \cdot f = a'(\sigma)h + \varepsilon'(\sigma)f$ with $a'(\sigma)$ and $\varepsilon'(\sigma)$ of degree $\deg f - 1$ and 0, respectively, we would have

$$(a(\sigma) - a'(\sigma))h = (\varepsilon'(\sigma) - \varepsilon(\sigma))f,$$

hence $h \mid (\varepsilon'(\sigma) - \varepsilon(\sigma))f$. But h cannot divide f, because then $(h, f) = (h)$ and X would not be a proper subset of H, so we conclude that $\varepsilon'(\sigma) = \varepsilon(\sigma)$, which in turn implies that $a'(\sigma) = a(\sigma)$. By a similar argument, we see that $\varepsilon(\sigma) \neq 0$, else we would have

$$\sigma \cdot f = a(\sigma)h, \quad \text{i.e.} \quad f = (\sigma^{-1} \cdot a(\sigma))h,$$

which is impossible for the same reason.

Now let $\sigma, \tau \in S_n$. If we apply σ to $\tau \cdot f = a(\tau)h + \varepsilon(\tau)f$, using the fact that h and constant polynomials are symmetric, we obtain

$$(\sigma\tau) \cdot f = \big(\sigma \cdot a(\tau) + \varepsilon(\tau)a(\sigma)\big)h + \varepsilon(\tau)\varepsilon(\sigma)f.$$

In particular, it follows by uniqueness that $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$, i.e. that $\varepsilon : S_n \to \mathbf{F}^\times$ is a linear character. Now consider the "averaged" polynomial

$$F := \sum_\sigma \varepsilon(\sigma)\, \sigma \cdot f = \left(\sum_\sigma a(\sigma)\varepsilon(\sigma)\right)h + \left(\sum_\sigma \varepsilon(\sigma)^2\right)f.$$

Since the only two possibilities for ε are the trivial or the sign character, which both have order 2, in both cases

$$\sum_\sigma \varepsilon(\sigma)^2 = n!,$$

which is invertible in $\mathbf{F}$, so that $(h, F) = (h, f)$. Now it is easily seen that

$$\sigma \cdot F = \varepsilon(\sigma)F \qquad \text{for all } \sigma \in S_n.$$

If $\varepsilon = \mathbf{1}$, then F is symmetric and we are done. On the other hand, if $\varepsilon = \mathrm{sg}$, then as above we can write F as $\Delta \cdot G$ where G is symmetric, and in this case it is easily checked that $Z(h, F)$ is reducible, hence singular if $n \geq 4$, contradicting the assumption that X is smooth. □

There are only two significant cases not treated by this proposition. The first one is that of S_2-hypersurfaces of type I, i.e. of finite collections of points $X \subseteq \mathbf{P}^1$ stable under the involution $z \mapsto 1/z$. Such as set is a disjoint union of pairs $\{z_i, 1/z_i\}$ with $z_i^2 \neq 1$, as well as maybe the points $z = 1$ or $z = -1$. The case where $1 \in X$ corresponds to a presence of a factor $\Delta = x_2 - x_1$ in the defining polynomial. The other case is that of S_3-hypersurfaces of type II, i.e. of collections of points $X \subseteq \mathbf{P}^1$ which are stable under the action of

$$S_3 \simeq \mathrm{Stab}\{0, 1, \infty\} \subseteq \mathrm{PGL}_2(\mathbf{F}).$$

Now, since the characteristic of $\mathbf{F}$ is large enough, a classical result in invariant theory states that the graded ring $\mathbf{F}[x_1, \ldots, x_n]^{S_n}$ of symmetric polynomials is a polynomial ring in elementary symmetric polynomials, $e_1, \ldots, e_n$, which are defined by the

formal identity

$$\prod_{i=1}^{n}(t - x_i) = t^n - e_1 t^{n-1} + e_2 t^{n-2} - \ldots + (-1)^n e_n.$$

Equivalently, instead of the elementary symmetric polynomials, we can use the power basis $p_1, \ldots, p_n$, where the j^{th} *power polynomial* is

$$p_j := x_1^j + \cdots + x_n^j.$$

Lemma 3.2.9. *Let $\alpha \in \mathbf{F}^\times$ of order d, $\sigma \in S_n$, and $j \geq 1$. If $d \nmid j$, then p_j vanishes on $\operatorname{Fix}_\alpha \sigma$. If $d \mid j$, then, in the homogeneous coordinates of $\mathbf{P}^{m_d(\sigma)-1}$,*

$$\iota_{\alpha,\sigma}^* p_j(\mathbf{x}) = \sum_{d|\lambda_i} \lambda_i \, x_i^j,$$

where $\iota_{\alpha,\sigma} : \mathbf{P}^{m_d(\sigma)-1} \hookrightarrow \mathbf{P}^{n-1}$ denotes the embedding described in the proof of Proposition 3.2.5.

Proof. Recall that $\iota_{\alpha,\sigma}(\mathbf{x}) = [x_1 \mathbf{z}_{\lambda_1}(\alpha) : \cdots : x_m \mathbf{z}_{\lambda_m}(\alpha)]$, with $x_i = 0$ unless $d \mid \lambda_i$, so that

$$\iota_{\alpha,\sigma}^* p_j(\mathbf{x}) = \sum_{d|\lambda_i} x_i^j \, p_j(\mathbf{z}_{\lambda_i}(\alpha)).$$

Finally, we note that , for $d \mid \lambda_i$,

$$p_j(\mathbf{z}_{\lambda_i}(\alpha)) = \sum_{r=1}^{\lambda_i} \alpha^{jr} = \begin{cases} 0 & \text{if } \alpha^j \neq 1, \\ \lambda_i & \text{if } \alpha^j = 1, \end{cases}$$

so the conclusion follows. □

As any symmetric polynomial can be written (uniquely) as a polynomial in the power basis $p_1, \ldots, p_n$, we can use this lemma to obtain information about the behavior a general symmetric polynomial on the fixed locus $\operatorname{Fix} \sigma$ of a permutation $\sigma \in S_n$. As the lemma holds not just for $j \leq n$ but for all values of j, it could be useful to allow power polynomials p_j with $j > n$ as well, at the cost of losing the uniqueness of the expression of a symmetric polynomial in terms of the power polynomials.

Accordingly, one is led to consider the graded algebra $\mathbf{F}[P_1, P_2, \ldots]$ of polynomials in a countable number of indeterminates P_j, $j \geq 1$, with $\deg P_j = j$, together with

the surjective map of graded algebras

$$\mathrm{ev} : \mathbf{F}[P_1, P_2, \dots] \longrightarrow \mathbf{F}[x_1, \dots, x_n]^{S_n}.$$

For any fixed integer $D \geq 1$ and partition $\lambda = \{\lambda_1, \dots, \lambda_m\}$ of D, define

$$P_\lambda := \prod_{i=1}^{m} P_{\lambda_i},$$

so that any homogeneous polynomial $F \in \mathbf{F}[P_1, P_2, \dots]$ of degree D can we written as

$$F = \sum_{\lambda \vdash D} a_\lambda P_\lambda, \qquad a_\lambda \in \mathbf{F}.$$

Definition 3.2.10. For $d \geq 1$, and $\lambda = \{\lambda_1, \dots, \lambda_m\}$ a partition, we write

$$d \mid \lambda \iff d \mid \lambda_i, \quad i = 1, \dots, m.$$

The *d-part* of a polynomial $F = \sum_\lambda a_\lambda P_\lambda \in \mathbf{F}[P_1, P_2, \dots]$ is defined to be

$$F_d := \sum_{d \mid \lambda} a_\lambda P_\lambda,$$

i.e. the sum of monomials in F involving only variables P_j with $d \mid j$.

With these new notations, we can rephrase Lemma 3.2.9 as follows.

Corollary 3.2.11. *Let $\sigma \in S_n$, $\alpha \in \mathbf{F}^\times$ of order d and $f \in \mathbf{F}[x_1, \dots, x_n]^{S_n}$ a symmetric polynomial. Write $f = \mathrm{ev}(F)$ and $f_d := \mathrm{ev}(F_d)$. Then, on $\mathrm{Fix}_\alpha \sigma$, we have*

$$\iota^*_{\alpha,\sigma} f = \iota^*_{\alpha,\sigma} f_d,$$

which can be evaluated using that for $d \mid j$,

$$\iota^*_{\alpha,\sigma} p_j(\mathbf{x}) = \sum_{d \mid \lambda_i} \lambda_i \, x_i^j.$$

We now introduce a class of polynomials for which the analysis can easily be carried out in a general fashion.

Definition 3.2.12. A polynomial $F \in \mathbf{F}[P_1, P_2, \dots]$ will be called *special* if for every $d \geq 1$, either $F_d = F$ or $F_d = 0$.

If F is a special polynomial, let D be the maximal integer d such that $F_d = F$. Then it is easy to check that for $d \geq 1$,

$$F_d = F \iff d \mid D,$$

i.e. that D is actually the least common multiple all the integers d such that $F_d = F$. We will call D the *primitive degree* of F. As $D \mid \deg F$, we might call the *bidegree* of F the pair (D, r) such that

$$\deg F = Dr.$$

Given a partition $\lambda = \{\lambda_1, \ldots, \lambda_m\}$, let $\gcd(\lambda) := \gcd(\lambda_1, \ldots, \lambda_m)$. Then a special polynomial of primitive degree D is any polynomial which can be written as

$$F = \sum_{\gcd(\lambda)=D} a_\lambda P_\lambda.$$

Remark. Writing $\Pi(n)$ for the set of partitions of n, and

$$\Pi_d(n) := \{\lambda \in \Pi(n) \mid \gcd(\lambda) = d\},$$

then clearly we have a decomposition

$$\Pi(n) = \bigsqcup_{d|n} \Pi_d(n).$$

Let $\pi(n)$, resp. $\pi_d(n)$, denote the cardinality of $\Pi(n)$, resp. $\Pi_d(n)$. As there is a natural bijection $\Pi_d(n) \xrightarrow{\sim} \Pi_1(n/d)$ given by $\lambda \mapsto \lambda/d$, it follows that

$$\pi(n) = \sum_{d|n} \pi_d(n) = \sum_{d|n} \pi_1(n/d) = \sum_{d|n} \pi_1(d).$$

By the Moebius inversion formula, we find the expression

$$\pi_1(n) = \sum_{d|n} \pi(d)\mu(n/d).$$

This gives a formula for the dimension $\pi_D(Dr) = \pi_1(r)$ of the vector space of special polynomials of bidegree (D, r) in terms of the partition function π and the Moebius function μ.

By extension, an S_n-hypersurface will be called *special of bidegree* (D, r) if it can be realized as $Z(f)$ or $Z(f, h)$ with $f = \mathrm{ev}(F)$ and F a special polynomial of bidegree (D, r). Thus if F is a special polynomial, then $Z(\mathrm{ev}(F))$ and $Z(\mathrm{ev}(F), h)$ will be special hypersurfaces *provided they are smooth.*

Example 3.2.13. For $\alpha \in \mathbf{F}$, consider the 0-dimensional variety $X_\alpha \subset \mathbf{P}^1$ defined by the symmetric polynomial

$$f_\alpha = (\alpha+1)x_1^5 + x_1^4x_2 + x_1^3x_2^2 + x_1^2x_2^3 + x_1x_2^4 + (\alpha+1)x_2^5.$$

By computing the discriminant of this polynomial, one sees that X_α is smooth provided

$$16(\alpha+1)(3\alpha+1)^3(\alpha^2+8\alpha+8)^2 \neq 0.$$

In that case, X_α is a special S_2-hypersurface of bidegree $(1, 5)$ since f_α can be written

$$f_\alpha = p_1p_4 + \alpha p_2p_3 = \mathrm{ev}(P_1P_4 + \alpha P_2P_3).$$

Note however that the expression of f_α as the evaluation of a special polynomial is not unique, since in $\mathbf{F}[x_1, x_2]$ we have

$$p_3 = \frac{3}{2}p_1p_2 - \frac{1}{2}p_1^3 \quad \text{and} \quad p_4 = p_1p_2^2 + \frac{1}{2}p_2^2 - \frac{1}{2}p_1^4,$$

so that f_α can also be written as

$$f_\alpha = \mathrm{ev}\left(P_1^2P_2^2 + \frac{1}{2}(\alpha+3)P_1P_2^2 - \frac{\alpha}{2}P_1^3P_2 - \frac{1}{2}P_1^5\right).$$

Moreover, note that a special polynomial can have the same evaluation as another special polynomial of different bidegree (e.g. P_3), or even of a non-special polynomial (e.g. P_4).

For special symmetric hypersurfaces we can give an explicit description of the character of S_n acting on the primitive cohomology.

Theorem 3.2.14. *Let $n \geq 3$ and X be a special S_n-hypersurface of bidegree (D, r). If X has type I, the character χ_{pr} of the action of S_n on the primitive cohomology*

$H^{n-2}_{\mathrm{pr}}(W)$ *of* X *is given by*

$$\chi_{\mathrm{pr}}(\sigma) = (-1)^n \left\{ 1 + \frac{1}{r}\left(\frac{1}{D} \sum_{d|D} \varphi(d)(1-Dr)^{m_d(\sigma)} - 1 \right) \right\} \qquad \text{for } \sigma \in S_n.$$

If X *has type II, the character* χ_{pr} *of the action of* S_n *on* $H^{n-3}_{\mathrm{pr}}(X)$ *is given by*

$$\chi_{\mathrm{pr}}(\sigma) = (-1)^{n+1} \left\{ 1 + \frac{1}{r}\left(\frac{1}{D} \sum_{d|D} \varphi(d)(1-Dr)^{m'_d(\sigma)} - 1 \right) \right\} \qquad \text{for } \sigma \in S_n,$$

where $m'_1(\sigma) = m_1(\sigma) - 1$ *and* $m'_d(\sigma) = m_d(\sigma)$ *for* $d \geq 1$.

Proof. Write $X = Z(f)$ or $X = Z(h, f)$ where $f = \mathrm{ev}(F)$ and F is a special polynomial primitive degree D, and for every $d \geq 1$ let $f_d := \mathrm{ev}(F_d)$. Fix $\sigma \in S_n$. For both types we have a decomposition of the fixed locus as

$$\operatorname{Fix} \sigma|_X = \bigsqcup_{\alpha \in \mathbf{F}^\times} \operatorname{Fix}_\alpha \sigma|_X,$$

with $\operatorname{Fix}_\alpha \sigma|_X = X \cap \mathbf{P}_{\alpha,\sigma}$, where $\mathbf{P}_{\alpha,\sigma}$ stands for $\operatorname{Fix}_\alpha \sigma \simeq \mathbf{P}^{m_d(\sigma)-1}$.

Consider first the case where X has type I. The inverse image of X in $\mathbf{P}^{m_d(\sigma)-1}$ via the inclusion $\iota_{\alpha,\sigma}$ is defined by $\iota^*_{\alpha,\sigma} f = \iota^*_{\alpha,\sigma} f_d$ by Corollary 3.2.11, so there are two cases.

- If $f_d = 0$, then $\operatorname{Fix}_\alpha \sigma|_X = \mathbf{P}_{\alpha,\sigma}$, hence $\chi(\operatorname{Fix}_\alpha \sigma|_X) = m_d(\alpha)$.
- If $f = f_d$, then $\operatorname{Fix}_\alpha \sigma|_X$ corresponds to the hypersurface $Z(\iota^*_{\alpha,\sigma} f)$ in $\mathbf{P}^{m_d(\sigma)-1}$. Using the chain rule and Lemma 3.2.9, for every i such that $d \mid \lambda_i(\sigma)$ we have

  $$\frac{\partial \iota^*_{\alpha,\sigma} f}{\partial x_i}(\mathbf{x}) = \lambda_i(\sigma) \frac{\partial f}{\partial y_j}(\iota_{\alpha,\sigma}(\mathbf{x})),$$

  where j is any index occurring in the i^{th} cycle σ_i of σ. By the Jacobian criterion and the fact that all parts $\lambda_i(\sigma)$ of $\lambda(\sigma)$ are invertible in $\mathbf{F}$, it follows that $\mathbf{x}$ is a singular point of $\iota^{-1}_{\alpha,\sigma}(X)$ if and only if $\iota_{\alpha,\sigma}(\mathbf{x})$ is a singular point of X. Since X is smooth, we conclude that $\operatorname{Fix}_\alpha \sigma|_X$ is a smooth projective hypersurface of dimension $m_d(\sigma) - 2$ and degree $\deg f_d = Dr$, so that, by Corollary 2.3.6,

  $$\chi(\operatorname{Fix}_\alpha \sigma|_X) = m_d(\sigma) + \frac{(1-Dr)^{m_d(\sigma)} - 1}{Dr}.$$

Putting everything together and using the identity from Lemma 3.2.6, we find that

$$\begin{aligned}\chi(\operatorname{Fix}\sigma) &= \sum_{\alpha} \chi(\operatorname{Fix}_\alpha \sigma|_X) \\ &= \sum_{d\nmid D} \varphi(d)\, m_d(\sigma) + \sum_{d\mid D} \varphi(d) \left(m_d(\sigma) + \frac{(1-Dr)^{m_d(\sigma)}-1}{Dr} \right) \\ &= n + \sum_{d\mid D} \varphi(d) \left(\frac{(1-Dr)^{m_d(\sigma)}-1}{Dr} \right) \\ &= n + \frac{1}{r}\left(\frac{1}{D} \sum_{d\mid D} \varphi(d)(1-Dr)^{m_d(\sigma)} - 1 \right).\end{aligned}$$

Then the announced formula follows by Proposition 3.2.2.

The case of a symmetric hypersurface of type II is very similar, except that now the inverse image of $\operatorname{Fix}_\alpha \sigma$ in $\mathbf{P}^{m_d(\alpha)-1}$ is defined by $Z(\iota_{\alpha,\sigma}^* f_d, \iota_{\alpha,\sigma}^* h_d)$ and a new situation can occur.

- If $d = 1$, then $h_d = h$, $f_d = f$, and we get a smooth hypersurface $Z(\iota_{\alpha,\sigma}^* f, \iota_{\alpha,\sigma}^* h)$ of degree $\deg f$ inside $Z(\iota_{\alpha,\sigma}^* h) \simeq \mathbf{P}^{m_1(\sigma)-2}$, of dimension $m_1(\sigma) - 3 = m_1'(\sigma) - 2$.
- If $d > 1$ and $d \nmid D$, then $f_d = h_d = 0$ and $\operatorname{Fix}_\alpha \sigma|_X = \mathbf{P}_{\alpha,\sigma}$ as before.
- If $d > 1$ and $d \mid D$, then $f_d = f$ and $h = 0$, hence we get a smooth hypersurface of dimension $m_d(\sigma) - 2$ as previously.

This finishes the proof. □

3.3 Existence of special symmetric hypersurfaces

In this section we describe examples of hypersurfaces yielding representations of the symmetric group given by the formulas in Theorem 3.2.14. The first thing to note is that there exists special symmetric hypersurfaces of type I of any primitive degree over fields of sufficiently large characteristic.

Indeed, for every $D \geq 1$, consider the hypersurface $X_D \subset \mathbf{P}^{n-1}$, $n \geq 3$, defined by the homogeneous special equation $P_D = x_1^D + \cdots + x_n^D = 0$ of degree $(D, 1)$. If $D \neq 0$ in $\mathbf{F}$, then X_D is a smooth hypersurface of degree D and dimension $n - 2$ which is stable under the action of S_n. By Theorem 3.2.14, the character χ_D of the action of

S_n on $H^{n-2}_{\mathrm{pr}}(X)$ is given by the class function

$$\chi_D = (-1)^n\left(1 + \frac{1}{D}\sum_{d|D}\varphi(d)\big((1-D)^{m_d} - 1\big)\right).$$

For small values of n one can explicitly decompose it into irreducible characters of S_n.

Proposition 3.3.1. *The character χ_{pr} of S_3 acting on the primitive cohomology of a S_3-curve of type I and bidegree $(D,1)$ satisfies*

$$6\chi_D = \begin{cases} (D-1)(D-5)\,\mathbf{1} \oplus (D-1)(D+1)\,\mathrm{sg} \oplus 2(D-1)(D-2)\,V & \text{if } (D,6)=1,\\ (D-2)(D-4)\,\mathbf{1} \oplus (D-2)(D+2)\,\mathrm{sg} \oplus 2(D-1)(D-2)\,V & \text{if } (D,6)=2,\\ (D-3)^2\,\mathbf{1} \oplus (D^2+3)\,\mathrm{sg} \oplus 2D(D-3)\,V & \text{if } (D,6)=3,\\ (D^2-6D+12)\,\mathbf{1} \oplus D^2\,\mathrm{sg} \oplus 2D(D-3)\,V & \text{if } (D,6)=6, \end{cases}$$

where V denotes the irreducible representation of degree 2 of S_3.

Proof. One only needs to compute the inner products of χ_{pr} with $\mathbf{1}$, sg and V. □

In particular, $\chi_1 = \chi_2 = 0$, and

$$\begin{aligned} \chi_3 &= 2\cdot\mathrm{sg},\\ \chi_4 &= 2\cdot\mathrm{sg} \oplus 2\cdot V,\\ \chi_6 &= 2\cdot\mathbf{1} \oplus 6\cdot\mathrm{sg} \oplus 6\cdot V,\\ \chi_7 &= 2\cdot\mathbf{1} \oplus 8\cdot\mathrm{sg} \oplus 10\cdot V, \end{aligned}$$

and these are the only cases where some irreducible representation of S_3 occur with multiplicity at most 2.

On the other hand, special symmetric hypersurfaces of type II need not exist in all primitive degrees, as the representation theory of S_n imposes certain conditions on the value of the parameters for which they can exist.

Proposition 3.3.2. *For $\ell \geq 1$, let θ'_ℓ be the class function on S_n defined by*

$$\theta'_\ell = \ell^{m'_1} = \ell^{m_1-1}.$$

If there exist a special S_n-hypersurface of type II and bidegree $(D,1)$, then θ'_{D-1} is the character of a characteristic 0 representation of S_n.

Proof. Suppose $X = Z(f,h)$ is a bidegree $(D,1)$ special S_n-hypersurface of type II, and let Y be a special S_n-hypersurface of type I of bidegree $(D,1)$, e.g. given by $P_D = 0$ as above. Then, by Theorem 3.2.14, in the character χ of the representation of S_n on $H^{n-2}_{\mathrm{pr}}(X) \oplus H^{n-3}_{\mathrm{pr}}(Y)$, the terms corresponding to $d > 1$ cancel out to leave

$$\chi = \frac{(-1)^n}{D}\Big(\big((1-D)^{m_1} - 1\big) - \big((1-D)^{m_1-1} - 1\big)\Big) = (-1)^{n-m_1}(D-1)^{m_1-1}.$$

Claim. For every permutation $\sigma \in S_n$, $\mathrm{sg}(\sigma) = (-1)^{n-m_1(\sigma)}$.

Indeed, write $\sigma = \sigma_1 \cdots \sigma_m$ as a product of disjoint cycles, of lengths $\lambda_1, \ldots, \lambda_m$. Then

$$\mathrm{sg}(\sigma) = \prod_{i=1}^{m} \mathrm{sg}(\sigma_i) = \prod_{i=1}^{m} (-1)^{\lambda_i - 1} = (-1)^{\sum_{i=1}^{m}(\lambda_i - 1)} = (-1)^{n-m}.$$

Hence, as the character of $H^{n-2}_{\mathrm{pr}}(X) \oplus H^{n-3}_{\mathrm{pr}}(Y)$ computed above is $\chi = \mathrm{sg} \otimes \theta'_{D-1}$, we conclude that $\theta'_{D-1} = \mathrm{sg} \otimes \chi$ is the character of a representation of S_n. □

We can also consider the closely related class function $\theta_\ell := \ell\theta'_\ell = \ell^{m_1}$ on S_n.

Proposition 3.3.3. *For $\ell \geq 1$, $\theta_\ell = \ell^{m_1}$ is the character of a representation of S_n.*

Proof. Let R be any finite ring with ℓ elements, and consider $T := R^n$, the R-linear standard permutation representation of S_n, as a *set* on which S_n acts. We can then form the associated E-linear permutation representation $E[T]$, thought of as the set of functions $T \to E$. The value of the character of this representation at $\sigma \in S_n$ is $\chi_{E[T]}(\sigma) = |\operatorname{Fix}_T(\sigma)|$. Let $\lambda(\sigma) = \{\lambda_1, \ldots, \lambda_m\}$ be the partition associated to σ. Without loss of generality, we can assume that σ lies in the image of $S_{\lambda_1} \times \cdots \times S_{\lambda_m}$ in S_n under the standard embedding; then it is easy to check that

$$\operatorname{Fix}_T(\sigma) = \{(\underbrace{r_1, \ldots, r_1}_{\lambda_1}, \ \ldots, \ \underbrace{r_m, \ldots, r_m}_{\lambda_m}) \mid r_1, \ldots, r_m \in R\}.$$

Since the set of fixed points $\operatorname{Fix}_T(\sigma)$ is a free R-module of rank $m_1(\sigma)$, we conclude that

$$\chi_{E[T]}(\sigma) = |\operatorname{Fix}_T(\sigma)| = |R|^{m_1(\sigma)} = \ell^{m_1(\sigma)} = \theta_\ell(\sigma).$$

Thus θ_ℓ is the character of the E-linear representation of S_n on $E[T]$. □

As $m_1 \geq 1$ on S_n, certainly all the values of $\theta_\ell = \ell^{m_1}$ are divisible by ℓ, i.e. the values of θ'_ℓ are integers. To ask whether θ'_ℓ is a character or not is equivalent to ask

whether

$$(\theta'_\ell, \phi) = \frac{1}{\ell}(\theta_\ell, \phi) \in \mathbf{N}, \quad \text{i.e.} \quad \ell \mid (\theta_\ell, \phi),$$

for all irreducible representations ϕ of S_n.

Proposition 3.3.4. *If ℓ is prime, then $\theta'_\ell = \ell^{m_1-1}$ is the character of a representation of S_n if and only if $\ell \nmid n$.*

Proof. For ($\Leftarrow$), let $R = \mathbf{Z}/\ell\mathbf{Z}$ and consider the function $f : R^n \to R$ defined by $f(r_1, \ldots, r_n) = \sum r_i$. If S_n acts on R^n via the standard permutation representation and trivially on R, then the short exact sequence

$$0 \longrightarrow \operatorname{Ker} f \longrightarrow R^n \longrightarrow R \longrightarrow 0$$

of $R[S_n]$-modules splits via the section $r \mapsto n^{-1}(r, \ldots, r)$ because n is invertible in R. Hence $R^n = R \oplus \operatorname{Ker} f$ as R-linear representations, which imply that $E[R^n]$ is isomorphic to $E[R] \otimes E[\operatorname{Ker} f]$, and since $E[R]$ is an ℓ-dimensional trivial representation, it follows that the character of $E[\operatorname{Ker} f]$ is $\theta_\ell/\ell = \theta'_\ell$.

Now for ($\Rightarrow$), suppose that θ'_ℓ is the character of a representation of S_n. In particular, the multiplicity $(\theta'_\ell, \mathbf{1}) = (\theta_\ell, \mathbf{1})/\ell$ of the trivial character in θ'_ℓ is a non-negative integer.

Claim.

$$(\theta_\ell, \mathbf{1}) = \frac{1}{n!} \sum_{\sigma \in S_n} \ell^{m_1(\sigma)} = \binom{n+\ell-1}{n}.$$

Indeed, the left-hand side is the dimension of the space of invariants $E[R^n]^{S_n} = E[R^n/S_n]$, so this multiplicity is the number of orbits for the action of S_n on R^n. The orbits correspond to unordered lists $r_1, \ldots, r_n$ of elements of R, with repetition allowed, and the number of these is the number of ways to put n identical balls (the coefficients r_i) into ℓ boxes (the elements of R), which is given by the right-hand side.

Hence, if θ'_ℓ is the character of a representation, then ℓ divides

$$(\theta_\ell, \mathbf{1}) = \binom{n+\ell-1}{n} = \frac{(n+\ell-1)\cdots(n+1)}{(\ell-1)!}.$$

Since ℓ is prime, it has to divide $n+i$ for some $1 \leq i < \ell$, hence cannot divide n. □

Along with Proposition 3.3.2, this combinatorial fact yields the following.

Corollary 3.3.5. *When ℓ is a prime, no special S_n-hypersurface of type II and bidegree $(\ell+1, 1)$ can exist when $\ell \mid n$.*

Remark. The proof of Proposition 3.3.4 actually shows that even when ℓ is composite, θ'_ℓ is a character of S_n when $(n,\ell)=1$, because the only thing that was needed was that n be invertible in $\mathbf{Z}/\ell\mathbf{Z}$. This suggests the following conjecture:

$$\theta'_\ell \text{ is a character of } S_n \iff (n,\ell)=1.$$

In addition of being true when ℓ is prime, this conjecture was checked by explicitly computing the decomposition into irreducibles of θ_ℓ for $n \leq 5$, as well as machine computations for $n, \ell \leq 20$. A proof in the general case probably requires explicit formulas for other multiplicities (θ_ℓ, ϕ), $\phi \neq \mathbf{1}$. If the conjecture is true, it means that a special S_n-hypersurface of type II and bidegree $(D,1)$ can only exist when n and $D-1$ are coprime.

It is important to note that not all hypersurfaces in $\mathbf{P}^{n-1}$ or in the diagonal hyperplane $H \simeq \mathbf{P}^{n-2}$ which are stable under the permutation action of S_n are special. Nevertheless, Corollary 3.2.11 can still be used to compute the character χ_{pr} of S_n on their primitive cohomology. Here is an interesting example.

