

# DIAGONAL VARIETIES AND MODULAR FORMS

ACADEMISCH PROEFSCHRIFT

TER VERKRIJGING VAN DE GRAAD VAN DOCTOR  
AAN DE UNIVERSITEIT VAN AMSTERDAM  
OP GEZAG VAN DE RECTOR MAGNIFICUS  
PROF. MR. P.F. VAN DER HEIJDEN  
TEN OVERSTAAN VAN EEN DOOR HET COLLEGE  
VOOR PROMOTIES INGESTELDE COMMISSIE,  
IN HET OPENBAAR TE VERDEDIGEN  
IN DE AULA DER UNIVERSITEIT  
OP VRIJDAG 11 MAART 2005, TE 12:00 UUR

DOOR

SIMON KRONEMEIJER

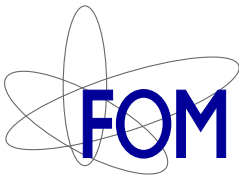
GEBOREN TE KAMPEN

## **Promotiecommissie**

Promotores: Prof. dr. R.H. Dijkgraaf  
Prof. dr. G.B.M. van der Geer

Overige leden: Prof. dr. T. Katsura  
Prof. dr. S.J. Edixhoven  
Prof. dr. E.M. Opdam  
Dr. J. Stienstra  
Dr. B.J.J. Moonen

Faculteit der Natuurwetenschappen, Wiskunde en Informatica



Dit werk maakt deel uit van het onderzoekprogramma van de Stichting voor Fundamenteel Onderzoek der Materie (FOM), die financieel wordt gesteund door de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO).

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	String theory . . . . .	2
1.2	Mirror symmetry . . . . .	3
1.3	Diagonal varieties . . . . .	4
1.4	Outline . . . . .	6
<b>2</b>	<b>Singular Toric Varieties</b>	<b>9</b>
2.1	Definitions . . . . .	9
2.2	Singularities . . . . .	11
2.3	Weighted projective spaces . . . . .	13
2.4	Singularities of diagonal varieties . . . . .	15
2.5	Hodge numbers of diagonal varieties . . . . .	17
<b>3</b>	<b>Combinatorics</b>	<b>21</b>
3.1	Diagonal equations . . . . .	21
3.2	Jacobi sums and Gauss sums . . . . .	22
3.3	The zeta function . . . . .	26
3.4	Weil's formula . . . . .	28
3.5	Zeta functions for all good primes . . . . .	32
3.6	Splitting the cohomology . . . . .	35
3.7	The $p$ -adic Gamma function . . . . .	39
3.8	The Gross-Koblitz formula . . . . .	41
3.9	Behaviour modulo $d$ . . . . .	43
<b>4</b>	<b>The Shioda-Katsura Construction</b>	<b>45</b>
4.1	The Shioda-Katsura maps . . . . .	45
4.2	Cohomological consequences . . . . .	48
<b>5</b>	<b>Modular forms and Galois representations</b>	<b>55</b>
5.1	Modular forms . . . . .	55
5.2	Galois representations . . . . .	58
5.3	Diagonal elliptic curves . . . . .	63

<b>6</b>	<b>Explicit representations</b>	<b>65</b>
6.1	Tensor product representations . . . . .	66
6.2	Representations of dimension 2 . . . . .	69
6.2.1	Representations of weight 1 . . . . .	69
6.2.2	Representations in degree 3 . . . . .	70
6.2.3	Representations in degree 4 . . . . .	72
6.2.4	Representations in degree 6 . . . . .	72
6.2.5	The representation $c = (1, 3, 4)$ . . . . .	73
6.2.6	Representations in degree 12 . . . . .	76
6.3	Zeta functions of varieties . . . . .	78
6.3.1	The Fermat quartic . . . . .	78
6.3.2	Exponents $(2, 6, 6, 6)$ . . . . .	79
6.3.3	Exponents $(3, 3, 6, 6)$ . . . . .	80
6.3.4	A tensor product representation . . . . .	80
6.3.5	A K3 surface of degree 8 . . . . .	82
6.4	Calabi-Yau threefolds . . . . .	84
6.4.1	The Calabi-Yau of degree 6 . . . . .	84
6.4.2	Exponents $(4, 4, 4, 8, 8)$ . . . . .	85
6.4.3	Exponents $(2, 8, 8, 8, 8)$ . . . . .	87
6.4.4	Exponents $(4, 4, 6, 6, 6)$ . . . . .	88
6.4.5	Exponents $(4, 4, 3, 12, 12)$ . . . . .	89
6.4.6	Exponents $(4, 4, 4, 6, 12)$ . . . . .	90
<b>A</b>	<b>Coefficients of modular forms</b>	<b>93</b>
<b>B</b>	<b>Relations for the <math>p</math>-adic Gamma functions</b>	<b>95</b>
	<b>Bibliography</b>	<b>97</b>
	<b>Samenvatting</b>	<b>101</b>
	<b>Dankwoord</b>	<b>103</b>
	<b>Curriculum Vitae</b>	<b>105</b>

# Chapter 1

## Introduction

Around 1990, new developments in theoretical physics caused a stir among mathematicians. Physicists had solved a counting problem in algebraic geometry by using string theory. This was very surprising, since until that time the problem was thought to be very hard and only a few special cases were known. Moreover, the method used was revolutionary and seemed to imply that each variety that can be used to define a string theory (a Calabi-Yau variety) came with a mirror partner that was completely different geometrically, but defined the same physical theory nonetheless. This would mean that many geometric invariants of these varieties were equal after proper translation. Since some of these invariants were almost impossible to calculate on one variety but easy to evaluate on the mirror partner, this promised unanticipated new techniques. Thus the challenge for mathematicians was to find out what was going on from a purely mathematical point of view, to prove the existence of mirror partners and to find a way to construct these.

For this reason Calabi-Yau varieties have become the subject of much recent research. This research mostly focuses on their properties as manifolds over  $\mathbb{C}$ , since in physics other fields are usually disregarded. But one might think that mirror symmetry has an arithmetic or algebraic analogue and that we could learn much from trying to see what mirror symmetry means in this context. If a Calabi-Yau variety is defined over a number field we can obtain a lot of information by studying the reduction of the variety modulo a prime. It is therefore interesting to have examples in which we can describe the arithmetic structure of a Calabi-Yau variety in detail. Unfortunately, few such examples are available.

In this thesis we will study the arithmetic and geometric aspects of diagonal varieties and in particular the Calabi-Yau varieties among them. A diagonal variety  $X$  is the set of projective solutions of a diagonal equation, that is, an equation of the form

$$a_0 X_0^{e_0} + a_1 X_1^{e_1} + \dots + a_n X_n^{e_n} = 0 \tag{1.1}$$

with integral exponents  $e_i$  and nonzero coefficients  $a_i$ . We will show that in a number of examples their cohomology splits into subspaces that are described

entirely by modular forms. This allows us to find the zeta functions of these varieties for all good primes, and they generate the numbers of points of these varieties over all finite fields.

## 1.1 String theory

The development of string theory in the 1980's has led to many new connections between physics and algebraic geometry. By that time it was clear to theoretical physicists that quantum mechanics and general relativity would be all but impossible to unite in a quantum field theory. On the other hand both theories gave excellent results in their regime of applicability. Countless astronomical measurements had confirmed general relativity, while quantum field theory had been confirmed to great precision by experiments in high energy physics. However, any attempt to unite these theories failed due to renormalisation problems; the hypothetical gravity particles interacted too strongly with one another and produced an infinite gravitational field. The aim of string theory was to unite all forces and particles into one consistent theory, that would have both general relativity and quantum field theory as limiting cases.

String theory replaced the point particle by a small 1-dimensional string, sweeping out a smooth surface in space-time. The interactions between particles became just the joining and separating of strings. As Figure 1.1 shows this can be done in a smooth way. In this way the interaction vertices from quantum field theory (which caused all kinds of divergences) were avoided. General relativity was found to be a natural consequence of these assumptions, which was a great success.

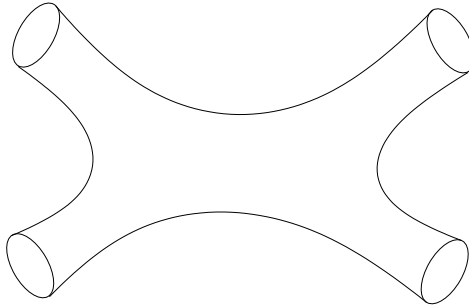


Figure 1.1: Two strings joining and separating sweep out a smooth surface in space-time.

However, string theory came with new problems of its own. The most striking of these was the fact that it was consistent only in 10 dimensions —at least, if it respected various symmetries like Lorentz and reparametrisation invariance. The solution to this problem was to replace the relativistic 4-dimensional space-time  $M_4$  by a direct product  $M_4 \times X$ , with  $X$  a very small (and hence unobserved)

compact manifold of real dimension 6. String theory put severe restrictions on the properties of  $X$ , in particular that it allow a Ricci-flat metric; this is the metric that describes relativistic space-time in regions where no mass is present.

These restrictions connected string theory to algebraic geometry, where such manifolds had been studied as well. Calabi had conjectured that a manifold  $X$  of real dimension 6 would allow a Ricci-flat metric if and only if  $X$  would be a complex Kähler variety with a trivial canonical bundle. Yau proved this in the 1970's. In this way the physical notion of Ricci-flatness was translated directly into constraints on well-known attributes of algebraic varieties. In honour of their work, such varieties were named Calabi-Yau varieties. The string moving in space as in Figure 1.1 can then be reinterpreted as a map embedding a Riemann surface  $\Sigma$  with some special points into  $X$ .

As a consequence of quantum mechanics, correlation functions in string theory are generally calculated by integrating an action functional over all such maps. Mathematically this is not possible, since the space to be integrated over is not measurable. But for some correlation functions (called topological correlation functions) the action functional depends only on the topology of the embedding. In those cases we need only sum over all different homotopy classes of maps  $\Sigma \rightarrow X$ , which is a problem that can be formulated mathematically. For this reason physicists and mathematicians became interested in the problem of counting the number of rational curves of a fixed degree lying on a Calabi-Yau variety.

For some varieties and low degrees this could be solved by ordinary mathematical methods, but in general the problem was found to be very hard. However, around 1990 theoretical physicists announced that they had found a formula that solved an instance of this problem for all degrees by using mirror symmetry. The variety they considered was a general member of the family of varieties given by the equation

$$X_0^5 + X_1^5 + X_2^5 + X_3^5 + X_4^5 + 5\psi X_0 X_1 X_2 X_3 X_4 = 0, \quad (1.2)$$

where  $\psi$  is a parameter. This family contains a diagonal fiber  $\psi = 0$ , which is a singular point of the family and plays a special role in the physical model connected to the variety.

## 1.2 Mirror symmetry

In string theory many physical quantities could be reinterpreted as mathematical objects associated to the Calabi-Yau variety  $X$ . In particular two operators in the superconformal algebra (which is the algebra associated to a symmetry under holomorphic reparametrisations of the string) could be identified with infinitesimal deformations of the Calabi-Yau variety. One of these was associated to deformations of the complex structure of the Calabi-Yau, which geometrically correspond to the space  $H^{2,1}(X, \mathbb{C})$ ; the other to deformations of the Kähler metric, which correspond to  $H^{1,1}(X, \mathbb{C})$ . These are very different objects in geometry; however, the corresponding operators in string theory differed only in the choice of a sign, which was just a matter of convention.

To resolve this asymmetry, it was conjectured that Calabi-Yau varieties would come in pairs  $(X, Y)$  such that both would correspond to the same superconformal string theory, but with the deformation spaces exchanged; so in particular  $h^{2,1}(X) = h^{1,1}(Y)$  and  $h^{1,1}(X) = h^{2,1}(Y)$ . These pairs were called mirror pairs, and the symmetry between them mirror symmetry. It should be understood that mirror symmetry is more than this equality of Hodge numbers; it means that the topological correlation functions in both theories should be equal after proper translation.

At first there was no supporting evidence for mirror symmetry, but soon Candelas and others constructed a large number of examples of Calabi-Yau varieties by considering hypersurfaces in weighted projective spaces. The resulting collection of varieties turned out to be almost symmetric under the exchange of Hodge numbers  $h^{1,1} \leftrightarrow h^{2,1}$ , which was at least some numerical support for mirror symmetry. Subsequently Green and Plesser [18] developed an orbifolding construction that indeed produced pairs of mirror varieties. They considered the conformal theory defined by a diagonal 3-dimensional Calabi-Yau hypersurface and showed that it was isomorphic to the theory obtained from a quotient of this variety by a finite group. Their construction was further elaborated by Batyrev, who showed that it fitted in the framework of hypersurfaces in toric varieties. Nevertheless a general construction for the mirror partner of a Calabi-Yau variety is still lacking.

A promising approach towards understanding mirror symmetry from a mathematical point of view is Kontsevich's Homological Mirror Conjecture. Kontsevich showed that a Calabi-Yau could be used to define two so-called  $A_\infty$  categories, one related to the complex structure and one to the Kähler metric via special Lagrangian submanifolds. He conjectured that mirror symmetry exchanges these categories and proved this together with Soibelman for the case of abelian varieties [23].

It may be possible to gain a better understanding of mirror symmetry by studying the arithmetic properties of mirror pairs of Calabi-Yau varieties. In mirror symmetry, the period map that describes the deformations of the complex structure of a variety has an important role. It is well-known among algebraic geometers that this map also contains information on the arithmetic of the variety. Since most known examples of mirror pairs of Calabi-Yau varieties are defined over number fields, it is quite conceivable that the phenomenon of mirror symmetry may be clarified by using this arithmetic information, which is usually ignored by physicists. This line of research may also reveal new insights entirely unrelated to mirror symmetry, since there is still a lot to be learned about varieties over fields in a positive characteristic. In this thesis, we will provide a number of examples of diagonal Calabi-Yau varieties where we can describe the arithmetic structure entirely in terms of modular forms.

### 1.3 Diagonal varieties

The subject of the arithmetic of diagonal equations has a very long history in mathematics. Many famous diophantine problems are related to diagonal equations. The oldest example is the Pythagorean Theorem; a Babylonian list of

integer solutions has been found dating from 1700 B.C. [22]. Another important example is Fermat's Last Theorem that  $x^n + y^n = z^n$  has no solutions in the positive integers for  $n > 2$ . This problem fascinated generations of mathematicians and has thus been a source of inspiration in the development of number theory. In the nineteenth century failed attempts to prove this theorem led Kummer to develop the theory of ideals, which is the cornerstone of modern algebraic geometry.

In all Diophantine problems, reduction modulo an integer is a useful technique. Especially the number of solutions of diagonal equations modulo a prime has been the subject of much study. An important result in this direction was found by Gauss [16], who obtained the numbers of solutions of the equation

$$ax^3 - by^3 \equiv 1 \pmod{p}$$

for an arbitrary prime  $p$  and integer coefficients  $a$  and  $b$ . He did this by introducing a new tool, the character sums that were subsequently called Gauss sums. Later he also applied his method to the case of degree 4, determining the number of solutions of

$$ax^4 - by^4 \equiv 1 \pmod{p}.$$

His character sums attracted the interest of Jacobi [21], who first saw their importance in their own right rather than as a combinatorial tool. Jacobi also introduced character sums of his own (called Jacobi sums by later mathematicians).

After that the subject received little attention until André Weil [47, 48] found a method to use the Gauss sums to count the points of a general diagonal variety in 1949. He showed that for any diagonal variety  $X$  with integer coefficients and any prime  $p$  a zeta function exists: a rational function over  $\mathbb{Z}$  that generates the numbers of points of  $X$  over the finite fields  $\mathbb{F}_{p^s}$  (with  $s \in \mathbb{Z}_{\geq 1}$ ). It is defined as

$$Z_p(X, t) := \exp \left( \sum_{s=1}^{\infty} \frac{1}{s} |X(\mathbb{F}_{p^s})| t^s \right).$$

As he showed, the Jacobi sums gave the roots and poles of this function. This example and similar results for curves led him to make the famous Weil conjectures, asserting that for any smooth projective variety  $Y$  with good reduction over a prime  $p$ , the function  $Z_p(Y, t)$  would be a rational function with integer coefficients. This function would have the form

$$Z_p(Y, t) = \frac{P_1(t)P_3(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)},$$

where  $n$  is the dimension of  $Y$ . Each polynomial  $P_i(t)$  has integer coefficients, roots of length  $p^{-i/2}$  and degree equal to the topological Betti number  $\beta_i(Y)$ , where  $Y$  is considered as a variety over  $\mathbb{C}$ .

These conjectures implied unknown connections between the arithmetic and topological properties of varieties, and they quickly became the focus of much interest. The polynomials  $P_i$  were interpreted as characteristic polynomials of

Frobenius operators, acting on the cohomology of the variety by a Galois representation. For this interpretation new algebraic techniques like the étale cohomology were developed, leading eventually to the proof (by Deligne [8]) of the Weil conjectures and the equivalent of the Riemann hypothesis for varieties over finite fields. Further developments in this field enabled Wiles [50] to prove Fermat's Last Theorem.

At present, there are few varieties for which the zeta functions are known for all primes. Taylor, Wiles and others [5, 50] proved that elliptic curves over  $\mathbb{Q}$  correspond to modular forms; in particular this implies that their zeta functions are determined by the Fourier coefficients of these forms. The correct modular form for a given elliptic curve can be found by calculating these coefficients for a finite number of primes, after which a criterion by Serre [38] can be used to prove it is the correct form. The zeta functions for all primes can then be deduced from this modular form.

Other examples where it was possible to determine all zeta functions were found in the category of Calabi-Yau varieties, which are a natural generalisation of elliptic curves to higher dimensions. Yui and others [19, 28, 46, 51] constructed some such varieties that were rigid; that is, the Hodge number  $h^{2,1}$  equals 0. They were able to prove that also in these cases, a modular form could be associated to the variety whose Fourier coefficients determined the zeta functions. It was even conjectured that this would hold for all rigid Calabi-Yau varieties of dimension three [36].

## 1.4 Outline

In this thesis we show a number of diagonal varieties for which the cohomology can be split entirely into parts that are described by modular forms and characters. A diagonal variety has a large symmetry group; it is invariant under multiplication of the  $i$ -th coordinate by any  $e_i$ -th root of unity. By taking the quotient of the diagonal variety by appropriate subgroups of this group, the cohomology of the variety (as a Galois representation) can be decomposed into subrepresentations. We use Weil's approach to express the number of points of the diagonal variety and its zeta functions in terms of Jacobi sums and we show how a factor of the zeta function can be assigned to each subrepresentation. This factor is a polynomial in  $\mathbb{Z}[t]$ , and the inverses of its roots are given by the Jacobi sums.

Subsequently we use the Gross-Koblitz formula to express the Jacobi sums in terms of the  $p$ -adic Gamma function. This allows us to approximate the Jacobi sums and hence the coefficients of the zeta function by a  $p$ -adic expansion. These coefficients are integers in a certain range and hence we can find them by applying a  $p$ -adic approximation to a finite order of precision. Since we can calculate the factors corresponding to each subrepresentation separately, the order of  $p$ -adic precision required is low enough to allow quick evaluation.

The form of some factors of the zeta function suggests strongly that the corresponding subrepresentations decompose as a tensor product of representations. We show that this is indeed the case by recalling a construction by Shioda and

Katsura and applying it to our case. In this way some inductive relations between the Jacobi sums are interpreted in a geometrical way.

Next we investigate which subrepresentations are described by modular forms. In diagonal varieties of degree 3, 4 and 6 the cohomology decomposes into subrepresentations of dimension 2; in that case we expect that the subrepresentations are modular. We apply theorems by Livné and Serre [27] and by Schütt [37] to determine modular forms corresponding to some of these. Since we also have an expression for the zeta functions of these varieties in terms of Jacobi sums, this allows us to relate these Jacobi sums directly to coefficients of modular forms.

This is useful to us when we study diagonal varieties of degree 8 and 12. Here the cohomology decomposes into subrepresentations of dimension 4. We show that in a number of examples, the Jacobi sums defining the zeta functions can be simplified to other Jacobi sums that we already know to correspond to modular forms. Hence we are able to show that the whole cohomology of these varieties can be described by modular forms as well, even though many of the 4-dimensional representations are irreducible. Some of these are twists of tensor products of modular representations, a fact that is not always explained by the Shioda-Katsura construction.

For these examples, we give the decomposition of the cohomology into subrepresentations. For each of these we give explicit expressions for the zeta functions in terms of the coefficients of the modular forms and certain twists.

The organisation of this thesis is as follows. In Chapter 2 we review the properties of diagonal varieties as geometric objects; we determine their Hodge numbers and study the resolution of their singularities. This is an exercise in the theory of hypersurfaces in weighted projective spaces; the theory here was developed by Dolgachev [14] and Dimca [13].

Then in Chapter 3 we turn to the theory of Jacobi and Gauss sums and express the zeta function of a diagonal variety in terms of these sums. We also show how the cohomology of a diagonal variety, interpreted as a Galois representation, can be split into subrepresentations. We use the Gross-Koblitz formula to express the Gauss sums in terms of the  $p$ -adic Gamma function.

In Chapter 4 we review the construction of Shioda and Katsura and apply it to our case. We formulate some corollaries concerning its consequences for the arithmetic of diagonal varieties.

Subsequently we review some results on modular forms, Galois representations and the connections between these in Chapter 5. We give the theorems by Livné and Schütt and apply them to determine the modular forms corresponding to some diagonal elliptic curves.

In Chapter 6, we use all techniques from the previous chapters to calculate the zeta functions of a number of diagonal Calabi-Yau varieties. For each subspace in the cohomology we give a description of the corresponding factors of the zeta function. Sometimes we can apply the theorems of Livné-Serre or Schütt directly to show that a subspace is isomorphic as a Galois representation to a modular representation. In other cases we express the factors in terms of the  $p$ -adic Gamma function and use the properties of that function to relate them to twists of modular

representations discovered previously. Often we find that these representations are twisted tensor products of known 2-dimensional representations. Of course representations corresponding to rational cycles are found as well. Explicit tables are given with the decomposition of the cohomology of these diagonal Calabi-Yau varieties and the modular forms and characters corresponding to each subspace. From this data the zeta functions and the  $L$ -series can be constructed up to factors at the primes of bad reduction.

# Chapter 2

## Singular Toric Varieties

Diagonal varieties are examples of what are called quasi-smooth varieties. Intuitively this means that they have singularities only where they intersect singularities of the ambient space, in this case a weighted projective space. Moreover, the singularities of the variety can be resolved by resolving the singularities of the ambient space. To make these remarks precise we need the theory of toric varieties. In this chapter we will introduce these and study their singularities and resolutions.

For a general introduction into toric varieties, we refer the reader to Fulton [15]. Results on hypersurfaces in toric varieties and their cohomology can be found in Batyrev [2] and Batyrev and Cox [3]. A useful article on the properties of weighted projective varieties is [14].

### 2.1 Definitions

To define a toric variety over some field  $k$  we need the notion of a fan.

**Definition 2.1** *Let  $V$  be a finite-dimensional real vector space. A set  $\Sigma$  of convex cones in  $V$  is called a fan if it satisfies the following properties:*

1. *Each  $\sigma \in \Sigma$  is finitely generated over  $\mathbb{R}_{\geq 0}$ ;*
2. *No  $\sigma \in \Sigma$  contains a whole line;*
3. *Each face of a cone in  $\Sigma$  is a cone in  $\Sigma$ ;*
4. *The intersection of any two cones in  $\Sigma$  is itself a cone in  $\Sigma$  and a face of both.*

A cone  $\sigma$  is called rational with respect to a lattice  $N \subset V$  if it is finitely generated over  $\mathbb{R}_{\geq 0}$  by generators in  $N$ . If  $\sigma$  is generated by linearly independent vectors, it is called simplicial. The fan  $\Sigma$  is called rational with respect to  $N$  if all its cones are; if no ambiguity is possible, we will just call this a rational fan.

To define a toric variety, we must specify a lattice  $N$  and a fan  $\Sigma$  in  $N_{\mathbb{R}} := N \otimes_{\mathbb{Z}} \mathbb{R}$  that is rational with respect to  $N$ . We denote the dual lattice by  $N^*$  and the pairing  $N \times N^* \mapsto \mathbb{Z}$  by  $\langle \cdot, \cdot \rangle$ .

For a cone  $\sigma \in \Sigma$ , we define the dual cone

$$\hat{\sigma} := \{y \in N_{\mathbb{R}}^* : \langle x, y \rangle \geq 0 \ \forall x \in \sigma\}. \quad (2.1)$$

This is a cone in  $N_{\mathbb{R}}^* = N^* \otimes_{\mathbb{Z}} \mathbb{R}$ , where  $N^*$  denotes the dual lattice. Then  $S_{\sigma} := \hat{\sigma} \cap N^*$  is a semigroup that is finitely generated over  $\mathbb{N}$ , and we can consider its group algebra. Let  $k[\{X_m : m \in S_{\sigma}\}]$  be the free algebra generated by the  $X_m$ , and let  $I$  be the ideal in this algebra generated by

$$\{X_m - X_{m_1}X_{m_2} : m = m_1 + m_2\}. \quad (2.2)$$

Then the group algebra  $k[S_{\sigma}]$  is defined as

$$k[S_{\sigma}] := k[\{X_m : m \in S_{\sigma}\}]/I. \quad (2.3)$$

Since  $S_{\sigma}$  is finitely generated as a semigroup,  $k[S_{\sigma}]$  is finitely generated as an algebra, and we define the affine variety associated to  $\sigma$  by

$$U_{\sigma} := \text{Spec } k[S_{\sigma}]. \quad (2.4)$$

If  $\sigma'$  is a face of  $\sigma$ , we have inclusions:

$$\begin{aligned} \sigma' &\subset \sigma \\ \hat{\sigma} &\subset \hat{\sigma}' \\ S_{\hat{\sigma}} &\subset S_{\hat{\sigma}'} \\ k[S_{\hat{\sigma}}] &\subset k[S_{\hat{\sigma}'}] \\ \text{Spec } k[S_{\hat{\sigma}'}] &\subset \text{Spec } k[S_{\hat{\sigma}}], \end{aligned} \quad (2.5)$$

so larger cones in  $N$  correspond to larger varieties. If  $\sigma' = \sigma \cap H$  for some hyperplane  $H \subset N_{\mathbb{R}}$  defined by a minimal  $m \in N^*$ , then  $U_{\sigma'} = U_{\sigma} \cap \{X_m \neq 0\}$  and this is a Zariski open subset. We can glue the affine varieties defined by the  $\sigma \in \Sigma$  along these subsets, and this defines the toric variety  $M_{\Sigma}$  associated to  $\Sigma$ .

**Definition 2.2** *Given a lattice  $N$  of finite rank and a fan  $\Sigma$  in  $N \otimes_{\mathbb{Z}} \mathbb{R}$  that is rational with respect to  $N$ , the toric variety  $M_{\Sigma}$  is the variety obtained by gluing the affine varieties  $U_{\sigma}$  (with  $\sigma \in \Sigma$ ) with the identifications induced by the canonical inclusions  $k[\{X_m : m \in S_{\sigma}\}] \subset k[\{X_m : m \in N^*\}]$ .*

**Example** Take  $N = \mathbb{Z}^2$  and  $\Sigma$  the set of all cones spanned over  $\mathbb{R}_{\geq 0}$  by a proper subset of  $\{e_1, e_2, -e_1 - e_2\}$ , together with the zero cone  $\{0\}$ . We name the 2-dimensional cones according to Figure 2.1. For each cone  $\sigma_i$ , the semigroup  $S_{\sigma_i}$  is generated by two independent variables; so the group algebra is free over  $k$  in two variables, and  $U_{\sigma_i} \cong \mathbb{A}^2$ .

The dual cone of  $\sigma_0$  is equal to  $\sigma_0$ , which is also generated by  $(1, 0)$  and  $(0, 1)$ . We denote the coordinates of  $U_{\sigma_0}$  by  $x = X_{(1,0)}$  and  $y = X_{(0,1)}$ . The dual cone

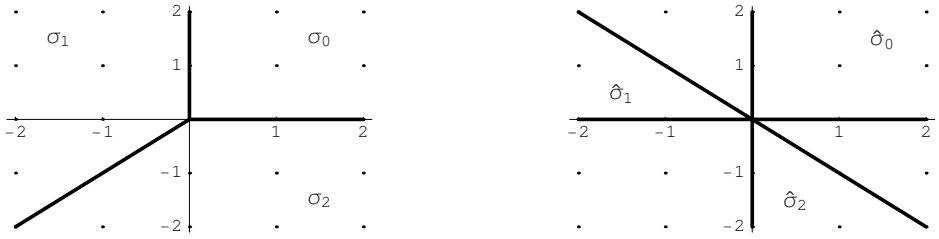


Figure 2.1: An example of a fan and its dual fan.

$\hat{\sigma}_1$  is generated by  $(-1, 0)$  and  $(-1, 1)$ . Therefore  $U_{\sigma_1}$  has coordinates  $x^{-1}$  and  $yx^{-1}$ , and the intersection  $U_{\sigma_0} \cap U_{\sigma_1}$  is the set  $x \neq 0$ . On this set, we may write  $x = X_1/X_0$  and  $y = X_2/X_0$  and hence  $x^{-1} = X_0/X_1$  and  $yx^{-1} = X_2/X_1$ . These are precisely the usual affine coordinates of the neighbourhoods  $X_0 \neq 0$  and  $X_1 \neq 0$  in the projective space  $\mathbb{P}^2$ , with the correct transition functions. We can check that  $\sigma_2$  corresponds likewise to the neighbourhood  $X_2 \neq 0$ . Hence  $M_\Sigma \cong \mathbb{P}^2$  in this case.

Many properties of toric varieties can be deduced from the fan. An important example is properness.

**Theorem 2.3** ([15], §2.4) *Let  $M$  be a toric variety defined by a lattice  $N$  and a fan  $\Sigma$ . Then  $M$  is proper if and only if*

$$\bigcup_{\sigma \in \Sigma} \sigma = N \otimes_{\mathbb{Z}} \mathbb{R}. \quad (2.6)$$

## 2.2 Singularities

The following proposition allows us to determine whether a toric variety is singular from the properties of the fan.

**Proposition 2.4** ([15], §2.1) *Let  $\sigma$  be an  $r$ -dimensional cone in a fan  $\Sigma$ , generated over  $\mathbb{R}_{\geq 0}$  by elements of the lattice  $N$ . Then the variety  $U_\sigma$  is non-singular if and only if  $\sigma$  is generated by  $r$  vectors that form a subset of a basis for the lattice.*

If  $U_\sigma$  is indeed nonsingular, we can deduce that

$$U_\sigma \cong \mathbb{A}^r \times (\mathbb{A}^*)^{n-r},$$

where  $n$  is the rank of  $N$ . This is the case if and only if  $\sigma$  is a simplicial cone. Since the  $U_\sigma$  constitute an open covering of the toric variety  $M_\Sigma$ , this variety is non-singular if and only if all of the  $U_\sigma$  are.

Singularities can be resolved by using refinements of fans.

**Definition 2.5** *Let  $\Sigma$  and  $\Sigma'$  be rational fans in  $N_{\mathbb{R}}$ . Then we call  $\Sigma'$  a refinement of  $\Sigma$  if every cone in  $\Sigma$  is a union of cones in  $\Sigma'$ .*

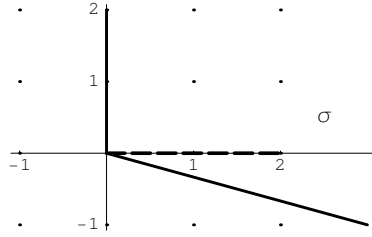


Figure 2.2: An example of resolution by subdividing

In this case there is a proper birational map  $M_{\Sigma'} \rightarrow M_{\Sigma}$  induced by the identity on  $N$ . So given a singular toric variety with fan  $\Sigma$ , we can find a resolution of singularities if it is possible to subdivide all singular cones into simplicial ones. It can be proved that this is always possible, but the resolution is generally not unique. Still it is very useful that resolutions exist even within the category of toric varieties.

**Proposition 2.6** ([15], §2.6) *For any toric variety  $M_{\Sigma}$ , there is a refinement  $\Sigma'$  of  $\Sigma$  such that the induced map  $M_{\Sigma'} \rightarrow M_{\Sigma}$  is a resolution of singularities.*

**Example** We study the cone  $\sigma$  in  $\mathbb{R}^2$  spanned over  $\mathbb{R}_{\geq 0}$  by  $(0, 1)$  and  $(3, -1)$  (see Figure 2.2). Clearly this cone is not generated by any basis for the lattice  $\mathbb{Z}^2$ . The dual cone is generated over  $\mathbb{R}_{\geq 0}$  by  $(1, 0)$  and  $(1, 3)$ ; to supplement these vectors to a generating set for  $\hat{\sigma} \cap \mathbb{Z}^2$  we need the vectors  $(1, 1)$  and  $(1, 2)$ , so  $U_{\sigma}$  is a surface  $X \subset \mathbb{A}^4$  given by equations

$$x_{(1,0)}^2 x_{(1,3)} = x_{(1,1)}^3 \text{ and } x_{(1,0)} x_{(1,3)}^2 = x_{(1,2)}^3$$

which is singular in 0, since these are affine coordinates. These equations define a cone over the twisted cubic.

To resolve the singularity, we subdivide  $\sigma$  by the ray spanned by  $(1, 0)$ . The resulting cones are both simplicial, so we have two copies of  $\mathbb{A}^2$ . We denote the upper cone spanned by  $(1, 0)$  and  $(0, 1)$  by  $\sigma_1$  and the lower cone by  $\sigma_2$ . Then the natural coordinates for  $U_{\sigma_1}$  are  $y_{(1,0)}$  and  $y_{(0,1)}$  and the coordinates of  $U_{\sigma_2}$  are given in terms of these by

$$(y_{(0,-1)}, y_{(1,3)}) = (y_{(0,1)}^{-1}, y_{(1,0)} y_{(0,1)}^3).$$

The resolution map is given by on  $U_{\sigma_1}$  by

$$\begin{aligned} \pi : U_{\sigma_1} &\rightarrow X \\ (y_{(1,0)}, y_{(0,1)}) &\rightarrow (y_{(1,0)}, y_{(1,0)} y_{(0,1)}, y_{(1,0)} y_{(0,1)}^2, y_{(1,0)} y_{(0,1)}^3). \end{aligned}$$

The line  $y_{(1,0)} = 0$  is blown down to a point, creating the singularity. In the other neighbourhood, we have

$$(y_{(0,-1)}, y_{(1,3)}) \rightarrow (y_{(1,3)} y_{(0,-1)}^3, y_{(1,3)} y_{(0,-1)}^2, y_{(1,3)} y_{(0,-1)}, y_{(1,3)}).$$

In these coordinates the line  $y_{(1,3)} = 0$  is blown down, which coincides with the line  $y_{(1,0)} = 0$  up to one point. The full curve blown down is a  $\mathbb{P}^1$  with self-intersection  $-3$ ; we have a cyclic quotient singularity of degree 3.

In fact, this is an example of an algorithm to resolve the singularities of toric varieties of dimension 2; given a singular cone  $\sigma$ , we change coordinates such that it is generated by  $(0, 1)$  and  $(r_1, -r_2)$  with  $0 < r_2 < r_1$ . Then we subdivide the cone by adding the ray through  $(1, 0)$ . One of the new cones is nonsingular, the other may not be. In that case we repeat the process.

This algorithm ends after a finite number of steps  $m$ ; in each step a point is blown up into a  $\mathbb{P}^1$ . The exceptional divisor consists of  $k$  components  $E_i \cong \mathbb{P}^1$ , with  $E_i \cdot E_j = 1$  if  $|i - j| = 1$  and zero if  $|i - j| > 1$ . The self-intersection numbers can also be determined from the toric data. There are unique integers  $a_1 \dots a_k \geq 2$  such that

$$\frac{r_1}{r_2} = a_1 - \frac{1}{a_2 - \frac{1}{a_3 - \frac{1}{\ddots a_{k-1} - \frac{1}{a_k}}}}$$

The self-intersection numbers of the components of the exceptional divisor are equal to  $-a_i$ . This follows from the details of the calculation; see also [15], Chapter 2.

If we take the singular cone generated by  $(r + 1, -r)$  and  $(0, 1) \in \mathbb{Z}^2$ , we find that the exceptional divisor consists of  $r$  curves isomorphic to  $\mathbb{P}^1$ , all with self-intersection  $-2$ . In this case the singularity is a rational double point of type  $A_r$ .

## 2.3 Weighted projective spaces

The toric varieties we will use are weighted projective spaces and (partial) resolutions of these. A weighted projective space over the field  $k$  can be defined as the quotient of ordinary projective space by a finite group action; given a set of weights  $w = (w_0, \dots, w_n) \in (\mathbb{Z}_{>0})^{n+1}$ , we define the group

$$G := \{(z_0, \dots, z_n) \in (k^*)^{n+1} \mid \forall i : z_i^{w_i} = 1\} \quad (2.7)$$

and we let  $G$  act on  $\mathbb{P}^n$  by componentwise multiplication. The quotient of  $\mathbb{P}^n$  by this group is the weighted projective space  $\mathbb{P}(w) = \mathbb{P}(w_0, \dots, w_n)$ . A point on the space is denoted by  $(X_0 : X_1 : \dots : X_n)$  just as in ordinary projective space, but the quotient map  $\pi : \mathbb{P} \rightarrow \mathbb{P}(w)$  is given by

$$(Y_0 : \dots : Y_n) \rightarrow (Y_0^{w_0} : \dots : Y_n^{w_n}).$$

For this reason the coordinate ring  $S(\mathbb{P}(w))$  is the graded ring  $k[X_0, \dots, X_n]$  graded by assigning a degree  $w_i$  to the variable  $X_i$ .

The weighted projective space can also be defined as a toric variety. To see this, we take the lattice  $N \cong \mathbb{Z}^n$  and we let  $\{e_i\}$  be the standard basis. Then we take vectors  $v_i = e_i$  (with  $i = 1 \dots n$ ) and  $v_0 = -\sum_{i=1}^n w_i e_i$ , and we let  $\Sigma(w)$  be the fan consisting of all cones spanned by  $n$  or less of these vectors. With this choice we have

$$M_{\Sigma(w)} \cong \mathbb{P}(w),$$

with the isomorphism induced by the map

$$X_{e_i^*} \mapsto \frac{X_i^{w_0/(w_0, w_i)}}{X_0^{w_i/(w_0, w_i)}},$$

where the  $X_i$  are the usual coordinates on the weighted projective space.

From this definition it is immediately clear that a common factor in the weights is irrelevant and can be discarded, since neither the cones nor the lattice are affected by this change. Another, less evident type of isomorphism of weighted projective spaces is given by Delorme [12].

