

Chapter 1

Introduction

One way to describe a mathematical discipline is to describe the equations studied in that discipline. General algebraic geometry is concerned with polynomial equations over arbitrary (commutative) rings, whereas number theory and arithmetic geometry specialize in polynomial equations over number fields, finite fields, p -adic fields and rings of integers.

A particularly famous example is the *Fermat equation* P_n^r over a ring R

$$X_1^r + X_2^r + \dots + X_n^r = 0$$

for natural numbers $r, n \geq 2$ and variables $X_1, \dots, X_n \in R$. The special case $r \geq 3, n = 3, R = \mathbb{Z}$ is subject of *Fermat's Last Theorem*, for hundreds of years the most famous mathematical conjecture, proved by Andrew Wiles in 1993.

In his way-breaking 1949 paper [Wei49], André Weil studied the special case where R is a finite field \mathbb{F}_q , using this to motivate his *Weil conjectures*, whose proof, completed by Deligne in 1974 ([Del74]), was undoubtedly one of the great triumphes of 20th century mathematics.

In modern algebraic geometry, Fermat equations (respectively *Fermat hypersurfaces*, the hypersurfaces defined by Fermat equations in projective space) have been studied intensely, especially by Tetsuji Shioda ([SK79], [Shi79], [Shi82], [Shi83], [Shi87], [Shi88]), and they are often used as examples and testing ground for open problems like the conjectures of Hodge and Tate.

But even though much more is known about Fermat hypersurfaces than about general hypersurfaces, not to mention general varieties, a lot of questions still remain open; both the Hodge and the Tate conjecture for example, though proven by Shioda for a large class of Fermat hypersurfaces, still

remain open for general Fermat hypersurfaces.

Now let $R = k = \mathbb{F}_q$ be a finite field. Then every homogenous equation $f(X_1, \dots, X_n) = 0$ over k has only a finite number $\nu^{(i)}$ of solutions in the finite extensions \mathbb{F}_{q^i} of k , and the collection of all these numbers in the *zeta function*

$$\zeta(f, T) := \exp \left(\sum_{i=1}^{\infty} \frac{\nu^{(i)}}{i} T^i \right) \in \mathbb{Q}[[T]],$$

is one of the most fundamental and important invariants of f respectively the $(n-2)$ -dimensional hypersurface $X(f)$ defined by f in \mathbb{P}_k^{n-1} .

A finer invariant is the l -adic cohomology $H_{\text{ét}}^*(\bar{X}(f), \mathbb{Q}_l)$ of X (for $\bar{X}(f) := X(f) \times_k \bar{k}$ and a prime $l \neq \text{char}(k)$), a finite dimensional \mathbb{Q}_l -linear representation of the absolute Galois group G_k . Knowing this representation means knowing the zeta function because of the formula

$$\nu^{(i)} = \sum_{j=0}^{2(n-2)} \text{Tr} \left[(F^*)^i \Big|_{\mathbf{H}_{\text{ét}}^j(\bar{X}(f), \mathbb{Q}_l)} \right],$$

where $F \in G_k$ is the *geometric Frobenius* in G_k , the inverse of the k -automorphism $x \mapsto x^q$.

The zeta function of the Fermat hypersurface $X_n^r := X(P_n^r)$ was already known to Weil; he computed it in the above mentioned article and showed in particular that it was not only a power series but a *rational* function, leading him to the conjecture that the zeta function of smooth, projective varieties over k is always rational.

Later Deligne computed the Galois-representation $H_{\text{ét}}^*(\bar{X}_n^r, \mathbb{Q}_l)$ (see [Del82]), which is particularly simple, since the cohomology decomposes into canonical one-dimensional subspaces on which the Frobenius acts by certain Hecke characters, the so called *Jacobi sums*.

Taking Fermat hypersurfaces as a starting point, it is a natural step to consider slightly more general hypersurfaces like *diagonal hypersurfaces*, given by *diagonal* equations of the form

$$a_1 X_1^r + \dots + a_n X_n^r = 0$$

for $a_i \in k$. These were studied thoroughly (for $k = \mathbb{F}_q$, $q \equiv 1 \pmod{r}$) by Fernando Q. Gouvêa und Noriko Yui in the book [GY95]; using Weil's and Deligne's results, it is not difficult to compute the zeta function of such

diagonal equations.