Example 3.3.6. Consider the 1-parameter family of curves $W_{\alpha:\beta} \subseteq \mathbf{P}^3$ defined by

$$\sum_{i=1}^{4} x_i = \alpha\Big(\sum_{i=1}^{4} x_i^4\Big) + \beta\Big(\sum_{i=1}^{4} x_i^2\Big)^2 = 0, \qquad (\alpha:\beta) \in \mathbf{P}^1.$$

Computing the appropriate discriminant, they are seen to be smooth over any field of characteristic different from 2 outside the exceptional values

$$(\alpha:\beta) \in \{(0:1), (2:-1), (4:-1), (12:-7)\}.$$

Using Corollary 3.2.11, one finds that χ_{pr} is given by the following table.

σ	1	(12)	(123)	(12)(34)	(1234)
χ_{pr}	6	-2	0	-2	2

It is thus readily seen that

$$\chi_{\mathrm{pr}} = 2 \cdot (\mathrm{sg} \otimes \mathrm{Perm}^\circ),$$

where Perm° denotes the irreducible permutation representation of S_4.

This family can be described in another way, taking advantage of the exceptional

homomorphism $S_4 \twoheadrightarrow S_3$. Let $H \subseteq \mathbf{P}^3$ be the hyperplane $x_1 + \cdots + x_4 = 0$. Away from characteristic 2, we have an isomorphism

$$\varphi : H \xrightarrow{\sim} \mathbf{P}^2$$

given by

$$\begin{cases} y_1 = \quad x_1 - x_2 - x_3 + x_4 \\ y_2 = -x_1 + x_2 - x_3 + x_4 \\ y_3 = -x_1 - x_2 + x3 + x4 \end{cases}$$

with inverse described by

$$\begin{cases} x_1 = \quad y_1 - y_2 - y_3 \\ x_2 = -y_1 + y_2 - y_3 \\ x_3 = -y_1 - y_2 + y_3 \\ x_4 = y_1 + y_2 + y_3. \end{cases}$$

Under this identification, S_4 acts by transport of structure on $\mathbf{P}^2$ as the semi-direct product $V_4 \rtimes S_3$, where S_3 permutes the coordinates and a non-trivial elements $(ij)(k4)$ of the Klein 4-group V_4, with $\{i, j, k\} = \{1, 2, 3\}$, acts by changing the sign of y_k. Under φ, the family $W_{\alpha:\beta}$ corresponds to the family of curves in $\mathbf{P}^2$ with S_4 action defined by

$$\alpha(y_1^4 + y_2^4 + y_3^4) + \beta(y_1^2y_2^2 + y_2^2y_3^2 + y_3^2y_1^2) = 0 \qquad (\alpha : \beta) \in \mathbf{P}^1,$$

where $(\alpha : \beta)$ is a new parameter related to the old one by a rational projective transformation. This family was studied extensively since its discovery more than a century ago, as it contains all the projective curves of genus 3 admitting S_4 as automorphisms (for a modern account, see [48]). Considered as defined over $\mathbf{Q}$, the fact that the L-function of $H^1(W_{\alpha:\beta})$ factors as the cube of the L-function of a compatible system of 2-dimensional representations can be explained geometrically by the fact that the Jacobian of $W_{\alpha:\beta}$ decomposes as 3 isogenous elliptic curves.

In the next section we turn to the description of a discrete family of hypersurfaces of varying dimension which includes some special hypersurfaces of type II.

3.4 The hypersurfaces $W_\ell^{m,n}$

Throughout this section we fix two integers $m, n \geq 0$ and $\mathbf{F}$ an algebraically closed field in which $(m+n)! \neq 0$. Let $\mathbf{A}^{m+n}$ denote the affine space $\mathbf{A}^m \times \mathbf{A}^n$ over $\mathbf{F}$, and by convention, points in $\mathbf{A}^{m+n}$ will be written as $(\mathbf{x}, \mathbf{y})$ with $\mathbf{x} \in \mathbf{A}^m$, $\mathbf{y} \in \mathbf{A}^n$. Similarly, $\mathbf{P}^{m+n-1}$ will denote the projective space $\mathbf{P}(\mathbf{A}^{m+n})$, with homogeneous coordinates $[\mathbf{x}; \mathbf{y}]$. Thus, as before, $m+n$ refers to the number of variables.

Definition 3.4.1. For any integer $\ell \geq 1$, let $W_\ell^{m,n}$ denote the projective variety in $\mathbf{P}^{m+n-1}$ defined by the two homogeneous equations

$$\sum_{i=1}^{m} x_i = \sum_{j=1}^{n} y_j, \qquad \sum_{i=1}^{m} x_i^{\ell+1} = \sum_{j=1}^{n} y_j^{\ell+1}.$$

To alleviate the notation, we will denote $W_\ell^{0,n}$ by W_ℓ^n.

These varieties will arise naturally in our study of distribution of certain exponential sums in the next chapter, generalizing the study of W_2^n made by Livné [39] in connection with cubic exponential sums.

Note that the varieties $W_\ell^{m,n}$ could be considered as schemes over $\mathbf{Z}$. They admit an action of the product $S_m \times S_n$ via its standard embedding in S_{m+n} which permutes the homogeneous coordinates in $\mathbf{P}^{m+n-1}$. In particular, W_ℓ^n is an hypersurface admitting an action of S_n defined by the power polynomials

$$p_1 = p_{\ell+1} = 0,$$

hence will be a special S_n-hypersurface of type II and bidegree $(\ell+1, 1)$ *when it is smooth.* And of course,

$$W_\ell^{m,n} \simeq W_\ell^{n,m}$$

under the automorphism of $\mathbf{P}^{m+n-1}$ which interchanges the roles of $\mathbf{x}$ and $\mathbf{y}$, so we will often make the tacit assumption that $n \geq m$.

Our first task is to decide when these varieties are smooth, and to describe their singular locus when they are not.

Lemma 3.4.2. *Suppose that $\ell \neq -1$ in $\mathbf{F}$. The singular locus of $W_\ell^{m,n}$ can be described as the set of points $[\mathbf{x}, \mathbf{y}] \in \mathbf{P}^{m+n-1}$ with all homogeneous coordinates $x_i, y_j \in \mu_\ell(\mathbf{F})$*

and satisfying

$$\sum_{i=1}^{m} x_i = \sum_{j=1}^{n} y_j.$$

Proof. The Jacobian matrix

$$\begin{pmatrix} 1 & \cdots & 1 & -1 & \cdots & -1 \\ (\ell+1)x_1^\ell & \cdots & (\ell+1)x_m^\ell & -(\ell+1)y_1^\ell & \cdots & -(\ell+1)y_n^\ell \end{pmatrix}$$

has rank 1 if and only if

$$(\ell+1)x_i^\ell = (\ell+1)y_j^\ell = \lambda, \qquad i = 1, \ldots, m,\ j = 1, \ldots, n,$$

for some constant $\lambda \in \mathbf{F}$. Since $\ell + 1$ is invertible in $\mathbf{F}$ and at least one homogeneous coordinate can be taken to be 1, these conditions reduce to

$$x_i^\ell = y_j^\ell = 1,$$

i.e. all the homogeneous coordinates x_i, y_j can be taken to be ℓ^{th} roots of unity in $\mathbf{F}$. Since $a^{\ell+1} = a$ for $a \in \mu_\ell(\mathbf{F})$, the two conditions that such a point has to satisfy to belong to $W_\ell^{m,n}$ degenerate to the single equation $\sum_i x_i = \sum_j y_j$. □

We can get a slightly more explicit description of the singular locus as follows.

Proposition 3.4.3. *Let ζ be a primitive ℓ^{th} root of unity in $\mathbf{F}$, and $m_\zeta(t)$ its minimal polynomial over the prime field $\mathbf{F}_0$. If $\ell \neq 1$ in $\mathbf{F}$, the singular locus of $W_\ell^{m,n}$ is the set of points of the form*

$$\sigma \cdot [\underbrace{\zeta^0}_{m_0} : \underbrace{\zeta^1}_{m_1} : \cdots : \underbrace{\zeta^\ell}_{m_\ell} : \underbrace{\zeta^0}_{n_0} : \underbrace{\zeta^1}_{} : \cdots : \underbrace{\zeta^\ell}_{n_\ell}]$$

where $\sigma \in S_m \times S_n$ and $\sum_k (n_k - m_k)t^k$ is divisible by $m_\zeta(t)$ in $\mathbf{F}_0[t]$.

Proof. Let $[\mathbf{x}; \mathbf{y}]$ be a point whose homogeneous coordinates are ℓ^{th} roots of unity, and for every $0 \leq k \leq \ell$, let

$$m_k := |\{i \mid x_i = \zeta^k\}| \quad \text{and} \quad n_k := |\{j \mid y_j = \zeta^k\}|.$$

According to Lemma 3.4.2, the condition that $[\mathbf{x};\mathbf{y}]$ is a singular point becomes

$$\sum_k m_k \zeta^k = \sum_k n_k \zeta^k,$$

i.e. the polynomial $\sum_k (n_k - m_k) t^k \in \mathbf{F}_0[t]$ vanishes at $t = \zeta$. □

We will now restrict ourselves to situations for which we have an explicit knowledge of $m_\zeta(t)$. Recall that if $\mathbf{F}$ has characteristic 0 and ℓ is prime, then

$$m_\zeta(t) = \Phi_\ell(t) = \frac{t^\ell - 1}{t - 1} = 1 + t + \cdots + t^{\ell-1}.$$

In positive characteristic p, for ℓ a prime different from p, the degree of $m_\zeta(t)$ is seen to be the smallest integer r for which $\ell \mid p^r - 1$, i.e. the order of p in $(\mathbf{Z}/\ell\mathbf{Z})^\times$. It follows that the degree of $m_\zeta(t)$ is $\ell - 1$ precisely when the prime p is inert in the cyclotomic extension $\mathbf{Q}(\zeta_\ell)$.

By a small abuse of terminology, we will decreet that *0 is inert in* $\mathbf{Q}(\zeta_\ell)$, so that we have

$$m_\zeta(t) = 1 + t + \cdots + t^{\ell-1} \iff \operatorname{char}\mathbf{F} \text{ is inert in } \mathbf{Q}(\zeta_\ell).$$

Under this condition, we can give an explicit description of the singularities of $W_\ell^{m,n}$.

Proposition 3.4.4. *Let ℓ be a prime such that* $\operatorname{char}\mathbf{F}$ *is inert in $\mathbf{Q}(\zeta_\ell)$ and $\ell \neq -1$ in $\mathbf{F}$. If $\ell \nmid n - m$, then $W_\ell^{m,n}$ is a smooth hypersurface of dimension $m + n - 3$. If $n - m = a\ell$,*

$$\operatorname{Sing} W_\ell^{m,n} = S_m \times S_n \cdot \{[\mathbf{x}; \underbrace{\zeta^0}_{a} : \underbrace{\zeta^1}_{a} : \cdots : \underbrace{\zeta^{\ell-1}}_{a} : \mathbf{x}] \mid \mathbf{x} \in \mu_\ell(\mathbf{F})^m\},$$

and these singularities are all ordinary double points. More precisely, the tangent cone at a singular point $t \in \operatorname{Sing} W_\ell^{m,n}$ is a smooth quadric Q_t defined over $\mathbf{F}_0(t) \subseteq \mathbf{F}_0(\zeta)$. When its dimension is even, it has signed determinant

$$\Delta = \begin{cases} 1 & \text{if } \ell = 2, \\ (-1)^{a/2} & \text{if } \ell > 2. \end{cases}$$

Proof. When $\operatorname{char}\mathbf{F}$ is inert in $\mathbf{Q}(\zeta_\ell)$, Proposition 3.4.3 tells us that there exists an

integer a such that

$$\sum_{k=0}^{\ell-1}(n_k - m_k)t^k = a\Phi_\ell(t) \text{ in } \mathbf{F}_0[t],$$

i.e. the differences $m_k - n_k$ are all congruent modulo the characteristic of $\mathbf{F}$. But the integers $n_k - m_k$ lie in the bounded interval $[-n, m]$ of length $m+n$. If $\mathbf{F}$ has positive characteristic, then by our hypothesis we have $\operatorname{char}\mathbf{F} > m+n$ so that the differences $m_k - n_k$ actually have to be equal in $\mathbf{Z}$. In all cases, we conclude that there exists an integer $a \in \mathbf{Z}$ such that $n_k = m_k + a$ for $0 \leq k < \ell$.

Summing over k, we find that this implies $n = m + a\ell$, so clearly $W_\ell^{m,n}$ can have no singularities when $\ell \nmid n - m$. On the other, when $\ell \mid n - m$, by writing $n = m + a\ell$ we obtain the announced description for the singular locus.

Let us now consider a singular point $[\mathbf{x}; \mathbf{y}]$ with $x_i = \zeta^{r_i}$ and $y_j = \zeta^{s_j}$. Setting $z_i = x_i + \zeta^{r_i}$ and $w_j = y_j + \zeta^{s_j}$ in the equations for $W_\ell^{m,n}$, we get

$$\sum_i z_i - \sum_j w_j = 0, \qquad \sum_{u=0}^{\ell+1}\binom{\ell+1}{u}\Big(\sum_i z_i^u\,\zeta^{r_i(\ell+1-u)} - \sum_j w_j^u\,\zeta^{s_j(\ell+1-u)}\Big) = 0.$$

Without loss of generality, let us assume that $r_0 = s_0 = 0$. Then, setting $w_0 = 0$, we get affine equations for the tangent cone,

$$\sum_i z_i = \sum_j{}' w_j, \qquad \sum_i z_i^2\,\zeta^{-r_i} = \sum_j{}' w_j^2\,\zeta^{-s_j}$$

where $\sum'$ means that we omit the index 1. From the first equation, we can isolate

$$w_1 = \sum_i{}' z_i - \sum_j{}' w_j$$

and substitute in the second one to get

$$\sum{}'(1+\zeta^{-r_i})z_i^2 + 2\sum{}' z_i z_{i'} + \sum{}'(1-\zeta^{-s_j})w_j^2 + 2\sum{}' w_j w_{j'} - 2\sum{}' z_i w_j = 0.$$

In other terms, the tangent cone is a quadric $Q(t)$ with defining matrix

$$\begin{pmatrix} E - D & -E \\ -E & E + D_1 \end{pmatrix},$$

where the E's denote matrices having all entries 1, D is the diagonal matrix with

the ζ^{r_i}'s on its diagonal ($2 \leq i \leq m$), and D_1 the diagonal matrix with the ζ^{s_j}'s ($2 \leq j \leq n$). Up to a reordering of the variables, D_1 can be written as

$$\begin{pmatrix} D & \\ & \delta \end{pmatrix}, \qquad \delta = \mathrm{diag}(I_a, \zeta I_a, \ldots, \zeta^{\ell-1} I_a).$$

Using standard manipulations, the matrix for $Q(t)$,

$$\begin{pmatrix} E-D & -E & -E \\ -E & E+D & E \\ -E & E & E+\delta \end{pmatrix}$$

can be transformed into

$$\begin{pmatrix} D-I & D & \\ D & 0 & \\ & & E+\delta \end{pmatrix}.$$

Now write D as $\mathrm{diag}(I, D')$ where no entry in D' is 1. Then the first block in the above quadric is equivalent to the square matrix of size $2(m-1) \times 2(m-1)$

$$\mathrm{diag}(2I, -2I, D'-I, -(D'-I)) \sim \mathrm{diag}(I, -I),$$

which has determinant $(-1)^{m-1} \neq 0$, and signed determinant $\Delta = 1$.

Lemma 3.4.5. *If $\delta = \mathrm{diag}(d_1, \ldots, d_n)$ is a diagonal matrix with non-zero entries, then*

$$\det(E+\delta) = \det\delta \left(1 + \sum_{i=1}^{n} \frac{1}{d_i}\right).$$

Proof. By adding a line of 1's and using elementary row operations, we get

$$\det(E+\delta) = \det \begin{pmatrix} E+\delta & 0 \\ E & 1 \end{pmatrix} = \det \begin{pmatrix} \delta & -E \\ E & 1 \end{pmatrix}.$$

In the permutation expansion for the determinant of this last matrix, the only contributing terms are those associated to the identity and the transpositions $(i \;\; n+1)$, $i = 1, \ldots, n$, yielding

$$\det(E+\delta) = \prod_{j=1}^{n} d_j + \sum_{i=1}^{n} \prod_{j \neq i} d_j = \det\delta \left(1 + \sum_{i=1}^{n} \frac{1}{d_i}\right),$$

which is the announced formula. □

In particular, for δ as above,

$$\det(E+\delta) = \det\delta = \left(\prod_{j=0}^{\ell-1}\zeta^j\right)^a = \zeta^{(\ell-1)\ell a/2} = \begin{cases}(-1)^a & \ell = 2,\\ 1 & \ell \text{ odd.}\end{cases}$$

From Section 2.4, this implies that the tangent cone $Q(t)$ is a smooth quadric of dimension $m+n-4 = 2(m-2)+a\ell$. When this dimension is odd, i.e. both a and ℓ are odd, we are done. Otherwise, $Q(t)$ is a quadric of even dimension and signed discriminant

$$(-1)^{a\ell/2}\det(E+\delta),$$

from which the conclusion follows by considering separately the cases $\ell = 2$ and $\ell > 2$ (in which case a needs to be even). □

3.5 Some explicit computations

In this section we carry some computations about the representations of the symmetric group(s) afforded by the varieties of the previous section.

First, let us consider the first few *smooth* varieties of the form W_2^n over a field $\mathbf{F}$ of odd characteristic larger than n (or 0). According to Proposition 3.4.5, W_2^n is smooth if and only if n is odd, in which case it is a special S_n-hypersurface of bidegree $(3,1)$ and dimension $n-3$. Accordingly, from Theorem 3.2.14, the character χ_n of the representation of S_n on $H^{n-3}_{\mathrm{pr}}(W_2^n)$ is given by

$$\chi_n = \frac{(-2)^{m_1-1} - (-2)^{m_3+1}}{3}. \tag{3.6}$$

The case $n = 1$ is trivially uninteresting, and W_2^3 consists of the 3 points

$$(1:-1:0), (1:0:-1); (0:1:-1),$$

which S_3 permutes transitively. Hence, $H^0(W_2^3)$ is the standard permutation representation of S_3, and we can check that (3.7) tells us that $\chi_3 = \mathrm{Perm}^\circ$, the 2-dimensional corresponding irreducible representation. For $n = 5$ and $n = 7$, the following can be easily obtained by looking at tables of irreducible characters (for example in [9]) and computing the appropriate inner products.

Proposition 3.5.1. *We have the following decompositions into irreducibles:*

$$\chi_5 = \mathrm{sg} \oplus \psi,$$
$$\chi_7 = 2 \cdot \mathrm{sg} \oplus (\mathrm{sg} \otimes \mathrm{Perm}^\circ) \oplus \theta,$$

where ψ is an irreducible character of degree 5 of S_5, and θ an irreducible character of degree 14 of S_7.

Considering W_2^5 and W_2^7 as defined over $\mathbf{Q}$, the compatible systems of Galois representations of $\mathrm{Gal}_{\mathbf{Q}}$ afforded by corresponding multiplicities and whose existence is guaranteed by Theorem 3.1.4 will be explicitly computed in Chapter 5. Of particular interest is the 2-dimensional compatible system

$$M_{\mathrm{sg}}(H^4_{\mathrm{pr}}(W_2^7)).$$

Let us write down further facts about W_2^7 for future reference in Section 5.7.

Proposition 3.5.2. *The variety W_2^7 has good reduction outside $\{3, 5, 7\}$ and primitive Hodge numbers*

$$h^{0,4} = h^{4,0} = 0, \quad h^{1,3} = h^{3,1} = 1, \quad h^{2,2} = 20.$$

Proof. From Proposition 3.4.5, we know that W_2^7 has good reduction for all primes $p > 7$. We need to show that it has good reduction at $p = 2$, i.e. that the variety W_2^7 over $\mathbf{F}_2$ is smooth. Lemma 3.4.2 still applies to show that the singularities in characteristic 2 are all the points with projective coordinates which are square roots of 1 lying in W_2^7. But the only square root of 1 over $\mathbf{F}_2$ is 1, and the point

$$(1 : 1 : 1 : 1 : 1 : 1 : 1)$$

does not belong to W_2^7. The Hodge numbers are obtained by expanding the generating series of Proposition 2.3.4 up to order 4. □

Note that the same argument used in the proof actually shows that for n odd, the smooth hypersurface W_2^n has good reduction at 2.

Chapter 4

Distribution of exponential sums

This chapter is concerned with how exponential sums of the form

$$\sum_{x \in \mathbf{F}_q} \exp\left(\frac{2\pi i}{p} \operatorname{tr}_{\mathbf{F}_q/\mathbf{F}_p}(f(x))\right)$$

are distributed, on average, as $q \to \infty$. By this, we mean that for every fixed prime power $q = p^r$, we consider the set of all such exponential sums corresponding to polynomials $f \in \mathbf{F}_q[x]$ of a fixed degree (in fact, we will also specify a set of weights corresponding to the powers of x that are allowed to appear in f). We are interested in the behavior of this set as $q \to \infty$, where it will always be understood that the characteristic p goes to infinity along with q. The motivation for this problem starts with the Sato-Tate conjecture [63]: if E is an elliptic curve over $\mathbf{Q}$ without complex multiplication, the angles

$$\theta_p(E) := \cos^{-1}\left(\frac{a_p(E)}{2\sqrt{p}}\right)$$

are equidistributed as $p \to \infty$ with respect to the measure $\sin^2\theta d\theta$. As the coefficient $a_p(E) = |E(\mathbf{F}_p)| - p - 1$ appearing above can be interpreted as the trace of Frob_p on the Tate module of E, this is really a conjecture about the distribution of the traces of Frobenius elements as p varies; a general framework for problems this type have been considered (see e.g. [56]). Birch [4] proved that the Sato-Tate conjecture holds *on average*, the average being taken over the set of Weierstrass equations $y^2 = x^3 + \alpha x + \beta$ for elliptic curves over $\mathbf{F}_p$. In the same paper, he suggested that the same should be

true if the coefficients $a_p(E_{\alpha,\beta})$ appearing above are replaced by the exponential sums

$$B_p(\alpha,\beta) = \sum_{x\in\mathbf{F}_p} \exp\left(\frac{2\pi i}{p}(\alpha x^3+\beta x)\right), \qquad \alpha,\beta\in\mathbf{F}_p, \alpha\neq 0.$$

This conjecture was later proved by Livné [39] by relating the n^{th} moment of the average of these exponential sums to the number of points on the variety W_2^n from Chapter 3 (in our notation). Asymptotics for the moments were obtained by analyzing the étale cohomology of these varieties, thus proving Birch's conjecture that the exponential sums $B_p(\alpha,\beta)$, when normalized to lie in $[-1,1]$ by dividing by $2\sqrt{p}$, are equidistributed on average with respect to the Sato-Tate measure when $p\to\infty$.

It should be noted that étale cohomology enters in two distinct ways in the picture. The first one is providing the bound $2\sqrt{p}$ for the *values* of the exponential sums $B_p(\alpha,\beta)$ under consideration. This follows from a very general machinery which interprets exponential sums as the traces of Frobenius on étale cohomology with values in a certain sheaf, from which estimates can be derived by purity [14, 33, 38]. The second way is by relating the *moments of the average* of these exponential sums to the number of points on varieties of varying dimension, which can then be estimated or computed using étale cohomology as well.

In this chapter we generalize Livné's treatment of the cubic exponential sums mentioned above by allowing more general sets of weights for the polynomial f. We first give in Section 4.1 a short discussion trying to explain the theoretical importance of these exponential sums by interpreting them as Fourier transforms for the function counting the number of solutions of a system of equations over $\mathbf{F}_q$, as is well-known. In Section 4.2 we give a brief review of the relevant notions from measure theory to justify why equidistribution problems can be translated into the study of the limit behavior of the relevant moments.

In Section 4.3, we define a very general class of exponential sums and, generalizing Livné, prove a key result (Theorem 4.3.2) relating the moments of their average with the number of points on certain varieties. A significant difference with [39] is that the cubic exponential sums considered there are *real-valued*, so that a 1-parameter family of moments is enough to study their distribution. In our case, the exponential sums are in general *complex-valued*, hence a 2-parameter family of moments is needed. This is why the relevant varieties come with a "bipartite" action of $S_m\times S_n$ (instead of S_n only in [39]).

In Section 4.4 we finally specialize to very specific sets of weights for which the

understanding of the cohomology of the relevant varieties is within our reach. Accordingly, after discussing a few easy cases, we concentrate mainly on the case of exponential sums of weights $\{1, \ell+1\}$, where ℓ is prime (note that the case $\ell = 2$ was the one studied by Livné). In this case, the relevant varieties are the varieties $W_\ell^{m,n}$ introduced in Section 3.4. Referring to Schoen's results (Section 2.5) about the cohomology of hypersurfaces with ordinary double points, we see that the moments are essentially related to the subprimitive cohomology of $W_\ell^{m,n}$ (or rather, its dual, the "supprimitive cohomology"). The main result is Theorem 4.4.7, which states precisely this relationship, generalizing the main result of [39].

It should be pointed out however that, except in some special cases, this does not prove that the exponential sums are equidistributed on average, but merely provides formulae for the moments of the limit distribution, if it exists. To prove equidistribution, one would need to know that these limits are actually the moments of some measure. This fact, although probably true (see [30]), is not proven here.

4.1 Exponential sums as Fourier transforms

Exponential sums, under various guises, are ubiquitous in number theory. For an overview of their many uses, see e.g. [35]. Here is one way of justifying their theoretical importance, following Katz [29], by interpreting them as the Fourier transforms of the number of solutions of equations over finite fields.

Let $f \in \mathbf{Z}[x]$ be a polynomial. Over any finite field $\mathbf{F}_q$, one may consider the equation $f(x) = 0$, or more generally the equation $f(x) = \alpha$, for $\alpha \in \mathbf{F}_q$. The number of solutions off all these equations, for fixed q, is encoded by the function

$$N_{f,q} : \mathbf{F}_q \longrightarrow \mathbf{N}, \qquad \alpha \mapsto |\{x \in \mathbf{F}_q \,|\, f(x) = \alpha\}|.$$

We lose no information if we consider $N_{f,q}$ as a complex-valued function on the additive group $\mathbf{F}_q$, and as such we can consider its Fourier decomposition

$$N_{f,q} = \sum_{\psi \in \widehat{\mathbf{F}_q}} \widehat{N_{f,q}}(\psi)\, \psi, \quad \text{with} \quad \widehat{N_{f,q}}(\psi) = \sum_{\alpha \in \mathbf{F}_q} N_{f,q}(\alpha)\, \psi(\alpha) = \sum_{x \in \mathbf{F}_q} \psi(f(x)).$$

Now the choice of a non-trivial additive character ψ_q on $\mathbf{F}_q$ identifies $\mathbf{F}_q$ with $\widehat{\mathbf{F}_q}$ via $a \mapsto \psi_{a,q}$, where $\psi_{a,q}(x) = \psi_q(ax)$. Under this identification, the Fourier coefficients

of $N_{f,q}$ are given by

$$\widehat{N_{f,q}}(a) = \sum_{x \in \mathbf{F}_q} \psi_q(af(x)).$$

More generally, if we start with a finite collection $\mathbf{f} = (f_1, \ldots, f_m) \in \mathbf{Z}[x]^m$ of polynomials, we can just as well consider the counting function for the corresponding system of equations

$$N_{\mathbf{f},q} : \mathbf{F}_q^m \longrightarrow \mathbf{N}, \qquad (\alpha_1, \ldots, \alpha_m) \mapsto |\{x \in \mathbf{F}_q \mid f_i(x) = \alpha_i,\ i = 1, \ldots, m\}|,$$

whose Fourier coefficients are given by

$$\widehat{N_{\mathbf{f},q}}(\mathbf{a}) = \sum_{x \in \mathbf{F}_q} \psi_q(a_1 f_1(x) + \cdots a_m f_m(x)),$$

and these are precisely the kind of exponential sums we want to consider here. In particular, obtaining asymptotics for these exponential sums yields information about the limit behavior of $N_{\mathbf{f},q}$ as $q \to \infty$, i.e. about how the number of solutions of the original system of equations behaves over larger and larger finite fields.

4.2 Equidistribution

This section summarizes the basic notions of measure theory which lie at the core of this chapter. Let X be a compact metric space, and denote by $B(X)$ the set of all finite signed Borel measures on X. We endow $B(X)$ with the topology of "setwise" convergence, i.e. we say that $\nu_n \to \nu$ if $\nu_n(A) \to \nu(A)$ for all Borel sets A.

Proposition 4.2.1 (Riesz representation theorem)**.** *The pairing*

$$\nu(f) := \int_X f d\nu$$

identifies $B(X)$ with the continuous dual of the space $C(X)$ of real-valued continuous functions on X (equipped with the norm of uniform convergence).

Since characteristic functions of Borel sets can be uniformly approximated by continuous functions, we see that

$$\nu_n \to \nu \iff \nu_n(f) \to \nu(f) \quad \text{for all } f \in C(X),$$

i.e. the topology we are considering on $B(X)$ is the so-called weak-* topology.

Definition 4.2.2. Let E be a Borel subset of X, endowed with a measure ν_E. The *characteristic measure* associated to the pair (E, ν_E) is the probability measure δ_E on X defined by

$$\delta_E(A) := \frac{\nu_E(A \cap E)}{\nu_E(E)}, \qquad \text{or equivalently} \qquad \delta_E(f) := \frac{\nu_E(f|_E)}{\nu_E(1)}.$$

For example, if $E = \{x\}$ consists of a single point, then $\delta_E = \delta_x$, the Dirac delta distribution concentrated at x. More generally, if E is a finite set endowed with the counting measure, then

$$\delta_E = \frac{1}{|E|} \sum_{x \in E} \delta_x.$$

Definition 4.2.3. A sequence of finite subsets (A_n) of X is said to be *equidistributed with respect to* ν if

$$\delta_{A_n} \to \nu.$$

If (a_n) is a sequence of distinct elements of X, then setting $A_n := \{a_1, \ldots, a_n\}$ we recover the usual notion of equidistribution for a sequence.