**Proposition 2.7** *Let  $d_i = \gcd(w_0, \dots, \hat{w}_i, \dots, w_n)$  (where the  $\hat{\phantom{x}}$  denotes omission) and  $a_i = \text{lcm}(d_0, \dots, \hat{d}_i, \dots, d_n)$ . Then*

$$\mathbb{P}(w_0, \dots, w_n) \cong \mathbb{P}(w_0/a_0, \dots, w_n/a_n).$$

So a weighted projective space is isomorphic to a weighted projective space of lower total weight  $w_0 + \dots + w_n$ , unless all  $d_i$  are equal to 1. In that case we call  $w$  a *reduced weight*. If we take the natural projective coordinates  $X_i$  on  $\mathbb{P}(w_0, \dots, w_n)$  and  $Y_i$  on  $\mathbb{P}(w_0/a_0, \dots, w_n/a_n)$ , the isomorphism is induced by the map  $Y_i = X_i^{d_i}$ .

Weighted projective spaces are almost always singular. Let a projective space  $\mathbb{P}(w_0, \dots, w_n)$  of reduced weight  $w$  and a prime  $p$  be given. Then we define

$$\text{Sing}_p(\mathbb{P}(w)) := \{x \in \mathbb{P}(w) \mid \forall i : x_i = 0 \vee p|w_i\} \quad (2.8)$$

and the singular part  $\text{Sing}(\mathbb{P}(w))$  of  $\mathbb{P}(w)$  is equal to the union over all primes  $p$  of  $\text{Sing}_p(\mathbb{P}(w))$  (see Dimca [13]).

A hypersurface  $X$  defined in a weighted projective space will also acquire a singularity where it intersects  $\text{Sing}(\mathbb{P}(w))$ . Often these will be the only singularities of  $X$ .

**Definition 2.8** *Let  $\mathbb{P}(w)$  be a projective space of reduced weight  $w$  and let  $X$  be a hypersurface of degree  $d$  in  $\mathbb{P}(w)$ . Define for each prime  $p$*

$$m(p) := \#\{i : p|w_i\}. \quad (2.9)$$

Let  $k(p) := 1$  if  $p|d$  and 0 otherwise, and set

$$q(p) := \dim(X) + 1 + k(p) - m(p). \quad (2.10)$$

Then  $X$  is said to be in general position with respect to  $\text{Sing}(\mathbb{P}(w))$  if and only if  $q(p) \geq 2$  for all  $p$ .

The motivation for this definition is the following proposition.

**Proposition 2.9** [13] *Let a projective space  $\mathbb{P}(w)$  of reduced weight  $w$  be given and let  $X$  be a hypersurface of degree  $d$  in  $\mathbb{P}(w)$  that is in general position with respect to  $\text{Sing}(\mathbb{P}(w))$ . Then  $\text{Sing}(X) = X \cap \text{Sing}(\mathbb{P}(w))$ .*

This result allows us to find the singular set of the diagonal varieties we are interested in quite easily, since they are all in general position.

## 2.4 Singularities of diagonal varieties

Let  $X$  be the diagonal hypersurface of dimension  $n$  defined over a field  $k$  by the equation

$$\sum_{i=0}^{n+1} a_i X_i^{e_i} = 0, \quad (2.11)$$

with all  $a_i \in \mathbb{Z}$  and unequal to zero, and all  $e_i \geq 2$ . The variety  $X$  lies in a weighted projective space; let  $d := \text{lcm}\{e_i\}$  and set  $w_i := d/e_i$ . Then  $X$  is a hypersurface in  $\mathbb{P}(w)$ , and it is easy to check that it is in general position with respect to the ambient weighted projective space. Throughout we will assume without loss of generality that the  $w$  is a reduced weight. We also assume that the characteristic of  $k$  is either zero or coprime to  $d$ .

For reasons mentioned in the Introduction, we are especially interested in Calabi-Yau hypersurfaces.

**Definition 2.10** *A variety  $X$  is called a Calabi-Yau variety if its dualizing sheaf  $\omega_X$  is trivial and*

$$H^i(X, \mathcal{O}_X) = 0$$

for  $0 < i < \dim(X)$ .

The dualizing sheaf is the sheaf of germs of differential forms that are regular at all nonsingular points of  $X$ . It is well-defined in this case, see for example Kunz [24]. On a smooth variety  $\omega_X$  is the canonical bundle.

By a theorem of Dolgachev [14], the diagonal variety  $X$  defined by (2.11) is a (singular) Calabi-Yau variety if and only if  $\sum_i 1/e_i = 1$ . This case has been studied by several authors, and for low-dimensional cases the resolution of singularities is known. See for example [51] and [34].

**Theorem 2.11** *Let  $X$  be a hypersurface of dimension  $n$  equal to 1 or 2, defined in  $\mathbb{P}(w)$  by (2.11) over a field  $k$  with either  $(\text{char}(k), e_i) = 1$  for all  $i$  or  $\text{char}(k) = 0$ . Assume that  $\sum_{i=0}^{n+1} 1/e_i = 1$ . If  $X$  has dimension 1, then  $X$  is smooth. If the dimension of  $X$  is 2, then  $X$  has a minimal resolution of singularities defined over  $\mathbb{Q}$ . Each prime  $p$  dividing two different weights  $w_a$  and  $w_b$  corresponds to a set of singular points  $\text{Sing}_p(X) = \text{Sing}_p(\mathbb{P}(w)) \cap X$  of  $X$  of cardinality*

$$|\text{Sing}_p(X)| = \frac{\text{lcm}(w)}{\text{lcm}(w_a, w_b)},$$

and these are all singular points of  $X$ .

Each point of  $\text{Sing}_p(X)$  is a rational double point of type  $A_{p-1}$ . Hence it is blown up into  $p - 1$  exceptional curves  $E_i$  by the resolution, with intersections

$$E_i \cdot E_j = \begin{cases} 0 & \text{if } |i - j| > 1 \\ 1 & \text{if } |i - j| = 1 \\ -2 & \text{if } |i - j| = 0. \end{cases}$$

The case  $n = 3$  is also known, but we need some more notation. For each integer  $\ell$  with  $0 \leq \ell < d$ , we define  $s_\ell := \{0 \leq i \leq n : e_i | \ell\}$ . Furthermore we set  $c_\ell = \gcd\{w_i : i \in s_\ell\}$ . These data suffice to describe the singularities of a diagonal Calabi-Yau threefold and its resolution.

By a result of Batyrev [2] we can find a resolution that is not only toric, but also “crepant” meaning that the canonical class of the resolution is just the pull-back of the canonical class of  $X$ ; there are no contributions of the exceptional fibers. If  $X$  is a Calabi-Yau variety, this implies that the resolution is a smooth Calabi-Yau threefold.

**Theorem 2.12** *Let  $X$  be a hypersurface of dimension 3 defined in the weighted projective space  $\mathbb{P}(w)$  by (2.11) over a field  $k$  with  $(\text{char}(k), e_i) = 1$  for all  $i$  and assume that  $\sum_{i=0}^{n+1} 1/e_i = 1$ . Then there is a toric crepant resolution defined over  $\mathbb{Q}$ , and all singularities of  $X$  are as follows.*

- If  $\#s_\ell < 3$  for all  $\ell \neq 0$ , then  $\text{Sing}(X)$  has no components of dimension 1.
- If  $\#s_\ell = 3$  for some  $\ell$ , then  $\text{Sing}(X)$  has a component of dimension 1

$$X_{s_\ell} = X \cap \bigcap_{j \notin s_\ell} \{X_j = 0\}. \quad (2.12)$$

This component is the diagonal curve with exponents  $e_i$  and coefficients  $a_i$  with  $i \in s_\ell$ . Its degree is  $d/c_\ell$  and the exceptional fiber of this singularity is birational to  $c_\ell - 1$  copies of  $X_{s_\ell} \times \mathbb{P}^1$ .

- Each set  $s_\ell$  with  $\#s_\ell = 2$  corresponds to a set of singular points  $X_{s_\ell}$  defined by (2.12). The exceptional fiber of each point is isomorphic to a  $\mathbb{P}^2$ .

The 1-dimensional components of  $\text{Sing}(X)$  are smooth diagonal curves. Here is a useful expression for the genus of such a curve.

**Lemma 2.13** *Let  $C$  be a diagonal curve with exponents  $e_i$  (with  $i = 0, 1, 2$ ) and degree  $d = \text{lcm}\{e_i\}$ , defined in the 2-dimensional projective space  $\mathbb{P}(w)$  with weight  $w_i = d/e_i$ , and assume that  $w$  is a reduced weight. Then the genus of  $C$  is equal to the coefficient of  $t^{d - \sum_i w_i}$  in the series expansion of  $\prod_i (1 - t^{w_i})^{-1}$ .*

This follows from the next section, where a basis for the middle cohomology of a diagonal variety is given in case  $k = \mathbb{C}$ .

**Example** We consider the diagonal threefold  $X$  of degree 20 defined by the equation

$$X_0^4 + X_1^4 + X_2^5 + X_3^5 + X_4^{10} = 0$$

in the weighted projective space  $\mathbb{P}(5, 5, 4, 4, 2)$  over a field of characteristic unequal to 2 and 5. To find its singularities, we must calculate the  $s_\ell$ . For  $\ell = 10$ , we have  $s_\ell = \{2, 3, 4\}$ ; for all other  $\ell$  with  $0 \leq \ell < 20$ , we have  $|s_\ell| \neq 3$ . So  $\text{Sing}(X)$  has a single 1-dimensional component, the curve  $C$  of degree 10 defined by

$$X_0 = X_1 = 0, \quad X_2^5 + X_3^5 + X_4^{10} = 0.$$

This curve has genus 6. This can be checked by Lemma 2.13, but in this case we can also apply the Plücker formula. The curve  $C$  can be considered as a subvariety of  $\mathbb{P}(2, 2, 1)$ , but this is a projective space of reducible weight. By reduction we see that  $C$  is isomorphic to the smooth curve of degree 5 defined by

$$X_2^5 + X_3^5 + X_4^5 = 0$$

in  $\mathbb{P}^2$ , and here the Plücker formula applies:

$$g = \frac{(d-1)(d-2)}{2}$$

with  $d$  the degree of the curve in  $\mathbb{P}^2$ , which is 5.

The number  $c_\ell$  is equal to 2 for  $\ell = 10$ , so the fiber of  $C$  under the resolution is just one copy of  $C \times \mathbb{P}^1$ .

For  $\ell \in \{4, 8, 12, 16\}$ , the set  $s_\ell = \{0, 1\}$  has cardinality 2. Therefore there are singular points, defined by

$$X_0^4 + X_1^4 = 0, \quad X_2 = X_3 = X_4 = 0.$$

So we have 4 singular points, but some may not be rational depending on the field of definition of  $X$ .

For  $\ell \in \{5, 15\}$ , we find  $s_\ell = \{2, 3\}$ . So the points defined by

$$X_0 = X_1 = X_4 = 0, \quad X_2^5 + X_3^5 = 0$$

are also singular.

## 2.5 Hodge numbers of diagonal varieties

With the results of the previous section we can compute Hodge numbers of diagonal Calabi-Yau threefolds (considered as varieties over  $\mathbb{C}$ ). First we need to know the Betti numbers of the singular threefold. For this purpose we use results by Batyrev and Cox, who wrote an extensive paper about the cohomology of hypersurfaces in toric varieties [3]. As is the case with ordinary hypersurfaces, only the middle cohomology is nontrivial in the sense that it is not generated by the hyperplane class. To separate this contribution, the primitive cohomology researched by Steenbrink [41] can be used. Consider a hypersurface  $X$  defined by  $f(x) = 0$  in  $\mathbb{P}(w)$ . Then its primitive cohomology  $PH(X)$  is defined by the sequence

$$0 \rightarrow H^r(\mathbb{P}(w)) \rightarrow H^r(X) \rightarrow PH^r(X) \rightarrow 0. \quad (2.13)$$

Let  $S$  be the coordinate ring of  $\mathbb{P}(w)$ , let  $J(X) = \langle \{X_i \partial f / \partial X_i\} \rangle$  be the Jacobian ideal in  $S$ , and  $R(f) = S/J(X)$  the quotient ring. Then  $R(f)$  has a grading derived from  $S$ , and we denote by  $R(f)_i$  its  $i$ -th graded part. We have the following theorem about the middle cohomology.

**Theorem 2.14** ([3], 10.13) *For all  $r \neq \dim(X) = n$  the space  $PH^r(X, \mathbb{C})$  is zero. For  $PH^n(X, \mathbb{C})$  we have a canonical isomorphism*

$$R(f)_{(n-j)d} \cong PH^{j, n-j}(X, \mathbb{C}). \quad (2.14)$$

If  $X$  is the diagonal hypersurface defined by (2.11), the space  $R(f)_{(n-j)d}$  can be described explicitly: it has a basis of monomials

$$\left\{ \prod_i X_i^{c_i e_i / d} : 0 < c_i < d, c_i e_i / d \in \mathbb{Z} \text{ and } \sum_i c_i \equiv 0 \pmod{d} \right\}.$$

These monomials also appear in a basis of the primitive cohomology in terms of differential forms. As Batyrev and Cox show, the middle primitive cohomology is isomorphic to the space generated over  $\mathbb{C}$  by the monomials

$$\frac{\prod_i X_i^{c_i e_i / d - 1} \sum_i (-1)^i w_i X_i dX_0 \wedge \dots \wedge \widehat{dX_i} \wedge \dots \wedge dX_{n+1}}{(\sum_i a_i X_i^{e_i})^{\sum_i c_i / d}} \quad (2.15)$$

So the middle Betti number can be determined by counting the vectors  $c$  that satisfy the given condition.

Knowing the number  $\beta_3(X)$  of a diagonal threefold  $X$  as well as the singularities of  $X$  and their resolution, we can also compute the non-singular third Betti number  $\beta_3(\tilde{X})$ . Since the isolated singular points are blown up to copies of  $\mathbb{P}^2$ , they do not contribute to  $\beta_3$ . The components of  $\text{Sing}(X)$  of dimension 1 are blown up to surfaces of the form  $\mathbb{P}^1 \times C$ , so they contribute  $\beta_1(C)$  each. As Roan [34] shows, these contributions can simply be added; the cycles are all independent.

**Theorem 2.15** [34] *Let  $\pi : \tilde{X} \rightarrow X$  be a toric crepant resolution of singularities of a diagonal Calabi-Yau threefold  $X$ . Then*

$$\beta_3(\tilde{X}) = \beta_3(X) + \sum_C m_C \beta_1(C)$$

where the sum is taken over the 1-dimensional components  $C$  of  $\text{Sing}(X)$ , and  $m_C$  is the multiplicity of  $C$  given in Theorem 2.12.

Roan also proves an explicit formula for the Euler number  $\chi(X)$ , which was first conjectured by Vafa based on arguments from string theory. Again  $X$  is a Calabi-Yau threefold of degree  $d$ , defined in reduced weighted projective 4-space  $\mathbb{P}(w)$ . Then we have

$$\chi(X) = \frac{1}{d} \sum_{a,b=0}^{d-1} \prod_{i:w_i|(a,b)} (1 - w_i). \quad (2.16)$$

Clearly we can deduce  $\beta_2(\tilde{X}) = \beta_4(\tilde{X})$  from  $\chi(\tilde{X})$  and  $\beta_3(\tilde{X})$ , since the other Betti numbers are trivial. From the definition of a Calabi-Yau variety we know that  $h^{2,1}(\tilde{X}) = (\beta_3(\tilde{X}) - 1)/2$  and  $h^{1,1}(\tilde{X}) = \beta_2(\tilde{X})$ .

**Example** We consider the variety  $X$  of degree 12 defined by

$$X_0^3 + X_1^3 + X_2^6 + X_3^{12} + X_4^{12} = 0 \quad (2.17)$$

in  $\mathbb{P}(4, 4, 2, 1, 1)$ . The inverses of the exponents add up to 1, so this is a Calabi-Yau threefold. The Betti number  $\beta_3(X)$  equals 202. There is a dimension 1 singularity; for  $\ell = 4$  or 8 we have  $s_\ell = \{0, 1, 2\}$ , which has length 3. Therefore the subvariety defined by  $X_3 = X_4 = 0$  is singularly embedded. This is the curve  $C$  defined by

$$X_0^3 + X_1^3 + X_2^6 = 0$$

in  $\mathbb{P}(2, 2, 1)$ , which is a reducible weighted projective space. By reducing the space we see that the curve is isomorphic to

$$X_0^3 + X_1^3 + X_2^3 = 0,$$

which is clearly an elliptic curve. The multiplicity of  $C$  equals  $\gcd(4, 4, 2) - 1 = 1$ , so the Betti number  $\beta_3(\tilde{X}) = 202 + 2 = 204$  and the Hodge number  $h^{2,1} = 101$ .

The Euler characteristic equals  $-192$  as follows from (2.16). Therefore we have  $\beta_2(\tilde{X}) = h^{1,1}(\tilde{X}) = 5$ .



# Chapter 3

## Combinatorics

### 3.1 Diagonal equations

In this chapter we study diagonal equations from an arithmetic point of view. Throughout the chapter,  $X$  will be the diagonal variety defined by

$$\sum_{i=0}^{n+1} a_i X_i^{e_i} = 0, \quad (3.1)$$

where we assume the coefficients  $a_i$  to be nonzero integers, and all  $e_i \in \mathbb{Z}_{>1}$ . This equation defines an  $n$ -dimensional hypersurface  $X$  over  $\mathbb{Q}$  in the weighted projective space  $\mathbb{P}(w_0, \dots, w_{n+1})$ , where we define the weights  $w_i := d/e_i$  and  $d := \text{lcm}(\{e_i\})$ . The most interesting case is  $\sum_i 1/e_i = 1$ , when  $X$  is a (singular) Calabi-Yau variety. In this case the weight is automatically reduced.

One reason why the hypersurface  $X$  is interesting is that it has a large symmetry group  $G(X)$ , acting on the coordinates  $X_i$  by multiplication with roots of unity. We define the group

$$G(X) := \{(\zeta^{b_0}, \dots, \zeta^{b_{n+1}}) \mid \forall i : b_i e_i \equiv 0 \pmod{d}\} / \langle (\zeta^{w_0}, \dots, \zeta^{w_{n+1}}) \rangle. \quad (3.2)$$

Here  $\zeta$  is a fixed but arbitrary primitive  $d$ -th root of unity. A group element  $(\zeta^{b_0}, \dots, \zeta^{b_{n+1}})$  acts on the weighted projective space by  $X_i \rightarrow \zeta^{b_i} X_i$  and obviously this action induces automorphisms of the hypersurface  $X$ . The subgroup generated by the element  $(\zeta^{w_0}, \dots, \zeta^{w_{n+1}})$  acts trivially.

Depending on the choice of  $e_i$  and  $a_i$ ,  $X$  may have also have permutation symmetry; for example, if  $X$  is a Fermat variety (that is, all  $e_i$  are equal and all  $a_i$  are 1), then  $X$  is clearly invariant under any permutation of the coordinates.

In this chapter, we will review the arithmetic of diagonal varieties; we will derive a formula for its zeta function for any  $q$ , and we will see how it can be calculated effectively.

## 3.2 Jacobi sums and Gauss sums

Before turning our attention to the diagonal varieties themselves, we will introduce Jacobi sums. They play a major role in the arithmetic of diagonal varieties but are also very interesting in themselves. The definition is quite natural.

**Definition 3.1** *Let  $q$  be a prime power,  $d \in \mathbb{Z}_{\geq 2}$  such that  $q \equiv 1 \pmod{d}$ , and let  $\chi$  be a character of  $\mathbb{F}_q^*$  of order  $d$ . Choose a  $c = (c_0, c_1, \dots, c_{n+1}) \in (\mathbb{Z}/d\mathbb{Z})^{n+2}$  and  $n \in \mathbb{Z}_{\geq 0}$  arbitrary. Then the Jacobi sum  $J_q^d(c, \chi)$  is defined as*

$$J_q^d(c, \chi) = \frac{(-1)^n}{(q-1)} \sum_{\substack{x_0 + \dots + x_{n+1} = 0 \\ x_i \in \mathbb{F}_q^*}} \chi^{c_0}(x_0) \dots \chi^{c_{n+1}}(x_{n+1}) \quad (3.3)$$

The number  $n$  is called the dimension of the Jacobi sum,  $d$  the degree.

Usually the definition is formulated a bit differently; the Jacobi sum is then defined as a function of the  $n+2$  characters  $\chi^{c_i}$  instead of  $c$ . Our definition will be more suited to our purpose of counting solutions to diagonal equations, and we will see that the vectors  $c$  have a geometric interpretation.

The set of solutions of  $x_0 + \dots + x_{n+1} = 0$  is invariant under scaling with any  $\lambda \in \mathbb{F}_q^*$ . This scaling multiplies  $J_q^d(c, \chi)$  by  $\chi^{\sum c_i}(\lambda)$ . It follows that  $\sum_i c_i \equiv 0 \pmod{d}$  (which we shall assume from this point) if  $J_q^d(c, \chi)$  is to be nonzero. We can use the scaling invariance again to set  $x_{n+1} = 1$ ; we find that

$$J_q^d(c, \chi) = (-1)^n \sum_{\substack{x_0 + \dots + x_n = -1 \\ x_i \in \mathbb{F}_q^*}} \chi^{c_0}(x_0) \dots \chi^{c_n}(x_n). \quad (3.4)$$

This does not depend explicitly on  $c_{n+1}$  any more, but we will not drop it from notation as a reminder of the fact that  $J_q^d(c, \chi)$  is invariant under permutation of  $(c_0, \dots, c_n, c_{n+1})$ .

**Lemma 3.2** *Let  $c \in (\mathbb{Z}/d\mathbb{Z})^{n+2}$ . If  $c$  is the zero vector, then  $J_q^d(c, \chi) = (-1)^n (q-1)^n$ . If the vector  $c$  is not zero, let  $\tilde{c}$  be the vector obtained from  $c$  by deleting all zero entries. Then*

$$J_q^d(c, \chi) = J_q^d(\tilde{c}, \chi). \quad (3.5)$$

**Proof** If  $c$  contains no zero entries there is nothing to prove. So assume that the last entry of  $c$  is zero. We use the fact that the conditions  $x_{n+1} \neq 0$  and  $\sum_{i=0}^{n+1} x_i = 0$  are equivalent to  $\sum_{i=0}^n x_i \neq 0$ ; we will abbreviate  $S = \{x \in (\mathbb{F}_q^*)^{n+1} : \sum_{i=0}^n x_i = 0\}$ . Then the Jacobi sum becomes

$$\begin{aligned} J_q^d((c_0, \dots, c_n, 0), \chi) &= (-1)^n \sum_{x \in (\mathbb{F}_q^*)^{n+1} \setminus S} \prod_{i=0}^n \chi^{c_i}(x_i) \\ &= (-1)^n \sum_{x \in (\mathbb{F}_q^*)^{n+1}} \prod_{i=0}^n \chi^{c_i}(x_i) - (-1)^n \sum_{x \in S} \prod_{i=0}^n \chi^{c_i}(x_i). \end{aligned} \quad (3.6)$$

Now the first term in the last expression vanishes if not all  $c_i$  are  $0 \pmod{d}$ , since  $\sum_{x \neq 0} \chi(x) = 0$  for any nontrivial  $\chi$  due to symmetry. The remaining term equals  $J_q^d((c_0, c_1, \dots, c_n), \chi)$ . So by induction all entries that are  $0 \pmod{d}$  can just be dropped from  $c$  in the Jacobi sum, as long as there is a nonzero entry present.

If  $c = 0$ , then we just have to count the  $x \in (\mathbb{F}_q^*)^n \setminus S$ . A similar inductive argument proves that  $J_q^d(c, \chi) = (-1)^n (q-1)^n$ .  $\square$

More properties of the Jacobi sums can be explained by using a factorisation into Gauss sums. These are defined as follows.

**Definition 3.3** *Let  $\psi$  be an arbitrary nontrivial additive character  $\psi : \mathbb{F}_q \rightarrow \mathbb{C}^*$  and  $\chi$  a multiplicative character of  $\mathbb{F}_q$ . Then we define*

$$g_q(\chi, \psi) = - \sum_{x \in \mathbb{F}_q^*} \chi(x) \psi(x). \quad (3.7)$$

The minus sign in the definition is used so that we have

$$g_q(\chi_1, \psi) = 1 \quad (3.8)$$

where  $\chi_1$  is the trivial character. Again we omit the  $q$  if no confusion is possible. From the symmetric definition of the Gauss sums, many properties can be derived easily. We will derive some for later use.

**Lemma 3.4** *If  $\chi$  is a nontrivial multiplicative character and  $\psi$  an additive character, then  $|g_q(\chi, \psi)|^2 = q$ .*

**Proof** The proof is typical of the way Gauss sums can be manipulated by rescalings and translations, and by using the identities  $\sum_{u \in \mathbb{F}_q^*} \chi(u) = 0$  and  $\sum_{v \in \mathbb{F}_q} \psi(v) = 0$  for nontrivial  $\chi$  and  $\psi$ . We have

$$\begin{aligned} g(\chi, \psi) \bar{g}(\chi, \psi) &= \sum_{u, v \neq 0} \chi\left(\frac{u}{v}\right) \psi(u-v) \\ &= \sum_{u, v \neq 0} \chi(u) \psi(v(u-1)) \\ &= \sum_{v \neq 0} \chi(1) \psi(0) + \sum_{\substack{u \neq 0, 1 \\ v \neq 0}} \chi(u) \psi(v) \\ &= (q-1) + (-\chi(1))(-\psi(0)) = q. \end{aligned} \quad (3.9)$$

$\square$

**Lemma 3.5** *Suppose  $c \in (\mathbb{Z}/d\mathbb{Z})^{n+2}$  has  $\sum_i c_i = 0$  and all  $c_i \neq 0$ . Then the Jacobi sum can be factorised as*

$$J_q^d(c, \chi) = g(\chi^{c_0}, \psi) g(\chi^{c_1}, \psi) \dots g(\chi^{c_{n+1}}, \psi) / q \quad (3.10)$$

and hence  $|J_q^d(c, \chi)| = q^{n/2}$ .

**Proof** To shorten the formulas, we abbreviate  $\chi^c(x) := \prod_{i=0}^{n+1} \chi(x_i)^{c_i}$ . By  $\mathbb{F}_q^*$  we denote a set of representatives  $x$  for the orbits of  $(\mathbb{F}_q^*)^{n+2}$  under scaling; by  $H$  the set of  $x \in (\mathbb{F}_q)^{n+2}$  with  $\sum_i x_i = 0$ .

The product of Gauss sums equals

$$\begin{aligned}
g(\chi^{c_0}, \psi) \dots g(\chi^{c_{n+1}}, \psi) &= (-1)^n \sum_{x \in (\mathbb{F}_q^*)^{n+2}} \chi^c(x) \psi(x_0 + \dots + x_{n+1}) \\
&= (-1)^n \sum_{x \in \mathbb{P}_q^*} \chi^c(x) \sum_{\lambda \in \mathbb{F}_q^*} \psi(\lambda(x_0 + \dots + x_{n+1})) \\
&= (-1)^{n+1} \sum_{x \in \mathbb{P}_q^* \setminus H} \chi^c(x) \psi(0) \\
&\quad + (q-1)(-1)^n \sum_{x \in \mathbb{P}_q^* \cap H} \chi^c(x) \psi(0) \\
&= (-1)^{n+1} \sum_{x \in \mathbb{P}_q^*} \chi^c(x) + q(-1)^n \sum_{x \in \mathbb{P}_q^* \cap H} \chi^c(x) \\
&= qJ_q^d(c) \tag{3.11}
\end{aligned}$$

as required. The final conclusion is obvious from Lemma 3.4.  $\square$

Using this factorisation, we can derive inductive relations between the Jacobi sums. There are two of them, that allow us to break them up into Jacobi sums with  $n = 0$  or  $1$ .

**Corollary 3.6** *Let  $\chi$  be a character of  $\mathbb{F}_q^*$  of order  $d$ , and let  $c \in (\mathbb{Z}/d\mathbb{Z})^{n_1+2}$  and  $b \in (\mathbb{Z}/d\mathbb{Z})^{n_2+2}$  have nonzero entries, such that  $\sum_{i=0}^{n_1+1} c_i \equiv \sum_{i=0}^{n_2+1} b_i \equiv 0 \pmod{d}$ . Then*

$$J_q^d(c_0, \dots, c_{n_1+1}, b_0, \dots, b_{n_2+1}) = qJ_q^d(c)J_q^d(b). \tag{3.12}$$

If  $c_0 + c_1 \not\equiv 0 \pmod{d}$ , then we have

$$J_q^d(c) = J_q^d(c_0 + c_1, -c_0 - c_1)J_q^d(c_0, c_1, -c_0 - c_1)J_q^d(c_0 + c_1, c_2, \dots, c_{n+1}). \tag{3.13}$$

It is not difficult to work out the case  $n = 0$ . So all Jacobi symbols can be reconstructed from those with  $n = 1$ .

**Lemma 3.7** *Let  $0 < c_0 < d$  be an integer,  $\chi$  a character of order  $d$  and  $d \mid (q-1)$ . Then we have*

$$J_q^d((c_0, d - c_0), \chi) = \begin{cases} (-1)^{c_0(q-1)/d} & \text{if } q \text{ is odd} \\ 1 & \text{if } q \text{ is even.} \end{cases} \tag{3.14}$$

From the definition we see that  $J_q^d((c_0, d - c_0), \chi) = \chi(-1)^{c_0}$ . We know  $\mathbb{F}_q^*$  is cyclic; we can pick a generator  $x$  with  $\chi(x) = e^{2\pi i/d}$ . Then  $-1 = x^{(q-1)/2}$  (unless  $q$  is even), so  $\chi(-1) = e^{\pi i(q-1)/d}$ .

It is useful to define some operations on the vectors  $c$ .

**Definition 3.8** *We define*

$$A_n^d := \{c \in (\mathbb{Z}/d\mathbb{Z})^{n+2} : \sum_{i=0}^{n+1} c_i \equiv 0 \pmod{d}, c_i \neq 0\}. \quad (3.15)$$

For  $c \in A_n^d$  and  $c' \in A_{n'}^d$ , we define the union  $c \cup c' \in A_{n+n'+2}^d$  as

$$c \cup c' := (c_0, \dots, c_{n+1}, c'_0, \dots, c'_{n'+1}). \quad (3.16)$$

If in addition  $c_{n+1} + c'_0 \equiv 0 \pmod{d}$ , we define the contraction  $c \vee c' \in A_{n+n'}^d$ :

$$c \vee c' := (c_0, \dots, c_n, c'_1, \dots, c'_{n'+1}). \quad (3.17)$$

We call  $c \in A_n^d$  irreducible if  $c$  is not decomposable as a union.

Clearly  $A_n^d$  is equal to  $C(X)$  if  $X$  is the Fermat variety of degree  $d$  and dimension  $n$ , and if  $X$  is any diagonal variety of the same dimension and degree, then  $C(X) \subset A_n^d$ .

The contraction is defined such that we have

$$J_q^d(c \vee c') = \pm J_q^d(c) J_q^d(c') \quad (3.18)$$

by (3.13), where the sign equals

$$J_q^d((c_{n+1}, c'_0)) = (-1)^{c_{n+1}(q-1)/d}. \quad (3.19)$$

The union is defined such that (3.12) can be written as

$$J_q^d(c \cup c') = q J_q^d(c) J_q^d(c'). \quad (3.20)$$

For later use, we investigate how the Gauss sums transform if we extend the base field from  $\mathbb{F}_q$  to  $\mathbb{F}_{q^s}$  for some  $s$ . For such an extension, there are two fundamental maps from  $\mathbb{F}_{q^s}$  to  $\mathbb{F}_q$ : the trace (which is additive) and the norm (which is multiplicative on  $\mathbb{F}_q^*$ ). They are defined by

$$\mathrm{Tr}(x) := x + x^q + \dots + x^{q^{s-1}} \quad (3.21)$$

$$\mathrm{Nr}(x) := x^{1+q+\dots+q^{s-1}}. \quad (3.22)$$

These functions allow us to pull characters on  $\mathbb{F}_q$  back to  $\mathbb{F}_{q^s}$ . The relation of the corresponding Gauss sums is given by Davenport and Hasse [7].

**Theorem 3.9** (*Davenport-Hasse*) *Let  $\chi$  be a character of  $\mathbb{F}_q^*$ , and let  $\psi$  be an additive character of  $\mathbb{F}_q$ . Then we have*

$$g_{q^s}(\mathrm{Nr}^* \chi, \mathrm{Tr}^* \psi) = g_q(\chi, \psi)^s. \quad (3.23)$$

**Corollary 3.10** *If  $q \equiv 1 \pmod{d}$  we have*

$$J_{q^s}^d(c, \mathrm{Nr}^*(\chi)) = J_q^d(c, \chi)^s. \quad (3.24)$$

This follows at once using (3.10).

There is also a relation connecting Jacobi sums of different degree. Suppose we have a  $c \in (\mathbb{Z}/d\mathbb{Z})^{n+2}$  with a common divisor  $d'$  of all  $c_i$  and  $d$ . Then  $c/d' \in (\mathbb{Z}/(d/d')\mathbb{Z})^{n+2}$ , and it is immediate from Definition 3.1 that

$$J_q^d(c, \chi) = J_q^{d/d'}(c/d', \chi^{d'}). \quad (3.25)$$

### 3.3 The zeta function

The zeta function  $Z_q(X, t)$  of a variety  $X$  defined over  $\mathbb{F}_q$  is a generating function for the numbers of points of  $X$  over finite fields  $\mathbb{F}_{q^s}$  for all  $s$ ; it is defined by

$$Z_q(X, t) := \exp\left(\sum_{s=1}^{\infty} \frac{1}{s} |X(\mathbb{F}_{q^s})| t^s\right), \quad (3.26)$$

The zeta function contains arithmetical information about  $X$ , but also information about its cohomology and the Galois representations associated thereto. The Galois representations appear as follows. Consider a proper algebraic variety  $X$  over a field  $k$  and let  $\bar{X} = X \otimes_k \bar{k}$  be the fibre of this variety over an algebraic closure of  $k$ . Take any prime  $\ell$  unequal to the characteristic of  $k$  and fix an integer  $i$ . Then we can define  $\ell$ -adic cohomology groups  $H^i(\bar{X}, \mathbb{Q}_\ell) = H_{\text{ét}}^i(\bar{X}, \mathbb{Q}_\ell)$ , where  $\mathbb{Q}_\ell$  is the field of  $\ell$ -adic numbers.

The precise definition of these cohomology groups requires use of the étale topology; it was developed by Grothendieck [1]. See Milne [31] for a more introductory text. The étale cohomology has the usual properties like the cup-product. If  $X$  is smooth and proper, we also have Poincaré duality; and if  $X$  is defined over a number field we have the comparison theorem  $H^i(\bar{X}, \mathbb{Q}_\ell) \otimes \mathbb{C} \cong H^i(X_h, \mathbb{C})$  where  $X_h$  is the complex manifold associated to  $X$ .

The property of  $\ell$ -adic cohomology that we need here is the Lefschetz fixed point formula, which is also proved by Grothendieck. Suppose  $X$  is defined over  $\mathbb{F}_q$  and let  $F_q$  be the  $q$ -th power Frobenius morphism, acting on  $X_{\mathbb{F}_q}$  by  $X_i \rightarrow X_i^q$ . Then

$$|X(\mathbb{F}_q)| = \sum_{i=0}^{2n} (-1)^i \text{Tr}(F_q; H^i(X \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q, \mathbb{Q}_\ell)). \quad (3.27)$$

This formula relates the action of the Galois group via the Frobenius elements to the cohomology of  $X$ . By using some standard relations between traces and determinants, it follows that

$$Z_q(X, t) = \prod_{i=0}^{2n} \det(1 - tF_q | H^i(\bar{X}, \mathbb{Q}_\ell))^{(-1)^{i-1}}. \quad (3.28)$$

We abbreviate

$$P^i(X, t) := \det(1 - tF_q | H^i(\bar{X}, \mathbb{Q}_\ell)). \quad (3.29)$$

This is the characteristic polynomial of the inverse of  $F_q$ . This inverse is usually called a geometric Frobenius element, whereas  $F_q$  itself is called an arithmetic Frobenius element.

Deligne [8] proved the following important theorem about the properties of the  $P^i(X, t)$ . It is known as the Riemann hypothesis for finite fields.

**Theorem 3.11** (*Deligne*) *Let  $X$  be a smooth and proper variety of dimension  $n$  defined over the finite field  $\mathbb{F}_q$ , and let  $\bar{X}$  be its fibre over an algebraic closure of  $\mathbb{F}_q$ . Let  $F_q$  be the  $q$ -th power Frobenius map, and choose a prime  $\ell$  unequal to  $\text{char}(\mathbb{F}_q)$ . Then for any  $0 \leq i \leq 2n$ , the characteristic polynomial  $P^i(X, t) =$*

$\det(1 - tF_q; H^i(\bar{X}, \mathbb{Q}_\ell))$  has integer coefficients which are independent of  $\ell$ , and all its roots have absolute value  $q^{-i/2}$ .

As we know, Poincaré duality provides isomorphisms between  $H^i(X, \mathbb{Q}_\ell)$  and  $H^{2n-i}(X, \mathbb{Q}_\ell)$ . This duality is duly reflected in the zeta function. It satisfies the functional equation

$$Z_q(X, \frac{1}{q^nt}) = \pm q^{n\chi(X)/2} t^{\chi(X)} Z_q(X, t). \quad (3.30)$$

Here  $\chi(X)$  is the Euler characteristic. The functional equation shows that for every root (resp. pole)  $\alpha$  of  $Z_q(X, t)$  with absolute value  $|\alpha| = q^{-i/2}$  there is a matching root (resp. pole)  $\alpha q^{i-n}$ , which is Poincaré duality for the zeta function.

The connection between the roots and poles of  $Z_q(X, t)$  and the numbers of points  $|X(\mathbb{F}_{q^s})|$  is very direct. Let us denote the set of inverses of roots of  $P^i(X, t)$  (or equivalently, the eigenvalues of  $F_q$  on  $H^i(\bar{X}, \mathbb{Q}_\ell)$ ) by  $A_i$ . Then we have

$$Z_q(X, t) = \prod_{i=0}^{2n} \prod_{\alpha \in A_i} (1 - \alpha t)^{(-1)^{i+1}}. \quad (3.31)$$

The number of points is easily found from (3.26):

$$|X(\mathbb{F}_{q^s})| = \sum_{i \text{ even}} \sum_{\alpha \in A_i} \alpha^s - \sum_{i \text{ odd}} \sum_{\alpha \in A_i} \alpha^s. \quad (3.32)$$

If  $Z_q(X, t)$  is known,  $Z_{q^s}(X, t)$  can be deduced; clearly

$$Z_{q^s}(X, t) = \prod_{i=0}^{2n} \prod_{\alpha \in A_i} (1 - \alpha^s t)^{(-1)^{i-1}} \quad (3.33)$$

as can be checked from (3.32).

