Arithmetic Properties of non-hyperelliptic genus 3 curves.

Elisa Lorenzo García

Universitat Politècnica de Catalunya

Advisor: Joan-Carles Lario Loyo

Thesis defense: 10th September 2014

Contents

Introduction **3**

Preliminars **7**

1 Twists of non-hyperelliptic curves **11**
1.1 Galois embedding problems 11
1.2 Equations of the twists 12
1.3 Description of the method 13
1.4 An example 16

2 Non-hyperelliptic genus 3 curves **21**
2.1 Henn classification 22
2.2 Modified Henn classification 23
2.3 A representative in the modified Henn classification 29

3 Twists of non-hyperelliptic genus 3 curves **35**
3.1 The Fermat quartic 35
3.2 Cases from I to X 45
3.3 The Klein quartic 51

4 The Sato-Tate conjecture for the twists of the Fermat and Klein quartics **61**
4.1 The Sato-Tate conjecture 62
4.2 The Sato-Tate groups 62
4.3 The Sato-Tate distributions 66
4.4 Example curves 67

5 The Sato-Tate conjecture for the Fermat hypersurfaces **69**
5.1 Étale cohomology 69
5.2 Jacobi sums 71
5.3 Sato-Tate groups 77
5.4 Proof of the conjecture 79

5.5 An example 79

Appendix **85**

Inverse Galois problems 85

Tables 90

Bibliography **111**

Abstract

We develope an algorithm for computing the twists of a given curve assuming that its automorphism group is known. And in the particular case in which the curve is non-hyperelliptic we show how to compute equations of the twists. The algorithm is based on a correspondence that we establish beetwen the set of twists and the set of solutions of a certain Galois embedding problem. As an application to our algorithm we give a classification with equations of the twists of all plane quartic curves, that is, the non-hyperelliptic genus 3 curves, defined over any number field k.

The study of the set of twists of a curve has been proven to be really useful for a better understanding of the behaviour of the Generalize Sato-Tate conjecture. We prove the Sato-Tate conjecture for the twists of the Fermat and Klein quartics and we compute the Sato-Tate groups and Sato-Tate distributions of them.

Following with the study of the Generalize Sato-Tate conjecture, we show how to compute the Sato-Tate groups and the Sato-Tate distributions of the Fermat hypersurfaces: $X_n^m : x_0^m + ... + x_{n+1}^m = 0$. We prove the Sato-Tate conjecture for them when they are considerd to be defined over $\mathbb{Q}(\zeta_m)$.

Introduction

This thesis explores the explicit computation of twists of curves. We develope an algorithm for computing the twists of a given curve assuming that its automorphism group is known. And in the particular case in which the curve is non-hyperelliptic we show how to compute equations of the twists. The algorithm is based on a correspondence that we establish beetwen the set of twists and the set of solutions of a certain Galois embedding problem. In general is not known how to compute all the solution to a Galois embedding problem. Through the thesis we give some ideas of how to solve these problems.

The twists of curves of genus ≤ 2 are well-known. While the genus 0 and 1 cases go back from long ago, see [55], the genus 2 case is due to the work of Cardona and Quer [8], [9]. All the genus 0, 1 or 2 curves are hyperelliptic, however for genus greater than 2 almost all the curves are non-hyperelliptic.

As an application to our algorithm we give a classification with equations of the twists of all plane quartic curves, that is, the non-hyperelliptic genus 3 curves, defined over any number field k. The first step for computing such twists is providing a classification of the plane quartic curves defined over a concrete number field k. The starting point for doing this is Henn classification of plane quartic curves with non-trivial automorphism group over $\mathbb{C}$.

An example of the importance of the study of the set of twists of a curve is that it has been proven to be really useful for a better understanding of the behaviour of the Generalize Sato-Tate conjecture, [16], [18], [21], [22]. We show a proof of the Sato-Tate conjecture for the twists of the Fermat and Klein quartics as a corollary of a deep result of Johansson, [34], and we compute the Sato-Tate groups and Sato-Tate distributions of them.

Following with the study of the Generalize Sato-Tate conjecture, in the last chapter of this thesis we explore such conjecture for the Fermat hypersurfaces $X_n^m : x_0^m + ... + x_{n+1}^m = 0$. We explicitly show how to compute the Sato-Tate groups and the Sato-Tate distributions of these Fermat hypersurfaces. We also prove the conjecture over $\mathbb{Q}$ for $n = 1$ and over $\mathbb{Q}(\zeta_m)$

if $n \neq 1$.

Content of chapters

In the first chapter of this thesis we describe an algorithm for computing the twists of curves via a correspondence between the twists and certain solutions to a Galois embedding problem, section (1.1). In section (1.2) we show how to compute equations for the twists when the curve is non-hyperelliptic. We give a detailed descripcion of the algorithm in section (1.3). Finally, for illustrating the algorithm, in section (1.4), we show a complete example of the computation to the twists and its equations of a genus 10 non-hyperelliptic curve.

In chapter 2 we do the preparations for giving a classification of the twists of all non-hyperelliptic genus 3 curves defined over a given number field k. In section (2.1) we show a classification due to Henn of the plane quartic curves with non trivial automorphism group, up to $\mathbb{C}$−isomorphism. In section (2.2) we modify this classification for getting it up to k−isomorphism. Finally, in section (2.3) we show, given any plane quartic with nontrivial automorphism group, how to find its representant in such classification.

After the results in chapter 2 we are ready for computing the twists of all plane quartic curves. In chapter 3 we give the classification of all such twists. In section (3.1) (resp. section 3.3) we compute the twists of the Fermat (resp. Klein) quartics, that are the harder cases, in part due to the fact that are, up to isomorphism, the two plane quartic curves with a biggest automorphism group. In section (3.2) we compute the twists of the rest of plane quartic curves. Just mentioning that this classification of the twists of the plane quartic curves is not totally complete, because we have not been able of computing a single case for the Klein quartic. The problem is that we have not been able of completely solving the corresponding galois embedding problem, so there is a single family of solutions/twists that we could not compute explicitly.

In chapter 4 we apply the former computations for computing new Sato-Tate distribution among the twists of the Fermat and Klein quartics. In section (4.1) we show a proof of the generalize Sato-Tate conjecture for these twists. The corresponding Sato-Tate groups and Sato-Tate distributions are computed in sections (4.2) and (4.3) respectively. Finally, in section (4.4) we show concrete examples of curves that attains such differente distributions and that have the corresponding Sato-Tate groups computed.

In chapter 5 we follow with the study of the Generalize Sato-Tate conejcture, but this time, we focus our study on the Fermat hypersurfaces $X_n^m : x_0^m + ... + x_{n+1}^m = 0$. In (5.1) we describe the Galois action on its étale cohomology and in (5.2) we explain some properties of the Jacobi Sums, both things will be necesary for computing the Sato-Tate groups in (5.3). In (5.4) we prove the conjecture over $\mathbb{Q}$ for $n = 1$ and over $\mathbb{Q}(\zeta_m)$ if $n \neq 1$. Finally we show a complete example in (5.5).

In the first part of the appendix we establish a correspondence between the solutions to a given Galois inverse problem and rational points in a certain variety that we explicitly show how to compute via an algorithm. This can useful for trying to solve Galois embedding problems as the ones that appear in section (1.1) for computing the twists of curves. Our idea is, once the algorithm will be implemented, try to find the missed solution of the Galois embedding problem corresponding to the Klein quartic.

Finally, in the last part of the appendix we show tables with all the data computed through out the thesis: automorphism groups of the families of plane quartic curves in Henn classification and in the modified one, Dixmier-Ohno invariants of some of the families, the Sato-Tate distributions and the example curves in chapter 4 and some tables with examples of chapter 5.

General notations

We now fix some notation and conventions that will be valid in all the chapters. For us $\mathbb{Z}$ (res. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) is the ring (resp. field) of integers (resp. of rational numbers, of real numbers, of complex numbers). And $\mathbb{F}_q$ denotes the finite field of $q = p^r$ elements where p is a prime number, $\mathbb{Z}_l$ the ring of $l-$adic integers and $\mathbb{Q}_l$ the field of $l-$adic numbers, where again l is a prime number. For a commutative unitary ring A, let $\mathcal{M}_n(A)$ (resp. $\mathrm{GL}_n(A)$, $\mathrm{SL}_n(A)$, $\mathrm{Sp}_n(A)$) denotes the ring of n by n matrices with coefficients in A (resp. that are inverible, that has determinant equal to 1, that are symplectic).

For any field F, we denote by $\bar{F}$ an algebraic closure of F. And by G_F the absolute Galois group $\mathrm{Gal}(\bar{F}/F)$. We will recurrently consider the action of G_F on several sets, and this action will be in general denoted by left exponentiation.

By k we will always mean a number field. All field extensions of k that we consider are contained in a fixed algebraic closure $\bar{k}$. We write ζ_n to refer to a primitive $n-$th root of the unity in $\bar{k}$. We denote by $\mathcal{O}_k$ the ring of integers of k. By abuse of language, we will refer to the prime ideals of $\mathcal{O}_k$ as prime ideals of k.

When we will work with groups we will usually use the SmallGroup Library-GAP, [24]. Where the group $\mathrm{GAP}(N, r)$ will be denote the group of order N that appears in the $r-$th position in such library. Very often we will also use the notation $< N, r >$. We denote by C_n (resp. D_n, S_n, A_n) the cyclic group of n elements (resp. the dihedral one of $2n$ elements, the symmetric one of $n!$ and the alternate one of $n!/2$). And by V_4 we denote the direct product $C_2 \times C_2$.

Acknowledgements

Preliminars

Non-hyperelliptic curves

Let C be a projective algebraic, smooth and irreducible genus g curve defined over a number field k. Let $\{\omega_1, ..., \omega_g\}$ be a basis of the regular differentials $\Omega^1(C)$ of C. We denote by K_C a canonical divisor of C. The canonical morphism is:

$$\phi_K : C \to \mathbb{P}^g, \qquad P \to (\omega_1(P) : ... : \omega_g(P))$$

Definition 0.0.1. *A curve C is said to be non-hyperelliptic if the canonical morphism is an embedding. In this case, the image, $\phi_K(C)$, is called the canonical model and it is a curve of degree $2g-2$. If the canonical morphism is not an embedding, then it is a degree 2 morphism and the curve is called hyperelliptic.*

All genus 1 and 2 curves are hyperelliptic, while for genus greater or equal to 3 there are as well hyperelliptic ones as non-hyperelliptic ones.

Proposition 0.0.2. *Given a non-hyperelliptic curve C defined over a number field k we can take a canonical model also defined over k.*

Proof. Since we can take a canonical divisor K_C defined over k, see [37], we can take a basis of the vector space $L(K_C) := \{f \in \bar{k}(C) : \mathrm{div}(f) \geq -K_C\} \cup \{0\}$ defined over k. And then, the algebraic relations satisfied by the elements of this base are defined over k. □

The automorphism group of C, denoted $\mathrm{Aut}(C)$, is the group of isomorphisms from C to itself defined over $\bar{k}$.

Remark 0.0.3. *Given a canonical model of a non-hyperelliptic curve, we can see the group $\mathrm{Aut}(C)$ as a subgroup of $\mathrm{PGL}_g(\bar{k})$, since any element in $\mathrm{Aut}(C)$ induces an automorphism in $\mathbb{P}^g$ via the canonical morphism and the automorphisms of $\mathbb{P}^g$ are given by projective matrices.*

Twists of curves

We reproduce here, for completeness, part of the twisting theory explained in [55]. Let C/k be a smooth and projective curve.

Definition 0.0.4. *A twist of C/k is a smooth curve C'/k which is isomorphic to C over $\bar{k}$. We identify two twists if they are isomorphic over k. The set of twists of C/k, modulo $k-$isomorphism, will be denoted by* $\operatorname{Twist}_k(C)$.

Let C'/k be a twist of C/k. Then, there is an isomorphism $\phi : C' \to C$ defined over $\bar{k}$. To measure the failure of ϕ to be defined over k, we consider the map

$$\xi : G_k \to \operatorname{Aut}(C) \qquad \xi_\sigma = \phi \circ {}^\sigma\phi^{-1}.$$

It turns out that ξ is a 1−cocycle, and the cohomology class of ξ in $\mathrm{H}^1(G_k, \operatorname{Aut}(C))$ is uniquely determined by the $k-$isomorphism class of C'.

Theorem 0.0.5. *The map*

$$\operatorname{Twist}_k(C) \to \mathrm{H}^1(G_k, \operatorname{Aut}(C)),$$

that sends a twist $\phi : C'/k \to C/k$ to $\xi_\sigma = \phi \circ {}^\sigma\phi^{-1}$ is a bijection.

Let us denote by K the minimal field where all the elements in $\operatorname{Aut}(C)$ can be defined. If $g \geq 2$, by Hurwitz's theorem [Hur], the group $\operatorname{Aut}(C)$ is finite, and then K/k is a finite Galois extension. Fix now a twist $\phi : C' \to C$, and call L/k the minimal field where all the isomorphisms between C' and C can be defined. Clearly, L/k is a finite Galois extension and K/k is a subextension of L/k. Moreover, L is the splitting field of the cocycle $\xi_\sigma = \phi \circ {}^\sigma\phi^{-1}$. That is, L/k is the minimal Galois extension such that $\xi(G_L) = \{1\}$.

Remark 0.0.6. *If* $\operatorname{Aut}(C)$ *is trivial, then* $\operatorname{Twist}_k(C)$ *is also trivial.*

The previous discussion applies when we interchange C by a smooth quasi-projective variety X.

Galois embedding problem

Here we define the Galois embedding problem, see for example section 9.4 in [41]. Given a field k and a finite group G one may pose the following question, the so called Inverse Galois problem: does exist a Galois extension F/k such that $\operatorname{Gal}(F/k) \simeq G$? The embedding problem is a generalization of the former one. It asks whether a given Galois extension K/k can be embedded into another Galois extension F/k in such a way that the restriction map between the corresponding Galois groups is given.

Given a Galois extension K/k with Galois group H, an embedding problem is a diagram:

$$\begin{tikzcd}
& G_k \arrow[d, two heads, "\pi"'] & \\
G \arrow[r, "f"'] & H \arrow[r] & 1
\end{tikzcd} \tag{1}$$

where π is the natural projection and f is an epimorphism. A solution to such embedding problem is a morphism $\Psi : G_k \to G$ such that next diagram is commutative:

$$\begin{tikzcd}
& G_k \arrow[d, two heads, "\pi"] \arrow[dl, dashed, "\Psi"'] & \\
G \arrow[r, "f"'] & H \arrow[r] & 1
\end{tikzcd} \tag{2}$$

A solution Ψ is called proper if it is surjective.

The Sato-Tate conjecture

We follow [16] to give a brief introduction to the Sato-Tate Conjecture. Let E be an elliptic curve defined over a number field k. Given a prime $\mathfrak{p}$ of k of good reduction of E, we denote by $a_{\mathfrak{p}}$ the trace of the Frobenius endomorphism. That is, if $\rho_l : G_k \to \mathrm{GL}_2(\mathbb{Q}_l)$ is the l–adic representation associated with the l–torsion of the elliptic curve E, and $\mathfrak{p}$ does not lie over l, then $\det(1 - \rho_l(\mathrm{Frob}_{\mathfrak{p}}^{-1})T) = N\mathfrak{p} - a_{\mathfrak{p}}T + T^2$, where $\mathrm{Frob}_{\mathfrak{p}}^{-1}$ is the geometric Frobenius at $\mathfrak{p}$.

One can think of $a_{\mathfrak{p}}/N\mathfrak{p}^{1/2}$ as a random variable on the set of primes of good reduction of E taking values on $[-2, 2]$. And we call the distribution of this random variable the Sato-Tate distribution of the elliptic curve E.

Conjecture 0.0.7. *(Sato-Tate) For an elliptic curve without CM, the normalized traces $a_{\mathfrak{p}}/N\mathfrak{p}^{1/2}$ are equidistributed with respect to the measure:*

$$\frac{1}{2\pi}\sqrt{4 - z^2}dz,$$

where dz is the restriction of the Lebesque measure on $[-2, 2]$.

The conjecture was independetly proposed by Sato and Tate in the 60's. And it is proven when k is a totally real field (in particular, for $k = \mathbb{Q}$) by Barnet-Lamb, Geraghty, Harris and Taylor [3]. When the elliptic curve E has complex multiplication the equivalent stamente was proved longtime ago by Hecke [30].

Theorem 0.0.8. *For an elliptic curve with CM defined over M, if $M \subseteq k$, then the normalized traces $a_{\mathfrak{p}}/N\mathfrak{p}^{1/2}$ are equidistributed with respect to the measure:*

$$\frac{1}{\pi}\frac{dz}{\sqrt{4-z^2}},$$

where dz is the restriction of the Lebesque measure on $[-2, 2]$. And for an elliptic curve with CM over M and such that $M \nsubseteq k$, it is equidistributed with respect to the measure:

$$\frac{1}{2\pi}\frac{dz}{\sqrt{4-z^2}}+\frac{1}{2}\delta,$$

where δ is Dirac delta centered in 0.

In [51], Jean-Pierre Serre formulates a generalization of the Sato-Tate conjucture for motives. We will just focus on the case of varieties. Let X/k be a smooth, projective variety. Let us call $n := \dim X$, and choose an integer $0 \leq \omega \leq 2n$. Let m denote the dimension of the ω–th étale cohomology $\mathrm{H}^{\omega}_{et}(X, \mathbb{Q}_l)$ for some prime l. The action of the Galois group G_k on $\mathrm{H}^{\omega}_{et}(X, \mathbb{Q}_l)$ gives rise to the l–adic representation:

$$\rho_{\omega} : G_k \to \mathrm{Aut}(\mathrm{H}^{\omega}_{et}(X, \mathbb{Q}_l)) \subseteq \mathrm{GL}_m(\mathbb{Q}_l).$$

Let $G^1_k := \mathrm{Ker}\,\chi_l$, where χ_l denotes the l–adic cyclotomic character. Let $G^{1,\omega}_l$ be the Zariski closure of $\rho_{\omega}(G^1_k)$. Choose an embedding $\iota : \bar{\mathbb{Q}}_l \hookrightarrow \mathbb{C}$. Define $G^{1,\omega}_{l,\iota} := G^{1,\omega}_l \otimes_{\iota} \mathbb{C} \subseteq \mathrm{GL}_m(\mathrm{C})$.

Definition 0.0.9. *The Sato-Tate group of X relative to the weight ω is a maximal compact subgroup of $G^{1,\omega}_{l,\iota}$. It is a compact real Lie group that we denote by $ST(X/k,\omega)$.*

Since all maximal compact subgroups of a Lie group are conjugate, the Sato-Tate group is well-defined. Now, for each prime $\mathfrak{p}$ of good reduction of X and not lying over l, we defined $s_{\mathfrak{p}}$ as the conjugacy class of $\rho_{\omega}(Frob^{-1}_{\mathfrak{p}}) \otimes_{\iota} N\mathfrak{p}^{-\omega/2}$ in $ST(X/k, \omega)$.

Conjecture 0.0.10. *(Generalized Sato-Tate) One has:*

i) The conjugacy class of $ST(X/k, \omega)$ in $\mathrm{GL}_m(\mathbb{C})$ does not depend on the choice neither of the prime l, nor of the embedding ι.

ii) Let $(ST(X/k, \omega))$ denote the set of conjugacy classes of $ST(X, \omega)$. For $\mathfrak{p}$ of good reduction and not lying over l, the conjugacy classes $s_{\mathfrak{p}}$ are equidistributed on $(ST(X/k, \omega))$ with respect to the projection on this set of the Haar measure of $ST(X/k, \omega)$.

Remark 0.0.11. *Proving the generalized Sato-Tate conjecture for a curve is equivalent to proving it for its jacobian variety. And for an abelian variety A is enought to prove it for $\omega = 1$, since $\mathrm{H}^{\omega}_{et}(A,\mathbb{Q}_l) = \wedge^{\omega}\mathrm{H}^1_{et}(A,\mathbb{Q}_l)$, where $\mathrm{H}^1_{et}(A,\mathbb{Q}_l) = \mathrm{V}_l(A)^*$, and then $\mathrm{ST}(A/k,\omega) = \wedge^{\omega}\mathrm{ST}(A/k, 1) = \mathrm{ST}(A/k)$.*

The generalized Sato-Tate conjecture is just proven in a few cases for some motives/varieties of weight/dimension 1, 2 and 3: [35], [18], [22], [19] and [21].