Proposition 4.2.4 (Weyl's criterion)**.** *Let X be a compact metric space and Σ a subset of $C(X)$ with dense span. Then $\nu_n \to \nu$ if and only if $\nu_n(f) \to \nu(f)$ for all $f \in \Sigma$.*

Note that it might often be more convenient to work with complex-valued functions instead of limiting ourselves to real-valued. This is mostly innocuous as

$$C(X, \mathbf{C}) = C(X) \otimes \mathbf{C} = C(X) \oplus C(X)i.$$

Example 4.2.5. The roots of unity $\mu_n(\mathbf{C})$ are uniformly equidistributed in the unit circle $\mathbf{S}^1 = \mathbf{R}/\mathbf{Z}$. This can easily be shown using Weyl's criterion applied to the dense set $\{e_n \,|\, n \in \mathbf{Z}\}$ where $e_n(t) := e^{2n\pi it}$.

Proposition 4.2.6 (Stone-Weierstrass)**.** *If X is a compact subset of $\mathbf{R}^n$, the polynomial functions are dense in $C(X)$.*

Consequently, together with Weyl's criterion, this means that a measure ν on a compact subset X of $\mathbf{R}^n$ is completely characterized by its *(real) moments*

$$M_\alpha(\nu) := \nu(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = \int_X x_1^{\alpha_1} \cdots x_n^{\alpha_n} d\nu, \qquad \alpha_i \geq 0.$$

If X is a compact subset of $\mathbf{C}^n \simeq \mathbf{R}^{2n}$ with coordinates $z_j = x_j + iy_j$, then since

$$\mathbf{C}[x_1, y_1, \ldots, x_n, y_n] = \mathbf{C}[z_1, \overline{z}_1, \ldots, z_n, \overline{z}_n],$$

we can use instead the *(complex) moments*

$$M^{\alpha,\beta}(\nu) := \nu(z_1^{\alpha_1}\overline{z}_1^{\beta_1} \cdots z_n^{\alpha_n}\overline{z}_n^{\beta_n}), \qquad \alpha_i, \beta_i \geq 0.$$

The problem of trying to reconstruct the measure ν from its moments $M_\alpha(\nu)$, or even deciding whether a sequence of numbers are the moments of some measure, has a long and interesting history, see e.g. [59]. In the case where $X = [0, 1]$, this is called the Hausdorff moment problem. However, we shall not be too much concerned with these matters here.

A classical example of an equidistribution result in number theory is Dirichlet's theorem on the distribution of primes in arithmetic progressions, which can be stated as: for every fixed $m \in \mathbf{N}$, the images of the set of primes

$$E_n := \{p \nmid m,\, p \leq n\}$$

are uniformly equidistributed in $(\mathbf{Z}/m\mathbf{Z})^\times$ as $n \to \infty$.

More generally, we have the following well-known result, strengthening the statement of Proposition 1.4.3.

Proposition 4.2.7 (Chebotarev density theorem)**.** *Let K be a number field and L a finite Galois extension of K. Then the sets*

$$E_n := \{\mathrm{Frob}_\mathfrak{p} \mid \mathfrak{p} \text{ prime of } K \text{ unramified in } L, N(\mathfrak{p}) \leq n\}$$

are uniformly equidistributed amongst the weighted conjugacy classes of $\mathrm{Gal}(L/K)$.

4.3 Exponential sums

For every finite field $\mathbf{F}_q$ with $q = p^r$ elements, consider $\psi_q : (\mathbf{F}_q, +) \to \mathbf{C}^\times$ a fixed non-trivial additive character. To every nonempty finite subset $\kappa \subset \mathbf{N}$ of *weights*, and

vector $\mathbf{a} = (a_k)_{k\in\kappa} \in \mathbf{F}_q^\kappa$, with $a_{\max\kappa} \neq 0$, we associate the *exponential sum*

$$B_\kappa(q, \mathbf{a}) := \sum_{x\in\mathbf{F}_q} \psi_q\Big(\sum_{k\in\kappa} a_k x^k\Big) \in \mathbf{C}. \tag{4.1}$$

Following Birch [4] and Livné [39], we would like to understand how these complex numbers are distributed, on average, when $q \to \infty$ (here it will always be understood that $p \to \infty$ as $q \to \infty$).

A trivial case is when $\kappa = \{1\}$ or $\kappa = \{0, 1\}$; then it is easily seen that $B_\kappa(q, \mathbf{a}) = 0$ for all $\mathbf{a}$ with $a_1 \neq 0$. This can be rephrased by saying that these exponential sums are equidistributed with respect to the Dirac distribution δ_0 concentrated at the origin. In other cases, the Weil estimate coming from purity [14] yields the following.

Proposition 4.3.1. *If* $\max\kappa > 0$ *and* $p > \max\kappa$*, then* $|B_\kappa(q, \mathbf{a})| \leq (\max\kappa - 1)\sqrt{q}$.

From now on, we will assume that $\max\kappa > 1$, i.e. we exclude the trivial cases considered above. Then the normalized exponential sums

$$b_\kappa(q, \mathbf{a}) := \frac{B_\kappa(q, \mathbf{a})}{(\max\kappa - 1)\sqrt{q}}$$

lie in the closed unit disk $\mathbf{D} = \{z \in C : |z| \leq 1\}$, and we would like to understand their limit average distribution as $q \to \infty$ (if it exists). More precisely, let $\delta_\kappa(q)$ denote the characteristic measure associated to the finite set

$$\left\{b_\kappa(q, \mathbf{a}) \mid \mathbf{a} \in \mathbf{F}_q^\kappa,\ a_{\max\kappa} \neq 0\right\}.$$

From Section 4.2, we know that a measure on $\mathbf{D}$ is determined by its action on the monomials $z^m\overline{z}^n$, for $m, n \geq 0$. If $\delta_\kappa(q)$ has a limit measure ν as $q \to \infty$, then the moments of $\delta_\kappa(q)$ converge to the moments of ν. As a consequence, we would like to understand the asymptotic behavior of the quantities

$$M_\kappa^{m,n}(q) := M^{m,n}(\delta_\kappa(q)) = \frac{1}{q^{|\kappa|-1}(q-1)}{\sum_{\mathbf{a}}}' b_\kappa(q, \mathbf{a})^m \overline{b_\kappa(q, \mathbf{a})}^n \qquad \text{as } q \to \infty,$$

where $\sum'$ means that the sum ranges over all vectors $\mathbf{a} = (a_k)_{k\in\kappa} \in \mathbf{F}_q^\kappa$ with $a_{\max\kappa} \neq 0$. Letting $N = m + n$, for ease of manipulation we will prefer to work instead with the

closely related quantities

$$\begin{aligned} V_\kappa^{m,n}(q) &:= (\max\kappa - 1)^N q^{N/2} M_\kappa^{m,n}(q) \\ &= \frac{1}{q^{|\kappa|-1}(q-1)} {\sum_{\mathbf{a}}}' B_\kappa(q,\mathbf{a})^m \overline{B_\kappa(q,\mathbf{a})}^n \end{aligned} \tag{4.2}$$

Define $W_{\kappa,\mathrm{aff}}^{m,n}$ to be the variety in $\mathbf{A}^{m+n} = \mathbf{A}^N$ cut out by the $|\kappa|$ homogeneous equations

$$\sum_{i=1}^m x_i^k = \sum_{j=1}^n y_j^k \qquad (k \in \kappa),$$

and let $W_\kappa^{m,n}$ the projective variety in $\mathbf{P}^{N-1}$ over which $W_{\kappa,\mathrm{aff}}^{m,n}$ is the affine cone. The following proposition, generalizing [39, lemma 4.1] attributed to Birch, is key to our analysis by relating the moments of exponential sums to the number of points on the varieties $W_{\kappa,\mathrm{aff}}^{m,n}$.

Theorem 4.3.2. *Let* $\kappa' := \kappa \setminus \{\max\kappa\}$. *Then*

$$V_\kappa^{m,n}(q) = \frac{1}{q-1}\Big(q\,|W_{\kappa,\mathrm{aff}}^{m,n}(\mathbf{F}_q)| - |W_{\kappa',\mathrm{aff}}^{m,n}(\mathbf{F}_q)| \Big).$$

In particular, this formula implies that $V_\kappa^{m,n}(q)$, hence the limit distribution as $q \to \infty$ of the exponential sums (4.1), if it exists, does not depend on the choice of the additive character $\psi_q \neq \mathbf{1}$.

Proof. By splitting the sum $\sum_{\mathbf{a}\in\mathbf{F}_q^\kappa} B_\kappa(q,\mathbf{a})^m \overline{B_\kappa(q,\mathbf{a})}^n$ into terms with $a_{\max\kappa} = 0$ and terms with $a_{\max\kappa} \neq 0$, using the expression (4.2) for $V_\kappa^{m,n}$ we obtain

$$\sum_{\mathbf{a}\in\mathbf{F}_q^\kappa} B_\kappa(q,\mathbf{a})^m \overline{B_\kappa(q,\mathbf{a})}^n = \sum_{\mathbf{a}'\in\mathbf{F}_q^{\kappa'}} B_{\kappa'}(q,\mathbf{a}')^m \overline{B_{\kappa'}(q,\mathbf{a}')}^n + q^{|\kappa|-1}(q-1)V_\kappa^{m,n}(q). \tag{4.3}$$

Now, by using (4.1) and distributivity, we find

$$\begin{aligned} \sum_{\mathbf{a}\in\mathbf{F}_q^\kappa} B_\kappa(q,\mathbf{a})^m \overline{B_\kappa(q,\mathbf{a})}^n &= \sum_{\mathbf{a}\in\mathbf{F}_q^\kappa} \Big(\prod_{i=1}^m B_\kappa(q,\mathbf{a})\Big)\Big(\prod_{j=1}^n \overline{B_\kappa(q,\mathbf{a})}\Big) \\ &= \sum_{\mathbf{a}\in\mathbf{F}_q^\kappa} \Big(\prod_{i=1}^m \sum_{x_i\in\mathbf{F}_q} \prod_{k\in\kappa} \psi_q(a_k x_i^k)\Big)\Big(\prod_{j=1}^n \sum_{y_j\in\mathbf{F}_q} \prod_{k\in\kappa} \psi_q(-a_k y_j^k)\Big) \\ &= \sum_{\mathbf{x}\in\mathbf{F}_q^m} \sum_{\mathbf{y}\in\mathbf{F}_q^n} \prod_{k\in\kappa} \sum_{a_k\in\mathbf{F}_q} \psi_q\Big(a_k\Big(\sum_{i=1}^m x_i^k - \sum_{j=1}^n y_j^k\Big)\Big). \end{aligned}$$

But by orthogonality of characters, we have

$$\sum_{a_k \in \mathbf{F}_q} \psi_q\Big(a_k\Big(\sum_{i=1}^{m} x_i^k - \sum_{j=1}^{n} y_j^k\Big)\Big) = \begin{cases} q & \text{if } (\mathbf{x},\mathbf{y}) \in W_{k,\mathrm{aff}}^{m,n}, \\ 0 & \text{else,} \end{cases}$$

from which is follows that

$$\prod_{k\in\kappa} \sum_{a_k \in \mathbf{F}_q} \psi_q\Big(a_k\Big(\sum_{i=1}^{m} x_i^k - \sum_{j=1}^{n} y_j^k\Big)\Big) = \begin{cases} q^{|\kappa|} & \text{if } (\mathbf{x},\mathbf{y}) \in \cap_{k\in\kappa} W_{\{k\},\mathrm{aff}}^{m,n} = W_{\kappa,\mathrm{aff}}^{m,n}, \\ 0 & \text{else.} \end{cases}$$

Consequently,

$$\sum_{\mathbf{a}\in\mathbf{F}_q^\kappa} B_\kappa(q,\mathbf{a})^m \overline{B_\kappa(q,\mathbf{a})}^n = q^{|\kappa|}\,|W_{\kappa,\mathrm{aff}}^{m,n}(\mathbf{F}_q)|,$$

and by the exact same argument applied to κ' we get

$$\sum_{\mathbf{a}'\in\mathbf{F}_q^{\kappa'}} B_{\kappa'}(q,\mathbf{a}')^m \overline{B_{\kappa'}(q,\mathbf{a}')}^n = q^{|\kappa|-1}\,|W_{\kappa',\mathrm{aff}}^{m,n}(\mathbf{F}_q)|.$$

Substituting these two last expressions in (4.3) and isolating $V_\kappa^{m,n}(q)$ concludes the proof. □

Corollary 4.3.3. *If $|\kappa| \geq 2$ and $0 \in \kappa$, then*

$$M_\kappa^{m,n}(q) = \begin{cases} 0 & \text{if } m \neq n, \\ M_{\kappa\setminus 0}^{m,n} & \text{if } m = n. \end{cases}$$

Proof. First, note that if κ is a set of weights such that $0 \in \kappa$, then one of the defining equations of $W_{\kappa,\mathrm{aff}}^{m,n}$ is $m = n$, so that

$$W_{\kappa,\mathrm{aff}}^{m,n} = \begin{cases} \varnothing & \text{if } m \neq n, \\ W_{\kappa\setminus 0,\mathrm{aff}}^{m,n} & \text{if } m = n. \end{cases}$$

Hence, if $0 \in \kappa$ and $|\kappa| \geq 2$, then $0 \in \kappa'$ as well, and the above remark applies to both κ and κ' to give

$$W_{\kappa,\mathrm{aff}}^{m,n} = W_{\kappa',\mathrm{aff}}^{m,n} = \varnothing \quad \text{when } m = n,$$

$$W_{\kappa,\mathrm{aff}}^{m,n} = W_{\kappa\setminus 0,\mathrm{aff}}^{m,n}, \quad W_{\kappa',\mathrm{aff}}^{m,n} = W_{\kappa'\setminus 0,\mathrm{aff}}^{m,n} \quad \text{when } m \neq n.$$

The conclusion follows by Theorem 4.3.2 and formula (4.2). □

Consequently, without real loss of generality we can restrict our attention to the cases where $0 \notin \kappa$.

Corollary 4.3.4. *When $0 \notin \kappa$, $\kappa \neq \varnothing$,*

$$V_\kappa^{m,n}(q) = 1 + q\,|W_\kappa^{m,n}(\mathbf{F}_q)| - |W_{\kappa'}^{m,n}(\mathbf{F}_q)|.$$

Proof. In this situation, since $W_{\kappa,\mathrm{aff}}^{m,n}$ is the affine cone over $W_\kappa^{m,n}$, we have

$$|W_{\kappa,\mathrm{aff}}^{m,n}(\mathbf{F}_q)| = 1 + (q-1)|W_\kappa^{m,n}(\mathbf{F}_q)|,$$

and similarly for κ'. It then follows from Theorem 4.3.2 that

$$V_\kappa^{m,n} = \frac{1}{q-1}\Big(q + q(q-1)|W_\kappa^{m,n}(\mathbf{F}_q)| - 1 - (q-1)|W_{\kappa'}^{m,n}(\mathbf{F}_q)|\Big),$$

which simplifies to the announced expression. □

It follows that asking for an asymptotic as $q \to \infty$ for $V_\kappa^{m,n}$ is the same as asking for asymptotics for the number of points on the projective varieties $W_\kappa^{m,n}$, which can in principle be read from their étale cohomology thanks to the trace formula.

4.4 Equidistribution results

In this section, we look at the cohomology of the varieties $W_\kappa^{m,n}$ in increasing order of complexity for κ to derive the corresponding statements for the moments of the exponential sums $b_\kappa(q, \mathbf{a})$, using the machinery developed in the previous section.

Case $\kappa = \{k\}$, $k > 1$. Suppose that $p = \operatorname{char} \mathbf{F}_q > k$, so that $W_\kappa^{m,n}$ is a smooth hypersurface of degree k and dimension $N-2$ over $\mathbf{F}_q$. Since as Galois modules we have (Corollary 2.3.3)

$$H^\bullet(W_\kappa^{m,n}) \simeq H^\bullet(\mathbf{P}^{N-2}) \oplus H_{\mathrm{pr}}^{N-2}(W_\kappa^{m,n}),$$

the trace formula yields

$$|W_\kappa^{m,n}(\mathbf{F}_q)| = \frac{q^{N-1}-1}{q-1} + (-1)^N \operatorname{tr}(\mathrm{Frob}_q \mid H_{\mathrm{pr}}^{N-2}(W_\kappa^{m,n})).$$

From Corollary 4.3.4 and the fact that $W_{\varnothing}^{m,n} = \mathbf{P}^{N-1}$, we get

$$\begin{aligned} V_{\kappa}^{m,n}(q) &= 1 + q\left(\frac{q^{N-1}-1}{q-1} + (-1)^N \operatorname{tr}(\mathrm{Frob}_q \mid H_{\mathrm{pr}}^{N-2}(W_{\kappa}^{m,n}))\right) - \left(\frac{q^N-1}{q-1}\right) \\ &= (-1)^N q \operatorname{tr}(\mathrm{Frob}_q \mid H_{\mathrm{pr}}^{N-2}(W_{\kappa}^{m,n})). \end{aligned}$$

From (4.2), it follows that

$$M_{\kappa}^{m,n}(q) = \frac{(-1)^N}{(k-1)^N q^{N/2-1}} \operatorname{tr}(\mathrm{Frob}_q \mid H_{\mathrm{pr}}^{N-2}(W_{\kappa}^{m,n})). \tag{4.4}$$

We see that, in this case, a precise asymptotic for $M_{\kappa}^{m,n}(q)$ as $q \to \infty$ depends crucially on the Galois representation afforded by the primitive cohomology of $W_{\kappa}^{m,n}$. We can obtain a crude estimate for the moments by using purity, which guarantees that

$$\begin{aligned} |\operatorname{tr}(\mathrm{Frob}_q \mid H_{\mathrm{pr}}^{N-2}(W_{\kappa}^{m,n}))| &\leq q^{(N-2)/2} \dim H_{\mathrm{pr}}^{N-2}(W_{\kappa}^{m,n}) \\ &= q^{N/2-1} \frac{(k-1)^N + (-1)^N(k-1)}{k}. \end{aligned}$$

by the formula for the dimension of the primitive cohomology of a smooth hypersurface (Corollary 2.3.5). Using this upper bound in (4.4), we find that

$$|M_{\kappa}^{m,n}(q)| \leq \frac{1}{k}\left(1 + \frac{(-1)^N}{(k-1)^{N-1}}\right).$$

In particular, the only conclusion that we may draw from purity is that if limit $M_{\kappa}^{m,n}$ of the moments $M_{\kappa}^{m,n}(q)$ as $q \to \infty$ exists, it satisfies

$$|M_{\kappa}^{m,n}| \leq \frac{1}{k}\left(1 + \frac{(-1)^N}{(k-1)^{N-1}}\right).$$

One needs more information about the Galois representation on the primitive cohomology, e.g. by evaluating the Gauss sums of Proposition 2.3.7 , to give a more precise estimate.

Special case $\kappa = \{2\}$. In this particular case, we can say more since $W_{\kappa}^{m,n}$ is a smooth quadric of dimension $N-2$ provided $p > 2$, hence the discussion of Section 2.4 applies to give a complete description of the Galois representation on the primitive cohomology.

Proposition 4.4.1. *For $\kappa = \{2\}$, the normalized exponential sums $b_\kappa(q,a)$, $a \neq 0$, are equidistributed on average with respect to $\delta_{\{1,-1\}}$ when $q \to \infty$ along $q \equiv 1 \bmod 4$, and with respect to $\delta_{\{i,-i\}}$ when $q \to \infty$ along $q \equiv -1 \bmod 4$.*

Proof. When $N = m + n$ is odd, the quadric $W_\kappa^{m,n}$ has no primitive cohomology, so that (4.4) gives

$$M_\kappa^{m,n}(q) = 0 \qquad (N \text{ odd}).$$

On the other hand, when $N = n + m$ is even, by Proposition 2.4.3, Frob_q acts on the 1-dimensional primitive cohomology by multiplication by $q^{N/2-1}\,\varepsilon_q(\Delta)$ with $\Delta = (-1)^{N/2}(-1)^n$, so that

$$V_\kappa^{m,n} = q \cdot q^{N/2-1}(-1)^{(\frac{N}{2}+n)\frac{q-1}{2}},$$

hence from (4.4) we conclude that

$$M_\kappa^{m,n}(q) = (-1)^{(\frac{N}{2}+n)\frac{q-1}{2}} \qquad (N \text{ even}).$$

On the other hand, we can easily check that

$$M^{m,n}(\delta_{\{1,-1\}}) = \frac{1^{m+n} + (-1)^{m+n}}{2} = \frac{1 + (-1)^N}{2},$$

$$M^{m,n}(\delta_{\{i,-i\}}) = \frac{i^m(-i)^n + (-i)^m i^n}{2} = \frac{i^N(-1)^n(1 + (-1)^N)}{2}.$$

Thus $M_\kappa^{m,n}(q) = M^{m,n}(\delta_{\{1,-1\}})$ when $q \equiv 1 \bmod 4$, while $M_\kappa^{m,n}(q) = M^{m,n}(\delta_{\{i,-i\}})$ when $q \equiv -1 \bmod 4$, and the conclusion follows. □

This result exhibits what seems to be a fundamental feature of equidistribution results for exponential sums: in general there might not exist a limit distribution as $q \to \infty$, but rather we expect different limit distributions along certain families of values of q, controlling for example the presence of certain roots of unity in $\mathbf{F}_q$.

Note that in this case we knew more *a priori*: when $q \equiv 1 \bmod 4$, since -1 is a square in $\mathbf{F}_q$,

$$\overline{b_\kappa(q,a)} = \sum_{x \in \mathbf{F}_q} \psi_q(-ax^2) = b_\kappa(q,a),$$

so that $b_\kappa(q,a)$ is actually a real number lying in the interval $[-1,1]$. On the other

hand, when $q \equiv -1 \bmod 4$, we have instead

$$\overline{b_\kappa(q,a)} + b_\kappa(q,a) = \sum_{x \in \mathbf{F}_q} \psi_q(-ax^2) + \sum_{x \in \mathbf{F}_q} \psi_q(ax^2) = 2 \sum_{x \in \mathbf{F}_q} \psi_q(ax) = 0,$$

so $b_\kappa(q,a)$ now lies in the imaginary interval $[-i,i]$. In both cases, Proposition 4.4.1 says that the normalized exponential sums accumulate towards the endpoints of the interval on average as $q \to \infty$.

From Corollary 4.3.3 we deduce at once another equidistribution result.

Corollary 4.4.2. *For $\kappa = \{0,2\}$, the normalized exponential sums $b_\kappa(q,\mathbf{a})$ are equidistributed on average along the boundary of $\mathbf{D}$, i.e. with respect to $\delta_{\mathbf{S}^1}$, as $q \to \infty$.*

Proof. From Corollary 4.3.3 and Proposition 4.4.1, we find that

$$M_\kappa^{m,n}(q) = \begin{cases} 0 & \text{when } m \neq n, \\ 1 & \text{when } m = n. \end{cases}.$$

These coincide with the moments of $\delta_{\mathbf{S}^1}$ as

$$M^{m,n}(\delta_{\mathbf{S}^1}) = \int z^m \overline{z}^n d\delta_{\mathbf{S}^1} = \frac{1}{2\pi} \int_0^{2\pi} e^{i(m-n)\theta} d\theta = \begin{cases} 0 & \text{when } m \neq n \\ 1 & \text{when } m = n, \end{cases}$$

and the conclusion follows. □

Case $\kappa = \{1, \ell+1\}$. This is our main case of interest and the varieties $W_\kappa^{m,n}$ are none other than the hypersurfaces $W_\ell^{m,n}$ from section 3.4. Following the geometrical analysis carried out there, we restrict ourselves to the case where ℓ is prime.

Proposition 4.4.3. *Let ℓ be a prime, $\kappa = \{1, \ell+1\}$ and $q = p^r$ where p is a prime which is inert in $\mathbf{Q}(\zeta_\ell)$. For $\ell \nmid n-m$,*

$$M_\kappa^{m,n}(q) = O\left(\frac{1}{\sqrt{q}}\right).$$

In particular, for $\ell \nmid n-m$, $M_\kappa^{m,n}(q) \to 0$ as $q \to \infty$ along inert primes.

Proof. Under these conditions, by Proposition 3.4.4, $W_\kappa^{m,n}$ is a smooth hypersurface over $\mathbf{F}_p$ of degree $\ell+1$ and dimension $N-3$, provided $p > \max(N,\ell)$. From Corollary 2.3.3,

$$H^\bullet(W_\kappa^{m,n}) \simeq H^\bullet(\mathbf{P}^{N-3}) \oplus H^{N-3}_{\mathrm{pr}}(W_\kappa^{m,n}),$$

from which it follows that

$$|W_\kappa^{m,n}(\mathbf{F}_q)| = \frac{q^{N-2}-1}{q-1} + (-1)^{N-3}\,\mathrm{tr}(\mathrm{Frob}_q \mid H_{\mathrm{pr}}^{N-3}(W_\kappa^{m,n})). \tag{4.5}$$

Moreover, since $\kappa' = \{1\}$, $W_{\kappa'}^{m,n} \simeq \mathbf{P}^{N-2}$, so that Corollary 4.3.4 yields

$$\begin{aligned} V_\kappa^{m,n}(q) &= 1 + q\left(\frac{q^{N-2}-1}{q-1} + (-1)^{N-3}\,\mathrm{tr}\,\mathrm{Frob}_q H_{\mathrm{pr}}^{N-3}(W_\kappa^{m,n})\right) - \frac{q^{N-1}-1}{q-1} \\ &= (-1)^{N-3} q\ \mathrm{tr}\,\mathrm{Frob}_q H_{\mathrm{pr}}^{N-3}(W_\kappa^{m,n}). \end{aligned} \tag{4.6}$$

By purity, this implies that

$$|V_\kappa^{m,n}(q)| \leq q \cdot q^{(N-3)/2} \dim H_{\mathrm{pr}}^{N-3}(W_\kappa^{m,n}) = q^{(N-1)/2} \dim H_{\mathrm{pr}}^{N-2}(W_\kappa^{m,n}).$$

Consequently, from (4.2) we obtain

$$|M_\kappa^{m,n}(q)| \leq \frac{1}{q}\left(\frac{1}{\ell^N} \dim H_{\mathrm{pr}}^{N-2}(W_\kappa^{m,n})\right),$$

and the result follows. □

This seems to suggest an ℓ-fold rotational symmetry for the putative limit distribution of the normalized exponential sums b_κ along inert primes. For, suppose that ν is a measure on the unit disk $\mathbf{D}$ which can be written in polar coordinates as

$$\nu = f(r)g(\theta)rdrd\theta.$$

The corresponding moments are

$$\begin{aligned} M^{m,n}(\nu) &= \int_0^{2\pi}\int_0^1 r^m e^{im\theta} r^n e^{in\theta} f(r)g(\theta)rdrd\theta \\ &= \int_0^1 r^{m+n+1} f(r)dr \int_0^{2\pi} e^{i(m-n)\theta} g(\theta)d\theta \\ &= 2\pi\, M_{N+1}(f)\, a_{n-m}(g), \end{aligned}$$

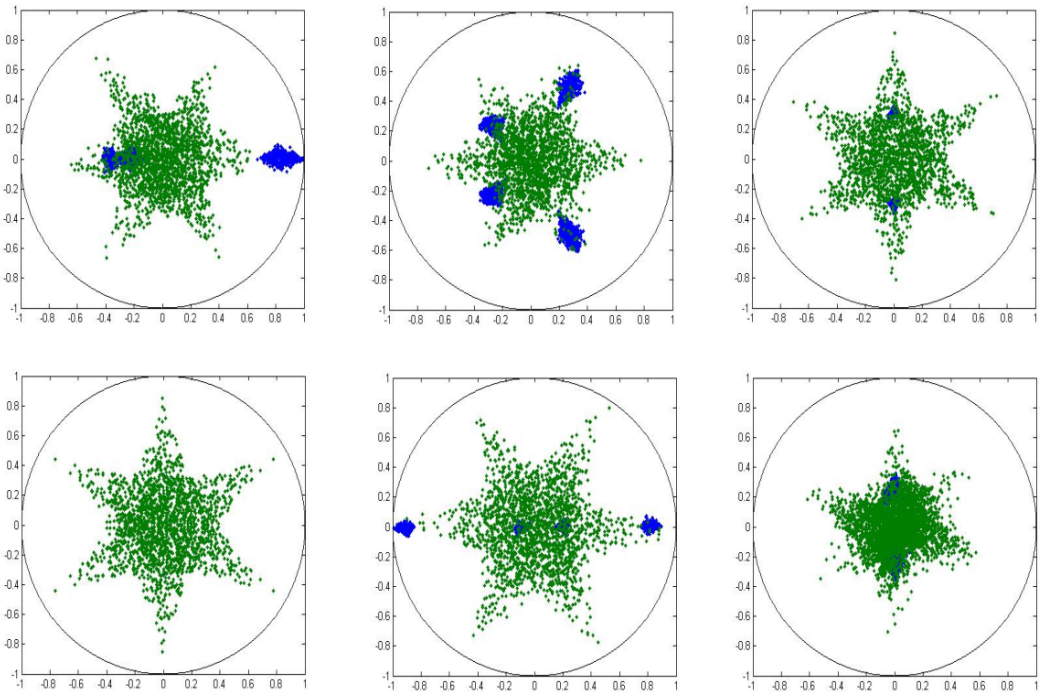
where $a_k(g)$ is the k^{th} Fourier coefficient of g. In particular, if all the moments of f on $[0,1]$ are non-zero, then

$$M^{m,n}(\nu) = 0 \implies a_{n-m}(g) = 0.$$

In particular, if $M^{m,n}(\nu) = 0$ unless some integer ℓ divides $n - m$, then $a_{n-m}(g) = 0$ unless $\ell \mid n - m$, so that g is actually a function of $\ell\theta$.