As an example, consider the case of a smooth elliptic curve  $E$  defined over  $\mathbb{Q}$ , and let  $p$  be a prime such that  $E$  has good reduction over  $p$ . Then from (3.28) and Deligne's theorem we see that the zeta function has the form

$$Z_p(E, t) = \frac{1 - a_p t \pm pt^2}{(1 \pm t)(1 \pm pt)} \quad (3.34)$$

where  $a_p$  is an integer. By applying the functional equation and the fact that  $|E(\mathbb{F}_{p^s})|$  is nonnegative for all  $s$  we can determine the signs;

$$Z_p(E, t) = \frac{1 - a_p t + pt^2}{(1 - t)(1 - pt)}. \quad (3.35)$$

The coefficient  $a_p$  is the only thing that depends on  $E$ . By counting the points of  $E(\mathbb{F}_p)$  we can determine its value; then the numbers  $|E(\mathbb{F}_{p^s})|$  are generated by the zeta function.

The factors  $1 - t$  and  $1 - pt$  in the denominator of (3.35) are typical; similar factors occur in the zeta function of any smooth and proper projective variety  $X \subset \mathbb{P}(w)$  of dimension  $n$ . In that case the cohomology of  $\mathbb{P}(w)$ , which is generated by the hyperplane class  $H$ , is injected into the cohomology of  $X$ . On this class a geometric Frobenius element acts by multiplication by  $q$ , as can be checked easily in the projective space. So we see that the cohomology class generated by the  $i$ -th power of the hyperplane class produces a factor  $1 - q^i t$  in  $P^{2i}(X, t)$ .

### 3.4 Weil's formula

After these preliminaries, we return to the hypersurface defined by the diagonal equation

$$\sum_{i=0}^{n+1} a_i X_i^{e_i} = 0 \quad (3.36)$$

in the weighted projective space  $\mathbb{P}(w_0, \dots, w_{n+1})$ . Since we have chosen integral coefficients  $a_i$ , we can consider the reduction  $X(\mathbb{F}_q)$  of  $X$  to the finite field with  $q$  elements; we write  $q = p^m$  with  $p$  prime. To count the number of points of this reduced variety, we use a method devised by André Weil [47]. We can write

$$|X(\mathbb{F}_q)| = \frac{1}{q-1} \sum_u N_{e_0}(u_0) N_{e_1}(u_1) \dots N_{e_{n+1}}(u_{n+1}), \quad (3.37)$$

where the sum is taken over nonzero  $u \in (\mathbb{F}_q)^{n+2}$  such that  $\sum a_i u_i = 0$  and  $N_e(x)$  denotes the number of solutions to  $x^e = u$  in  $\mathbb{F}_q$ .

As in the case of an ordinary projective space, we find the number of points in weighted projective space from the number of points in affine space. In the projective case it is obvious that we must divide by  $q-1$  to do this; in a weighted projective space  $\mathbb{P}(w_0, \dots, w_{n+1})$  it is not quite, since the orbit of a point  $x = (x_0, \dots, x_{n+1})$  under the natural action of  $\mathbb{F}_q^*$  by

$$\lambda \cdot x = (\lambda^{w_0} x_0, \dots, \lambda^{w_{n+1}} x_{n+1}) \quad (3.38)$$

does not always have length  $(q-1)$ . In fact, if  $g(x)$  is the gcd of  $(q-1)$  and the weights  $w_i$  for which  $x_i \neq 0$ , then the length of this orbit of  $x$  is  $(q-1)/g(x)$ . However, for such points we must modify the action of  $\mathbb{F}_q^*$  to

$$\lambda \cdot x = (\lambda^{w_0/g(x)} x_0, \dots, \lambda^{w_{n+1}/g(x)} x_{n+1}) \quad (3.39)$$

which has length  $q-1$ . If  $f$  is a homogeneous polynomial in the weighted projective variables of degree  $d$ , then this action will still preserve the zero-set of  $f$ , since  $f(\lambda \cdot x) = \lambda^{d/g(x)} f(x)$ . The same holds for all elements of the coordinate ring of  $\mathbb{P}(w_0, \dots, w_{n+1})$ . Therefore, the orbit of  $x$  under the modified action should be mapped to one point in the weighted projective space; so the factor  $1/(q-1)$  is exactly right.

Since  $\mathbb{F}_q^*$  is a cyclic group of order  $q-1$ , the map  $x \rightarrow x^e$  is a group automorphism for any  $e$  with  $(e, q-1) = 1$ . For the purpose of counting points, we can

use such maps for reparametrisation of the  $X_i$ . Therefore we can assume that  $e_i|(q-1)$  for every  $i$ , if we are interested in  $|X(\mathbb{F}_q)|$  only. To calculate the zeta function we will also want to know  $|X(\mathbb{F}_{q^s})|$  for all  $s$ ; in that case things are a bit more complicated, since the reparametrisations are dependent on  $s$ . We ignore this for the time being and assume that  $e_i|(q-1)$  for all  $i$ , and hence  $d|(q-1)$ .

If we pick a character  $\chi$  of  $\mathbb{F}_q^*$  of order  $e|(q-1)$ , we can write

$$N_e(u) = \sum_{\alpha=0}^{e-1} \chi^\alpha(u) \quad (3.40)$$

(we use the convention that  $\chi^i(0) = 0$  if  $i$  is not divisible by the order of  $\chi$ , but  $\chi^i(0) = 1$  if it is.) We now pick a single character  $\chi$  of order  $d$ , and define characters  $\chi_i = \chi^{d/e_i}$  of order  $e_i$ . Then we can rewrite the expression (3.37). We let  $H = \{u \in \mathbb{F}_q^{n+2} : \sum_i u_i = 0\}$ . Then (3.37) becomes

$$\begin{aligned} (q-1)|X(\mathbb{F}_q)| &= \sum_{u \in H} \prod_{j=0}^{n+1} N_{e_j}(a_j^{-1}u_j) - 1 \\ &= \sum_{u \in H} \sum_{0 \leq \alpha_i < e_i} \chi_0^{\alpha_0}(a_0^{-1}u_0) \cdots \chi_{n+1}^{\alpha_{n+1}}(a_{n+1}^{-1}u_{n+1}) - 1. \end{aligned} \quad (3.41)$$

The  $-1$  removes the zero solution. Now if one of the  $\alpha_i$  (say  $\alpha_0$ ) is zero, then the remaining sum factors as a product

$$\prod_{i=1}^{n+1} \left( \sum_{0 \leq \alpha_i < e_i} \sum_{u_i \in \mathbb{F}_q} \chi_i^{\alpha_i}(a_i^{-1}u_i) \right) \quad (3.42)$$

and each of the factors will be nonzero only if  $\alpha_i = 0$ , in which case it equals  $q$ . So we can separate the contribution of the  $\alpha$  with zero components to find

$$|X(\mathbb{F}_q)| = \frac{q^{n+1} - 1}{q - 1} + (-1)^n \sum_{0 < \alpha_i < e_i} J_q^d\left(\left(\frac{d}{e_0}\alpha_0, \dots, \frac{d}{e_{n+1}}\alpha_{n+1}\right), \chi\right) \prod_{j=0}^{n+1} \bar{\chi}_j^{\alpha_j}(a_j) \quad (3.43)$$

This formula relates the number of points directly to the Jacobi sums defined in section 3.2. Since  $d|q^s - 1$  for any  $s$ , we can do the same calculation for  $|X(\mathbb{F}_{q^s})|$ . So

$$|X(\mathbb{F}_{q^s})| = \frac{q^{s(n+1)} - 1}{q^s - 1} + (-1)^n \sum_{0 < \alpha_i < e_i} J_{q^s}^d\left(\left(\frac{d}{e_0}\alpha_0, \dots, \frac{d}{e_{n+1}}\alpha_{n+1}\right), \chi_s\right) \prod_{i=0}^{n+1} \bar{\chi}_i^{\alpha_i}(a_i) \quad (3.44)$$

where  $\chi_s : \mathbb{F}_{q^s}^* \rightarrow \mathbb{C}^*$  is a character of order  $d$ . Now we apply Theorem 3.9; we choose  $\chi_s$  equal to  $\text{Nr}^* \chi$  (which has the right order), and we find that

$$\begin{aligned} |X(\mathbb{F}_{q^s})| &= 1 + q^s + \dots + q^{ns} + \\ &\quad (-1)^n \sum_{\alpha_i: 0 < \alpha_i < e_i} \prod_{i=0}^{n+1} \bar{\chi}_i^{s\alpha_i}(a_i) J_q^d\left(\left(\frac{d}{e_0}\alpha_0, \dots, \frac{d}{e_{n+1}}\alpha_{n+1}\right), \chi\right)^s \end{aligned} \quad (3.45)$$

Note that  $\chi_s(a_i)$  is equal to  $\chi(a_i^s) = \chi(a_i)^s$  since  $a_i \in \mathbb{F}_q$ ; this is a property of the norm.

In (3.45), we have succeeded in writing the number of points  $|X(\mathbb{F}_{q^s})|$  as a sum of the form (3.32). The following theorem is an immediate consequence. We abbreviate again  $\chi(a)^c = \prod_{i=0}^{n+1} \chi(a_i)^{c_i}$ .

**Theorem 3.12** (Weil) *Let  $X$  be the diagonal hypersurface over  $\mathbb{Z}$  defined by the equation  $\sum_{i=0}^{n+1} a_i X_i^{e_i} = 0$  in weighted projective space  $\mathbb{P}(w_0, \dots, w_{n+1})$  (where  $w_i = d/e_i$  and  $d = \text{lcm}(\{e_i\})$ ), let  $q$  be a prime power and assume that  $e_i | (q-1)$  for all  $i$ . Then the zeta function  $Z_q(X, t)$  is given by*

$$Z_q(X, t) = \frac{\prod_{c \in C} (1 - \bar{\chi}(a)^c J_q^d(c, \chi) t)^{(-1)^{n-1}}}{(1-t)(1-qt) \dots (1-q^n t)}. \quad (3.46)$$

where  $\chi$  is a character of order  $d$  of  $\mathbb{F}_q^*$ ,  $a = (a_0, \dots, a_{n+1})$ , and  $C = C(X)$  is the set

$$C(X) := \{c \in (\mathbb{Z}/d\mathbb{Z})^{n+2} \mid \sum_i c_i \in d\mathbb{Z} \text{ and } \forall i : e_i c_i \in d\mathbb{Z}, 0 < c_i < d\}. \quad (3.47)$$

In (3.46) we recognise the factors  $1 - q^i t$  produced by the hyperplane class and its powers. The other factors in zeta function are described by the Jacobi sums. Each of them has absolute value  $q^{n/2}$  by Lemma 3.5 and corresponds to an eigenvector in the cohomology of  $X$ . Since  $X$  is a hypersurface, the middle cohomology is the only space available.

So we have for  $0 \leq j \leq 2n$ :

$$\beta_j(X) = \begin{cases} |C| + 1 & \text{if } j = n \text{ is even} \\ |C| & \text{if } j = n \text{ is odd} \\ 1 & \text{if } j \neq n \text{ and } j \text{ even} \\ 0 & \text{if } j \neq n \text{ and } j \text{ odd.} \end{cases} \quad (3.48)$$

Note that these are the Betti numbers of the possibly singular variety; they will be modified if we resolve singularities (see Section 2.4).

The appearance of the set  $C$  is in fact quite natural; we have seen it before in Section 2.5, where it was used to give a basis for the middle primitive cohomology  $PH^n(X)$ . The set  $C$  can also be interpreted as a subset of the dual group of the group that acts on  $X$  by multiplication with roots of unity. Recall the definition of the group  $G$  in (3.2):

$$G := \{(\zeta^{b_0}, \dots, \zeta^{b_{n+1}}) \mid \forall i : b_i e_i \equiv 0 \pmod{d}\} / \langle (\zeta^{w_0}, \dots, \zeta^{w_{n+1}}) \rangle \quad (3.49)$$

The dual or character group can be identified with

$$\hat{G} = \{c \in (\mathbb{Z}/d\mathbb{Z})^{n+2} \mid c_i e_i \equiv 0 \pmod{d} \text{ and } \sum_i c_i e_i \equiv 0 \pmod{d}\} \quad (3.50)$$

with the pairing

$$\langle c, (\zeta^{b_0}, \dots, \zeta^{b_{n+1}}) \rangle = \prod_i \zeta^{b_i c_i / w_i}. \quad (3.51)$$

Obviously  $C(X) \subset \hat{G}$ .

Weil's formula implies that the eigenvalues of the Frobenius element are algebraic combinations of  $(q-1)$ -th roots of unity. This allows us to determine the action of the Galois group on the eigenvalues explicitly.

**Theorem 3.13** *Let  $X$  be the diagonal hypersurface over  $\mathbb{Z}$  defined by the equation  $\sum_{i=0}^{n+1} a_i X_i^{e_i} = 0$  in weighted projective space  $\mathbb{P}(w_0, \dots, w_{n+1})$  (where  $w_i = d/e_i$  and  $d = \text{lcm}(\{e_i\})$ ), let  $q$  be a prime power and assume that  $e_i | (q-1)$  for all  $i$ . Then the action of the Galois group on the roots of  $Z_q(X, t)$  is equivalent to the action of the group  $(\mathbb{Z}/d\mathbb{Z})^*$  on  $C$  by multiplication modulo  $d$ . Denote the orbit of an element  $c \in C$  under this action by  $\bar{c}$ , and the quotient space  $C/(\mathbb{Z}/d\mathbb{Z})^*$  by  $\bar{C}$ . Then*

$$Z_q^d(\bar{c}, t) := \prod_{c \in \bar{c}} \left(1 - \bar{\chi}\left(a, \frac{(q-1)c}{d}\right) J_q^d(c, \chi) t\right) \quad (3.52)$$

is a polynomial with integer coefficients which is independent of the choice of  $\chi$ , and

$$Z_q(X, t) = \frac{\left(\prod_{\bar{c} \in \bar{C}} Z_q^d(\bar{c}, t)\right)^{(-1)^{n-1}}}{(1-t)(1-qt) \dots (1-q^n t)} \quad (3.53)$$

is a factorisation of the zeta function over  $\mathbb{Z}[t]$ . This implies that  $Z_q(X, t)$  factors over the integers into factors of degree  $\phi(d) = |(\mathbb{Z}/d\mathbb{Z})^*|$  or less.

**Proof** We know that the Galois group acting on the set of characters of order  $d$  is  $(\mathbb{Z}/d\mathbb{Z})^*$  acting by powers. From the definition of the Jacobi sum it is clear that  $\chi \rightarrow \chi^g$  is equivalent to  $c \mapsto gc \pmod{d}$  for a  $g \in (\mathbb{Z}/d\mathbb{Z})^*$ . The same holds for the factors  $\bar{\chi}(a, c)$ . Therefore the coefficients of  $Z_q^d(\bar{c}, t)$  are just symmetric polynomials in the Galois conjugates of  $\bar{\chi}(a, c) J_q^d(c, \chi)$ , hence invariant. Since the polynomial has 0-th order coefficient 1 and is a factor of the entire zeta function, this means it must be in  $\mathbb{Z}[t]$ .  $\square$

The cohomology of diagonal varieties has been studied before; especially the Fermat varieties have been a subject of investigation. The diagonal variety  $X$  can be obtained as a quotient of the twisted Fermat variety  $F(a)$  defined in  $\mathbb{P}^{n+1}$  by

$$\sum_{i=0}^{n+1} a_i X_i^d = 0,$$

so the cohomology of  $X$  is contained in that of  $F(a)$ .

Deligne [10] calculated the cohomology of a Fermat hypersurface of arbitrary dimension and degree. He considered only the case where all coefficients are equal to 1, but more general coefficients can easily be taken into account; see for example Gouvêa and Yui [17]. Deligne showed that the cohomology  $H_{\text{ét}}^n(F(a), \mathbb{Q}_\ell)$  decomposes into 1-dimensional subrepresentations under the action of the symmetry group  $G$ . These are the characters defined by the elements  $c \in C(X) \subset \hat{G}$  in our notation.

The group  $G$  is defined using a  $d$ -th root of unity  $\zeta$ , on which the Galois group  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  acts nontrivially; therefore the subrepresentations under the action of  $G$  are no subrepresentations for the Galois group. However, on a character  $\chi^c$  of  $G$  occurring in  $H_{\text{ét}}^n(X, \mathbb{Q}_\ell)$  the group  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta))$  acts trivially, so the action of the full Galois group on  $\chi^c$  is described by the small group  $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/d\mathbb{Z})^*$ . Therefore the orbit of  $\chi^c$  under this group generates a subrepresentation in  $H_{\text{ét}}^n(F(a), \mathbb{Q}_\ell)$  of both  $G$  and  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  (and in fact of the semi-direct product of these)<sup>1</sup>.

So we see that the middle cohomology decomposes into representations that are induced by characters. This means their  $L$ -series have good properties. More on this in Chapter 5, where we discuss modular forms.

### 3.5 Zeta functions for all good primes

Up to this point, we have dealt mainly with the case that  $d|(q-1)$ . Eventually we will need to calculate zeta functions for all  $q$ . They can be found via counting points using the methods above;

$$|X(\mathbb{F}_q)| = |\tilde{X}_q(\mathbb{F}_q)| \quad (3.54)$$

where we define  $\tilde{X}_q$  to be the variety with the equation

$$\sum_{i=0}^{n+1} a_i X_i^{(q-1, e_i)} = 0. \quad (3.55)$$

This follows from the fact that the map  $x \mapsto x^e$  is a permutation of  $\mathbb{F}_q$  if  $(e, q-1) = 1$ . We see immediately that the degree of  $\tilde{X}_q$  equals  $(q-1)d$ . This degree divides  $q-1$ , so the number of points  $|X_q(\mathbb{F}_{q^s})|$  can be calculated by the methods of the previous section. In this way we can calculate  $|X(\mathbb{F}_{q^s})|$  for any  $s$  and calculate the zeta function  $Z_q(X, T)$  for any  $X$ . Following this procedure leads to a formula to construct  $Z_p(X, t)$  by some simple substitutions.

**Theorem 3.14** *Let  $X$  be the diagonal hypersurface over  $\mathbb{Z}$  defined by the equation  $\sum_{i=0}^{n+1} a_i X_i^{e_i} = 0$  in weighted projective space  $\mathbb{P}(w_0, \dots, w_{n+1})$  (where  $w_i = d/e_i$  and  $d = \text{lcm}(\{e_i\})$ ) and let  $q$  be a prime power with  $(q, d) = 1$ . Define for any  $c \in C(X)$  the order  $\text{ord}(c)$  to be the smallest  $r > 0$  such that  $(q^r - 1)c \equiv 0 \pmod{d}$ . Then*

$$Z_q^d(X, t) = \frac{\left( \prod_{\bar{c} \in \bar{C}} Z_{q^{\text{ord}(\bar{c})}}(\bar{c}, a, t^{\text{ord}(\bar{c})})^{1/\text{ord}(\bar{c})} \right)^{(-1)^{n-1}}}{(1-t)(1-qt) \dots (1-q^nt)} \quad (3.56)$$

and each of the factors in the product is a polynomial in  $\mathbb{Z}[t]$ .

**Proof** For any  $s$  the variety  $\tilde{X}_{q^s}$  has degree  $\tilde{d} := \text{lcm}(\{(q^s - 1, e_i)\}) = (q^s - 1, \text{lcm}\{e_i\}) = (q^s - 1, d)$ ; so the set  $C(\tilde{X}_{q^s})$  is by definition a subset of  $(\mathbb{Z}/\tilde{d}\mathbb{Z})^{n+2}$ .

<sup>1</sup>Thanks to professor Edixhoven for pointing this out

However, there is a canonical injection into  $C(X)$  via  $c \mapsto dc/\tilde{d}$ , and its image consists of all the  $c \in C(X)$  such that  $d/\tilde{d}$  divides all  $c_i$ . Hence we have

$$\begin{aligned} |X(\mathbb{F}_{q^s})| &= |\tilde{X}_{q^s}(\mathbb{F}_{q^s})| \\ &= 1 + q^s + \dots + q^{sn} + (-1)^n \sum_{c \in C(X): d|\tilde{d}c} \bar{\chi}(a)^c J_{q^s}^d(c, \chi) \end{aligned} \quad (3.57)$$

So we see that an element  $c$  gives a nonzero contribution to the number of points if and only if  $d/\tilde{d}$  divides  $\gcd(\{c^i\}, d)$ , that is, if  $d|(q^s - 1)c$ . Hence the appearance of the order  $\text{ord}(c)$  in the formula.

Here we take a fixed character  $\chi : \mathbb{F}_{q^{\text{ord}(c)}} \rightarrow \mathbb{C}$  of order  $d$ , and we compose it with the norm from  $\mathbb{F}_{q^{s \cdot \text{ord}(c)}} \rightarrow \mathbb{F}_{q^{\text{ord}(c)}}$  to form characters  $\chi_s$  of the right order from  $\mathbb{F}_{q^{s \cdot \text{ord}(c)}}$  to  $\mathbb{C}$ .

We want to separate the contribution of an orbit  $\bar{c}_0$  under the action of  $(\mathbb{Z}/d\mathbb{Z})^*$ . Therefore we define

$$N(\bar{c}, q^s) = \begin{cases} (-1)^n \sum_{c' \in \bar{c}} \bar{\chi}_s(a)^{c'} J_{q^s}^d(c', \chi) & \text{if } \text{ord}(c)|s \\ 0 & \text{otherwise.} \end{cases} \quad (3.58)$$

so that for any  $s$ ,

$$|X(\mathbb{F}_{q^s})| = 1 + q^s + \dots + q^{ns} + \sum_{\bar{c} \in \bar{C}(X)} N(\bar{c}, q^s). \quad (3.59)$$

With this expression we can calculate the factor in the zeta function generated by an orbit  $\bar{c}$ . We abbreviate  $r := \text{ord}(c)$ . Notice that we insert an extra factor  $(-1)^n$  to ensure that the factor  $Z_q(\bar{c}, t)$  will be a polynomial in  $t$  rather than a rational function.

$$\begin{aligned} Z_q(\bar{c}, t) &:= \exp \sum_s \frac{(-1)^n}{s} N(\bar{c}, q^s) t^s \\ &= \exp \sum_s \frac{(-1)^n}{rs} N(\bar{c}, q^{rs}) t^{rs} \\ &= \exp \left( (-1)^n \sum_s \frac{1}{s} N(\bar{c}, q^{rs}) (t^r)^s \right)^{1/r} \\ &= \exp \left( \sum_{c' \in \bar{c}} \sum_s \frac{1}{s} \bar{\chi}_s(a)^{c'} J_{q^r}^d(c')^s (t^r)^s \right)^{1/r} \\ &= \prod_{c' \in \bar{c}} (1 - \bar{\chi}(a, c') J_{q^r}^d(c', \chi) t^r)^{1/r} \\ &= Z_{q^r}(\bar{c}, t^r)^{1/r}. \end{aligned} \quad (3.60)$$

The full zeta function then satisfies

$$\begin{aligned}
 Z_q(X, t) \prod_{i=0}^n (1 - q^i t) &= \exp \left( \sum_s \sum_{\bar{c} \in \bar{C}(X)} \frac{1}{s} N(\bar{c}, q^s) t^s \right) \\
 &= \prod_{\bar{c} \in \bar{C}} \exp \left( \sum_s \frac{1}{s} N(\bar{c}, q^s) t^s \right) \\
 &= \prod_{\bar{c} \in \bar{C}} \left( Z_{q^{\text{ord}(c)}}(\bar{c}, t^{\text{ord}(c)})^{1/\text{ord}(c)} \right)^{(-1)^n}, \quad (3.61)
 \end{aligned}$$

as required.

Finally, we need to show that the roots of the polynomials exist in  $\mathbb{Z}[t]$ . To do this, we will show that each root of the polynomial  $Z_{q^{\text{ord}(c)}}(\bar{c}_0, t)$  occurs with multiplicity  $\text{ord}(c)$  (or a multiple). This can be done by using the Gross-Koblitz formula introduced later on, but it is not difficult to see that

$$J_q^d(c, \chi) = J_q^d(p c, \chi) \quad (3.62)$$

(with  $q = p^{\text{ord}(c)}$ ) from the definition. We have

$$\begin{aligned}
 J_q^d(p c, \chi) &= \frac{(-1)^n}{q-1} \sum_{\sum x_i=0} \prod_i \chi(x_i)^{p c_i} \\
 &= \frac{(-1)^n}{q-1} \sum_{\sum x_i^q=0} \prod_i \chi(x_i^p)^{c_i} \\
 &= \frac{(-1)^n}{q-1} \sum_{\sum x_i^{q/p}=0} \prod_i \chi(x_i)^{c_i} \\
 &= J_q^d(c, \chi) \quad (3.63)
 \end{aligned}$$

since the conditions  $\sum x_i^{q/p} = 0$  and  $\sum x_i = 0$  are the same in  $\mathbb{F}_q$ . Hence the Jacobi sums  $J_q^d(c, \chi)$  are constant on the orbit of  $c$  under the action of the subgroup generated by  $p$  in  $(\mathbb{Z}/d\mathbb{Z})^*$ . The length of this orbit is clearly  $\text{ord}(c)$ . Also  $\bar{\chi}(a)^c$  is constant on this orbit, since the coefficients  $a_i$  are integers and hence  $a_i^p = a_i$  in  $\mathbb{F}_q$ . So the roots  $\bar{\chi}(a, c) J_q^d(c, \chi)$  occur with multiplicity  $\text{ord}(c)$  or a multiple of this.  $\square$

Of course, the definition of  $Z_p(\bar{c}_0, t)$  in (3.60) is in agreement with the one given for  $Z_q(\bar{c}_0, t)$  in Theorem 3.13, which was only applicable if  $d|q-1$ . The theorem allows us to find  $Z_p(X, t)$  for all good primes, from which the other zeta functions follow.

As an example, we treat the case  $n = 0$ . Fix a degree  $d > 1$ , an odd prime  $p$  with  $(p, d) = 1$  and a  $c = (c_0, -c_0)$  with  $c_0 \in (\mathbb{Z}/d\mathbb{Z})^*$ . Choose  $m$  equal to the

order of  $p$  in  $(\mathbb{Z}/d\mathbb{Z})^*$ . Then

$$Z_p^d(c, t) = \prod_{g \in (\mathbb{Z}/d\mathbb{Z})^*} (1 - (-1)^{g(p^m-1)/d} t^m)^{1/m} \quad (3.64)$$

since the  $c_0$  can just be absorbed in the  $g$ . Now if  $d$  is even, then all  $g$  are odd and hence all factors are equal. In that case

$$Z_p^d(c, t) = (1 - (-1)^{(p^m-1)/d} t^m)^{\phi(d)/m}. \quad (3.65)$$

If  $d$  is odd, then we clearly have

$$Z_p^d(c, t) = (1 - t^m)^{\phi(d)/m}. \quad (3.66)$$

If  $p = 2$ , then the Jacobi sums are trivial. So we just have

$$Z_2^d(c, t) = (1 - t^m)^{\phi(d)/m}. \quad (3.67)$$

## 3.6 Splitting the cohomology

From Theorems 3.13 and 3.14 it seems likely that an orbit  $\bar{c} \in \bar{C}$  corresponds to a Galois representation  $\rho_c$  of rank equal to the length of the orbit, with characteristic polynomials  $Z_q(\bar{c}, t)$  of the inverse Frobenius elements  $F_q^{-1}$ . To justify this conclusion we have to do more than counting points, as we have done so far; we need to decompose the cohomology  $H^n(X, \mathbb{Q}_\ell)$  into invariant subspaces under the Galois action.

We consider again the group of automorphisms  $G(X)$  defined in (3.49). Given a character  $c \in \hat{G}$ , we study the subgroup  $G_c \subset G$  that is sent to 1 by  $c$ .

$$G_c = \ker(c) = \{g \in G \mid c(g) = 1\}. \quad (3.68)$$

This subgroup is invariant under the action of  $(\mathbb{Z}/d\mathbb{Z})^*$  on  $c$ ; in fact  $G_c \subset G_{ac}$  for any integer  $a$ . So we will consider the quotient of  $X$  by this subgroup. By its definition,  $G_c$  acts trivially on the monomial  $\prod_i X_i^{e_i c_i/d}$  and its Galois conjugates; so the part of cohomology associated to them will be preserved under this quotient.

**Lemma 3.15** *The quotient  $X/G_c$  is given by two equations in  $\mathbb{P}^{n+2}$ :*

$$\sum_{i=0}^{n+1} a_i Y_i = 0; \quad Y_{n+2}^d = \prod_{i=0}^{n+1} Y_i^{c_i}. \quad (3.69)$$

This result was stated with out proof in [17].

**Proof** This is a standard calculation; we need to find the invariant subring under the action by  $G_c$ . By construction it contains the monomials  $X_i^{e_i}$  (identified with  $Y_i$ ) and  $\prod_i X_i^{g c_i e_i/d}$  (for any  $g \in \mathbb{Z}/d\mathbb{Z}$ ), which we name  $Y_{i+1+g}$ . Then we have relations  $Y_{i+1+g}^d = \prod_{i=0}^{n+1} Y_i^{g c_i}$ . Elimination of as many variables as possible produces the equations given.

We need to check that there are no other monomials that are invariant under  $G_c$  than the  $Y_i$  defined above. To do this, we use the structure theorem for finite abelian groups to decompose  $G$  as

$$G = \bigoplus_{i=0}^k \mathbb{Z}/t_i\mathbb{Z} \quad (3.70)$$

with each  $t_i$  equal to a prime power. Clearly  $t_i|d$  for all  $i$ . The dual group  $\hat{G}$  is isomorphic to  $G$ , with the pairing

$$G \times \hat{G} \rightarrow \mathbb{C}^* : (g, c) \rightarrow \zeta^{\sum_{i=0}^k c_i g_i d/t_i}. \quad (3.71)$$

The subgroup  $G_c$  equals

$$G_c = \{g \in G : \sum_{i=0}^k c_i g_i d/t_i \equiv 0 \pmod{d}\}. \quad (3.72)$$

We will consider each prime  $p$  dividing  $d$  separately. Suppose that  $t_i = p^{\alpha_i}$  (with  $\alpha_i > 0$ ) for  $i = 0 \dots m$  and  $(p, t_i) = 1$  for all other  $t$ , and let  $r := \text{ord}_p(d)$ . Then  $g \in G_c$  implies that

$$\sum_{i=0}^k c_i g_i d/t_i \equiv 0 \pmod{p^r} \iff \sum_{i=0}^m (c_i p^{r-\alpha_i}) g_i \equiv 0 \pmod{p^r}. \quad (3.73)$$

We need to keep track of all powers of  $p$ , so we call  $\beta_i = \text{ord}_p(c_i)$  and write  $c_i = p^{\beta_i} c'_i$  if needed. Now we can find an  $i \leq m$  (say  $i = 0$ ) such that  $r + \beta_i - \alpha_i$  is minimal. Then we can solve for  $g_0$ :

$$g_0 \equiv -(c'_0)^{-1} \sum_{i=1}^m g_i c'_i p^{\alpha_0 + \beta_i - \alpha_i - \beta_0} \pmod{p^{\alpha_0 - \beta_0}}, \quad (3.74)$$

where the inverse of  $c'_0$  is taken in  $\mathbb{Z}/p^{\alpha_0 - \beta_0}\mathbb{Z}$ . Since  $0 \leq \beta_0 < \alpha_0$ , we have at least one solution  $g_0$  for any choice of the other  $g_i$  ( $1 \leq i \leq m$ ).

Now consider an arbitrary  $\gamma \in \hat{G}$  that is invariant under  $G_c$ ; so we have

$$\sum_{i=0}^m \gamma_i g_i p^{r-\alpha_i} \equiv 0 \pmod{p^r} \quad (3.75)$$

for all  $g \in G_c$ . We need to prove that  $\gamma$  is a multiple of  $c$ . So we substitute the condition (3.74) that  $g \in G_c$  to find

$$\sum_{i=1}^m (\gamma_i - \gamma_0 (c'_0)^{-1} c'_i p^{\alpha_0 + \beta_i - \alpha_i - \beta_0}) g_i p^{r-\alpha_0} + \gamma_0 \delta p^{r-\beta_0} \equiv 0 \pmod{p^r}. \quad (3.76)$$

All  $g_i$  ( $1 \leq i \leq m$ ) can be chosen freely and independently; and the same holds for  $\delta$ , which parametrises all solutions  $g_0$ . Therefore the coefficients of  $g_i$  and  $\delta$

in (3.76) must vanish. For the term with  $\delta$ , this implies that  $\gamma_0 \equiv 0 \pmod{p^{\beta_0}}$ ; so we can write  $\gamma_0 = p^\lambda \gamma'_0$  with  $\lambda \geq \beta_0$ . Setting the coefficients of the  $g_i$  to zero, we find that

$$\gamma_i \equiv \gamma'_0 (c'_0)^{-1} c_i p^{\lambda - \beta_0} \pmod{p^{\alpha_i}} \quad (3.77)$$

for  $1 \leq i \leq m$ . But (3.77) also holds for  $i = 0$ , so we see that  $(\gamma_0, \dots, \gamma_m)$  is a multiple of  $(c_0, \dots, c_m)$  by  $f_p := \gamma'_0 (c'_0)^{-1} p^{\lambda - \beta_0} \in \mathbb{Z}/p^r \mathbb{Z}$ .

We can do this calculation for each prime  $p$ , and by the Chinese remainder theorem we can find an  $f \in \mathbb{Z}/d\mathbb{Z}$  such that  $f \equiv f_p \pmod{p^{\text{ord}_p(d)}}$  for all  $p$ . Then  $\gamma \equiv fc$  in  $G$ .  $\square$

We can calculate the zeta function of the quotient variety by counting points. For clarity, we only treat the case where the coefficients  $a_i$  are equal to 1. We let  $H := \{(Y_0, \dots, Y_{n+1}) \in \mathbb{F}_q^{n+2} : \sum_i Y_i = 0\}$  and  $H^* := H \cap (\mathbb{F}_q^*)^{n+2}$ . Then we have

$$|(X/G_c)(\mathbb{F}_q)| = \frac{1}{q-1} \left( \sum_{Y \in H} N_d \left( \prod_{i=0}^{n+1} Y_i^{c_i} \right) - 1 \right) \quad (3.78)$$

where we recall that  $N_d(y)$  is the number of solutions to  $x^d = y$  in  $\mathbb{F}_q$ . Reusing formula (3.40), we find that

$$\begin{aligned} |(X/G_c)(\mathbb{F}_q)| &= \frac{1}{q-1} \left( \sum_{j=1}^{d-1} \sum_{Y \in H^*} \prod_{i=0}^{n+1} \chi^j(Y_i^{c_i}) + q^{n+1} - 1 \right) \\ &= 1 + q + \dots + q^n + (-1)^n \sum_{j=1}^{d-1} J_q^d(jc, \chi), \end{aligned} \quad (3.79)$$

where  $\chi$  is again a character of order  $d$  on  $\mathbb{F}_q$ . Note that it may happen that  $d|jc_i$  for some  $j$  and  $i$ . In that case we use Lemma 3.2, showing that the entries that are  $0 \pmod{d}$  can be dropped from  $c$  in the Jacobi sum. We assume that  $\gcd(\{c_i\}, d) = 1$  so that the orbit of  $c$  has maximal length.

**Theorem 3.16** *Let  $c \in C(X)$  and assume that  $(d, q) = 1$  and  $\gcd(\{c_i\}, d) = 1$ . Then the quotient variety  $X/G_c$  has zeta function*

$$Z_q(X/G_c) = \left( \prod_{j|d, j \neq d} Z_q^d(\overline{j}c, t) \right)^{(-1)^n} / \prod_{i=0}^n (1 - q^i t) \quad (3.80)$$

This follows directly from the calculation of the number of points given above. We have split the set  $\{jc \mid 0 < j < d\}$  into orbits under the action of  $(\mathbb{Z}/d\mathbb{Z})^*$  to find the factorisation.

We see that the expected factor  $Z_q^d(\overline{j}c, t)$  occurs in the zeta function. The other factors correspond to parts of the cohomology that are invariant under larger subgroups than  $G_c$ ; they will occur already in diagonal varieties of lower degree. This opens the way to a proof by induction. But first, we have to make precise the relations between diagonal varieties of different degrees.

**Lemma 3.17** *Let  $X$  be a diagonal variety as before; let  $f_i$  be a divisor of  $e_i$  for all  $0 \leq i \leq n+1$ , and let  $X'$  be the diagonal variety with equation*

$$\sum_{i=0}^{n+1} a_i X_i^{e_i/f_i} = 0 \quad (3.81)$$

and degree  $d' = \text{lcm}(\{e_i/f_i\})$ . Then

$$X' \cong X/G_f(X), \quad (3.82)$$

where  $G_f$  is the subgroup of  $G(X)$  given by

$$G_f(X) = \{(\zeta^{b_0}, \dots, \zeta^{b_{n+1}}) \in G(X) : f_i | b_i\} / H \quad (3.83)$$

and  $H$  is the subgroup generated by  $(\zeta^{w_0}, \dots, \zeta^{w_{n+1}})$ . The zeta function of the quotient variety is

$$Z_q(X') = \left( \prod_{\bar{c} \in \bar{C}_f(X)} Z_q(\bar{c}, t) \right)^{(-1)^{n-1}} / \prod_{i=0}^n (1 - q^i t). \quad (3.84)$$

**Proof** The relation between  $X'$  and  $X$  is clear by inspection of the invariants under the action of  $G_f(X)$ . We denote by

$$C_f(X) := \{c \in C(X) | c_i e_i / f_i \equiv 0 \pmod{d}, c_i \equiv 0 \pmod{d/d'}\} \quad (3.85)$$

the set of  $c$  fixed under the action of  $G_f$ . Then we have a bijection from  $C(X')$  to  $C_f(X)$  given by

$$c_i \pmod{d'} \mapsto c_i d / d' \pmod{d}. \quad (3.86)$$

From (3.25) the equality of the Jacobi sums, and hence of the zeta functions, follows.  $\square$

**Theorem 3.18** *Let a diagonal variety  $X$  be given. Then the middle primitive cohomology  $PH^n(X, \mathbb{Q}_\ell)$  decomposes as a Galois representation into invariant subspaces  $H(\bar{c}, a)$  of rank  $|\bar{c}|$ . The space  $H(\bar{c}, a)$  is contained in the part of  $PH^n(X, \mathbb{Q}_\ell)$  fixed by  $G_c$ . The characteristic polynomial of the action of the geometric Frobenius element  $F_q^{-1}$  on  $H(\bar{c}, a)$  equals  $Z_q(\bar{c}, a, t)$ .*

Note that these invariant subspaces may or may not be irreducible. Calculations suggest that they are irreducible unless permutation symmetries are present.