Chapter 1

Twists of non-hyperelliptic curves

In this chapter we develop a method for computing the twists of any non-hyperelliptic curve C defined over a number field k. Firstly, via the well-known correspondence between twists of a curve and the Galois cohomology set $\mathrm{H}^1(G_k, \mathrm{Aut}(C))$, we establish a correspondence between the twists and the solutions to a Galois embedding problem, see (1.3). Then, we show how to get equations for the twists studying an action on the space of regular differentials $\Omega^1(C)$. This step is in which we use that the curve is non-hyperelliptic, because in that case, the canonical morphism is an isomorphism. Finally, we illustrate the method computing the twists of the non-hyperelliptic genus 6 curve: $x^7 - y^3z^4 - z^7 = 0$.

1.1 Galois embedding problems

Let C/k be a projective curve. Let us denote by K the minimal field over where all the automorphisms of C can be defined. And let us define $\Gamma := \mathrm{Aut}(C) \rtimes \mathrm{Gal}(K/k)$, where $\mathrm{Gal}(K/k)$ acts naturally on $\mathrm{Aut}(C)$, and the multiplication rule is $(\alpha,\sigma)(\beta,\tau) = (\alpha\,{}^{\sigma}\beta, \sigma\tau)$. Then, there are natural one-to-one correspondences between the following three sets:

$$\mathrm{Twist}_k(C) = \left\{C'/k\,\text{curve} \mid \exists\, \overline{k}\text{-isomorphism } \phi\colon C' \to C\right\}/k\text{-isomorphism},$$

$$\mathrm{H}^1(G_k, \mathrm{Aut}(C)) = \{\xi\colon G_k \to \mathrm{Aut}(C) \mid \xi_{\sigma\tau} = \xi_\sigma\,{}^{\sigma}\xi_\tau\}/\sim, \tag{1.1}$$

$$\widetilde{\mathrm{Hom}}(G_k, \Gamma) = \{\Psi\colon G_k \to \Gamma \mid \Psi\ \mathrm{epi}_2 - \mathrm{morphism}\}/\sim, \tag{1.2}$$

where $\xi \sim \xi'$ are cohomologous if there is $\varphi \in \mathrm{Aut}(C)$ such that $\xi'_\sigma = \varphi \cdot \xi_\sigma \cdot {}^{\sigma}\varphi^{-1}$, and $\Psi \sim \Psi'$ if there is $(\varphi, 1) \in \mathrm{Aut}(C) \rtimes \mathrm{Gal}(K/k)$ such that $\Psi'_\sigma = (\varphi,1)\Psi_\sigma(\varphi,1)^{-1}$. Here, the meaning of epi_2 − morphism is that Ψ is a group homomorphism such that the composition $\pi \cdot \Psi\colon G_k \to \Gamma \to \mathrm{Gal}(K/k)$ is surjective where $\pi\colon \Gamma \to \mathrm{Gal}(K/k)$ is the natural projection on the second component of the elements of Γ.

These correspondences send ϕ to $\xi_\sigma = \phi\cdot{}^\sigma\phi^{-1}$, and ξ to $\Psi_\sigma = (\xi_\sigma, \overline{\sigma})$, where $\overline{\sigma}$ denotes the projection of $\sigma \in G_k$ onto $\mathrm{Gal}(K/k)$.

Attached to every twist $\phi\colon C' \to C$ we shall consider its splitting field L, which by definition is the splitting field of the corresponding homomorphism Ψ; one has, $\mathrm{Ker}(\Psi) = \mathrm{Gal}(\bar{k}/L)$ and $\mathrm{Gal}(L/k) \simeq \mathrm{Image}(\Psi) \subseteq \Gamma$. Notice that ϕ is defined over L, also $\xi_\sigma = 1$ for all $\sigma \in \mathrm{Gal}(\bar{k}/L)$, and L contains K. In fact, the homomorphism Ψ is a solution of the Galois embedding problem:

$$\begin{tikzcd}
& & & G_k \arrow[dl, dashed, "\Psi"'] \arrow[d] & \\
1 \arrow[r] & \mathrm{Aut}(C) \arrow[r, hook] & \Gamma \arrow[r, "\pi"'] & \mathrm{Gal}(K/k) \arrow[r] & 1
\end{tikzcd} \tag{1.3}$$

Reciprocally, every solution Ψ of the above embedding problem gives rise to a twist of C. Notice that in order to keep track of the equivalence classes of twists we must here consider two solutions Ψ and Ψ' equivalent only under the restricted conjugations allowed in the definition of the set $\widetilde{\mathrm{Hom}}(G_k, \Gamma)$.

1.2 Equations of the twists

Let $\Omega^1(C)$ be the $k-$vector space of regular differentials of C. Let $\omega_1, ..., \omega_g$ be a basis of $\Omega^1(C)$, where g is the genus of C. Given a twist $\phi\colon C' \to C$ and its splitting field L, we consider the extension of scalars $\Omega^1_L(C) = \Omega^1(C) \otimes_k L$ which is a $k-$vector space of dimension $g[L:k]$. We can (and do) identify $\Omega^1_L(C)$ with $L < \omega_1, ..., \omega_g >= \{\sum \lambda_i\omega_i \mid \lambda_i \in L\}$ considered as $k-$vector space. For every $\sigma \in \mathrm{Gal}(L/k)$, we can consider the twisted action on $\Omega^1_L(C)$ defined as follows:

$$(\sum \lambda_i\omega_i)^\sigma_\xi := \sum {}^\sigma\lambda_i \xi^{*-1}_\sigma(\omega_i)$$

for $\lambda_i \in L$. Here, $\xi^*_\sigma \in \mathrm{End}_K(\Omega^1(C))$ denotes the pull-back of $\xi_\sigma = \phi \cdot^\sigma \phi^{-1} \in \mathrm{Aut}_K(C)$. One readly checks that

$$\rho_\xi\colon \mathrm{Gal}(L/k) \to \mathrm{GL}(\Omega^1_L(C)),\ \ \rho_\xi(\sigma)(\omega) := \omega^\sigma_\xi$$

is a $k-$linear representation. Indeed, since $\xi^*_{\sigma\tau} = {}^\sigma\xi^*_\tau \cdot \xi^*_\sigma$, we have

$$\begin{aligned}
\rho_\xi(\sigma\tau)(\sum \lambda_i\omega_i) &= \sum {}^{\sigma\tau}\lambda_i\xi^{*-1}_{\sigma\tau}(\omega_i)\\
&= \sum {}^{\sigma\tau}\lambda_i\xi^{*-1}_\sigma \cdot^\sigma \xi^{*-1}_\tau(\omega_i)\\
&= \rho_\xi(\sigma)(\sum {}^\tau\lambda_i\xi^{*-1}_\tau(\omega_i))\\
&= \rho_\xi(\sigma)\rho_\xi(\tau)(\sum \lambda_i\omega_i).
\end{aligned}$$

Recall that the function field $k(C')$ is the fixed field $\overline{k}(C)_{\xi}^{G_k}$ where the action of the Galois group G_k on $\overline{k}(C)$ is twisted by ξ according to $f_{\xi}^{\sigma} := f \cdot \xi_{\sigma}$. From this, we can identify

$$\Omega^1(C') = \Omega^1_L(C)_{\xi}^{\mathrm{Gal}(L/k)} \tag{1.4}$$

For explicit computations, one can use

$$\Omega^1(C') = \bigcap_{\sigma \in \mathrm{Gal}(L/k)} \mathrm{Ker}(\rho_{\xi}(\sigma) - \mathrm{Id}).$$

This can be useful for non-hyperelliptic curves when equations for the twisted curves are wanted. From equations of the canonical model of the initial curve,

$$C : \{F_h(x_1, ..., x_g) = 0\}$$

taking a basis $\{\omega'_j\}$ of $\Omega^1(C')$ and via identification (1.4) (notice that there is not a canonical one)

$$\omega_i = \sum_{j=1}^{g} \eta^i_j \omega'_j$$

we obtain equations for the twist making the substitution

$$C' : \left\{ F_h(\sum_{j=1}^{g} \eta^1_j \omega'_j, ..., \sum_{j=1}^{g} \eta^g_j \omega'_j) = 0 \right\},$$

and an isomorphism $\phi : C' \to C$ is given by the projective matrix $\phi = (\eta^i_j)_{ij}$.

This method for getting equations of the twists is explicitly used in a paper of Fernández, González and Lario [13] for computing equations of twists of some non-hyperelliptic genus 3 curves, case for which the canonical model is given by a plane quartic.

1.3 Description of the method

Let C be a non-hyperelliptic genus g curve defined over a number field k. Assume that $\mathrm{Aut}(C)$ is known. We take a basis of $\Omega^1(C)$, and then we obtain a canonical model $\mathcal{C}/k$ via a canonical embedding $C \hookrightarrow \mathbb{P}^{g-1}$ that we can take also defined over k. Hence, $\mathcal{C}$ and C belong to the same class in $\mathrm{Twist}_k(\mathcal{C})$ and $\mathrm{Twist}_k(\mathcal{C}) = \mathrm{Twist}_k(C)$.

In addition the automorphisms group $\mathrm{Aut}(\mathcal{C})$ can be viewed in a natural way as a subgroup of $\mathrm{PGL}_g(\bar{k})$. In fact, as a subgroup of $\mathrm{PGL}_g(K)$. And any isomorphism $\phi : \mathcal{C}' \to \mathcal{C}$ can be viewed also as a matrix in $\mathrm{PGL}_g(\bar{k})$.

Remark 1.3.1. *Two twists $\phi_i : \mathcal{C}_i \to \mathcal{C}$ are equivalent, if and only if there exists a matrix $M \in \mathrm{PGL}_g(k)$ such that $\phi_1 = \phi_2 \circ M$; that is, if the columns of ϕ_1, as an element in $\mathrm{PGL}_g\left(\bar{k}\right)$, are $k-$linear combination of the columns of ϕ_2, again as an element in $\mathrm{PGL}_g\left(\bar{k}\right)$.*

Firstly we will compute the set $\widetilde{\mathrm{Hom}}\left(G_k, \Gamma\right)$. From this set we will compute $\mathrm{H}^1\left(G_k, \mathrm{Aut}\left(\mathcal{C}\right)\right)$. And finally, we will compute equations for the twists in $\mathrm{Twist}\left(\mathcal{C}\right)$ using (1.4).

Given $\Psi \in \widetilde{\mathrm{Hom}}\left(G_k, \Gamma\right)$, let L be the splitting field of Ψ. We have $\Psi(G_K) \simeq \mathrm{Gal}(L/K)$ and $\Psi(G_k) \simeq \mathrm{Gal}(L/k)$. Then Ψ can be seen as a proper solution to the Galois embedding problem:

$$\begin{tikzcd}
 & & & G_k \arrow[dl, dashed, "\Psi"'] \arrow[d] & \\
1 \arrow[r] & \Psi(G_K) \arrow[r] & \Psi(G_k) \arrow[r] & \mathrm{Gal}(K/k) \arrow[r] & 1
\end{tikzcd} \tag{1.5}$$

As it was noticed in section 1.1, we have $\mathrm{Gal}\left(L/k\right) \simeq \mathrm{Image}\left(\Psi\right) \subseteq \Gamma$ and $\mathrm{Gal}\left(L/K\right) \simeq \Psi\left(G_K\right) \subseteq \mathrm{Aut}\left(\mathcal{C}\right) \rtimes \{1\}$. Hence, for computing $\widetilde{\mathrm{Hom}}\left(G_k, \Gamma\right)$ we should compute all the pairs (G, H) where $G \subseteq \Gamma$, $H = G \cap \mathrm{Aut}\left(C\right) \rtimes \{1\}$ and $[G : H] = \left|\mathrm{Gal}\left(K/k\right)\right|$ up to conjugacy by elements $(\varphi, 1) \in \Gamma$, and then find all proper solutions (and then the corresponding splitting fields L) to the Galois embedding problems:

$$\begin{tikzcd}
 & & & G_k \arrow[dl, dashed, "\Psi"'] \arrow[d] & \\
1 \arrow[r] & H \arrow[r] & G \arrow[r] & \mathrm{Gal}(K/k) \arrow[r] & 1
\end{tikzcd} \tag{1.6}$$

Every such a solution can be lifted to a solution to the Galois embedding problem (1.3). Notice that the same field L can appear as the splitting field of more than one solution Ψ corresponding to a pair (G, H). This is because given an automorphism α of $\mathrm{Gal}(L/k)$ that leaves $\mathrm{Gal}(K/k)$ fixed, $\alpha\Psi$ is other solution with L as splitting field. Two such solutions are equivalent if and only if there exists $\beta \in \mathrm{Aut}(\mathcal{C})$ such that $\alpha\Psi = \beta\Psi\beta^{-1}$. So, the number of non-equivalent solutions with splitting field L and $\Psi(\mathrm{G}_k) = G$ is the cardinality of the group (see [9]):

$$\mathrm{Aut}_2\left(G\right) / \mathrm{Inn}_G\left(\mathrm{Aut}\left(\mathcal{C}\right) \rtimes \{1\}\right), \tag{1.7}$$

where $\mathrm{Aut}_2\left(G\right)$ is the group of automorphisms of G such that leave the second coordinate invariant and $\mathrm{Inn}\left(\mathrm{Aut}\left(\mathcal{C}\right) \rtimes \{1\}\right)$ is the group of inner automorphisms of $\mathrm{Aut}\left(\mathcal{C}\right) \rtimes \{1\}$ lifted in the natural way to $\mathrm{Aut}\left(G\right)$.

The proper solutions to these Galois embedding problems should be computed case-by-case for each pair (G, H).

Next proposition, that is a generalization of lemma 9.6 for $q = 3$ in [10], will be useful for solving some of the Galois embedding problems that will appear:

Proposition 1.3.2. *Let $q = p^r$, where p is a prime number, let k be a number field, and let ζ be a fixed q-th primitive root of the unity in $\bar{k}$. We denote $K = k(\zeta)$ and we assume $[k(\zeta) : k] = p^{r-1}(p-1)$. Let us define $G_q = \mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/q\mathbb{Z})^*$ where the action of $(\mathbb{Z}/q\mathbb{Z})^*$ on $\mathbb{Z}/q\mathbb{Z}$ is given by the multiplication rule $(a,b)(a',b') = (a + ba', bb')$. And let us consider the Galois embedding problem:*

$$\begin{tikzcd}
 & & & G_k \arrow[d, "\pi"'] & , \\
1 \arrow[r] & \mathbb{Z}/q\mathbb{Z} \arrow[r] & G_q \arrow[r] & (\mathbb{Z}/q\mathbb{Z})^* \arrow[r] & 1
\end{tikzcd}$$

where the horizontal morphisms are the natural ones, and the projection π is given by $\pi(\sigma) = (0,b)$ if $\sigma(\zeta) = \zeta^b$. Then, the splitting fields to the proper solutions to this Galois embedding problem are of the form $L = K(\sqrt[q]{m})$ where $m \in \mathcal{O}_k$ is an integer in k that is not a p-power. Moreover, every such field is the splitting field for a solution Ψ to the above Galois embedding problem.

Proof. Firstly, notice that there exist proper solutions Ψ to the Galois embedding problem. Given a field $L = K(\sqrt[q]{m})$ with m not a p-power, we have an isomorphism $\mathrm{Gal}(L/k) \simeq G_q$ compatible with the projection $G_q \to (\mathbb{Z}/q\mathbb{Z})^*$ and then a solution to the Galois embedding problem above is obtained by the natural projection of $G_k \to \mathrm{Gal}(L/k)$.

Now, let Ψ be any proper solution to the problem, and let us denote by L its splitting field. Let G be the subgroup of G_q that contains all the elements of the form $(0,b)$. And let $\sigma \in G_k$ be such that $\Psi(\sigma) = (1,1)$.

Let α be a primitive element of the extension L^G/k that moreover is an algebraic integer. Then $L = K(\alpha)$ because $[K : k] = p^{r-1}(p-1)$, $[L^G : k] = q$ and $L^G \cap K = k$. Now, define for $i = 0, 1, ..., q-1$ the numbers:

$$u_i = \alpha + \zeta^i \sigma^{-1}(\alpha) + \zeta^{2i}\sigma^{-2}(\alpha) + ... + \zeta^{(q-1)i}\sigma^{-(q-1)}(\alpha).$$

Then $\sigma(u_i) = \zeta^i u_i$ and for any $\tau \in G_k$ such that $\Psi(\tau) = (0,b)$ we have $\Psi(\tau\sigma^j) = (0,b)(j,1) = (bj,1)(0,b) = \Psi(\sigma^{bj}\tau)$, so $\tau(u_i) = u_i$. In particular, $u_0, u_1^q, ..., u_{q-1}^q \in \mathcal{O}_k$. If $u_j \neq 0$ for some $j > 0$, then $L = K(u_j)$, because $L^G = k(u_j)$, then $m = u_j^q$ and $L = K(\sqrt[q]{m})$. If $u_1 = u_2 = ... = u_{q-1} = 0$, then $u_0 = u_0 + u_1 + ... + u_{q-1} = q\alpha \in \mathcal{O}_k$, that is a contradiction with α being a primitive element of the extension L^G/k.

□

Once we have the data (G,H) and a field L, and using the correspondence between (1.1) and (1.2) we obtain immediately the corresponding cocycle $\xi \in \mathrm{H}^1(G_k, \mathrm{Aut}(\mathcal{C}))$. Next step is getting equations for the twits associated to this cocycle. For this purpose we use the method explained in section 1.2.

Remark 1.3.3. *Notice that if all the elements in $\xi(G_k)$ as a matrices in $\mathrm{PGL}_g(K)$ are of the form:*

$$\begin{pmatrix} A_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & A_r \end{pmatrix}, \tag{1.8}$$

with $\sum_{j=1}^r \mathrm{size}(A_j) = g$, then the representation ρ_ξ is reducible and we can take a basis of $\Omega_L^1(C)_\xi^{\mathrm{Gal}(L/k)}$ such that an isomorphism $\phi : C' \to C$ is also of the form (1.8). In particular, if $\xi(G_k)$ is made of diagonal matrices, then we can take a basis of $\Omega_L^1(C)_\xi^{\mathrm{Gal}(L/k)}$ such that ϕ is a diagonal matrix.

1.4 An example

For illustrating the method we will apply it to the non-hyperelliptic genus 6 curve:

$$C : x^7 - y^3z^4 - z^7 = 0.$$

Firstly, we have to find a canonical model by the usual procedure: finding a basis of holomorphic differentials. Let us call $X = x/z$ and $Y = y/z$. One has:

$$\mathrm{div}(X) = (0 : -1 : 1) + (0 : -\zeta_3 : 1) + (0 : -\zeta_3^2 : 1) - 3(0 : 1 : 0) = P_1 + P_2 + P_3 - 3\infty,$$

$$\mathrm{div}(Y) = Q_1 + Q_2 + Q_3 + Q_4 + Q_5 + Q_6 + Q_7 - 7\infty,$$

where $Q_i = (\zeta_7^i : 0 : 1)$. Then, dX is an uniformizer for all points except for the Q_i's, because, exactly these ones are the ones that have tangent space of the form $X - \alpha$ for some $\alpha \in \bar{k}$, $(d(X - \alpha) = dX)$. For these ones we have to work with the expression:

$$dX = -\frac{3y^2}{7x^6}dY$$

So, finally (proposition 4.3, [55]), we get:

$$\mathrm{div}(dX) = 2(Q_1 + Q_2 + Q_3 + Q_4 + Q_5 + Q_6 + Q_7) - 4\infty.$$

And, we compute a basis of holomorphic differentials:

$$\omega_1 = \frac{XdX}{Y},\ \omega_2 = \frac{XdX}{Y^2},\ \omega_3 = \frac{dX}{Y},\ \omega_4 = \frac{dX}{Y^2},\ \omega_5 = \frac{X^2dX}{Y^2},\ \omega_6 = \frac{X^3dX}{Y^2}.$$

Thus, we get a canonical model given by the equations:

$$\mathcal{C} : \omega_1\omega_4 = \omega_2\omega_3,\ \ \omega_4\omega_5 = \omega_2^2,\ \ \omega_4\omega_6 = \omega_2\omega_5,\ \ \omega_3^3\omega_4^4 - \omega_2^7 + \omega_4^7 = 0.$$

The last equation comes of substituting $x = \omega_2/\omega_4$ and $y = \omega_3/\omega_4$ in the original equation. Using the three first equalities, we can exchange the last one by $\omega_3^3 - \omega_5^2\omega_6 + \omega_4^3 = 0$. In fact, by Noether-Enriques-Petri theorem we know that the ideal associated to a canonical curve is generated by quadrics if the curve is not trigonal neither has genus 6 or by quadrics and an element of degree 3 in such cases.