The ℓ-fold limit rotational symmetry seems verified by numerical experiments. In the following pictures, the whole sets of normalized exponential sums $b_\kappa(p; \alpha, \beta)$ with $\alpha, \beta \in \mathbf{F}_p$, $\alpha \neq 0$, are shown for $\ell = 3$ and

$$p = 1993, 1997, 1999, 2011, 2017, 2999.$$



Note that there is repetition among these exponential sums, as for $\beta \neq 0$ we have

$$b_\kappa(p; \alpha, \beta) = b_\kappa(p; \alpha\beta^{-\ell-1}, 1),$$

hence these values get repeated $p-1$ times. They correspond to the blue (heavy) dots in the pictures; green (light) dots represent the normalized sums $b_\kappa(p; \alpha, 0)$, $\alpha \neq 0$.

To obtain information about moments when $\ell \mid n - m$, we need to take a deeper look at the singular set T of $W_\ell^{m,n}$, described by Proposition 3.4.4. If $n - m = \ell a$, recall that

$$T = S_m \times S_n \cdot \{[\mathbf{x}; \underbrace{\zeta^0}_{a} : \underbrace{\zeta^1}_{a} : \cdots : \underbrace{\zeta^{\ell-1}}_{a} : \mathbf{x}] \mid \mathbf{x} \in \mu_\ell(\mathbf{F})^m\}.$$

If $\mathbf{x} \in \mu_\ell(\overline{\mathbf{F}}_q)^m$, let λ_i be the number of times that ζ_i appears as in $\mathbf{x}$, $0 \leq i < \ell$. We obtain this way a *composition* of m in at most ℓ parts, i.e. an *ordered* ℓ-tuple $\lambda = (\lambda_0, \lambda_1, \cdots, \lambda_{\ell-1})$ of non-negative integers adding up to m. Let us write $\lambda \models_\ell m$ to signify that λ is such a composition of m in at most ℓ parts. These compositions parametrize the orbits of $S_m \times S_n$ on T, and by taking scaling into account we find that

$$|T(\overline{\mathbf{F}}_q)| = \frac{1}{\ell} \sum_{\lambda \models \ell} \binom{m}{\lambda} \binom{m + a\ell}{\lambda + a}.$$

For ease of notation, let us now denote $W_\ell^{m,n}$ by W, and let $\widetilde{W}$ be its blow-up along the singular set T. We can relate the number of points on W to that of $\widetilde{W}$, generalizing [39, lemma 4.3].

Lemma 4.4.4. *With Δ as in Proposition 3.4.5 if $n - m = \ell a$ is even, and the convention that $\varepsilon_q(\Delta) = 0$ if $n - m$ is odd, we have*

$$|W(\mathbf{F}_q)| = |\widetilde{W}(\mathbf{F}_q)| - q\,|T(\mathbf{F}_q)| \left(\frac{q^{N-4} - 1}{q - 1} + q^{N/2-3}\, \varepsilon_q(\Delta) \right).$$

Proof. Since $W \setminus T$ is isomorphic to $\widetilde{W} \setminus \widetilde{T}$ over $\mathbf{F}_q$, we have

$$|W(\mathbf{F}_q)| = |\widetilde{W}(\mathbf{F}_q)| + |T(\mathbf{F}_q)| - |\widetilde{T}(\mathbf{F}_q)|. \tag{4.7}$$

At the level of cohomology (cf. the discussion at the end of Section 2.5), we have

$$H^\bullet(\widetilde{T}) = \bigoplus_{t \in T} H^\bullet(Q_t) = H^0(T) \otimes H^\bullet(Q),$$

where Q is *any* fiber since they all carry the same Galois action by Propositions 2.4.3 and 3.4.5. It follows that

$$|\widetilde{T}(\mathbf{F}_q)| = |T(\mathbf{F}_q)|\,|Q(\mathbf{F}_q)| = |T(\mathbf{F}_q)| \left(\frac{q^{N-3} - 1}{q - 1} + q^{N/2-2}\, \varepsilon_\Delta(q) \right)$$

with our convention that $\varepsilon_\Delta(q) = 0$ if N is odd (that is, when Q, a smooth quadric of dimension $N - 4$, has no primitive cohomology). Using this formula in (4.7) finishes the proof. □

Using this lemma, the formula of Corollary 4.3.4 now reads

$$V_\kappa^{m,n} = 1 + q\,|\widetilde{W}(\mathbf{F}_q)| - q^2\,|T(\mathbf{F}_q)|\left(\frac{q^{N-4}-1}{q-1} + q^{N/2-3}\,\varepsilon_\Delta(q)\right) - \frac{q^{N-1}-1}{q-1}. \quad (4.8)$$

Let us treat separately the case where N is even and the case where it is odd, since we know from Section 2.5 that the cohomology of $\widetilde{W}$ will behave differently. The easy case is when $\widetilde{W}$ has no subprimitive cohomology, that is, when its dimension $N-3$ is even (cf. Proposition 2.5.5).

Proposition 4.4.5. *For $\kappa = \{1, \ell+1\}$, ℓ prime, $N = m+n$ odd and $\ell \mid n-m$,*

$$M_\kappa^{m,n}(q) = O\left(\frac{1}{\sqrt{q}}\right) \longrightarrow 0$$

as $q \to \infty$ along inert primes.

Proof. By the results of section 2.5, as Galois modules, for $i \leq N-3$ we have

$$H^i(\widetilde{W}) \cong \begin{cases} 0 & i \text{ odd}, \\ 1 & i = 0, \\ \big(1 \oplus H^0(T)\big) \otimes \chi_{\text{cycl}}^{i/2} & i \text{ even} \neq 0, N-3, \\ \big(1 \oplus H^0(T)\big) \otimes \chi_{\text{cycl}}^{i/2} \oplus H_{\text{pr}}^{N-3}(\widetilde{W}) & i = N-3. \end{cases}$$

Using Poincaré duality for $N-3 < i \leq 2(N-3)$, the trace formula yields

$$\begin{aligned} |\widetilde{W}(\mathbf{F}_q)| &= 1 + \sum_{j=1}^{N-4}(1 + |T(\mathbf{F}_q)|)q^j + \operatorname{tr}(\operatorname{Frob}_q \mid H_{\text{pr}}^{N-3}(\widetilde{W})) + q^{N-3} \\ &= \frac{q^{N-2}-1}{q-1} + q\,|T(\mathbf{F}_q)|\,\frac{q^{N-4}-1}{q-1} + \operatorname{tr}(\operatorname{Frob}_q \mid H_{\text{pr}}^{N-3}(\widetilde{W})). \end{aligned}$$

Substituting this expression in (4.8), in which $\varepsilon_q(\Delta) = 0$ since the exceptional fibers have odd dimension, everything cancels out, leaving only

$$V_\kappa^{m,n}(q) = q\ \operatorname{tr}(\operatorname{Frob}_q \mid H_{\text{pr}}^{N-3}(\widetilde{W})).$$

Putting this in (4.2) gives

$$M_\kappa^{m,n}(q) = \frac{1}{\ell^N q^{N/2-1}}\operatorname{tr}(\operatorname{Frob}_q \mid H_{\text{pr}}^{N-3}(\widetilde{W})),$$

and the conclusion follows from purity. □

The case when N is even is more interesting, because then the exceptional fibers, of dimension $N-4$, have primitive cohomology, and thus the subprimitive cohomology of $\widetilde{W}$ does not vanish.

Proposition 4.4.6. *For $\kappa = \{1, \ell+1\}$, ℓ prime, $N = n+m$ even and $\ell \mid n-m$,*

$$M_\kappa^{m,n}(q) = \frac{\varepsilon_q(\Delta)}{\ell^N} \dim H_{\mathrm{sub}}^{N-4}(\widetilde{W}) + O\left(\frac{1}{\sqrt{q}}\right)$$

for q above an inert prime.

Proof. Mimicking the proof of Proposition 4.4.5, this time Section 2.5 tells us that

$$|\widetilde{W}(q)| = \frac{q^{N-2}-1}{q-1} + q\,|T(\mathbf{F}_q)|\,\frac{q^{N-4}-1}{q-1} + \operatorname{tr}\mathrm{Frob}_q M^\bullet,$$

with $M^\bullet = H_{\mathrm{sub}}^{N-4}(\widetilde{W}) \oplus H_{\mathrm{pr}}^{N-3}(\widetilde{W}) \oplus H_{\mathrm{sub}}^{N-4}(\widetilde{W})^\vee(1)$. Substituting into (4.8), a lot of cancelation still occurs to leave only

$$V_\kappa^{m,n}(q) = q\,\operatorname{tr}(\mathrm{Frob}_q \mid M^\bullet) - q^{N/2-1}\,|T(\mathbf{F}_q)|\,\varepsilon_q(\Delta).$$

From (4.2) we then obtain

$$M_\kappa^{m,n}(q) = \frac{1}{\ell^N q^{N/2-1}}\left((1+q)\operatorname{tr}(\mathrm{Frob}_q \mid H_{\mathrm{sub}}^{N-4}(\widetilde{W})) - \operatorname{tr}(\mathrm{Frob}_q \mid H_{\mathrm{pr}}^{N-3}(\widetilde{W}))\right).$$

From purity, the dominant term is seen to be

$$\frac{1}{\ell^N q^{N/2-1}} q\,\operatorname{tr}(\mathrm{Frob}_q \mid H_{\mathrm{sub}}^{N-4}(\widetilde{W})) = \frac{1}{\ell^N q^{N/2-2}}\operatorname{tr}(\mathrm{Frob}_q \mid H_{\mathrm{sub}}^{N-4}(\widetilde{W})).$$

Now, from Proposition 2.5.5, the subprimitive cohomology of $\widetilde{W}$ is the image of the hyperplane classes spanning the primitive cohomology of the exceptional fibers; it follows that Frob_q acts on it by multiplication by $q^{(N-4)/2}\varepsilon_q(\Delta)$, from which the conclusion follows. □

We summarize Propositions 4.4.3, 4.4.5 and 4.4.6 in the following theorem.

Theorem 4.4.7. *Suppose that ℓ is a prime and $\kappa = \{1, \ell+1\}$. For q of characteristic p which is split in $\mathbf{Q}(\zeta_\ell)$, the moments of the normalized exponential sums $b_\kappa(q)$ can*

be written as

$$M_\kappa^{m,n}(q) = N_\kappa^{m,n} + O\left(\frac{1}{\sqrt{q}}\right),$$

with $N_\kappa^{m,n}(q) = 0$ *if* $\ell \nmid n-m$ *or* $2 \nmid n-m$*, and*

$$N_\kappa^{m,n}(q) = \frac{\varepsilon_q(\Delta)}{\ell^N} \dim H_{\mathrm{sub}}^{N-4}(\widetilde{W}_\ell^{m,n}) \qquad \text{if } 2, \ell \mid n-m.$$

Using Corollary 4.3.3 we deduce the following.

Corollary 4.4.8. *For* $\kappa = \{0, 1, \ell+1\}$*, where* ℓ *is prime, the normalized exponential sums* $b_\kappa(q)$ *are equidistributed on average with respect to the Dirac delta measure* δ_0 *as* $q \to \infty$ *along inert primes in* $\mathbf{Q}(\zeta_\ell)$*.*

Proof. By Corollary 4.3.3 and Theorem 4.4.7, we have $M_\kappa^{m,n} = 0$ for all $m, n \geq 0$, which are indeed the moments of δ_0. □

In [39], Livné managed to obtain an explicit formula the dimension of the subprimitive cohomology appearing in Theorem 4.4.7 in the special case $\ell = 2$, $m = 0$, by using the isomorphism of Proposition 2.5.5 to compute its decomposition into irreducibles as a representation for S_n. Such a task can be attempted in our case to obtain explicit values for the average moments in terms of Kostka numbers, at least for some specific values of the parameters; however, this will have to be pursued elsewhere.

Chapter 5

Comparing Galois representations

This chapter is devoted to criteria allowing to decide algorithmically whether two ℓ-adic representations of the absolute Galois group Gal_K of a number field K are equivalent or not.

Faltings [18] was the first to remark that this could in principle be achieved through a finite computation when the representations are ramified at only a finite number of places. This was shortly afterwards turned by Serre [58] into a usable tool, the so-called "method of quartic fields" (see Section 5.2) which allowed one to prove that certain elliptic curves over $\mathbf{Q}$ were isogenous (for example in [41]).

Another instance of the criterion, applicable to 2-dimensional 2-adic representations with *even* trace, was devised and used by Livné [40] to prove the modularity of the variety W_2^{10} from Chapter 3. This version was widely used, for example in [51], and in the recent years to show modularity of certain $K3$ surfaces and rigid Calabi-Yau varieties (see [26] for a survey), before the proof of the Serre conjectures were announced.

In section 5.1, the current state of affairs for 2-dimensional representations of $\mathrm{Gal}_{\mathbf{Q}}$ arising in the cohomology of varieties is discussed. In a nutshell, the Serre conjectures imply that all such representations (satisfying some obvious requirements) are modular; but an *ad hoc* tool might sometimes still be useful to pinpoint the exact modular form in the absence of precise information about the ramification. And of course, general techniques applicable in principle to more general situations are still desirable.

We then try to work out the details of the Faltings-Serre method in a general setting since the literature is very scarce on this subject, the best source being the very concise summary [58]. We thus define in Section 5.2 the basic object of the construc-

tion, the *deviation group* of two integer-valued λ-adic representations of a group G, which is a finite quotient of G on which we can check by computing traces whether or not the two representations are equivalent. In Section 5.3 a more concrete quotient of this deviation group is described in the case where the two initial representations are not isomorphic. Showing that such a quotient cannot exist is thus sufficient to prove that the two representations under consideration are indeed isomorphic, and this was the way that Serre's quartic fields method was used, for instance in [41]. It is also true that in certain situations, this quotient could be advantageously substituted for the deviation group; see the remark there.

In Section 5.4, the Faltings-Serre-Livné criterion for equivalence of 2-adic, 2-dimensional representations with even trace is presented together with its proof. This is the basis for our generalization, Theorem 5.5.13 of Section 5.5, in which we remove the hypothesis of evenness of traces at the price of increasing the list of groups that can arise. The precise criterion for Galois representations is stated in Theorem 5.5.15.

In order to apply this generalized criterion to compute the modular form associated to the 2-dimensional compatible system of Galois representations arising in the primitive cohomology of W_2^7 in Section 5.7, we first state some facts in Section 5.6 which allows one to list all the quadratic extensions of a number field which are unramified outside a given finite set of primes.

5.1 Isogeny and modularity

Faltings made his observation about the possibility of detecting the equivalence of ℓ-adic representations by a finite computation in connection with his work on abelian varieties [18] in which he proved the following pair of results. Recall that if A is an abelian variety of dimension g, its *ℓ-adic Tate module*

$$T_\ell(A) := \varprojlim_n A[\ell^n]$$

is a free $\mathbf{Z}_\ell$-module of rank $2g$.

Theorem 5.1.1. *If A is defined over a number field K, then $V_\ell(A) := T_\ell(A) \otimes \mathbf{Q}_\ell$ is a semisimple representation for the absolute Galois group Gal_K of K.*

Theorem 5.1.2. *For A and A' two abelian varieties defined over a number field K,*

the natural map

$$\mathrm{Hom}_K(A, A') \otimes \mathbf{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell(A), T_\ell(A'))^{\mathrm{Gal}_K}$$

is an isomorphism.

Recall from section 1.1 that we use the notation $V \sim W$ to mean that two representations in characteristic 0 are equivalent, i.e. that they have isomorphic semisimplifications.

Corollary 5.1.3. *A and A' are K-isogenous $\iff$ $V_\ell(A) \sim V_\ell(A')$.*

In particular, an algorithm to decide the equivalence of Galois representations yields an algorithm to solve the isogeny problem (see for example [1]). In the special case of elliptic curves over $\mathbf{Q}$, the situation is considerably easier now that modularity is known.

Theorem 5.1.4 (Modularity theorem)**.** *Let ρ be the compatible system of representations associated to an elliptic curve E over $\mathbf{Q}$ of conductor N_E. Then there exists a newform $f \in S_2(N_E, 1)$ such that $\rho \simeq \rho_f$.*

In particular, it implies that the isogeny problem for elliptic curves over $\mathbf{Q}$ is very easy.

Corollary 5.1.5. *Two elliptic curves E_1 and E_2 over $\mathbf{Q}$ are $\mathbf{Q}$-isogenous if and only if they have the same conductor $N_{E_1} = N_{E_2} = N$ and $|E_1(\mathbf{F}_p)| = |E_2(\mathbf{F}_p)|$ for all primes $p \nmid N$ such that* [1]

$$p \leq \frac{N}{6} \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

Proof. Let ρ_i be the compatible system of 2-dimensional Galois representations associated to E_i, and f_i the corresponding modular form, for $i = 1, 2$. Then

$$E_1 \sim E_2 \iff \rho_1 \sim \rho_2 \iff f_1 = f_2.$$

[1] Nicolas Billerey pointed out to me that this is not quite correct; one has to either make sure that the decomposition types (split or non-split) agree at all small primes of multiplicative reduction, or use a slightly bigger bound, cf. [15, §5.C].

By [45, th. 1], a cusp form f of weight 2 and level N is determined by its first

$$\frac{N}{6}\prod_{p|N}\left(1+\frac{1}{p}\right)$$

Fourier coefficients $a_n(f)$; for eigenforms, we can restrict our attention to Fourier coefficients $a_p(f)$ where p is prime.

In our situation, if $p \mid N$, from multiplicity 1 it is automatic that $a_p(f_1) = a_p(f_2)$ since f_1 and f_2 are newforms of the same level N. For $p \nmid N$, since

$$a_p(f_i) = \operatorname{tr}\rho_i(\mathrm{Frob}_p) = 1 - |E_i(\mathbf{F}_p)| + p,$$

the result follows. □

More generally, the Serre conjectures (when they are completely proven) will imply modularity for all reasonable 2-dimensional systems coming from the cohomology of algebraic varieties. Recall that to a residual representation $\overline{\rho} : \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_\ell)$, Serre associates a triple of invariants: a weight $k(\overline{\rho})$, a level $N(\overline{\rho})$ and a character $\varepsilon(\overline{\rho})$.

Conjecture 5.1.6 (Serre [55])**.** *If $\overline{\rho}$ is odd and absolutely irreducible, then there exists a newform $f \in S_{k(\overline{\rho})}(N(\overline{\rho}), \varepsilon(\overline{\rho}))$ such that $\overline{\rho} \sim \overline{\rho}_f$.*

As of 2008, a significant part of the conjecture is considered to be proved and a full proof is expected soon.

Theorem 5.1.7 (Khare-Wintenberger [32])**.** *The Serre conjecture is true when $N(\overline{\rho})$ is odd.*

Corollary 5.1.8. *Let ρ be a compatible system of 2-dimensional odd irreducible representations of Hodge-Tate weights (a, b) arising in the cohomology of an algebraic variety X defined over $\mathbf{Q}$. Then, assuming the full Serre conjectures (or unconditionally if ρ is unramified at 2), there exists a newform $f \in S_{b-a}(N, \varepsilon)$ such that $\rho \simeq \chi_{\mathrm{cycl}}^a \otimes \rho_f$, where $\varepsilon = \chi_{\mathrm{cycl}}^{-2a} \otimes \det\rho$ and*

$$N \mid \prod_{p \in \mathrm{Ram}\,\rho} N_p, \quad \textit{with}$$

$$N_p = \begin{cases} 2^8 & \text{if } p = 2 \notin \mathrm{Ram}(\det \rho), \\ 2^{11} & \text{if } p = 2 \in \mathrm{Ram}(\det \rho), \\ 3^5 & \text{if } p = 3, \\ p^2 & \text{if } p > 5. \end{cases}$$

Here is an outline of the proof (for more details, see [55] or [31]).

Proof. Consider $\rho' := \chi_{\mathrm{cycl}}^{-a} \otimes \rho$, which has Hodge-Tate weights $(0, b-a)$. Setting $\varepsilon := \det \rho'$, we then have $\varepsilon(\overline{\rho}'_\ell) = \varepsilon$ for all primes ℓ, and $k(\overline{\rho}'_\ell) = b - a$ for infinitely many ℓ. Also, for infinitely many primes ℓ, one can show that the level $N(\overline{\rho}'_\ell)$ has to divide the bound on the conductor given above [55]. By the pigeonhole principle, it follows that there exists a divisor N of that bound such that $N(\overline{\rho}'_\ell) = N$ for an infinite number of primes ℓ.

Hence we conclude that the triple of Serre invariants associated to $\overline{\rho}'_\ell$ is $(b-a, \varepsilon, N)$ for an infinite number of values of ℓ. By the Serre conjectures, for each of these there exists a newform $f_\ell \in S_{b-a}(N, \varepsilon)$ associated to $\overline{\rho}'_\ell$. Since there exists only a finite number of such newforms, one finds a single $f \in S_{b-a}(N, \varepsilon)$ such that for infinitely many ℓ, one has $\overline{\rho}'_\ell \sim \overline{\rho}_f$. But this means that for an infinite number of primes ℓ we have

$$\mathrm{tr}\, \rho' \equiv \mathrm{tr}\, \rho_f \bmod \ell,$$

which is only possible if $\mathrm{tr}\, \rho' = \mathrm{tr}\, \rho_f$, i.e. $\rho' \simeq \rho_f$. □

Example 5.1.9. Let ρ be the 2-dimensional compatible system of representations of $\mathrm{Gal}_{\mathbf{Q}}$ afforded by $M_{\mathrm{sg}}(H^4_{\mathrm{pr}}(W_2^7))$, whose existence is guaranteed by Theorem 1.2.2 and Proposition 3.5.1. In Section 5.7, we will see that ρ has Hodge-Tate weights $(1, 3)$ and that $\det \rho = \chi_{\mathrm{cycl}}^4 \otimes \varepsilon_{35}$, where ε_{35} is the quadratic character of conductor 35. Hence

$$\{5, 7\} \subseteq \mathrm{Ram}\, \rho \subseteq \{3, 5, 7\},$$

since W_2^7 has good reduction outside $\{3, 5, 7\}$. It follows (unconditionally) from Corollary 5.1.8 that

$$\rho \simeq \chi_{\mathrm{cycl}} \otimes \rho_f,$$

where f is a newform of weight 3, character ε_{35} and level dividing $3^5\, 5^2\, 7^2 = 297675$. However, numerical evidence suggests that the level of f is actually 35, as will be proven in Section 5.7.

Keeping with the notations of Corollary 5.1.8, if we assume that the traces of $\rho(\mathrm{Frob}_p)$ for unramified primes p are computable, there exists in theory an algorithm to determine f from ρ.

1. Find a finite set of primes S such that $\mathrm{Ram}\,\rho \subseteq S$.

2. Make a list of all newforms $\{f_1, \ldots . f_r\}$ of the right weight, and level N dividing $\prod_{p \in S} N_p$.

3. Compute successively all the traces $\mathrm{tr}\,\rho(\mathrm{Frob}_p)$ for $p \notin S$; at each step, eliminate f_i if it does not have the right $a_p(f_i)$.

4. Eventually only one newform is left (by 1.4.4); this is the f we are looking for.

In practice, the problem is that if (as is often the case) we do not know explicitly the Artin conductor of ρ, we have to use the naive bound above, which is often much too large to be practical. For example, if ρ comes from the cohomology of a variety X, we can take for S the set of primes of bad reduction of X in step 1, but this might be overkill. Thus we turn to a different kind of algorithm to compare Galois representations, which can sometimes be used more efficiently to pinpoint the exact modular form f.

5.2 Deviation groups

In this section, we introduce the basic construction involved in the *Faltings-Serre method*, following loosely [58].

For the moment, let G be an arbitrary group, and $\mathcal{O}_\lambda$ the ring of integers in a local number ring E_λ, with maximal ideal λ and residue field k. We consider two integer-valued representations $\rho_1, \rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda)$ of G. The product homomorphism $\rho_1 \times \rho_2$ extends to an $\mathcal{O}_\lambda$-algebra map

$$\rho : \mathcal{O}_\lambda[G] \longrightarrow \mathrm{M}_n(\mathcal{O}_\lambda) \oplus \mathrm{M}_n(\mathcal{O}_\lambda).$$

Let M be its image, and consider the composition

$$\delta : G \longrightarrow M^\times \longrightarrow (M/\lambda M)^\times.$$

Definition 5.2.1. The image $\delta(G)$ of G in $(M/\lambda M)^\times$ will be called the *deviation group* of the pair (ρ_1, ρ_2).

Proposition 5.2.2. *$\delta(G)$ is a finite group. More precisely, $|\delta(G)| < |k|^{2n^2}$.*

Proof. M is a submodule of the free $\mathcal{O}_\lambda$-module $\mathrm{M}_n(\mathcal{O}_\lambda) \oplus \mathrm{M}_n(\mathcal{O}_\lambda)$, hence M is itself free, of rank

$$r \leq \operatorname{rank}\big(\mathrm{M}_n(\mathcal{O}_\lambda) \oplus \mathrm{M}_n(\mathcal{O}_\lambda)\big) = 2n^2.$$

It follows that $M/\lambda M$ is a k-algebra of dimension r, hence

$$|\delta(G)| \leq |(M/\lambda M)^\times| < |k|^r \leq |k|^{2n^2},$$

as claimed. □

Remark. It might be tempting to think of $\delta(G)$ as a subgroup of $\mathrm{GL}_n(k) \times \mathrm{GL}_n(k)$, but it is important to note that in general *this is not the case*. Indeed, consider the short exact sequence associated to reduction modulo λ,

$$0 \longrightarrow \mathrm{M}_n(\lambda) \longrightarrow \mathrm{M}_n(\mathcal{O}_\lambda) \longrightarrow \mathrm{M}_n(k) \longrightarrow 0.$$

Writing R for the $\mathcal{O}_\lambda$-algebra $\mathrm{M}_n(\mathcal{O}_\lambda) \oplus \mathrm{M}_n(\mathcal{O}_\lambda)$, it identifies $\mathrm{M}_n(k) \oplus \mathrm{M}_n(k)$ with $R/\lambda R$. Now call $\overline{M}$ the image of M in $R/\lambda R$, so that

$$\overline{M} = M/(M \cap \lambda R)$$

Since $\lambda M \subseteq M \cap \lambda R$, it follows that there is a short exact sequence

$$0 \longrightarrow (M \cap \lambda R)/\lambda M \longrightarrow M/\lambda M \longrightarrow \overline{M} \longrightarrow 0.$$

Recall that the deviation group $\delta(G)$ is the image of G in $(M/\lambda M)^\times$. Writing $\overline{G}$ for the image of G in $\overline{M}^\times \subseteq (R/\lambda R)^\times = \mathrm{GL}_n(k) \times \mathrm{GL}_n(k)$, what we have is a short exact sequence

$$1 \longrightarrow N(G) \longrightarrow \delta(G) \longrightarrow \overline{G} \longrightarrow 1, \tag{5.1}$$

where the kernel $N(G)$ is the image of $\rho(G) \cap (1 + \lambda R)$ in $(M/\lambda M)^\times$.

The following proposition shows that one can detect whether ρ_1 and ρ_2 are equivalent by computing finitely many well-chosen traces, even though ρ_1 and ρ_2 typically do not factor through any finite quotient of G.

Proposition 5.2.3. *Let Σ be a subset of G surjecting onto $\delta(G)$. Then, as E-valued representations,*

$$\rho_1 \sim \rho_2 \iff \operatorname{tr}\rho_1|_\Sigma = \operatorname{tr}\rho_2|_\Sigma.$$

Proof. ($\Rightarrow$) is obvious. For ($\Leftarrow$), we prove the contrapositive. Suppose that $\rho_1 \nsim \rho_2$, so that $\operatorname{tr}\rho_1 \neq \operatorname{tr}\rho_2$, and let α be the greatest integer such that

$$\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \bmod \lambda^\alpha.$$

Now choose an uniformizer π; the function $\pi^{-\alpha}(\operatorname{tr}\rho_1 - \operatorname{tr}\rho_2)$ extends to an $\mathcal{O}_\lambda$-linear map

$$\theta : M \longrightarrow \mathcal{O}_\lambda, \qquad \theta(M) \nsubseteq \lambda,$$

which descends to a nonzero k-linear map $M/\lambda M \to k$, hence to a function,

$$\Theta : \delta(G) \longrightarrow k,$$

which is nonzero because $\delta(G)$ spans $M/\lambda M$. It implies that there exists an element $g \in \Sigma$ such that $\Theta(\delta(g)) \neq 0$, i.e.,

$$\theta(g) = \pi^{-\alpha}(\operatorname{tr}\rho_1(g) - \operatorname{tr}\rho_2(g)) \notin \lambda.$$

In particular, $\operatorname{tr}\rho_1(g) \neq \operatorname{tr}\rho_2(g)$, so $\operatorname{tr}\rho_1|_\Sigma \neq \operatorname{tr}\rho_2|_\Sigma$. □

Corollary 5.2.4. *Let $\mathcal{R}$ be a class of representations of G defined over $\mathcal{O}_\lambda$ and Σ be a subset of G surjecting onto all the deviation groups of pairs ρ_1, $\rho_2 \in \mathcal{R}$. Then, given two such representations ρ_1 and ρ_2,*

$$\rho_1 \sim \rho_2 \iff \operatorname{tr}\rho_1|_\Sigma = \operatorname{tr}\rho_2|_\Sigma.$$

In particular, in light of Proposition 5.2.2, for $\mathcal{R}$ consisting of representations of degree n, it is sufficient to ask that Σ surjects onto all quotients of G of size bounded by $|k|^{2n^2}$. If G has only a finite number of such quotients, this yields in principle an algorithm to decide the equivalence of n-dimensional λ-adic representations of G.