**Proof** The proof is by divisor-induction over  $d$  and induction over  $n$ ; so the induction hypothesis is that the theorem holds for all  $X$  of degree  $d'|d$  with  $d' \neq d$ , and all  $n' < n$ . If  $d$  is a prime, then Theorem 3.16 shows that the required subspace is the part of  $H^n(X, \mathbb{Q}_\ell)$  fixed by  $G_c$ . If  $d$  is composite, the fixed part  $PH^n(X, \mathbb{Q}_\ell)^{G_c}$  contains the subspaces  $PH^n(X, \mathbb{Q}_\ell)^{G_{j^c}}$  with  $j$  a proper divisor of  $d$ , and hence  $H(\overline{j^c})$ . But such a subspace  $PH^n(X, \mathbb{Q}_\ell)^{G_{j^c}}$  is already contained in the cohomology of a variety with lower degree or dimension. To see this, select

a prime factor  $r$  of  $j$ , let  $f_i = (e_i, r)$  for all  $i$  and apply Lemma 3.17. Clearly  $jc \in C_f(X)$ , and hence the space  $PH^n(X, \mathbb{Q}_\ell)^{G_{jc}}$  is contained in  $PH^n(X, \mathbb{Q}_\ell)^{G_f}$ , the fixed part under the group  $G_f$ . By the lemma, we can identify  $PH^n(X, \mathbb{Q}_\ell)^{G_f}$  with  $PH^n(X/G_f, \mathbb{Q}_\ell)$  and since  $X/G_f$  has degree  $d/r < d$ , we can apply the induction hypothesis to conclude that each space  $PH^n(X, \mathbb{Q}_\ell)^{G_{jc}}$  decomposes into invariant subspaces under the Galois group.

It follows from representation theory that there must be an complementing invariant space  $H(\bar{c})$  such that  $PH^n(X, \mathbb{Q}_\ell)^{G_c} = \bigoplus_{j|d, j < d} H(\bar{j}c)$ . Since we know the zeta factors corresponding to  $PH^n(X, \mathbb{Q}_\ell)^{G_c}$  (Theorem 3.16) and the spaces  $H(\bar{j}c)$  (by the induction hypothesis and Lemma 3.17) we deduce that the zeta factor corresponding to  $H(\bar{c})$  is indeed  $Z_q(\bar{c}, t)$ .  $\square$

We use the notation  $\rho^d(c, a)$  for the subrepresentation found in the previous theorem. We will omit the coefficient vector  $a$  if all coefficients are equal. We will also omit the  $d$  if no confusion is possible.

### 3.7 The $p$ -adic Gamma function

Now that we have expressed the zeta function in terms of Jacobi sums, we will discuss how they can be calculated. For this purpose we need some properties of the  $p$ -adic variant of the Gamma function. This variant was developed by Yasuo Morita [33] in the seventies, and he showed that many well-known properties of the ordinary Gamma function have a  $p$ -adic analogue.

A common way to define a  $p$ -adic function  $f$  is to give its values on  $\mathbb{N}$ . Since  $\mathbb{N}$  is dense in  $\mathbb{Z}_p$ , there is at most one  $p$ -adically continuous extension of  $f$  to  $\mathbb{Z}_p$ . If we try to extend the ordinary Gamma function in this way, it is clear that no such extension will exist; for example, we need  $\Gamma(1) = \lim_{n \rightarrow \infty} \Gamma(1 + p^n)$  by continuity, but the right-hand side tends to zero in the  $p$ -adic norm. The solution to this problem is simply to leave out the offending factors of  $p$  and adjust the sign. So we define on  $\mathbb{N}$

$$\Gamma_p(n) := (-1)^n \prod_{\substack{1 \leq i < n \\ p \nmid i}} i. \quad (3.87)$$

The alternating sign is necessary, since (at least for odd  $p$ ) we have

$$\prod_{\substack{n \leq i < n+p^k \\ p \nmid i}} i \equiv -1 \pmod{p^k}. \quad (3.88)$$

This can be seen by noting that  $i$  runs over all equivalence classes in  $(\mathbb{Z}/p^k\mathbb{Z})^*$  and pairing each  $i$  with its inverse in this ring. The case  $p = 2$  is a bit more complicated, but the answer is the same.

With the definition (3.87) the function  $\Gamma_p$  satisfies

$$\Gamma_p(a + p^n) \equiv \Gamma_p(a) \pmod{p^n} \quad (3.89)$$

which means that it is uniformly continuous in the  $p$ -adic sense, and hence there is a continuous extension to  $\mathbb{Z}_p$ .

**Definition 3.19** Let  $p$  be a prime. Then we define the  $p$ -adic Gamma function as the  $p$ -adically continuous extension to  $\mathbb{Z}_p$  of the function defined on  $\mathbb{N}$  by

$$\Gamma_p(n) := (-1)^n \prod_{\substack{1 \leq i < n \\ p \nmid i}} i \quad (3.90)$$

We note a few properties of the Gamma function for future use.

**Theorem 3.20** Let  $p$  be an odd prime. Then  $\Gamma_p$  has the following properties:

1. the image of  $\Gamma_p$  is contained in  $\mathbb{Z}_p^*$ ; so  $|\Gamma_p(x)|_p = 1$  for all  $x \in \mathbb{Z}_p$ ;
2.  $|\Gamma_p(x) - \Gamma_p(y)|_p \leq |x - y|_p$ ;
3.  $\Gamma_p(x)\Gamma_p(1-x) = (-1)^{r_p(x)}$ , where  $r_p(x) \equiv x \pmod{p}$  and  $1 \leq r_p(x) \leq p$ ;
4.  $\Gamma_p(\frac{1}{2})^2 = (-1)^{(p+1)/2}$ .

For  $\Gamma_2$ , we have

5. the image of  $\Gamma_2$  is contained in  $\mathbb{Z}_2^*$ ;
6.  $|\Gamma_2(x) - \Gamma_2(y)|_2 \leq |x - y|_2$ , unless  $|x - y|_2 > \frac{1}{8}$ ;
7.  $\Gamma_2(x)\Gamma_2(1-x) = 1$  if  $x \equiv 0$  or  $x \equiv 1 \pmod{4}$ , and  $-1$  otherwise.

The third property, called the reflection formula, is similar to one of the ordinary Gamma function:

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin \pi z}. \quad (3.91)$$

We will also use a multiplication formula similar to the Gauss multiplication formula for the ordinary Gamma function. Fix an integer  $n$  with  $(n, p) = 1$  and an  $x \in \mathbb{Z}_p$ . Then

$$\prod_{i=0}^{n-1} \Gamma_p\left(\frac{x+i}{n}\right) = \sigma_p(n, x)\Gamma_p(x) \prod_{i=1}^{n-1} \Gamma_p\left(\frac{i}{n}\right) \quad (3.92)$$

The product of Gamma functions on the right side can be simplified by the reflection formula. The function  $\sigma_p$  is defined by

$$\sigma_p(n, x) := n^{1-r(x)} (n^{p-1})^{-(x-r(x))/p}. \quad (3.93)$$

We must take care in handling the  $p$ -adic power on the right. In general, the function  $x \rightarrow n^x$  is defined for  $p$ -adic  $x$  by the binomial series. However, it can only be applied to numbers  $n$  with  $n \equiv 1 \pmod{p}$ , otherwise the  $p$ -adic continuity condition fails;  $n^{x+O(p^k)} = n^x + O(p^k)$  only for such  $n$ .

We will use this formula mostly with  $x = a/d$  for some  $0 < a < d$  and  $d|p-1$ . In that case, the following observation is useful.

**Lemma 3.21** *Let  $x = a/(p-1) \in \mathbb{Z}_p$  for some integer  $0 < a < p-1$  and let  $n \in \mathbb{Z}_p^*$  with  $(n, p) = 1$ . Then  $\sigma_p(n, x)$  equals a  $(p-1)$ -th root of unity in  $\mathbb{Z}_p$ ; more precisely it equals the unique root that is congruent to  $n^a$  modulo  $p$ . The function  $(n, a) \rightarrow \sigma_p(n, \frac{1}{p-1})$  defines a group character from  $\mathbb{Z}_p^* \times (\mathbb{Z}/(p-1)\mathbb{Z})$  to  $\mu_{p-1}$ .*

**Proof** The  $p$ -adic expansion of  $x$  is

$$x = 1 + (p-1-a)(1+p+p^2+\dots), \quad (3.94)$$

so  $r(x) = p-a$  and  $-(x-r(x))/p = -(p-1-a)(1+p+p^2+\dots) = (p-1-a)/(p-1)$ . It follows that

$$\sigma_p(n, x)^{p-1} = n^{(p-1)(a-(p-1))} (n^{p-1})^{p-1-a} = 1 \quad (3.95)$$

So  $\sigma_p(n, x)$  is a  $(p-1)$ -th root of unity, and since  $n^{p-1} \equiv 1 \pmod{p}$  it is congruent to  $n^{1-r(x)} = n^a$  modulo  $p$ . By Hensel's lemma there is one root of unity in  $\mathbb{Z}_p$  in each equivalence class modulo  $p$ , so these conditions determine  $\sigma_p(n, x)$ . The final conclusion is obvious.  $\square$

**Corollary 3.22** *Let  $x = a/b \in \mathbb{Z}_p$  for integers  $a$  and  $b$  with  $(a, b) = 1$ ,  $0 < a < b$  and  $b|(p-1)$ . Let  $n \in \mathbb{Z}$  with  $(n, p) = 1$ , and let  $r$  be its order in  $(\mathbb{Z}/p\mathbb{Z})^*$ . Then  $\sigma(n, x)$  is a root of unity with order  $b/(b, (p-1)/r)$ .*

**Proof** We know by the previous Lemma that  $\sigma(n, x) \equiv n^{a(p-1)/b} \pmod{p}$ . Let  $g$  be a generator of  $(\mathbb{Z}/p\mathbb{Z})^*$ , such that  $n = g^{(p-1)/r}$ . Then

$$\sigma(n, x) \equiv g^{a(p-1)^2/rb} \pmod{p}$$

and hence the order of  $\sigma(n, x)$  equals

$$\frac{p-1}{(p-1, a(p-1)^2/b)} = \frac{b}{(b, (p-1)/r)}.$$

$\square$

## 3.8 The Gross-Koblitz formula

One reason why we are using the factorisation of a Jacobi sum into Gauss sums is that the latter can be evaluated quickly for an appropriate choice of  $\chi$  and  $\psi$  by using the Gross-Koblitz formula. This allows us to calculate the Jacobi sums and from them the number of points  $|X(\mathbb{F}_q)|$ . To state the formula, we must first define some characters for  $\mathbb{F}_q$ .

The Teichmüller character  $\omega_q : \mathbb{F}_q^* \rightarrow \mu_{q-1}$  is a multiplicative character of  $\mathbb{F}_q^*$  of the maximal order  $q-1$ ; here  $\mu_{q-1}$  is the group of  $(q-1)$ -th roots of unity. We can realise  $\mathbb{F}_q$  as the residue class field of an ideal  $\mathfrak{p}$  of the cyclotomic field

$\mathbb{Q}(\mu_{q-1})$ . The roots of  $x^{q-1} - 1$  are all different modulo this ideal, so there is an isomorphism

$$\omega_q : \mathbb{F}_q^* \rightarrow \mu_{q-1} \quad (3.96)$$

such that  $\omega_q(x) \equiv x \pmod{\mathfrak{p}}$ . This is the Teichmüller character.

We also need an additive character of  $\mathbb{F}_q$ . Fix a number  $\varpi \in \mathbb{C}_p$ , the completion of the algebraic closure of the  $p$ -adic field  $\mathbb{Q}_p$ , satisfying  $\varpi^{p-1} = -p$ . Then there is a unique non-trivial  $p$ -th root of unity  $\zeta_\varpi$  such that  $\zeta_\varpi \equiv 1 + \varpi \pmod{\varpi^2}$  (see e.g. Lang [26], Lemma 14.3.1) and a corresponding character  $\psi_\varpi$  of  $\mathbb{F}_p$  such that  $\psi_\varpi(1) = \zeta_\varpi$ . By composing this map with the trace  $\text{Tr}_q : \mathbb{F}_q \rightarrow \mathbb{F}_p$ , we find an additive character

$$\psi_{q,\varpi} : \mathbb{F}_q \rightarrow \mu_p. \quad (3.97)$$

**Theorem 3.23** (*Gross-Koblitz formula*) *Let  $q = p^m$  with  $p$  a prime. Let  $\omega_q, \varpi$  and  $\psi_{\varpi,q}$  be as above. Let  $b$  be any integer strictly between 0 and  $q-1$ , and write its  $p$ -adic expansion  $b = \sum_{j=0}^{m-1} b_j p^j$ . Then*

$$g(\omega_q^b, \psi_{\varpi,q}) = (-1)^{m-1} q \varpi^{-\sum b_j} \prod_{i=0}^{m-1} \Gamma_p \left( 1 - \text{frac} \left( \frac{p^i b}{p^m - 1} \right) \right) \quad (3.98)$$

in  $\mathbb{Q}_p(\varpi)$ . Here “frac” denotes the fractional part.

This is the Gross-Koblitz formula. It gives a  $p$ -adic value for the Gauss sum. However, we know that the Jacobi sums have values in  $\mathbb{Q}(\zeta_d)$ , independent of  $\varpi$ , so the powers of  $\varpi$  must recombine to form integral powers of  $-p$ . We can easily see how this happens. Given a vector  $c$  with  $\sum c_i \equiv 0 \pmod{d}$ , we calculate the Jacobi sum

$$J_q^d(c, \omega_q^{(q-1)/d}). \quad (3.99)$$

According to the factorisation (3.10), we have to multiply  $g(\chi_q^{c_i(q-1)/d}, \psi_{\varpi,q})$  for all  $i$ . So the total power of  $\varpi$  appearing in the Jacobi sum is

$$\sum_{i=0}^{n+1} \sum_{j=0}^{m-1} \left( c_i \frac{q-1}{d} \right)_j, \quad (3.100)$$

where the subscript  $j$  again denotes the  $j$ -th digit in the  $p$ -adic expansion. Then  $\sum c_i \equiv 0 \pmod{d}$  implies that

$$\sum_i c_i \frac{q-1}{d} \equiv \sum_{i,j} \left( c_i \frac{q-1}{d} \right)_j p^j \equiv 0 \pmod{q-1}. \quad (3.101)$$

Since  $p-1$  divides  $q-1$ , this implies that  $\sum_{i,j} (c_i \frac{q-1}{d})_j p^j \equiv 0 \pmod{p-1}$ , so  $\sum_{i,j} (c_i \frac{q-1}{d})_j \equiv 0 \pmod{p-1}$ .

It is convenient to use a special notation for the sum of digits. Let  $b$  be any positive integer and let  $b' \equiv b \pmod{q-1}$  be such that  $0 \leq b' \leq q-2$ . Then we can write the base- $p$  expansion  $b' = \sum b'_j p^j$  and we define

$$s_q(b) := \sum_{j=0}^{m-1} b'_j \quad (3.102)$$

Alternatively, we may write

$$s_q(b) = (p-1) \sum_{j=0}^{m-1} \text{frac} \left( \frac{bp^j}{q-1} \right) \quad (3.103)$$

(see [26], Lemma 1.2.1).

So to determine the Jacobi sums, we can use the factorisation (3.10) and the Gross-Koblitz formula to express them in terms of the  $p$ -adic Gamma function and powers of  $p$ . The  $p$ -adic Gamma function takes values in  $\mathbb{Z}_p$ , so it can be approximated by a  $p$ -adic expansion.

By Theorems 3.13 and 3.14 we can express the zeta function of a diagonal variety  $X$  in terms of Jacobi sums. The coefficients of the zeta function are symmetric expressions in the Jacobi sums and since we know that the Jacobi sums have complex absolute value  $q^{n/2}$ , we have an upper bound for the absolute value of these coefficients. We also know they are integers, so we can find their value by approximating them to a finite order of  $p$ -adic accuracy.

In [4], a useful expansion for the Gamma function can be found. Recall that the Pochhammer symbol is defined by

$$\text{Poch}_n(x) := x(x+1) \dots (x+n-1),$$

and define numbers  $\gamma_i$  by

$$\gamma_i = \begin{cases} 0 & \text{if } i < 0 \\ 1 & \text{if } i = 0 \\ (\gamma_{i-1} + \gamma_{i-p})/i & \text{if } i > 0. \end{cases} \quad (3.104)$$

Then the  $p$ -adic Gamma function can be expanded as

$$\Gamma_p(1+px) = - \sum_{i=0}^{\infty} \gamma_{ip} \text{Poch}_i(x) p^i. \quad (3.105)$$

This series is to be used carefully since the  $\gamma_i$  generally have a negative  $p$ -adic valuation. Therefore convergence is a bit slower than (3.105) seems to suggest. In [4] it is shown that

$$\text{ord}_p(\gamma_{np}) \geq n \frac{1-2p}{p(p-1)},$$

from which the rate of convergence of (3.105) can be estimated.

## 3.9 Behaviour modulo $d$

When doing numerical calculations, one quickly observes that the equivalence class of  $p$  modulo  $d$  is important; for example, for fixed  $c$  and  $d$  we will often see that the factor  $Z_p^d(c, t)$  is irreducible for all  $p \equiv 1 \pmod{d}$ , but factorises for other equivalence classes  $p$  and is equal to a power of  $(1 - q^{n/2}t)$  for yet other

equivalence classes. With the Gross-Koblitz formula this observation can be made precise.

Let  $d > 1$  and  $c \in (\mathbb{Z}/d\mathbb{Z})^{n+2}$  be given such that  $c_i \not\equiv 0 \pmod{d}$  and  $\sum_i c_i \equiv 0 \pmod{d}$ ; choose a prime  $p$  with  $(p, d) = 1$  and let  $m \in \mathbb{Z}_{>0}$  be minimal such that  $c(p^m - 1)/d$  has integral coefficients. Then

$$J_{p^m}^d(c, \omega_{p^m}) = \pm p^{m(n+1)} \prod_{i=0}^{n+1} \prod_{j=0}^{m-1} (-p)^{-\text{frac}(c_i p^j/d)} \Gamma_p \left( 1 - \text{frac} \left( \frac{c_i p^j}{d} \right) \right) \quad (3.106)$$

(with  $\pm 1 = (-1)^{(n-1)(m-1)}$ ), as can be found from the Gross-Koblitz formula (3.98) combined with the factorisation in Gauss sums (3.10). As we see, the arguments of the Gamma functions depend only on  $p \pmod{d}$  rather than  $p$  itself. The same holds for the exponent of  $p$ . Therefore any cancellation in (3.106) or in  $Z_q^d(\bar{c}, t)$  due to the multiplication formula (3.92) will occur for all  $p$  in the same equivalence class.

As an example, we work out the case  $d = 9$  and  $c = (1, 4, 7, 6)$ . To handle the many products of Gamma functions appearing in the following formulas, we abbreviate

$$\Gamma_p(x_1, x_2, \dots) := \Gamma_p(x_1) \Gamma_p(x_2) \dots \quad (3.107)$$

First take a prime  $p \equiv 4 \pmod{9}$ . Then  $Z_p^d(c, t)$  equals

$$(1 - p^3 \Gamma_p(\frac{1}{9}, \frac{4}{9}, \frac{7}{9}, \frac{2}{3})^3 t^3) (1 - p^3 \Gamma_p(\frac{2}{9}, \frac{5}{9}, \frac{8}{9}, \frac{1}{3})^3 t^3). \quad (3.108)$$

Applying (3.92) with  $n = 3$ ,  $X = 1/3$  we see that

$$\Gamma_p(\frac{1}{9}, \frac{4}{9}, \frac{7}{9}) = \sigma_p(3, 1/3) \Gamma_p(1/3) (-1)^{r_3(1/3)} \quad (3.109)$$

and hence

$$\begin{aligned} Z_p^d(c, t) &= (1 - p^3 \sigma_p(3, 1/3)^3 (-1)^{r_3(1/3)} \Gamma_p(\frac{1}{3}, \frac{2}{3})^3 t^3) \\ &\quad (1 - p^3 \sigma_p(3, 2/3)^3 (-1)^{r_3(1/3)} \Gamma_p(\frac{1}{3}, \frac{2}{3})^3 t^3) \\ &= (1 - p^3 \sigma_p(3, 1/3)^3 t^3) (1 - p^3 \sigma_p(3, 2/3)^3 t^3) = (1 - p^3 t^3)^2. \end{aligned} \quad (3.110)$$

Here we used that  $\sigma_p(3, 1/3) \equiv 3^{(p-1)/3} \pmod{p}$  by Lemma 3.21, so that its third power is just 1.

If we choose  $p \equiv 7 \pmod{9}$ , the same formulas hold unchanged. If  $p \equiv 1 \pmod{9}$ , we find

$$Z_p^d(c, t) = (1 - p \sigma_p(3, 1/3) (-1)^{r_p(1/3)} t)^3 (1 - p \sigma_p(3, 2/3) (-1)^{r_p(1/3)} t)^3 \quad (3.111)$$

Here  $r_p(1/3)$  is odd, and  $\sigma_p(3, 1/3)$  and  $\sigma_p(3, 2/3)$  are third roots of unity. If 3 is a third power modulo  $p$ , then they are both 1 and the zeta factor equals  $(1 - pt)^6$ . Otherwise they are a conjugated pair of primitive third roots of unity; then the factor is  $(1 + pt + p^2 t^2)^3$ . This clearly depends on  $p$ .

The cases  $p \equiv 2 \pmod{9}$  and  $5 \pmod{9}$  both give an expression that simplifies to  $(1 - p^6 t^6)$ ;  $p \equiv 8 \pmod{9}$  gives  $(1 - pt)^3 (1 + pt)^3$ . So in this case we can determine the zeta factors  $Z_p^d(\bar{c}, t)$  for all primes except 3 without counting a single point.

## Chapter 4

# The Shioda-Katsura Construction

As we have seen, there are many relations between Jacobi sums of equal degree. These relations are not just combinatorially interesting, they can also be interpreted geometrically. Shioda and Katsura [40] pointed out that a Fermat variety of dimension  $n$  and degree  $d$  is related to the direct product of  $n$  Fermat curves of degree  $d$  via a blow-up, a quotient and a blow-down. In this chapter we will investigate this relation, focusing on arithmetical consequences.

### 4.1 The Shioda-Katsura maps

Let us denote by  $M_n^d(a)$  the diagonal variety defined over  $\mathbb{Q}$  in  $\mathbb{P}^{n+1}$  by

$$a_0X_0^d + a_1X_1^d + \dots + a_{n+1}X_{n+1}^d = 0, \quad (4.1)$$

with all  $a_i \in \mathbb{Z}_{\neq 0}$ , and abbreviate  $M_n^d = M_n^d(1, \dots, 1)$ . The result of Shioda and Katsura is:

**Theorem 4.1** *Let  $n_1, n_2$  be positive integers. Then  $M_{n_1+n_2}^d$  is isomorphic to the variety obtained from  $M_{n_1}^d \times M_{n_2}^d$  by first blowing up a subvariety isomorphic to  $M_{n_1-1}^d \times M_{n_2-1}^d$ , then taking a quotient by a group action of  $\mathbb{Z}/d\mathbb{Z}$ , and finally blowing down two subvarieties isomorphic to  $\mathbb{P}^{n_1} \times M_{n_2-1}^d$  and  $M_{n_1-1}^d \times \mathbb{P}^{n_2}$ .*

The exact definitions of these maps are too long to fit in the theorem, but they will be given in the following. The connection between  $M_{n_1}^d \times M_{n_2}^d$  and  $M_{n_1+n_2}^d$  is based on the rational map  $M_{n_1}^d \times M_{n_2}^d \dashrightarrow M_{n_1+n_2}^d$

$$\begin{aligned} \phi : (X_0, \dots, X_{n_1+1}) \times (Y_0, \dots, Y_{n_2+1}) &\mapsto \\ (X_0Y_{n_2+1}, \dots, X_{n_1}Y_{n_2+1}, \varepsilon X_{n_1+1}Y_0, \dots, \varepsilon X_{n_1+1}Y_{n_2}), & \end{aligned} \quad (4.2)$$

where  $\varepsilon$  is fixed number satisfying  $\varepsilon^d = -1$ , but is otherwise arbitrary. We may need to pass to an extension field to find such an  $\varepsilon$ . It is easy to check that this

map takes the subset of  $M_{n_1}^d \times M_{n_2}^d \subset \mathbb{P}^{n_1+1} \times \mathbb{P}^{n_2+1}$  where it is regular into  $M_{n_1+n_2}^d \subset \mathbb{P}^{n_1+n_2+1}$ .

The map  $\phi$  is undefined on the set  $N := \{X_{n_1+1} = Y_{n_2+1} = 0\}$ . It stands to reason that its properties can be improved by blowing up this subvariety. The blow-up is best described in local coordinates, so we define affine neighbourhoods  $U_i$  and  $V_j$ :

$$\begin{aligned} U_i &= M_{n_1}^d \cap \{X_i \neq 0\} \subset \mathbb{P}^{n_1+1} & (0 \leq i \leq n_1) \\ V_j &= M_{n_2}^d \cap \{Y_j \neq 0\} \subset \mathbb{P}^{n_2+1} & (0 \leq j \leq n_2) \end{aligned} \quad (4.3)$$

Then the blow-up of  $M_{n_1}^d \times M_{n_2}^d$  along  $N$  is given in local coordinates in the neighbourhoods  $U_i \times V_j$  by

$$Z_{ij} := \{(X, Y, t) \in U_i \times V_j \times \mathbb{P}^1 : t_1 X_{n_1+1}/X_i = t_0 Y_{n_2+1}/Y_j\} \quad (4.4)$$

and the blow-up  $Bl_N(M_{n_1}^d \times M_{n_2}^d)$  is defined by gluing these local blow-ups in the usual way. The blow-up map is denoted by  $\pi$ .

The composition  $\phi \circ \pi : Bl_N(M_{n_1}^d \times M_{n_2}^d) \mapsto M_{n_1+n_2}^d$  is a morphism of varieties; we have

$$\phi \circ \pi(X, Y, t) = (t_1 \frac{X_0}{X_i}, \dots, t_1 \frac{X_{n_1}}{X_i}, \varepsilon t_0 \frac{Y_0}{Y_j}, \dots, \varepsilon t_0 \frac{Y_{n_2}}{Y_j}) \quad (4.5)$$

for a triple  $(X, Y, t) \in U_i \times V_j \times \mathbb{P}^1$ . This map is rational of degree  $d$ .

We let the group  $\mathbb{Z}/d\mathbb{Z}$  act on  $M_{n_1}^d \times M_{n_2}^d$  by

$$\begin{aligned} (X_0, \dots, X_{n_1+1}) \times (Y_0, \dots, Y_{n_2+1}) &\mapsto \\ (X_0, \dots, X_{n_1}, \zeta^i X_{n_1+1}) \times (Y_0, \dots, Y_{n_2}, \zeta^i Y_{n_2+1}) &\end{aligned} \quad (4.6)$$

where  $i \in \mathbb{Z}/d\mathbb{Z}$  and  $\zeta$  is a primitive  $d$ -th root of unity. The orbits of this action are the fibers of points in  $M_{n_1+n_2}^d$  under  $\phi$ . Clearly the set of fixed points in  $M_{n_1}^d \times M_{n_2}^d$  is precisely  $N$ ; all other points have orbits of maximal length. So it is natural to consider the quotient under the action. The action can be pulled back to  $Bl_N(M_{n_1}^d \times M_{n_2}^d)$ , and we find that the quotient  $Bl_N(M_{n_1}^d \times M_{n_2}^d)/(\mathbb{Z}/d\mathbb{Z})$  is smooth. We will call the natural projection

$$\psi : Bl_N(M_{n_1}^d \times M_{n_2}^d) \mapsto Bl_N(M_{n_1}^d \times M_{n_2}^d)/(\mathbb{Z}/d\mathbb{Z}) \quad (4.7)$$

We can calculate this quotient explicitly in local coordinates; for example, in the neighbourhood  $U_0 \times V_0 \times \{t_1 \neq 0\}$  the blow-up has equation

$$\left(1 + \left(\frac{X_1}{X_0}\right)^d + \dots + \left(\frac{X_{n_1}}{X_0}\right)^d\right) \left(\frac{t_0}{t_1}\right)^d - \left(1 + \left(\frac{Y_1}{Y_0}\right)^d + \dots + \left(\frac{Y_{n_2}}{Y_0}\right)^d\right) \quad (4.8)$$

Now the map  $\phi$  in (4.2) can be pulled back to the blow-up and passed to the quotient under  $\mathbb{Z}/d\mathbb{Z}$ . Therefore it defines a map from  $Bl_N(M_{n_1}^d \times M_{n_2}^d)/(\mathbb{Z}/d\mathbb{Z})$  to  $M_{n_1+n_2}^d$ . In coordinates it reads

$$\tilde{\phi}(X, Y, t) = (t_1 X_0, t_1 X_1, \dots, t_1 X_{n_1}, \varepsilon t_0 Y_0, \varepsilon t_0 Y_1, \dots, \varepsilon t_0 Y_{n_2}). \quad (4.9)$$

This map is birational and it blows up two non-singular subvarieties of  $M_{n_1+n_2}^d$ , the images under  $\tilde{\phi}$  of the sets  $\{t_0 = 0\}$  and  $\{t_1 = 0\}$ . These subvarieties are isomorphic to  $M_{n_1-1}^d$  and  $M_{n_2-1}^d$ , and can be identified as

$$\begin{aligned} M_{n_1-1}^d &= \{Z \in M_{n_1+n_2}^d \mid \sum_{i=0}^{n_1} Z_i^d = 0; Z_{n_1+1} = \dots = Z_{n_1+n_2+1} = 0\} \\ M_{n_2-1}^d &= \{Z \in M_{n_1+n_2}^d \mid \sum_{i=n_1+1}^{n_1+n_2+1} Z_i^d = 0; Z_0 = \dots = Z_{n_1} = 0\}. \end{aligned} \quad (4.10)$$

The map  $\tilde{\phi}$  is a birational map blowing down a  $\mathbb{P}^{n_1}$ -bundle on  $M_{n_1-1}^d$  and a  $\mathbb{P}^{n_2}$ -bundle on  $M_{n_2-1}^d$ . So we see that the blow-up of  $M_{n_1+n_2}^d$  along  $M_{n_1-1}^d$  and  $M_{n_2-1}^d$  is isomorphic to the quotient of  $Bl_N(M_{n_1}^d \times M_{n_2}^d)$  by the action (4.6), which is the content of Theorem 4.1.

In a commutative diagram, the construction looks as follows:

$$\begin{array}{ccc} Bl_N(M_{n_1}^d \times M_{n_2}^d) & \xrightarrow{\psi} & Bl_{M_{n_1-1}^d, M_{n_2-1}^d}(M_{n_1+n_2}^d) \\ \downarrow \pi & & \downarrow \tilde{\phi} \\ M_{n_1}^d \times M_{n_2}^d & \xrightarrow{\phi} & M_{n_1+n_2}^d \end{array} \quad (4.11)$$

As Shioda and Katsura remark, the same construction applies for more general hypersurfaces.

**Theorem 4.2** [40] *Let  $M_1$ ,  $M_2$  and  $M_3$  be non-singular hypersurfaces of degree  $d$  and dimensions  $n_1$ ,  $n_2$  and  $n_1 + n_2$  given by equations*

$$\begin{aligned} M_1 &: f_1(X_0, \dots, X_{n_1}) + X_{n_1+1}^d = 0 \\ M_2 &: f_2(Y_0, \dots, Y_{n_2}) + Y_{n_2+1}^d = 0 \\ M_3 &: f_1(Z_0, \dots, Z_{n_1}) + f_2(Z_{n_1+1}, \dots, Z_{n_1+n_2}) = 0 \end{aligned} \quad (4.12)$$

*defined over a field containing an  $\varepsilon$  with  $\varepsilon^d = -1$ . Then  $M_3$  is isomorphic to the variety obtained from  $M_1 \times M_2$  by first blowing up the subvariety  $X_{n_1+1} = Y_{n_2+1} = 0$ ; then taking the quotient by the simultaneous group action of  $\mathbb{Z}/d\mathbb{Z}$  on  $X_{n_1+1}$  and  $Y_{n_2+1}$  by multiplication with  $\zeta^i$ ; and finally blowing down two subvarieties isomorphic to  $\mathbb{P}^{n_1} \times \{f_2 = 0\}$  and  $\{f_1 = 0\} \times \mathbb{P}^{n_2}$ .*

When we go on to consider the arithmetic consequences of these morphisms, it is inconvenient that the number  $\varepsilon$  appears in the calculations, since not every field contains a number with this property. Therefore it useful to adapt the construction slightly. We modify  $\phi$  by simply setting  $\varepsilon = 1$ :

$$\begin{aligned} \phi &: (X_0, \dots, X_{n_1+1}) \times (Y_0, \dots, Y_{n_2+1}) \mapsto \\ & (X_0 Y_{n_2+1}, \dots, X_{n_1} Y_{n_2+1}, X_{n_1+1} Y_0, \dots, X_{n_1+1} Y_{n_2}). \end{aligned} \quad (4.13)$$

Then when we redo the calculations, we find the following.

**Theorem 4.3** *Let  $M_1$ ,  $M_2$  and  $M_3$  be non-singular hypersurfaces of degree  $d$  and dimensions  $n_1$ ,  $n_2$  and  $n_1 + n_2$  given by equations*

$$\begin{aligned} M_1 &: f_1(X_0, \dots, X_{n_1}) + X_{n_1+1}^d = 0 \\ M_2 &: f_2(Y_0, \dots, Y_{n_2}) + Y_{n_2+1}^d = 0 \\ M_3 &: f_1(Z_0, \dots, Z_{n_1}) - f_2(Z_{n_1+1}, \dots, Z_{n_1+n_2}) = 0. \end{aligned} \quad (4.14)$$

*Then  $M_3$  is isomorphic to the variety obtained from  $M_1 \times M_2$  by first blowing up the subvariety  $X_{n_1+1} = Y_{n_2+1} = 0$ ; then taking the quotient by the simultaneous group action of  $\mathbb{Z}/d\mathbb{Z}$  on  $X_{n_1+1}$  and  $Y_{n_2+1}$  by multiplication with  $\zeta^i$ ; and finally blowing down two subvarieties isomorphic to  $\mathbb{P}^{n_1} \times \{f_2 = 0\}$  and  $\{f_1 = 0\} \times \mathbb{P}^{n_2}$ .*

When applied to Fermat surfaces, this implies that  $M_{n_1+n_2}^d$  is isomorphic to the blowdown of a quotient of a blow-up of  $M_{n_1}^d$  times the variety with equation

$$Y_0^d + Y_1^d + \dots + Y_{n_2}^d - Y_{n_2+1}^d = 0. \quad (4.15)$$

Notice that the quotient variety under the group action is well-defined, even if  $\zeta$  is not an element of the field of definition of the variety. So we can use this construction over any field.

## 4.2 Cohomological consequences

We will now study the consequences of the previous section for the cohomology and the arithmetic of the varieties involved. We take a Weil cohomology theory and denote the corresponding cohomology groups by  $H^i(X)$ . Then the cohomology of the direct product of varieties can be calculated by the Künneth formula. For two projective varieties  $X_1$  and  $X_2$  over  $\mathbb{Q}$  we have

$$H^i(X_1 \times X_2) = \sum_{j=0}^i H^j(X_1) \otimes H^{i-j}(X_2). \quad (4.16)$$

From representation theory it follows that the eigenvalues of the Frobenius map on  $H_{\text{ét}}^i(X_1 \times X_2, \mathbb{Q}_\ell)$  are all possible products of an eigenvalue on  $H_{\text{ét}}^j(X_1, \mathbb{Q}_\ell)$  and one on  $H_{\text{ét}}^{i-j}(X_2, \mathbb{Q}_\ell)$ , for all  $j$ . This can also be derived from the Zeta functions; suppose  $A_i(X_r)$  (with  $r = 1, 2$ ) is the set of eigenvalues of  $F_q$  acting on  $H_{\text{ét}}^i(X_r, \mathbb{Q}_\ell)$  that have absolute value  $q^{i/2}$ . Then we know

$$|X_r(F_{q^s})| = \sum_{i=0}^{2n} (-1)^i \sum_{\alpha \in A_i(X_r)} \alpha^s \quad (4.17)$$

So

$$|X_1 \times X_2(F_{q^s})| = \sum_{i=0}^{2n_1} \sum_{j=0}^{2n_2} (-1)^{i+j} \sum_{\alpha \in A_i(X_1)} \sum_{\beta \in A_j(X_2)} \alpha^s \beta^s. \quad (4.18)$$

By (3.31), it follows that

$$Z_q(X_1 \times X_2) = \prod_{i=0}^{2n_1} \prod_{j=0}^{2n_2} \prod_{\alpha \in A_i(X_1)} \prod_{\beta \in A_j(X_2)} (1 - \alpha\beta t)^{(-1)^{i+j-1}}. \quad (4.19)$$

So by Künneth, we know the cohomology of  $M_{n_1}^d \times M_{n_2}^d$ . The following standard result is used to calculate the cohomology of blow-ups.

**Lemma 4.4** *Let  $Y \subset X$  be a subvariety of the projective variety  $X$ , with  $X$  and  $Y$  both non-singular and defined over an algebraically closed field  $k$ . Fix  $\ell \neq \text{char } k$  prime, and let  $\delta$  be the codimension of  $Y$  in  $X$ . Then*

$$H_{\text{ét}}^i(\text{Bl}_Y X, \mathbb{Q}_\ell) = H_{\text{ét}}^i(X, \mathbb{Q}_\ell) \oplus \sum_{j=1}^{\delta} H_{\text{ét}}^{i-2j}(Y, \mathbb{Q}_\ell) \otimes H_{\text{ét}}^2(\mathbb{P}^1, \mathbb{Q}_\ell)^{\otimes j} \quad (4.20)$$

The tensoring with  $H^2(\mathbb{P}^1)$  occurs often and is called a Tate twist. It is commonly denoted by

$$H^i(X)(-j) := H^i(X) \otimes H_{\text{ét}}^2(\mathbb{P}^1)^{\otimes j}. \quad (4.21)$$

This has the effect that the Frobenius eigenvalue for  $F_q$  is multiplied by  $q$ , for any prime power  $q$  such that the representation is unramified over  $q$ .