“Geometrically”, i.e. over \bar{k} , every diagonal equation of degree r in n unknowns is isomorphic to the Fermat equation P_n^r , in the sense that there is a linear change of variables ($X_i \mapsto \sqrt[r]{a_i} X_i$) transforming the given equation into P_n^r . Thus diagonal equations are only interesting if k is not algebraically closed, so that “arithmetical” questions come into play.

Look at the following two quadratic diagonal equations in three unknowns over \mathbb{Q} :

$$P_3^2 : X_1^2 + X_2^2 + X_3^2 = 0 \quad \text{and} \\ Q : X_1^2 - 2X_2^2 - X_3^2 = 0.$$

Whereas P_3^2 has no non-trivial solution in \mathbb{Q} , equation Q has infinitely many (“Pell’s equation”), so even though P_3^2 and Q become isomorphic over $\bar{\mathbb{Q}}$, they seem to be completely unrelated over \mathbb{Q} .

But in fact it *is* possible to use the isomorphism over $\bar{\mathbb{Q}}$ to gain information over \mathbb{Q} by a general principle known as *Galois descent*: If K/k is a Galois extension with Galois group G , and if X is an object “defined over k ”, then every object Y over k which becomes isomorphic to X “over K ” (and is then called a K/k -form of X) defines a class in $H^1(G, A(X))$, where $A(X)$ is the (not necessarily abelian) automorphism group of X over K . The idea of descent is to deduce properties of Y from properties of X by “twisting” with this class. In particular this can be done in the case of diagonal equations, since they are \bar{k}/k -forms of Fermat equations.

This immediately leads to the following question: *Are there \bar{k}/k -forms of Fermat equations, so-called “twisted Fermat equations”, which are not diagonal?* — If the answer is “yes”, one can then try to use Galois descent to answer questions about the cohomology and zeta function of such twisted equations.

In the case $K = \bar{k}$, the automorphism group $A(P_n^r)$ equals $\mu_r \wr S_n$, the wreath product of the group of r -th roots of unity in K with the symmetric group S_n ; here S_n acts on P_n^r by permuting the X_i , and $(\zeta_i) \in \mu_r^n$ acts by $X_i \mapsto \zeta_i X_i$.

The K/k -forms of P_n^r are then given by classes in $H^1(G_k, \mu_r \wr S_n)$, and it turns out that the diagonal equations are precisely those whose class already comes from $H^1(G_k, \mu_r^n)$, so that from this point of view, considering diagonal equations alone is an unnatural restriction.

In this book we therefore want to equally consider *all* forms of P_n^r , first classify them, then study them with the method of descent and (in the case $k = \mathbb{F}_q$) compute their zeta function.

In contrast to the case of diagonal equations, it is difficult to see in general whether a given equation is a form of the Fermat equation or not — the equation

$$4X_1^2X_2 + 3X_1X_2^2 + 3X_1^2X_3 + 4X_2^2X_4 + 4X_1X_3X_4 + X_1X_4^2 \\ + 4X_2X_3^2 + X_2X_3X_4 + X_3X_4^2 + 2X_3^3 + X_3^2X_4 + 2X_3X_4^2 + 3X_4^3 = 0$$

for example is a form of the Fermat equation P_4^3 over the field \mathbb{F}_5 which is *not* diagonal. And even for equations as complicated as this one the method of descent will enable us to compute the group of automorphisms over k and the zeta function.

On the other hand, it is of course a slight disadvantage of general twisted Fermat equations that they do not show any apparent symmetry, because this fact often makes it difficult to decide whether a given equation is a twisted Fermat equation or not.

An interesting exception is the case $r = 3$, $n = 2$, the case of *binary cubic equations*, because in that case *all* “non-singular” equations are forms of P_2^3 . Using the methods explained in this book, we can not only classify all such forms, but make this classification completely explicit, enabling us to compute the class and (if k is a finite field) the zeta function for any given (non-singular) binary cubic equation.