The automorphism group $\mathrm{Aut}(C)$ is generated by the automorphisms, (see Swinarski [58]):

$$(x:y:z) \to (x:\zeta_3 y:z) \text{ and } (x:y:z) \to (\zeta_7 x:y:z).$$

Then, the automorphism group of the canonical model $\mathcal{C}$, is generated by the matrices in $\mathrm{PGL}_6\left(\bar{\mathbb{Q}}\right)$:

$$r = \begin{pmatrix} \zeta_3^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_3^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_3 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_3 & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_3 \end{pmatrix}, \; s = \begin{pmatrix} \zeta_7^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \zeta_7^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \zeta_7 & 0 & 0 & 0 \\ 0 & 0 & 0 & \zeta_7 & 0 & 0 \\ 0 & 0 & 0 & 0 & \zeta_7^3 & 0 \\ 0 & 0 & 0 & 0 & 0 & \zeta_7^4 \end{pmatrix}.$$

Let k be a number field, we consider $\mathcal{C}/k$ and we want to compute its twists over k. Let $K = k(\zeta_7, \zeta_3)$ and assume that $[K:k] = 12$. Then, we get, using MAGMA [6], the following possibilities for the pairs (G, H) as in section 1.3:

	$\mathrm{ID}(G)$	$\mathrm{ID}(H)$	$\mathrm{gen}(H)$
1	$< 12, 5 >$	$< 1, 1 >$	1
2	$< 36, 12 >$	$< 3, 1 >$	r
3	$< 84, 7 >$	$< 7, 1 >$	s
4	$< 252, 26 >$	$< 21, 2 >$	r, s

In the table above the fourth column shows generators of the group H. And in all the cases G is the group generated by the elements $(g, 1)$ for g in H together with the elements $(1, \tau_1)$ and $(1, \tau_2)$ where τ_1 is the element in $\mathrm{Gal}(K/k)$ that sends ζ_3 to ζ_3^2 and ζ_7 to ζ_7, and τ_2 is the one that sends ζ_3 to ζ_3 and ζ_7 to ζ_7^3.

Now, we have to find the proper solutions to the Galois embedding problems associated to each of these pairs:

$$\begin{tikzcd} & & & G_k \arrow[d] \arrow[dl, dashed] & \\ 1 \arrow[r] & H \arrow[r] & G \arrow[r] & \mathrm{Gal}(K/k) \arrow[r] & 1 \end{tikzcd} \tag{1.9}$$

1. The first case is clear: $L = K$.

2. For the second one notice that $L = k(\zeta_7)M$, where M/k is a solution for the Galois embedding problem in proposition (1.3.2) with $q = 3$. Hence, $L = k(\zeta_3,\ \zeta_7,\ \sqrt[3]{m})$, where $m \in \mathcal{O}_k$ is not a 3-power.

3. In this case $L = k(\zeta_3)$, where M/k is a solution for the Galois embedding problem in proposition(1.3.2) with $q = 7$. Hence, $L = k(\zeta_3,\ \zeta_7,\ \sqrt[7]{n})$, where $n \in \mathcal{O}_k$ is not a 7-power.

4. In the last case, $L = M_1M_2$, where M_i/k is a solution for the Galois emebedding problem in proposition(1.3.2) with $q = 3, 7$. Hence, $L = k(\zeta_3,\ \zeta_7,\ \sqrt[3]{m},\ \sqrt[7]{n})$, where $m, n \in \mathcal{O}_k$ and m is not a 3-power and m is not a 7-power.

For each of these fields we have to compute how many different twists are defined over them. For this purpose we use formula (1.7).

1. In the first case $\mathrm{Aut}_2(G) = 1$, then L is the splitting field of only one solution.

2. In the second case $\mathrm{Aut}_2(G) = C_2 \times C_3$ and $\mathrm{Inn}_G(\mathrm{Aut}(\mathcal{C}) \rtimes 1) = C_3$, so the field L is the splitting fields for two different solutions.

3. In the third case $\mathrm{Aut}_2(G) = C_6 \times C_7$ and $\mathrm{Inn}_G(\mathrm{Aut}(\mathcal{C}) \rtimes 1) = C_7$, so the field L is the splitting fields for six different solutions.

4. In the last case, $\mathrm{Aut}_2(G) = C_2 \times C_3 \times C_6 \times C_7$ and $\mathrm{Inn}_G(\mathrm{Aut}(\mathcal{C}) \rtimes 1) = C_3 \times C_7$, so the field L is the splitting fields for twelve different solutions.

We will compute equations for a solution for each splitting field L and then the others will be easily computed using symmetries. Then we fix the action:

$$(r,1): \sqrt[3]{m},\ \sqrt[7]{n} \to \zeta_3\sqrt[3]{m},\ \sqrt[7]{n},$$

$$(s,1): \sqrt[3]{m},\ \sqrt[7]{n} \to \sqrt[3]{m},\ \zeta_7\sqrt[7]{n}.$$

1. Clearly this solution gives us the trivial twist.

2. The correspondence between (1.1) and (1.2) gives us the cocycle given by $\xi_{\tau_1} = 1$, $\xi_{\tau_2} = 1$ and $\xi_{(r,1)} = r$. If we take the basis of $\Omega^1_L(\mathcal{C})$ given by $\{(a,b,c,i)\} := \left\{\sqrt[3]{m^a}\zeta_3^b\zeta_7^c\omega_i\right\}$ where $a, b \in \mathbb{F}_3$, $c \in \mathbb{F}_7$ and $i = 1,2,3,4,5,6$ we obtain the action of $\mathrm{Gal}(L/k)$ on $\Omega^1_L(\mathcal{C})$ given in section 1.2:

$$\begin{aligned}
\tau_1(a,b,c,1) &= (a,2b,c,1),\ \tau_2(a,b,c,1) &&= (a,b,3c,1),\ (r,1)(a,b,c,1) = (a,a+b+2,c,1)\\
\tau_1(a,b,c,2) &= (a,2b,c,2),\ \tau_2(a,b,c,2) &&= (a,b,3c,2),\ (r,1)(a,b,c,2) = (a,a+b+1,c,2)\\
\tau_1(a,b,c,3) &= (a,2b,c,3),\ \tau_2(a,b,c,3) &&= (a,b,3c,3),\ (r,1)(a,b,c,3) = (a,a+b+2,c,3)\\
\tau_1(a,b,c,4) &= (a,2b,c,4),\ \tau_2(a,b,c,4) &&= (a,b,3c,4),\ (r,1)(a,b,c,4) = (a,a+b+1,c,4)\\
\tau_1(a,b,c,5) &= (a,2b,c,5),\ \tau_2(a,b,c,5) &&= (a,b,3c,5),\ (r,1)(a,b,c,5) = (a,a+b+1,c,5)\\
\tau_1(a,b,c,6) &= (a,2b,c,6),\ \tau_2(a,b,c,6) &&= (a,b,3c,6),\ (r,1)(a,b,c,6) = (a,a+b+1,c,6)
\end{aligned}$$

So, we get a basis of $\Omega^1(\mathcal{C}') \simeq \Omega^1_L(\mathcal{C})_\xi^{\mathrm{Gal}(L/k)}$ given by:

$$\left\{\sqrt[3]{m}\omega_1,\ \sqrt[3]{m^2}\omega_2,\ \sqrt[3]{m}\omega_3,\ \sqrt[3]{m^2}\omega_4,\ \sqrt[3]{m^2}\omega_5,\ \sqrt[3]{m^2}\omega_6\right\}.$$

And then, we get the equations of the twist:

$$\omega_1\omega_4 = \omega_2\omega_3,\quad \omega_4\omega_5 = \omega_2^2,\quad \omega_4\omega_6 = \omega_2\omega_5,\quad m\omega_3^3 - \omega_5^2\omega_6 + \omega_4^3 = 0.$$

The equations for the other solution Ψ with splitting field L comes from exchanging m by m^2.

3. The correspondence between (1.1) and (1.2) gives us the cocycle given by $\xi_{\tau_1} = 1$, $\xi_{\tau_2} = 1$ and $\xi_{(s,1)} = s$. If we take the basis of $\Omega^1_L(\mathcal{C})$ given by $\{(a,b,c,i)\} := \left\{\sqrt[7]{n^a}\zeta_3^b\zeta_7^c\omega_i\right\}$ where $a,c \in \mathbb{F}_7$, $b \in \mathbb{F}_3$ and $i = 1,2,3,4,5,6$ we obtain the action of $\mathrm{Gal}(L/k)$ on it given in section 1.2:

$$\begin{aligned}
\tau_1(a,b,c,1) &= (a,2b,c,1),\ \tau_2(a,b,c,1) &&= (a,b,3c,1),\ (s,1)(a,b,c,1) = (a,b,a+c+2,1)\\
\tau_1(a,b,c,2) &= (a,2b,c,2),\ \tau_2(a,b,c,2) &&= (a,b,3c,2),\ (s,1)(a,b,c,2) = (a,b,a+c+2,2)\\
\tau_1(a,b,c,3) &= (a,2b,c,3),\ \tau_2(a,b,c,3) &&= (a,b,3c,3),\ (s,1)(a,b,c,3) = (a,b,a+c+1,3)\\
\tau_1(a,b,c,4) &= (a,2b,c,4),\ \tau_2(a,b,c,4) &&= (a,b,3c,4),\ (s,1)(a,b,c,4) = (a,b,a+c+1,4)\\
\tau_1(a,b,c,5) &= (a,2b,c,5),\ \tau_2(a,b,c,5) &&= (a,b,3c,5),\ (s,1)(a,b,c,5) = (a,b,a+c+3,5)\\
\tau_1(a,b,c,6) &= (a,2b,c,6),\ \tau_2(a,b,c,6) &&= (a,b,3c,6),\ (s,1)(a,b,c,6) = (a,b,a+c+4,6)
\end{aligned}$$

So, we get a basis of $\Omega^1(\mathcal{C}') \simeq \Omega^1_L(\mathcal{C})_\xi^{\mathrm{Gal}(L/k)}$ given by:

$$\left\{\sqrt[7]{n^5}\omega_1,\ \sqrt[7]{n^5}\omega_2,\ \sqrt[7]{n^6}\omega_3,\ \sqrt[7]{n^6}\omega_4,\ \sqrt[7]{n^4}\omega_5,\ \sqrt[7]{n^3}\omega_6\right\}.$$

And then, we get the equations of the twist:

$$\omega_1\omega_4 = \omega_2\omega_3,\quad \omega_4\omega_5 = \omega_2^2,\quad \omega_4\omega_6 = \omega_2\omega_5,\quad \omega_3^3 - n\omega_5^2\omega_6 + \omega_4^3 = 0.$$

The equations for the other solutions Ψ's with splitting field L come from exchanging n by n^2, n^3, n^4, n^5, n^6.

4. In the last case we have the cocycle given by $\xi_\tau = 1$, $\xi_{(r,1)} = r$ and $\xi_{(s,1)} = s$. We take the basis of $\Omega^1_L(\mathcal{C})$ given by $\{(a,b,c,d,i)\} := \left\{\sqrt[3]{m^a}\sqrt[7]{n^b}\zeta_3^c\zeta_7^d\omega_i\right\}$ where $a, c \in \mathbb{F}_3$, $b, d \in \mathbb{F}_7$ and $i = 1,2,3,4,5,6$, and we consider on $\Omega^1_L(\mathcal{C})$ the action of $\mathrm{Gal}(L/k)$ given in section (1.2).

   So, we get a basis of $\Omega^1(\mathcal{C}') \simeq \Omega^1_L(\mathcal{C})_\xi^{\mathrm{Gal}(L/k)}$ given by:

   $$\left\{\sqrt[3]{m}\sqrt[7]{n^5}\omega_1,\ \sqrt[3]{m^2}\sqrt[7]{n^5}\omega_2,\ \sqrt[3]{m}\sqrt[7]{n^6}\omega_3,\ \sqrt[3]{m^2}\sqrt[7]{n^6}\omega_4,\ \sqrt[3]{m^2}\sqrt[7]{n^4}\omega_5,\ \sqrt[3]{m^2}\sqrt[7]{n^3}\omega_6\right\}.$$

   And then, we get the equations of the twist:

   $$\omega_1\omega_4 = \omega_2\omega_3,\ \ \omega_4\omega_5 = \omega_2^2,\ \ \omega_4\omega_6 = \omega_2\omega_5,\ \ m\omega_3^3 - n\omega_5^2\omega_6 + \omega_4^3 = 0.$$

   The equations for the other solutions Ψ's with splitting field L come from exchanging m and n by m, m^2 and n, n^2, n^3, n^4, n^5, n^6.

We can summarize these results as follows: the twists of the curve $\mathcal{C}/k$ are in 1 to 1 correspondence with the curves

$$\omega_1\omega_4 = \omega_2\omega_3,\ \ \omega_4\omega_5 = \omega_2^2,\ \ \omega_4\omega_6 = \omega_2\omega_5,\ \ m\omega_3^3 - n\omega_5^2\omega_6 + \omega_4^3 = 0.$$

where $m \in \mathcal{O}_k$ is free of 3-powers and $n \in \mathcal{O}_k$ is free of 7-powers. Or equivanlently, we can consider the plane models:

$$nx^7 - my^3z^4 - z^7 = 0.$$

Actually, these twists could be computed by hand from the beginning, but we did not know if they were the only ones and if they were equivalent or not.

Chapter 2

Non-hyperelliptic genus 3 curves

In this chapter 2 we prepair the goal of chapter 3, which is to compute the twists of the non-hyperelliptic genus 3 curves defined over a number field k. If the automorphism group of a curve is trivial, then the set of twists is also trivial. Moreover, notice that if $C_2 \in \mathrm{Twist}_k(C_1)$, then $\mathrm{Twist}_k(C_1) = \mathrm{Twist}_k(C_2)$. So, it is enough to compute $\mathrm{Twist}_k(C)$ for C a representative for each class of non-hyperelliptic genus 3 curves defined over k up to $\bar{k}$-isomorphism. Henn's classification, see [31], [59], provides a classification of non-hyperelliptic genus 3 curves over $\mathbb{C}$ with non-trivial automorphisms up to $\mathbb{C}$-isomorphism. There are 12 possibilities for the automorphism group of a non-hyperelliptic genus 3 curve with non-trivial automorphism group. Henn classification shows 12 different families that parametrize all such possibilities.

Unfortunately, the stratifications provided by these families of the coarse moduli space of genus 3 curves, M_3, is not good enough to represent each geometric point of the moduli space over a non algebrically closed field. In other words, the problem is that given a non-hypereliptic genus 3 curve defined over a number field k, its representative in Henn's classification is not necesarly defined also over k. The aim of this chapter is modify the families in Henn's classification for getting this property, that we will call *complete*. Concurrently to the writing of this thesis, R. Lercier, C. Ritzenthaler, F. Rovetta and J. Sijsling have also obtained families with this property [38]. They use a more systematic approach, and they introduce the notion of *representative family*. We also take the notion of "complete" from this reference because is just what we need for the computation of the twists, but in fact, except for the case in which the automorphism group is isomorphic to the cyclic group of order two, what we obtain, as well as them, is representative families for the stratification.

In the last section of this chapter we will explain how to compute, given a non-hyperelliptic genus 3 curve, a representative in the modified Henn classification. And in the next chapter we will compute the twists of each of these representatives.

Since the image of the canonical morphism of a non-hyperelliptic genus 3 curve is a degree $2g-2=4$ curve into $\mathbb{P}^2$, it is a plane quartic curve. And, if the non-hyperelliptic genus 3 curve is defined over k, then we can take a $k-$isomorphic plane quartic curve defined over k as its canonical model by proposition (0.0.2). So, from now on, we will speak about non-singular plane quartic curves instead of smooth non-hyperelliptic genus 3 curves.

2.1 Henn classification

In 1976 Henn gives the next classification up to $\mathbb{C}-$ isomorphism of the non-singular plane quartic curves:

Case	Model	$\mathrm{Aut}\,(C)$	PM
I	$x^4+x^2F\,(y,z)+G\,(y,z)$	C_2	$F\,(y,z)\neq 0,$ not below
II	$x^4+y^4+z^4+ax^2y^2+by^2z^2+cz^2x^2$	V_4	$a\neq\pm b\neq c\neq\pm a$
III	$z^3y+x\,(x-y)\,(x-ay)\,(x-by)$	C_3	not below
IV	$x^3z+y^3z+x^2y^2+axyz^2+bz^4$	S_3	$a\neq b$ and $ab\neq 0$
V	$x^4+y^4+z^4+ax^2y^2+bxyz^2$	D_4	$b\neq 0,\ \pm\frac{2a}{\sqrt{1-a}}$
VI	$z^3y+x^4+ax^2y^2+y^4$	C_6	$a\neq 0$
VII	$x^4+y^4+z^4+ax^2y^2$	$\mathrm{GAP}\,(16,13)$	$\pm a\neq 0,\ 2,\ 6,\ 2\sqrt{-3}$
VIII	$x^4+y^4+z^4+a\,(x^2y^2+y^2z^2+z^2x^2)$	S_4	$a\neq 0,\ \frac{-1\pm\sqrt{-7}}{2}$
IX	$x^4+xy^3+yz^3$	C_9	-
X	$x^4+y^4+xz^3$	$\mathrm{GAP}\,(48,33)$	-
XI	$x^4+y^4+z^4$	$\mathrm{GAP}\,(96,64)$	-
XII	$x^3y+y^3z+z^3x$	$\mathrm{PSL}_2\,(\mathbb{F}_7)$	-

Where PM means parameter restrictions and "not below" means not $\mathbb{C}-$isomorphic to any model below.

In table (5.1) of the Apendix 3, generators of each of these automorphism groups are given. Now, we show an example of a plane quartic curve defined over $\mathbb{Q}$ such that its reprensentative in Henn's classification is not defined over $\mathbb{Q}$: the quartic curve $5x^4+y^4+z^4+x^2y^2=0$ that belongs to the case VII has as representative the curve with parameter $a=1/\sqrt{5}$. Moreover, notice that the representative does not have to be unique, in the former case we can take also $a=-1/\sqrt{5}$.

For getting the modified classification we need to introduce the Weil's restriction principle [62] and the Dixmier-Onho invariants.

Theorem 2.1.1. *(Weil's restriction principle) Let C/F be a curve defined over a number field F which is an extension F/k, then the curve C/F admits a model C' defined over k if and only if for all $\sigma \in \mathrm{Gal}(\tilde{F}/k)$, where $\tilde{F}$ is the Galois clousure of F/k, there exists an isomorphism $\phi_\sigma : {}^\sigma C \to C$ defined over $\tilde{F}$ and such that for all $\tau \in \mathrm{Gal}(\tilde{F}/k)$ one has $\phi_{\sigma\tau} = \phi_\sigma {}^\sigma\phi_\tau$.*

The idea of the proof, that will be useful in the following, is that if there is an isomorphism $\phi : C' \to C$, then we can define $\phi_\sigma = \phi^\sigma \phi^{-1}$ for all $\sigma \in \mathrm{Gal}(\tilde{F}/k)$ and the relation $\phi_{\sigma\tau} = \phi_\sigma {}^\sigma\phi_\tau$ is satisfied for all $\sigma, \tau \in \mathrm{Gal}(\tilde{F}/k)$. Conversely, if we assume that C and C' are canonical curves, given a familly of isomorphisms ϕ_σ such that the relation $\phi_{\sigma\tau} = \phi_\sigma {}^\sigma\phi_\tau$ holds, Hilbert's 90th Problem states that is possible to find an isomorphism $\phi : C' \to C$ such that $\phi_\sigma = \phi^\sigma \phi^{-1}$ for all $\sigma \in \mathrm{Gal}(\tilde{F}/k)$.