From the Lemma 4.4 we immediately find the cohomology of the blow-ups in the previous section. For the blow-up of  $M_{n_1}^d \times M_{n_2}^d$  we have

$$H^i(\text{Bl}_N(M_{n_1}^d \times M_{n_2}^d)) = H^i(M_{n_1}^d \times M_{n_2}^d) \oplus H^{i-2}(M_{n_1-1}^d \times M_{n_2-1}^d)(1). \quad (4.22)$$

The cohomology of the blow-up of  $M_{n_1+n_2}^d$  can be found in the same way.

$$\begin{aligned} H^i(\text{Bl}_{M_{n_1-1}^d, M_{n_2-1}^d} M_{n_1+n_2}^d) = \\ H^i(M_{n_1+n_2}^d) \oplus \sum_{j=1}^{n_1} H^{i-2j}(M_{n_1}^d) \oplus \sum_{j=1}^{n_2} H^{i-2j}(M_{n_2}^d). \end{aligned} \quad (4.23)$$

On the other hand, the cohomology of the last blow-up can also be found from the cohomology of  $\text{Bl}_N(M_{n_1}^d \times M_{n_2}^d)$ ; since the quotient variety under the group action in nonsingular, the cohomology of the quotient is just the invariant part of the cohomology of  $\text{Bl}_N(M_{n_1}^d \times M_{n_2}^d)$  under the group action.

$$\begin{aligned} H^i(\text{Bl}_N(M_{n_1}^d \times M_{n_2}^d)/(\mathbb{Z}/d\mathbb{Z})) &= H^i(\text{Bl}_N(M_{n_1}^d \times M_{n_2}^d))^{\mathbb{Z}/d\mathbb{Z}} \\ &= H^i(M_{n_1}^d \times M_{n_2}^d)^{\mathbb{Z}/d\mathbb{Z}} \oplus H^i(M_{n_1-1}^d \times M_{n_2-1}^d)(1) \end{aligned} \quad (4.24)$$

since the group  $\mathbb{Z}/d\mathbb{Z}$  acts trivially on the exceptional divisor  $M_{n_1-1}^d \times M_{n_2-1}^d$ .

This relation can be interpreted by using the description of the middle cohomology given in Section 3.4. We know a basis for  $H^{n_1}(M_{n_1}^d)$  from Section 3.4, given by differential forms as in (2.15):

$$f_1(c) := \frac{\prod_i X_i^{c_i-1} \sum_i (-1)^i X_i dX_0 \wedge \dots \wedge \widehat{dX_i} \dots \wedge dX_{n+1}}{(\sum_i a_i X_i^{e_i})^{\sum_i c_i/d}}. \quad (4.25)$$

with  $c \in C(M_{n_1}^d)$ , and supplemented by the  $n_1/2$ -th power of the hyperplane class if  $n_1$  is even.

Under the action of  $1 \in \mathbb{Z}/d\mathbb{Z}$ ,

$$f_1(c) \rightarrow \zeta^{c_{n_1+1}} f_1(c). \quad (4.26)$$

Given  $c^1 \in C(M_{n_1}^d)$  and  $c^2 \in C(M_{n_2}^d)$ , the tensor product cohomology class transforms as

$$f_1(c^1) \otimes f_2(c^2) \rightarrow \zeta^{c_{n_1+1}^1 + c_{n_2+1}^2} f_1(c^1) \otimes f_2(c^2). \quad (4.27)$$

Hence this cycle is invariant under the group action precisely if  $c_{n_1+1}^1 + c_{n_2+1}^2 \equiv 0 \pmod{d}$ . In that case, we can apply the map  $\vee$  from Definition 3.8 to map the pair  $(c^1, c^2)$  into  $C(M_{n_1+n_2}^d)$ ;

$$c^1 \vee c^2 = (c_0^1, \dots, c_{n_1}^1, c_0^2, \dots, c_{n_2}^2). \quad (4.28)$$

From the inductive relation (3.13) we have

$$J_q^d(c^1 \vee c^2) = J_q^d(c^1) J_q^d(c^2) J_q^d(c_{n_1+1}^1, c_{n_2+1}^2), \quad (4.29)$$

which is now interpreted as a relation between Frobenius eigenvalues of the varieties. The Jacobi sums  $J_q^d(c^1 \vee c^2)$ ,  $J_q^d(c^1)$  and  $J_q^d(c^2)$  give Frobenius eigenvalues of  $M_{n_1+n_2}^d$ ,  $M_{n_1}^d$  and  $M_{n_2}^d$  respectively; the sum  $J_q^d(c_{n_1+1}^1, c_{n_2+1}^2)$  is a twist that is due to the fact that the map identifying  $M_{n_1+n_2}^d \cong M_{n_1}^d \times M_{n_2}^d$  is not defined over all fields  $\mathbb{F}_q$ .

From Theorem 4.3 we know that  $M_{n_1+n_2}^d \cong M_{n_1}^d \times M_{n_2}^d$  over  $\mathbb{Q}$ , where  $M_2$  is the variety defined by

$$Y_0^d + \dots + Y_{n_2}^d - Y_{n_2+1}^d = 0. \quad (4.30)$$

From (3.46) we see that the Frobenius eigenvalues of the class  $f_2(c^2)$  in  $M_2$  equals  $\chi(-1)^{c_{n_2+1}^2} J_q^d(c^2)$ . Since  $\chi(-1)^{c_{n_2+1}^2} = J_q^d(c_{n_1+1}^1, c_{n_2+1}^2)$ , we see that (4.29) gives a Frobenius eigenvalue of  $M_{n_1+n_2}^d$  as a product of eigenvalues in  $M_{n_1}^d$  and  $M_2$ .

The map  $\vee$  is injective; its image consists of all the  $c \in C(M_{n_1+n_2}^d)$  such that  $\sum_{i=0}^{n_1} c_i \not\equiv 0 \pmod{d}$ . So consider the set of  $c \in C(M_{n_1+n_2}^d)$  for which this sum is zero. These  $c$  split as a union of a  $c^3 \in C(M_{n_1-1}^d)$  and a  $c^4 \in C(M_{n_2-1}^d)$ . Hence we expect they correspond to cohomology classes in the space  $H^{n_1+n_2-2}(M_{n_1-1}^d \times M_{n_2-1}^d)(1)$  in (4.22). This space is invariant under the group action and is therefore mapped unchanged into the cohomology of the quotient variety  $Bl_N(M_{n_1}^d \times M_{n_2}^d)/(\mathbb{Z}/d\mathbb{Z})$  (see (4.24)). The Frobenius eigenvalue associated to  $c^3$  and  $c^4$  in  $H^{n_1+n_2-2}(M_{n_1-1}^d \times M_{n_2-1}^d)(1)$  is

$$q J_q^d(c^3) J_q^d(c^4) = J_q^d(c^3, c^4) \quad (4.31)$$

by the inductive relation (3.12), and this is indeed a Frobenius eigenvalue of  $M_{n_1+n_2}^d$ . So we see that both inductive relations can be understood geometrically.

**Theorem 4.5** *The primitive cohomology  $PH^{n_1+n_2}(M_{n_1+n_2}^d)$  is isomorphic to the direct sum of*

$$PH^{n_1}(M_{n_1}^d) \otimes PH^{n_2}(M_{n_2}^d(-1, 1, 1, \dots)) \quad (4.32)$$

and

$$PH^{n_1-1}(M_{n_1-1}^d) \otimes PH^{n_2-1}(M_{n_2-1}^d)(1) \quad (4.33)$$

**Proof** To show this, we just have to track the primitive part of the cohomology through the maps relating  $M_{n_1+n_2}^d$  and  $M_{n_1}^d \times M_{n_2}^d(-1, 1, 1, \dots)$ . We abbreviate  $M_2 := M_{n_2}^d(-1, 1, 1, \dots)$ . Generally, we know that

$$H^n(M_n^d) = H^{n/2} \oplus PH(M_n^d) \quad (4.34)$$

where  $H$  denotes the space spanned by the hyperplane class, and since we want to handle the cases with  $n$  odd and  $n$  even at the same time, we use the convention that  $H^{n/2} = \{0\}$  if  $n$  is odd. Furthermore we set  $n_3 = n_1 + n_2$ , and we denote by  $nV$  the direct sum of  $n$  copies of  $V$ .

From Lemma 4.4 we have that

$$H^{n_1+n_2}(Bl_N(M_{n_1}^d \times M_2)) = H^{n_3}(M_{n_1}^d \times M_2) \oplus H^{n_3-2}(M_{n_1-2}^d \times M_{n_2-1}^d)(1). \quad (4.35)$$

The right-hand side can be expanded; by Künneth we have

$$\begin{aligned} H^{n_3}(M_{n_1}^d \times M_2) &= \min(n_1, n_2)H^{n_3/2} \oplus PH^{n_1}(M_{n_1}^d) \otimes H^{n_2/2} \oplus \\ &\oplus H^{n_1/2} \otimes PH^{n_2}(M_2) \oplus PH^{n_1}(M_{n_1}^d) \otimes PH^{n_2}(M_2) \end{aligned} \quad (4.36)$$

and

$$\begin{aligned} H^{n_3-2}(M_{n_1-2}^d \times M_{n_2-1}^d)(1) &= \\ &\min(n_1-1, n_2-1)H^{n_3/2} \oplus PH^{n_1-1}(M_{n_1-1}^d) \otimes PH^{n_2}(M_{n_2-1}^d) \otimes H \\ &\oplus PH^{n_1-1}(M_{n_1-1}^d) \otimes H^{(n_2+2)/2} \oplus H^{(n_1+2)/2} \otimes PH^{n_2-1}(M_{n_2-1}^d). \end{aligned} \quad (4.37)$$

Now we select the terms that are invariant under the group action to find the cohomology of the quotient variety. We will call the group  $\mathbb{Z}/d\mathbb{Z} = G$  for the moment. So  $H^{n_3}(Bl_N(M_{n_1}^d \times M_2)/G)$  is the direct sum of five parts:

$$(2 \min(n_1, n_2) - 1)H^{n_3/2} \quad (4.38a)$$

$$(PH^{n_1}(M_{n_1}^d) \otimes PH^{n_2}(M_2))^G \quad (4.38b)$$

$$PH^{n_1-1}(M_{n_1-1}^d) \otimes H^{(n_2+2)/2} \quad (4.38c)$$

$$H^{(n_1+2)/2} \otimes PH^{n_2-1}(M_{n_2-1}^d) \quad (4.38d)$$

$$PH^{n_1-1}(M_{n_1-1}^d) \otimes PH^{n_2-1}(M_{n_2-1}^d) \otimes H \quad (4.38e)$$

We compare this to the cohomology of the blow-up of  $M_{n_3}^d$  along  $M_{n_1-1}^d \times M_{n_2-1}^d$ , which is

$$\begin{aligned}
H^{n_3}(Bl M_{n_3}^d) &= \\
&= H^{n_3}(M_{n_3}^d) \oplus \sum_{j=1}^{n_2-1} H^{n_3-2j}(M_{n_1-1}^d)(j) \oplus \sum_{j=1}^{n_1-1} H^{n_3-2j}(M_{n_2-1}^d)(j) \\
&= PH^{n_3}(M_{n_3}^d) \oplus (2 \min(n_1, n_2) - 1) H^{n_3/2} \\
&\quad \oplus PH^{n_1-1}(M_{n_1-1}^d) \otimes H^{(n_2+1)/2} \oplus PH^{n_2-1}(M_{n_2-1}^d) \otimes H^{(n_1+1)/2}.
\end{aligned} \tag{4.39}$$

Comparing this with (4.38), we conclude that

$$\begin{aligned}
PH^{n_3}(M_{n_3}^d) &= (PH^{n_1}(M_{n_1}^d) \otimes PH^{n_2}(M_{n_2}^d))^G \\
&\quad \oplus PH^{n_1-1}(M_{n_1-1}^d) \otimes PH^{n_2}(M_{n_2-1}^d) \otimes H
\end{aligned} \tag{4.40}$$

as required.  $\square$

This theorem obviously has some consequences for the Galois representations  $\rho(c)$  occurring in the cohomology of  $M_{n_1+n_2}^d$ .

**Corollary 4.6** *Let  $c \in C(M_{n_1+n_2}^d)$  be equal to the union  $c^1 \cup c^2$ , with  $c^1 \in C(M_{n_1-1}^d)$  and  $c^2 \in C(M_{n_2-1}^d)$ . Then  $H^{n_1+n_2}(M_{n_1+n_2}^d)$  contains the representation*

$$(\rho(c^1) \otimes \rho(c^2))(1) \tag{4.41}$$

as a subrepresentation.

**Proof** The subrepresentation given is spanned by the classes  $f(x_1 c^1 \cup x_2 c^2)$  with  $x_i \in (\mathbb{Z}/d\mathbb{Z})^*$  (for  $i = 1, 2$ ). Clearly  $x_i c^i \in C(M_{n_i-1}^d)$ . Formula (3.12) shows that the Frobenius eigenvalues, given by the Jacobi sums, satisfy

$$J_q(x_1 c^1 \cup x_2 c^2) = q J_q(x_1 c^1) J_q^d(x_2 c^2) \tag{4.42}$$

as required.  $\square$

Notice that these subrepresentation will generally not be irreducible; for any  $x_1 \in (\mathbb{Z}/d\mathbb{Z})^*$  it contains the subrepresentations spanned by  $f(x_1 (x_1 c^1 \cup c^2))$  (with  $x \in (\mathbb{Z}/d\mathbb{Z})^*$ ).

**Corollary 4.7** *Assume that  $d$  is even and that  $c \in C(M_{n_1+n_2}^d)$  is equal to the contraction  $c^1 \vee c^2$ , with  $c^1 \in C(M_{n_1-1}^d)$  and  $c^2 \in C(M_{n_2-1}^d)$ , such that  $(c^1)_{n_1+1} \equiv \frac{1}{2}d \pmod{d}$ . Then  $H^{n_1+n_2}(M_{n_1+n_2}^d)$  contains the representation*

$$\rho(c^1) \otimes \rho(c^2) \otimes \rho\left(\frac{d}{2}, \frac{d}{2}\right) \tag{4.43}$$

as a subrepresentation.

**Proof** Here the subrepresentation given is spanned by the classes  $f(x_1c^1 \vee x_2c^2)$  with  $x_i \in (\mathbb{Z}/d\mathbb{Z})^*$  (for  $i = 1, 2$ ). Since  $(c^1)_{n_1+1} \equiv (c^2)_{n_2+1} \equiv \frac{1}{2}d \pmod{d}$  is invariant under the action of  $(\mathbb{Z}/d\mathbb{Z})^*$ , this contraction exists.

Clearly  $x_i c^i \in C(M_{n_i}^d)$  for  $i = 1, 2$ . Formula (3.13) shows that the Frobenius eigenvalues satisfy

$$J_q^d(x_1c^1 \cup x_2c^2) = J_q^d(x_1c^1)J_q^d(x_2c^2)J_q^d\left(\frac{d}{2}, \frac{d}{2}\right) \quad (4.44)$$

as required. □



# Chapter 5

## Modular forms and Galois representations

If we have a smooth and proper variety  $X$  defined over  $\mathbb{Z}$  that reduces to a smooth variety  $X(\mathbb{F}_q)$  over the finite field  $\mathbb{F}_q$ , then we have an action of the Frobenius element  $F_q$  on the étale cohomology of  $X \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ . This action is induced by a representation of the absolute Galois group  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ . Sometimes such a representation can be connected to a modular form. In that case, Fourier coefficients of the form are given by the traces of the Frobenius operators. So the representation can be studied via the reduction of  $X$  to finite fields.

In this chapter we will recall the properties of modular forms and Galois representations that we need for this purpose. We quote some theorems that specify conditions for a Galois representation to be modular. Then we apply these results to some diagonal elliptic curves and determine the modular forms associated to these. We find that many of them are scaled products of the Dedekind  $\eta$ -function.

### 5.1 Modular forms

We recall a few basic facts about modular forms and fix the notation. In this section we will give no proofs, since they can be found in any standard introduction to modular forms, e.g. Lang [25].

It is well-known that the space of lattices of rank 2 in  $\mathbb{C}$  modulo multiplication with complex scalars can be parametrised by the quotient of the complex upper half-plane

$$\mathcal{H} := \{\tau \in \mathbb{C} : \text{Im } \tau > 0\} \tag{5.1}$$

by the action of the group  $\text{SL}_2(\mathbb{Z})$  defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau := \frac{a\tau + b}{c\tau + d}. \tag{5.2}$$

There is a small subgroup  $\{\pm I\}$  (with  $I$  the identity matrix) acting trivially; since we are interested only in the action, it is natural to take the quotient. The

resulting group is

$$\mathrm{PSL}_2(\mathbb{Z}) := \mathrm{SL}_2(\mathbb{Z}) / \{I, -I\}. \quad (5.3)$$

Modular forms can be interpreted as functions on the space of lattices in  $\mathbb{C}$  that scale with  $\lambda^{-k}$  if the lattice is multiplied by  $\lambda \in \mathbb{C}$ . In terms of the group action on  $\mathcal{H}$ , this leads to the following definition.

**Definition 5.1** *A modular form of weight  $k$  for  $\mathrm{SL}_2(\mathbb{Z})$  is a holomorphic function  $f : \mathcal{H} \rightarrow \mathbb{C}$  such that for any  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$  we have*

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \quad (5.4)$$

and with Fourier expansion of the form

$$f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i n \tau}. \quad (5.5)$$

Note that by (5.4) we have  $f(\tau + 1) = f(\tau)$ , so it is very natural to consider the Fourier expansion. It is customary to use the variable  $q$  for  $e^{2\pi i \tau}$ , but since this might cause confusion we will use  $w$  in this thesis.

From the definition it is obvious that the space of modular forms of some fixed weight is a vector space over  $\mathbb{C}$ , and that the direct sum of these vector spaces forms a graded algebra under multiplication of functions; for modular forms  $f_1$  and  $f_2$  of weights  $k_1$  and  $k_2$ , the product  $f_1 f_2$  is a modular form of weight  $k_1 + k_2$ . Definition 5.1 turns out to be so restrictive that this algebra is finitely generated.

More modular forms can be found by loosening the restrictions. For this reason several types of subgroups of  $\mathrm{SL}_2(\mathbb{Z})$  have been defined. Select a positive integer  $N$ . Then we define

- $\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv I \pmod{N} \right\}$
- $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$
- $\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$ .

**Definition 5.2** *Let  $\Gamma$  be equal to  $\Gamma(N)$ ,  $\Gamma_0(N)$  or  $\Gamma_1(N)$  and let  $k \in \mathbb{Z}$ . Then we define the vector space  $M_k(\Gamma)$  as the space of holomorphic functions  $f : \mathcal{H} \rightarrow \mathbb{C}$  that transform as*

$$f(B \cdot \tau) = (c\tau + d)^k f(\tau) \quad (5.6)$$

for all  $B \in \Gamma$ , and such that  $\lim_{\tau \rightarrow i\infty} f(A \cdot \tau)$  exists and is finite for all  $A \in \mathrm{SL}_2(\mathbb{Z})$ .

These vector spaces are all finite-dimensional. The condition on the limit  $\tau \rightarrow i\infty$  ensures that  $f$  can be extended to a continuous function on a compactification of  $\mathcal{H}$ .

There is an important subspace of the space of modular forms.

**Definition 5.3** A modular form  $f$  for a group  $\Gamma$  as above is called a cusp form if  $\lim_{\tau \rightarrow i\infty} f(A \cdot \tau) = 0$  for all  $A \in \mathrm{SL}_2(\mathbb{Z})$ . The space of cusp forms of weight  $k$  is denoted by  $S_k(\Gamma)$ .

Central in the study of modular forms are the Hecke operators. Let  $f \in S_k(\Gamma_1(N))$  and choose a prime  $p$  not dividing  $N$ . Let  $f(\tau) = \sum_{n=0}^{\infty} a_n w^n$  be the Fourier series of  $f$ . Then the Hecke operator  $T_p$  acts on  $f$  by

$$T_p f(z) := \sum_{n=0}^{\infty} a_n(p) w^n \quad (5.7)$$

where

$$a_n(p) = \begin{cases} a_{np} & \text{if } p \nmid n \\ a_{np} + p^{k-1} a_{n/p} & \text{if } p \mid n. \end{cases} \quad (5.8)$$

The Hecke operators  $T_p$  with  $p \nmid N$  commute and they can be simultaneously diagonalised. An eigenfunction for all  $T_p$  is called a Hecke eigenform. The Hecke operators are closely related to the Fourier coefficients; if we normalise a Hecke eigenform  $f$  such that  $a_1 = 1$ , then

$$T_p f = a_p f. \quad (5.9)$$

To a cusp form, a useful series can be associated.

**Definition 5.4** Given a cusp form  $f$  with Fourier expansion  $f = \sum_{n=1}^{\infty} a_n w^n$ , we define the Dirichlet  $L$ -series by the formal series

$$L_f(s) := \sum_{n=1}^{\infty} a_n n^{-s}. \quad (5.10)$$

By using some estimates for the asymptotic behaviour of Fourier coefficients as  $n \rightarrow \infty$ , it can be shown that the series converges to an analytic function on the complex upper half plane  $\{\mathrm{Re} s > k/2 + 1\}$ . The series can also be related to  $f$  using an integral transform. This is the Mellin transform, given by

$$\tilde{f}(s) := \int_0^{\infty} f(it) t^{s-1} dt \quad (5.11)$$

By substituting the Fourier expansion, we find

$$\tilde{f}(s) = \Gamma(s) (2\pi)^{-s} L_f(s). \quad (5.12)$$

For Hecke eigenforms the Dirichlet series is especially interesting, since in that case it factors as an Euler product:

$$\sum_{n=1}^{\infty} a_n n^{-s} = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{k/2-2s}}, \quad (5.13)$$

where the product is taken over all primes  $p \nmid N$ . This construction is closely related to the Riemann zeta function, which is defined as

$$\zeta(s) := \sum \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - p^{-s}} \quad (5.14)$$

for all  $s$  with  $\operatorname{Re} s > 1$ , so that the series converge.

Many nice examples of modular forms can be constructed using the Dedekind  $\eta$ -function, defined by

$$\eta(\tau) := w^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - w^n) \quad (5.15)$$

This function transforms as

$$\eta(S \cdot \tau) = \sqrt{-i\tau} \eta(\tau), \quad (5.16)$$

so it is not a modular form. However, its 24-th power is;

$$\Delta(\tau) := w \prod_{n=1}^{\infty} (1 - w^n)^{24} \quad (5.17)$$

is a cusp form of weight 12 for the full modular group  $\operatorname{SL}_2(\mathbb{Z})$ , and no such form of lower weight exists. Other modular forms can be constructed by multiplying scalings of  $\eta(\tau)$ ; for example,

$$\eta(\tau)^2 \eta(11\tau)^2 \quad (5.18)$$

is modular of weight 2 for the group  $\Gamma_1(11)$ . A full list of such combinations has been compiled by Y. Martin [29].

## 5.2 Galois representations

In Chapter 3 we have shown how to count points of a diagonal variety  $X$  over a finite field  $\mathbb{F}_q$  and how to determine the zeta functions. Here we used the action of the Frobenius element  $F_q$  on the étale cohomology of  $X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ . To see how the representations defined by elements  $F_q$  for different characteristics are related, we need the concept of a Galois representation. For references, see for example [31, 42, 44].

A Galois representation is a representation of the group  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  of automorphisms of the algebraic closure  $\overline{\mathbb{Q}}$  fixing  $\mathbb{Q}$ . For a finite Galois extension  $L$  of  $\mathbb{Q}$ , we know that subgroups of the Galois group correspond one to one with field extensions; a group  $G \subset \operatorname{Gal}(L/\mathbb{Q})$  corresponds to the subfield of  $L$  that is fixed by  $G$ . For the infinite extension  $\overline{\mathbb{Q}}/\mathbb{Q}$  this does not hold, but we can define a topology on  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  such that its closed subgroups in this topology correspond in the same way to Galois extensions of  $\mathbb{Q}$ . A basis for this topology is given by the sets  $\operatorname{Gal}(\overline{\mathbb{Q}}/K)$  for all finite Galois extensions  $K$  of  $\mathbb{Q}$ . Then topologically closed subgroups indeed correspond bijectively to algebraic extensions of  $\mathbb{Q}$ .

Now take a continuous representation  $\rho : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \operatorname{GL}_r(\mathbb{C})$ , where we use the discrete topology on  $\operatorname{GL}_r(\mathbb{C})$ . Then the image of  $\rho$  is finite, since  $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

is compact. The kernel of  $\rho$  is a closed and open subgroup of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ ; hence it defines an extension  $K$  of  $\mathbb{Q}$ , which has finite degree because  $\text{Im}(\rho)$  is finite. The representation  $\rho$  then factors through  $\text{Gal}(K/\mathbb{Q})$  as follows.

$$\begin{array}{ccc} \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho} & \text{GL}_r(\mathbb{C}) \\ & \searrow & \nearrow \rho' \\ & \text{Gal}(K/\mathbb{Q}) & \end{array}$$

We say that  $\rho$  is unramified over a prime  $p$  if the ideal  $(p)$  is unramified in the ring of integers  $O_K$ .<sup>1</sup> For each prime  $p$  that is not ramified in  $K$ , we can choose an  $F_p \in \text{Gal}(K/\mathbb{Q})$  such that for any ideal  $\mathfrak{p}$  dividing  $p$  we have

$$F_p(a) \equiv a^p \pmod{\mathfrak{p}}$$

for all  $a \in O_K$ . This choice is unique up to conjugation in  $\text{Gal}(K/\mathbb{Q})$ . Hence  $\rho'(F_p)$  is also unique up to conjugation, and therefore the characteristic polynomial  $\det(1 - \rho'(F_p)t)$  is well-defined. If  $q = p^s$ , we set  $F_q = (F_p)^s$ . The group generated by  $F_p$  is called a decomposition group. If we set  $\mathbb{F}_{\mathfrak{p}} = O_K/\mathfrak{p}$ , the decomposition group is isomorphic to  $\text{Gal}(\bar{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$  under reduction modulo  $\mathfrak{p}$ .

If we take a smooth projective variety  $X$  defined over  $\mathbb{Q}$ , the group  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  acts on the base change  $X \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$  by acting on  $\bar{\mathbb{Q}}$ . Therefore we have an induced action on the étale cohomology  $H_{\text{ét}}^i(X \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}, \mathbb{Q}_{\ell})$  of  $X$  (where  $\ell$  is an arbitrary prime). This defines a representation of the Galois group and by the work of Grothendieck we know that this representation is continuous and unramified over all primes where  $X$  has good reduction.

The structure of this representation can be studied via the reduction  $X_{\mathbb{F}_q}$  of  $X$  to a finite field of characteristic  $p$ . Then the Galois group  $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$  is isomorphic to the subgroup of  $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$  generated by the Frobenius element  $F_q$ . Hence the Galois representation defined by  $X \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}$  induces a representation of  $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$  and we can calculate the trace of  $F_q$  in either representation.

To do this, we use the Lefschetz trace formula. Denote by  $F_q^*$  the induced action of the Frobenius elements  $F_q$  on the cohomology  $H_{\text{ét}}^i(X_{\mathbb{F}_q} \otimes \bar{\mathbb{F}}_q, \mathbb{Q}_{\ell})$ . We know that the fixed points of  $X(F_q) \otimes \bar{\mathbb{F}}_q$  under  $F_q$  are precisely the points that are rational over  $\mathbb{F}_q$ , that is, the points of  $X(\mathbb{F}_q)$ . The Lefschetz trace formula in this context is

$$|X(\mathbb{F}_q)| = \sum_{i=0}^{2n} (-1)^i \text{Tr}(F_q^*; H_{\text{ét}}^i(X \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q, \mathbb{Q}_{\ell})). \quad (5.19)$$

So we can gain information about the trace of the Frobenius operator by counting points of the reduction of the variety  $X$  to a finite field. Note that this does not depend on the prime  $\ell$  chosen, as long as it is different from the characteristic of

<sup>1</sup>It is actually more common to say that  $\rho$  is unramified if it vanishes on the inertia group  $I_p \subset \text{Gal}(K/\mathbb{Q})$ , but in this case both definitions are equivalent. If any  $\sigma \in I_p$  vanishes under  $\rho'$  then  $\sigma$  fixes  $K$  by definition of  $K$ , and hence  $\sigma$  is the identity in  $\text{Gal}(K/\mathbb{Q})$ .

$\mathbb{F}_q$ . The set of representations  $H_{\text{ét}}^i(X_{\mathbb{F}_q} \otimes \bar{\mathbb{F}}_q, \mathbb{Q}_\ell)$  with  $\ell$  varying over all primes is an example of a compatible system of Galois representations, meaning that the characteristic polynomial of the Frobenius element  $\mathbb{F}_q$  does not depend on  $\ell$ .

To connect Galois representations to modular forms, we need to collect information from all different elements  $F_q$  in one function. This is the Hasse-Weil  $L$ -function.

**Definition 5.5** *Let  $\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_r(\mathbb{Q}_\ell)$  be a continuous  $\ell$ -adic Galois representation of rank  $r$  that is unramified except on a finite set of primes  $S$ , but ramifies at each prime in  $S$ . Let  $P_q(\rho, t) = \det(1 - \rho(F_q)t)$  be the characteristic polynomial; this is called the local  $L$ -factor at  $q$ . Then the local  $L$ -function of  $\rho$  at  $q$  is defined as*

$$L_q(\rho, s) := \frac{1}{P_q(\rho, q^{-s})} \quad (5.20)$$

for any  $q$  not divisible by a bad prime. The Hasse-Weil  $L$ -series is defined by

$$L_{HW}(\rho, s) := \prod_{p \in \mathcal{P} \setminus S} L_p(\rho, s). \quad (5.21)$$

In the cases we consider the  $\ell$ -adic representation comes from the cohomology of a smooth and proper algebraic variety. Hence we know by Deligne [8] that the characteristic polynomials  $P_q$  have integer coefficients independent of  $\ell$ . Then the  $L$ -series can be expanded as a formal series:

$$L_{HW}(\rho, s) = \sum_{n \in \mathbb{N}} b_n n^{-s}. \quad (5.22)$$

Often when  $\rho$  is irreducible of rank 2 this series is equal to the Mellin transform of a modular form. Work by Deligne, Serre and Shimura ([11], [39]) has shown that for a given Hecke eigenform, it is always possible to find a Galois representation with the same  $L$ -series (up to factors from the bad primes).

**Theorem 5.6** *Let  $N > 0$ , let  $\ell$  be a prime and let  $f = \sum_{n=1}^{\infty} a_n w^n \in S_k(\Gamma_1(N))$  be a normalised Hecke eigenform of weight  $k$ . Then there is a continuous irreducible representation*

$$\rho_\ell(f) : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Q}_\ell) \quad (5.23)$$

such that for all primes  $p$  with  $p \nmid N$  and  $p \neq \ell$ , the representation  $\rho_\ell(f)$  is unramified at  $p$  and has  $\text{Tr} \rho_\ell(f)(F_p) = a_p$  and  $\det \rho_\ell(f)(F_p) = p^{k-1}$ .

We call a representation isomorphic to some  $\rho_\ell(f)$  a *modular* representation.

The inverse problem of characterising which 2-dimensional continuous irreducible Galois representations are modular is very difficult; certainly they are not all modular. For elliptic curves, the answer is the famous Shimura-Taniyama conjecture, proved in [50] and [5] by Wiles, Taylor and others. The conjecture can be stated as follows.

**Theorem 5.7** *Let  $E$  be a smooth elliptic curve defined over  $\mathbb{Q}$  and  $\ell$  a prime. Let  $\rho_E$  be the Galois representation in  $H_1^{\text{ét}}(E \otimes_{\mathbb{Q}} \bar{\mathbb{Q}}, \mathbb{Q}_{\ell})$ . Then the  $L$ -series of  $\rho$  is equal to the  $L$ -series of a Hecke eigenform on  $\Gamma_1(N)$  up to factors at the bad primes for  $E$ .*

A useful tool to identify a Galois representation as being modular is a theorem by Livné [27] and Serre. It allows us to conclude (under certain conditions) that two Galois representations are isomorphic by calculating a finite number of traces of Frobenius elements for both representations. If these are equal, we may conclude that they are equal for almost all primes.

Recall the following.

**Definition 5.8** *Let a finite-dimensional representation  $\rho : G \rightarrow \text{GL}(V)$  of a group  $G$  be given. Choose  $\rho$ -invariant subspaces  $V = V^{(0)} \supset V^{(1)} \supset \dots \supset V^{(m)} = \{0\}$  such that  $V^{(i)}/V^{(i+1)}$  is irreducible. Then the semi-simplification  $\tilde{\rho}$  of  $\rho$  is defined as*

$$\tilde{\rho} = V^{(0)}/V^{(1)} \oplus \dots \oplus V^{(m-1)}/V^{(m)}.$$

The semi-simplification does not depend on the subspaces  $V^{(i)}$  chosen.

To state the theorem, we also need the technical notion of a non-cubic set.

**Definition 5.9** *Let  $A$  be a subset of the finite-dimensional vector space  $V$ . Then  $A$  is called non-cubic if any homogeneous polynomial  $P$  of degree 3 on  $V$  that vanishes on  $A$ , vanishes on all of  $V$ .*

In particular, it is sufficient if  $A$  equals all of  $V$ .

**Theorem 5.10** (Livné-Serre, [27]) *Let  $S$  be a finite set of primes and  $\rho_1$  and  $\rho_2$  be continuous Galois representations in  $\text{GL}_2(\mathbb{Q}_2)$  that are unramified outside  $S$ . Let  $\mathbb{Q}_S$  be the composite of all quadratic extensions of  $\mathbb{Q}$  that are also unramified outside  $S$ . Suppose that*

$$\text{Tr}\rho_1 \equiv \text{Tr}\rho_2 \equiv 0 \pmod{2} \quad \text{and} \quad \det(\rho_1) \equiv \det(\rho_2) \pmod{2}$$

and suppose there is a set of primes  $T$  with  $T \cap S = \emptyset$ , such that

- $\{F_p : p \in T\}$  is non-cubic as a subset of  $\text{Gal}(\mathbb{Q}_S/\mathbb{Q})$ , interpreted as a  $\mathbb{F}_2$  vector space; and
- for all  $p \in T$ , we have  $\text{Tr}\rho_1(F_p) = \text{Tr}\rho_2(F_p)$  and  $\det \rho_1(F_p) = \det \rho_2(F_p)$ .

Then  $\rho_1$  and  $\rho_2$  have isomorphic semi-simplifications.

The group  $\text{Gal}(\mathbb{Q}_S/\mathbb{Q})$  is isomorphic to a finite dimensional vector space over  $\mathbb{F}_2$ , since  $\mathbb{Q}_S$  is a composite of quadratic extensions and the Galois group acts as  $\mathbb{F}_2$  independently on each conjugate pair of roots. The proof of this theorem relies on the fact that this group can be generated by a sufficiently large set of Frobenius elements. The notion of a non-cubic set tells us exactly how large this set should be.

In the cases where we will use this theorem, both representations are usually irreducible. Then both representations are equal to their semi-simplification.

A finite non-cubic set  $T$  exists for each finite set  $S$  and it can be computed easily for small  $S$ . This means that we have to calculate only a finite number of local  $L$ -factors of the two representations if we want to prove that they are isomorphic. The first condition in Theorem 5.10 has to be checked for all primes, but there is a number of tricks that can be used to do this. One is given by Livné.

**Lemma 5.11** *Suppose  $\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Q}_2)$  is unramified except possibly on  $S = \{2, 5\}$  and  $\text{Tr}\rho(F_3) \equiv 0 \pmod{2}$ . Then  $\text{Tr}\rho(g) \equiv 0 \pmod{2}$  for all  $g \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ .*

Another case that applies to some of our examples is given by Verrill [46].

**Lemma 5.12** *Suppose  $\rho : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Q}_2)$  is unramified outside  $S = \{2, 3\}$  and*

$$\text{Tr}\rho(F_5) \equiv \text{Tr}\rho(F_7) \equiv \text{Tr}\rho(F_{11}) \equiv \text{Tr}\rho(F_{13}) \equiv 0 \pmod{2}. \quad (5.24)$$

*Then  $\text{Tr}\rho(g) \equiv 0 \pmod{2}$  for all  $g \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ .*

As an alternative, when we calculate  $L$ -factors by counting points, we may use involutions to determine the parity of the trace.

For the construction of suitable sets  $T$ , we refer to Livné's paper [27]. For example, if the set  $S = \{2, 3, 5\}$ , then the set

$$T = \{7, 11, 13, 17, 19, 23, 29, 31, 41, 43, 53, 61, 71, 73\} \quad (5.25)$$

satisfies the conditions of the theorem.

Recently a similar result was published by Schütt [37], which applies only in the case that the representations are unramified outside  $\{2, 3\}$ . However, it also works if not all traces are even.

**Theorem 5.13** *Let  $\rho_1$  and  $\rho_2$  be 2-dimensional 2-adic Galois representations unramified outside  $\{2, 3\}$ . Suppose that  $\det \rho_1 = \det \rho_2$  and at least one of  $\text{Tr}\rho_1(F_{11})$  and  $\text{Tr}\rho_1(F_{13})$  is even. Then  $\rho_1$  and  $\rho_2$  have isomorphic semi-simplifications if and only if*

$$\text{Tr}\rho_1(F_p) = \text{Tr}\rho_2(F_p) \quad (5.26)$$

*for all  $p \in \{5, 7, 11, 13, 17, 19, 23, 31, 37\}$ .*

When we consider diagonal varieties, we have Theorem 3.13 and the remark following its proof which give the upper bound  $\phi(d)$  (the Euler  $\phi$ ) on the rank of the irreducible Galois representations that occur in its middle cohomology; so we expect to find 2-dimensional representations in the cases that  $d = 3$ ,  $d = 4$  and  $d = 6$ . For diagonal varieties of these degrees it can be proved directly that the 2-dimensional irreducible representations that occur in the middle cohomology are always modular. The reason is that the cohomology is induced by characters of the extension  $\mathbb{Q}(\zeta)/\mathbb{Q}$ , with  $\zeta$  a primitive  $d$ -th root of unity. Since this extension is imaginary quadratic, a theorem by Weil applies, stating that the Mellin

transform of the  $L$ -function is a modular form of level equal to the conductor of the representation. See for example Miyake [32].

The same result can be applied to 2-dimensional irreducible representations in diagonal varieties of higher degree  $d$  if the  $d$ -th root of unity is found in an imaginary quadratic extension. However, these 2-dimensional representations are usually isomorphic to representations in varieties of degree 3, 4 or 6, so this provides little new information.

## 5.3 Diagonal elliptic curves

There are three sets of exponents such that the corresponding diagonal equation defines an elliptic curve. In these cases we will certainly find modular forms. Their equations are:

$$E_3 : X_0^3 + X_1^3 + X_2^3 = 0 \quad (5.27)$$

$$E_4 : X_0^2 - X_1^4 + X_2^4 = 0 \quad (5.28)$$

$$E_6 : X_0^2 - X_1^3 + X_2^6 = 0 \quad (5.29)$$

We take the coefficients  $a_i$  equal to  $\pm 1$  here, but they can be varied. We treat this case first since it is the simplest.