Application to Galois representations. We now specialize to the case where $G = \mathrm{Gal}_K$, the absolute Galois group of a number field K.

Lemma 5.2.5. *Let ρ_1 and ρ_2 be two λ-adic representations of Gal_K. Then $\delta(\mathrm{Gal}_K)$ is unramified outside $\operatorname{Ram}\rho_1 \cup \operatorname{Ram}\rho_2$.*

Proof. For a prime $\mathfrak{p} \notin \operatorname{Ram}\rho_1 \cup \operatorname{Ram}\rho_2$, we have $I(\mathfrak{p}) \subset \operatorname{Ker}\rho_1 \cap \operatorname{Ker}\rho_2$. It follows that $I(\mathfrak{p}) \subset \operatorname{Ker}\rho$, where $\rho = \rho_1 \times \rho_2$. That is, the image $\rho(\mathrm{Gal}_K)$ is unramified at $\mathfrak{p}$. Hence $\delta(\mathrm{Gal}_K)$, being a finite quotient of $\rho(\mathrm{Gal}_K)$, is also unramified at $\mathfrak{p}$. □

From this, we can deduce the following strengthening of Proposition 1.4.4.

Corollary 5.2.6. *Given a finite set S of places of K and an integer $n \geq 1$, there exists a* finite *set of primes T disjoint from S such that if ρ_1, ρ_2 are any two λ-adic representations of degree n of Gal_K, unramified outside S, then*

$$\rho_1 \sim \rho_2 \iff \operatorname{tr}\rho_1|_\Sigma = \operatorname{tr}\rho_2|_\Sigma,$$

where $\Sigma = \{\mathrm{Frob}_\mathfrak{p} \mid \mathfrak{p} \in T\}$.

Proof. By the Hermite-Minkowski theorem, there are only a finite number of Galois extensions L/K unramified outside S and of degree bounded by $|k|^{2n^2}$. One can take for T a finite set of primes $\mathfrak{p}$ for which the Frobenius substitutions $\mathrm{Frob}_\mathfrak{p}$ exhaust all conjugacy classes of $\mathrm{Gal}(L/K)$ for such extensions L/K. □

Using effective Chebotarev density results, we can even give explicit bounds on the required size of the set T appearing above. For K a number field and N a positive integer, we define, following [1]:

$$\Delta^*(K,S,N) := |\Delta_{K/\mathbf{Q}}|^N (N \prod_{\mathfrak{p}\in S} p_\mathfrak{p}^{1-1/N})^{N[K:\mathbf{Q}]},$$

where $p_\mathfrak{p}$ denotes the residual characteristic of the prime ideal $\mathfrak{p}$,

$$B(K,S,N) := \begin{cases} \Delta^*(K,S,N)^c & \text{if } K \neq \mathbf{Q}, \\ 2\Delta^*(K,S,N)^c & \text{if } K = \mathbf{Q}, \end{cases}$$

where c the absolute constant A_1 of [36], as well as

$$B_1(K,S,N) := 70(\log \Delta^*(K,S,N))^2,$$

$$B_2(K,S,N) := (4\log \Delta^*(K,S,N) + 5N[K:\mathbf{Q}]/2 + 5)^2,$$

$$B'(K,S,N) := \min\{B_1(K,S,N), B_2(K,S,N)\}.$$

Theorem 5.2.7 (Effective Chebotarev)**.** *Let K be a number field, S a finite set of places of K and L a finite Galois extension of K, of degree at most N, unramified outside S. Then every conjugacy class of* $\mathrm{Gal}(L/K)$ *can be realized as* $\mathrm{Frob}_{\mathfrak{p}}$ *with*

$$N_{K/\mathbf{Q}}\,\mathfrak{p} \leq B(K,S,N).$$

Under the generalized Riemann hypothesis, the same conclusion holds with $B(K,S,N)$ replaced by $B'(K,S,N)$.

Corollary 5.2.8. *Two ℓ-adic n-dimensional representations ρ_1 and ρ_2 of K, unramified outside S, are equivalent if and only if*

$$\mathrm{tr}\,\rho_1(\mathrm{Frob}_{\mathfrak{p}}) = \mathrm{tr}\,\rho_2(\mathrm{Frob}_{\mathfrak{p}})$$

for all unramified primes $\mathfrak{p}$ of K such that

$$N_{K/\mathbf{Q}}\,\mathfrak{p} \leq B(K,S,\ell^{2n^2}-1)$$

Under the generalized Riemann hypothesis, the same conclusion holds with B'.

Example 5.2.9. For $K=\mathbf{Q}$, $\ell=2$, $n=2$, ρ_1,ρ_2 unramified outside $S=\{2,3,5,7\}$, and assuming the generalized Riemann hypothesis, one would need to check that $\mathrm{tr}\,\rho_1(\mathrm{Frob}_p) = \mathrm{tr}\,\rho_2(\mathrm{Frob}_p)$ for all primes $p \neq 2,3,5,7$ such that

$$p \leq \lfloor B_1(\mathbf{Q},S,255)\rfloor = 137,528,394.$$

In particular, this is what one would have to go through to prove that the 2-adic 2-dimensional Galois representation in the primitive cohomology of W_2^7 considered in Example 5.1.9 is associated to a newform of level 35.

5.3 The method of quartic fields

In order to gain more insight into the deviation group $\delta(G)$ associated to a pair $\rho_1,\rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda)$ of semisimple integer-valued λ-adic representations, we can try to give it a concrete realization.

Let us suppose that the residual representations $\overline{\rho}_1$, $\overline{\rho}_2$ are equal, but that the representations $\rho_1\otimes E$ and $\rho_2\otimes E$ are not *isomorphic*, i.e. conjugated by an element of $\mathrm{GL}_n(E)$. Let β be the maximal integer such that ρ_1 and ρ_2 are conjugated modulo λ^β.

On one hand, the fact that $\overline{\rho_1} = \overline{\rho_2}$ implies that $\beta \geq 1$. On the other hand, since $\rho_1 \not\simeq \rho_2$, there exists a maximal integer α such that $\operatorname{tr}\rho_1 \not\equiv tr\rho_2 \bmod \lambda^\alpha$, as in the proof of Proposition 5.2.3. Hence certainly ρ_1 and ρ_2 are not conjugated modulo $\lambda^{\alpha+1}$, hence $\beta \leq \alpha$. In particular, this shows that β is finite. Moreover, by replacing ρ_2 by a conjugate if necessary, we can assume that

$$\rho_1 \equiv \rho_2 \bmod \lambda^\beta, \qquad \rho_1 \not\equiv \rho_2 \bmod \lambda^{\beta+1}.$$

We can thus write $\rho_2 = (1 + \pi^\beta\theta)\rho_1$, where $\theta : G \to \mathrm{M}_n(\mathcal{O}_\lambda)$ is a function whose image is not contained in the maximal ideal λ.

Proposition 5.3.1. *If $\rho_1 \not\simeq \rho_2$, the function $\varphi : G \to \mathrm{M}_n(k) \rtimes \mathrm{GL}_n(k)$ defined by*

$$g \mapsto (\theta \bmod \lambda, \rho_1 \bmod \lambda)$$

is a group homomorphism which factors through the deviation group $\delta(G)$.

Proof. For $g, h \in G$, using

$$\begin{aligned}\rho_2(g) &= (1 + \pi^\beta\theta(g))\rho_1(g),\\ \rho_2(h) &= (1 + \pi^\beta\theta(h))\rho_1(h),\end{aligned}$$

we find that

$$\begin{aligned}\rho_2(gh) = \rho_1(g)\rho_1(h) &+ \pi^\beta\theta(g)\rho_1(g)\rho_1(h)\\ &+ \pi^\beta\rho_1(g)\theta(h)\rho_1(h) + \pi^{2\beta}\theta(g)\rho_1(g)\theta(h)\rho_1(h).\end{aligned}$$

Comparing this expression with $\rho_2(gh) = (1 + \pi^\beta\theta(gh))\rho_1(gh)$, we find that

$$\theta(gh) = \theta(g) + \theta(h)^{\rho_1(g)} + \pi^\beta\theta(g)\theta(h)^{\rho_1(g)},$$

where x^y denotes the conjugation yxy^{-1}. Since $\beta \geq 1$, it follows that

$$\theta(gh) \equiv \theta(g) + \theta(h)^{\rho_1(g)} \bmod \lambda,$$

hence that $\varphi(gh) = \varphi(g)\varphi(h)$ with the group law coming from the action of $\mathrm{GL}_n(k)$ on $\mathrm{M}_n(k)$ by conjugation.

Now, to show that φ factors through $\delta(G)$, we need to show that $\operatorname{Ker}\delta \subseteq \operatorname{Ker}\varphi$.

Let $g \in \operatorname{Ker}\delta$, which means that (using the notations of Section 5.2) $\rho(g) \in 1 + \lambda M$, i.e., there exists elements $a_h \in \mathcal{O}_\lambda$, with $a_h = 0$ for almost all $h \in G$, such that

$$\rho(g) = 1 + \pi \sum_h a_h \rho(h).$$

Since $\rho = \rho_1 \times \rho_2$, this is really a pair of equations

$$\rho_i(g) = 1 + \pi \sum_h a_h \rho_i(h), \qquad i = 1, 2.$$

For $i = 1$, we see that this implies that $\rho_1(g) \equiv 1 \bmod \lambda$. Moreover, using the fact that $\rho_2 = (1 + \pi^\beta \theta)\rho_1$, the equation for $i = 2$ can be rewritten as

$$\rho_1(g) + \pi^\beta \theta(g)\rho_1(g) = 1 + \pi \sum_h a_h \rho_1(h) + \pi \sum_h a_h \pi^\beta \theta(h)\rho_1(h).$$

Substracting the first equation, we find that

$$\theta(g)\rho_1(g) = \pi \sum_h a_h \theta(h)\rho_1(h),$$

hence

$$\theta(g) = \pi \sum_h a_h \theta(h)\rho_1(hg^{-1}) \equiv 0 \bmod \lambda,$$

so that $\varphi(g) = (0, 1)$, i.e. $g \in \operatorname{Ker}\varphi$. □

It $\varphi(G)$ denotes the image of G in the semi-direct product $\mathrm{M}_n(k) \rtimes \mathrm{GL}_n(k)$, it follows that the residual surjection $\delta(G) \twoheadrightarrow \overline{G}$ of (5.1) can be refined to

$$\delta(G) \twoheadrightarrow \varphi(G) \twoheadrightarrow \overline{G}.$$

Note also that from $\rho_2 = (1 + \pi^\beta \theta)\rho_1$, we have

$$\det \rho_2 = (1 + \pi^\beta \operatorname{tr}\theta + O(\pi^{\beta^2})) \det \rho_1,$$

so that if in addition we require that $\det \rho_1 = \det \rho_2$, it follows that

$$\operatorname{tr}\theta \equiv 0 \bmod \lambda^\beta.$$

In particular, the homomorphism φ then has values in

$$\mathrm{M}_n^\circ(k) \rtimes \mathrm{GL}_n(k),$$

where M_n° denotes the set of $n \times n$ matrices of trace 0.

However, in general, $\delta(G) \twoheadrightarrow \varphi(G)$ *may or may not* be an isomorphism. From the proof of Proposition 5.3.1, we see that an element $g \in G$ lies in $\operatorname{Ker}\delta$ if and only

$$\rho_1(g) = 1 + \pi \sum_h a_h \rho_1(h), \tag{5.2}$$

$$\theta(g) = \pi \sum_h a_h \theta(h)\rho_1(h)\rho_1(g)^{-1} \tag{5.3}$$

for some $a_h \in \mathcal{O}_\lambda$, $h \in G$.

Proposition 5.3.2. *For $G = \mathbf{Z}$, $\rho_1 = \mathbf{1}$ and $\rho_2 : G \to \mathrm{GL}_n(\mathcal{O}_\lambda)$ any non-trivial semisimple representation such that $\rho_2 \equiv \mathbf{1} \bmod \lambda$, we have*

$$\delta(G) = \varphi(G) \simeq (k, +).$$

Proof. Since for any $n \in G$ we have $\rho_2(n) = \rho_2(1)^n$, we have

$$1 + \pi^\beta \theta(n) = (1 + \pi^\beta \theta(1))^n = \sum_{j=0}^{n} \binom{n}{j} \pi^{j\beta} \theta(1)^j$$

by the binomial formula, so that

$$\theta(n) = \sum_{j=1}^{n} \binom{n}{j} \pi^{(j-1)\beta} \theta(1)^j \equiv n\theta(1) \bmod \lambda.$$

Consequently, if $n \in \operatorname{Ker}\varphi$, then $\pi \mid n$ in $\mathcal{O}_\lambda$, so that $n = a\pi$ for some $a \in \mathcal{O}_\lambda$. But then we may write

$$\begin{aligned} \rho_1(n) &= 1 + a\rho_1(1) - a\rho_1(0), \\ \theta(n) &= \pi\big(a\theta(1) - a\theta(0)\big), \end{aligned}$$

which show according to (5.2) that $n \in \operatorname{Ker}\delta$. Hence here $\operatorname{Ker}\delta = \operatorname{Ker}\varphi$, and the conclusion follows. □

Note that this proposition can be used to construct examples where $\delta(G) = \varphi(G)$

and G is a profinite group. The representation ρ_2 in the proposition, which is trivial modulo λ, actually has values in $1+\lambda\,\mathrm{M}_n(\mathcal{O}_\lambda)$, which is a pro-$\ell$-group since it embeds into the additive group $\lambda\,\mathrm{M}_n(\mathcal{O}_\lambda)$ via the logarithm (ℓ being the residual characteristic). It follows that

$$\rho_2 : \mathbf{Z} \longrightarrow 1+\lambda\,\mathrm{M}_n(\mathcal{O}_\lambda)$$

extends to $\mathbf{Z}_\ell$, and the proposition holds with $G=\mathbf{Z}_\ell$.

However, in certain situations, we can have $\operatorname{Ker}\delta \subsetneq \operatorname{Ker}\varphi$.

Remark. Serre, in [58], seems to imply that if $\rho_1, \rho_2 : G \to \mathrm{GL}_2(\mathbf{Z}_2)$ are two 2-adic representations such that $\det\rho_1 = \det\rho_2$ and the residual representations $\overline{\rho}_1$ and $\overline{\rho_2}$ are equal and surjective, we have

$$\delta(G) \simeq \varphi(G).$$

In a recent conversation with the author of this thesis, he said that maybe he did not actually prove that the map $\delta(G) \to \varphi(G)$ was surjective, but merely, in an unpublished letter to Tate, that the β in the construction of φ was equal to the α in the proof of Proposition 5.2.3, i.e. that ρ_1 and ρ_2 are conjugated modulo 2^α if and only if $\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \bmod 2^\alpha$. This would mean that the function

$$2^{-\alpha}(\operatorname{tr}\rho_1 - \operatorname{tr}\rho_2) \bmod 2,$$

considered in the proof of Proposition 5.2.3, descends to $\varphi(G)$. Consequently, $\varphi(G)$ could be used in place of the deviation group in Corollary 5.2.4 as explained below, making its application to decide whether two representations satisfying the hypotheses of this remark are equivalent or not a lot easier.

Indeed, to make this even more explicit, note that note that as an S_3-module, under the action by conjugation of $S_3 \simeq \mathrm{GL}_2(\mathbf{F}_2)$,

$$\mathrm{M}_2(\mathbf{F}_2) \simeq \mathbf{F}_2^2 \oplus V_4,$$

with

$$\mathbf{F}_2^2 = \left\{0, 1, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}, \quad V_4 = \left\{0, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}\right\}.$$

Likewise, the subgroup $\mathrm{M}_2^\circ(\mathbf{F}_2)$ has the decomposition $\mathbf{F}_2 \oplus V_4$ with $\mathbf{F}_2 = \{0,1\}$.

It follows that the only possibilities for $\varphi(G)$ when $\det\rho_1 = \det\rho_2$ and $\overline{\rho}_1 = \overline{\rho}_2$ is surjective are

$$\{\pm 1\} \times S_3, \quad V_4 \rtimes S_3 \simeq S_4, \quad \text{and} \quad (\mathbf{F}_2 \oplus V_4) \rtimes S_3 \simeq \{\pm 1\} \times S_4,$$

hence the name "quartic fields method".

A last consequence worth remarking from the identity $\rho_2 = (1 + \pi^\beta\theta)\rho_1$ is that

$$\operatorname{tr}\rho_2 = \operatorname{tr}\rho_1 + \pi^\beta \operatorname{tr}(\theta\rho_1),$$

and that $\operatorname{tr}(\theta\rho_1) \equiv \operatorname{tr}(\overline{\theta}\overline{\rho_1}) \bmod \lambda$. Thus,

$$\pi^{-\beta}(\operatorname{tr}\rho_1 - \operatorname{tr}\rho_2) \bmod \lambda$$

descends to a function on $\varphi(G)$. If $\rho_1 \not\sim \rho_2$, and *if* the β from this section happens to be equal to the α from the proof of Proposition 5.2.3, and Σ is a subset of G surjecting onto $\varphi(G)$, then we conclude that there exists $g \in \Sigma$ such that

$$\operatorname{tr}\rho_1(g) \neq \operatorname{tr}\rho_2(g).$$

However, *if* $\beta < \alpha$, then we are not guaranteed to find such a "certificate of non-equivalence" in Σ if we merely require that Σ surjects onto $\varphi(G)$.

5.4 The Faltings-Serre-Livné criterion

In this section we restrict our attention to 2-dimensional λ-adic representations

$$\rho_1, \rho_2 : G \longrightarrow \mathrm{GL}_2(\mathcal{O}_\lambda)$$

where $\mathcal{O}_\lambda$ has residual characteristic 2. Moreover, we impose that

$$\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \equiv 0 \bmod \lambda \qquad \text{and} \qquad \det\rho_1 \equiv \det\rho_2 \equiv 1 \bmod \lambda. \tag{5.4}$$

In this context, we present a proof of the Faltings-Serre-Livné criterion [40] to decide whether $\rho_1 \sim \rho_2$, in a form which will lend itself to generalization in the next section. The following set will play a crucial role.

Definition 5.4.1. Define Ξ to be the set of elements $g \in G$ for which the characteristic

polynomials of $\rho_1(g)$ and $\rho_2(g)$ coincide (or, equivalently, such that $\operatorname{tr}\rho_1(g^i) = \operatorname{tr}\rho_2(g^i)$ for $i = 1, 2$).

The strategy to decide whether ρ_1 and ρ_2 are equivalent, which will also be used in the next section, can roughly be described as follows. Suppose we were to test every element of G individually to see whether it belongs to Ξ or not. If we meet a single element which is not in Ξ, meaning that $\Xi \neq G$, then we know that $\rho_1 \not\sim \rho_2$. On the other hand, if all the group elements that we encounter lie in Ξ, we might think that there is "a good chance" that ρ_1 and ρ_2 are equivalent.

More precisely, call Σ the set of elements that we know are in Ξ. The bigger Σ is, the stronger is the evidence that ρ_1 and ρ_2 might actually be equivalent, and we know that to turn this evidence into a proof we just need to take Σ big enough so that it surjects onto $\delta(G)$. The problem is that computing precisely $\delta(G)$ requires a lot more information on ρ_1 and ρ_2 than we are able to get by computing a finite number of traces. On the other hand, we might try to list all the possibilities *a priori* for $\delta(G)$, and then just take Σ large enough to cover all such possibilities.

But then again, it is hard to say something precise on the structure of $\delta(G)$ (apart from the bound on its size from Proposition 5.2.2). So we use a bootstrap strategy in three steps.

- First, classify all possibilities for $\delta(G)$ if ρ_1 and ρ_2 *were* equivalent.
- Build sufficient evidence that ρ_1 and ρ_2 might be equivalent to force $\delta(G)$ to actually belong to the list established in the previous step.
- Then take Σ large enough to cover all the possibilities for $\delta(G)$ in that list.

The "bootstrap" aspect of the strategy comes from the fact that what we want in the end is a statement of the form *if a large enough set Σ is known, then ρ_1 and ρ_2 are equivalent* (with a precise meaning of "large enough"), so the second and third step of the strategy are actually achieved at the same time by having this large enough Σ.

So let us first see what $\delta(G)$ looks like when ρ_1 and ρ_2 are equivalent.

Proposition 5.4.2. *If $g \in \Xi$, then $\delta(g)^2 = 1$ in $\delta(G)$.*

Proof. For $g \in \Xi$, we write $\operatorname{tr} g$ for the common value of $\operatorname{tr}\rho_i(g)$, and similarly for $\det g$. Since the characteristic polynomials of $\rho_1(g)$ and $\rho_2(g)$ are equal, we have

$$\rho(g)^2 = (\operatorname{tr} g)\rho(g) - (\det g)\rho(1).$$

Hence, by the hypothesis (5.4),

$$\rho(g)^2 - \rho(1) = (\operatorname{tr} g)\rho(g) - (\det g + 1)\rho(1) \in \lambda\rho(g) + (2+\lambda)\rho(1) \subseteq \lambda M,$$

so that $\rho(g)^2 \equiv \rho(1) \bmod \lambda M$, i.e. $\delta(g)^2 = \delta(1) = 1$ in $\delta(G)$. □

Corollary 5.4.3. *If $\rho_1 \sim \rho_2$, then $\delta(G)$ is an abelian group of exponent 2.*

Proof. If $\rho_1 \sim \rho_2$, then $\Xi = G$, hence $\delta(G) = \delta(\Xi)$ has exponent 2. □

In general however, we cannot say much more than the following.

Proposition 5.4.4. *The deviation group $\delta(G)$ is a 2-group.*

More precisely, Proposition 5.2.2 implies that $|\delta(G)| = 2^r$ with $0 \leq r \leq 7$.

Proof. Recall from Remark 5.2 that $\delta(G)$ fits into a short exact sequence

$$1 \longrightarrow N(G) \longrightarrow \delta(G) \longrightarrow \overline{G} \longrightarrow 1$$

where $N(G)$ is a finite quotient of $\rho(G) \cap (1+\lambda R)$, where $R = \mathrm{M}_2(\mathcal{O}_\lambda) \oplus \mathrm{M}_2(\mathcal{O}_\lambda)$. Now the multiplicative group $1 + \lambda R$ embeds (via the logarithm) into the additive group λR, hence is a pro-2-group. It follows (e.g. [3, Cor. 10.4]) that $N(G)$ is a 2-group.

Moreover, by the condition 5.4, the characteristic polynomial of ρ_i, $i = 1, 2$, is

$$1 - (\operatorname{tr} \rho_i)t + (\det \rho_i)t^2 \equiv 1 + t^2 \bmod \lambda.$$

By Cayley-Hamilton, for every $g \in G$, one has

$$\rho_i(g)^2 \equiv -1 \equiv 1 \bmod \lambda, \quad i = 1, 2.$$

It follows that $\rho(g)^2 \equiv 1 \bmod \lambda$, i.e. that $\overline{G}$ has exponent 2, hence in particular is an abelian 2-group. So we conclude that $\delta(G)$, being an extension of $\overline{G}$ by N, is a 2-group. □

The bootstrap process rests heavily on a technical group-theoretical lemma.

Definition 5.4.5. For H any group, we denote $N_2(H) = \langle\, h^2 \mid h \in H \,\rangle$ the subgroup generated by squares.

It is clear that $N_2(H)$ is a characteristic subgroup of H; hence we can consider $H_2 := H/N_2(H)$ the 2-*quotient* (for lack of a better term) of H.

Proposition 5.4.6. *H_2 is the greatest quotient of H of exponent 2. Moreover, if N is a normal subgroup of H, then*

$$(H/N)_2 \simeq H/(N_2(H) \cdot N).$$

In particular, $(H/N)_2 = H_2$ if and only if $N \subseteq N_2(H)$.

Proof. H/N is a quotient of H of exponent 2 if and only if N is a normal subgroup which contains all the squares, that is, $N \supseteq N_2(H)$. The first part follows from the fact that $N_2(H)$ is itself normal. For the second part, if N is any normal subgroup of H, it is easily seen that $N_2(H/N) = (N_2(H) \cdot N)/N$, from which the conclusion follows. □

We also use the notation $H[2]$ for the set of elements of 2-torsion in H. Note that $H[2]$ need not be a subgroup of H when H is not abelian.

Lemma 5.4.7. *Let H be a 2-group such that every element in H_2 has a lift to an element of $H[2]$. Then H has exponent 2, i.e. $H = H_2$.*

Proof. Consider the defining short exact sequence for H_2,

$$1 \longrightarrow N_2(H) \longrightarrow H \longrightarrow H_2 \longrightarrow 1.$$

By contradiction: suppose that $N_2(H) \neq 1$.

- Without loss of generality, we can assume that $N_2(H)$ is cyclic of order 2.

  Indeed, let Ω be the set of subgroups of index 2 of $N_2(H)$. Writing the abelianization of the 2-group $N_2(H)$ as

  $$N_2(H)_{\mathrm{ab}} = \bigoplus_{i=1}^{k} \mathbf{Z}/2^{a_i}\mathbf{Z}, \qquad k, a_i \geq 1,$$

  we see that $|\Omega| = 2^k - 1$ is odd so that H acts on Ω by conjugation with at least one fixed point $N \in \Omega$. Replacing H by H/N (which doesn't change its 2-quotient thanks to Proposition 5.4.6), we get the desired situation.

- Remark that $N_2(H) = \langle n \rangle$ is then necessarily central: for $h \in H$, hnh^{-1} must be an element of order 2 in N, hence $hnh^{-1} = n$.

- The elements of order 2 in H commute.

  For two elements h, h' of order 2, consider their product hh'. It is either of the form h'' or $h''n$ where h'' has order 2. In both cases we see that $(hh')^2 = 1$.

- So we can find a section of $H \to H_2$ by picking generators of H_2 and sending them to some lifts of order 2 in H.

We conclude that $H \simeq N \times H_2$, which contradicts the definition of the 2-quotient. □

With this tool we can derive a criterion for equivalence.

Theorem 5.4.8. *Let $\rho_1, \rho_2 : G \to \mathrm{GL}_2(\mathcal{O}_\lambda)$ be two representations satisfying condition (5.4), and*

$$\Xi = \{g \in G \mid \operatorname{tr}\rho_1(g) = \operatorname{tr}\rho_2(g),\ \det\rho_1(g) = \det\rho_2(g)\}.$$

Then $\rho_1 \sim \rho_2$ if and only if Ξ surjects onto G_2.

Proof. For ($\Rightarrow$) there is nothing to prove since $\Xi = G$. Now for ($\Leftarrow$), consider the following diagram of quotients of G.

$$\begin{array}{ccc} G & \twoheadrightarrow & G_2 \\ \downarrow & & \downarrow \\ \delta(G) & \twoheadrightarrow & \delta(G)_2 \end{array}$$

Since Ξ surjects onto G_2 by hypothesis, it also surjects onto $\delta(G)_2$. But, by Proposition 5.4.2, the images of the elements of Ξ in $\delta(G)$ lie in $\delta(G)[2]$, hence we can apply the lemma to $\delta(G)$ to conclude that $\delta(G) = \delta(G)_2$. In particular, it follows that Ξ surjects onto $\delta(G)$, which guarantees the equivalence of ρ_1 and ρ_2 by Proposition 5.2.3. □

Actually, the version of the theorem proved in [40] is slightly stronger, stating that $\rho_1 \sim \rho_2$ if and only if the image of Ξ in G_2, considered as an affine space over $\mathbf{F}_2$, is not contained in any proper cubic hypersurface. However, this does not make a big difference unless the set S of allowed ramification is large.

Application to Galois representations. This is the criterion essentially as is stated in [40].

Theorem 5.4.9. *Let K be a number field and E_λ a finite extension of $\mathbf{Q}_2$ with ring of integers $\mathcal{O}_\lambda$ and maximal ideal λ. Let*

$$\rho_1, \rho_2 : \mathrm{Gal}_K \longrightarrow \mathrm{GL}_2(E_\lambda)$$

be two continuous representations unramified outside a finite set S of primes of K, and such that

$$\mathrm{tr}\,\rho_1 \equiv \mathrm{tr}\,\rho_2 \equiv 0 \bmod \lambda \qquad \textit{and} \qquad \det\rho_1 \equiv \det\rho_2 \equiv 1 \bmod \lambda.$$

Let $K_{2,S}$ be the compositum of all quadratic extensions of K unramified outside S and suppose that there exists a set of primes T disjoint from S such that:

1. $\{\mathrm{Frob}_\mathfrak{p} \mid \mathfrak{p} \in T\}$ *surjects onto* $\mathrm{Gal}(K_{2,S}/K)$*;*
2. $\mathrm{tr}\,\rho_1(\mathrm{Frob}_\mathfrak{p}) = \mathrm{tr}\,\rho_2(\mathrm{Frob}_\mathfrak{p})$ *and* $\det\rho_1(\mathrm{Frob}_\mathfrak{p}) = \det\rho_2(\mathrm{Frob}_\mathfrak{p})$ *for all* $\mathfrak{p} \in T$*.*

Then ρ_1 and ρ_2 are equivalent.

Proof. Remark that since $\mathrm{Gal}(\overline{K}/K)$ is compact, ρ_1 and ρ_2 preserve an $\mathcal{O}_\lambda$-lattice in E_λ^2, so that we may view them as taking values in $\mathrm{GL}_2(\mathcal{O}_\lambda)$. Then we only need to apply the previous proposition to $G = \mathrm{Gal}(\overline{K}/K)_S = \mathrm{Gal}(K_S/K)$, where K_S is the maximal extension of K unramified outside S, since then $G_2 = \mathrm{Gal}(K_{2,S}/K)$. □

To apply this criterion, one needs to describe explicitly the compositum $K_{2,S}$ of all the quadratic extensions of K unramified outside S, together with its Galois group. This will be addressed in general in section 5.6, but when $K = \mathbf{Q}$ the situation is particularly simple.