Dixmier-Ohno invariants

For elliptic curves the $j-$ invariants allow us to determine when given two elliptic curves they are isomorphic. For genus two curves the Igusa invariants play this role. And for non-hyperelliptic genus three curves we have the absolute Dixmier-Ohno invariants. In [25] there is a survey about the topic.

Theorem 2.1.2. *(Dixmier-Ohno) Two plane quartic curves are isomorphic if and only if they have the same absolute Dixmier-Ohno invariants.*

Remark 2.1.3. *If a plane quartic curve is defined over a number field k, then its absolute invariants of Dixmier-Ohno are also defined over k. But, the converse is not true.*

Girard, Kohel and Ritzenthaler have implemented an algorithm in SAGE for computing the absolute Dixmier-Ohno invariants of a plane quartic curve, even if such curve is given by parameters, [26].

2.2 Modified Henn classification

Since cases IX, X, XI, XII are already defined over $\mathbb{Q}$, we have just to study the cases from I to VIII. Let F be a number field, and let C/F be a plane quartic curve given by its Henn model and such that it belongs to the cases I, III, IV, V, VI or VII. Then its automorphisms group is given by projective matrices (after a suitable permutation of the variables):

$$\begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Assume that C/F is isomorphic to another curve C' defined over a subextension $k \subseteq F$. Then, by Weil restriction Principle, for all $\sigma \in \mathrm{G}_k$ there exists an isomorphism $\phi_\sigma : {}^\sigma C \to C$, that we can see as a projective matrix. Then we have that $\phi_\sigma^{-1} \operatorname{Aut}(C)\phi_\sigma = \operatorname{Aut}({}^\sigma C)$. So, in particular (check the eigenvalues or the elements in the center of $\operatorname{Aut}(C)$):

$$\phi_\sigma^{-1} A \phi_\sigma = B,$$

where:

Case	A	B
I	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
III	$\begin{pmatrix} \zeta_3 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \zeta_3 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
IV	$\begin{pmatrix} \zeta_3 & 0 & 0 \\ 0 & \zeta_3^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} \zeta_3 & 0 & 0 \\ 0 & \zeta_3^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}^\alpha$ where $\alpha = 1, 2$
V	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
VI	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta_3 \end{pmatrix}$	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \zeta_3 \end{pmatrix}$
VII	$\begin{pmatrix} i & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} i & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & 1 \end{pmatrix}^\alpha$ where $\alpha = 1, 3$

A case by case computation shows that:

$$\phi_\sigma = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

And, in the case VI, moreover we deduce that ϕ_σ has to be a diagonal matrix.

Case I

Here, $C : z^4 + F(x,y)z^2 + G(x,y) = 0$ is defined over F and we assume that there is a model C' of C defined over a subextension F/k. Since we know that for all $\sigma \in \mathrm{G}_k$:

$$\phi_\sigma = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

we can take the ϕ in the idea of the proof of the Weil's restriction principle also in the form, see remark (1.3.3):

$$\phi = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

And then, $C' : z^4 + F'(x,y)z^2 + G'(x,y) = 0$, so the family for this strata in the Henn classification was alredy complete.

Case II

After a suitable change of coordinates we can work with the model $C : ax^4 + by^4 + cz^4 + x^2y^2 + y^2z^2 + z^2x^2 = 0$. Let $\sigma \in \mathrm{Gal}(\tilde{F}/k)$ be such that the conjugation by ϕ_σ on $\mathrm{Aut}(C)$ leaves a non trivial automorphism fixed. Then we can assume that:

$$\phi_\sigma = \begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{pmatrix} : {}^\sigma C \to C.$$

Then, it is easy to check that ${}^\sigma c = c$ and ${}^\sigma a = a$ and ${}^\sigma b = b$ or ${}^\sigma a = b$ and ${}^\sigma b = a$. If ϕ_σ only leaves fixed the trivial automorphism, then it is easy to check again that we can assume:

$$\phi_\sigma = \begin{pmatrix} 0 & \alpha & 0 \\ 0 & 0 & \beta \\ \gamma & 0 & 0 \end{pmatrix}.$$

And then $\alpha^2 = 1/\beta^2 = \gamma^2 = 1/\alpha^2$. So, ${}^{\sigma}a = c$, ${}^{\sigma}b = a$ and ${}^{\sigma}c = b$. Hence, in any case a, b, c are the roots of a degree 3 polynomial with coefficients in k. And then we can consider the model:

$$C' : (x + ay + a^2z)^4 + (x + by + b^2z)^4 + (x + cy + c^2z)^4 + (x + ay + a^2z)^2(x + by + b^2z)^2 +$$

$$+(x + by + b^2z)^2(x + cy + c^2z)^2 + (x + cy + c^2z)^2(x + ay + a^2z)^2 = 0 \qquad (2.1)$$

given by the isomorphism:

$$\phi = \begin{pmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{pmatrix} : C' \to C.$$

Case III

We have $C : z^3y + x(x - y)(x - a)(x - b) = 0$, and we can take the ϕ in the idea of the proof of the Weil's restriction principle of the form:

$$\phi = \begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

And then we get the equation $z^3(\gamma x + \delta y) + Q(x, y) = 0$ where $Q(x, y)$ is an homogenous degree 4 polynomial in x and y. Since that equation is defined over k, then $\delta/\gamma \in k$. Hence, we can do the change of variables $x' = x$ and $y' = \gamma x + \delta y$ and then we get the $k-$rational model $C' : z^3y + P(x, y) = 0$.

Case IV

We start with the variation of the Henn's model $C : z^4 + axyz^2 + b(x^3 + y^3)z + x^2y^2 = 0$. In this case again:

$$\phi_\sigma = \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then, we can take:

$$\phi = \begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

And then, if we get an equation of C' from the equation of C and the isomorphism ϕ, we conclude:

$$(\alpha x + \beta y)^2(\gamma x + \delta y)^2 = x^2y^2.$$

So, after maybe permuting the variables x and y we can assume $\beta = \gamma = 0$ and then $\delta = \pm 1/\alpha$ and ${}^{\sigma}a = \pm a$. If we look at the coefficient of degree 1 in z of the equation of C', we conclude $\alpha^3 = i^{\epsilon}$, where $\epsilon = 0, 1, 2$ or 3. And then ${}^{\sigma}b = i^{\epsilon}b$. Hence, there exist $k-$rational numbers m, q such that $b = \sqrt[4]{m}$ and $a = q\sqrt{m}$. After dividing z by $\sqrt[4]{m}$ we obtain the rational model:

$$C' : z^4/m + qxyz^2 + (x^3 + y^3)z + x^2y^2 = 0.$$

So the family for this strata in the Henn classification was alredy complete.

Case V

In that case $C : x^4 + y^4 + z^4 + ax^2y^2 + bxyz^2$. Let

$$\phi_{\sigma} = \begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then, $x^4 + y^4 + z^4 + {}^{\sigma}ax^2y^2 + {}^{\sigma}bxyz^2 = (\alpha x + \beta y)^4 + (\gamma x + \delta y)^4 + z^4 + a(\alpha x + \beta y)^2(\gamma x + \delta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y)z^2$. If we look at the coefficient of xyz^2 in the left hand side: ${}^{\sigma}bxyz^2 = b(\alpha x + \beta y)(\gamma x + \delta y)z^2$, and then, after maybe permuting the variables x, y we can assume $\beta = \gamma = 0$. So, $\alpha^4 = \delta^4 = 1$ and then ${}^{\sigma}a = \pm a$ and ${}^{\sigma}b = i^{\epsilon}b$, where $\epsilon = 0, 1, 2$ or 3. Hence, there exist $k-$rational numbers m, q such that: $b = \sqrt[4]{m}$ and $a = q\sqrt{m}$. We find the $k-$rational model: $C' : 1/mx^4 + y^4 + z^4 + qx^2y^2 + xyz^2 = 0$ and the isomorphism:

$$\phi = \begin{pmatrix} \sqrt[4]{m^3} & 0 & 0 \\ 0 & m & 0 \\ 0 & 0 & m \end{pmatrix} : C' \to C.$$

Case VI

We have the plane quartic $C : z^3y + x^4 + ax^2y^2 + y^4 = 0$, and since the automorphism group in this case is made up of diagonal matrices, we can take

$$\phi_{\sigma} = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \beta \end{pmatrix}.$$

Then $\alpha^4 = 1$ and ${}^{\sigma}a = \pm a$. So, there exists a $k-$rational number m such that $a = \sqrt{m}$. And after dividing x by $\sqrt[4]{m}$ we obtain the $k-$rational model:

$$C' : z^3y + 1/mx^4 + x^2y^2 + y^4 = 0.$$

Actually, in that case, it was also easy to get this condition just looking at the Dixmier-Ohno invariants of this model, see table (5.3).

Caso VII

In this case we have $C : x^4 + y^4 + z^4 + ax^2y^2$. Let again

$$\phi_\sigma = \begin{pmatrix} \alpha & \beta & 0 \\ \gamma & \delta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

be an isomorphism $\phi_\sigma : {}^\sigma C \to C$. Then,

$$\alpha^4 + \gamma^4 + a\alpha^2\gamma^2 = 1$$

$$4\alpha^3\beta + 4\gamma^3\delta + a(2\alpha^2\gamma\delta + 2\alpha\beta\gamma^2) = 0$$

$$6\alpha^2\beta^2 + 6\gamma^2\delta^{+}a(\alpha^2\delta^2 + \beta^2\gamma^2 + 4\alpha\beta\gamma\delta) = {}^\sigma a$$

$$4\alpha\beta^3 + 4\gamma\delta^3 + a(2\beta^2\gamma\delta + 2\alpha\beta\delta^2) = 0$$

$$\beta^4 + \delta^4 + a\beta^2\delta^2 = 1$$

If we subtract $\beta\delta$ times the second equation to $\alpha\gamma$ times the fourth one, we get $\gamma\delta = \pm\alpha\beta$. If we plug this condition into the second equation we get $\alpha\beta = 0$ or $\alpha^2 = \pm\gamma^2$. The second condition gives to us $k-$rational values of a, while the first one gives ${}^\sigma a = \pm a$. Then, $C : x^4 + y^4 + z^4 + \sqrt{m}x^2y^2 = 0$ for some $m \in k$. And we find the $k-$rational model: $C' : x^4/m + y^4 + z^4 + x^2y^2 = 0$ via the isomorphism:

$$\phi = \begin{pmatrix} 1/\sqrt[4]{m} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : C' \to C.$$

Case VIII

In this case the previous arguments do not work. We will use here the Dixmier-Ohno invariants that are computed in table (5.4). If $C : x^4 + y^4 + z^4 + a(x^2y^2 + y^2z^2 + z^2x^2) = 0$ is isomorphic to curve defined over k then its Dixmier-Ohno invariants are also defined over k. We will prove that in this case, necersarly we have $a \in k$. We have the following relations:

$$q := \frac{\mathrm{I}_9}{\mathrm{I}_{12}} = \frac{(a+3)(a+18)}{a^2 - 9a - 6} \in k,$$

$$q' := \frac{\mathrm{I}_{18}}{\mathrm{I}_{12}} \frac{\mathrm{I}_{15}}{\mathrm{I}_{27}} = \frac{5a^2 + 12a + 36}{(a+3)^2} \in k.$$

If $a \in k$ we are done, then lets us assume that $a \notin k$ and then it is in a quadratic extension of k. Hence, the two equations above should be one a multiple of the other, both give the minimal polynomial of a over k. We get $q = \frac{1}{2}$ or $-\frac{5}{2}$, and then 4 possible values of a. If we plug these values in the other invariants we do not get $k-$rational numbers. Then $a \in k$ and the family for this strata in the Henn classification is alredy complete.

We summarize all the previous results in next table. In table (5.2), generators of each of these automorphism groups are given.

Case	Model	Aut (C)	PM
I	$x^4 + x^2F(y,z) + G(y,z)$	C_2	$F(y,z) \neq 0$, not below
II	see 2.1	V_4	$a \neq b \neq c \neq a$
III	$z^3y + P(x,y)$	C_3	not below
IV	$x^3z + y^3z + x^2y^2 + axyz^2 + bz^4$	S_3	$a \neq b$ and $ab \neq 0$
V	$ax^4 + y^4 + z^4 + bx^2y^2 + xyz^2$	D_4	$b \neq 0$, $a \neq 4b^2(2b+1)^2$
VI	$z^3y + ax^4 + x^2y^2 + y^4$	C_6	-
VII	$ax^4 + y^4 + z^4 + x^2y^2$	GAP $(16,13)$	$\pm a \neq 1/4,\ 1/36,\ 1/-12$
VIII	$x^4 + y^4 + z^4 + a(x^2y^2 + y^2z^2 + z^2x^2)$	S_4	$a \neq 0,\ \frac{-1\pm\sqrt{-7}}{2}$
IX	$x^4 + xy^3 + yz^3$	C_9	-
X	$x^4 + y^4 + xz^3$	GAP $(48,33)$	-
XI	$x^4 + y^4 + z^4$	GAP $(96,64)$	-
XII	$x^3y + y^3z + z^3x$	$\mathrm{PSL}_2(\mathbb{F}_7)$	-

Table 2.2: Modified Henn classification

2.3 A representative in the modified Henn classification

Let C/k be a plane quartic curve. Assume that the automorphism group $\mathrm{Aut}(C)$ is non-trivial and known, and given by proyective matrices. We will show how to find a Henn model C_H of C, that is a representative of this curve in the Henn classification, and an isomorphism from C to it. Then the modified Henn model is easily computed from the discussion in last section. We will deal with each case separately, but the idea is the same one in all of them. Let $\varphi : C \to C_H$ be an isomorphism from the curve C to its Henn model, then $\mathrm{Aut}(C_H) = \varphi\,\mathrm{Aut}(C)\varphi^{-1}$. So, the idea will be find a projective matrix φ such that the last equality holds.

Case I

In that case there is only one non-trivial automorphism $\alpha \in \mathrm{Aut}(C)$. The automorphism α is similar to the matrix:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Find the eigenvector v_1 of the projective matrix α corresponding to the eigenvalue that is different from the other two and two eigenvectors v_2 and v_3 corresponding to these two equal eigenvalues, then

$$\varphi^{-1} = (v_1 \mid \lambda_1 v_2 + \lambda_2 v_3 \mid \lambda_3 v_2 + \lambda_4 v_3).$$

Get the equation of C_H via this φ and the equation of C and adjust the scalars λ_1, λ_2, λ_3 and λ_4 for getting C_H defined over k.

Case II

Each of the 3 non-trivial automorphisms in $\mathrm{Aut}(C)$ diagonalize simultaneously into:

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Let v_i for $i = 1, 2, 3$ the eigenvector corresponding to the eigenvalue -1 for each automorphism. Then

$$\varphi^{-1} = (v_1 \mid \lambda_1 v_2 \mid \lambda_2 v_3).$$

Now, get the equation of C_H via this φ and the equation of C; and adjust the scalars λ_1 and λ_2 for getting C_H defined over k.

Example 2.3.1. *Let be*

$$C : 3x^4 + 10x^2y^2 + 5x^2z^2 - 2xyz^2 + 3y^4 + 5y^2z^2 + z^4 = 0,$$

the automorphism group $\mathrm{Aut}(C)$ *is generated by the matrices:*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

For the first one we obtain the eigenvector with eigenvalue -1*:* $(0:0:1)$*, the other two eigenvalues are equal to* 1*. For the second one we obtain* $(1:-1:0)$ *with eigenvalue equal to* -1*, the other two eigenvalues are equal to* 1*. The other non-trivial automorphism is*

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

and we find $(1:1:0)$ *with eigenvalue equal to* 1*, the other two eigenvalues are equal to* -1*. Then the isomorphism* $\varphi^{-1} : C_H \to C$ *is given by:*

$$\varphi^{-1} = \begin{pmatrix} \lambda_1 & \lambda_2 & 0 \\ -\lambda_1 & \lambda_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We subtitute in the equation of C *for getting an equation of* C_H*:*

$$C_H : 16\lambda_1^4x^4 + 16\lambda_2^4y^4 + z^4 + 16\lambda_1^2\lambda_2^2x^2y^2 + 8\lambda_2^2y^2z^2 + 12\lambda_1^2z^2x^2 = 0.$$

Then $\lambda_1^2 = \frac{\pm1}{4} = \lambda_2^2$*, and hence,* $a = 1, b = 2$ *and* $c = 3$ *(in case II of Henn classification multiplying a parameter by* -1 *gives us the same quartic curve up to isomorphism). Finally,*

$$C_H : x^4 + y^4 + z^4 + x^2y^2 + 2y^2z^2 + 3z^2x^2 = 0.$$

Case III

In that case we proceed as in the case I but considering the automorphism:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi_3 \end{pmatrix}.$$

Cases from IV to VII and from IX to XII

Find a matrix in $\mathrm{Aut}(C)$ such that is similar to M (see the table above). Next, find the eigenvectors corresponding to the different eigenvalues: v_1, v_2, v_3. Then

$$\varphi^{-1} = (v_1 \mid \lambda_1 v_2 \mid \lambda_2 v_3).$$

Finally, get the equation of C_H via this φ^{-1} and the equation of C and adjust the scalars λ_1 and λ_2 for getting C_H defined over k.

Case	M
IV	$\begin{pmatrix} \xi_3 & 0 & 0 \\ 0 & \xi_3^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
V	$\begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{pmatrix}$
VI	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi_3 \end{pmatrix}$
VII	$\begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{pmatrix}$
IX	$\begin{pmatrix} \xi_3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi_9 \end{pmatrix}$
X	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & \xi_3 \end{pmatrix}$
XI	$\begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{pmatrix}$
XII	$\begin{pmatrix} \xi_7^4 & 0 & 0 \\ 0 & \xi_7^2 & 0 \\ 0 & 0 & \xi_7 \end{pmatrix}$

Case VIII

We proceed as in the case II with the subgroup of $\mathrm{Aut}(C)$ generated by the matrices:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Finally, given a plane quartic curve C/F such that $\mathrm{Aut}(C)$ is known, we can find its Henn model C_H/k with $k \subseteq F$ the minimal field over which a curve isomorphic to C is defined. And we will be able of computing its twists looking at the results that we obtain in chapter 3, that is, the computation of the twists of the quartic curves in the modified Henn classification.

In general is not easy at all to compute the automorphism group of a curve. This is why we assume that it is known. However, in the case of plane quartic curves, we can compute the automorphism group studying the Weiertrass points. Any automorphism of a plane quartic curve permutes the Weiertrass points. Once we have computed the Weiertrass points, that is the inflection points, we have to check which matrices that permute them are or not automorphisms of the curve. See [46] for an example of this idea for computing the automorphism of the Klein quartic.

Chapter 3

Twists of non-hyperelliptic genus 3 curves

In this chapter we compute the twists of each representative in the families of the modified Henn classification over a number field k. There are some cases in which all the machinery developed in chapter 1 is not needed. Firstly, we will deal with the case of the twists of the Fermat quartic, a difficult case for which we need all the tools in chapter 1. Then, we will compute the twists of cases from I to X. For the cases II, V, VII and VIII we will use the knowledge about the twists of the Fermat quartic. The other cases will be done just inspeccioning the form of the equations using remark (1.3.3) and we will use remark (1.3.1) for checking when they are equivalent. Finally, case XII, the case of the Klein quartic, the more difficult one, will be done using again the machinery in chapter 1. This case becomes so hard because the Galois embedding problems that appear are difficult to solve.