The curve  $E_3$  is clearly smooth and has good reduction over all primes unequal to 3. The modular form corresponding to  $\rho(H^1(E, \mathbb{Q}_\ell))$  is well-known.

**Theorem 5.14** *The Galois representation  $\rho(H^1(E_3, \mathbb{Q}_3))$  is isomorphic to the representation  $\rho(f_3)$ , where*

$$f_3(\tau) = \eta(3\tau)^2 \eta(9\tau)^2 \quad (5.30)$$

*is a cusp form for  $\Gamma_0(27)$  of weight 2.*

The first terms of the expansion for  $f_3$  are

$$f_3(\tau) = w - 2w^4 - w^7 + 5w^{13} + 4w^{16} - 7w^{19} + O(w)^{25} \quad (5.31)$$

**Proof** This is most easily proved using Schütt's Theorem 5.13; so we consider  $\rho(H^1(E_3, \mathbb{Q}_2))$  first. We know that the determinant of  $\rho(f_3)(F_p)$  is equal to  $p$  by Deligne's theorem 5.6. The determinant of  $\rho(E_3)(F_p)$  is also equal to  $p$ , as was deduced in Section 3.3. The trace of  $F_{11}$  is zero in both representations, which is even. So we only need to check that the Frobenius traces are equal for the other primes listed in Theorem 5.13. For  $\rho(E_3)$ , the traces are calculated by counting points; for  $\rho(f_3)$  we can look them up in any number of tables or calculate them from the product expansion of the  $\eta$  function.

We conclude that  $\rho(H^1(E_3, \mathbb{Q}_2))$  is isomorphic to  $\rho(f_3)$ . On the other hand  $\rho(H^1(E_3, \mathbb{Q}_2))$  and  $\rho(H^1(E_3, \mathbb{Q}_3))$  have equal traces at all primes except 2 and 3, and these cases can be checked by hand.  $\square$

Alternatively, we can compute the conductor of  $E_3$ ; its Weierstrass form is  $y^2 - 27y = x^3$ , which gives a conductor of 27. Therefore the modular form

Elliptic curve	Modular form	Level
$X_0^3 + X_1^3 + X_2^3 = 0$	$\eta(3\tau)^2\eta(9\tau)^2$	27
$X_0^2 + X_1^4 + X_2^4 = 0$	$\eta(4\tau)^{-2}\eta(8\tau)^8\eta(16\tau)^{-2}$	64
$X_0^2 + X_1^4 - X_2^4 = 0$	$\eta(4\tau)^2\eta(8\tau)^2$	32
$X_0^2 + X_1^3 + X_2^6 = 0$	$\eta(6\tau)^{-4}\eta(12\tau)^{12}\eta(24\tau)^{-4}$	144
$X_0^2 + X_1^3 - X_2^6 = 0$	$\eta(6\tau)^4$	36

Table 5.1: Some diagonal elliptic curves and their modular forms. These forms have weight 2.

corresponding to  $E_3$  by Taniyama-Shimura-Wiles is an element of  $S_2(\Gamma_1(27))$ . This space is known, so by computing a few traces the right form can easily be identified.

**Theorem 5.15** *The Galois representation  $\rho(H^1(E_4, \mathbb{Q}_2))$  is isomorphic to the representation  $\rho(f_4)$ , where*

$$f_4(\tau) = \eta(4\tau)^2\eta(8\tau)^2 \quad (5.32)$$

*is a cusp form for  $\Gamma_1(32)$  of weight 2.*

**Proof** Here we use Theorem 5.10. The representation  $\rho(H^1(E_4, \mathbb{Q}_2))$  ramifies only at  $p = 2$ . The set  $T$  in this case equals  $T = \{3, 5, 7\}$ . By the methods of Chapter 3 or by elementary means we can easily ascertain that the characteristic polynomials of  $\rho(H^1(E_4, \mathbb{Q}_2))(F_p)$  and  $\rho(f_4)(F_p)$  coincide on these primes. Both representations clearly satisfy the conditions of Lemma 5.11, since both have  $a_3 = \text{Tr}\rho(F_3) = 0$ ; so both have even traces on all primes. By Deligne's work we know that  $\det \rho(F_p) = p$  for all good  $p$ . We conclude that all requirements of Livné's theorem are fulfilled, so the representations have isomorphic semi-simplifications. Since they are clearly irreducible we conclude that the representations are isomorphic.  $\square$

**Theorem 5.16** *The Galois representation  $\rho(H^1(E_6, \mathbb{Q}_2))$  is isomorphic to the representation  $\rho(f_6)$ , where*

$$f_6(\tau) = \eta(6\tau)^4 \quad (5.33)$$

*is a cusp form for  $\Gamma_1(36)$  of weight 2.*

This can be proved along the same lines as the previous theorem. Proceeding in this way, we construct a small table containing all diagonal elliptic curves with coefficients  $\pm 1$ . Some elliptic curves with other coefficients are listed in the next chapter.

# Chapter 6

## Explicit representations

In this chapter we use the techniques developed so far to identify representations occurring in diagonal varieties. We will find modular representations, tensor products of representations and so on. This will allow us to find the zeta functions of a number of diagonal varieties. As a preparation, we investigate under which conditions we can find tensor product representations among them. Everywhere we will only consider primes where the variety in question has good reduction, even though a subrepresentation may sometimes be unramified over a prime of bad reduction for the variety.

Up to this point, we have only counted points of diagonal varieties, without caring whether they were singular or not. In this chapter we will use the techniques from Chapter 2 to resolve singularities, and we will compute the zeta factors the exceptional fibers. Since the resolution of a variety is unique up to birational morphisms, we can apply a result by Ito [20].

**Theorem 6.1** *Let  $X$  and  $Y$  be smooth minimal models over  $\mathbb{Q}$  that are birational to each other and have good reduction to  $\mathbb{F}_q$ . Then  $|X(\mathbb{F}_q)| = |Y(\mathbb{F}_q)|$ .*

Here a minimal model is a projective variety  $X$  such that  $K_X \cdot C \geq 0$  for all curves  $C$  in  $X$ . In particular all Calabi-Yau varieties are minimal models, since they have vanishing canonical bundle.

We use the following notations for the representations in this chapter. Irreducible 2-dimensional representations that are associated to a modular form via Deligne's Theorem 5.6 are denoted by the label of this modular form, as given by Stein [43]. If the form has weight 2, this label consists of the level and a code giving the character, separated by a letter enumerating the forms with this level and character; e.g. 64A1 denotes a form of level 64 with trivial character, with weight 2 implied. A form of level 64 and weight 3 would be denoted 64k3A[1,0]1, etcetera. We will just use these codes to identify the forms. All forms we will find are normalized Hecke eigenforms.

Another representation that will appear is  $\rho_0(d)$ , which is a representation of weight one associated to a zero-dimensional variety; it is discussed in Section 6.2. A Tate twist in a representation is denoted as usual by  $\otimes \mathbb{Q}(-k)$ ; so  $\mathbb{Q}(-k)$  is

the trivial 1-dimensional representation of weight  $2k$ , such that the characteristic polynomial of a Frobenius element  $F_p$  is equal to  $(1 - p^k t)$ .

In many of our calculations, we use the formula (3.106) to express the Jacobi sums and hence the zeta functions in terms of the  $p$ -adic Gamma function. To simplify the resulting expressions, we use the Gamma multiplication formula (3.92). In the Appendix a list of the relevant formulas is given. Since our formulas contain a lot of products of  $\Gamma_p$ , it is convenient to use a special notation for this. Hence we use the convention that

$$\Gamma_p(x_1 x_2 \dots) := \Gamma_p(x_1) \Gamma_p(x_2) \dots$$

We will also use the reflection formula frequently (Theorem 3.20, property 3), as well as the function  $r_p$  is defined there.

## 6.1 Tensor product representations

In the previous chapter we saw that we can associate modular forms to some diagonal elliptic curves; this is also possible for other 2-dimensional subrepresentations in the cohomology of diagonal varieties, as we shall see later in this chapter. If we look at representations of higher rank we expect to find more complicated behaviour. In general, there is no reason to assume that there is a direct connection to modular forms. However, in a number of cases of low degree we find irreducible 4-dimensional representations that are isomorphic to a tensor product of two modular representations.

We use the following notation for tensor products.

**Definition 6.2** *Let  $P$  and  $Q$  be given by*

$$P(t) = \prod_{i=1}^{d_P} (1 - \alpha_i t) \text{ and } Q(t) = \prod_{j=1}^{d_Q} (1 - \beta_j t)$$

*in  $\mathbb{C}[t]$  with  $d_P$  and  $d_Q$  positive. Then we define their tensor product  $P \otimes Q$  by*

$$(P \otimes Q)(t) = \prod_{i=1}^{d_P} \prod_{j=1}^{d_Q} (1 - \alpha_i \beta_j t).$$

*If  $\chi$  is a constant, we define*

$$(P \otimes \chi)(t) := P \otimes (1 - \chi t) = P(\chi t).$$

This definition is made such that for any two finite-dimensional representations  $\rho_i$  with  $i = 1, 2$  of a group  $G$

$$\det(1 - t(\rho_1 \otimes \rho_2)(g)) = \det(1 - t\rho_1(g)) \otimes \det(1 - t\rho_2(g))$$

for all  $g \in G$ .

**Lemma 6.3** *Suppose  $\rho_1$  and  $\rho_2$  are two-dimensional Galois representations of weights  $k_1$  and  $k_2$ , such that their local  $L$ -factors are given by  $1 - A_i(q)t + q^{k_2-1}t^2$  for  $i = 1, 2$ . Then the local  $L$ -factor at  $q$  of the tensor representation  $\rho_1 \otimes \rho_2$  is*

$$P_q(\rho_1 \otimes \rho_2, t) = 1 - A_1 A_2 t + (q^{k_1-1} A_2^2 + q^{k_2-1} A_1^2 - q^{k_1+k_2-2}) t^2 - q^{k_1+k_2-2} A_1 A_2 t^3 + q^{2(k_1+k_2-2)} t^4. \quad (6.1)$$

**Proof** If we decompose  $1 - A_i t + q^{k_2-1} t^2 = (1 - \alpha_i t)(1 - \alpha'_i t)$ ,  $\alpha_i$  and  $\alpha'_i$  are the inverses of the complex eigenvalues of  $\rho_i(F_q)$ . The tensor product representation has eigenvalues that are the products of eigenvalues of  $\rho_1$  and  $\rho_2$ :

$$P_q(\rho_1 \otimes \rho_2, t) = (1 - \alpha_1 \alpha_2 t)(1 - \alpha'_1 \alpha_2 t)(1 - \alpha_1 \alpha'_2 t)(1 - \alpha'_1 \alpha'_2 t), \quad (6.2)$$

which simplifies to the expression given.  $\square$

The appearance of tensor products of representations is a consequence of the construction of Katsura and Shioda (see Chapter 4), but it can also be interpreted as a consequence of the inductive relation (3.13).

**Example** We consider the case that  $d = 12$ ,  $c = (2, 4, 3, 3)$ . Take a  $p \equiv 1 \pmod{d}$ . Then  $J_p^{12}(2, 4, 3, 3) = J_p^{12}(6, 6) J_p^{12}(2, 4, 6) J_p^{12}(3, 3, 6)$ , and the polynomial  $Z_p^d(c, t)$  equals:

$$\begin{aligned} Z_p^{12}(c, t) = & (1 - J_p^{12}(6, 6) J_p^{12}(2, 4, 6) J_p^{12}(3, 3, 6) t) \\ & (1 - J_p^{12}(6, 6) J_p^{12}(10, 8, 6) J_p^{12}(3, 3, 6) t) \\ & (1 - J_p^{12}(6, 6) J_p^{12}(2, 4, 6) J_p^{12}(9, 9, 6) t) \\ & (1 - J_p^{12}(6, 6) J_p^{12}(10, 8, 6) J_p^{12}(9, 9, 6) t) \end{aligned} \quad (6.3)$$

So apart from the overall factor  $J^{12}(6, 6)$ , the polynomial  $Z_q^d(t)$  has the form of (6.2). Therefore  $Z_q^d$  is equal to the characteristic polynomial of the tensor product representation of the 2-dimensional Galois representations associated to  $c = (3, 3, 6)$  and  $c = (2, 4, 6)$ , twisted with the Dirichlet character  $J_p^{12}(6, 6)$ . After dividing out common factors in  $d$  and the components of  $c$ , we see that one of these representations is isomorphic to the one defined by the modular form  $\eta(4\tau)^{-2} \eta(8\tau)^8 \eta(16\tau)^{-2}$  (Table 5.1 with  $d = 4$  and  $c = (1, 1, 2)$ ), and the other to the representation defined by  $\eta(6\tau)^{-4} \eta(12\tau)^{12} \eta(24\tau)^{-4}$  (same with  $d = 6$  and  $c = (1, 2, 3)$ ).

With this example in mind, we can describe more generally the cases where we expect to find tensor products of modular representations. Recall the notations in Definition 3.8.

**Theorem 6.4** *Take  $c \in A_n^d$  and assume that  $d$  and the entries of  $c$  have no common factor. Suppose  $c$  can be written as a contraction  $c = c^1 \vee c^2$  for some  $c^1 \in A_{n_1}^d$  and  $c^2 \in A_{n_2}^d$ , such that the orbit of the pair  $(c^1, c^2)$  under the action of*

$(\mathbb{Z}/d\mathbb{Z})^*$  equals  $\{(c^1, c^2), (-c^1, c^2), (c^1, -c^2), (-c^1, -c^2)\}$ . Then  $d$  is even and the representation associated to  $c$  is isomorphic to

$$H^d(c) \cong H^d(c^1) \otimes H^d(c^2) \otimes H^d(d/2, d/2) \quad (6.4)$$

**Proof** First consider  $(c^2)_0$ , which equals  $(c^1)_{n_1+1}$  by construction. This number is a common entry of  $c^1$  and  $c^2$  and hence it is invariant under the action by  $(\mathbb{Z}/d\mathbb{Z})^*$ . Since it is also nonzero, this implies that  $(c^2)_0 = d/2$ ; in particular,  $d$  is even. We abbreviate  $c^0 = (d/2, d/2)$ .

The requirements on the action of  $(\mathbb{Z}/d\mathbb{Z})^*$  imply that it acts like  $\{1, -1\}^2$  on the set  $\{(c^1, c^2), (c^1, -c^2), (-c^1, c^2), (-c^1, -c^2)\}$ , with the  $i$ -th copy of  $\{1, -1\}$  acting by multiplication on the  $i$ -th component. So we have for a  $p \equiv 1 \pmod{d}$ :

$$Z_p^d(c, t) = \left( \prod_{x \in (\mathbb{Z}/d\mathbb{Z})^*} (1 - J_p^d(xc^1, \chi)J_p^d(xc^2, \chi)J_p^d(c^0, \chi)t) \right). \quad (6.5)$$

Working out the action of  $(\mathbb{Z}/d\mathbb{Z})^*$  explicitly, we find

$$\begin{aligned} Z_p^d(c, t) &= \prod_{x \in (\mathbb{Z}/d\mathbb{Z})^*} (1 - J_p^d(xc^1, \chi)J_p^d(xc^2, \chi)J_p^d(c^0, \chi)t) \\ &= (1 - (J_p^d(c^1) + J_p^d(-c^1))t + p^{n_1}t^2) \otimes \\ &\quad \otimes (1 - (J_p^d(c^2) + J_p^d(-c^2))t + p^{n_2}t^2) \otimes (1 - J_p^d(c^0, \chi)t) \\ &= Z_p^d(c^1, t) \otimes Z_p^d(c^2, t) \otimes Z_p^d(c^0, t). \end{aligned} \quad (6.6)$$

Now consider a prime  $p \not\equiv 1 \pmod{d}$ . From the assumptions it follows that  $p^2 \equiv 1 \pmod{d}$ , so we have

$$\begin{aligned} Z_p^d(c, t) &= \prod_{x \in (\mathbb{Z}/d\mathbb{Z})^* / \langle p \rangle} (1 - J_{p^2}^d(xc, \chi)t^2) \\ &= \prod_{x \in (\mathbb{Z}/d\mathbb{Z})^* / \langle p \rangle} (1 - J_{p^2}^d(xc^1, \chi)J_{p^2}^d(xc^2, \chi)J_{p^2}^d(c^0, \chi)t^2). \end{aligned} \quad (6.7)$$

We must distinguish between a number of cases.

**Case 1.** Suppose  $pc^1 \equiv c^1 \pmod{d}$  and  $pc^2 \equiv -c^2 \pmod{d}$ . From  $pc^1 \equiv c^1 \pmod{d}$  it follows that  $J_p^d(c^1)$  is well-defined, so  $J_{p^2}^d(c^1) = J_p^d(c^1)^2$  by the Davenport-Hasse theorem 3.9. The same holds for  $c^0$ . For  $c^2$ , we have  $J_{p^2}^d(c^2) = J_{p^2}^d(-c^2) = \overline{J_{p^2}^d(c^2)}$ , since we know that the Jacobi sum is invariant under multiplication of  $c^2$  by  $p$ . Therefore  $J_{p^2}^d(c^2) = \pm p^{n_2}$ , and  $Z_p(c^2, t) = (1 - J_{p^2}^d(c^2)t^2)$ .

This implies that

$$\begin{aligned} Z_p^d(c, t) &= (1 - (J_p^d(c^1) + J_p^d(-c^1))t + p^{n_1}t^2) \otimes \\ &\quad \otimes (1 - J_{p^2}^d(c^2)t^2) \otimes (1 - J_p^d(c^0)t) \\ &= Z_p(c^1, t) \otimes Z_p(c^2, t) \otimes Z_p(c^0, t). \end{aligned} \quad (6.8)$$

The same argument holds if the roles of  $c^1$  and  $c^2$  are reversed.

**Case 2.** Suppose  $pc^1 \equiv c^1 \pmod{d}$  and  $pc^2 \equiv c^2 \pmod{d}$ . Then  $pc_i \equiv c_i \pmod{d}$  for all  $i$ , and hence  $p \equiv 1 \pmod{d}$  since the  $c_i$  and  $d$  have no common factor. This case has been done.

**Case 3.** Suppose  $pc^1 \equiv -c^1 \pmod{d}$  and  $pc^2 \equiv -c^2 \pmod{d}$ . Then  $J_{p^2}^d(c^1)$  and  $J_{p^2}^d(c^2)$  are both equal to  $\pm$  times the appropriate power of  $p$ . So

$$\begin{aligned} Z_p^d(c, t) &= \left( (1 - J_{p^2}^d(c^1, \chi) J_{p^2}^d(c^2, \chi) J_{p^2}^d(c^0, \chi) t^2) \right)^2 \\ &= Z_p(c^1, t) \otimes Z_p(c^2, t) \otimes Z_p(c^0, t) \end{aligned} \quad (6.9)$$

as required.  $\square$

## 6.2 Representations of dimension 2

### 6.2.1 Representations of weight 1

Given a degree  $d$ , a vector  $c = (c_0, d - c_0)$  defines a representation  $\rho(c)$  of weight 1, meaning that the determinants  $\det \rho(c)(F_q) = \pm 1$  for all good primes  $q$ . We can determine the local  $L$ -factors of  $\rho(c)$  explicitly. First assume that  $(c_0, d) = 1$  and  $d > 2$ . Given a prime  $p$  with  $(p, d) = 1$ , we let  $m$  be the order of  $p$  in  $(\mathbb{Z}/d\mathbb{Z})^*$ . Then we have from equation (3.65)

$$Z_p^d(c, t) = \begin{cases} (1 - (-1)^{(p^m-1)/d} t^m)^{\phi(d)/m} & \text{if } d \text{ is even,} \\ (1 - t^m)^{\phi(d)/m} & \text{if } d \text{ is odd or } p \text{ is even.} \end{cases} \quad (6.10)$$

The factors do not depend on the actual value of  $c_0$ . Therefore we will call this representation  $\rho_0(d)$ . If  $(c_0, d) > 1$ , then we can simply remove the common factor and we will find the representation  $\rho_0(d/(c_0, d))$  defined above.

The  $L$ -factor of  $p$  is

$$\begin{aligned} L_p(s) &= \frac{1}{1 - p^{-sm} (-1)^{\frac{p^m-1}{d}}} \\ &= 1 + (-1)^{\frac{p^m-1}{d}} p^{-sm} + p^{-2sm} + (-1)^{\frac{p^m-1}{d}} p^{-3sm} + \dots \end{aligned} \quad (6.11)$$

Another representation of weight 1 that we will encounter is given by  $d = 2$  and  $c = (1, 1)$ . This defines a representation of dimension 1, and it is related to the “zero-dimensional” Calabi-Yau defined by the equation  $X_0^2 + X_1^2 = 0$ . From the definition of the Jacobi sum, we see that  $J_q^2(1, 1) = (-1)^{\frac{q-1}{2}}$ , and the zeta factor of this representation is  $1 - (-1)^{\frac{q-1}{2}} t$ . Indeed the number of solutions to the equation is generated by the “zeta function”

$$\frac{1}{(1-t)(1 - (-1)^{\frac{q-1}{2}} t)}$$

The representations of weight 1 often occur as twists of other representations. It is useful to devote a little lemma to this phenomenon in the case  $d = 12$ .

**Lemma 6.5** *Let  $d = 12$ , a dimension  $n \geq 4$  and a  $c \in A_n^d$  be given. Suppose that  $c_0 + c_1 \equiv 0 \pmod{d}$ , and write  $c = (c_0, c_1) \cup c'$ . Let  $\chi$  be any Dirichlet character modulo 24 with  $\chi^2 = 1$  and  $\chi(p) = (-1)^{c_0 \frac{p-1}{d}}$  if  $p \equiv 1 \pmod{d}$ . Then  $\rho(c)$  is isomorphic to  $|\bar{c}|/|c'|$  copies of  $\rho(c') \otimes \chi \otimes \mathbb{Q}(-1)$ .*

**Proof** Take an arbitrary prime  $p$  with  $(p, d) = 1$ , and let  $q = p^m$  be minimal such that  $(q-1)c/d$  has integer coefficients. Then

$$\begin{aligned} Z_p^d(\bar{c}, t) &= \prod_{c \in \bar{c}} (1 - J_q^d(c)t^m)^{\frac{1}{m}} \\ &= \prod_{x \in (\mathbb{Z}/d\mathbb{Z})^*} (1 - qJ_q^d(c_0, c_1)J_q^d(xc')t^m)^{1/m}. \end{aligned} \tag{6.12}$$

Now  $J_q^d(c_0, c_1) = (-1)^{c_0(q-1)/d}$ , so if  $m > 1$  then  $q^m \equiv 1 \pmod{8}$  and hence  $J_q^d(c_0, c_1) = 1$ . In this case the twist with  $\chi$  acts trivially.

For a prime  $p \equiv 1 \pmod{d}$  the factor  $J_p^d(c_0, c_1) = \chi(p)$  by definition.  $\square$

## 6.2.2 Representations in degree 3

$c=(1,1,1)$

As we have seen in Section 5.3, these representation occurs in the diagonal elliptic curve defined by  $a_0X_0^3 + a_1X_1^3 + a_2X_2^3 = 0$ . The representation ramifies at 3 and possibly at primes dividing the  $a_i$ . Generally the traces of the representation are not even, so Theorem 5.10 is not applicable. We can use Theorem 5.13 if the representation is unramified outside  $\{2, 3\}$ .

As an example, take the curve  $C$  defined over  $\mathbb{Q}$  by

$$X_0^3 + X_1^3 + 2X_2^3 = 0.$$

This curve is clearly smooth and it has good reduction to any finite field with characteristic unequal to 2 and 3. Since it is an elliptic curve, its zeta function over the prime field  $\mathbb{F}_p$  (with  $p \neq 2, 3$ ) equals

$$\frac{1 - a_p t + p t^2}{(1-t)(1-pt)}$$

and its number of points equals  $|C(\mathbb{F}_p)| = 1 + p - a_p$ .

We determine the numbers  $a_p$  for some small primes by counting points, either in the naive way or by the methods of Chapter 3. We find the following.

$p$	5	7	11	13	17	19	23	29	31	37
$a_p$	0	-4	0	2	0	8	0	0	-4	-10

These are the traces of the Frobenius operators under the Galois representation  $H_{\text{ét}}^1(C, \mathbb{Q}_\ell)$ ; the determinants are equal to  $p$ . As we see the traces  $a_{11}$  and  $a_{13}$  are

even, so Schütt's Theorem 5.13 is applicable. Checking a table of modular forms, we find that the  $a_p$  are also the coefficients of the modular form

$$f(\tau) = \eta(6\tau)^4 = w - 4w^7 + 2w^{13} + 8w^{19} - 5w^{25} - 4w^{31} - 10w^{37} + O(w^{43}).$$

So the traces of the Galois representation associated to this modular form are equal to those of  $\rho_f$ , and since this modular form has weight 2 the determinants are  $\det(\rho_f(F_q)) = q$  for all prime powers  $q$ .

Thus we have checked all premisses of Theorem 5.13, and we conclude that the representations  $H_{\text{ét}}^1(C, \mathbb{Q}_\ell)$  and  $\rho_f$  have isomorphic semi-simplifications. In particular, the traces  $a_p$  equal the coefficients of  $f$  for all primes  $p > 3$ .

In this way, we identify the following representations.

$a$	Modular form	Weight	Level
(1, 1, 1)	27A1 = $\eta(3\tau)^2\eta(9\tau)^2$	2	27
(1, 1, 3)	243B1	2	243
(1, 3, 3)	243A1	2	243
(1, 3, 9)	27A1	2	27
(1, 1, 2)	36A1 = $\eta(6\tau)^4$	2	36
(1, 2, 2)	108A1	2	108
(1, 2, 4)	27A1	2	27

Table 6.1: Representations for  $d = 3$ ,  $c = (1, 1, 1)$ .

$\mathbf{c} = (1, 1, 1, \dots)$

If  $d = 3$  and  $c$  has more than 3 entries, then we can decompose  $c$  as a union of two smaller  $c$ . By Section 4.2, such a decomposition corresponds to a tensor product of representations. That gives us one way to identify the representation associated to such a  $c$ . However, we know by Theorem 3.18 that the representation is reducible into subrepresentations of dimension 2 or less, so we can also identify these subrepresentations directly.

Notice the following relation. We denote by  $(1_k)$  a vector with  $k$  entries equal to 1. Then

$$\begin{aligned} J_q^d(1_{3k}) &= J_q^d(1, 1, 1)J_q^d(2, 1_{3k-2})J_q^d(2, 1) \\ &= J_q^d(1, 1, 1)J_q^d(1_{3(k-1)})(J_q^d(2, 1))^2. \end{aligned} \tag{6.13}$$

Hence  $J_q^d(1_{3k}) = J_q^d(1, 1, 1)^k$ .

$c$	Modular form	Weight	Level
(1, 1, 1)	27A1	2	27
(1 <sub>6</sub> )	27k3A[9]1 $\otimes \mathbb{Q}(-1)$	5	27
(1 <sub>9</sub> )	9k4A1 $\otimes \mathbb{Q}(-2)$	8	9
(1 <sub>12</sub> )	27k5A[9]1 $\otimes \mathbb{Q}(-3)$	11	27

Table 6.2: Some possible  $c$  in the case  $d = 3$ ,  $a_i = 1$  and the modular forms associated to the representations  $H(c)$ .

Again we find some products of  $\eta$ -functions;  $27A1 = \eta(3\tau)^2\eta(9\tau)^2$  as we saw before, and  $9k4A1 = \eta(3\tau)^8$ .

### 6.2.3 Representations in degree 4

$c=(2,1,1)$

Representations of degree 4 occur in diagonal equations of degree 4. In this case there are involutions of the type  $X_i \rightarrow -X_i$ , and for this reason the traces found are usually even. In particular, if we consider the diagonal elliptic curve defined by  $a_0X_0^2 + a_1X_1^4 + a_2X_2^4 = 0$  we see that the total number of points over an odd prime field is even, and since the contribution of the hyperplane sections equals  $p+1$ , the trace of the Frobenius action is also even. Therefore we can use Livné's theorem to identify the representations by comparing traces. The coefficients  $a_i$  can be chosen arbitrarily. We focus on coefficients that are powers of 2, since other coefficients introduce new bad primes. This raises the conductor of the curve and hence the level of the modular form, thus making it harder to find.

$a$	Modular form	Weight	Level
(1, 1, 1)	$64A1 = \eta(4\tau)^{-2}\eta(8\tau)^8\eta(16\tau)^{-2}$	2	64
(1, 1, 2)	256C1	2	256
(2, 1, 1)	$32A1 = \eta(4\tau)^2\eta(8\tau)^2$	2	32
(1, 1, 4)	32A1	2	32
(1, 2, 2)	32A1	2	32
(1, 2, 4)	256A1	2	256
(2, 1, 4)	64A1	2	64
(1, 1, 3)	288A1	2	288

Table 6.3: Representations for  $d = 4$ ,  $c = (2, 1, 1)$

$c=(1,1,1,1)$

This case is of special interest, since the corresponding diagonal equation of degree 4 defines a K3 surface. Again we take coefficients that are powers of 2.

$a$	Modular form	Weight	Level
(1, 1, 1, 1)	$16k3A[1,0]1 = \eta(4\tau)^6$	3	16
(1, 1, 1, 2)	256k3A[1,0]1	3	256
(1, 1, 1, 4)	16k3A[1,0]1	3	16
(1, 1, 2, 2)	16k3A[1,0]1	3	16
(1, 1, 4, 4)	$64k3A[1,0]1 = \eta(4\tau)^{-6}\eta(8\tau)^{18}\eta(16\tau)^{-6}$	3	64
(1, 2, 4, 4)	64k3A[1,0]1	3	64
(1, 4, 4, 4)	64k3A[1,0]1	3	64

Table 6.4: Representations for  $d = 4$ ,  $c = (1, 1, 1, 1)$ .

### 6.2.4 Representations in degree 6

As the degree becomes larger, the number of possible representations grows very quickly. Therefore we will calculate just one or two coefficient vectors  $a$  for each irreducible  $c$ . Again we have ramification only at 2 and 3. In the case  $n = 1$  the representation corresponds to the elliptic curve defined by  $a_0X_0^2 + a_1X_1^3 + a_2X_2^6 =$

0; so the traces of these representations are even for the same reason as given in 6.2.3. In all cases, we can use Schütt's Theorem 5.13 to identify the representations with those associated to modular forms.

$c$	$a$	Modular form	Weight	Level
(1, 2, 3)	(-1, 1, 1)	36A1	2	36
(1, 2, 3)	(1, 1, 1)	144B1	2	144
(1, 1, 4)	(-1, 1, 1)	108A1	2	108
(1, 1, 4)	(1, 1, 1)	432G1	2	432
(1, 1, 1, 3)	(1, 1, 1, 1)	27k3A[9]1	3	27
(1, 1, 1, 3)	(1, -1, 1, -1)	27k3A[9]1	3	27
(1, 1, 2, 2)	(1, 1, 1, 1)	48k3A[0,0,1]1	3	48
(1, 1, 2, 2)	(1, -1, -1, 1)	12k3A[0,1]1	3	12
(1, 1, 1, 1, 2)	(1, 1, 1, 1, 1)	108k4A1	4	108
(1, 1, 1, 1, 1, 1)	(1, 1, 1, -1, -1, -1)	27k5A[9]1	5	27
(1, 1, 1, 1, 1, 1)	(1, 1, 1, 1, 1, 1)	27k5A[9]1 $\otimes (-1)^{\frac{p-1}{2}}$	5	108

Table 6.5: Possible  $c$  in the case  $d = 6$  with  $a_i = \pm 1$  and the modular forms associated to the representations  $H(c, a)$ .

Again we find some products of  $\eta$ -functions:

- $12k3A[0,1]1 = \eta(2\tau)^3 \eta(6\tau)^3$ ;
- $36A1 = \eta(6\tau)^4$ ;
- $144B1 = \eta(6\tau)^{-4} \eta(12\tau)^{12} \eta(24\tau)^{-4}$ ;
- $48k3[0,0,1]1 = \eta(2\tau)^{-3} \eta(4\tau)^9 \eta(6\tau)^{-3} \eta(8\tau)^{-3} \eta(12\tau)^9 \eta(24\tau)^{-3}$ .

### 6.2.5 The representation $c = (1, 3, 4)$

In varieties of degrees 4 and 6 there are little problems in linking representations to modular forms, since the representations are all 2-dimensional. In degree 8 this is not the case. Nevertheless it is not too difficult to handle the case that all coefficients are equal, since then there is essentially just one representation in varieties of degree 8 that produces problems. By the inductive relations (3.12) and (3.13) we can reduce any Jacobi sum  $J_q^8(c)$  to a product of Jacobi sums of dimension 1 or 0. In degree 8 and dimension 1, the only possible vectors  $c$  (up to multiplication by a unit in  $\mathbb{Z}/8\mathbb{Z}$ ) are  $(1, 1, 6)$ ,  $(1, 2, 5)$  and  $(1, 3, 4)$ .

Now the Jacobi sum  $J_p(1, 1, 6)$  equals (for a prime  $p \equiv 1 \pmod{8}$ )

$$\begin{aligned}
 J_p(1, 1, 6) &= -p\Gamma_p\left(\frac{7}{8}\frac{7}{8}\frac{1}{4}\right) \\
 &= -(-1)^{r_p(3/8)} p\Gamma_p\left(\frac{1}{4}\frac{7}{8}\frac{7}{8}\frac{3}{8}\frac{5}{8}\right) \\
 &= -(-1)^{r_p(\frac{3}{8})} \sigma\left(2, \frac{3}{4}\right) p\Gamma_p\left(\frac{1}{4}\frac{1}{2}\frac{3}{4}\frac{7}{8}\frac{5}{8}\right) \\
 &= (-1)^{(p-1)/8} \sigma\left(2, \frac{1}{4}\right) p\Gamma_p\left(\frac{1}{2}\frac{7}{8}\frac{5}{8}\right) \\
 &= -(-1)^{(p-1)/8} \sigma\left(2, \frac{1}{4}\right) J_p(1, 3, 4)
 \end{aligned} \tag{6.14}$$

where we used the Gamma multiplication formula (3.92) with  $n = 2$  and  $X = \frac{3}{4}$ .

The same relation can be used to simplify  $J_p^8(1, 2, 5)$ :

$$\begin{aligned} J_p^8(1, 2, 5) &= -p\Gamma_p\left(\frac{3}{4}\frac{3}{8}\frac{7}{8}\right) \\ &= -\sigma\left(2, \frac{3}{4}\right)p\Gamma_p\left(\frac{3}{4}\frac{1}{2}\frac{3}{4}\right) \\ &= \sigma\left(2, \frac{3}{4}\right)J_p^8(2, 2, 4) = \sigma\left(2, \frac{3}{4}\right)J_p^4(1, 1, 2). \end{aligned} \tag{6.15}$$

The last Jacobi sum has degree 4 and is the eigenvalue of the modular representation with  $c = (1, 1, 2)$  we already know. So we see that the only Jacobi sum of degree 8 that we need to determine is  $J_q^8(1, 3, 4)$ . Therefore we will study the representation  $\rho(1, 3, 4)$  and the simplest diagonal variety that contains it: the curve  $C$  defined by

$$X_0^8 + X_1^8 + X_2^2 = 0$$

in  $\mathbb{P}(1, 1, 4)$ . This is a smooth curve of genus 3, and its middle cohomology decomposes into representations  $\rho(1, 3, 4)$  of dimension 4 and  $\rho(2, 2, 4)$  of dimension 2. Our aim is the following result.

**Proposition 6.6** *The rank 4 representation  $\rho(1, 3, 4)$  decomposes as a direct sum of two irreducible subrepresentations of rank 2. These representations are associated to the modular forms 256B1 and 256D1.*

**Proof** The orbit of  $c = (1, 3, 4)$  under  $(\mathbb{Z}/8\mathbb{Z})^*$  is equal to

$$\overline{(1, 3, 4)} = \{(1, 3, 4), (3, 1, 4), (5, 7, 4), (7, 5, 4)\}.$$

Since we have set all coefficients  $a_i$  equal to 1, we have permutation symmetry; the Frobenius eigenvalues are given by Jacobi sums, and these are invariant under permutation of arguments. It is tempting to conclude that  $\rho(1, 3, 4)$  is the direct sum of two isomorphic 2-dimensional representations, and hence the zeta factors would all be squares. Unfortunately this is only correct for primes  $p \equiv 1 \pmod{8}$ ; for other primes the relation between the elements of  $\overline{(1, 3, 4)}$  and the Frobenius eigenvalues is given by (3.60) and the fractional power in that formula destroys the expected square polynomial. Indeed, if we calculate some zeta factors we quickly see that they are no squares for primes equal to 3 modulo 8; however, they are decomposable over  $\mathbb{Z}[t]$  into factors of degree 2.

Since the permutation symmetry is clearly involved here, it is logical to consider the quotient of  $C$  under the symmetry  $S$  interchanging  $X_0$  and  $X_1$ . This is the smooth elliptic curve  $C'$  in  $\mathbb{P}(1, 1, 2)$ , defined by

$$Y_0^4 - 4Y_0^2Y_1^2 + 2Y_1^4 + Y_2^2 = 0.$$

(To see this, identify  $Y_0 = X_0^2 + X_1^2$  and  $Y_1 = X_0X_1$ .)

Everything being smooth except in characteristic 2, we know that the middle cohomology of  $C'$  equals

$$H_{\text{ét}}^1(C', \mathbb{Q}_\ell) = H_{\text{ét}}^1(C, \mathbb{Q}_\ell)^S,$$

the fixed part under the action of  $S$ . To determine which part this is, we calculate the zeta factors of  $F_{17}$  on  $C$ :

$$\begin{aligned} Z_{17}^8(2, 2, 4) &= (1 - 2t + 17t^2) \\ Z_{17}^8(1, 3, 4) &= (1 + 6t + 17t^2)^2 \end{aligned}$$

and hence the eigenvalues of the Frobenius element  $F_{17}$  with the proper multiplicities are  $\{1 \pm 4i, -3 \pm i\sqrt{2}, -3 \pm i\sqrt{2}\}$ .

By counting points we see that the trace  $\text{Tr}(F_{17}, H_{\text{ét}}^1(C', \mathbb{Q}_\ell)) = -6$ , which means that the only eigenvalues of  $F_{17}$  in  $H_{\text{ét}}^1(C', \mathbb{Q}_\ell)$  are  $-3 \pm i\sqrt{2}$  (with multiplicity one). This proves that the representation  $\rho(2, 2, 4)$  does not occur in  $H_{\text{ét}}^1(C', \mathbb{Q}_\ell)$ ; it consists of a 2-dimensional subspace of  $\rho(1, 3, 4)$ .