- For p an odd prime, set $d_p = \left(\frac{-1}{p}\right) p$ so that $\mathbf{Q}_{2,p} = \mathbf{Q}(\sqrt{d_p})$, and Frob_t, $t \notin S \cup \{2\}$, goes to $\left(\frac{d_p}{t}\right) = \left(\frac{t}{p}\right)$ under

$$\varepsilon_p : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Gal}(\mathbf{Q}_{2,p}/\mathbf{Q}) \simeq \{\pm 1\}.$$

- $\mathbf{Q}_{2,2} = \mathbf{Q}(i, \sqrt{2}) = \mathbf{Q}(\zeta_8)$, and Frob_t, $t \notin S$, goes to $t \bmod 8$ under

$$\varepsilon_2 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Gal}(\mathbf{Q}_{2,2}/\mathbf{Q}) \simeq (\mathbf{Z}/8\mathbf{Z})^\times.$$

- For a general S, $\mathbf{Q}_{2,S} = \prod_{p\in S} \mathbf{Q}_{2,p}$ and

$$\varepsilon_S = \prod_{p\in S} \varepsilon_p : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Gal}(\mathbf{Q}_{2,S}/\mathbf{Q}) \simeq \prod_{p\in S} \mathrm{Gal}(\mathbf{Q}_{2,p}/\mathbf{Q}).$$

So applying the criterion involves comparing the traces of ρ_1 and ρ_2 at $2^{|S|+1}$ primes at most.

Example 5.4.10. This criterion was used in [39] to prove the modularity of the compatible systems of representations of $\mathrm{Gal}_{\mathbf{Q}}$ occurring in the middle-degree cohomology of $\widetilde{W}_2^{10}$. The trace of the representation could be shown to be even by using the symmetries to show that the number of points over finite fields were always even.

5.5 Generalization

In this section, we restrict ourselves to the case $\mathcal{O}_\lambda = \mathbf{Z}_2$ to keep the complexity under control, but we only assume that

$$\mathrm{tr}\,\rho_1 \equiv \mathrm{tr}\,\rho_2 \bmod 2.$$

Note that in this context, it is automatic that $\det\rho_1 \equiv \det\rho_2 \equiv 1 \bmod 2$. We adapt to this setting each result from the previous section. Recall that we use C_n to denote the cyclic group of order n, and S_n for the symmetric group on n letters.

Proposition 5.5.1. *In this setting, the residual group $\overline{G}$ is either isomorphic to 1, C_2, $C_2 \times C_2$, C_3, or S_3.*

Proof. In $\mathrm{GL}_2(\mathbf{F}_2) \simeq S_3$, the elements of order 3 are those with trace 1, while the elements with trace 0 have order 1 or 2. Thus the hypothesis on the traces of ρ_1 and ρ_2 implies that for an element (x, y) in $\overline{G} \subseteq \mathrm{GL}_2(\mathbf{F}_2) \times \mathrm{GL}_2(\mathbf{F}_2)$, one has

$$O(x) = 3 \iff O(y) = 3.$$

If $\overline{G}$ contains no element (x, y) with $O(x) = O(y) = 3$, then

$$\overline{G} \subseteq \{1, (12), (13), (23)\} \times \{1, (12), (13), (23)\}.$$

It is readily checked that $\overline{G}$ is then an abelian group of exponent 2 and order at most 4.

On the other hand, suppose that $\overline{G}$ contains an element (x, y) where x and y have order 3, so that it contains the cyclic subgroup $H := \langle (x, y) \rangle$. It is not possible that $\overline{G}$ contains any other element of order 3, because then the order of $\overline{G}$ would be divisible by 9, hence $\delta(G)$ would contain the whole 3-Sylow subgroup of $S_3 \times S_3$,

$$\{1, (123), (132)\} \times \{1, (123), (132)\},$$

which is forbidden by the hypothesis on the traces.

If $\overline{G} \neq H$, then $\overline{G} \setminus H$ consists entirely of elements of the form (a, b) where a and b both have order 2. If (a, b) and (a', b') are two distinct such elements, it is impossible to have $a = a'$ or $b = b'$, because then the product (aa', bb') would have one trivial component and the other of order 3. So, if $(a, b) \in \overline{G} \setminus H$, we see that

$$\overline{G} = \{1, (x, y), (x^2, y^2), (a, b), (ax, by), (ax^2, by^2)\} \simeq S_3,$$

and this concludes the proof. □

Corollary 5.5.2. *The order of $\delta(G)$ is of the form $2^a 3^b$ with $b \leq 1$.*

Again, together with Proposition 5.2.2, this implies that the order of the deviation group is either 2^a with $0 \leq a \leq 7$, or $3 \cdot 2^a$ with $0 \leq a \leq 6$.

Proof. This follows at once from the reduction modulo 2 short exact sequence

$$1 \longrightarrow N(G) \longrightarrow \delta(G) \longrightarrow \overline{G} \longrightarrow 1$$

and the previous proposition, because $N(G)$ is a 2-group. □

The following generalizes Proposition 5.4.8.

Proposition 5.5.3. *Let $\rho_1, \rho_2 : G \to \mathrm{GL}_2(\mathbf{Z}_2)$ be two representations such that $\operatorname{tr} \rho_1 \equiv \operatorname{tr} \rho_2 \bmod 2$. Then $\rho_1 \sim \rho_2$ if and only if Ξ surjects onto all quotients of G of the form $G/N_2(W)$, where W ranges over all the normal subgroups of G such that*

$$G/W \simeq 1, C_3 \text{ or } S_3.$$

Note that when W is normal, $N_2(W)$ is automatically normal in G as well since it is a characteristic subgroup of W.

Proof. Again ($\Rightarrow$) is clear because if $\rho_1 \sim \rho_2$ then $\Xi = G$. Now for ($\Leftarrow$), if $\delta(G)$ is a 2-group, then, taking $W = G$, we conclude as in the proof of 5.4.8 that $\rho_1 \sim \rho_2$. So let us consider the case where the order of $\delta(G)$ is divisible by 3. Let W be the kernel of the reduction map $G \to \overline{G}$, so that $G/W = \overline{G}$ is isomorphic to C_3 or S_3, and let N be the kernel of $\delta : G \to \delta(G)$. The kernel $N(G)$ in the short exact sequence

$$1 \longrightarrow N(G) \longrightarrow \delta(G) \longrightarrow \overline{G} \longrightarrow 1$$

is thus identified with W/N. Modding out by $N_2(N(G))$, we obtain a new short exact sequence

$$1 \longrightarrow N(G)_2 \longrightarrow \delta(G)/N_2(N(G)) \longrightarrow \overline{G} \longrightarrow 1.$$

Now $N(G)_2$ is a quotient of exponent 2 of $N(G) = W/N$; in particular, it is a quotient of exponent 2 of W, so $N(G)_2$ is a quotient of the 2-quotient W_2. We have the following commutative diagram.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & W_2 & \longrightarrow & G/N_2(W) & \longrightarrow & G/W & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & N(G)_2 & \longrightarrow & \delta(G)/N_2(N(G)) & \longrightarrow & \overline{G} & \longrightarrow & 1 \end{array}$$

By hypothesis, since G/W is isomorphic to C_3 or S_3, we know that Ξ surjects onto $G/N_2(W)$, so that it surjects onto $\delta(G)/N_2(N(G))$. It follows that every element of $N(G)_2$ has a lift in $N(G)[2]$, so by Lemma 5.4.7, we conclude that $N_2(N(G)) = 1$. Hence Ξ actually surjects onto $\delta(G)/N_2(N(G)) = \delta(G)$, proving that $\rho_1 \sim \rho_2$. □

Corollary 5.5.4. *Let K be a number field and $\rho_1, \rho_2 : \mathrm{Gal}_K \to \mathrm{GL}_2(\mathbf{Q}_2)$ two continuous 2-adic Galois representations unramified outside a finite set of primes S and such that $\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \bmod 2$. If L/K is a Galois extension unramified outside S, denote by $L_{2,S}$ the compositum of all quadratic extensions of L unramified at primes above S (then $L_{2,S}$ is itself a Galois extension of K unramified outside S). Suppose that there exists a set of primes T disjoint from S such that*

1. $\{\mathrm{Frob}_\mathfrak{p} \mid \mathfrak{p} \in T\}$ *surjects onto* $\mathrm{Gal}(L_{2,S}/K)$ *for all* L/K *with*

$$\mathrm{Gal}(L/K) \simeq 1, C_3 \text{ or } S_3;$$

2. $\operatorname{tr}\rho_1(\mathrm{Frob}_\mathfrak{p}) = \operatorname{tr}\rho_2(\mathrm{Frob}_\mathfrak{p})$ *and* $\det\rho_1(\mathrm{Frob}_\mathfrak{p}) = \det\rho_2(\mathrm{Frob}_\mathfrak{p})$ *for all* $t \in T$.

Then ρ_1 and ρ_2 have isomorphic semisimplifications.

Example 5.5.5. This is essentially the approach used by Socrates and Whitehouse [60] to prove that the Galois representation on the Tate module of a certain elliptic curve E over $\mathbf{Q}(\sqrt{5})$ was associated to a Hilbert modular form f. More precisely, in this example there was a priori only one possibility for $W \subseteq G_{\mathbf{Q}(\sqrt{5})}$, the kernel of the modulo 2 representations. Using the original Faltings-Serre-Livné criterion, one could then prove that ρ_E and ρ_f were equivalent as representations of W, and then conclude that are equivalent as $G_{\mathbf{Q}(\sqrt{5})}$ as well using a Frobenius reciprocity argument.

Note that in practice, the first thing to do when trying to decide if two representations $\rho_1, \rho_2 : G \to \mathrm{GL}_2(\mathbf{Z}_2)$ are isomorphic is first to check whether the residual representations $\overline{\rho}_1$ and $\overline{\rho}_2$ are conjugated in $\mathrm{GL}_2(\mathbf{F}_2)$. If not, then $\rho_1 \not\simeq \rho_2$. If they are conjugated, then without loss of generality when can assume that $\overline{\rho}_1 = \overline{\rho}_2$.

Remark. If two subgroups H_1, H_2 of $\mathrm{GL}_2(\mathbf{F}_2) \simeq S_3$ have the same cardinality, then not only are they abstractly isomorphic, but they are also conjugated. It follows that if $|\operatorname{Im}\overline{\rho}_1| = |\operatorname{Im}\overline{\rho}_2|$, then without loss of generality, up to conjugation we may assume that $\operatorname{Im}\overline{\rho}_1 = \operatorname{Im}\overline{\rho}_2$ since

$$1 \longrightarrow 1 + 2\,\mathrm{M}_2(\mathbf{Z}_2) \longrightarrow \mathrm{GL}_2(\mathbf{Z}_2) \longrightarrow \mathrm{GL}_2(\mathbf{F}_2) \longrightarrow 1$$

splits. This does *not*, however, imply that the representations $\overline{\rho}_1$ and $\overline{\rho}_2$ are isomorphic.

It is possible to improve the straightforward generalization obtained in Proposition 5.5.3 by examining more carefully the possible structures of the deviation group.

Proposition 5.5.6. *For $g \in \Xi$, the order of $\delta(g)$ in $\delta(G)$ is*

$$\begin{cases} 1 \text{ or } 2 & \text{if } \operatorname{tr} g \equiv 0 \bmod 2, \\ 3 & \text{if } \operatorname{tr} g \equiv 1 \bmod 2. \end{cases}$$

Proof. First, note that if $\delta(g) = 1$, then $\overline{g} = 1$ in $\overline{G}$, so that the traces of $\rho_1(g)$ and $\rho_2(g)$ are even. For $g \in \Xi$, we still have

$$\rho(g)^2 = (\operatorname{tr} g)g - \det g \equiv (\operatorname{tr} g)g + 1 \bmod 2M.$$

If $\operatorname{tr} g \equiv 0 \bmod 2$, again $\delta(g)^2 = 1$ in $M/2M$ hence in $\delta(G)$. If $\operatorname{tr} g \equiv 1 \bmod 2$,

however, $\rho(g)^2 = \rho(g) + 1$ in $M/2M$, so that

$$\delta(g)^3 = \delta(g)(\delta(g) + 1) = \delta(g)^2 + \delta(g) = 1,$$

which concludes the proof. □

Corollary 5.5.7. *If $\rho_1 \sim \rho_2$, every nontrivial element of $\delta(G)$ has order 2 or 3.*

Hence, under the hypothesis that $\rho_1 \sim \rho_2$, we know that $\delta(G)$ is a group of order $2^a 3^b$, with $b = 0$ or 1, in which every nontrivial element has order 2 or 3. Let us classify all possibilities *a priori* for such a group.

Example 5.5.8. Of course, any finite group of exponent 2, i.e. ${C_2}^r$, is of this form.

Example 5.5.9. The symmetric group S_3 is a group of order 6 in which every element has order 2 or 3.

Example 5.5.10. Another important example is the alternating group A_4: it is a group of order 12 in which every nontrivial element has order 2 or 3. Remark that $A_4 = V_4 \rtimes C_3$, where C_3 permutes cyclically the 3 nontrivial elements in the Klein group

$$V_4 = \{1, (12)(34), (13)(24), (14)(23)\} \simeq {C_2}^2.$$

More generally, if one considers the diagonal action of C_3 on r copies of V_4, the semi-direct product ${V_4}^r \rtimes C_3$ is a group of order $3 \cdot 4^r$ in which all nontrivial elements have order 2 – those of the form $(x, 1)$ – or 3 – those of the form (x, σ), $\sigma \neq 1$.

The following theorem states that these examples form a complete list of such groups (up to isomorphism).

Theorem 5.5.11. *The finite groups of order $2^a 3^b$, $b = 0, 1$, in which every nontrivial element has order 2 or 3 are*

$$ {C_2}^r, \quad r \geq 0, \qquad {V_4}^r \rtimes C_3, \quad r \geq 0, \qquad \text{and} \quad S_3. $$

Proof. Let G be a group of order $2^a 3^b$, $b = 0, 1$, in which every nontrivial element has order 2 or 3.

- First let us consider the easy case where $b = 0$: in this case G is a 2-group, hence cannot contain any element of order 3. We conclude that G has exponent 2, so that $G \simeq {C_2}^r$ for some $r \geq 0$.

In the case where $b = 1$, we can distinguish two situations: the number of 2-Sylow subgroups of G is either 1 or 3.

- If there is a unique 2-Sylow subgroup P of G, then P is a normal subgroup and we have a short exact sequence

$$1 \longrightarrow P \longrightarrow G \longrightarrow C_3 \longrightarrow 1$$

which necessarily splits since G contains at least an element of order 3 which we call σ. Moreover, P is a group of exponent 2 and we can consider it as a finite-dimensional vector space over $\mathbf{F}_2$ on which $C_3 = \langle\sigma\rangle$ acts linearly. Let $v \in P$ be a nonzero element. Then the element $x := (v, \sigma) \in G = P \rtimes C_3$ has to have order 3 by our assumption on the orders of elements of G; this is equivalent to saying that

$$v + \sigma(v) + \sigma^2(v) = 0.$$

If follows that the σ-invariant subspace generated by v is

$$\{0, v, \sigma(v), \sigma^2(v)\},$$

which is isomorphic to V_4 with the standard σ-action. By induction on the dimension of P, it follows that $P \simeq V_4^r$ as a $\mathbf{F}_2[\sigma]$-module, hence

$$G = P \rtimes \langle\sigma\rangle \simeq {V_4}^r \rtimes C_3.$$

- The last case to consider is the case where the number of 2-Sylow subgroups in G is 3. The action of G by conjugation on these 3 subgroups P_1, P_2, P_3 yields a homomorphism

$$G \longrightarrow S_3$$

whose image is either C_3 or S_3 (because its kernel is a 2-group). But the former is impossible, because then the kernel would be a normal 2-Sylow subgroup; hence the latter holds and we have a short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow S_3 \longrightarrow 1.$$

Again we can check that this short exact sequence splits (using the fact that the set of elements in G acting on the 2-Sylow subgroups as (ij) is $P_k \setminus N$ for

$\{i, j, k\} = \{1, 2, 3\}$), hence we may view G as $N \rtimes S_3$ where N is a vector space over $\mathbf{F}_2$ on which S_3 acts.

Let τ be an element of order 2 in $S_3 \subseteq G$ and consider elements of the form (v, τ) in G with $v \in N$. These need to have order 2, which means that

$$v + \tau(v) = 0, \quad \text{or} \quad \tau(v) = v \qquad \text{for all } v \in N.$$

Since S_3 is generated by its elements of order 2, it follows that it acts trivially on N, so that $G = N \times S_3$. Then, in order for G to contain no element of order 6, we need to have $N = 1$, i.e. $G = S_3$.

This concludes the proof. □

This group-theoretic fact, together with Corollary 5.5.7, Corollary 5.5.2 and the remark directly following it, implies the following.

Corollary 5.5.12. *If $\rho_1, \rho_2 : G \to \mathrm{GL}_2(\mathcal{O})$ are two equivalent 2-adic representations such that $\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \bmod 2$, then their deviation group is isomorphic to*

$$C_2^r, \quad 0 \le r \le 7, \qquad V_4^r \rtimes C_3, \quad 0 \le r \le 3, \qquad \text{or} \qquad S_3.$$

We can now complete the "bootstrap" argument. Recall that the generalized quaternion group Q_n is defined by the presentation

$$Q_n := \langle a, b \mid a^2 = b^n, b^{2n} = 1, bab = a \rangle.$$

It has order $2n$ and fits into a non-split short exact sequence

$$1 \longrightarrow \langle \tau \rangle \longrightarrow Q_n \longrightarrow D_n \longrightarrow 1,$$

where $\tau = a^2 = b^n$ is the unique element of order 2 in Q_n.

Theorem 5.5.13. *Let $\rho_1, \rho_2 : G \to \mathrm{GL}_2(\mathbf{Z}_2)$ be two representations satisfying*

$$\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \bmod 2.$$

Then $\rho_1 \sim \rho_2$ if and only if

1. *Ξ surjects onto all quotients of G of the form ${C_2}^r$, ${V_4}^r \rtimes C_3$, or S_3;*

2. *The image of Ξ in every quotient of G of the form C_6 or Q_6 contains an element of order 6;*

3. *The image of Ξ in every quotient of G which is an extension of S_3 by V_4 contains an element of order greater than 3.*

Of course, if one know explicitly the residual group $\overline{G}$ as a quotient of G (not just as an abstract group), one needs only in the above to consider the given quotients of G which are extensions of $\overline{G}$.

Proof. Again ($\Rightarrow$) is clear because if $\rho_1 \sim \rho_2$ then $\Xi = G$. Now for ($\Leftarrow$), consider the deviation group $\delta(G)$. As in the proof of Theorem 5.5.11, we have the following trichotomy for the deviation group.

- If $\delta(G)$ is a 2-group, consider the short exact sequence

$$1 \longrightarrow N_2(\delta(G)) \longrightarrow \delta(G) \longrightarrow \delta(G)_2 \longrightarrow 1$$

  Since by assumption Ξ surjects onto G_2, it also surjects onto its quotient $\delta(G)_2$. Hence, by Proposition 5.5.6, every element if $\delta(G)_2$ lifts in $\delta(G)$ to an element of order 2; by Lemma 5.4.7 it follows that Ξ surjects onto $\delta(G) = \delta(G)_2$, proving that $\rho_1 \sim \rho_2$.

- If $\overline{G} \simeq C_3$, consider the split short exact sequence

$$1 \longrightarrow N(G)_2 \longrightarrow \delta(G)/N_2(N(G)) \longrightarrow C_3 \longrightarrow 1,$$

  the splitting being induced by the choice of an element of order 3 in the middle group. Now we may consider $N(G)_2$ as a vector space over $\mathbf{F}_2$, endowed with a linear action of C_3. By the standard theory of group representations (which applies because $3 \neq 0 \in \mathbf{F}_2$), as C_3-modules we have

$$N(G)_2 \simeq {\mathbf{F}_2}^s \oplus {V_4}^r, \qquad \text{for some } s, r \geq 0.$$

  If $s > 0$, choose a subspace W of $N(G)_2$ which is isomorphic to ${\mathbf{F}_2}^{s-1} \oplus {V_4}^r$. Viewed as a subgroup of $N(G)_2 \rtimes C_3$, W is normal since it is abelian and stable under the action of C_3. Hence we conclude that $\delta(G)$ admits a quotient H of the form

$$N(G)_2/W \rtimes C_3 \simeq \mathbf{F}_2 \rtimes C_3 \simeq C_2 \times C_3 \simeq C_6.$$

By hypothesis, Ξ surjects onto H; but the element of order 6 in H cannot have a lift of order 2 or 3 in $\delta(G)$, contradiction.

Hence we conclude that $s = 0$, so that $\delta(G) \simeq {V_4}^r \rtimes C_3$. By hypothesis, Ξ surjects onto $\delta(G)$, which implies that $\rho_1 \sim \rho_2$.

- In the remaining case, consider the short exact sequence

$$1 \longrightarrow N(G)_2 \longrightarrow \delta(G)/N_2(N(G)) \longrightarrow S_3 \longrightarrow 1.$$

Note that it needs not be split, but in any case the abelian group $N(G)_2$ can be viewed as linear representation for S_3 over $\mathbf{F}_2$, where the elements of S_3 act by conjugation by theirs lifts.

If $N(G)_2 \neq 0$, let $W \subseteq N(G)_2$ be a maximal S_3-invariant subspace of $N(G)_2$; viewed as a subgroup of $H := \delta(G)/N_2(N(G))$, it is normal, so we can consider the short exact sequence

$$1 \longrightarrow N(G)_2/W \longrightarrow H/W \longrightarrow S_3 \longrightarrow 1.$$

By [54, th. 41], the simple $\mathbf{F}_2[S_3]$-module $N(G)_2$ is either isomorphic to $\mathbf{F}_2$ with the trivial S_3-action, or to V_4 with the standard action of $S_3 \simeq \mathrm{GL}_2(\mathbf{F}_2)$.

In the first case, we have a short exact sequence

$$1 \longrightarrow C_2 \longrightarrow H/W \longrightarrow S_3 \longrightarrow 1.$$

There are, up to isomorphism, only two such short exact sequences. If it is split, then $H/W \simeq C_2 \times S_3 \simeq D_6$, while if it is non-split, H/W is isomorphic to Q_6. In both cases, by hypothesis an element of order 6 is in the image of Ξ. But such an element cannot have a lift to an element of order 2 or 3 in $\delta(G)$, contradiction.

In the second case,

$$1 \longrightarrow V_4 \longrightarrow H/W \longrightarrow S_3 \longrightarrow 1,$$

by hypothesis H/W contains an element of order > 3 which is the image of an element of Ξ, which cannot lift to an element of order 2 or 3 in $\delta(G)$, contradiction again.

Overall, we conclude that $N(G)_2$ is trivial, which forces the 2-group $N(G)$ to be trivial as well and $\delta(G)$ to be isomorphic to $\overline{G} \simeq S_3$. Since by hypothesis Ξ surjects onto $\delta(G)$, we conclude that $\rho_1 \sim \rho_2$.

This concludes the proof. □

In light of the previous result, we make the following definition.

Definition 5.5.14. Let K be a number field, S a finite set of primes ideals of K and L/K a Galois extension of type $1, C_3$ or S_3 unramified outside S. For T a set of primes disjoint from S, let

$$\Sigma := \{\mathrm{Frob}_{\mathfrak{p}} \mid \mathfrak{p} \in T\} \cup \{\mathrm{Frob}_{\mathfrak{p}}^{-1} \mid \mathfrak{p} \in T\} \cup \{1\}.$$

We say that T is (L, S)-*sufficient* if Σ surjects onto $\mathrm{Gal}(L/K)$, and in addition:

- if $L = K$, Σ surjects onto the Galois group $\mathrm{Gal}(K_{2,S}/K)$ of the compositum $K_{2,S}$ of all quadratic extensions of K unramified outside S;
- if $\mathrm{Gal}(L/K) \simeq C_3$, Σ surjects onto the Galois group $\mathrm{Gal}(L'/\mathbf{Q})$ of the largest extension L'/L such that $\mathrm{Gal}(L'/L) \simeq V_4^r$ as a C_3-module; and, for every quadratic extension L'/K, the image of Σ in $\mathrm{Gal}(LL'/K)$ contains an element of order 6;
- if $\mathrm{Gal}(L/K) \simeq S_3$, for every Galois extension L'/L of type C_2 (resp. V_4) such that L'/K is Galois and S_3 acts on $\mathrm{Gal}(L'/L)$ trivially (resp. via the standard representation), the image of Σ in $\mathrm{Gal}(L'/K)$ contains an element of order greater than 3.

The set T is *sufficient for* S if it is (L, S)-sufficient for every Galois extension L/K of type $1, C_3$ or S_3 unramified outside S.

Using the elementary observation that $g \in \Xi \implies g^{-1} \in \Xi$, and that we always have $1 \in \Xi$, we obtain at once the following criterion.

Theorem 5.5.15. *Let K be a number field, $\rho_1, \rho_2 : \mathrm{Gal}_K \to GL_2(\mathbf{Q}_2)$ two continuous 2-adic representations unramified outside a finite set of primes S and satisfying*

$$\mathrm{tr}\,\rho_1 \equiv \mathrm{tr}\,\rho_2 \bmod 2,$$

and T a sufficient set of primes for S. Then $\rho_1 \sim \rho_2$ if and only if

$$\operatorname{tr}\rho_1(\mathrm{Frob}_\mathfrak{p}) = \operatorname{tr}\rho_2(\mathrm{Frob}_\mathfrak{p}), \quad \det\rho_1(\mathrm{Frob}_\mathfrak{p}) = \det\rho_2(\mathrm{Frob}_\mathfrak{p}) \quad \textit{for all } \mathfrak{p} \in T.$$

Moreover, if L is the Galois extension of K cut out by $\mathrm{Ker}(G \to \overline{G})$, then the same holds if T is merely an (L,S)-sufficient set of primes.

Note that if we know in advance that $\operatorname{Ker}\overline{\rho}_1 = \operatorname{Ker}\overline{\rho}_2$, then the hypothesis on the traces follows immediately, and $L = \operatorname{Ker}\overline{\rho}_1 = \operatorname{Ker}\overline{\rho}_2$.

5.6 Listing quadratic extensions

The task of computing sufficient sets of primes depends on being able to compute various quadratic extensions, unramified outside S, of certain cubic number fields of the base field K (and K itself), so we begin by summarizing some facts about quadratic extensions and their discriminants.

Recall from Kummer theory that the Galois extensions of a number field K having a Galois group of exponent 2, i.e. the compositums of quadratic extensions, are in 1-1 correspondence with the subgroups of $K^\times/(K^\times)^2$. To be precise, denote the set of all subgroups of $K^\times/(K^\times)^2$ by $\mathscr{S}_2(K)$ and let $\mathscr{E}_2(K)$ be the set of all abelian extensions of exponent 2 of K. Then we have a bijection

$$\mathrm{Kum}_K : \mathscr{E}_2(K) \xrightarrow{\sim} \mathscr{S}_2(K)$$

given by $L \mapsto \mathrm{Ker}\{K^\times/(K^\times)^2 \to L^\times/(L^\times)^2\}$ and with inverse $B \mapsto K(\sqrt{B})$ – where we make the abuse of confusing a subgroup $B \in \mathscr{S}_2(K)$ with its inverse image in $K^\times$.

Note that a subgroup $B \in \mathscr{S}_2(K)$ can be thought of as a vector space over the field $\mathbf{F}_2$. As such, the Galois group of $K(\sqrt{B})$ is identified with the dual $B^\vee$ of B under the map

$$\varphi_{K,B} : \mathrm{Gal}(K(\sqrt{B})/K) \xrightarrow{\sim} B^\vee \tag{5.5}$$

defined by $\varphi_{K,B}(\sigma) : b \mapsto \sigma(\sqrt{b})/\sqrt{b} \in \{\pm 1\}$. In particular, it follows that

$$[K(\sqrt{B}) : K] = 2^{\dim B} = |B|.$$

Note that the Kummer correspondence is well-behaved with respect to Galois automorphisms in the following sense: for every $\sigma \in \mathrm{Gal}_\mathbf{Q}$, the following diagram

commutes.

$$\begin{array}{ccc} \mathscr{E}_2(K) & \xrightarrow{\mathrm{Kum}_K} & \mathscr{S}_2(K) \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ \mathscr{E}_2(\sigma K) & \xrightarrow{\mathrm{Kum}_{\sigma K}} & \mathscr{S}_2(\sigma K) \end{array}$$

Similarly, if $L = K(\sqrt{B})$, then the isomorphisms given by (5.5) fit in a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \xrightarrow{\varphi_{K,B}} & B^\vee \\ \downarrow & & \downarrow \\ \mathrm{Gal}(\sigma L/\sigma K) & \xrightarrow{\varphi_{\sigma K,\sigma B}} & (\sigma B)^\vee \end{array}$$

where the left vertical arrow is $\tau \mapsto \sigma \circ \tau \circ \sigma^{-1}$ and the right one is $f \mapsto f \circ \sigma^{-1}$.