3.1 The Fermat quartic

We consider the Fermat quartic $C_F : x^4 + y^4 + z^4 = 0$ defined over a number field k. The automorphism group $\mathrm{Aut}(C_F)$ is isomorphic to $< 96, 64 >$ in GAP notation [24], and as subgroup of $\mathrm{PGL}_3\left(\bar{k}\right)$ it is generated by the matrices:

$$s = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad u = \begin{pmatrix} i & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Let us firstly suppose that $i \notin k$, then $K = k(i)$, $\mathrm{Gal}(K/k) \simeq \mathbb{Z}/2\mathbb{Z}$ and $\Gamma = \mathrm{Aut}(C_F) \rtimes \mathrm{Gal}(K/k) \simeq < 192, 956 >$. Then, it is easily checked with MAGMA [6], see the code in table (5.5) in the appendix, that the possible pairs (G, H) in (1.3) are the ones given in the tables below. We have divided these pairs into three types: diagonal, almost diagonal and non-diagonal. The diagonal type corresponds to the cases in which all the elements in $G \subseteq \mathrm{Aut}(C_F) \rtimes \mathrm{Gal}(K/k)$ have a diagonal matrix as first component. The second type will be called almost-diagonal and it corresponds to the cases where G is a 2-group not included in the diagonal cases of the former type. Finally, the third type will cover the pairs (G, H) of the remaining cases.

In the tables below the fourth and fifth columns serve to reconstruct G and H. The fourth column contains a list of generators of H, and the fifth column contains a single matrix h. The meaning is that G is the group which elements are $(g, 1)$ for g in H together with the elements (gh, τ) for g in H and τ the non-trivial automorphism in $\mathrm{Gal}(K/k)$. As an easy way to remember, we can write the non-sense expression $G = H \rtimes 1 + Hh \rtimes \tau$.

Type I: Diagonal twists

	ID(G)	ID(H)	gen(H)	h
1	$<2,1>$	$<1,1>$	1	1
2	$<2,1>$	$<1,1>$	1	t^3utu
3	$<4,2>$	$<2,1>$	t^2	1
4	$<4,2>$	$<2,1>$	t^2	u
5	$<4,2>$	$<2,1>$	t^2	t^3utu
6	$<8,5>$	$<4,2>$	t^2, u^2	1
7	$<8,5>$	$<4,2>$	t^2, u^2	u
8	$<8,3>$	$<4,1>$	t^3utu	1
9	$<8,3>$	$<4,1>$	t^3utu	u
10	$<8,3>$	$<4,1>$	t^3utu^3	1
11	$<8,3>$	$<4,1>$	t^3utu^3	u
12	$<16,11>$	$<8,2>$	t^3utu, u^2	1
13	$<16,11>$	$<8,2>$	t^3utu, u^2	u
14	$<32,34>$	$<16,2>$	u, t^3ut	1

Type II: Almost-diagonal twists

	ID(G)	ID(H)	gen(H)	h
1	$<2,1>$	$<1,1>$	1	u^2t
2	$<4,2>$	$<2,1>$	t^2	u^2t
3	$<4,1>$	$<2,1>$	t^2	t
4	$<4,2>$	$<2,1>$	u^2t	1
5	$<4,2>$	$<2,1>$	u^2t	t^3utu
6	$<8,4>$	$<4,1>$	t^3utu	t
7	$<8,1>$	$<4,1>$	t^3utu^3	tu

8	$<8,3>$	$<4,2>$	t^2, u^2	u^2t
9	$<8,2>$	$<4,1>$	t	1
10	$<8,5>$	$<4,2>$	u^2t, t^2	1
11	$<8,2>$	$<4,1>$	t^3utu^3	u^2t
12	$<8,3>$	$<4,1>$	t^3utu	u^2t
13	$<8,5>$	$<4,2>$	u^2t, t^2	t^3utu
14	$<8,3>$	$<4,1>$	t	t^3utu^3
15	$<8,2>$	$<4,1>$	t	t^3utu
16	$<8,3>$	$<4,2>$	u^2t, t^2	u^2
17	$<8,3>$	$<4,2>$	u^2t, t^2	t^3utu^3
18	$<8,3>$	$<4,1>$	t	u^2
19	$<16,6>$	$<8,2>$	t^3utu, u^2	ut
20	$<16,13>$	$<8,2>$	t^3utu, u^2	u^2t
21	$<16,8>$	$<8,1>$	u^2tu	u
22	$<16,7>$	$<8,3>$	t^3utu^3, u^2t	u
23	$<16,8>$	$<8,4>$	t^3utu^3, t	u
24	$<16,11>$	$<8,3>$	t, u^2	1
25	$<16,13>$	$<8,4>$	t^3utu^3, t	1
26	$<16,13>$	$<8,2>$	t, utu	1
27	$<16,11>$	$<8,2>$	t, utu	u^2
28	$<16,11>$	$<8,3>$	t, u^2	utu
29	$<16,7>$	$<8,1>$	tu^2tut	$tutu^2$
30	$<16,11>$	$<8,3>$	t^3utu^3, u^2t	1
31	$<32,43>$	$<16,6>$	tu^2tut, u^2	u
32	$<32,11>$	$<16,2>$	u, t^3ut	u^2t
33	$<32,43>$	$<16,13>$	t^3utu, u^2, t	u
34	$<32,7>$	$<16,6>$	tu^2tut, u^2	1
35	$<32,49>$	$<16,13>$	utu, u^2, t	1
36	$<64,134>$	$<32,11>$	t, u	1

Type III: Non-diagonal twists

	ID(G)	ID(H)	gen(H)	h
1	$<6,1>$	$<3,1>$	s	u^2t
2	$<6,2>$	$<3,1>$	s	1
3	$<12,4>$	$<6,1>$	s, u^2t	1
4	$<24,12>$	$<12,3>$	s, u^2	u^2t
5	$<24,13>$	$<12,3>$	s, u^2	1
6	$<48,48>$	$<24,12>$	s, t	1
7	$<96,64>$	$<48,3>$	s, u, t^3ut	u^2t
8	$<96,72>$	$<48,3>$	s, u, t^3ut	1
9	$<192,956>$	$<96,64>$	s, t, u	1

Galois embedding problems

Proposition 3.1.1 (Diagonal twists)**.** *The embedding problems corresponding to the fourteen pairs* (G,H) *of diagonal type have a solution. The corresponding splitting fields are* $L = k(i, \sqrt[4]{a}, \sqrt[4]{b})$*, where* a, $b \in k^*$*. The different cases are:*

Type I: Diagonal twists

	ID(G)	ID(H)	a, b mod k^{*4}
1	$<2,1>$	$<1,1>$	$a = b = 1$
2	$<2,1>$	$<1,1>$	$a = b = -4$
3	$<4,2>$	$<2,1>$	$a = b \in k^{*2}$
4	$<4,2>$	$<2,1>$	$a = -4b \in k^{*2}$
5	$<4,2>$	$<2,1>$	$a = b \in -4k^{*2}$
6	$<8,5>$	$<4,2>$	$a,\ b,\ ab \in k^{*2}$
7	$<8,5>$	$<4,2>$	$-4a,\ b,\ -4ab \in k^{*2}$
8	$<8,3>$	$<4,1>$	$a = b \notin k^{*2}$
9	$<8,3>$	$<4,1>$	$a = -4b \notin k^{*2}$
10	$<8,3>$	$<4,1>$	$a = b^3 \notin k^{*2}$
11	$<8,3>$	$<4,1>$	$a = -4b^3 \notin k^{*2}$
12	$<16,11>$	$<8,2>$	$a \notin k^2, ab^3 \in k^{*2}$
13	$<16,11>$	$<8,2>$	$a \notin k^2, -4ab^3 \in k^{*2}$
14	$<32,34>$	$<16,2>$	$a,\ b,\ ab^3 \notin k^{*2}$

Proof. Let us consider any of these pairs and assume first that there is a proper solution Ψ to the Galois embedding problem (1.6). As it was observed in section 1.1, the existence of Ψ implies the existence of a one-cocycle ξ such that $\xi(\sigma) = \phi \cdot {}^{\sigma}\phi^{-1}$ for $\sigma \in \mathrm{Gal}(L/k)$, where L is the splitting field of the twist of C attached to ϕ. From the assumption that $\xi(\sigma)$ are diagonal matrices for all $\sigma \in \mathrm{Gal}(L/k)$, it follows that the ξ-twisted action on $\Omega^1_L(C_F)$ is diagonal and, hence, the corresponding twist of C_F admits a canonical embedding into the projective space $\mathbf{P}^2$ whose image is a plane quartic given by $ax^4+by^4+z^4=0$, see remark (1.3.3). Then we conclude the existence of solutions taking $L=k(i,\sqrt[4]{a},\sqrt[4]{b})$ and analyzing case by case the proper solutions that give rise to the different fourteen cases. □

Remark 3.1.2. *Two of these twists, $ax^4+by^4+z^4=0$ and $a'x^4+b'y^4+z^4=0$ are equivalent if and only if there exists $m\in k$ such that the sets $\{a,b,1\}$ and $\{ma',mb',m\}$ are congruent modulo k^{*4}.*

Proposition 3.1.3 (Almost-diagonal twists)**.** *The following table gives the obstruction to the thirty six cases in which (G,H) is of type II. Whenever it is solvable, the corresponding splitting field is $L=k(i,\sqrt{m},\sqrt[4]{a+b\sqrt{m}},\sqrt[4]{a-b\sqrt{m}})$, where a, b, $m\in k^*$. The different cases are:*

Type II: Almost diagonal twists

	ID(G)	ID(H)	m mod k^{*2}	n_1	n_2	*Obstruction*
1	$<2,1>$	$<1,1>$	-1	1	1	
2	$<4,2>$	$<2,1>$	-1	2	1	$a+bi=(c+di)^2,\ c^2+b^2=n^2$
3	$<4,1>$	$<2,1>$	-1	2	1	$a+bi=(c+di)^2, c^2+b^2=-n^2$
4	$<4,2>$	$<2,1>$	$\neq 0,-1$	1	1	$a+b\sqrt{m}=(c+d\sqrt{m})^4$
5	$<4,2>$	$<2,1>$	$\neq 0,-1$	1	1	$a+b\sqrt{m}=-4(c+d\sqrt{m})^4$
6	$<8,4>$	$<4,1>$	-1	4	1	$a=0,\ \sqrt{2}\in k$
7	$<8,1>$	$<4,1>$	-1	4	1	$a^2+b^2=-4n^4$
8	$<8,3>$	$<4,2>$	-1	2	2	$a+bi=(c+di)^2$
9	$<8,2>$	$<4,1>$	$\neq 0,-1$	2	1	$a+b\sqrt{m}=(c+d\sqrt{m})^2, c^2-d^2m=mn^2$
10	$<8,5>$	$<4,2>$	$\neq 0,-1$	2	1	$a+b\sqrt{m}=(c+d\sqrt{m})^2, c^2-d^2m=n^2$
11	$<8,2>$	$<4,1>$	-1	4	1	$a^2+b^2=n^4$
12	$<8,3>$	$<4,1>$	-1	4	1	$b=0$
13	$<8,5>$	$<4,2>$	$\neq 0,-1$	2	1	$a+b\sqrt{m}=-(c+d\sqrt{m})^2, c^2-d^2m=n^2$
14	$<8,3>$	$<4,1>$	$\neq 0,-1$	2	1	$a+b\sqrt{m}=-(c+d\sqrt{m})^2, c^2-d^2m=-mn^2$
15	$<8,2>$	$<4,1>$	$\neq 0,-1$	2	1	$a+b\sqrt{m}=-(c+d\sqrt{m})^2, c^2-d^2m=mn^2$
16	$<8,3>$	$<4,2>$	$\neq 0,-1$	2	1	$a+b\sqrt{m}=(c+d\sqrt{m})^2, c^2-d^2m=-n^2$
17	$<8,3>$	$<4,2>$	$\neq 0,-1$	2	1	$a+b\sqrt{m}=-(c+d\sqrt{m})^2, c^2-d^2m=-n^2$
18	$<8,3>$	$<4,1>$	$\neq 0,-1$	2	1	$a+b\sqrt{m}=(c+d\sqrt{m})^2, c^2-d^2m=-mn^2$
19	$<16,6>$	$<8,2>$	-1	4	2	$a^2+b^2=-n^2$
20	$<16,13>$	$<8,2>$	-1	4	2	$a^2+b^2=n^2$
21	$<16,8>$	$<8,1>$	$\neq 0,-1$	4	1	$a=0$ and $m=2$ or $\sqrt{2}\in k$
22	$<16,7>$	$<8,3>$	$\neq 0,-1$	4	1	$a^2-b^2m=-4n^4$

23	$<16,8>$	$<8,4>$	$\neq 0,-1$	4	1	$a^2-b^2m=-4m^2n^4$
24	$<16,11>$	$<8,3>$	$\neq 0,-1$	2	2	$a+b\sqrt{m}=(c+d\sqrt{m})^2$
25	$<16,13>$	$<8,4>$	$\neq 0,-1$	4	1	$a^2-b^2m=m^2n^4$
26	$<16,13>$	$<8,2>$	$\neq 0,-1$	4	1	$a^2-b^2m=l^2, l=-2q^2(a-l)$
27	$<16,11>$	$<8,2>$	$\neq 0,-1$	4	1	$a^2-b^2m=l^2, l=2q^2(a-l)$
28	$<16,11>$	$<8,3>$	$\neq 0,-1$	2	2	$a+b\sqrt{m}=-(c+d\sqrt{m})^2$
29	$<16,7>$	$<8,1>$	$\neq 0,-1$	4	1	$a=0$ and $m=-2$ or $\sqrt{2}\in k$
30	$<16,11>$	$<8,3>$	$\neq 0,-1$	4	1	$a^2-b^2m=n^4$
31	$<32,43>$	$<16,6>$	$\neq 0,-1$	4	2	$a^2-b^2m=-mn^2$
32	$<32,11>$	$<16,2>$	-1	4	4	
33	$<32,43>$	$<16,13>$	$\neq 0,-1$	4	2	$a^2-b^2m=-n^2$
34	$<32,7>$	$<16,6>$	$\neq 0,-1$	4	2	$a^2-b^2m=mn^2$
35	$<32,49>$	$<16,13>$	$\neq 0,-1$	4	2	$a^2-b^2m=n^2$
36	$<64,134>$	$<32,11>$	$\neq 0,-1$	4	4	

here $m,n\in k^*/k^{*2}$ and the degrees $n_1=[M:k(i,\sqrt{m})]$ and $n_2=[L:M]$ are given in terms of the intermediate field $M=k(i,\sqrt{m},\sqrt[4]{a+b\sqrt{m}})$.

Proof. Let us consider any of these pairs (G,H) and assume first that there is a solution Ψ associated to it. Again, the existence of Ψ implies the existence of a one-cocycle ξ such that $\xi(\sigma)=\phi\cdot{}^{\sigma}\phi^{-1}$ for $\sigma\in\mathrm{Gal}(L/k)$, where L is the splitting field of the twist of C_F attached to ϕ. The type II assumption implies that, up to conjugation in $\mathrm{Aut}(C_F)$, the first components of the elements of G are of the form

$$\xi(\sigma)=\begin{pmatrix} * & * & 0\\ * & * & 0\\ 0 & 0 & 1\end{pmatrix}$$

for all $\sigma\in\mathrm{Gal}(L/k)$, and taking into account the ξ-action on $\Omega^1_L(C_F)$ it also implies that we can take

$$\phi=\begin{pmatrix} \alpha & \alpha\beta & 0\\ \gamma & \gamma\delta & 0\\ 0 & 0 & 1\end{pmatrix}$$

where α, β, δ, $\gamma\in L$ and $\alpha\gamma\neq 0$. Hence, the corresponding twist C'_F of C_F admits a canonical embedding into the projective space $\mathbf{P}^2$ whose image is a plane quartic given by

$$\alpha^4(x+\beta y)^4+\gamma^4(x+\delta y)^4+z^4=0\,.$$

Since C'_F is defined over k, this imposes several conditions on α, β, δ, γ. For instance, β and δ should be conjugate over an extension $k(\sqrt{m})$ for certain $m \in k^*$. Also α^4 and γ^4 should be conjugate over the same extension. By remark (1.3.1) we can (and do) take $\beta = -\delta = \sqrt{m}$ and $\alpha = \sqrt[4]{a + b\sqrt{m}}$, $\gamma = \sqrt[4]{a - b\sqrt{m}}$ with a, $b \in k$. Now, a case-by-case analysis yields the tables above matching the different subcases with the different pairs (G, H). □

Remark 3.1.4. *Two of these twists are equivalents if and only if their splitting fields have the same quadratic subextension $k(\sqrt{m})/k$ and the columns of the matrix associated to one isomorphism $\phi : C'_F \to C_F$ are $k-$rational linear combination of the columns of the matrix associated to the other isomorphism $\phi' : C''_F \to C_F$, see remark (1.3.1). That is, if there exist $c, d \in k$ such that*

$$(a + b\sqrt{m}) = (c + d\sqrt{m})^4(a' \pm b'\sqrt{m}).$$

Proposition 3.1.5 (Non-diagonal twists)**.** *The embedding problems corresponding to the nine pairs (G, H) of type III have a solution. The corresponding splitting fields are $L = k(i, \sqrt[n]{a}, \sqrt[n]{b}, \sqrt[n]{c})$, where a, b, c are the three roots of a degree three irreducible polynomial with coefficients in k with $\sqrt[n]{abc} \in k$. The different cases are:*

Type III: Non-diagonal twists				
	ID(G)	ID(H)	$\triangle$ *mod* k^{*2}	n
1	$< 6, 1 >$	$< 3, 1 >$	-1	1
2	$< 6, 2 >$	$< 3, 1 >$	1	1
3	$< 12, 4 >$	$< 6, 1 >$	$\neq \pm 1$	1
4	$< 24, 12 >$	$< 12, 3 >$	-1	2
5	$< 24, 13 >$	$< 12, 3 >$	1	2
6	$< 48, 48 >$	$< 24, 12 >$	$\neq \pm 1$	2
7	$< 96, 64 >$	$< 48, 3 >$	-1	4
8	$< 96, 72 >$	$< 48, 3 >$	1	4
9	$< 192, 956 >$	$< 96, 64 >$	$\neq \pm 1$	4

Here, $\triangle$ denotes the absolute discriminant of the extension $k(a, b, c)/k$.

Proof. The solutions associated to the first three pairs are well-known, see for example [23]. For the sixth pair, since Gal(L/K) is isomorphic to S_4 and Gal(L/k) is isomorphic to $S_4 \times \mathbb{Z}_2$, we conclude that $L = k_f(i)$ where k_f is the splitting field of an irreducible monic degree 4 polynomial $f(x) = x^4 + a_2x^2 + a_1x + a_0 \in k[x]$, such that the splitting field of its cubic resolvent $g(x) = x^3 + 2a_2x^2 + (a_2^2 - 4a_0)x - a_1^2$ has Galois group isomorphic to S_3. Let r_0, r_1, r_2 and r_3 be the four roots of f, and let us define

$$s_1 = \frac{1}{2}(r_0 - r_1 + r_2 - r_3)$$

$$s_2 = \frac{1}{2}(r_0 + r_1 - r_2 - r_3)$$

$$s_3 = \frac{1}{2}(r_0 - r_1 - r_2 + r_3).$$

Then the roots of $g(x) = 0$ are s_1^2, s_2^2 and s_3^2 and $g(x^2) = (x^2 - s_1^2)(x^2 - s_2^2)(x^2 - s_3^2)$ is also irreducible over k and $L = k(s_1, s_2, s_3)$. Letting $a = s_1^2$, $b = s_2^2$ and $c = s_3^2$ we get $L = k(\sqrt{a}, \sqrt{b}, \sqrt{c})$ and $\sqrt{abc} \in k$. Similar arguments yield the solutions for the pairs 4 and 5.