Therefore the cohomology of  $C$  decomposes into 2-dimensional subspaces

$$H_{\text{ét}}^1(C, \mathbb{Q}_\ell) = \rho(2, 2, 4) \oplus \rho(1, 3, 4)^S \oplus \rho(1, 3, 4)^{S^\perp}.$$

Here we denote by  $\rho(1, 3, 4)^{S^\perp}$  the complementing  $\rho$ -invariant space such that  $\rho(1, 3, 4) = \rho(1, 3, 4)^S \oplus \rho(1, 3, 4)^{S^\perp}$ . We know that  $\rho(2, 2, 4)$  is the representation associated to the modular form 64A1. By counting points and comparing traces we deduce that  $\rho(1, 3, 4)^S$  is the representation associated to the form 256B1; since  $\text{Tr}(\rho(1, 3, 4)^S)(F_{13}) = 0$ , Schütt's theorem applies and proves this identification.

Knowing the traces of the Frobenius elements on  $H_{\text{ét}}^1(C, \mathbb{Q}_\ell)$ ,  $\rho(2, 2, 4)$  and  $\rho(1, 3, 4)^S$ , we can calculate their traces on the subrepresentation  $\rho(1, 3, 4)^{S^\perp}$ . By another application of Schütt's theorem we conclude that this representation is associated to the modular form 256D1.  $\square$

In a totally analogous way we can prove the following.

**Proposition 6.7** *The rank 4 representation  $\rho(1, 5, 6)$  decomposes as a direct sum of two irreducible subrepresentations of rank 2. These representations are associated to the modular forms 576F1 and 576G1.*

**Proof** In this case we consider the diagonal curve  $C$  of degree 12 defined by

$$X_0^{12} + X_1^{12} + X_2^2 = 0$$

in  $\mathbb{P}(1, 1, 6)$ ; it has genus 5 and contains the representations  $\rho(1, 5, 6)$ ,  $\rho(2, 4, 6)$  (with multiplicity 2) and  $\rho(3, 3, 6)$ . The last two representations are modular and correspond to the forms 144B1 and 64A1 respectively.

Again we consider the quotient of this curve by  $S$ , the map exchanging  $X_0$  and  $X_1$ . The quotient curve  $C'$  has equation

$$Y_0^6 - 6Y_0^4Y_1^2 + 9Y_0^2Y_1^4 - 2Y_1^6 + Y_2^2 = 0$$

in  $\mathbb{P}(1, 1, 3)$ . This is a curve of genus 2. Again we check easily that both curves are smooth, and by calculating a few traces of Frobenius elements we deduce that

$$H_{\text{ét}}^1(C', \mathbb{Q}_\ell) = \rho(144B1) \oplus \rho(576F1).$$

Proceeding as in the previous theorem we can also calculate the traces of Frobenius on  $\rho(1, 5, 6)/\rho(1, 5, 6)^S$  and determine the modular form associated to it. This is 576G1.  $\square$

## 6.2.6 Representations in degree 12

In the Fermat curve of degree 12, there are two 4-dimensional representations that appear to behave differently than the others. This curve  $C$  is given by the equation

$$X_0^{12} + X_1^{12} + X_2^{12} = 0$$

in  $\mathbb{P}^2$ . The middle cohomology splits into subrepresentations of degree 4 or less; each is isomorphic to a representation  $\rho(c)$  with one of the  $c$  in

$$\{(1, 1, 10), (1, 2, 9), (1, 3, 8), (1, 4, 7), (1, 5, 6), (2, 2, 8), (2, 4, 6), (3, 3, 6), (4, 4, 4)\}.$$

To connect a representation like  $\rho(1, 4, 7)$  to a modular form we proceed as follows. First we express the corresponding factor in the zeta function in terms of the  $p$ -adic Gamma function. For a prime  $p \equiv 1 \pmod{12}$  (which is usually the hardest case) this is

$$\begin{aligned} Z_p^{12}(1, 1, 10) = & (1 + \Gamma_p(\frac{1}{12} \frac{1}{12} \frac{5}{6})t)(1 + \Gamma_p(\frac{5}{12} \frac{5}{12} \frac{1}{6})t) \\ & (1 - p\Gamma_p(\frac{7}{12} \frac{7}{12} \frac{5}{6})t)(1 - p\Gamma_p(\frac{11}{12} \frac{11}{12} \frac{1}{6})t) \end{aligned} \quad (6.16)$$

We focus on the first factor and simplify it by using properties of the  $p$ -adic Gamma function:

$$\begin{aligned} \Gamma_p(\frac{1}{12} \frac{1}{12} \frac{5}{6}) &= (-1)^{r_p(5/12)} \Gamma_p(\frac{1}{12} \frac{1}{12} \frac{5}{6} \frac{5}{12} \frac{7}{12}) \\ &= (-1)^{(p+11)/12+r_p(1/4)} \sigma(2, \frac{1}{6}) \Gamma_p(\frac{1}{6} \frac{5}{6} \frac{1}{12} \frac{5}{12} \frac{9}{12} \frac{3}{12} \frac{1}{2}) \\ &= (-1)^{r_p(1/6)} \sigma(2, \frac{1}{6}) \sigma(3, \frac{1}{4}) \Gamma_p(\frac{1}{3} \frac{2}{3} (\frac{1}{4})^2 \frac{1}{2}) \\ &= -\sigma(2, \frac{1}{6}) \sigma(3, \frac{1}{4}) \Gamma_p((\frac{1}{4})^2 \frac{1}{2}). \end{aligned} \quad (6.17)$$

The powers of  $-1$  can easily be determined since we know the equivalence class of  $p$  modulo 12. We repeatedly use identities from Section 3.7; in particular the Gamma multiplication formula (3.92) is used twice. A totally analogous calculation shows that

$$\begin{aligned} \Gamma_p(\frac{5}{12} \frac{5}{12} \frac{1}{6}) &= \sigma(2, \frac{5}{6}) \sigma(3, \frac{1}{4}) \Gamma_p(\frac{3}{4} \frac{2}{4} \frac{1}{2}), \\ \Gamma_p(\frac{7}{12} \frac{7}{12} \frac{5}{6}) &= -\sigma(2, \frac{1}{6}) \sigma(3, \frac{3}{4}) \Gamma_p(\frac{1}{4} \frac{2}{4} \frac{1}{2}), \\ \Gamma_p(\frac{11}{12} \frac{11}{12} \frac{1}{6}) &= \sigma(2, \frac{5}{6}) \sigma(3, \frac{3}{4}) \Gamma_p(\frac{3}{4} \frac{2}{4} \frac{1}{2}). \end{aligned} \quad (6.18)$$

These products of Gamma functions also occur in the representation  $\rho(1, 1, 2)$  in degree 4. This representation has zeta factor

$$Z_p^4(1, 1, 2) = (1 + \Gamma_p(\frac{1}{4} \frac{1}{4} \frac{1}{2})t)(1 - p\Gamma_p(\frac{3}{4} \frac{3}{4} \frac{1}{2})t).$$

Furthermore we know that 3 is always a square in  $\mathbb{Z}/p\mathbb{Z}$  if  $p \equiv 1 \pmod{12}$ . Therefore  $\sigma(3, \frac{1}{4}) = \sigma(3, \frac{3}{4}) = \pm 1$  for these primes by Corollary 3.22. So we have

$$Z_p^{12}((1, 1, 10), t) = Z_p^4((1, 1, 2), \sigma(3, \frac{1}{4})t) \otimes (1 + \sigma(2, \frac{1}{6})t)(1 + \sigma(2, \frac{5}{6})t).$$

Both factors are polynomials, since  $\sigma(2, \frac{1}{6})$  and  $\sigma(2, \frac{5}{6})$  are conjugate sixth roots of unity.

If we do the same calculation for the other equivalence classes of  $p$  modulo 12, we find that  $Z_p^{12}((1, 1, 10), t)$  equals

$$\begin{aligned} Z_p^4((1, 1, 2), \sigma(3, \frac{1}{4})t) \otimes (1 + \sigma(2, \frac{1}{6})t)(1 + \sigma(2, \frac{5}{6})t) & \text{ if } p \equiv 1 \pmod{12} \\ Z_p^4((1, 1, 2), t) \otimes (1 + t^2) & \text{ if } p \equiv 5 \pmod{12} \\ Z_p^4((1, 1, 2), t) \otimes (1 + \sigma(2, \frac{1}{6})t)(1 + \sigma(2, \frac{5}{6})t) & \text{ if } p \equiv 7 \pmod{12} \\ Z_p^4((1, 1, 2), t) \otimes (1 - t^2) & \text{ if } p \equiv 11 \pmod{12}. \end{aligned}$$

In this way the zeta function of this representation can be linked to the modular representation  $\rho(1, 1, 2)$ .

Similar calculations can be done for representations  $\rho(c)$  with  $c = (1, 4, 7)$  and  $c = (1, 5, 6)$ . If we consider  $c = (1, 3, 8)$ , this does not work so well. For this reason we can not connect the zeta factors  $Z_p(c, t)$  of these representations to modular forms directly; however, for the factors  $Z_{p^m}(c, t)$  this is possible for a sufficiently high  $m$ . Geometrically this means that we pass to a finite extension field; we consider  $C$  as a curve over  $\mathbb{Q}(\alpha)$ , with  $\alpha$  an appropriate algebraic number, instead of  $\mathbb{Q}$ .

Let us consider  $c = (1, 3, 8)$  first. Using similar manipulations as before we can show that

$$J_p^{12}(1, 3, 8)^2 = \sigma(3, \frac{1}{4})(-1)^{r_p(5/12)+r_p(1/2)} J_p^4(1, 1, 2)^2,$$

which indicates that we should expect  $\rho(1, 3, 8)$  to be associated to the modular form 64A1 in the appropriate extension field. We find the following:

$$\begin{aligned} Z_{p^2}^{12}((1, 3, 8), t) &= Z_{p^2}^4((1, 1, 2), \sigma(3, \frac{1}{4})t)^2 & \text{ if } p \equiv 1 \pmod{12} \\ Z_{p^4}^{12}((1, 3, 8), t) &= Z_{p^4}^4((1, 1, 2), -t)^2 & \text{ if } p \equiv 5 \pmod{12} \\ Z_p^{12}((1, 3, 8), t) &= Z_p^4((1, 1, 2), it)^2 & \text{ if } p \equiv 7 \pmod{12} \\ Z_p^{12}((1, 3, 8), t) &= Z_p^4((1, 1, 2), t)^2 & \text{ if } p \equiv 11 \pmod{12}. \end{aligned}$$

For the number  $\alpha$  we could take  $\sqrt[4]{3}$ . Since 3 and  $-3$  are both not square for any  $p \equiv 5 \pmod{12}$ , the polynomial  $X^4 - 3$  is irreducible and  $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^4}$  for such  $p$ .

Along the same lines we can treat the representation  $\rho(1, 2, 9)$ . It is connected to the modular form 144B1 =  $\eta(6\tau)^{-4}\eta(12\tau)^{12}\eta(24\tau)^{-4}$ , which is the form corresponding to the representation with  $c = (1, 2, 3)$ . The zeta factors are

$$\begin{aligned} Z_{p^2}^{12}((1, 2, 9), t) &= Z_{p^2}^6((1, 2, 3), t)^2 \otimes (-1)^{\frac{p-1}{12}} \sigma(3, \frac{1}{4}) & \text{ if } p \equiv 1 \pmod{12} \\ Z_{p^4}^{12}((1, 2, 9), t) &= Z_{p^4}^6((1, 2, 3), -t)^2 & \text{ if } p \equiv 5 \pmod{12} \\ Z_{p^2}^{12}((1, 2, 9), t) &= Z_{p^2}^6((1, 2, 3), -t)^2 & \text{ if } p \equiv 7 \pmod{12} \\ Z_{p^4}^{12}((1, 2, 9), t) &= Z_{p^4}^6((1, 2, 3), t)^2 & \text{ if } p \equiv 11 \pmod{12}. \end{aligned}$$

It seems inconvenient that we need to pass to an extension field of degree 4 before the factors can be identified, but this happens just because we insisted that  $Z_p^{12}(1, 2, 9)$  should be related to  $Z_p^6(1, 2, 3)$ . In fact, we have

$$Z_p^{12}((1, 2, 9), t) = 1 + p^2 t^4$$

for all  $p \equiv 5 \pmod{12}$  and

$$Z_p^{12}((1, 2, 9), t) = (1 + pt^2)^2$$

for  $p \equiv 11 \pmod{12}$ . So to find the factors of the zeta function we need only an extension of degree 2.

## 6.3 Zeta functions of varieties

It is interesting to have examples where we can give the zeta function of the entire variety. This is possible for many diagonal varieties of low degree. We have already seen this for a number of curves. In this section we will give some more examples, focusing on the case of Calabi-Yau varieties.

The tables in this section give decompositions of the middle cohomology of diagonal varieties. Given such a variety  $X$  of degree  $d$ , we subsequently give a representative  $c$  of an orbit in  $C(X)$  under the action of  $(\mathbb{Z}/d\mathbb{Z})^*$ , the multiplicity of the corresponding representation  $\rho(c)$  found by permuting the entries of  $c$ , the dimension of the representation and a description of the corresponding zeta-factors. For singular varieties, we denote the contribution from the singular fibers below a second horizontal line. If a power of the hyperplane class  $H$  is present in the middle cohomology, it is listed first of all.

Since the varieties considered are Calabi-Yau, there is one special orbit  $\bar{c}$  such that  $\rho(c)$  contains  $H^0(X, \Omega_X)$ . This  $\bar{c}$  is always listed first.

We start with Calabi-Yau varieties of dimension 2, which are commonly called K3 surfaces.

### 6.3.1 The Fermat quartic

The simplest example of a diagonal K3 surface is the Fermat surface  $M_4$  of degree 4, defined over  $\mathbb{Q}$  by the equation

$$X_0^4 + X_1^4 + X_2^4 + X_3^4 = 0 \tag{6.19}$$

in  $\mathbb{P}^3$ . This surface is obviously smooth, it has degree 4 and it has good reduction to any field of odd characteristic. Like any K3 surface, its Hodge diamond is

$$\begin{array}{ccccc} & & & & 1 \\ & & & 0 & 0 \\ & & 1 & 20 & 1 \\ & & 0 & 0 & \\ & & & & 1 \end{array} \tag{6.20}$$

The middle cohomology can be broken up into subrepresentations as follows.

Subspace	Mult.	Dim.	Representation
$H$	—	1	$\mathbb{Q}(-1)$
$(1, 1, 1, 1)$	1	2	$16k3A[1,0]1$
$(1, 1, 3, 3)$	3	2	$\mathbb{Q}(-1) \oplus \mathbb{Q}(-1) \otimes \rho_0(2)$
$(1, 2, 2, 3)$	6	2	$\rho_0(4) \otimes \rho_0(2) \otimes \mathbb{Q}(-1)$
$(2, 2, 2, 2)$	1	1	$\mathbb{Q}(-1)$

Table 6.6: The middle cohomology of the Fermat quartic and its decomposition into subrepresentations.

This describes the entire middle cohomology; as expected, we see that the total dimension is 22.

### 6.3.2 Exponents (2,6,6,6)

Another example of a K3 surface where we can determine all zeta factors is the the variety defined by

$$X_0^2 + X_1^6 + X_2^6 + X_3^6 = 0 \tag{6.21}$$

in  $\mathbb{P}(3, 1, 1, 1)$ , with degree  $d = 6$ . This variety is smooth. The middle cohomology decomposes as follows.

Subspace	Mult.	Dim.	Representation
$H$	—	1	$\mathbb{Q}(-1)$
$(3, 1, 1, 1)$	1	2	$27k3A[9]1$
$(3, 1, 3, 5)$	3	2	$\mathbb{Q}(-1) \otimes \rho_0(2) \otimes \rho_0(6)$
$(3, 1, 4, 4)$	3	2	(see below)
$(3, 3, 2, 4)$	3	2	$\mathbb{Q}(-1) \otimes \rho_0(2) \otimes \rho_0(3)$
$(3, 3, 3, 3)$	1	1	$\mathbb{Q}(-1)$

Table 6.7: The middle cohomology of the diagonal K3 surface with exponents (2, 6, 6, 6).

Most of these representations have been treated before; only  $c = (3, 1, 4, 4)$  is unknown. The zeta-factors of this representation can be found by using the Gamma multiplication formula (3.92) with  $n = 2$  and  $X = 1/3$  or  $X = 2/3$ . For primes  $p$  that are  $1 \pmod{6}$  we have

$$\begin{aligned} Z_p(c, t) &= (1 - pt\Gamma_p(\frac{1}{2}, \frac{1}{6}, \frac{2}{3}, \frac{2}{3}))(1 - pt\Gamma_p(\frac{1}{2}, \frac{5}{6}, \frac{1}{3}, \frac{1}{3})) \\ &= (1 - pt\Gamma_p(\frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{2}{3})\sigma(2, \frac{1}{3}))(1 - pt\Gamma_p(\frac{1}{2}, \frac{1}{2}, \frac{1}{3}, \frac{2}{3})\sigma(2, \frac{2}{3})) \\ &= (1 - (-1)^{(p-1)/2}pt\sigma(2, \frac{1}{3}))(1 - (-1)^{(p-1)/2}pt\sigma(2, \frac{2}{3})) \\ &= \begin{cases} (1 - pt)^2 & \text{if } p \equiv 1 \pmod{4} \text{ and } 2 \text{ is a third power} \\ (1 + pt)^2 & \text{if } p \equiv 3 \pmod{4} \text{ and } 2 \text{ is a third power} \\ 1 + pt + p^2t^2 & \text{if } p \equiv 1 \pmod{4} \text{ and } 2 \text{ is no third power} \\ 1 - pt + p^2t^2 & \text{if } p \equiv 3 \pmod{4} \text{ and } 2 \text{ is no third power.} \end{cases} \end{aligned} \tag{6.22}$$

If  $p \equiv 5 \pmod{6}$  we have

$$\begin{aligned} Z_p(c, t) &= 1 - p^2t^2\Gamma_p((\frac{1}{2})^2, \frac{1}{6}, \frac{5}{6}, (\frac{1}{3})^2, (\frac{2}{3})^2) \\ &= 1 - p^2t^2 \end{aligned} \tag{6.23}$$

Again we find that the middle cohomology has dimension 22. This is correct, since this surface does not intersect the only singular point  $(1 : 0 : 0 : 0)$  of the weighted projective space and hence it is smooth.

### 6.3.3 Exponents (3,3,6,6)

Next, we consider the K3 surface that is the resolution of the singular variety defined by

$$X_0^3 + X_1^3 + X_2^6 + X_3^6 = 0. \quad (6.24)$$

This surface has a singular point  $(1 : -1 : 0 : 0)$ , existing over any field of definition, and if the field of definition contains a primitive third root of unity  $\zeta$  there are two more singular points  $(1 : -\zeta : 0 : 0)$  and  $(1 : -\zeta^2 : 0 : 0)$ . Each is resolved to a  $\mathbb{P}^1$ , which implies that the resolution contains  $3q$  extra points if  $q \equiv 1 \pmod{3}$ , and just  $q$  if  $q \equiv 2 \pmod{3}$ . So in the first case we have a factor of  $(1 - qt)^3$  corresponding to the exceptional divisor in the zeta function, and in the second case  $(1 - qt)(1 - q^2t^2)$ .

The middle cohomology of the variety decomposes as follows.

Subspace	Mult.	Dim.	Representation
$H$	—	1	$\mathbb{Q}(-1)$
$(2, 2, 1, 1)$	1	2	$12k3A[0,1]1$
$(4, 4, 1, 3)$	2	2	See above
$(2, 2, 4, 4)$	3	2	$\rho_0(3) \otimes \mathbb{Q}(-1)$
$(2, 4, 1, 5)$	2	2	$\mathbb{Q}(-1) \oplus \mathbb{Q}(-1) \otimes \rho_0(2)$
$(2, 4, 3, 3)$	1	2	$\rho_0(3) \otimes \rho_0(2) \otimes \mathbb{Q}(-1)$
Exceptional	—	3	$\mathbb{Q}(-1) \oplus \mathbb{Q}(-1) \otimes \rho_0(3)$

As expected, the total dimension adds up to 19. Together with the three cycles produced by the resolution of singularities this adds up to 22.

### 6.3.4 A tensor product representation

Many varieties under consideration contain a tensor product of representations. Consider the surface defined by the equation

$$X_0^2 + X_1^3 + X_2^{12} + X_3^{12} = 0. \quad (6.25)$$

This surface contains one singular point  $(1 : -1 : 0 : 0)$ , which is blown up into a  $\mathbb{P}_1$ . The middle cohomology of the variety decomposes as follows.

Subspace	Mult.	Dim.	Representation
$H$	—	1	$\mathbb{Q}(-1)$
$(6, 4, 1, 1)$	1	4	$27A1 \otimes 64A1 \otimes \chi_1$
$(6, 4, 3, 11)$	2	4	See below
$(6, 4, 4, 10)$	2	2	See Table 6.7
$(6, 4, 6, 8)$	2	2	$\rho_0(3) \otimes \mathbb{Q}(-1) \otimes \rho_0(2)$
Exceptional	—	1	$\mathbb{Q}(-1)$

Table 6.8: The middle cohomology for  $e = (2, 3, 12, 12)$ .

The representation  $\rho(6, 4, 1, 1)$  is closely related to the tensor product representation we treated as an example in Section 6.1. We can decompose  $(6, 4, 1, 1) = (6, 5, 1) \vee (1, 4, 7)$ . The Jacobi sums corresponding to the factors can be simplified

using the Gamma multiplication formula. For the first one we have (for a prime  $p \equiv 1 \pmod{12}$ )

$$J_p^{12}(6, 5, 1) = p\Gamma_p\left(\frac{1}{2}, \frac{7}{12}, \frac{11}{12}\right) \quad (6.26)$$

and the multiplication formula (3.92) with  $n = 3$  and  $X = \frac{3}{4}$  yields

$$\Gamma_p\left(\frac{3}{12}, \frac{7}{12}, \frac{11}{12}\right) = \Gamma_p\left(\frac{3}{4}, \frac{1}{3}, \frac{2}{3}\right)\sigma\left(3, \frac{3}{4}\right).$$

So we find that

$$\begin{aligned} J_p^{12}(6, 5, 1) &= \sigma\left(3, \frac{1}{4}\right)(-1)^{r_p(\frac{1}{4})+r_p(\frac{1}{3})} J_p^{12}(6, 3, 3) \\ &= -\sigma\left(3, \frac{1}{4}\right)(-1)^{r_p(\frac{1}{4})} J_p^{12}(6, 3, 3) \end{aligned} \quad (6.27)$$

and we know  $J_p^{12}(6, 3, 3) = J_p^4(2, 1, 1)$  is an eigenvalue in the Galois representation associated to the diagonal elliptic curve with exponents  $(2, 4, 4)$ . The symbol  $\sigma\left(3, \frac{1}{4}\right)$  is  $\pm 1$  by Corollary 3.22, since 3 is a square for all primes  $p \equiv 1 \pmod{12}$ . Therefore the zeta factors corresponding to  $c = (1, 5, 6)$  are equal to those corresponding to  $c = (6, 3, 3)$  with a possible substitution  $t \rightarrow -t$ . They are the characteristic polynomials of the representation associated to the modular form 64A1.

The Jacobi sum  $J_p^{12}(1, 4, 7)$  can be simplified likewise by taking  $n = 2$  and  $X = \frac{5}{6}$  in (3.92). This produces the relation

$$\Gamma_p\left(\frac{5}{12}, \frac{11}{12}\right) = \Gamma_p\left(\frac{5}{6}, \frac{1}{2}\right)\sigma\left(2, \frac{5}{6}\right),$$

and for the Jacobi sum this yields

$$J_p^{12}(1, 4, 7) = J_p^{12}(2, 4, 6)\sigma\left(2, \frac{5}{6}\right) = J_p^6(1, 2, 3)\sigma\left(2, \frac{5}{6}\right). \quad (6.28)$$

It is convenient to simplify this further by using the multiplication formula again with  $n = 2$ ,  $X = 2/3$ . We find

$$\begin{aligned} J_p^6(1, 2, 3)\sigma\left(2, \frac{5}{6}\right) &= J_p^6(2, 2, 2)(-1)^{r_p(\frac{1}{2})+r_p(\frac{1}{3})}\sigma\left(2, \frac{5}{6}\right)\sigma\left(2, \frac{2}{3}\right) \\ &= J_p^6(2, 2, 2)\sigma\left(2, \frac{1}{2}\right) \end{aligned} \quad (6.29)$$

since  $\sigma$  is additive in its second component. Again the  $\sigma$  symbol is  $\pm 1$ ; in fact, it is 1 if  $p \equiv 1 \pmod{8}$  and  $-1$  if  $p \equiv 5 \pmod{8}$ . The factors  $J_p^6(2, 2, 2) = J^3(1, 1, 1)$  have been found before; they are associated to the modular form 27A1.

So we find that  $Z_p^{12}(6, 4, 1, 1) = Z_p^4(2, 1, 1) \otimes Z_p^3(1, 1, 1) \otimes \chi_1$ , where  $\chi_1$  is a twist:

$$\chi_1(t) = \begin{cases} (-1)^{r_p(\frac{1}{4})}\sigma\left(2, \frac{1}{2}\right)\sigma\left(3, \frac{1}{4}\right) & \text{if } p \equiv 1 \pmod{12} \\ 1 & \text{otherwise.} \end{cases} \quad (6.30)$$

For primes  $p \not\equiv 1 \pmod{12}$  we have similar (but simpler) expressions for the Jacobi sums and the zeta factors, which can be manipulated by the same relations. We find that the same relation between zeta factors holds, but the  $\chi_1$  can be ignored; it always acts trivially.

The representation with  $c = (6, 4, 3, 11)$  can also be determined by using the Gamma functions, but only up to a sign. If we calculate its zeta factors for some primes, we see that all eigenvalues seem to be fourth roots of unity times  $p$ , but it is not always possible to determine which.

Again we start by considering the zeta factor for a prime  $p \equiv 1 \pmod{12}$ . Then we have

$$Z_p^{12}(6, 4, 3, 11) = (1 - pt\Gamma_p(\frac{1}{2}\frac{1}{3}\frac{1}{4}\frac{11}{12}))(1 - pt\Gamma_p(\frac{1}{2}\frac{2}{3}\frac{3}{4}\frac{1}{12})) \\ (1 - pt\Gamma_p(\frac{1}{2}\frac{2}{3}\frac{1}{4}\frac{7}{12}))(1 - pt\Gamma_p(\frac{1}{2}\frac{1}{3}\frac{3}{4}\frac{5}{12})). \quad (6.31)$$

From the Reflection formula (Theorem 3.20) we deduce that for all odd  $p$  we have  $\Gamma_p(\frac{1}{2}\frac{1}{3}\frac{1}{4}\frac{11}{12}) = 1/\Gamma_p(\frac{1}{2}\frac{2}{3}\frac{3}{4}\frac{1}{12})$  and  $\Gamma_p(\frac{1}{2}\frac{1}{3}\frac{3}{4}\frac{5}{12}) = 1/\Gamma_p(\frac{1}{2}\frac{2}{3}\frac{1}{4}\frac{7}{12})$ . Furthermore, we can use the multiplication formula twice to deduce that

$$\Gamma_p(\frac{1}{2}\frac{1}{3}\frac{1}{4}\frac{11}{12}) = \sigma(2, \frac{1}{2})(-1)^{r_p(1/2)+r_p(5/12)}\Gamma_p(\frac{1}{2}\frac{1}{3}\frac{3}{4}\frac{7}{12}) = \Gamma_p(\frac{1}{2}\frac{1}{3}\frac{3}{4}\frac{7}{12}).$$

So we have a double root. By another application of the multiplication formula we find

$$\Gamma_p(\frac{1}{2}\frac{2}{3}\frac{1}{4}\frac{7}{12}) = (-1)^{r_p\frac{1}{12}}\sigma(3, \frac{3}{4})\Gamma_p(\frac{1}{2}\frac{2}{3}\frac{3}{4}\frac{1}{12})$$

and since  $\sigma(3, \frac{3}{4}) = \pm 1$  as noted before, this implies that  $\Gamma_p(\frac{1}{2}\frac{1}{3}\frac{1}{4}\frac{11}{12})$  is either equal to its inverse or equal to minus its inverse. In the latter case the factor  $Z_p^{12}(6, 4, 3, 11) = (1 + p^2t^2)^2$ ; in the former it can be either  $(1 - pt)^4$  or  $(1 + pt)^4$ . Both occur; at present it is unclear what mechanism determines this.

The other equivalence classes modulo 12 can be determined easily, since the Gamma functions mostly cancel each other; we find

$$Z_p^{12}(6, 4, 3, 11) = \begin{cases} 1 + p^4t^4 & \text{if } p \equiv 5 \pmod{12} \\ (1 + p^2t^2)^2 & \text{if } p \equiv 7 \pmod{12} \\ (1 - p^2t^2)^2 & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

### 6.3.5 A K3 surface of degree 8

Tensor products also appear in diagonal varieties of degree 8. As an example, we consider the variety defined by

$$X_0^2 + X_1^4 + X_2^8 + X_3^8 = 0 \quad (6.32)$$

in the weighted projective space  $\mathbb{P}(4, 2, 1, 1)$ . This surface has two singular points at  $X_2 = X_3 = 0$ , that are blown up to a  $\mathbb{P}^1$  each. The resolution of singularities is a K3 surface.

Subspace	Mult.	Dim.	Representation
$H$	—	1	$\mathbb{Q}(-1)$
$(4, 2, 1, 1)$	1	4	$64A1 \otimes 256D1 \otimes \chi_2$
$(4, 2, 3, 7)$	1	4	See below
$(4, 4, 1, 7)$	1	4	See below
$(4, 2, 4, 6)$	3	2	$\rho_0(8) \otimes \rho_0(2) \otimes \mathbb{Q}(-1)$
$(4, 4, 4, 4)$	1	1	$\mathbb{Q}(-1)$
Exceptional	2	1	$\mathbb{Q}(-1)$

Table 6.9: The middle cohomology for  $e = (2, 4, 8, 8)$ .

The first representation in our list can be identified by manipulating its expression in terms of Gamma functions. The essence of the calculation is the manipulation of the Jacobi sum  $J_p^8(1, 1, 2, 4)$  for a  $p \equiv 1 \pmod{8}$ . We have by (3.10)

$$\begin{aligned}
 J_p^8(1, 1, 2, 4) &= p^2 \Gamma_p\left(\frac{7^2 3}{8} \frac{1}{4} \frac{1}{2}\right) \\
 &= p^2 (-1)^{r_p(3/8)} \Gamma_p\left(\frac{7^2 3}{8} \frac{5}{8} \frac{3}{8} \frac{1}{4} \frac{1}{2}\right) \\
 &= p^2 (-1)^{r_p(3/8)} \sigma\left(2, \frac{3}{4}\right) \Gamma_p\left(\frac{7}{8} \frac{5}{8} \frac{3}{4} \frac{1}{2} \frac{1}{2}\right) \\
 &= p (-1)^{r_p(3/8)} \sigma\left(2, \frac{3}{4}\right) \Gamma_p\left(\frac{7}{8} \frac{5}{8} \frac{1}{2}\right) J_p^4(1, 1, 2),
 \end{aligned} \tag{6.33}$$

and  $p \Gamma_p\left(\frac{7}{8} \frac{5}{8} \frac{1}{2}\right)$  is the Frobenius eigenvalue of the representation  $\rho(256D1)$  found in subsection 6.2.5. By comparing the exact expressions for the zeta factors we find that

$$\rho(1, 1, 2, 4) = \rho(1, 1, 2) \otimes \rho(256D1) \otimes \chi_2,$$

where  $\chi_2$  is a symbol defined by

$$\chi_2(p) = \begin{cases} (-1)^{(p-1)/8} \sigma\left(2, \frac{1}{4}\right) & \text{If } p \equiv 1 \pmod{8} \\ i & \text{If } p \equiv 3 \pmod{8} \\ 1 & \text{otherwise.} \end{cases}$$

The representation with  $c = (4, 2, 3, 7)$  can be identified in the same way. The Jacobi sum  $J_p^8(4, 2, 3, 7)$  contains the factors  $\Gamma_p\left(\frac{1}{8}\right)$  and  $\Gamma_p\left(\frac{5}{8}\right)$ , that can be simplified using the Gamma multiplication formula with  $n = 2$  and  $X = \frac{1}{4}$ . We find that its zeta factors are

$$Z_p^8(4, 2, 3, 7) = \begin{cases} (1 - \sigma\left(2, \frac{1}{4}\right)pt)^4 & \text{If } p \equiv 1 \pmod{8} \\ (1 + p^2t^2)^2 & \text{If } p \equiv 5 \pmod{8} \\ (1 - p^2t^2)^2 & \text{If } p \equiv 3 \pmod{4}. \end{cases}$$

The other representations in this variety have a reducible  $c$  and hence they give very simple expressions. For  $c = (4, 4, 1, 7)$  we have

$$Z_p^8(4, 4, 1, 7) = \begin{cases} (1 - (-1)^{(p-1)/8}pt)^4 & \text{If } p \equiv 1 \pmod{8} \\ (1 + p^2t^2)^2 & \text{If } p \equiv 3 \pmod{8} \text{ or } p \equiv 5 \pmod{8} \\ (1 - p^2t^2)^2 & \text{If } p \equiv 7 \pmod{8}. \end{cases}$$

## 6.4 Calabi-Yau threefolds

In some cases we can find zeta functions and  $L$ -series of a Calabi-Yau threefold. In each case there are just a few representations with an irreducible  $c$ .

### 6.4.1 The Calabi-Yau of degree 6

There is one set of exponents  $e$  that define a diagonal Calabi-Yau threefold with degree 6. The corresponding equation is

$$X_0^3 + X_1^6 + X_2^6 + X_3^6 + X_4^6 = 0. \tag{6.34}$$

Using Theorem 2.12 we see that the variety defined by this equation is smooth. By the formulas given in Section 2.5 we can compute its Hodge numbers.

$$\begin{array}{ccccccc}
 & & & & 1 & & \\
 & & & & 0 & & 0 \\
 & & & 0 & 1 & & 0 \\
 1 & & 103 & & 103 & & 1 \\
 & & 0 & & 1 & & 0 \\
 & & 0 & & 0 & & \\
 & & & & 1 & & 
 \end{array} \tag{6.35}$$

The middle cohomology decomposes as follows.

Subspace	Mult.	Dim.	Representation
(2, 1, 1, 1, 1)	1	2	108k4A1
(2, 1, 3, 1, 5)	12	2	36A1 $\otimes$ $\mathbb{Q}(-1)$
(2, 1, 1, 4, 4)	18	2	432G1 $\otimes$ $\mathbb{Q}(-1)$
(2, 2, 2, 1, 5)	12	2	27A1 $\otimes$ $(-1)^{\frac{p-1}{2}} \otimes \mathbb{Q}(-1)$
(2, 1, 2, 3, 4)	36	2	144B1 $\otimes$ $\mathbb{Q}(-1)$
(2, 1, 3, 3, 3)	4	2	36A1 $\otimes$ $\mathbb{Q}(-1)$
(4, 5, 1, 1, 1)	4	2	108A1 $\otimes$ $\mathbb{Q}(-1)$
(2, 2, 2, 2, 4)	5	2	27A1 $\otimes$ $\mathbb{Q}(-1)$
(2, 2, 2, 3, 3)	6	2	27A1 $\otimes$ $(-1)^{\frac{p-1}{2}} \otimes \mathbb{Q}(-1)$
(4, 5, 1, 1, 1)	6	2	108A1 $\otimes$ $\mathbb{Q}(-1)$

Table 6.10: The middle cohomology of the diagonal variety with exponents (3, 6, 6, 6, 6) .

The first of these representations can be identified via Schütt’s theorem 5.13. The other are all reducible; for example,  $(2, 1, 3, 1, 5) = (2, 1, 3) \cup (1, 5)$ . From Table 5.5 we know that  $c = (2, 1, 3)$  gives the representation associated to the modular form 144B1. The (1,5) just gives a twist to this representation, as can be checked by Lemma 6.5. Alternatively, we can apply either Schütt’s or Livné’s theorem directly to  $\rho(2, 1, 3, 1, 5)$ . In this way we can prove that the twist transforms 144B1 into 36A1.

### 6.4.2 Exponents (4,4,4,8,8)

Passing to degree 8, we find there are two sets of exponents that define diagonal Calabi-Yau threefolds. First we consider the variety defined by

$$X_0^4 + X_1^4 + X_2^4 + X_3^8 + X_4^8 = 0 \tag{6.36}$$

in  $\mathbb{P}(2, 2, 2, 1, 1)$ . Its singular part consists of the curve  $C$  defined by

$$X_0^4 + X_1^4 + X_2^4 = 0, \quad X_3 = X_4 = 0$$

which is resolved to  $C \times \mathbb{P}^1$ .

The Hodge numbers of the resolved variety are

$$\begin{array}{ccccccc}
 & & & & 1 & & \\
 & & & & 0 & & 0 \\
 & & & 0 & 2 & & 0 \\
 & & 1 & 86 & 86 & & 1 \\
 & & & 0 & 2 & & 0 \\
 & & & 0 & 0 & & \\
 & & & & 1 & & 
 \end{array} \tag{6.37}$$

as follows from Chapter 2.

The middle cohomology decomposes as follows.

Subspace	Mult.	Dim.	Representation
$(2, 2, 2, 1, 1)$	1	4	$64k3A[1,0]1 \otimes 256D1 \otimes \chi_2$
$(2, 2, 2, 3, 7)$	1	4	$36A1 \otimes \mathbb{Q}(-1) \otimes \psi_1$ (See below)
$(2, 2, 4, 1, 7)$	6	4	$64A1 \otimes \rho_0(8) \otimes \mathbb{Q}(-1)$
$(2, 2, 6, 1, 5)$	3	4	$64A1 \otimes \mathbb{Q}(-1) \otimes \psi_1$
$(2, 6, 6, 1, 1)$	3	4	$64A1 \otimes \mathbb{Q}(-1) \otimes \psi_2$
$(2, 4, 4, 1, 5)$	3	4	$64A1 \otimes \mathbb{Q}(-1) \otimes \psi_1$
$(6, 4, 4, 1, 1)$	3	4	$64A1 \otimes \mathbb{Q}(-1) \otimes \psi_2$
$(2, 6, 4, 1, 3)$	6	4	$256B1 \otimes 256D1 \otimes \mathbb{Q}(-1)$
$(4, 4, 4, 1, 3)$	1	4	$256B1 \otimes 256D1 \otimes \mathbb{Q}(-1)$
$(2, 2, 2, 4, 6)$	20	2	$32A1 \otimes \mathbb{Q}(-1)$
$(2, 2, 4, 4, 4)$	10	2	$64A1 \otimes \mathbb{Q}(-1)$
Exceptional	3	2	$64A1 \otimes \mathbb{Q}(-1)$

Table 6.11: The middle cohomology for  $e = (4, 4, 4, 8, 8)$ .