In the particular case where K is itself a Galois extension of $\mathbf{Q}$, the first commutative diagram tells us that the Kummer map

$$\mathrm{Kum}_K : \mathscr{E}_2(K) \xrightarrow{\sim} \mathscr{S}_2(K)$$

is Galois-equivariant (note that the action of $\mathrm{Gal}_{\mathbf{Q}}$ factors through $\mathrm{Gal}(K/\mathbf{Q})$). Consequently, the extensions $L \in \mathscr{E}_2(K)$ that are Galois over $\mathbf{Q}$ correspond under the Kummer map to subgroups B which are stable under the action of $\mathrm{Gal}(K/\mathbf{Q})$. For $L = K(\sqrt{B})$ such an extension, the identification (5.5) is then $\mathrm{Gal}(K/\mathbf{Q})$-equivariant, the action on $\mathrm{Gal}(L/K)$ being by conjugation.

We now want to explicit which subgroups correspond under the Kummer map to extensions of exponent 2 of K which are unramified outside a given set of primes S.

Proposition 5.6.1 ([7])**.** *Let $D \in \mathcal{O}_K$, and $L = K(\sqrt{D})$. Writing $(D) = \mathfrak{f}^2\mathfrak{d}$, where $\mathfrak{d}$ is a squarefree ideal, the discriminant ideal $\mathfrak{d}(L/K)$ satisfies*

$$\mathfrak{d} \mid \mathfrak{d}(L/K) \mid 4\mathfrak{d}.$$

Moreover, if $\mathfrak{p}$ is a prime ideal of K above 2, and $\mathfrak{p} \nmid \mathfrak{d}$, then $\mathfrak{p}$ divides $\mathfrak{d}(L/K)$ if and only if D is not congruent to a square modulo $\mathfrak{p}^{2e(\mathfrak{p}/2)}$.

Proposition 5.6.2. *Let K be a number field with group of principal ideals $\mathcal{P}$, group of fractional ideals $\mathcal{I}$ and class group $\mathcal{C}\ell$. We have the following exact sequences:*

$$1 \longrightarrow \mathcal{O}^\times/(\mathcal{O}^\times)^2 \longrightarrow K^\times/(K^\times)^2 \longrightarrow \mathcal{P}/\mathcal{P}^2 \longrightarrow 1$$

and

$$1 \longrightarrow \mathcal{C}\ell[2] \longrightarrow \mathcal{P}/\mathcal{P}^2 \longrightarrow \mathcal{I}/\mathcal{I}^2 \longrightarrow \mathcal{C}\ell/\mathcal{C}\ell^2 \longrightarrow 1.$$

Proof. First, the snake lemma, applied to the map $x \mapsto x^2$ on the short exact sequence

$$1 \longrightarrow \mathcal{O}^\times \longrightarrow K^\times \longrightarrow \mathcal{P} \longrightarrow 1,$$

yields a long exact sequence

$$1 \longrightarrow \mathcal{O}^\times[2] \longrightarrow K^\times[2] \longrightarrow \mathcal{P}[2] \longrightarrow \mathcal{O}^\times/(\mathcal{O}^\times)^2 \longrightarrow K^\times/(K^\times)^2 \longrightarrow \mathcal{P}/\mathcal{P}^2 \longrightarrow 1.$$

But by unique factorization in $\mathcal{P} \subseteq \mathcal{I}$, we have $\mathcal{P}[2] = 1$, which yields the first claim. (Remark incidentally that $\mathcal{O}^\times[2] = K^\times[2] = \{\pm 1\}$.)

The second short exact sequence can be obtained in much the same fashion, by applying the snake lemma to the power-2 map on

$$1 \longrightarrow \mathcal{P} \longrightarrow \mathcal{I} \longrightarrow \mathcal{C}\ell \longrightarrow 1,$$

which yields a long exact sequence,

$$1 \longrightarrow \mathcal{P}[2] \longrightarrow \mathcal{I}[2] \longrightarrow \mathcal{C}\ell[2] \longrightarrow \mathcal{P}/\mathcal{P}^2 \longrightarrow \mathcal{I}/\mathcal{I}^2 \longrightarrow \mathcal{C}\ell/\mathcal{C}\ell^2 \longrightarrow 1,$$

in which $\mathcal{P}[2] = \mathcal{I}[2] = 1$ by unique factorization. □

In particular, if the class number of K is odd, so that the 2-power map is bijective on the class group, the second exact sequence degenerates to $\mathcal{P}/\mathcal{P}^2 \simeq \mathcal{I}/\mathcal{I}^2$.

Since Proposition 5.6.1 tells us that the primes away from 2 that ramify in $K(\sqrt{D})$ only depend on the image of D in $\mathcal{I}/\mathcal{I}^2$, we can state the description we were after.

Corollary 5.6.3. *Let S be a set a primes of K containing all the primes above 2. Under the Kummer correspondence, the extensions of exponent 2 of K that are unramified outside S correspond bijectively to the subgroups of $K^\times/(K^\times)^2$ whose image in $\mathcal{I}/\mathcal{I}^2$ is supported on S.*

If S is a finite set of primes, this gives an algorithm to find all the quadratic extensions of K unramified outside S, stated here in the case where the class number h_K is odd for simplicity.

1. First, list all the square-free ideals $\mathfrak{d}$ supported on S (there are $2^{|S|}$ of them).

2. For every such $\mathfrak{d}$, there exists a unique ideal class $[\mathfrak{f}]$ such that $\mathfrak{f}^2\mathfrak{d}$ is principal (changing $\mathfrak{f}$ in its class changes $\mathfrak{f}^2\mathfrak{d}$ by the square of a principal ideal). We can choose $\mathfrak{f}$ suitably so that $\mathfrak{f}^2\mathfrak{d}$ is an integral ideal, and find $D_\mathfrak{d} \in \mathcal{O}$ such that $\mathfrak{f}^2\mathfrak{d} = (D_\mathfrak{d})$.

3. Now let ζ be a primitive root of 1 in $\mathcal{O}$, and $\varepsilon_1, \ldots, \varepsilon_r$ a set a fundamental units, so that
$$\mathcal{O}^\times = \langle\zeta\rangle \times \langle\varepsilon_1, \ldots, \varepsilon_r\rangle \simeq C_{2n} \times \mathbf{Z}^r.$$
Then $\mathcal{O}^\times/(\mathcal{O}^\times)^2$ is an abelian group of exponent 2 and rank $r+1$, spanned by the images of $\zeta, \varepsilon_1, \ldots, \varepsilon_r$. Let Ω be the set of all products of these units, each taken at most once, so that Ω is a complete set of representatives for the cosets of $(\mathcal{O}^\times)^2$ in $\mathcal{O}^\times$.

   So far, we know that the quadratic extensions $K(\sqrt{D})$, where $D = \omega D_\mathfrak{d}$, $\omega \in \Omega$ and $\mathfrak{d}$ a square-free ideal supported on S (not both trivial), form a complete list of quadratic extensions of K which are unramified outside $S \cup \{\mathfrak{p} : \mathfrak{p} \mid 2\}$. There are $2^{|S|+r+1} - 1$ of them.

4. For every prime ideal $\mathfrak{p}$ above 2, $\mathfrak{p} \notin S$, keep only the D's from the previous step which reduce to a square in $\mathcal{O}/\mathfrak{p}^{2e(\mathfrak{p}/2)}$.

In particular, this whole discussion, applied to $K = \mathbf{Q}$, yields exactly the familiar description given at the end of Section 5.4.

5.7 Modularity of W_2^7

Consider again the smooth projective quadric $W_2^7 \subseteq \mathbf{P}^6$ of dimension 4 defined over $\mathbf{Q}$ by the equations
$$\sum_{i=1}^{7} x_i = \sum_{i=1}^{7} x_i^3 = 0.$$
Let $V := H^4_{\mathrm{pr}}(W_2^7)$ be its primitive cohomology, considered as a 22-dimensional compatible system of ℓ-adic representations of $\mathrm{Gal}_\mathbf{Q}$, unramified outside $\{3, 5, 7\}$. From Proposition 3.5.1, we know that V decomposes as
$$V = M_{\mathrm{sg}}(V) \otimes W_{\mathrm{sg}} \oplus M_\psi(V) \otimes W_\psi \oplus M_\theta(V) \otimes W_\theta,$$

where ψ, θ are irreducible representations of S_7 of degree 6 and 14, respectively, and

$$\dim M_{\mathrm{sg}}(V) = 2, \qquad \dim M_\psi(V) = \dim M_\theta(V) = 1.$$

Let ρ_{sg}, ρ_ψ and ρ_θ be the three corresponding compatible systems of ℓ-adic Galois representations (cf. Theorem 1.2.2). Note that the formula (4.6) established in Chapter 4 tells us that for every q away from $3, 5$ and 7,

$$\mathrm{tr}(\mathrm{Frob}_q \mid V) = \frac{1}{q^2(q-1)} \sum_{a \in \mathbf{F}_q^\times} \sum_{b \in \mathbf{F}_q} \sum_{x \in \mathbf{F}_q} \exp\left(\frac{2\pi i}{p} \mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}(ax^3 + bx)\right). \tag{5.6}$$

Proposition 5.7.1. *As compatible systems of ℓ-adic representations of $\mathrm{Gal}_{\mathbf{Q}}$, we have*

$$\rho_\theta = \chi_{\mathrm{cycl}}^2 \quad \textit{and} \quad \rho_\psi = \chi_{\mathrm{cycl}}^2 \otimes \varepsilon_5.$$

Moreover, ρ_{sg} is a compatible system with Hodge-Tate weights $(1, 3)$ and

$$\det \rho_{\mathrm{sg}} = \chi_{\mathrm{cycl}}^2 \otimes \varepsilon_{35}.$$

Proof. First, note that any $\mathbf{Q}$-rational system ρ of compatible 1-dimensional representations coming from geometry has to be of the form $\chi_{\mathrm{cycl}}^a \otimes \varepsilon$, where ε is a quadratic character of conductor $N(\rho)$. In particular, ρ has Hodge-Tate weight a. Here, we thus have that $\rho_\theta = \chi_{\mathrm{cycl}}^2 \otimes \varepsilon_\theta$, $\rho_\psi = \chi_{\mathrm{cycl}}^2 \otimes \varepsilon_\psi$, where ε_θ and ε_ψ are quadratic characters of $\mathrm{Gal}_{\mathbf{Q}}$ of conductors dividing $3 \cdot 5 \cdot 7$. We can decide which ones if we are able to compute the values of ε_θ and ε_ψ on sufficiently many Frobenius substitutions. Now for q away from $3, 5$ and 7, we have

$$\begin{aligned} \mathrm{tr}(\mathrm{Frob}_q \mid V) &= \mathrm{tr}\, \rho_{\mathrm{sg}}(\mathrm{Frob}_q) + 6\, \mathrm{tr}\, \rho_\psi(\mathrm{Frob}_q) + 14\, \mathrm{tr}\, \rho_\theta(\mathrm{Frob}_q) \\ &= q\, \mathrm{tr}\, \rho(\mathrm{Frob}_q) + 6\varepsilon_\psi(q)q^2 + 14\varepsilon_\theta(q)q^2, \end{aligned} \tag{5.7}$$

with $|\mathrm{tr}\, \rho_{\mathrm{sg}}(\mathrm{Frob}_q)| \leq 2q^2$ by purity. Since $\varepsilon_\psi(q), \varepsilon_\theta(q) \in \{\pm 1\}$, it turns out by a happy turn of events that we can recover the values of $\mathrm{tr}\, \rho_{\mathrm{sg}}(\mathrm{Frob}_q)$, $\varepsilon_\psi(q)$ and $\varepsilon_\theta(q)$ from the value of $\mathrm{tr}(\mathrm{Frob}_q \mid V)$, which can be computed numerically by (5.6). For example, for $p = 11$, we find that $\mathrm{tr}(\mathrm{Frob}_{11} \mid V) = 2277$, so that

$$\frac{\mathrm{tr}\, \mathrm{Frob}_{11} V}{11^2} = \frac{2277}{121} = 18.\overline{81}.$$

But the only possible values of $\pm 6 \pm 14$ are ± 8 and ± 20, and intervals of radius 2 centered at these values are disjoint. Hence $\varepsilon_\psi(11) = \varepsilon_\theta(11) = 1$, so that

$$\operatorname{tr} \rho(\mathrm{Frob}_{11}) = \frac{1}{11}\left(\operatorname{tr}(\mathrm{Frob}_{11} \mid V) - 6 \cdot 11^2 - 14 \cdot 11^2\right) = -13.$$

Comparing the values tabulated in Table 5.1 with those of the 2^3 quadratic characters of conductor dividing $3 \cdot 5 \cdot 7$, we find that $\varepsilon_\theta = \mathbf{1}$ and $\varepsilon_\psi = \varepsilon_5$.

From the Hodge numbers of W_2^7, we then know that ρ_{sg} has to have Hodge-Tate weights $(1, 3)$, so that $\rho := \chi_{\mathrm{cycl}}^{-1} \otimes \rho_{\mathrm{sg}}$ is a compatible system of 2-dimensional representations with Hodge-Tate weights $(0, 2)$, and whose determinant $\det \rho$ is a 1-dimensional system of Hodge-Tate weight 2, i.e. $\det \rho = \chi_{\mathrm{cycl}}^2 \otimes \varepsilon$, where ε is a quadratic character of conductor dividing $3 \cdot 5 \cdot 7$. Again from Table 5.1, we may conclude that $\varepsilon = \varepsilon_{35}$. To compute the values of ε, one uses the fact that for σ a 2×2 matrix, we have

$$\det \sigma = \frac{(\operatorname{tr} \sigma)^2 - \operatorname{tr}(\sigma^2)}{2}.$$

Hence it follows that

$$\varepsilon(\mathrm{Frob}_p) = \frac{\operatorname{tr} \rho(\mathrm{Frob}_p)^2 - \operatorname{tr} \rho(\mathrm{Frob}_{p^2})}{2p^2},$$

which can then be evaluated using (5.6). Note that only the needed values were computed because the running time of the computations grow much quicker with p here as the finite field $\mathbf{F}_{p^2}$ is involved, and not just $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ as above. □

Looking at the numerical values of $\operatorname{tr} \rho(\mathrm{Frob}_p)$, we see that they seem to agree perfectly with the Hecke eigenvalues of the newform $f \in S_3(35, \varepsilon_{35})$ labeled 35k3A[2,3]1 (cf. [61]). As mentioned in Example 5.1.9, this is compatible with the Serre conjectures, although they cannot be used to provide a direct proof that

$$\rho \simeq \rho_f.$$

Our goal here is to prove this equivalence using the generalized Faltings-Serre method applied to the corresponding 2-adic representations. We first have to gain some information about the residual representations.

Proposition 5.7.2. *Let $N_p(g)$ denote the number of roots in $\mathbf{F}_p$ of the polynomial $g(x) = x^3 + 8x^2 + 16x + 10$. For $p > 7$, we have $\operatorname{tr} \rho(\mathrm{Frob}_p) \equiv 1 + N_p(g) \bmod 2$.*

Table 5.1: Numerical values of ε_ψ, ε_θ, ε, ε_3, ε_5, ε_7 and $\operatorname{tr}\rho$

p	ε_ψ	ε_θ	ε	ε_3	ε_5	ε_7	$\operatorname{tr}\rho(\mathrm{Frob}_p) = a_p(f)$
11	1	1	1	−1	1	1	−13
13	−1	1	1	1	−1	−1	−19
17	−1	1	1	−1	−1	−1	29
19	1	1	−1	1	1	−1	0
23	−1	1	−1	−1	−1	1	0
29	1	1	1	−1	1	1	23
31	1	1		1	1	−1	0
37	−1	1		1	−1	1	0
41	1	1		−1	1	−1	0
43	−1	1		1	−1	1	0
47	−1	1		−1	−1	−1	−31
53	−1	1		−1	−1	1	0
59	1	1		−1	1	−1	0
61	1	1		1	1	−1	0
67	−1	1		1	−1	1	0
71	1	1		−1	1	1	2
73	−1	1		1	−1	−1	−34
79	1	1		1	1	1	−157
83	−1	1		−1	−1	−1	86
89	1	1		−1	1	−1	0
97	−1	1		1	−1	−1	149
101	1	1		−1	1	−1	0
103	−1	1		1	−1	−1	−199
107	−1	1		−1	−1	1	0
109	1	1		1	1	1	−97
113	−1	1		−1	−1	1	0
127	−1	1		1	−1	1	0
131	1	1		−1	1	−1	0
137	−1	1		−1	−1	1	0
139	1	1		1	1	−1	0
149	1	1		−1	1	1	−262
151	1	1		1	1	1	−13
157	−1	1		1	−1	−1	134

Proof. Consider the following 2-Sylow subgroup of S_7:

$$H := \langle (12), (34), (56), (3546) \rangle = \langle (12) \rangle \times \langle (34), (56), (3546) \rangle.$$

Using (3.5) and the explicit parametrizations of Proposition 3.2.5, the fixed locus of H acting on $\mathbf{P}^6$ can be seen to be equal to $A \cup B$ with

$$\begin{aligned} A &= \{(1 : -1 : 0 : 0 : 0 : 0 : 0), (0 : 0 : 1 : 1 : -1 : -1 : 0)\}, \\ B &= \{(x : x : y : y : y : y : z) \mid (x : y : z) \in \mathbf{P}^2\}. \end{aligned}$$

Consequently, as $A \subseteq W_2^7$, we find that $\operatorname{Fix} H|_{W_2^7} = A \cup (B \cap W_2^7)$. Now $B \cap W_2^7$ is isomorphic to subvariety in $\mathbf{P}^2$ defined by the two equations

$$2x + 4y + z = 0, \qquad 2x^3 + 4y^3 + z^3 = 0.$$

Isolating z in the first one and substituting in the second, we find that this is isomorphic to the zero locus in $\mathbf{P}^1$ of

$$2x^3 + 4y^3 + (-2x - 4y)^3 = -6(x^3 + 8x^2y + 16xy^2 + 10y^3).$$

Away from 2 and 3, this is isomorphic with the subset of the affine line

$$C := \{x \in \mathbf{A}^1 \mid g(x) = 0\}.$$

If $p > 3$ is a prime, we thus have

$$|W_2^7(\mathbf{F}_p)^H| = |A(\mathbf{F}_p)| + |C(\mathbf{F}_p)| = 2 + |C(\mathbf{F}_p)| = 2 + N_p(g),$$

so that the orbit-stabilizer formula applied to the action of H on $W_2^7(\mathbf{F}_p)$ yields

$$|W_2^7(\mathbf{F}_p)| \equiv |W_2^7(\mathbf{F}_p)^H| \equiv N_p(g) \bmod 2.$$

On the other hand, combining equations (4.5) and (5.7), we get

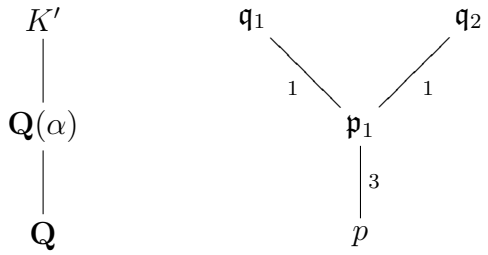
$$|W_2^7(\mathbf{F}_p)| = 1 + p + p^2 + p^3 + p^4 + p \operatorname{tr} \rho(\mathrm{Frob}_p) + 6\varepsilon_\psi(p)p^2 + 14\varepsilon_\theta(p)p^2,$$

so that $|W_2^7(\mathbf{F}_p)| \equiv 1 + \operatorname{tr} \rho(\mathrm{Frob}_p) \bmod 2$, hence the conclusion follows. □

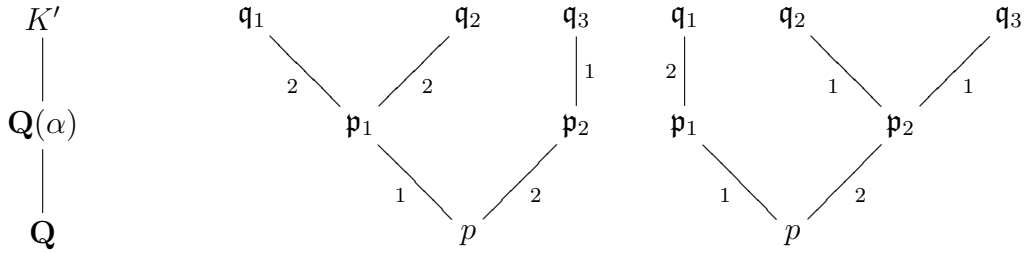
Corollary 5.7.3. *Let $\overline{\rho}_2 : \mathrm{Gal}_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_2)$ denote the residual representation of the 2-adic representation ρ_2. The Galois extension K of $\mathbf{Q}$ cut out by the closed subgroup $\mathrm{Ker}\,\overline{\rho}_2$ of $\mathrm{Gal}_{\mathbf{Q}}$ is the splitting field of the polynomial $x^3 + 2x - 2$.*

Proof. Let $K' = \mathbf{Q}(g)$ be the splitting field of the polynomial from Proposition 5.7.2. Since the discriminant of g is -140, we find that K' is an S_3-extension of $\mathbf{Q}$, unramified outside 2, 5 and 7. If α is a root of g, PARI tells us that $\mathbf{Z}[\alpha]$ is the whole integer ring of $\mathbf{Q}(\alpha)$. For p an unramified prime in K', consider the number of roots of g in $\mathbf{F}_p$.

1. If g has no roots, then it remains irreducible over $\mathbf{F}_p$, so that there is only one prime $\mathfrak{p}$ above p in $\mathbf{Q}(\alpha)$, of residual degree 3. Then, since S_3 contains no element of order 6, p has to split in K', so the decomposition of p in K' is $\mathfrak{q}_1\mathfrak{q}_2$ with $f(\mathfrak{q}_i/p) = 3$. This means that the order of $\mathrm{Frob}(\mathfrak{q}/p)$ in $\mathrm{Gal}(K'/\mathbf{Q})$ is 3.



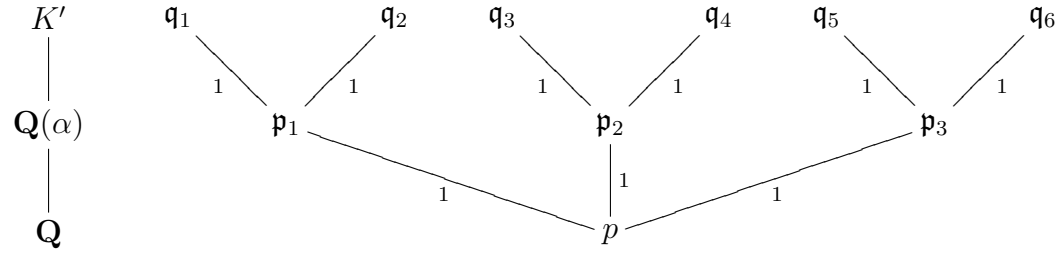
2. If g has exactly one root, then p decomposes as $\mathfrak{p}_1\mathfrak{p}_2$ in $K(\alpha)$, with $f(\mathfrak{p}_1/p) = 1$ and $f(\mathfrak{p}_2/p) = 2$. The two possibilities of decompositions for $\mathfrak{p}_1$ and $\mathfrak{p}_2$ in K' are illustrated below; in both cases we find that the total residual index of p is 2.



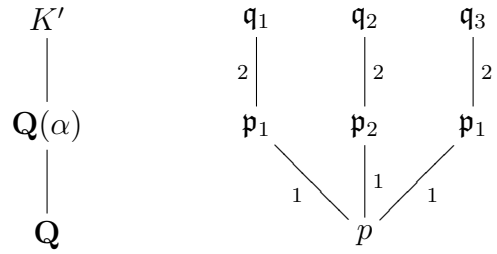
Then $\mathfrak{p}_1$ has to be inert in K', while $\mathfrak{p}_2$ splits, so that the total residual index of Frob_p in $\mathrm{Gal}(K'/\mathbf{Q})$ is 2.

3. If g has 3 roots in $\mathbf{F}_p$, then p is totally split in $\mathbf{Q}(\alpha)$. Then either these primes

above p are themselves split in K', in which case p is totally split in K',



or they stay inert, in which case p has residual degree 2.



These observations are summarized in the following table, in which $f_{K'}(p)$ denotes the residual index of an unramified prime p in K'.

$N_p(g)$	0	1	3
$f_{K'}(p)$	3	2	1 or 2

Using Proposition 5.7.2, we observe that for $p > 7$,

$$\begin{aligned} f_{K'}(p) = 3 &\iff N_p(g) \equiv 0 \bmod 2 \\ &\iff \operatorname{tr} \rho(\mathrm{Frob}_p) \equiv 1 \bmod 2 \\ &\iff f_K(p) = 3, \end{aligned} \tag{5.8}$$

since the elements with odd trace in $\mathrm{GL}_2(\mathbf{F}_2) \supseteq \mathrm{Gal}(K/\mathbf{Q})$ are exactly those of order 3. Let us now proceed to show that this fact implies that $K = K'$.

Indeed, suppose that $K \neq K'$. Then $K \cap K'$ is a proper subfield of K', which is Galois over $\mathbf{Q}$. Thus, either $K \cap K' = \mathbf{Q}$, or $K \cap K'$ is the unique quadratic subfield of K'. In the first case, consider the compositum $K \cdot K'$, which is a Galois extension of $\mathbf{Q}$ with Galois group

$$\mathrm{Gal}(K \cdot K'/\mathbf{Q}) = \mathrm{Gal}(K/\mathbf{Q}) \times \mathrm{Gal}(K'/\mathbf{Q}).$$

By weak Chebotarev, there exists a prime $p > 7$ such that Frob_p restricts to the identity in $\mathrm{Gal}(K/\mathbf{Q})$ and to an element of order 3 in $\mathrm{Gal}(K'/\mathbf{Q})$, contradicting (5.8).

Similarly, if $L := K \cap K'$ is the quadratic subfield of K', we have

$$\mathrm{Gal}(K \cdot K'/\mathbf{Q}) = \mathrm{Gal}(K/\mathbf{Q}) \times_{\mathrm{Gal}(L/\mathbf{Q})} \mathrm{Gal}(K'/\mathbf{Q}).$$

Again, since the restriction $\mathrm{Gal}(K'/\mathbf{Q}) \twoheadrightarrow \mathrm{Gal}(L/\mathbf{Q})$ corresponds to the alternating character of S_3, from weak Chebotarev we can find a prime p such that Frob_p is trivial in $\mathrm{Gal}(K/\mathbf{Q})$ and has order 3 in $\mathrm{Gal}(K'/\mathbf{Q})$. Contradiction.

The proof is thus complete since $K = K' = \mathbf{Q}(g)$ also happens to be the splitting field of the simpler polynomial $x^3 + 2x - 2$. □

The corresponding statement is also true for the representation ρ_f attached to our modular form f.

Proposition 5.7.4. *The Galois extension cut out by* $\mathrm{Ker}\,\overline{\rho}_{f,2}$ *is the* S_3*-extension* K *appearing in Corollary 5.7.3.*

Proof. Since f has level 35, we know that the 2-adic representation $\rho_{f,2}$ is unramified outside $\{2, 5, 7\}$. If K' denotes the number field cut out by $\mathrm{Ker}\,\overline{\rho}_{f,2}$, it is thus a Galois extension of $\mathbf{Q}$, unramified outside $\{2, 5, 7\}$, with Galois group injecting in $\mathrm{GL}_2(\mathbf{F}_2) \simeq S_3$. Looking at Table 5.1, we see that $\mathrm{Gal}(K'/\mathbf{Q})$ must contain an element of order 3 (for example the image of Frob_{11}, which has odd trace).

Now one can explicitly list all cubic extensions L of $\mathbf{Q}$ unramified outside 2, 5 and 7 (see [28]). One of them is of course K itself; for all the others, the following table gives a generating polynomial $h(x)$, the structure of the Galois group, the discriminant Δ of the degree 3 extension generated by a root of $h(x)$, and the smallest prime $p > 7$ for which Frob_p has order 3 in exactly one of $\mathrm{Gal}(K'/\mathbf{Q})$ and $\mathrm{Gal}(L/\mathbf{Q})$, thus proving that $K' \neq L$ (see the Appendix for the implementation).

$h(x)$	$\mathrm{Gal}(L/\mathbf{Q})$	Δ	p
$x^3 - x^2 - 2x + 1$	C_3	7^2	13
$x^3 - x^2 + 2x + 2$	S_3	$-2^3 \cdot 5^2$	13
$x^3 - x^2 + 2x - 3$	S_3	$-5^2 \cdot 7$	13
$x^3 - x^2 + 5x - 13$	S_3	$-2^2 \cdot 5 \cdot 7^2$	11
$x^3 - x^2 + 5x + 15$	S_3	$-2^3 \cdot 5 \cdot 7^2$	17
$x^3 - x^2 - 23x - 13$	S_3	$2^3 \cdot 5^2 \cdot 7^2$	11

Hence the only remaining possibility is that $K' = K$. □

Note that the same "brute force" approach could have been used in the proof of Corollary 5.7.3 to identify the extension corresponding to $\operatorname{Ker}\overline{\rho}_2$ instead of invoking Proposition 5.7.2. However, ρ is not yet known to be unramified at 3, so we have to pinpoint K inside a bigger list of extensions. Fortunately the list of cubic extensions unramified outside $\{2, 3, 5, 7\}$ can also be found in [28] – there are 4 of them with Galois group C_3 and 104 of them with full S_3. Given that list, it is still a very straightforward task to eliminate all these number fields except K using the method given in the Appendix (one finds that biggest prime which is needed is $p = 29$).

We can now turn to the task of computing a suitable sufficient set of primes.

Proposition 5.7.5. *The set* $T = \{11, 13, 19, 23, 31, 47, 97\}$ *is* (K, S)*-sufficient.*

Proof. According to Definition 5.5.14, the requirement on T is two-fold.

- We first need to find a set of primes T_1, disjoint from S, such that for every quadratic extension L of K unramified outside S, there exists a prime $p \in T_1$ such that Frob_p has order 6 in $\mathrm{Gal}(L/\mathbf{Q})$.