For the ninth pair one considers the Galois extension M over k given by the normal subgroup $\langle u \rtimes 1, t^3ut \rtimes 1, 1 \rtimes \tau \rangle$. It has Galois group isomorphic to S_3 and its quadratic subextension is different from $k(i)$. Consider now the Galois extension M_1 over M given by the subgroup $\langle u \rtimes 1 \rangle$. Then $\mathrm{Gal}(M_1/M(i)) \simeq \mathbb{Z}_4$ and $\mathrm{Gal}(M_1/M) \simeq D_4$. Hence, applying lemma (1.3.2), $M_1 = M(i, \sqrt[4]{\alpha})$ with $\alpha \in M$. Since $M_1/k(\alpha)$ is a normal extension we conclude $\mathrm{Gal}(k(\alpha)/k) \simeq \mathbb{Z}_3$. Idem with M_2 given by the subgroup $\langle t^3ut \rtimes 1 \rangle$, we get $M_2 = M(i, \sqrt[4]{\beta})$ with $\beta \in M$ and $\mathrm{Gal}(k(\beta)/k) \simeq \mathbb{Z}_3$. Also $k(\alpha) \neq k(\beta)$. Since the subgroups that give M_1 and M_2 have intersection equal to the identity, we have $L = M_1 M_2$. Finally, since L/k is a normal extension and there is no other normal extension over $k(\beta)$ having Galois group isomorphic to $D_4 \times \mathbb{Z}_2$, we can take β to be a conjugate of α. Let γ be the third conjugated. If we inspect the action of $\mathrm{Gal}(L/k)$ on $\sqrt[4]{\alpha\beta\gamma}$ we obtain $\sqrt[4]{\alpha\beta\gamma} \in k$, and then the result follows. The pairs 7 and 8 follow using the same arguments. □

Remark 3.1.6. *In the first six cases two of these twists are equivalents if and only if they have the same splitting field. In the cases seventh and ninth, the same field L provides two different twists, because in that case, see formula (1.7):*

$$\mathrm{Aut}_H(G) / Inn_G(\mathrm{Aut}(C_F) \rtimes \{1\}) = 2.$$

And in the eighth one each field L provides four different twists.

Plane quartic equations

Once we know the cocycles and the splitting fields of the twists we can compute equations for them. Fix a basis $(\omega_1, \omega_2, \omega_3)$ of $\Omega_k^1(C_F)$ and we proceed as in section 1.2 using the isomorphism (1.4):

$$\Omega_k^1(C_F') \simeq (\Omega_L^1(C_F))_\xi^{\mathrm{Gal}(L/k)}.$$

Theorem 3.1.7 (Diagonal twists)**.** *A diagonal twist with parameters $a, b \in k$ and splitting field $L = k(i, \sqrt[4]{a}, \sqrt[4]{b})$, is defined by the equation:*

$$ax^4 + by^4 + z^4 = 0.$$

Theorem 3.1.8 (Almost diagonal twists)**.** *An almost diagonal twist with parameters a,b,m and splitting field $L = k(i,\sqrt[4]{a+b\sqrt{m}},\sqrt[4]{a-b\sqrt{m}},\sqrt{m})$, is defined by the equation:*

$$2ax^4 + 8bmx^3y + 12max^2y^2 + 8bm^2xy^3 + 2am^2y^4 + z^4 = 0.$$

Theorem 3.1.9 (Non-diagonal twists)**.** *A non-diagonal twist with parameters a,b,c,n and splitting field $L = k(i,\sqrt[n]{a},\sqrt[n]{b},\sqrt[n]{c})$, is defined by the equation:*

$$\sum_{\substack{j+k+l=4\\ j,k,l\geq 0}} \binom{4}{j}\binom{4-j}{k} S_{2(n-1)+k+2l}x^jy^kz^l = 0$$

if $n=1$ or $n=2$, where $S_j = a^j + b^j + c^j$. If $n=4$ this splitting field produces more than one twist, that are given by the equation:

$$\sum_{\substack{j+k+l=4\\ j,k,l\geq 0}} \binom{4}{j}\binom{4-j}{k} S_{1+k+2l}x^jy^kz^l = 0,$$

where for the seventh and ninth cases we have also the twist coming from replacing a,b,c with a^3,b^3,c^3 and for the eighth also the ones coming from replacing a,b,c with $a/b,b/c,c/a$ and a‘$3/b^3,b^3/c^3,c^3/a^3$.

Proof. For $n=1$ we can take the isomorphism $\phi\colon C_F' \to C_F$:

$$\phi = \begin{pmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{pmatrix},$$

and we get the equation in the statement of the theorem. For $n=2$ we take:

$$\phi = \begin{pmatrix} \sqrt{a} & a\sqrt{a} & a^2\sqrt{a} \\ \sqrt{b} & b\sqrt{b} & b^2\sqrt{b} \\ \sqrt{c} & c\sqrt{c} & c^2\sqrt{c} \end{pmatrix}.$$

And for $n=4$ we consider the isomorphism:

$$\phi = \begin{pmatrix} \sqrt[4]{a} & a\sqrt[4]{a} & a^2\sqrt[4]{a} \\ \sqrt[4]{b} & b\sqrt[4]{b} & b^2\sqrt[4]{b} \\ \sqrt[4]{c} & c\sqrt[4]{c} & c^2\sqrt[4]{c} \end{pmatrix},$$

and the ones coming from replacing a,b,c with the numbers in the statement of the theorem. The equivalence of twists is a consequence of remark (3.1.6). □

Remark 3.1.10. *If i belongs to the number field k we define $k_0 = k \cap \mathbb{R}$, then $[k : k_0] = 2$ and $i \notin k_0$. We obtain for k the pairs (H, H) where (G, H) is pair for k_0. And any proper solution to the Galois embedding problem (1.6) for the pair (H, H) is given by $\Psi\mid_{G_k}$ where Ψ is a proper solution for the Galois embedding problem (1.6) associated to a pair (G, H) of k_0. Then we obtain once again the statements of theorems (3.1.7), (3.1.8) and (3.1.9).*

We can summarize all these results in next theorem.

Theorem 3.1.11. *The set of k-isomorphism classes of non-hyperelliptic genus 3 curves with automorphism group isomorphic to $\langle 96, 64\rangle$ is parametrized by the set $Pol_3^4(k)/\sim$ where $Pol_3^4(k)$ is the set of degree 3 separable polynomials with coefficients in k and whose independent coefficient belongs to $-1 \cdot k^{*4}$, and where the equivalence is given by: $P(T) \sim P'(T)$ if and only if they have the same splitting field M and*

$$\{a, b, c\} \equiv \{a', b', c'\}\, mod\, M^{*4}$$

where a, b, c are the roots of $P(T)$ and a', b', c' the roots of $P'(T)$. A representative plane quartic corresponding to $P(T) = T^3 - AT^2 + BT - C^4$ is given by:

$$\sum_{\substack{i+j+k=4\\ i,j,k\geq 0}} \binom{4}{i}\binom{4-i}{j} S_{1+j+2k} x^i y^j z^k = 0$$

where $S_j = a^j + b^j + c^j$.

Proof. The only non-hyperelliptic genus 3 curve up to $\mathbb{C}$–isomorphism with automorphism group isomorphic to $\langle 96, 64\rangle$ is the Fermat quartic, see section 2.1. Then we only have to parametrize its twists. Then, it is clear that given such a polynomial $P(T) \in Pol_3^4(k)$ with roots a, b, c we can attach to it the twist given by the isomorphism:

$$\phi = \begin{pmatrix} \sqrt[4]{a} & a\sqrt[4]{a} & a^2\sqrt[4]{a} \\ \sqrt[4]{b} & b\sqrt[4]{b} & b^2\sqrt[4]{b} \\ \sqrt[4]{c} & c\sqrt[4]{c} & c^2\sqrt[4]{c} \end{pmatrix}$$

that gives the equation in the stament of the theorem.

Now, let us prove that any of the twists of the Fermat quartic can be written in such a way. For the non-diagonal twists is clear. For the diagonal twists given by an isomorphism of the form:

$$\phi = \begin{pmatrix} \sqrt[4]{a} & 0 & 0 \\ 0 & \sqrt[4]{b} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

we can suppose that $1 \neq a \neq b \neq 1$ after right multiplication by a suitable rational matrix and then we can take the equivalent twist given by the isomorphism:

$$\phi = \begin{pmatrix} \sqrt[4]{qa} & qa\sqrt[4]{qa} & q^2a^2\sqrt[4]{qa} \\ \sqrt[4]{qb} & qb\sqrt[4]{qb} & q^2b^2\sqrt[4]{qb} \\ \sqrt[4]{q} & q\sqrt[4]{q} & q^2\sqrt[4]{q} \end{pmatrix}$$

where $q = ab$. For an almost-diagonal twist:

$$\phi = \begin{pmatrix} \sqrt[4]{c} & \sqrt{m}\sqrt[4]{c} & 0 \\ \sqrt[4]{\bar{c}} & -\sqrt{m}\sqrt[4]{\bar{c}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where $c = a + b\sqrt{m}$ and $\bar{c} = a - b\sqrt{m}$, we can assume $b \neq 0$ after rigth multiplication, if necessary, by the rational matrix:

$$\begin{pmatrix} 1 & m & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and then we can take the equivalent twist:

$$\phi = \begin{pmatrix} \sqrt[4]{qc} & qc\sqrt[4]{qc} & q^2c^2\sqrt[4]{qc} \\ \sqrt[4]{q\bar{c}} & q\bar{c}\sqrt[4]{q\bar{c}} & q^2\bar{c}^2\sqrt[4]{q\bar{c}} \\ \sqrt[4]{q} & q\sqrt[4]{q} & q^2\sqrt[4]{q} \end{pmatrix}$$

where $q = a^2 - b^2m$, that has the form in the statement of the theorem.

Finally, the equivalence of the different twists is a consequence of remarks (3.1.2), (3.1.4) and (3.1.6). □

Remark 3.1.12. *In [7] it is showed that every form of a Fermat equation has to have this shape, even if it is not given the explicit form of the field of definition L.*

3.2 Cases from I to X

Case I

In this case we have $\Gamma \simeq \mathrm{Gal}(L/k) \simeq \mathrm{C}_2$, then all the non-trivial twists are quadratics ones and there is only one twist for each quadratic extension of k. So, for each free square $m \in k$, we have the twist:

$$m^2x^4 + mx^2F(y,z) + G(y,z) = 0.$$

Case II

Let us consider a curve in the modified Henn classification for the case II defined over a number field k:

$$C_{A,B,C} : A(x + Ay + A^2z)^4 + B(x + By + B^2z)^4 + C(x + Cy + C^2z)^4 +$$

$$(x+Ay+A^2z)^2(x+By+B^2z)^2+(x+By+B^2z)^2(x+Cy+C^2z)^2+(x+Cy+C^2z)^2(x+Ay+A^2z)^2 = 0,$$

where A, B, C are the three roots of a degree 3 polynomial with coefficients in k. There is a natural inclusion of the automorphism group of $C_{A,B,C}$ into the automorphism group of the twist C'_F of the Fermat curve given by the isomorphism

$$\varphi = \begin{pmatrix} 1 & A & A^2 \\ 1 & B & B^2 \\ 1 & C & C^2 \end{pmatrix} : C'_F \to C_F.$$

Then, we have a natural inclusion of $\mathrm{Z}^1(\mathrm{G}_k, \mathrm{Aut}(C_{A,B,C}))$ in $\mathrm{Z}^1(\mathrm{G}_k, \mathrm{Aut}(C'_F))$. We know all the twists of the curve C'_F: they are given by the isomorphisms $\varphi^{-1} \circ \phi$, where $\phi : C' \to C_F$ is a twist of the Fermat quartic from section 3.1. Then, we have just to check what of this twists are also twists of $C_{A,B,C}$. Moreover, notice that the matrix φ^{-1} defines also an isomorphism $\varphi^{-1} : C_H \to C_{A,B,C}$ where $C_H : Ax^4 + By^4 + Cz^4 + x^2y^2 + y^2z^2 + z^2x^2 = 0$. So we have just to check what twists of the Fermat quartic define also twists defined over k for the quartic curve C_H.

Diagonal twists. Let us assume that

$$\phi = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

gives a twists of $C_{A,B,C}$ defined over k. Then $m = \alpha^2, n = \beta^2 \in k$ and $A, B, C \in k$. And we obtain the twists:

$$Am^2x^4 + Bn^2y^4 + Cz^4 + mnx^2y^2 + ny^2z^2 + mz^2x^2 = 0$$

where $m, n \in k$ are square-free.

Almost-diagonal twists. In this case we have

$$\phi = \begin{pmatrix} \sqrt[4]{a + b\sqrt{m}} & \sqrt{m}\sqrt[4]{a + b\sqrt{m}} & 0 \\ \sqrt[4]{a - b\sqrt{m}} & -\sqrt{m}\sqrt[4]{a - b\sqrt{m}} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

And we obtain the conditions(up to permutation of A, B, C): $C \in k$ and $A, B \in k(\sqrt{m})$ are conjugate numbers, and $a + b\sqrt{m} = (c + d\sqrt{m})^2$.

Non-diagonal twists. In this case we have

$$\phi = \begin{pmatrix} \sqrt[n]{a} & a\sqrt[n]{a} & a^2\sqrt[n]{a} \\ \sqrt[n]{b} & b\sqrt[n]{b} & b^2\sqrt[n]{b} \\ \sqrt[n]{c} & c\sqrt[n]{c} & c^2\sqrt[n]{c} \end{pmatrix}.$$

And we get the conditions $n = 1, 2$ and $\mathrm{Gal}(k(A, B, C)/k) \simeq C_3$ or S_3, and $a \in k(A)$, $b \in k(B)$ and $c \in k(C)$.

The equivalence for these twists is the same one that for the twists of the Fermat quartic.

Case III

In this case $\Gamma = \mathrm{Aut}(C) \rtimes \mathrm{Gal}(K/k) \simeq C_3$ or S_3 depending on $\xi_3 \in k$ or not. In both cases, applying Kummer theory or lemma (1.3.2), we get $L = K(\sqrt[3]{m})$ for some $m \in k$. Then all the twists of a quartic curve $C : z^3y + P(x, y) = 0$ in case III are in one to one correspondence with elements $m \in k^*/k^{*3}$ and are given by the equations:

$$C' : mz^3y + P(x, y) = 0$$

Case IV

Since the automorphism group in this case is made from matrices of the form

$$\begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

we can take

$$\phi = \begin{pmatrix} \alpha & \alpha\beta & 0 \\ \gamma & \gamma\delta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Then, $\alpha\gamma(x^2 + (\beta + \delta)xy + \beta\delta y^2) \in k[x, y]$, and so $\alpha\gamma \in k$ and $\beta\delta$, $\beta + \delta \in k$. Hence there are two cases: or β, $\delta \in k$ or β and δ are conjugate over a quadratic extension of k. In the first case and up to k−isomorphism, we can assume

$$\phi = \begin{pmatrix} s & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

And in the second case:

$$\phi = \begin{pmatrix} \alpha & \alpha\sqrt{m} & 0 \\ \gamma & -\gamma\sqrt{m} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Hence, the twists are given by the equations:

$$nx^3z + q^3n^2y^3z + q^2n^2x^2y^2 + aqnxyz^2 + bz^4 = 0,$$

where we get $s^3 = n \in k$ and $st = qm \in k$. And

$$2\alpha_1(x^3z + 3mxy^2z) + 2\alpha_2 m(3x^2yz + my^3z) + q^2(x^2 - my^2)^2 + aq(x^2 - my^2)z^2 + bz^4 = 0,$$

where $\alpha = \alpha_1 + \alpha_2\sqrt{m}$, $\gamma = \alpha_1 - \alpha_2\sqrt{m}$ with $\alpha_1, \alpha_2, m \in k$ and satisfying the condition $\alpha_1^2 - m\alpha_2^2 = q^3$, where $q \in k$.

Case V

The automorphism group of the curve $C_{A,B}: Ax^4 + y^4 + z^4 + Bx^2y^2 + xyz^2 = 0$ is contained in a natural way in the one of the Fermat twist $C'_F: Ax^4 + y^4 + z^4 = 0$. We know all the twists of C'_F:

$$\begin{pmatrix} 1/\sqrt[4]{A} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \circ \phi$$

where ϕ is a twist of the Fermat curve described in the section 3.1. And $\mathrm{Z}^1(\mathrm{G}_k, \mathrm{Aut}(C_{A,B}))$ is a subset of $\mathrm{Z}^1(\mathrm{G}_k, \mathrm{Aut}(C'_F))$. So we have just to check what twists of C'_F can be also seen as twists of $C_{A,B}$. Clearly, any of the non-diagonal twists can be.

Diagonal twists. The diagonal twists are:

$$amx^4 + q^4m^3y^4 + z^4 + q^2m^2Bx^2y^2 + qmxyz^2 = 0,$$

where m and q are free of fourth powers in k.

Almost-diagonal twists. The almost-diagonal twists are given by taking:

$$\phi = \begin{pmatrix} \sqrt[4]{a + b\sqrt{m}} & \sqrt{m}\sqrt[4]{a + b\sqrt{m}} & 0 \\ \sqrt[4]{a - b\sqrt{m}} & -\sqrt{m}\sqrt[4]{a - b\sqrt{m}} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Where there exists a k–rational number q such that $a^2 - b^2m = q^4A$. Two of these twists are equivalent if and only if their splitting fields have the same quadratic subextension $k(\sqrt{m})/k$ and if

$$a + b\sqrt{m} = (c + d\sqrt{m})^4(a' \pm b'\sqrt{m}),$$

for some $c, d \in k$.

Case VI

Since in this case the automorphism group is made of diagonal matrices, we know that all the twists are given by matrices, see remark (1.3.3):

$$\phi = \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & b \end{pmatrix}.$$

Then $C' : b^3z^3y + Aa^4x^4 + a^2x^2y^2 + y^4 = 0$. Hence a^2, $b^3 \in k$. So, $a = \sqrt{m}$ and $b = \sqrt[3]{n}$ for some m, $n \in k$. Then, $C' : nz^3y + Am^2x^4 + mx^2y^2 + y^4 = 0$. If we take m square-free and n free of third powers, then two different twists are not equivalent, see remark (1.3.1).

Case VII

The automorphism group of the curve $C_A : Ax^4 + y^4 + z^4 + x^2y^2 = 0$ is contained in a natural way in the one of the Fermat twist $C'_F : Ax^4 + y^4 + z^4 = 0$. We know all the twists of C'_F:

$$\begin{pmatrix} 1/\sqrt[4]{A} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \circ \phi$$

where ϕ is a twist of the Fermat curve described in the section 3.1. And $\mathrm{Z}^1(\mathrm{G}_k, \mathrm{Aut}(C_A))$ is a subset of $\mathrm{Z}^1(\mathrm{G}_k, \mathrm{Aut}(C'_F))$. So we have just to check which twists of C'_F can also be seen as twists of C_A. Clearly, any of the non-diagonal twists can be.

Diagonal twists. The diagonal twists are:

$$amx^4 + q^2my^4 + z^4 + qmx^2y^2 = 0,$$

where m is free of fourth powers and q is free square in k.

Almost-diagonal twists. The almost-diagonal twists are given by taking:

$$\phi = \begin{pmatrix} \sqrt[4]{a + b\sqrt{m}} & \sqrt{m}\sqrt[4]{a + b\sqrt{m}} & 0 \\ \sqrt[4]{a - b\sqrt{m}} & -\sqrt{m}\sqrt[4]{a - b\sqrt{m}} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Where there exists a $k-$rational number q such that $a^2 - b^2m = q^2A$. Two of these twists are equivalent if and only if they have the same quadratic subextension $k(\sqrt{m})/k$ and if

$$a + b\sqrt{m} = (c + d\sqrt{m})^4(a' \pm b'\sqrt{m}),$$

for some $c, d \in k$.

Caso VIII

The Henn model for this case is $C_A : x^4+y^4+z^4+A(x^2y^2+y^2z^2+z^2x^2)=0$. And since for $A=0$ we recover the Fermat quartic C_F, we can see in a natural way the automorphism group of C_A into the automorphism group of C_F. Then, as in case II, we get a natural inclusion of $\mathrm{Z}^1(\mathrm{G}_k,\mathrm{Aut}(C_A))$ into $\mathrm{Z}^1(\mathrm{G}_k,\mathrm{Aut}(C_F))$. In that way we see each twist of C_A as a twists of the Fermat quartic. We will just have to check which twists of the Fermat quartic give also twists of C_A defined over k.

Diagonal twists. The diagonal twists are:

$$a^2x^4+b^2y^4+z^4+A(abx^2y^2+by^2z^2+az^2x^2)=0$$

where a, $b\in k$ are square-free. And two of these twists are equivalente if and only if, there exists $m\in k$ such that the sets $\{a,b,1)\}$ and $\{ma',mb',m)\}$ are congruent modulo k^{*4}.