In the *second chapter* we will introduce one of the key concepts of this book, the *zeta function* of a variety over a finite field, and we will state the Weil-conjectures.

Even though the method of descent is “folklore”, the details can be somewhat tricky. Therefore in the *third chapter*, we explain what we mean by “Galois descent” and axiomatize an important class of situations in which Galois descent holds:

Definition: A *coefficient extension* (from k to K) consists of two categories \mathcal{C}_k and \mathcal{C}_K , a covariant functor $F : \mathcal{C}_k \rightarrow \mathcal{C}_K$ and for all $Y, Z \in \text{Ob}(\mathcal{C}_k)$ a G -action (from the left) on $\text{Iso}_{\mathcal{C}_K}(FY, FZ)$ (the set of isomorphisms between FY and FZ in \mathcal{C}_K), so that the following two conditions are satisfied:

(CE1): The action is compatible with compositions, i.e. for objects $X, Y, Z \in \text{Ob}(\mathcal{C}_k)$, isomorphisms $X \xrightarrow{g} Y$ and $Y \xrightarrow{f} Z$ and an element $s \in G$, we have:

$${}^s(fg) = {}^s f {}^s g.$$

(CE2): Exactly those isomorphisms that come from \mathcal{C}_k are fix under the action of G , i.e. for objects $Y, Z \in \text{Ob}(\mathcal{C}_k)$ we have:

$$\text{Im} \left(\text{Iso}_{\mathcal{C}_k}(Y, Z) \xrightarrow{F} \text{Iso}_{\mathcal{C}_K}(FY, FZ) \right) = \left[\text{Iso}_{\mathcal{C}_K}(FY, FZ) \right]^G.$$

Two examples of coefficient extensions are particularly important for our study of K/k -forms of Fermat equations: First the categories $\mathcal{F}_k^{n,r}$ and $\mathcal{F}_K^{n,r}$ whose objects are homogenous equations of degree r in n unknowns with coefficients in k respectively K and whose morphisms are elements of $\text{GL}(n, k)$ respectively $\text{GL}(n, K)$, considered as linear changes of variables. The coefficient extension is then given by the obvious functor $\mathcal{F}_k^{n,r} \rightarrow \mathcal{F}_K^{n,r}$ and the natural G -action on $\text{GL}(n, K)$.

The importance of this coefficient extension for us is obvious: The Fermat equation P_n^r is an object of $\mathcal{F}_k^{n,r}$, and the twisted Fermat equations are exactly those objects of $\mathcal{F}_k^{n,r}$ that become isomorphic to P_n^r in $\mathcal{F}_K^{n,r}$.

The second important example is given by the categories $\mathbf{Rep}_{\mathbb{Q}_l}^{G_k}$ and $\mathbf{Rep}_{\mathbb{Q}_l}^{G_K}$ of \mathbb{Q}_l - G_k -representations respectively \mathbb{Q}_l - G_K -representations, together with the functor $\mathbf{Rep}_{\mathbb{Q}_l}^{G_k} \rightarrow \mathbf{Rep}_{\mathbb{Q}_l}^{G_K}$ that maps a representation $G_k \xrightarrow{\varphi} \text{Aut}_{\mathbb{Q}_l}(V)$ to its restriction $\varphi|_{G_K}$. Here the action of an element \bar{s} of $G = G_k/G_K$ on $(V, \varphi) \xrightarrow{f} (W, \psi)$ is defined by “conjugation”, i.e. by $f \mapsto \psi(\bar{s})f\varphi(\bar{s})^{-1}$.

This coefficient extension is important for us, because the l -adic cohomology $\mathbf{H}_{\text{ét}}^*(\bar{X}_n^r, \mathbb{Q}_l)$ is an object of $\mathbf{Rep}_{\mathbb{Q}_l}^{G_k}$ and because the cohomology of a form of the Fermat hypersurface X_n^r is a form of $\mathbf{H}_{\text{ét}}^*(\bar{X}_n^r, \mathbb{Q}_l)$.

Although these two examples are the most important for our purposes, coefficient extensions occur in many more situations, and we will give some interesting additional examples like the base change functor from the category of k -varieties to the category of K -varieties.