  Such an extension L can be described as the compositum of K and a quadratic extension L' of $\mathbf{Q}$ unramified outside S, and linearly disjoint from K. We then have

  $$\mathrm{Gal}(L/\mathbf{Q}) = \mathrm{Gal}(L'/\mathbf{Q}) \times \mathrm{Gal}(K/\mathbf{Q}),$$

  and we are looking for primes such that Frob_p has order 3 in $\mathrm{Gal}(K/\mathbf{Q})$ and is non-trivial in $\mathrm{Gal}(L'/\mathbf{Q})$.

  By the discussion at the end of Section 5.4, quadratic number fields unramified outside S are the $\mathbf{Q}(\sqrt{d})$ with d a square-free element in $\langle -1, 2, -3, 5, -7\rangle$. Since the discriminant of K is $\Delta = -2^2 \cdot 5 \cdot 7$, we see that the unique quadratic subextension of K is $\mathbf{Q}(\sqrt{\Delta}) = \mathbf{Q}(\sqrt{-35})$. It follows that -35 is a square in $K^\times$, so that 5 and -7 are equal in $K^\times/(K^\times)^2$. Thus the quadratic extensions we are looking for are obtained by adjoining a square root of a non-square $d \in \langle -1, 2, -3, 5\rangle$.

  For $d \in \{-1, 2, -3, 5\}$, let ε_d be the quadratic character, associated to $\mathbf{Q}(\sqrt{d})$, i.e. for unramified primes p,

  $$\varepsilon_{-1}(p) = \begin{cases} 0 & \text{if } p \equiv 1 \bmod 4, \\ 1 & \text{if } p \equiv -1 \bmod 4, \end{cases}$$

$$\varepsilon_2(p) = \begin{cases} 0 & \text{if } p \equiv \pm 1 \bmod 8, \\ 1 & \text{if } p \equiv \pm 3 \bmod 8, \end{cases}$$

and ε_{-3}, ε_5 are the Legendre symbols $(\frac{\cdot}{3})$, $(\frac{\cdot}{5})$, written additively.

Consider the following table for the first few primes $p > 7$ and such that Frob_p has order 3 in $\mathrm{Gal}(K/\mathbf{Q})$.

p	11	13	17	29	47	79	97
ε_{-1}	1	1	0	1	0	0	0
ε_2	1	1	0	1	1	1	0
ε_{-3}	1	0	1	1	1	0	0
ε_5	0	1	1	0	1	0	1

By standard linear algebra, we find that the images of 11, 13, 47 and 97 form a basis of the Galois group of the Kummer extension of $\mathbf{Q}$ corresponding to $B = \langle -1, 2, -3, 5\rangle$. It follows that we can take $T_1 = \{11, 13, 47, 97\}$.

- We also want a set T_2, disjoint from S, such that for every V_4-extension L of K unramified outside the primes above S, there exists a prime $p \in T_2$ such that Frob_p has order 4 in $\mathrm{Gal}(L/\mathbf{Q})$.

  For L such an extension, we have a short exact sequence

$$1 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/\mathbf{Q}) \longrightarrow \mathrm{Gal}(K/\mathbf{Q}) \longrightarrow 1, \tag{5.9}$$

  in which the action of $\mathrm{Gal}(K/\mathbf{Q}) \simeq S_3$ by conjugation on $\mathrm{Gal}(L/K)$ is the standard V_4 action. By the Kummer correspondence discussed in Section 5.4, $L = K(\sqrt{B})$, where B is a subgroup of $K^\times/(K^\times)^2$, supported on S, stable under the action of $\mathrm{Gal}(K/\mathbf{Q})$, and for which this action is the standard V_4 action.

  As explained in the Appendix, there are 7 such subgroups B, hence 7 corresponding extensions $L = K(\sqrt{B})$ to consider. It turns out that the set $T_2 = \{19, 23, 31\}$ is sufficient to yield an element of order 4 in each of their Galois groups.

Clearly the set $T = T_1 \cup T_2$ is (K, S)-sufficient. □

Remark. All 2-dimensional 2-adic representations having residual extension K are residually absolutely irreducible, and are up to conjugation residually equal. We could

thus also have used Serre's original quartic fields method described in Section 5.3. This might in theory yield a smaller set of sufficient primes, since we only need to consider the V_4-extensions L/K for which the short exact sequence (5.9) *splits*. However, if one does not want to bother deciding whether the short exact sequences corresponding to the list of possible extensions L are split or not, then surely taking them all into account does not hurt; this is exactly what our implementation of Faltings-Serre does.

According to Theorem 5.5.15, this means that

$$\rho \simeq \rho_f \iff \operatorname{tr}\rho(\mathrm{Frob}_p) = a_f(p) \text{ for } p \in \{11, 13, 19, 23, 31, 47, 97\},$$

and a glance at Table 5.1 tells us that this is indeed the case.

Corollary 5.7.6. *The compatible systems of Galois representations ρ and ρ_f are isomorphic.*

We can summarize everything we learned about the Galois module structure of the cohomology of W_2^7 in the following theorem.

Theorem 5.7.7. *The Hasse-Weil zeta function of W_2^7 factors as*

$$\zeta(W_2^7, s) = \zeta(s)\zeta(s+1)\zeta(s+2)^{15}L(\varepsilon_5, s+2)^6 L(f, s+1)\zeta(s+3)\zeta(s+4),$$

where $f \in S_3(35, \varepsilon_{35})$ is the newform $35k3A[2,3]1$.

Conclusion

In the previous pages, some of the many interactions between different parts of arithmetic geometry were explored. One could say the main object of study in this thesis were the hypersurfaces

$$W_\ell^{m,n}, \quad \ell \text{ prime.}$$

When $W_\ell^{m,n}$ is smooth, it is actually a special hypersurface of type II (in the language of Chapter 3) with respect to the Young subgroup $G := S_m \times S_n$ of S_{m+n}; as such, the character of the representation of G on its primitive cohomology is obtained as the restriction to G of the type II character of S_{m+n} from Theorem 3.2.14. Consequently, the Galois representation on its primitive cohomology decomposes into compatible systems of smaller dimension on the G-isotypic components according to Theorem 3.1.4, and proving its modularity should be easier than for a general hypersurface of degree ℓ and dimension $m+n-3$. Some variation on the Faltings-Serre method described in Chapter 5 could be use to prove numerically such sporadic modularity statements. On the other hand, $W_\ell^{m,n}$ can be considered as a "generating variety" for the average moments of the normalized exponential sums considered in Chapter 4, and we have seen (Theorem 4.4.7) that the limit distribution of these exponential sums is controlled by the subprimitive cohomology of the desingularization $\widetilde{W}_\ell^{m,n}$. This limit distribution might be studied from a different point of view using the theory developed in [30], in which equidistribution of exponential sums is interpreted as the shadow of equidistribution of operators with respect to the Haar measure on some associated topological group G_{geom}.

Several issues raised in this thesis beg for future investigation.

The character formulae of Proposition 3.2.14, for example, as well as the related class function θ'_ℓ discussed in Section 3.3, seem to warrant a more thorough examination in terms of combinatorics and representation theory of the symmetric group. The class functions $m_d, d \geq 1$, counting the number of disjoint cycles in a permutation whose lengths are divisible by d, do not seem to have attracted much attention before

despite the natural fashion in which they appeared in Chapter 3. The author of this thesis tried unsuccessfully to find in the literature identities in which they appear in order to compute inner products of the primitive character of special symmetric hypersurfaces with other irreducible representations, such as the alternating character. The application of these representation-theoretical considerations to the existence of special hypersurfaces for S_n or related groups seems an interesting problem to look at in more detail.

From the geometrical point of view, our treatment of ramification for Galois representations coming from geometry was fairly crude in that we only used the smooth base change theorem to assert that a prime of good reduction for the variety was unramified for the representation. However, it is known that all smooth proper varieties are potentially semistable, i.e. become semistable after a finite extension of the base field, and the semistable base change theorem may be used to gain more precise information about ramified primes using the machinery of vanishing cycles. It was also remarked in our discussion of the Serre conjecture (Section 5.1) that being able to compute the Artin conductor of representations coming from geometry in terms of geometrical data would be of great interest. This raises several practical questions. Given equations for a variety, how does one find a semistable model (after eventual base change)? Except for curves, not much seems to been known. Perhaps de Jong's theory of alterations [10], which seem more computationally accessible than semistable models, could be used to gain some insight into the cohomology of the original variety; this is a direction to explore. On the other hand, even if one is given an explicit semistable model for a variety, how does one proceed to extract from it information about the Galois representation on cohomology? This fits in a general theme of reading information about the Galois representation from the geometry. The converse is interesting as well; for example, the compatible system of representations on the cohomology of W_2^7 was seen in Section 5.7 to be unramified outside 5 and 7, even though it is not clear if it admits a model with good reduction at 3.

A major occupation of arithmetic geometry, especially in recent years, is that of actually computing the number of points on varieties over finite fields, i.e. computing their zeta function. Algorithms to do this exists (see e.g. [37, 2]), but are mostly useful in practice only for curves of low genera or over finite fields of small characteristic. In this regard, it is a fortunate feature of the varieties $W_\ell^{m,n}$ that their number of points over finite fields can be easily computed by taking advantage of their relationship to the average moments of exponential sums (Theorem 4.3.2), for which the dependence

on the dimension $m+n-3$ is mostly innocuous. It is this author's hope that similar "happy incidents" could occur for other varieties with a large automorphism group.

Moreover, as seen in Section 5.7, the computations performed to recover the traces of Frobenius on the different isotypic components were possible because the dimensions of the irreducible representations of the automorphism group that arise were suitably well spaced relative to each other, so that in the sum of traces the individual traces could be separated using purity. It would be interesting to seek other instances of this phenomenon and to see if it could be suitably formalized.

However, the most promising direction of research in this writer's mind lies in future extensions of the Faltings-Serre method. The treatment of Chapter 5 lends itself nicely to generalization and application to other cases than 2-dimensional 2-adic representations of $\mathrm{Gal}_{\mathbf{Q}}$, and as such will be helpful to prove explicitly cases of modularity in situations for which no general result is currently known. For example, suitable rank 2 motives over a totally real field F are expected to arise in connection with Hilbert modular forms. In this regard, the 2-dimensional compatible system of representations of $\mathrm{Gal}_{\mathbf{Q}(\sqrt{5})}$ on the cohomology of the quintic threefold studied in [8] seems an ideal test example.

Appendix

Here we provide a description of how certain computations of Section 5.7 were implemented in PARI. Note that we make no claim regarding the efficiency of these implementations. To avoid any problems we first explicitly declare the precedence order of the variables we will use.

```
x; y; z; t;
```

Distinguishing cubic extensions

If L is a number field (as produced by `nfinit`), and p a prime number, the following function outputs the residual degree of *one* of the primes above p in L.

```
resindex(L,p) = idealprimedec(L,p)[1][4]
```

Let L be a number field such that the Galois group of its normal closure L^{c} injects in S_3 (let us call this a *weak S_3-extension*). For p an unramified prime in L, the considerations on prime decompositions in the proof of Corollary 5.7.3 tell us that Frob_p has order 3 in $\mathrm{Gal}(L^{\mathrm{c}}/\mathbf{Q})$ if and only if p has residual index 3 in L. Consequently, the following function computes the trace of Frob_p viewed as an element in $\mathrm{GL}_2(\mathbf{F}_2) \simeq S_3$.

```
trmod2(L,p) = (resindex(L,p) == 3)
```

Let L_1 and L_2 be two weak S_3-extensions unramified for $p > N$ and such that one of them has degree at least 3. If $L_1^{\mathrm{c}} \neq L_2^{\mathrm{c}}$, the weak Chebotarev argument used in the proof of Corollary 5.7.3 shows that there exists a prime $p > N$ such that Frob_p has order 3 in exactly one of $\mathrm{Gal}(L_1^{\mathrm{c}}/\mathbf{Q})$ or $\mathrm{Gal}(L_1^{\mathrm{c}}/\mathbf{Q})$. The following function produces the first such "certificate of difference" $p < 10^5$, if it exists.

```
smallestp(L1, L2, N) = {
 forprime(p = N + 1, 10^5,
  if(trmod2(L1, p) != trmod2(L2, p), return(p))
 )
}
```

For example, the following code outputs the table of Proposition 5.7.4, the defining polynomials being found in [28].

```
{ pols = [ t^3 - t^2 - 2*t + 1,
           t^3 - t^2 + 2*t + 2,
           t^3 - t^2 + 2*t - 3,
           t^3 - t^2 + 5*t - 13,
           t^3 - t^2 + 5*t + 15,
           t^3 - t^2 - 23*t - 13 ];

  K0 = nfinit(t^3 + 2*t + 2);

  for(i = 1, length(pols),
   L = nfinit(pols[i]);
   print( "L", i, ": ", polgalois(L.pol)[4], " ",
    factor(L.disc), " ", smallestp(L,K0,7) )
  )
}
```

Enumerating V_4-extensions

Our field K from Section 5.7 is the normal closure of the degree 3 number field K_0 appearing above. Since the discriminant of K_0 is $\Delta = -140$, we find that $K = K_0(\sqrt{\Delta}) = K_0(\sqrt{-35})$. We initialize K to a `bnf` object since to follow the strategy outlined in Section 5.6 we will need to compute with its units and class group.

```
K = nfinit(rnfequation(K0, z^2+35),2);
K = bnfinit(K);
bnfcertify(K) \\ 1
```

We first investigate how the primes in $S = \{2, 3, 5, 7\}$ decompose in K.

```
P = idealprimedec(K,2);
Q = idealprimedec(K,3);
R = idealprimedec(K,5);
S = idealprimedec(K,7);
```

We find that

$$(2) = \mathfrak{p}_1^3,\ (3) = \mathfrak{q}_1\mathfrak{q}_2,\ (5) = (\mathfrak{r}_1\mathfrak{r}_2\mathfrak{r}_3)^2,\ (7) = (\mathfrak{s}_1\mathfrak{s}_2\mathfrak{s}_3)^2,$$

hence the subgroup of $\mathcal{I}/\mathcal{I}^2$ supported on S is $\langle \mathfrak{p}_1, \mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{s}_1, \mathfrak{s}_2, \mathfrak{s}_3\rangle$. By Proposition 5.6.2, the elements of this subgroup which come from $\mathcal{P}/\mathcal{P}^2$ are those whose image is trivial in $\mathcal{C}\ell/\mathcal{C}\ell^2$.

The class number of K is seen to be 2; let $\mathfrak{a}$ be an ideal generating its class group, and $a \in K^\times$ such that $\mathfrak{a}^2 = (a)$.

```
A = K.clgp.gen[1];
a = bnfisprincipal(K,idealpow(K,A,2))[2];
```

The prime $\mathfrak{p}_1$ above 2 is principal, since its order in the class group has to be divisible by 3. The primes above 3, 5 and 7 are seen to be non-principal, hence we can write them as $(x)\mathfrak{a}$ for some $x \in K^\times$.

```
p = bnfisprincipal(K, P[1])[2];
q = vector(2, i, bnfisprincipal(K, Q[i])[2]);
r = vector(3, i, bnfisprincipal(K, R[i])[2]);
s = vector(3, i, bnfisprincipal(K, S[i])[2]);
```

We now have $\mathfrak{p}_1 = (p),\ \mathfrak{q}_i = (q_i)\mathfrak{a},\ \mathfrak{r}_i = (r_i)\mathfrak{a},\ \mathfrak{s}_i = (s_i)\mathfrak{a}$. Conveniently, it turns out that the generator $\mathfrak{a}$ for the class group that PARI chose was $\mathfrak{s}_1$, so that $s_1 = 1$.

Accordingly, we find that the subgroup of elements of $\mathcal{I}/\mathcal{I}^2$ supported on S that lift to $\mathcal{P}/\mathcal{P}^2$ is

$$\langle \mathfrak{p}_1, \mathfrak{q}_1/\mathfrak{a}, \mathfrak{q}_2/\mathfrak{a}, \mathfrak{r}_1/\mathfrak{a}, \mathfrak{r}_2/\mathfrak{a}, \mathfrak{s}_2/\mathfrak{a}, \mathfrak{s}_3/\mathfrak{a}\rangle,$$

and the subgroup of possible lifts in $\mathcal{P}/\mathcal{P}^2$ is

$$\langle (a), (p), (q_1), (q_2), (r_1), (r_2), (r_3), (s_2), (s_3)\rangle,$$

since the kernel of the reduction map is the image of the map $\mathcal{C}\ell \to \mathcal{P}/\mathcal{P}^2$ which sends $[\mathfrak{a}]$ to (a) by Proposition 5.6.2.

It follows that the subgroup $\mathcal{B}$ of $K^\times/(K^\times)^2$ corresponding to exponent 2 extensions of K unramified outside S is

$$\mathcal{B} = \mathcal{O}^\times/(\mathcal{O}^\times)^2 \times \langle a, p, q_1, q_2, r_1, r_2, r_3, s_2, s_3\rangle.$$

Here $\mathcal{O}^\times$ has rank 2, and $\mathcal{O}^\times = \langle -1\rangle \times \langle \varepsilon_2, \varepsilon_3\rangle$. Hence $\mathcal{B}$, as a vector space over $\mathbf{F}_2$, has a basis consisting of

$$\{-1, \varepsilon_2, \varepsilon_3, a, p, q_1, q_2, r_1, r_2, r_3, s_2, s_3\}.$$

```
eps = K.tufu;
gen = concat(eps, [a, p, q[1], q[2], r[1], r[2], r[3], s[2], s[3]]);
gen = nfbasistoalg(K, gen);
```

We now explicitly compute representatives in $K^\times$ for the 2^{12} elements of $\mathcal{B}$.

```
drop(list) = if(length(list) <= 1, [], vecextract(list, "2.."))

products(list) = {
 if(list == [], [1],
  tmp = products(drop(list)); concat(tmp, list[1]*tmp)
 )
}

repr = products(gen);
```

To find all the subgroups $B \subset \mathcal{B}$ which are isomorphic to V_4 as an $\mathbf{F}_2[S_3]$-module, we need to be able to decide when two elements of $K^\times$ are equal in $K^\times/(K^\times)^2$.

```
sqroot(d) = {

 fact = idealfactor(K, d);

 id = 1;
 for(i = 1, matsize(fact)[1],
  if(fact[i,2] % 2 != 0, return(0),
   id = idealmul(K, id, idealpow(K, fact[i,1], fact[i,2]/2))
```

```
  )
 );

 \\ now (d) = id^2
 fact = bnfisprincipal(K,id);
 if(fact[1] == [1]~, return(0), rac = fact[2]);

 \\ now (d) = (rac)^2, d = u*rac^2
 u = nfeltdiv(K, d, nfeltpow(K, rac, 2));
 fact = bnfisunit(K, u);
 if(fact[3] == Mod(1,2), return(0)); \\ sign

 v = 1;
 for(i=1, 2,
  if(fact[i] % 2 != 0, return(0),
   v = v * K.fu[i]^(fact[i]/2);
  )
 );

 \\ now x = v^2 rac^2
 nfeltmul(K, v, rac)

}
```

For $x, y \in K^\times$, the following function returns an element z such that $x = z^2 y$ if it exists; else it returns 0.

```
congmodsquares(x,y) = sqroot(nfeltdiv(K,x,y))
```

By computing their iterates on the primitive element of K we identify the three transpositions in $G = \mathrm{Gal}(K/\mathbf{Q}) \simeq S_3$.

```
ord(g) = {
 pow = Mod(g, K.pol); id = Mod(z, K.pol); n = 1;
 while(pow != id, pow = nfgaloisapply(K,g,pow); n++);
 return(n)
}
```

```
G = nfgaloisconj(K);

tau = [];
for(i = 1, length(G), if(ord(G[i]) == 2, tau = concat(tau, [G[i]])))
```

We now search for all the subgroups B of type V_4. They are the subsets of $\mathcal{B}$ of the form $\{1, \alpha, \beta, \gamma\}$, where $\{\alpha, \beta, \gamma\}$ is an orbit for the action of G on $K^\times/(K^\times)^2$ such that $\alpha \cdot \beta = \gamma$.

```
{ list = [];

  for(i = 1, length(repr), alpha = repr[i];

   \\ check if we already found a B containing alpha
   found = 0;
   for(j = 1, length(list), for(k = 1, 3,
    if(congmodsquares(alpha, list[j][k]), found = 1)
   ) );
   if(found, next);

   \\ looks for transpositions fixing alpha
   compt = 0;
   for(j = 1, 3,
     if( congmodsquares(alpha, nfgaloisapply(K, tau[j], alpha)),
     compt++; fix = j
    )
   );

   \\ |Orb| = 3 iff Stab contains a unique transposition
   if( compt != 1, next );

   \\ let tau[j], tau[k] be the two others
   if( fix == 1, j = 2; k = 3 );
   if( fix == 2, j = 1; k = 3 );
   if( fix == 3, j = 1; k = 2 );
```

```
   beta = nfgaloisapply(K, tau[j], alpha);
   gama = nfgaloisapply(K, tau[k], alpha);  \\ sic

   \\ if alpha*beta = gama we found a new B
   if( congmodsquares(nfeltmul(K, alpha, beta), gama),
    list = concat(list, [[alpha, beta, gama]])
   )

 );

}
```

Now `list` contains 7 triples corresponding to the subgroups B of $\mathcal{B}$ of type V_4, as claimed in the proof of Proposition 5.7.5. For every corresponding extension L, we look for a prime $p > 7$ such that Frob_p has order 4 in $\mathrm{Gal}(L/\mathbf{Q})$.

```
smallestP(L, N) = {
 forprime(p = N + 1, 10^5, if(resindex(L,p) == 4, return(p)))
}

{ for(i = 1, length(list),

  B = 49*list[i]; \\ for some reason PARI complains without the 49
  alpha = B[1];
  F = rnfinit(K, y^2 - alpha);  \\ intermediate extension
  beta = rnfeltup(F, B[2]);
  F = nfinit(F.pol);

  L = nfinit(rnfequation(F, x^2 - beta));
  print("L", i, ": ", smallestP(L,7))

) }
```

We find $19, 23$ and 31, as claimed in the proof of Proposition 5.7.5.

Bibliography

[1] J. Achter. Detecting complex multiplication. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 38–50. World Sci. Publ., Hackensack, NJ, 2005.

[2] L. Adleman and M.-D. Huang. Counting points on curves and abelian varieties over finite fields. *Symbolic Comput.*, 32(3):171–189, 2001.

[3] M. Atiyah and I. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co.

[4] B. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 43:57–60, 1968.

[5] N. Bourbaki. *Algèbre commutative, chapitre 8: dimension*. Masson, Paris, 1983.

[6] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[7] H. Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[8] C. Consani and J. Scholten. Arithmetic on a quintic threefold. *Internat. J. Math.*, 12(8):943–972, 2001.

[9] J. Conway, R. Curtis, S. Norton, R. Parker, and R. Wilson. *Atlas of finite groups*. Oxford University Press, Eynsham, 1985.

[10] A. de Jong. Smoothness, semi-stability and alterations. *Inst. Hautes Études Sci. Publ. Math.*, (83):51–93, 1996.

[11] P. Deligne. Formes modulaires et représentations ℓ-adiques. In *Séminaire Bourbaki 1968/1969, Exp. 355*, Lecture Notes in Mathematics, Vol. 179. Springer-Verlag, Berlin, 1971.

[12] P. Deligne. Cohomologie des intersections complètes. In *SGA 7: Groupes de monodromie en géométrie algébrique II*, Lecture Notes in Mathematics, Vol. 340. Springer-Verlag, Berlin, 1973.

[13] P. Deligne. La conjecture de Weil. I. *Inst. Hautes études Sci. Publ. Math.*, (43):273–307, 1974.

[14] P. Deligne. *SGA* $4\frac{1}{2}$*: Cohomologie étale*, volume 569 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1977.

[15] P. Deligne. Représentations ℓ-adiques. *Astérisque*, (127):249–255, 1985.

[16] P. Deligne and G. Lusztig. Representations of reductive groups over finite fields. *Ann. of Math. (2)*, 103(1):103–161, 1976.

[17] M. Deuring. On the zeta-function of an elliptic function field with complex multiplications. In *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*. Science Council of Japan, Japan, 1956.

[18] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[19] J.-M. Fontaine and Y. Ouyang. *Theory of p-adic Galois representations*. Springer. In preparation.

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

[21] W. Fulton and J. Harris. *Representation theory, a first course*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.

[22] P. Griffiths and J. Harris. *Principles of algebraic geometry*. Wiley Classics Library. John Wiley & Sons Inc., New York, 1994.

[23] A. Grothendieck. Formule de lefschetz et rationalité des fonctions L. In *Dix exposés sur la cohomologie des schémas*, volume 3 of *Advanced Studies in Pure Mathematics*. North-Holland Publishing Co., Amsterdam, 1968.

[24] R. Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1977.

[25] F. Hirzebruch. *Topological methods in algebraic geometry*. Classics in Mathematics. Springer-Verlag, Berlin, 1995.

[26] K. Hulek, R. Kloosterman, and M. Schütt. Modularity of Calabi-Yau varieties. In *Global aspects of complex geometry*, pages 271–309. Springer, Berlin, 2006.

[27] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[28] J. Jones. Tables of number fields with prescribed ramification, June 2001. `http://math.asu.edu/~jj/numberfields/`.

[29] N. Katz. On a certain class of exponential sums. *J. Reine Angew. Math.*, 377:12–17, 1987.

[30] N. Katz. *Gauss sums, Klossterman sums, and monodromy groups*, volume 116 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1988.

[31] C. Khare. Modularity of Galois representations and motives with good reduction properties. *J. Ramanujan Math. Soc.*, 22(1):75–100, 2007.

[32] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture: the case of odd conductors (I). *Preprint*, 2006.

[33] R. Kiehl and R. Weissauer. *Weil conjectures, perverse sheaves and ℓ-adic Fourier transform*, volume 42 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 2001.

[34] S. Kobayashi. Fixed points of isometries. *Nagoya Math. J.*, 13:63–68, 1958.

[35] N. Korobov. *Exponential sums and their applications*, volume 80 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1992.

[36] J. Lagarias, H. Montgomery, and A. Odlyzko. A bound for the least prime ideal in the Chebotarev density theorem. *Invent. Math.*, 54(3):271–296, 1979.

[37] A. Lauder. Counting solutions to equations in many variables over finite fields. *Found. Comput. Math.*, 4(3):221–267, 2004.

[38] G. Laumon. Exponential sums and ℓ-adic cohomology: a survey. *Israel J. Math.*, 120(part A):225–257, 2000.

[39] R. Livné. The average distribution of cubic exponential sums. *J. Reine Angew. Math.*, 375/376:362–379, 1987.

[40] R. Livné. Cubic exponential sums and Galois representations. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 247–261. Amer. Math. Soc., Providence, RI, 1987.

[41] J.-F. Mestre. Courbes de Weil de conducteur 5077. *C. R. Acad. Sci. Paris Sér. I Math.*, 300(15):509–512, 1985.

[42] J. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[43] J. Milnor. *Singular points of complex hypersurfaces*. Annals of Mathematics Studies, No. 61. Princeton University Press, Princeton, NJ, 1968.

[44] D. Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Bombay, 1970.

[45] R. Murty. Congruences between modular forms. In *Analytic number theory (Kyoto, 1996)*, volume 247 of *London Math. Soc. Lecture Note Ser.*, pages 309–320. Cambridge Univ. Press, Cambridge, 1997.

[46] J. Neukirch. *Class field theory*, volume 280 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1986.

[47] K. Ribet. Report on mod ℓ representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 639–676. Amer. Math. Soc., Providence, RI, 1994.

[48] R. Rodríguez and V. González-Aguilera. Fermat's quartic curve, Klein's curve and the tetrahedron. In *Extremal Riemann surfaces (San Fransisco, 1995)*, volume 201 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 1997.

[49] B. Sagan. *The symmetric group: representations, combinatorial algorithms, and symmetric functions*, volume 203 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001.

[50] C. Schoen. Algebraic cycles on certain desingularized nodal hypersurfaces. *Math. Ann.*, 270(1):17–27, 1985.

[51] A. Scholl. The ℓ-adic representations attached to a certain noncongruence subgroup. *J. Reine Angew. Math.*, 392:1–15, 1988.

[52] J.-P. Serre. Zeta and L functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 82–92. Harper & Row, New York, 1965.

[53] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[54] J.-P. Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, revised edition, 1978.

[55] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[56] J.-P. Serre. Répartition asymptotique des valeurs propres de l'opérateur de Hecke T_p. *J. Amer. Math. Soc.*, 10(1):179–230, 1997.

[57] J.-P. Serre. *Abelian ℓ-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A.K. Peters Ltd., Wellesley, MA, 1998.

[58] J.-P. Serre. Résumé des cours au Collège de France 1984–1985. In *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000.

[59] J. Shohat and J. Tamarkin. *The Problem of Moments*. American Mathematical Society Mathematical surveys, vol. II. American Mathematical Society, New York, 1943.

[60] J. Socrates and D. Whitehouse. Unramified Hilbert modular forms, with examples relating to elliptic curves. *Pacific J. Math.*, 219(2):333–364, 2005.

[61] W. Stein. The modular forms database, 2004. `http://modular.math.washington.edu/Tables/`.

[62] G. Tamme. *Introduction to étale cohomology*. Universitext. Springer-Verlag, Berlin, 1994.

[63] J. Tate. Algebraic cycles and poles of zeta functions. In *Arithmetica Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 93–110. Harper & Row, New York, 1965.

[64] R. Taylor. Galois representations. *Ann. Fac. Sci. Toulouse Math. (6)*, 13(1):73–119, 2004.

[65] R. Taylor and A. Wiles. Ring-theoretic properties of certain hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[66] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

[67] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.