Almost-diagonal twists. The almost-diagonal twists are given by isomorphisms $\phi: C'\to C$ defined by:

$$\phi=\begin{pmatrix}\sqrt{a+b\sqrt{m}} & \sqrt{m}\sqrt{a+b\sqrt{m}} & 0\\ \sqrt{a-b\sqrt{m}} & -\sqrt{m}\sqrt{a-b\sqrt{m}} & 0\\ 0 & 0 & 1\end{pmatrix}.$$

Two of these twists are equivalent if and only if their splitting fields have the same quadratic subextension $k(\sqrt{m})/k$ and if

$$a+b\sqrt{m}=(c+d\sqrt{m})^4(a'\pm b'\sqrt{m}),$$

for some $c,d\in k$.

Non-diagonal twists. The non-diagonal twists are the ones for the Fermat quartic with $n=1$, 2.

Case IX

In that case, since the automorphism group is made of diagonal matrices, given a twist $\phi: C'\to C$, we can assume that ϕ is given by a diagonal matrix:

$$\phi=\begin{pmatrix}a&0&0\\0&1&0\\0&0&b\end{pmatrix}.$$

Then $C' : a^4x^4+axy^3+b^3yz^3=0$. Hence a^3, $b^3/a\in k$. So, $a=\sqrt[3]{m}$ and $b=\sqrt[3]{q\sqrt[3]{m}}$ for some m, $q\in k$. Then, $C' : mx^4+xy^3+qyz^3=0$. If we take m and q free of third powers, then two different twists are not equivalent.

Case X

In this case we have only one curve $C : x^4 + y^4 + xz^3 = 0$. And looking at its automorphism group we conclude that the twists are given by isomorphisms of the form:

$$\phi = \begin{pmatrix} a & 0 & ab \\ 0 & 1 & 0 \\ c & 0 & cd \end{pmatrix}.$$

And then we get:

$$\begin{aligned} a^4 + ac^3 = A + B &= q_1 \in k \\ 4Ab + B(b + 3d) &= q_2 \in k \\ 6Ab^2 + B(3d^2 + 3bd) &= q_3 \in k \\ 4Ab^3 + B(d^3 + 3bd^2) &= q_4 \in k \\ Ab^4 + Bbd^3 &= q_5 \in k \end{aligned}$$

We can assume $q_1 \neq 0$ and then $q_2 = 0$. Hence $B = q_1 - A$. Then from the second equation we get $A = -\frac{q_1(b+3d)}{3(b-d)}$ (notice that $b \neq d$) and then $B = \frac{4q_1 b}{3(b-d)}$. Substituting in the other equations we get:

$$\begin{aligned} b(2d + b) &= -\frac{q_3}{2q_1}, \\ b(b^2 + 4bd + d^2) &= -\frac{3q_4}{4q_1}, \\ b^2(2d + b)^2 &= -\frac{3q_5}{q_1} \end{aligned}$$

So, in particular, $q_3^2 = -12q_1q_5$, and $d = \frac{b^2 + \frac{q_3}{2q_1}}{2b}$ and:

$$q_1 b^4 + q_3 b^2 - q_4 b - \frac{q_3^2}{12q_1} = 0.$$

So, given q_1, q_3, $q_4 \in k$ we have the twist:

$$C' : q_1 x^4 + q_3 x^2 z^2 + q_4 x z^3 - \frac{q_3^2}{12q_1} z^4 + y^4 = 0.$$

And two such twist are equivalent if and only if $q_i' = q^4 q_i$ for some $q \in k$ for $i = 1, 3, 4$ as can be checked using remark (1.3.1).

3.3 The Klein quartic

In this section we will compute the twists of the Klein quartic:

$$C_K : x^3 y + y^3 z + z^3 x = 0,$$

defined over a number field k. Let us consider the twist:

$$C: x^4+y^4+z^4+6(xy^3+yz^3+zx^3)-3(x^2y^2+y^2z^2+z^2x^2)+3xyz(x+y+z)=0,$$

given by the isomorphism:

$$\phi_0=\begin{pmatrix} 1 & 1+\zeta\alpha & \zeta^2+\zeta^6 \\ 1+\zeta\alpha & \zeta^2+\zeta^6 & 1 \\ \zeta^2+\zeta^6 & 1 & 1+\zeta\alpha \end{pmatrix}\circ\begin{pmatrix} -\alpha & 1 & 2\alpha+3 \\ 2\alpha+3 & -\alpha & 1 \\ 1 & 2\alpha+3 & -\alpha \end{pmatrix}: C\to C_K.$$

Here $\alpha=\frac{-1+\sqrt{-7}}{2}$ and $\zeta=\zeta_7$. We have $\mathrm{Twist}_k(C_K)=\mathrm{Twist}_k(C)$, and C has the advantage that its automorphism group $\mathrm{Aut}(C)$ is defined over $k(\sqrt{-7})$ instead of over $k(\zeta_7)$. So, we will compute $\mathrm{Twist}_k(C)$. We will use the method described in chapter 1. The group $\mathrm{Aut}(C)$ is generated by the projective matrices:

$$g=\frac{1}{\sqrt{-7}}\begin{pmatrix} -2 & \alpha & -1 \\ \alpha & -1 & 1-\alpha \\ -1 & 1-\alpha & -1-\alpha \end{pmatrix},\ h=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},\ s=\frac{1}{7}\begin{pmatrix} -3 & -6 & 2 \\ -6 & 2 & -3 \\ 2 & -3 & -6 \end{pmatrix}$$

Let us first assume that $\sqrt{-7}\notin k$, and let $K=k(\sqrt{-7})$. Then, the possibilities for the pairs (G,H) are:

	ID(G)	ID(H)	gen(H)	h
1	$<2,1>$	$<1,1>$	1	1
2	$<4,2>$	$<2,1>$	s	1
3	$<6,1>$	$<3,1>$	h	s
4	$<6,2>$	$<3,1>$	h	1
5	$<14,1>$	$<7,1>$	g	1
6	$<8,1>$	$<4,1>$	$g^2sg^3sg^2$	g^2sg^5
7	$<8,3>$	$<4,1>$	$g^2sg^3sg^2$	1
8	$<12,4>$	$<6,1>$	h, s	1
9	$<42,1>$	$<21,1>$	g, h	1
10	$<16,7>$	$<8,3>$	$g^2sg^3sg^2$, g^2sg^5	1
11	$<336,208>$	$<168,42>$	s, g, h	1

Where the meaning is that G is the group which elements are $(g,1)$ for g in H together with the elements (gh,τ) for g in H and τ the non-trivial automorphism in $\mathrm{Gal}(K/k)$. As an easy way to remember, we can write the non-sense expression $G=H\rtimes 1+Hh\rtimes\tau$.

The case ID(G) =< 2, 1 >

In that case $L = K = k(\sqrt{-7})$ and there only a single twist, the trivial twist.

The case ID(G) =< 4, 2 >

In that case $L = K(\sqrt{m}) = k(\sqrt{-7}, \sqrt{m})$, where $m \notin k^2$ or $-7k^2$. So, for each quadratic extension L/K we obtain a single twist with equation:

$$-49x^4 - m^2y^4 + 31m^2z^4 + 210mx^2yz - 12m^2y^3z - 66m^2yz^3 - 63mx^2y^2 + 51m^2y^2z^2 - 126mx^2z^2 = 0,$$

and given by the isomorphism:

$$\phi = \begin{pmatrix} 2 & \sqrt{m} & 0 \\ -3 & 0 & \sqrt{m} \\ 1 & -2\sqrt{m} & 3\sqrt{m} \end{pmatrix}.$$

The case ID(G) =< 6, 1 >

In that case $L = k(a, b, c)$, where a, b, c are the three roots of degree 3 polynomial with coefficents in k and such that its splitting field over k has Galois group isomorphic to S_3 and whose discriminant is $-7q^2$ for some $q \in k$. Two twists are equivalent if and only if they have the same splitting field by formula (1.7). They are given by the isomorphism:

$$\phi = \begin{pmatrix} \sqrt{-7} & -3a + 2b + c & ab - 3bc + 2ca \\ \sqrt{-7} & a - 3b + 2c & 2ab + bc - 3ca \\ \sqrt{-7} & 2a + b - 3c & -3ab + 2bc + ca \end{pmatrix}.$$

The equation is the one for the case ID(G) =< 12, 4 > with $\Delta = -7$.

The case ID(G) =< 6, 2 >

In that case $L = K(a, b, c)$, where a, b, c are the three roots of degree 3 polynomial with coefficients in k and such that its splitting field has Galois group isomorphic to C_3. Two twists are equivalent if and only if they have the same splitting field by formula (1.7). They are given by the isomorphism:

$$\phi = \begin{pmatrix} 1 & -3a + 2b + c & ab - 3bc + 2ca \\ 1 & a - 3b + 2c & 2ab + bc - 3ca \\ 1 & 2a + b - 3c & -3ab + 2bc + ca \end{pmatrix}.$$

The equation is the one for the case ID(G) =< 12, 4 > with $\Delta = 1$. In this case, we recover the the Klein quartic taking $a = \zeta + \zeta^6$, $b = \zeta^2 + \zeta^5$ and $c = \zeta^4 + \zeta^3$.

The case $\mathrm{ID}(G) =< 14, 1 >$

Let us consider the field $\tilde{L} = L(\zeta_7)$. Then $\left[\tilde{L} : L\right] = 3$ and $\tilde{L} = k(\zeta_7, \sqrt[7]{\alpha})$ where $\alpha \in k(\zeta_7)$ by Kummer theory and since $\mathrm{Gal}(\tilde{L}/k) \simeq < 42, 4 >$ then $\alpha \notin K$. We will prove that we can assume $\alpha \in k(\zeta_7 + \zeta_7^6)$. Let $\tau \in \mathrm{Gal}(\tilde{L}/k)$ of order 6, then $\sqrt[7]{\alpha} + \tau^3(\sqrt[7]{\alpha})$ is only fixed by τ^3 but $(\sqrt[7]{\alpha} + \tau^3(\sqrt[7]{\alpha}))^7$ is also fixed by any of the order seven elements (let us call σ one of them), so if we call $\beta = (\sqrt[7]{\alpha} + \tau^3(\sqrt[7]{\alpha}))^7$, we have $\tilde{L} = k(\zeta_7, \sqrt[7]{\beta})$ and $\beta \in k(\zeta_7 + \zeta_7^6)$. And L is the only normal subextension of index 3. Let us call $\beta_1 = \beta$ and β_2 and β_3 its two conjugates in $\tilde{L}$. Then $\sqrt[7]{\beta_1\beta_2\beta_3} \in k$. And then it is easy to check that the action of τ and σ is given by:

$$\sigma(\sqrt[7]{\beta_1}) = \zeta_7 \sqrt[7]{\beta_1},\ \ \sigma(\sqrt[7]{\beta_2}) = \zeta_7^4 \sqrt[7]{\beta_2},\ \ \sigma(\sqrt[7]{\beta_3}) = \zeta_7^2 \sqrt[7]{\beta_3}.$$

$$\tau(\sqrt[7]{\beta_1}) = \sqrt[7]{\beta_2},\ \ \tau(\sqrt[7]{\beta_2}) = \sqrt[7]{\beta_3},\ \ \tau(\sqrt[7]{\beta_3}) = \sqrt[7]{\beta_1}.$$

Then we obtain the twist with equation:

$$\sqrt[7]{\beta_1^3\beta_2}(x + \beta_1 y + \beta_1^2 z)^3(x + \beta_2 y + \beta_2^2 z) + \sqrt[7]{\beta_2^3\beta_3}(x + \beta_2 y + \beta_2^2 z)^3(x + \beta_3 y + \beta_3^2 z)$$

$$+\sqrt[7]{\beta_3^3\beta_1}(x + \beta_3 y + \beta_3^2 z)^3(x + \beta_1 y + \beta_1^2 z) = 0.$$

And the isomorphism is given by:

$$\phi_0^{-1} \circ \begin{pmatrix} \sqrt[7]{\beta_1} & \beta_1\sqrt[7]{\beta_1} & \beta_1^2\sqrt[7]{\beta_1} \\ \sqrt[7]{\beta_2} & \beta_2\sqrt[7]{\beta_2} & \beta_2^2\sqrt[7]{\beta_2} \\ \sqrt[7]{\beta_3} & \beta_3\sqrt[7]{\beta_3} & \beta_3^2\sqrt[7]{\beta_3} \end{pmatrix} : C' \to C.$$

For each such field L we find to different twists, the one showed before and the one coming from replacing β_1, β_2 and β_3 with β_1^6, β_2^6 and β_3^6.

The case $\mathrm{ID}(G) =< 8, 1 >$

Let $\phi : C' \longrightarrow C$ be a twists corresponding to a solution Ψ associated to the pair $(G, H) = (< 8, 1 >, < 4, 1 >)$, and let L be the field of definition of the twist, that is the splitting field of the solution Ψ.

Lemma 3.3.1. *In the above conditions, we have $k(i, \sqrt{2}) = k$ and $L = k(\sqrt[8]{-7\gamma^2})$ for some $\gamma \in k$.*

Proof. Let us consider $k_0 = k(i, \sqrt{2})$ and $L_0 = L(i, \sqrt{2})$. Then, by Kummer theory $L_0 = k_0(\sqrt[8]{-7\gamma^2})$ for some $\gamma \in k_0$. Let us first assume that $[L_0 : L] = 4$, then $\mathrm{Gal}(L_0/k) \simeq C_8 \times V_4$

and it is generated by:

$$\begin{array}{rccclrccclrccc}
a: & i & \longrightarrow & i & \quad & b: & i & \longrightarrow & -i & \quad & c: & i & \longrightarrow & i \\
 & \sqrt{2} & \longrightarrow & \sqrt{2} & & & \sqrt{2} & \longrightarrow & \sqrt{2} & & & \sqrt{2} & \longrightarrow & -\sqrt{2} \\
 & \sqrt[8]{-7\gamma^2} & \longrightarrow & \zeta_8\sqrt[8]{-7\gamma^2} & & & \sqrt[8]{-7\gamma^2} & \longrightarrow & \sqrt[8]{-7\gamma_1^2} & & & \sqrt[8]{-7\gamma^2} & \longrightarrow & \sqrt[8]{-7\gamma_2^2}
\end{array}$$

where $\gamma_1, \gamma_2, \gamma_3$ are the other conjugates of γ in k_0 and $a^8 = b^2 = c^2$ and they commute. Since they commute and have the order especified before we can assume:

$$\begin{array}{rccclrccclrccc}
a: & \sqrt[8]{-7\gamma_1^2} & \longrightarrow & \sqrt[8]{-7\gamma_1^2} & \quad & b: & \sqrt[8]{-7\gamma_2^2} & \longrightarrow & \sqrt[8]{-7\gamma_1^3} & \quad & c: & \sqrt[8]{-7\gamma_1^2} & \longrightarrow & \sqrt[8]{-7\gamma_1^3} \\
 & \sqrt[8]{-7\gamma_2^2} & \longrightarrow & \zeta_8^5\sqrt[8]{-7\gamma_2^2} & & & & & & & & & & \\
 & \sqrt[8]{-7\gamma_3^2} & \longrightarrow & \zeta_8^3\sqrt[8]{-7\gamma_3^2} & & & & & & & & & &
\end{array}$$

Notice that $\sqrt[4]{-7\gamma\gamma_1}$ is fixed by the action of a and b, then $-7\gamma\gamma_1 = s^4$ for some $s \in k(\sqrt{2})$. Moreover, $\gamma_1 = q^8\gamma^7$ for some $q \in k_0$, then $-7q^8\gamma^8 = s^4$ and $\sqrt{-7} \in k_0$, which is a contradiction.

Assume now that $[L_0 : L] = 2$. Then $\mathrm{Gal}(L_0/k) \simeq C_8 \times C_2$, and it is generated by:

$$\begin{array}{rccclrccc|ccc}
a: & i & \longrightarrow & i & \quad & b: & i & \longrightarrow & \epsilon_1 i & \epsilon_1 & \epsilon_2 & A \\
 & \sqrt{2} & \longrightarrow & \sqrt{2} & & & \sqrt{2} & \longrightarrow & \epsilon_2\sqrt{2} & 1 & -1 & 5 \\
 & \sqrt[8]{-7\gamma^2} & \longrightarrow & \zeta_8\sqrt[8]{-7\gamma^2} & & & \sqrt[8]{-7\gamma^2} & \longrightarrow & \sqrt[8]{-7\gamma_1^2} & -1 & 1 & 7 \\
 & \sqrt[8]{-7\gamma_1^2} & \longrightarrow & \zeta_8^A\sqrt[8]{-7\gamma_1^2} & & & & & & -1 & -1 & 3
\end{array}$$

Cases $(\epsilon_1, \epsilon_2) = (-1, 1), (-1, -1)$ follow as case $[L_0 : L] = 4$. For case $(\epsilon_1, \epsilon_2) = (1, -1)$ we get $\gamma_1 = q^8\gamma^5$, so $\frac{\gamma_1}{\gamma} = s^4$ for some $s \in k_0$, but $a : \frac{\sqrt[8]{-7\gamma_1^2}}{\sqrt[8]{-7\gamma^2}} = s \longrightarrow -s$, which is a contradiction. So, finally, $L_0 = L$ and $k_0 = k = k(i, \sqrt{2})$. □

Then, we find the isomorphism $\phi : C' \longrightarrow C$ given by:

$$\phi = \begin{pmatrix} \sqrt[8]{-7\gamma^2} & 0 & 0 \\ 0 & \frac{\sqrt{-7}\sqrt[4]{-7\gamma^2}\sqrt[8]{-7\gamma^2}}{7} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{1+2\sqrt{2}+\sqrt{-7}} \end{pmatrix} \begin{pmatrix} 1/2 & 1/2 & 0 \\ -i/2 & i/2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \phi_2^{-1}$$

where

$$\phi_2 = \begin{pmatrix} -\alpha & 1 & 2\alpha+3 \\ 2\alpha+3 & -\alpha & 1 \\ 1 & 2\alpha+3 & -\alpha \end{pmatrix},$$

will be also useful later. We get the equation:

$$C' : -7\gamma x^4 + \gamma^3 y^4 + \frac{z^4}{64(1+2\sqrt{2})^2} - 6\gamma^2 x^2 y^2 + \frac{8\gamma x y z^2}{8(1+2\sqrt{2})} = 0.$$

Given such a splitting field L we find two different twists, the one showed before and the one comming by replacing γ by γ^3, see formula (1.7).

The case $\mathrm{ID}(G) =< 8,3 >$

In this case $L = k(\sqrt{-7}, \sqrt{a+b\sqrt{m}})$ where $a^2 - mb^2 = -7mq^2$ with $a, b, m, q \in k$ and m square-free. We call $S = \sqrt{a+b\sqrt{m}}$ and $A = \frac{\sqrt{a-b\sqrt{m}}}{\sqrt{-7}\sqrt{a+b\sqrt{m}}}$. Then we have the twist given by the isomorphism:

$$\phi = \begin{pmatrix} 3 & (5A-1)S & \sqrt{m}(5A+1)S \\ -1 & (3A-3)S & \sqrt{m}(3A+3)S \\ -2 & 6AS & 6\sqrt{m}AS \end{pmatrix}.$$

And we have the equation:

$$-49x^4 - 252ax^2y^2 + 504bmx^2yz - 252amx^2z^2 + (124a^2 + 980q^2m - 448qbm)y^4 + (896q - 496b)amy^3z +$$

$$+24m(22a^2 + 9b^2m)y^2z^2 - 16m(31m + 56qa)yz^3 + 7m^3q(47q + 64b)z^4 = 0$$

Given such a field L we find two different twists, the one showed before and the one coming from replacing a with $2a$, b with q, m with $-7m$ and $2q$ with and q with $\frac{2}{7}b$.