As already mentioned above, the classification of forms using Galois descent will involve the cohomology $H^1(G, A)$ for not necessarily abelian coefficients A , because the automorphism groups of objects we study will often be nonabelian — the wreath product $A(P_n^r) = \mu_r \wr S_n$ for example is not abelian for $n \geq 2$. Therefore in the *fourth chapter* we want to explain the basic definitions and results from the theory of nonabelian cohomology. We will closely follow Serre's presentation from [Ser97], being slightly more general by considering general topological groups G and not only profinite ones. This will in particular enable us to treat our Galois group G as both a discrete and a profinite group.

The *fifth chapter* will give a brief introduction to l -adic cohomology and Weil cohomology theories and explain how these topics are related to the Weil conjectures and their proof. In particular, we will see how the zeta function of a variety X can be computed from the Galois-action on the l -adic cohomology $H_{\text{ét}}^*(\bar{X}, \mathbb{Q}_l)$ of X .

In the *sixth chapter* we are going to explain how to use Galois descent in the framework of arbitrary coefficient extensions $F : \mathcal{C}_k \rightarrow \mathcal{C}_K$ to classify forms: If X is an object of \mathcal{C}_k , then by $E(\mathcal{C}_K/\mathcal{C}_k, X)$ we denote the set² of $\mathcal{C}_K/\mathcal{C}_k$ -forms of X , i.e. of isomorphism classes $[Y]$ of objects of \mathcal{C}_k such that FY is isomorphic to FX in \mathcal{C}_K .

If $[Y]$ is such a $\mathcal{C}_K/\mathcal{C}_k$ -form of X , and if $FY \xrightarrow{f} FX$ is an isomorphism in \mathcal{C}_K , then $s \mapsto f^s(f^{-1})$ defines a 1-cocycle $a = (a_s)$ of $G := \text{Gal}(K/k)$ in $A(X) := \text{Aut}_{\mathcal{C}_K}(FX)$ whose cohomology class $\vartheta[Y]$ in $H^1(G, A(X))$ will turn out to be independent of Y and f :

Proposition: *The assignment $[Y] \mapsto \vartheta[Y]$ is a well defined injection from $E(\mathcal{C}_K/\mathcal{C}_k, X)$ into $H^1(G, A(X))$.*

As a first application we will compute the group of automorphisms of Y in \mathcal{C}_k : It is $\text{Aut}_{\mathcal{C}_k}(Y) = (A(X)_{\vartheta[Y]})^G$, where $A(X)_{\vartheta[Y]}$ is the group $A(X)$

²A priori this is only a class, but we will prove that it is indeed a set

with its G -action *twisted by the class* $\vartheta[Y]$, i.e. $s \in G$ acts by $b \mapsto a_s {}^s b a_s^{-1}$.

If $\mathcal{C}_k' \rightarrow \mathcal{C}_{K'}$ is another coefficient extension, and if we have functors $\mathcal{C}_k \xrightarrow{H_k} \mathcal{C}_k'$ and $\mathcal{C}_K \xrightarrow{H_K} \mathcal{C}_{K'}$ which are compatible with each other and with the G -actions (a notion to be made precise, of course), we talk about a *morphism of coefficient extensions*, and we get a commutative diagram

$$\begin{array}{ccc}
 E(K/k, X) & \xrightarrow{[Y] \mapsto [H_k Y]} & E(K/k, H_k X) \\
 \vartheta \downarrow & = & \downarrow \vartheta \\
 H^1(G, A(X)) & \xrightarrow{(a_s) \mapsto (H_K a_s)} & H^1(G, A(H_k X))
 \end{array}$$

This result is very important for our purposes if we apply it to the coefficient extensions $\mathcal{F}_k^{n,r} \rightarrow \mathcal{F}_K^{n,r}$ and $\mathbf{Rep}_{\mathbb{Q}_l}^{G_k} \rightarrow \mathbf{Rep}_{\mathbb{Q}_l}^{G_K}$ introduced above and the functors H_k and H_K induced by l -adic cohomology, because it then states the following:

If Q is a $\mathcal{F}_K^{n,r} / \mathcal{F}_k^{n,r}$ -form of the Fermat equation P_n^r , characterized by a cohomology class $\vartheta[Q]$, then the cohomology of the hypersurface $X(Y)$ and hence its zeta function are determined by the class $H_{\text{ét}}^ \vartheta[Q]$.*

So instead of having to compute the cohomology of $X(Q)$ directly, to get the zeta function, we can compute the composition $\vartheta^{-1} \circ H_{\text{ét}}^* \circ \vartheta$ which explicitly involves the following steps:

- We have to understand the l -adic cohomology of the Fermat hypersurface X_n^r with its Galois action — this is achieved by Deligne’s result mentioned above.
- For an automorphism $a \in A(P_n^r)$, we have to compute the associated automorphism $H_{\text{ét}}^*(a)$ on $H_{\text{ét}}^*(\bar{X}_n^r, \mathbb{Q}_l)$.
- We must compute the preimage of any given class under the injection ϑ .

The *seventh chapter* is devoted to the study of the nonabelian cohomology $H^1(G, \mu_r \wr S_n)$ and hence to the study of $\mathcal{F}_K^{n,r} / \mathcal{F}_k^{n,r}$ -forms of P_n^r for $K := \bar{k}$. We mainly follow the lines of Christopher Rupprecht’s diploma thesis [Rup96], making the maps and constructions involved more explicit though in order to later allow us to compute zeta functions explicitly.

Furthermore, we are going to compute the groups of automorphisms of twisted Fermat equations.

The main results from that chapter are:

If $r \geq 3$, we have a bijection

$$E(\mathcal{F}_K^{n,r} / \mathcal{F}_k^{n,r}, P_n^r) \cong \coprod_L \text{Aut}_k(L) \setminus (L^\times / L^{\times r})$$

where the disjoint union is taken over k -isomorphism classes of separable k -algebras L of degree n over k . If Q denotes the equation corresponding to the pair (L, x) under this bijection and if $L = \prod_{i=1}^m L_i$ with fields L_i/k , then we have the following canonical exact sequence of groups:

$$1 \rightarrow \prod_{i=1}^m (L_i \cap \mu_r) \rightarrow \text{Aut}_{\mathcal{F}_k^{n,r}}(Q) \rightarrow \left\{ a \in \text{Aut}_k(L)^{\text{opp}} \mid \frac{ax}{x} \in L^{\times r} \right\} \rightarrow 1.$$

In *chapter eight* we will look at the special case of binary cubic equations of a field k with $\text{char}(k) \geq 5$. As already mentioned above, in that case *all* non-singular objects of $\mathcal{F}_k^{2,3}$ (i.e. those with non vanishing discriminant) are forms of the Fermat equation P_2^3 .

As an application of chapter seven, we are first going to give a complete list of $\mathcal{F}_K^{2,3} / \mathcal{F}_k^{2,3}$ -forms of P_2^3 for *finite* fields k . Then we will show how the classification achieved in chapter seven can be made totally explicit in $\mathcal{F}_k^{2,3}$: For a given non-singular binary cubic equation, the corresponding pair (L, x) from the bijection above can be computed as follows:

Theorem: Let $Q(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3$ be a non-singular equation over k with $a \neq 0$. Put

$$\delta := -\frac{\Delta(Q)}{27} \in k^\times,$$

$$e := \frac{a}{2} - \frac{27a^2d + 2b^3 - 9abc}{2\Delta(Q)} \sqrt{\delta} \in k(\sqrt{\delta})^\times,$$

where

$$\Delta(Q) := -27a^2d^2 + 18abcd + b^2c^2 - 4b^3d - 4ac^3$$

is the discriminant of Q and where the square root of δ has to be chosen in such a way that $e \neq 0$.

Then Q corresponds to the pair:

$$\begin{cases} \left(k \times k, \left(e, \frac{\sqrt{\delta}}{e} \right) \right) & \text{if } \delta \in k^{\times 2}, \\ (k(\sqrt{\delta}), e) & \text{otherwise.} \end{cases}$$

The real polynomials $x^4 + y^4 + z^4$ and $-x^4 - y^4 - z^4$ are not isomorphic in $\mathcal{F}_{\mathbb{R}}^{3,4}$, i.e. there is no linear change of variables with coefficients in \mathbb{R} that transforms the one into the other.