The representation with  $c = (2, 2, 2, 1, 1)$  can be identified using the same calculation we used in subsection 6.3.5 to identify the representation  $\rho(1, 1, 2, 4)$ ; the symbol  $\chi_2$  is also the same.

The second representation  $\rho(2, 2, 2, 3, 7)$  likewise resembles the representation  $\rho(4, 2, 3, 7)$ . We find that its zeta factors are

$$Z_p^t(2, 2, 2, 3, 7) = Z_p^t(36A1) \otimes (1 - pt) \otimes \chi_3(p, t),$$

where the factor  $\psi_1$  equals

$$\psi_1(p, t) = \begin{cases} (1 - \sigma(2, \frac{1}{4})t)^2 & \text{If } p \equiv 1 \pmod{8} \\ (1 + t^2) & \text{If } p \equiv 5 \pmod{8} \\ (1 - t^2) & \text{otherwise.} \end{cases}$$

The next representation  $c = (2, 2, 6, 1, 5)$  has a reducible  $c$  that can also be simplified by the Gamma multiplication formula. We find the same twisting factor  $\psi_1$ .

For  $c = (2, 6, 6, 1, 1)$  we have a twisting factor that is just a bit different:

$$\psi_2(p, t) = \begin{cases} (1 - (-1)^{(p-1)/8}\sigma(2, \frac{1}{4})t)^2 & \text{If } p \equiv 1 \pmod{8} \\ (1 + t^2) & \text{If } p \equiv 3 \pmod{8} \\ (1 - t^2) & \text{otherwise.} \end{cases}$$

### 6.4.3 Exponents (2,8,8,8,8)

The other set of exponents defining a diagonal Calabi-Yau variety of degree 8 is  $\{2, 8, 8, 8, 8\}$ . So this the variety defined by

$$X_0^2 + X_1^8 + X_2^8 + X_3^8 + X_4^8 = 0 \quad (6.38)$$

in  $\mathbb{P}(4, 1, 1, 1, 1)$ . This variety is smooth; no singularities need to be resolved. Hence  $h^{11}(X)$  equals 1. The other non-trivial Hodge number  $h^{12}(X)$  is 149.

The middle cohomology decomposes as follows.

Subspace	Mult.	Dim.	Representation
(4, 1, 1, 1, 1)	1	4	} 64A1 $\otimes$ 256D1 $\otimes$ 256D1
(4, 1, 1, 5, 5)	1	4	
(4, 1, 1, 5, 5)	2	4	(32A1 $\oplus$ 64A1) $\otimes$ $\mathbb{Q}(-1)$
(4, 1, 1, 3, 7)	12	4	(256B1 $\oplus$ 256D1) $\otimes$ $\chi_3 \otimes \mathbb{Q}(-1)$
(4, 1, 1, 4, 6)	12	4	(256B1 $\oplus$ 256D1) $\otimes$ $\chi_4 \otimes \mathbb{Q}(-1)$
(4, 1, 2, 2, 7)	12	4	(32A1 $\oplus$ 64A1) $\otimes$ $\chi_3 \otimes \mathbb{Q}(-1)$
(4, 1, 3, 2, 6)	12	4	(256B1 $\oplus$ 256D1) $\otimes$ $\mathbb{Q}(-1)$
(4, 1, 3, 4, 4)	6	4	(256B1 $\oplus$ 256D1) $\otimes$ $\mathbb{Q}(-1)$
(4, 1, 2, 2, 7)	12	4	(32A1 $\oplus$ 64A1) $\otimes$ $\chi_3 \otimes \chi_4 \otimes \mathbb{Q}(-1)$
(4, 2, 2, 2, 6)	4	2	32A1 $\otimes$ $\mathbb{Q}(-1)$
(4, 2, 2, 4, 4)	4	2	64A1 $\otimes$ $\mathbb{Q}(-1)$

Table 6.12: The middle cohomology for  $e = (2, 8, 8, 8, 8)$ .

There are 3 representations  $\rho(c)$  with  $c$  a permutation of (4,1,1,5,5) in this variety, but we used one to complete the tensor product in the first line. The other is given separately. The triple tensor product representation is obviously reducible, unlike most tensor products of irreducible representations we have seen so far.

The symbol  $\chi_3$  is defined by

$$\chi_3(p) := \begin{cases} (-1)^{(p-1)/8} & \text{if } p \equiv 1 \pmod{8} \\ 1 & \text{if } p \equiv 7 \pmod{8} \\ i & \text{otherwise} \end{cases}$$

and  $\chi_4$  is equal to

$$\chi_4(p) := \begin{cases} \sigma(2, \frac{1}{4})(-1)^{(p-1)/8} & \text{if } p \equiv 1 \pmod{8} \\ i & \text{if } p \equiv 3 \pmod{8} \\ 1 & \text{otherwise.} \end{cases}$$

With these twists, all representations in this variety can be expressed in terms of modular forms. Since almost all  $c$  are reducible the calculations are easy; these representations are twists of representations that occur in dimension 1 and degree 8. We know all representations in that case.

### 6.4.4 Exponents (4,4,6,6,6)

Consider the threefold defined as the resolution of singularities of the diagonal variety defined by

$$X_0^4 + X_1^4 + X_2^6 + X_3^6 + X_4^6 = 0. \quad (6.39)$$

There is a 1-dimensional singularity, the curve  $C$  of degree 6 defined by  $X_0 = X_1 = 0$ , with multiplicity 1 (meaning that its fiber under the resolution consists of one copy of  $C \times \mathbb{P}^1$ ). There are also isolated singular points with  $X_2 = X_3 = X_4 = 0$ . The nontrivial Hodge numbers of the resolution are  $h^{11} = 6$  and  $h^{21} = 60$ .

The middle cohomology of the singular variety decomposes as follows.

Subspace	Mult.	Dim.	Representation
(3, 3, 2, 2, 2)	1	4	27k3A1 $\otimes$ 64A1
(3, 3, 2, 8, 8)	3	4	64A1 $\otimes$ $\rho(6, 2, 8, 8) \otimes \mathbb{Q}(-1)$
(3, 3, 4, 6, 8)	3	4	64A1 $\otimes$ $\rho_0(3) \otimes \mathbb{Q}(-1)$
(3, 3, 2, 6, 10)	3	4	64A1 $\otimes$ $\rho_0(3) \otimes \mathbb{Q}(-1)$
(3, 9, 2, 2, 8)	3	4	432G1 $\otimes$ $\rho_0(4) \otimes \mathbb{Q}(-1)$
(3, 9, 2, 4, 6)	6	4	144B1 $\otimes$ $\rho_0(4) \otimes \mathbb{Q}(-1)$
(3, 9, 4, 4, 4)	1	4	27A1 $\otimes$ $\rho_0(4) \otimes \mathbb{Q}(-1)$
(3, 3, 6, 6, 6)	1	2	64A1 $\otimes \mathbb{Q}(-1)$
(6, 6, 2, 2, 8)	3	2	432G1 $\otimes (-1)^{(p-1)/2} \otimes \mathbb{Q}(-1)$
(6, 6, 2, 4, 6)	6	2	144B1 $\otimes (-1)^{(p-1)/2} \otimes \mathbb{Q}(-1)$
(6, 6, 4, 4, 4)	1	2	27A1 $\otimes (-1)^{(p-1)/2} \otimes \mathbb{Q}(-1)$
(3, 3, 6)	3	2	64A1 $\otimes \mathbb{Q}(-1)$

Table 6.13: The middle cohomology of the diagonal variety with exponents (4, 4, 6, 6, 6).

All but the first two of these representations are more or less trivial; they correspond to a reducible  $c$ , and therefore by Corollary 4.6 they are subrepresentations of a Tate-twisted tensor product representation. In the case at hand these tensor product representations are equal to the  $\rho(c)$  themselves, but in general they may contain more than one  $\rho(c)$ .

The first two representations satisfy the conditions of Corollary 4.7. So the first can be decomposed as  $(3, 3, 3, 2, 2) = (3, 3, 6) \vee (2, 2, 2, 6)$ , and the corresponding representations have been identified before. Notice that the twist with  $\rho_0(2)$  has been omitted, since it acts trivially. It is nontrivial only for primes  $p \equiv 3 \pmod{4}$ ; but for such primes we have

$$\begin{aligned} Z_p((3, 3, 6), t) &= 1 + pt^2 \Gamma_p\left(\frac{1}{4}\right)^2 \Gamma_p\left(\frac{1}{2}\right)^2 \Gamma_p\left(\frac{3}{4}\right)^2 \\ &= (1 - pt^2) \end{aligned} \quad (6.40)$$

and this factor is invariant under the twist.

The second representation in the list factors as  $(3, 3, 2, 8, 8) = (3, 3, 6) \vee (2, 8, 8, 6)$ . The twist has no effect in this case as well, for the same reason as above. The representation  $\rho(2, 8, 8, 6)$  has been treated in subsection 6.3.1.

### 6.4.5 Exponents (4,4,3,12,12)

Next, we consider the Calabi-Yau threefold defined by the equation

$$X_0^4 + X_1^4 + X_2^3 + X_3^{12} + X_4^{12} = 0. \tag{6.41}$$

This variety has no 1-dimensional singularities, and singular points defined by  $X_0^4 + X_1^4 = 0, X_2 = X_3 = X_4 = 0$ . Each of these adds one to the Betti number  $\beta_2$ . Here is the Hodge diamond.

$$\begin{array}{ccccccc}
 & & & & & & 1 \\
 & & & & 0 & & 0 \\
 & & & 0 & 5 & & 0 \\
 & & 0 & 89 & 89 & & 1 \\
 & & 0 & 5 & 0 & & \\
 & & & 0 & 0 & & \\
 & & & & & & 1
 \end{array} \tag{6.42}$$

The middle cohomology decomposes as follows.

Subspace	Mult.	Dim.	Representation
(3, 3, 4, 1, 1)	1	4	} 64A1 ⊗ 64A1 ⊗ 27A1 ⊗ χ <sub>1</sub> ⊗ ρ <sub>0</sub> (2)
(3, 3, 4, 7, 7)	1	4	
(3, 3, 4, 3, 11)	2	4	} 64A1 ⊗ ρ <sub>0</sub> (2) ⊗ (6, 4, 3, 11)
(3, 3, 4, 5, 9)	2	4	
(3, 9, 4, 5, 3)	4	4	(3, 8, 1) ⊗ χ <sub>6</sub> ⊗ ℚ(-1)
(3, 3, 4, 4, 10)	2	4	64A1 ⊗ (6, 2, 8, 8) ⊗ ρ <sub>0</sub> (2)
(3, 6, 4, 1, 10)	4	4	(1, 3, 8) ⊗ χ <sub>6</sub> ⊗ ψ <sub>4</sub> ⊗ ℚ(-1)
(3, 6, 2, 4, 9)	6	4	144B1 ⊗ ρ <sub>0</sub> (4) ⊗ ℚ(-1)
(3, 6, 4, 4, 7)	4	4	27A1 ⊗ (6, 4, 3, 11) (Twice)
(3, 6, 4, 5, 6)	6	4	(3, 8, 1) ⊗ ρ <sub>0</sub> (2) ⊗ ℚ(-1)
(3, 9, 4, 1, 7)	2	4	27A1 ⊗ ℚ(-1)
(3, 9, 4, 4, 4)	1	4	27A1 ⊗ ρ <sub>0</sub> (4) ⊗ ℚ(-1)
(3, 9, 4, 10, 10)	1	4	432G1 ⊗ ρ <sub>0</sub> (4) ⊗ ℚ(-1)
(6, 6, 4, 1, 7)	1	4	27A1 ⊗ ρ <sub>0</sub> (4) ⊗ ρ <sub>0</sub> (2) ⊗ ℚ(-1)
(6, 6, 4, 2, 6)	2	2	144B1 ⊗ ρ <sub>0</sub> (2) ⊗ ℚ(-1)
(6, 6, 4, 4, 4)	1	2	27A1 ⊗ ρ <sub>0</sub> (2) ⊗ ℚ(-1)
(6, 6, 4, 10, 10)	1	2	432G1 ⊗ ρ <sub>0</sub> (2) ⊗ ℚ(-1)

Table 6.14: The middle cohomology in the case of exponents (4, 4, 3, 12, 12).

The first two representations can be identified using Corollary 4.7. Again we find a triple tensor product representation that decomposes as the sum of two representations  $\rho(3, 3, 4, 1, 1)$  and  $\rho(3, 3, 4, 7, 7)$ . The character  $\chi_1$  in defined in (6.30).

There are 6 permutations of (3, 9, 4, 5, 3) that occur in the cohomology of this variety. Two of those have been coupled to permutations of (3, 3, 4, 3, 11) to form another tensor product; the other 4 have been given separately.

We used an auxiliary symbol  $\chi_6$ , which is equal to  $(-1)^{(p-1)/4}$  if  $p \equiv 1 \pmod{4}$ , and 1 otherwise. The symbol  $\psi_4$  is related to  $\sigma(2, \frac{1}{6})$ ; it is defined by

$$\psi_4(t) := \begin{cases} (1 - \sigma(2, \frac{1}{6})t)(1 - \sigma(2, \frac{5}{6})t) & \text{if } p \equiv 1 \pmod{6} \\ 1 - t^2 & \text{otherwise.} \end{cases}$$

The representation with  $c = (3, 9, 1, 4, 7)$  is equal to a twist of  $\rho(1, 4, 7)$ . The characteristic polynomials of this representation  $(1, 4, 7)$  can be expressed explicitly in terms of the modular representation  $\rho^3(1, 1, 1)$ . For a prime  $p \equiv 1 \pmod{12}$  we find that

$$\begin{aligned} Z_p^{12}((1, 4, 7), t) &= (1 + t\Gamma_p(\frac{1}{12}, \frac{7}{12}, \frac{1}{3}))^2 \\ &\quad (1 - pt\Gamma_p(\frac{5}{12}, \frac{11}{12}, \frac{2}{3}))^2 \\ &= (1 + t\Gamma_p(\frac{1}{3})^3 \sigma(2, \frac{1}{2}) (-1)^{r_p(\frac{1}{3})+r_p(\frac{1}{2})})^2 \\ &\quad (1 - t\Gamma_p(\frac{2}{3})^3 \sigma(2, \frac{1}{2}) (-1)^{r_p(\frac{1}{3})+r_p(\frac{1}{2})})^2 \\ &= Z_p^3((1, 1, 1), (-1)^{(p-1)/4}t)^2 \end{aligned} \quad (6.43)$$

The calculations for other primes are similar but simpler. We find that

$$Z_p^{12}((1, 4, 7), t) = Z_p^3((1, 1, 1), t) \otimes \rho_0(4). \quad (6.44)$$

The representation  $\rho(3, 6, 4, 4, 7)$  is a remarkable case; by manipulating its zeta factor we can show that the direct sum of two copies of this representation together are isomorphic to the representation  $27A1 \otimes (6, 4, 3, 11)$ . The calculation amounts to the following manipulation of Jacobi sums:

$$\begin{aligned} J_p^{12}(3, 6, 8, 8, 11) &= -p\Gamma_p(\frac{3}{4}, \frac{1}{2}, \frac{1}{3}, \frac{1}{3}, \frac{1}{12}) \\ &= -p\Gamma_p(\frac{3}{4}, \frac{1}{2}, \frac{1}{12}, \frac{2}{3}, \frac{1}{3})^3 (-1)^{r_p(1/3)} \\ &= J_p^{12}(3, 6, 4, 11) J_p^3(1, 1, 1) (-1)^{r_p(1/3)}. \end{aligned} \quad (6.45)$$

### 6.4.6 Exponents (4,4,4,6,12)

This Calabi-Yau variety is defined by the equation

$$X_0^4 + X_1^4 + X_2^4 + X_3^6 + X_4^{12} = 0 \quad (6.46)$$

in the weighted projective space  $\mathbb{P}(3, 3, 3, 2, 1)$ . From Chapter 2 we see that it contains a 1-dimensional singularly embedded curve  $X_0^4 + X_1^4 + X_2^4$  with  $X_3 = X_4 = 0$ , with multiplicity 2, but no isolated singular points. This is its Hodge diamond.

$$\begin{array}{ccccccc} & & & & 1 & & \\ & & & & 0 & & 0 \\ & & & 0 & 3 & & 0 \\ & & 0 & 69 & 69 & & 0 \\ 1 & & & & & & 1 \\ & & 0 & 3 & & & 0 \\ & & & & 0 & & 0 \\ & & & & 1 & & \end{array} \quad (6.47)$$

Subspace	Mult.	Dim.	Representation
(3, 3, 3, 2, 1)	1	4	} 64A1 $\otimes$ (6, 3, 2, 1) $\otimes$ $\rho_0(2)$
(9, 9, 3, 2, 1)	3	4	
(3, 3, 3, 4, 11)	1	4	} 64A1 $\otimes$ (6, 4, 3, 11) $\otimes$ $\rho_0(2)$
(9, 9, 3, 4, 11)	3	4	
(3, 3, 6, 2, 10)	3	4	64A1 $\otimes$ $\rho_0(6)$
(3, 3, 6, 4, 8)	3	4	64A1 $\otimes$ $\rho_0(3)$
(9, 6, 6, 2, 1)	3	4	$\rho(9, 2, 1) \otimes \rho_0(2) \otimes \mathbb{Q}(-1)$
(3, 6, 6, 4, 5)	3	4	$\rho(3, 8, 1) \otimes \rho_0(2) \otimes \mathbb{Q}(-1)$
(3, 6, 9, 2, 4)	6	4	144B1 $\otimes$ $\rho_0(4) \otimes \mathbb{Q}(-1)$
(3, 3, 3, 6, 9)	4	2	32A1 $\otimes$ $\mathbb{Q}(-1)$
(3, 3, 6, 6, 6)	6	2	64A1 $\otimes$ $\mathbb{Q}(-1)$
(6, 6, 6, 2, 4)	2	2	144B1 $\otimes$ $\rho_0(2) \otimes \mathbb{Q}(-1)$
(3, 3, 6)	6	2	64A1 $\otimes$ $\mathbb{Q}(-1)$

Table 6.15: The middle cohomology for the case  $e = (4, 4, 4, 6, 12)$ .

Most of these representations can be identified using the Corollaries 4.6 and 4.7. The representation  $\rho(6, 3, 2, 1)$  has so far resisted identification, although it seems to be related to the form 144B1; for example, we have

$$\mathrm{Tr}\rho(144B1)(F_p) \mid \mathrm{Tr}\rho(6, 3, 2, 1)(F_p)$$

for all primes calculated where both traces are nonzero. So we can try to decompose the zeta factors of  $\rho(6, 3, 2, 1)$  as if it were a tensor product of  $\rho(144B1)$  and another representation of weight 2. So we try to solve

$$Z_p((6, 3, 2, 1), t) = Z_p(\rho(144B1), t) \otimes (1 - a_p + pt^2).$$

Since the traces of  $\rho(144B1)$  are equal to zero for all primes  $\equiv 5 \pmod{6}$ , we have some freedom in choosing the  $a_p$  for those  $p$ . For all primes calculated, they may be chosen within  $\mathbb{Z}[\sqrt{2}]$ , or inside  $\mathbb{Z}[\sqrt{-2}]$ . For primes  $p$  equal to  $1 \pmod{6}$  the  $a_p$  are integers.

There may be a choice of  $a_p$  corresponding to the coefficients of a modular form, but we have not found such a form; it has level at least 500 if it exists at all.



# Appendix A

## Coefficients of modular forms

Since there is no universally accepted way to attach labels to modular forms, we will give some coefficients for the forms in this thesis. Together with weight and level this should be enough to identify the forms.

Label	Weight	Level	$a_2$	$a_3$	$a_5$	$a_7$	$a_{11}$	$a_{13}$	$a_{17}$	$a_{19}$	$a_{23}$
27A1	2	27	0	0	0	-1	0	5	0	-7	0
32A1	2	32	0	0	-2	0	0	6	2	0	0
36A1	2	36	0	0	0	-4	0	2	0	8	0
64A1	2	64	0	0	2	0	0	-6	2	0	0
108A1	2	108	0	0	0	5	0	-7	0	-1	0
144B1	2	144	0	0	0	4	0	2	0	-8	0
256B1	2	576	0	-2	0	0	-6	-2	0	0	0
256D1	2	576	0	2	0	0	6	2	0	0	0
432G1	2	432	0	0	0	-5	0	-7	0	1	0
576F1	2	576	0	0	4	0	0	6	-8	0	0
576G1	2	576	0	0	-4	0	0	6	8	0	0
12k3A[0,1]1	3	12	0	-3	0	2	0	-22	0	26	0
16k3A[1,0]1	3	16	0	0	-6	0	0	10	-30	0	0
27k3A[9]1	3	27	0	0	0	-13	0	-1	0	11	0
48k3A[0,0,1]1	3	48	0	3	0	-2	0	-22	0	-26	0
64k3A[1,0]1	3	16	0	0	6	0	0	-10	-30	0	0
27k5A[9]1	5	27	0	0	0	71	0	-337	0	-601	0



## Appendix B

# Relations for the $p$ -adic Gamma functions

The Gamma multiplication formula (3.92) produces a number of identities between values of the  $p$ -adic Gamma function. Some of these will be used over and over again, so we will give those here. The symbols  $\sigma$  are defined by equation (3.93).

$$\Gamma_p\left(\frac{1}{4}\right)\Gamma_p\left(\frac{3}{4}\right) = \sigma\left(2, \frac{1}{2}\right)\Gamma_p\left(\frac{1}{2}\right)^2 = (-1)^{r_p\left(\frac{1}{4}\right)} \quad (\text{B.1})$$

$$\Gamma_p\left(\frac{1}{8}\right)\Gamma_p\left(\frac{5}{8}\right) = \sigma\left(2, \frac{1}{4}\right)\Gamma_p\left(\frac{1}{4}\right)\Gamma_p\left(\frac{1}{2}\right) \quad (\text{B.2})$$

$$\Gamma_p\left(\frac{1}{6}\right)\Gamma_p\left(\frac{2}{3}\right) = \sigma\left(2, \frac{1}{3}\right)\Gamma_p\left(\frac{1}{3}\right)\Gamma_p\left(\frac{1}{2}\right) \quad (\text{B.3})$$

$$\Gamma_p\left(\frac{5}{6}\right)\Gamma_p\left(\frac{1}{3}\right) = \sigma\left(2, \frac{2}{3}\right)\Gamma_p\left(\frac{2}{3}\right)\Gamma_p\left(\frac{1}{2}\right) \quad (\text{B.4})$$

$$\Gamma_p\left(\frac{1}{12}\right)\Gamma_p\left(\frac{7}{12}\right) = \sigma\left(2, \frac{1}{6}\right)\Gamma_p\left(\frac{1}{6}\right)\Gamma_p\left(\frac{1}{2}\right) \quad (\text{B.5})$$

$$\Gamma_p\left(\frac{11}{12}\right)\Gamma_p\left(\frac{5}{12}\right) = \sigma\left(2, \frac{5}{6}\right)\Gamma_p\left(\frac{5}{6}\right)\Gamma_p\left(\frac{1}{2}\right) \quad (\text{B.6})$$

$$\Gamma_p\left(\frac{1}{6}\right)\Gamma_p\left(\frac{5}{6}\right) = \sigma\left(3, \frac{1}{2}\right)\Gamma_p\left(\frac{1}{3}\right)\Gamma_p\left(\frac{2}{3}\right) = \sigma\left(3, \frac{1}{2}\right)(-1)^{r_p\left(\frac{1}{3}\right)} \quad (\text{B.7})$$

$$\Gamma_p\left(\frac{1}{12}\right)\Gamma_p\left(\frac{5}{12}\right)\Gamma_p\left(\frac{9}{12}\right) = \sigma\left(3, \frac{1}{4}\right)\Gamma_p\left(\frac{1}{4}\right)\Gamma_p\left(\frac{1}{3}\right)\Gamma_p\left(\frac{2}{3}\right) \quad (\text{B.8})$$

$$\Gamma_p\left(\frac{3}{12}\right)\Gamma_p\left(\frac{7}{12}\right)\Gamma_p\left(\frac{11}{12}\right) = \sigma\left(3, \frac{3}{4}\right)\Gamma_p\left(\frac{3}{4}\right)\Gamma_p\left(\frac{1}{3}\right)\Gamma_p\left(\frac{2}{3}\right) \quad (\text{B.9})$$

$$\Gamma_p\left(\frac{1}{12}\right)\Gamma_p\left(\frac{7}{12}\right)\Gamma_p\left(\frac{10}{12}\right) = \sigma\left(4, \frac{1}{3}\right)\Gamma_p\left(\frac{1}{4}\right)\Gamma_p\left(\frac{1}{2}\right)\Gamma_p\left(\frac{3}{4}\right) \quad (\text{B.10})$$

$$\Gamma_p\left(\frac{2}{12}\right)\Gamma_p\left(\frac{5}{12}\right)\Gamma_p\left(\frac{11}{12}\right) = \sigma\left(4, \frac{2}{3}\right)\Gamma_p\left(\frac{1}{4}\right)\Gamma_p\left(\frac{1}{2}\right)\Gamma_p\left(\frac{3}{4}\right) \quad (\text{B.11})$$



# Bibliography

- [1] Michael Artin, Alexandre Grothendieck, and Jean-Louis Verdier, *Théorie des topos et cohomologie étale des schémas*, Lecture Notes in Mathematics, vol. 269, 270, 305, Springer-Verlag, Heidelberg, 1972–1973.
- [2] Victor V. Batyrev, *Dual polyhedra and mirror symmetry for calabi-yau hypersurfaces in toric varieties*, J. Alg. Geom. **3** (1994), 493, alg-geom/9310003.
- [3] Victor V. Batyrev and David A. Cox, *On the hodge structure of projective hypersurfaces in toric varieties*, Duke Math. J. **75 no. 2** (1994), 293, alg-geom/9306011.
- [4] Maurizio Boyarsky, *p-adic gamma functions and Dwork cohomology*, Trans. Amer. Math. Soc. **257** (1980), no. 2, 359–369.
- [5] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over  $\mathbb{Q}$ : wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).
- [6] Philip Candelas, Xenia de la Ossa, and Fernando Rodriguez-Villegas, *Calabi-Yau manifolds over finite fields. II*, Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), Fields Inst. Commun., vol. 38, Amer. Math. Soc., Providence, RI, 2003, See also hep-th/0012233., pp. 121–157.
- [7] Harold Davenport and Helmut Hasse, *Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1935), 151.
- [8] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307.
- [9] ———, *La conjecture de Weil. II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252.
- [10] Pierre Deligne, James S. Milne, Arthur Ogus, and Kuang-yen Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin, 1982, Philosophical Studies Series in Philosophy, 20.

- 
- [11] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids 1*, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530 (1975).
- [12] Charles Delorme, *Espaces projectifs anisotropes*, Bull. Soc. Math. France **103** (1975), no. 2, 203–223.
- [13] Alexandru Dimca, *On the homology and cohomology of complete intersections with isolated singularities*, Compositio Math. **58** (1986), no. 3, 321–339.
- [14] Igor Dolgachev, *Weighted projective varieties*, Group actions and vector fields (Vancouver, B.C., 1981), Lecture Notes in Math., vol. 956, Springer, Berlin, 1982, pp. 34–71.
- [15] William Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies, vol. 131, Princeton University Press, New Jersey, 1993.
- [16] Carl Friedrich Gauss, *Werke*, vol. I, II, X.
- [17] Fernando Q. Gouvêa and Noriko Yui, *Arithmetic of diagonal hypersurfaces over finite fields*, London Math. Soc. Lecture Note Ser., vol. 209, Cambridge Univ. Press, Cambridge, 1995.
- [18] Brian R. Greene and Ronen Plesser, Nucl. Phys. B **338** (1990), 15.
- [19] Klaus Hulek and Noriko Yui, *On modularity of rigid and nonrigid Calabi-Yau varieties associated to the root lattice  $A_4$* , (2003), math.AG/0304169.
- [20] Tetsushi Ito, *Birational smooth minimal models have equal Hodge numbers in all dimensions*, Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), Fields Inst. Commun., vol. 38, Amer. Math. Soc., Providence, RI, 2003, pp. 183–194.
- [21] Carl G.J. Jacobi, *Gesammelte werke*, vol. VI, VII.
- [22] Victor J. Katz, *A history of mathematics*, HarperCollins College Publishers, New York, 1993, An introduction.
- [23] Maxim Kontsevich and Yan Soibelman, *Homological mirror symmetry and torus fibrations*, Symplectic geometry and mirror symmetry (Seoul, 2000), World Sci. Publishing, River Edge, NJ, 2001, pp. 203–263.
- [24] Ernst Kunz, *Holomorphe Differentialformen auf algebraischen Varietäten mit Singularitäten. I*, Manuscripta Math. **15** (1975), 91–108.
- [25] Serge Lang, *Introduction to modular forms*, Grundlehren der mathematischen Wissenschaften, vol. 222, Springer-Verlag, New York, 1976.
- [26] ———, *Cyclotomic fields I and II*, Graduate Texts in Mathematics, vol. 121, Springer-Verlag, New York, 1990.
- [27] R. Livné, *Cubic exponential sums and galois representations*, Cont. Math. **67** (1985), 247.

- [28] Ron Livné and Noriko Yui, *The modularity of certain non-rigid Calabi-Yau threefolds*, (2003), math.AG/0304497.
- [29] Yves Martin, *Multiplicative  $\eta$ -quotients*, Trans. Amer. Math. Soc. **348** (1996), 4825.
- [30] Preda Mihailescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.
- [31] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.
- [32] Toshitsune Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989.
- [33] Yasuo Morita, *A  $p$ -adic analogue of the  $\Gamma$ -function*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **22** (1975), no. 2.
- [34] Shi-Shyr Roan, *On Calabi-Yau orbifolds in weighted projective spaces*, Internat. J. Math. **1** (1990), no. 2, 211–232.
- [35] Alain M. Robert, *A course in  $p$ -adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000.
- [36] Masa-Hiko Saito and Noriko Yui, *The modularity conjecture for rigid Calabi-Yau threefolds over  $\mathbb{Q}$* , J. Math. Kyoto Univ. **41** (2001), no. 2, 403–419.
- [37] Matthias Schütt, *On the modularity of three Calabi-Yau threefolds with bad reduction at 11*, math.AG **0405450** (2004).
- [38] Jean-Pierre Serre, *Sur les représentations modulaires de degré 2 de  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54** (1987), no. 1.
- [39] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971, Kanô Memorial Lectures, No. 1.
- [40] Tetsuji Shioda and Toshiyuki Katsura, *On fermat varieties*, Tôhoku Math. Journ. **31** (1979), 97–115.
- [41] Joseph Steenbrink, *Intersection forms for quasi-homogeneous singularities*, Compositio Math. **34** (1977), no. 2, 211–223.
- [42] William A. Stein, *A brief introduction to classical and adelic algebraic number theory*, 2004, <http://modular.fas.harvard.edu/papers/ant>.
- [43] ———, *The Modular Forms Database*, <http://modular.fas.harvard.edu/Tables> (2004).
- [44] Peter Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Mathematical Society Student Texts, vol. 50, Cambridge University Press, Cambridge, 2001.

- 
- [45] Cumrun Vafa, *String vacua and orbifoldized LG models*, Modern Phys. Lett. A **4** (1989), no. 12, 1169–1185.
- [46] Helena A. Verrill, *The L-series of certain rigid Calabi-Yau threefolds*, J. Number Theory **81** (2000), no. 2, 310–334.
- [47] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497.
- [48] ———, *Jacobi sums as “Größencharaktere”*, Trans. Amer. Math. Soc. **73** (1952), 487.
- [49] ———, *Adeles and algebraic groups*, Progress in Mathematics, vol. 23, Birkhäuser Boston, Mass., 1982, With appendices by M. Demazure and Takashi Ono.
- [50] Andrew Wiles, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.
- [51] Noriko Yui, *The arithmetic of certain Calabi-Yau varieties over number fields*, The arithmetic and geometry of algebraic cycles (Banff, AB, 1998), NATO Sci. Ser. C Math. Phys. Sci., vol. 548, Kluwer Acad. Publ., Dordrecht, 2000, pp. 515–560.

# Samenvatting

Dit proefschrift gaat over de oplossingen van diagonale variëteiten en hun verband met modulaire vormen. Een diagonale variëteit is de verzameling van oplossingen van een bepaald type algebraïsche vergelijking en kenmerkt zich door een grote symmetriegroep. We kunnen deze oplossingen in  $\mathbb{C}$  zoeken zoals gebeurt in de natuurkunde, maar ook andere lichamen zijn mogelijk. Een manier om de variëteit te bestuderen is door het aantal oplossingen te tellen over een eindig lichaam, of beter nog een reeks eindige lichamen met dezelfde karakteristiek. Uit het werk van André Weil blijkt dat de genererende functie voor deze aantallen punten, de zetafunctie, een rationale functie over  $\mathbb{Z}$  is. In het bijzonder wordt hij vastgelegd door eindig veel gehele coëfficiënten. Deze kunnen berekend worden door over een klein aantal eindige lichamen het aantal punten van de variëteit te tellen. Dan kennen we de zetafunctie en daardoor de aantallen punten voor alle eindige lichamen van die karakteristiek.

De graden van teller en noemer van de zetafunctie worden bepaald door de Betti-getallen van de variëteit, topologische invarianten die eenvoudig te berekenen zijn door de diagonale variëteit te beschouwen als een oppervlak in een torische variëteit. In deze context kunnen ook eventuele singulariteiten van de variëteit beschreven en opgelost worden.

Voor de meeste variëteiten is het tellen van punten tamelijk bewerkelijk, maar door de grote symmetrie van een diagonale variëteit is het mogelijk dit zeer efficiënt te doen. Met behulp van oude technieken (de karaktersommen van Gauss en Jacobi) kunnen we een uitdrukking voor de aantallen punten geven. De Jacobisommen blijken overeen te komen met de nulpunten of polen van de zetafunctie, wat de berekening nog verder versnelt. Op deze manier kunnen we voor een gegeven diagonale variëteit en een vaste karakteristiek de bijbehorende zetafunctie bepalen.

De zetafunctie kan gefactoriseerd worden in factoren die overeenkomen met deelruimtes van de cohomologie van de variëteit. Deze ontbinding in deelruimtes is onafhankelijk van de karakteristiek van het gekozen lichaam. Via de Dirichlet  $L$ -reeks kunnen we bij elke deelruimte de bijbehorende factoren voor alle karakteristieken verenigen in één functie. In dit proefschrift laten we zien dat in veel gevallen deze functie een zeer bijzondere is, namelijk een modulaire vorm, of eenvoudig in dergelijke vormen uitgedrukt kan worden.

Een modulaire vorm is een holomorfe functie op het complexe bovenhalfvlak, die eenvoudig transformeert onder een grote groep van transformaties in  $SL(2, \mathbb{Z})$ .

In het bijzonder is hij invariant onder een translatie, zodat hij kan worden uitgedrukt in een Fourierreeks. Voor sommige van deze vormen, de Hecke eigenvormen, zijn de Fouriercoëfficiënten gehele getallen. In ons geval blijkt dat voor elk priemgetal  $p$  de  $p$ -de coëfficiënt van de modulaire vorm direct gerelateerd is aan de zetafunctie van de variëteit over het lichaam met  $p$  elementen. Door voor voldoende priemgetallen punten te tellen kunnen we ontdekken welke modulaire vorm van toepassing is. Uit de Fouriercoëfficiënten van deze vorm kan dan voor ieder priemgetal de zetafunctie bepaald worden.

# Dankwoord

Aan het eind van dit proefschrift wil ik iedereen bedanken die direct of indirect heeft bijgedragen aan de totstandkoming ervan. Allereerst gaat mijn dank uit naar mijn promotores, die dit project geïnitieerd hebben en die mij ruim vier jaar lang met raad en daad terzijde gestaan hebben. Zonder hun inbreng was dit proefschrift nooit zo geworden als het is. Ook de leden van de commissie dank ik voor hun zorgvuldige lezing van het manuscript en hun commentaar.

Ik dank het FOM dat de financiële ruimte voor mij heeft geschapen om mijn promotieonderzoek te verrichten en het Korteweg–De Vries instituut dat mij van een werkplek en allerhande faciliteiten heeft voorzien. Ook de NS die mij dagelijks van Utrecht naar Amsterdam Amstel vervoerde (de enkele keer dat ik in Amsterdam Sloterdijk of op de A12 belandde daargelaten) was onmisbaar.

De medewerkers van het instituut, en vooral mijn collega-promovendi, wil ik bedanken voor de goede sfeer, de lunchgesprekken, filmavonden en grote hoeveelheden thee. Mijn (soms te) gezellige kamergenoten hebben zeer bijgedragen aan een prettig verblijf aan het Korteweg–De Vries instituut. Buiten de werksfeer zorgden schaakclub Paul Keres en het Studentenkoor Amsterdam voor de nodige ontspanning en nieuwe energie.

Verder dank ik mijn studievrienden, die steeds vol interesse mijn wel en wee gevolgd hebben. Boven alles ben ik mijn ouders, broer en zus en mijn verdere familie zeer dankbaar voor hun voortdurende steun.



# Curriculum Vitae

Simon Kronemeijer werd geboren te Kampen op 4 februari 1976. Van 1988 tot 1994 volgde hij onderwijs aan het Johannes Calvijn Lyceum te Kampen, waar hij in juni 1994 zijn VWO-diploma behaalde met als eindexamenvakken Nederlands, Engels, Frans, Duits, Wiskunde, Natuurkunde, Scheikunde, Latijn en Grieks. In september 1994 verhuisde hij naar Utrecht, waar hij wiskunde en natuurkunde studeerde aan de Universiteit Utrecht. In deze periode gaf hij vele werkcolleges aan eerste- en tweedejaars studenten wis- en natuurkunde. In juni 1999 studeerde hij cum laude af in de wiskunde met een afstudeerscriptie getiteld *Residues of Hyperplane Arrangements*. In augustus 2000 behaalde hij cum laude zijn doctoraal in de natuurkunde met de scriptie *The Rainbow Model* op het gebied van de quantumveldentheorie. Van november 2000 tot november 2004 deed hij promotieonderzoek aan het Korteweg-De Vries Instituut voor Wiskunde van de Universiteit van Amsterdam onder begeleiding van Gerard van der Geer en Robbert Dijkgraaf. Dit onderzoek mondde uit in het proefschrift *Diagonal Varieties and Modular Forms*. Vanaf juni 2000 was hij tevens bestuurslid van schaakvereniging Paul Keres.