If we interpret polynomials as equations, then this fact seems unnatural, since both polynomials obviously have the same set of solutions and “ought to be” isomorphic. Following this intuition, in *chapter nine* we are going to consider a slightly modified coefficient extension $\widetilde{\mathcal{F}}_k^{n,r} \rightarrow \widetilde{\mathcal{F}}_K^{n,r}$ in which polynomials that only differ by a scalar become isomorphic. Morphisms in these categories are no longer elements of $\text{GL}(n, k)$ respectively $\text{GL}(n, K)$ but of $\text{PGL}(n, k)$ respectively $\text{PGL}(n, K)$. It seems plausible that there will be “less” $\widetilde{\mathcal{F}}_K^{n,r} / \widetilde{\mathcal{F}}_k^{n,r}$ -forms of P_n^r than $\mathcal{F}_K^{n,r} / \mathcal{F}_k^{n,r}$ -forms, and we are going to show how to make this intuitive notion precise:

Proposition: *Two pairs (L, x) and (L, x') define the same form in $\widetilde{\mathcal{F}}_k^{n,r}$ if and only if there is $a \in \text{Aut}_k(L)$, $\lambda \in k^\times$ and $y \in L^\times$, such that $x' = a[\lambda xy^r]$.*

The fact that we have an action of the wreath product $\mu_r \wr S_n$ on X_n^r implies that there is a decomposition of the l -adic cohomology of X_n^r into eigenspaces corresponding to the characters of the abelian group μ_r^n .

In the *tenth chapter* we will more generally study the situation of a semidirect product $A \rtimes S$ (A being finite abelian) acting on an object M of a pseudo-abelian category. It will turn out that again we get a decomposition of M into eigenspaces M_χ corresponding to the characters χ of A , and if p_χ denotes the injection $M_\chi \rightarrow M$, then for any $s \in S$ we get an induced morphism $s_\chi : M_{s\chi} \rightarrow M_\chi$ such that the following diagram commutes:

$$\begin{array}{ccc} M_{s\chi} & \xrightarrow{s_\chi} & M_\chi \\ p_{s\chi} \downarrow & & \downarrow p_\chi \\ M & \xrightarrow{s} & M. \end{array}$$

So we see that the decomposition of $H_{\text{ét}}^*(\bar{X}_n^r, \mathbb{Q}_l)$ into eigenspaces is a “motivic” one, the l -adic realization of a corresponding decomposition of the Grothendieck motif $h(X_n^r)$ of X_n^r .

Chapter eleven is the technical heart of this book where we will compute the isomorphism induced on the l -adic cohomology of X_n^r by an element $\tau \in \mu_r \wr S_n$.

The result for $\tau \in \mu_r^n$ is already known from chapter ten, so that we can concentrate on $\tau \in S_n$ and even reduce further to the case where τ is the transposition (12).

As a result we will be able to prove the existence of a basis $\{v_a\}_a$ of $H_{\text{ét}}^{n-2}(\bar{X}_n^r, \mathbb{Q}_l)$ in terms of which we explicitly know the action of $\mu_r^n \wr S_n$.

In the papers of Shioda, Gouvêa und Yui, it is always assumed that the base field k contains the r -th roots of unity, and in this case the Galois action with respect to the basis $\{v_a\}_a$ is well known, so that we can use the results from chapter six to explicitly describe the Galois action on the l -adic cohomology of any $\mathcal{F}_K^{n,r}/\mathcal{F}_k^{n,r}$ -form of P_n^r .

In addition to that, we will be able to show that it is often possible to do the same in the general case over arbitrary finite base fields.

In *chapter twelve* we will sum up the results needed for the computation of the zeta function of a given twisted Fermat equation, and we will give a step-by-step explanation of how to use these results for explicit computations, finally illustrating everything with an instructive example.

At the end of the book, two appendices can be found, one explaining some basic definitions and facts about *pseudo-abelian categories*, the other explicitly computing a certain *Jacobi sum* needed in the examples.