The case $\mathrm{ID}(G) =< 12,4 >$

In that case $L = k(a, b, c)$, where a, b, c are the three roots of degree 3 polynomial with coefficents in k and such that its splitting field over k has Galois group isomorphic to S_3 and whose discriminant Δ is not of the form $-7q^2$ with $q \in k$. Two twists are equivalent if and only if they have the same splitting field by formula (1.7). They are given by the isomorphism:

$$\phi = \begin{pmatrix} \sqrt{\Delta} & -3a + 2b + c & ab - 3bc + 2ca \\ \sqrt{\Delta} & a - 3b + 2c & 2ab + bc - 3ca \\ \sqrt{\Delta} & 2a + b - 3c & -3ab + 2bc + ca \end{pmatrix}.$$

And have the equation:

$$3\Delta^2x^4 + 21(A^2 - 3B)\Delta x^2y^2 + 21(9C - AB)\Delta x^2yz + 21(B^2 - 3AC)\Delta x^2z^2 - 147\Delta xy^3 + 147A\Delta xy^2z -$$

$$-147B\Delta xyz^2 + 147C\Delta xz^3 + 49(-A^4 + 6A^2B - 9B^2)y^4 + 98(A^3B - 9A^2C - 3AB^2 + 27BC)y^3z +$$

$$+147(2A^4B - A^2B^2 + 2B^3 - 27C^2)y^2z^2 + 98(-3A^2BC + AB^3 + 27AC^2 - 9B^2C)yz^3 +$$

$$+49(-9A^2C^2 + 6AB^2C - B^4)z^4 = 0,$$

where $A = a + b + c$, $B = ab + bc + ca$ and $C = abc$.

The case $\mathrm{ID}(G) =< 42, 1 >$

If $\zeta_7 \in L$, then we apply proposition (1.3.2) and $L = k(\zeta_7, \sqrt[7]{m})$ for some $m \in k$. And given the field L there are two different twists: $mx^3y+y^3z+z^3x = 0$ and $m^3x^3y+y^3z+z^3x = 0$. Otherwise, let us consider the field $\tilde{L} = L(\xi_7)$. Then $\left[\tilde{L} : L\right] = 3$. There is a normal subextension of order 3 over k not contained in $k(\xi_7)$, let us call such subextension F_0. Then $F = F_0(\zeta_7)$ is a subextenion of index 7 of $\tilde{L}$. Then by Kummer theory we have $\tilde{L} = k(\zeta_7, \sqrt[7]{\beta})$ with $\beta \in F$. And again, as in the case $< 14, 1 >$ we can assume $\beta \in F_0$. And L/k is the only normal subextension of degree 42 of $\tilde{L}/k$. Let us call $\beta_1 = \beta$ and β_2 and β_3 its two conjugates in $\tilde{L}$. Then $\sqrt[7]{\beta_1\beta_2\beta_3} \in k$. And then it is easy to check that $\mathrm{Gal}(\tilde{L}/k)$ is generated by the elements σ, τ and ν with:

$$\sigma(\zeta_7) = \zeta_7,\ \ \sigma(\sqrt[7]{\beta_1}) = \zeta_7\sqrt[7]{\beta_1},\ \ \sigma(\sqrt[7]{\beta_2}) = \zeta_7^4\sqrt[7]{\beta_2},\ \ \sigma(\sqrt[7]{\beta_3}) = \zeta_7^2\sqrt[7]{\beta_3}.$$

$$\tau(\zeta_7) = \zeta_7,\ \ \tau(\sqrt[7]{\beta_1}) = \sqrt[7]{\beta_2},\ \ \tau(\sqrt[7]{\beta_2}) = \sqrt[7]{\beta_3},\ \ \tau(\sqrt[7]{\beta_3}) = \sqrt[7]{\beta_1}.$$

$$\nu(\zeta_7) = \zeta_7^3,\ \ \nu(\sqrt[7]{\beta_1}) = \sqrt[7]{\beta_1},\ \ \nu(\sqrt[7]{\beta_2}) = \sqrt[7]{\beta_2},\ \ \nu(\sqrt[7]{\beta_3}) = \sqrt[7]{\beta_3}.$$

Finally, we obtain the twist with equation:

$$\sqrt[7]{\beta_1^3\beta_2}(x+\beta_1y+\beta_1^2z)^3(x+\beta_2y+\beta_2^2z) + \sqrt[7]{\beta_2^3\beta_3}(x+\beta_2y+\beta_2^2z)^3(x+\beta_3y+\beta_3^2z)$$

$$+\sqrt[7]{\beta_3^3\beta_1}(x+\beta_3y+\beta_3^2z)^3(x+\beta_1y+\beta_1^2z) = 0.$$

And the isomorphism is given by:

$$\phi_0^{-1} \circ \begin{pmatrix} \sqrt[7]{\beta_1} & \beta_1\sqrt[7]{\beta_1} & \beta_1^2\sqrt[7]{\beta_1} \\ \sqrt[7]{\beta_2} & \beta_2\sqrt[7]{\beta_2} & \beta_2^2\sqrt[7]{\beta_2} \\ \sqrt[7]{\beta_3} & \beta_3\sqrt[7]{\beta_3} & \beta_3^2\sqrt[7]{\beta_3} \end{pmatrix} : C' \to C.$$

Given such a field L we find two different twists, the one showed above and the one coming from replacing β_1, β_2 and β_3 with β_1^6, β_2^6 and β_3^6.

The case $\mathrm{ID}(G) =< 16, 7 >$

Let $\phi : C' \longrightarrow C$ be a twist corresponding to the pair $(G, H) = (< 16, 7 >, < 8, 3 >)$, and let L be the field of definition of the twist. Then, by lemma (3.3.1), we have: $L = k(\sqrt{m}, \sqrt[8]{-7\gamma^2})$ where $\gamma \in k(\sqrt{m})$ and $k(i, \sqrt{2}) \subseteq k(\sqrt{m})$. We will check that, in fact, $k = k(\sqrt{2})$, $k(i) = k(\sqrt{m})$ and $\gamma \in k$, then for the splitting field L we will get 4 different twists, the two ones given in case $\mathrm{ID}(G) =< 8, 1 >$ and the two ones coming from replacing γ with $\bar{\gamma}$. The difference between case $\mathrm{ID}(G) =< 8,1 >$ and this one is just that in the first one $i \in k$ and in the second one not.

The group $\mathrm{Gal}(L/k)$ is generated by:

$$\begin{array}{ccccccccc|ccc}
a: & \sqrt{m} & \longrightarrow & \sqrt{m} & b: & \sqrt{m} & \longrightarrow & -\sqrt{m} & & \epsilon_1 & \epsilon_2 & A \\
 & i & \longrightarrow & i & & i & \longrightarrow & \epsilon_1 i & & 1 & 1 & 7 \\
 & \sqrt{2} & \longrightarrow & \sqrt{2} & & \sqrt{2} & \longrightarrow & \epsilon_2\sqrt{2} & & 1 & -1 & 3 \\
 & \sqrt[8]{-7\gamma^2} & \longrightarrow & \zeta_8\sqrt[8]{-7\gamma^2} & & \sqrt[8]{-7\gamma^2} & \longrightarrow & \sqrt[8]{-7\gamma_1^2} & & -1 & 1 & 1 \\
 & \sqrt[8]{-7\gamma_1^2} & \longrightarrow & \zeta_8^A\sqrt[8]{-7\gamma_1^2} & & & & & & -1 & -1 & 5
\end{array}$$

Where we get the conditions on A looking at the relations $a^8 = b^2 = 1$ and $ab = ba^7$. Now, we can discard cases $(\epsilon_1, \epsilon_2) = (1,1), (1,-1), (-1,-1)$ proceeding as in the proof of lemma 3.3.1. Then $\sqrt{2} \in k$, $i \notin k$, and $L = k(i\sqrt[8]{-7\gamma^2})$ for some $\gamma \in k(i)$. But since $A = 1$, we can take $\gamma \in k$.

The case $\mathrm{ID}(G) =< 336,208 >$

We have not been able to compute the solutions to the Galois embedding problem corresponding to this pair (G,H). We are waiting for a efficient implementation of the algorithm in Appendix for computing the twists.

Now, let us suppose that $\sqrt{-7} \in k$, then we obtain in this case the following possibilities for the pairs (G,H) where $G = H$ because here $\mathrm{Gal}(K/k)$ is trivial:

	$\mathrm{ID}(G)$	$\mathrm{gen}(G)$
1	$< 1,1 >$	1
2	$< 2,1 >$	s
3	$< 3,1 >$	h
4	$< 7,1 >$	g
5	$< 4,1 >$	$g^2sg^3sg^2$
6	$< 6,1 >$	$h,\ s$
7	$< 21,1 >$	$g,\ h$
8	$< 8,3 >$	$g^2sg^3sg^2,\ g^2sg^5$
9	$< 168,42 >$	$s,\ g,\ h$
10	$< 12,3 >$	$h,\ sg^2sg^5$
11	$< 24,12 >$	$s,\ h,\ g^2sg^5$

The first nine cases appeared also when $\sqrt{-7} \notin k$. We have just two new cases: 10 and

11. For computing the twists in that case we will use the twist:

$$C_{S_4} : x^4 + y^4 + z^4 + 3\alpha(x^2y^2 + y^2z^2 + z^2x^2) = 0,$$

where again $\alpha = \frac{-1+\sqrt{-7}}{2}$ and given by the isomorphism:

$$\phi_1 = \begin{pmatrix} 1 & 1+\zeta\alpha & \zeta^2+\zeta^6 \\ 1+\zeta\alpha & \zeta^2+\zeta^6 & 1 \\ \zeta^2+\zeta^6 & 1 & 1+\zeta\alpha \end{pmatrix} : C_{S_4} \to C_K.$$

The form of this twist in the corresponding to the case VIII in Henn classification. We have computed the twists for this model in section 3.2. And we obtain $L = k(\sqrt{a}, \sqrt{b}, \sqrt{c})$ where a, b, c are the three roots of a degree 3 polynomial with coefficients in k and such that its splitting field has Galois group over k isomorphic to C_3 or S_3 respectively. Two such twists are equivalent if and only if the have the same splitting field L and are given by the equation:

$$C' : a^2(x+ay+a^2z)^4 + b^2(x+by+b^2z)^4 + c^2(x+cy+c^2z)^4 + 3\alpha(ab(x+ay+a^2z)^2(x+by+b^2z)^2 +$$

$$+bc(x+by+b^2z)^2(x+cy+c^2z)^2 + ca(x+cy+c^2z)^2(x+ay+a^2z)^2) = 0.$$

Chapter 4

The Sato-Tate conjecture for the twists of the Fermat and Klein quartics

In (proposition 16, [34]) the Generalize Sato-Tate conjecture (0.0.10) is proven for abelian varieties A/k that are isogenous to a product of abelian varieties with complex multiplication over a finite extension of k. We will show that this is the case for the twists of the Fermat and the Klein quartics. We also compute the Sato-Tate groups and the Sato-Tate distributions. Finally, we give example curves for each of the distributions obtained. We follow the ideas in [2], [18], [22] and [35] for computing the Sato-Tate groups and the Sato-Tate distributions of the twists computed in chapter 3. In fact, for the distributions, what we compute is the sequence of moments of the distributions, that by proposition 1 in [35] completly determines them. Finally, we use the results in chapter 3 for giving example curves of each of the distributions.

All these results are part of a forthcoming paper in collaboration with F. Fité and A.V. Sutherland, [21]. In this paper is also showed how to compute the Sato-Tate distributions studying a Galois representation attached to each twist, without having to use the knowledge of the Sato-Tate groups. Moreover, graphics of the distributions are showed using a powerful algorithm for counting the number of points over finite fields of non-hyperelliptic curves due to A.V. Sutherland, [57].

We denote by $C_1 : x^4 + y^4 + z^4 = 0$ the Fermat quartic and by

$$C_7 : x^4 + y^4 + z^4 + 6(xy^3 + yz^3 + zx^3) - 3(x^2y^2 + y^2z^2 + z^2x^2) + 3xyz(x + y + z) = 0$$

the twist of the Klein quartic that we used in chapter 3. We consider the elliptic curves

$$E_1 : y^2 = x^3 + x, \quad E_7 : y^2 = 4x^3 + 21x^2 + 28x,$$

with complex multiplication by $M_1 = \mathbb{Q}(i)$ and $M_7 = \mathbb{Q}(\sqrt{-7})$, respectively.

Proposition 4.0.2. *One has that the jacobian variety $J(C_d)$ is $\mathbb{Q}-$isogenous to $E_d \times E_d \times E_d$ for $d = 1$ and 7.*

See [40] for a proof of the case of $d = 1$ and [12] for $d = 7$.

4.1 The Sato-Tate conjecture

We prove that we have the hypothesis in next proposition, and we apply it for proving the Generalize Sato-Tate conjecture for the twists of the Fermat and the Klein quartics.

Proposition 4.1.1. *(Johansson, [34]) Let A be an abelian variety defined over a number field k, and such that becomes isogenous to a product of abelian varieties with complex multiplication over a finite extension of k. Then the Generalize Sato-Tate conjecture holds for A/k.*

Corollary 4.1.2. *The generalized Sato-Tate conjecture holds for the twists of the Fermat and Klein quartic.*

Proof. Since by proposition (4.0.2), we have $\mathrm{J}(C_d) \sim_{\mathbb{Q}} E_d^3$ and E_d has complex multiplication by M_d, for any twist we have

$$\mathrm{J}(C'_d) \simeq_L \mathrm{J}(C_d) \sim_{\mathbb{Q}} E_d^3,$$

where L is the field of definition of the twist. Then $\mathrm{J}(C'_d) \sim_L E_d^3$ with L a finite extension of k and we can apply proposition (4.1.1). □

4.2 The Sato-Tate groups

By theorem (6.10) in [2] the Algebraic Sato-Tate conjecture holds for the twists of the Fermat and the Klein quartics. That is, there exists an algebraic group $\mathrm{AST}_k(C') \subseteq \mathrm{Sp}_6$ over $\mathbb{Q}$ such that

$$\mathrm{AST}_k(C'_d)_{\mathbb{Q}_l} = \mathrm{G}_{l,\iota}^{1,\omega}(C'_d),$$

where $\mathrm{G}_{l,\iota}^{1,\omega}$ is defined as in (0.0.9). Moreover, theorem (6.10) in [2] sais that $\mathrm{AST}_k(C'_d)$ is equal to $L(\mathrm{J}(C'_d))$ the Lefschetz group of the jacobian variety of C'_d. The Lefschetz group of an abelian variety is defined to be:

$$L(A) = \bigcup L(A,\tau) = \bigcup \left\{\gamma \in \mathrm{Sp}_{2g} : \gamma^{-1}\alpha\gamma =^{\tau} \alpha \;\forall\, \alpha \in \mathrm{End}(A) \otimes \mathbb{Q}\right\},$$

where the union is over the $\tau \in \mathrm{Gal}(L/k)$. Given a twist C' of the Fermat or of the Klein quartics, we have associated to it a pair (G,H) as in section 1.3 if $k \subsetneq K_d := kM_d$ and (H,H)

if $k = K_d$. For the Fermat quartic we have 59 different pairs up to conjugacity and for the Klein quartic 22 pairs. In the case in which $k \subsetneq K_d$, we have the equality $G = H \cup Hh \cdot (1, \tau)$ where τ in the non-trivial element in $\mathrm{Gal}(K_d/k)$.

Let us first consider the monomorphism:

$$\iota : \mathrm{Aut}(C_d) \hookrightarrow^{\iota_1} \mathrm{End}(\Omega^1(C_d)) \simeq^{\iota_2} \mathrm{End}(\Omega^1(E_d^3)) \simeq^{\iota_3} \mathrm{End}(T_l(E_d)^3) \hookrightarrow \mathrm{GSp}_6(\mathbb{Q}),$$

given by

$$\iota(s_1) = \begin{pmatrix} 0 & 0 & I_2 \\ I_2 & 0 & 0 \\ 0 & I_2 & 0 \end{pmatrix}, \quad \iota(t_1) = \begin{pmatrix} 0 & -I_2 & 0 \\ I_2 & 0 & 0 \\ 0 & 0 & -I_2 \end{pmatrix}, \quad \iota(u_1) = \begin{pmatrix} -I_2 & 0 & 0 \\ 0 & -J_2 & 0 \\ 0 & 0 & -J_2 \end{pmatrix}$$

and

$$\iota(s_7) = \begin{pmatrix} 0 & I_2 & 0 \\ 0 & 0 & I_2 \\ I_2 & 0 & 0 \end{pmatrix}, \quad \iota(t_7) = \frac{1}{7}\begin{pmatrix} -3I_2 & -6I_2 & 2I_2 \\ -6I_2 & 2I_2 & -3I_2 \\ 2I_2 & -3I_2 & -6I_2 \end{pmatrix}, \quad \iota(u_7) = \frac{1}{7}\begin{pmatrix} -2I_2 - 4K_2 & 3I_2 - K_2 & -I_2 - 2K_2 \\ 3I_2 - K_2 & -I_2 - 2K_2 & -2I_2 + 3K_2 \\ -I_2 - 2K_2 & -2I_2 + 3K_2 & -4I_2 - K_2 \end{pmatrix}.$$

Where we define the matrices:

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad J_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad K_2 = \begin{pmatrix} 0 & -2 \\ 1 & -1 \end{pmatrix}.$$

The embedding ι_1 is the natural one given by the canonical model that we have choosen for the Fermat and the Klein quartic. The isomorphism ι_2 is the one given by identifing the basis associated to the canonical model to $\{(\omega_d, 0, 0), (0, \omega_d, 0), (0, 0, \omega_d)\}$ where ω_d is the invariant differential of the elliptic curve E_d. Finally, ι_3 is the natural isomorphism when we see one of the vector spaces as the dual of the other.

Remark 4.2.1. *Notice that the matrices $\iota(s_d)$, $\iota(t_d)$, $\iota(u_d)$ are symplectic with respect to $(J_2)_3$. And in fact, they are contained in* $\mathrm{USp}(6)$.

Lemma 4.2.2. *The above monomorphism extends to a monomorphism*

$$\iota : \Gamma = \mathrm{Aut}(C_d) \rtimes \mathrm{Gal}(K_d/k) \hookrightarrow \mathrm{USp}(6)$$

in a trivial way if $K_d = k$, and by defining

$$\iota((1,\tau)) = \begin{cases} \frac{1}{\sqrt{2}}\begin{pmatrix} i & i \\ i & -i \end{pmatrix}_3 & \text{in case } C = C_1, \\ \begin{pmatrix} i & -i \\ 0 & -i \end{pmatrix}_3 & \text{in case } C = C_7, \end{cases}$$

if $k \subsetneq K_d$, and where we use the notation $B_3 = Id_3 \otimes B$ for a matrix B.

Theorem 4.2.3. *Let $\phi : C'_d \to C_d$ be a twist of C_d with pair (G,H). Then, the Sato-Tate group of C'_d is then given by*

$$\mathrm{ST}_k(C'_d) = \left\{ \begin{pmatrix} \cos(2\pi r) & \sin(2\pi r) \\ -\sin(2\pi r) & \cos(2\pi r) \end{pmatrix}_3 \mid r \in [0,1] \right\} \cdot \iota(H)$$

in case $C_d = C_1$, and by

$$\mathrm{ST}_k(C'_d) = \left\{ \begin{pmatrix} \cos(2\pi r) - \frac{1}{\sqrt{7}}\sin(2\pi r) & \frac{4}{\sqrt{7}}\sin(2\pi r) \\ -\frac{2}{\sqrt{7}}\sin(2\pi r) & \cos(2\pi r) + \frac{1}{\sqrt{7}}\sin(2\pi r) \end{pmatrix}_3 \mid r \in [0,1] \right\} \cdot \iota(H)$$

in case $C_d = C_7$.

Proof. We consider the case $k \subsetneq K_d$, which is the most complex one. By [2], we have that $\mathrm{ST}_k(E_d)$ is a maximal compact subgroup of $\mathrm{AST}(E_d) \otimes \mathbb{C}$, where $\mathrm{AST}_k(E_d) = \mathrm{L}(E_d,1) \cup \mathrm{L}(E_d,\tau)$, where for $\sigma \in \mathrm{Gal}(K_d/k)$ one has

$$\mathrm{L}(E_d,\sigma) \coloneqq \{\gamma \in \mathrm{Sp}_2 \mid \gamma^{-1}\alpha\gamma = {}^{\sigma}\alpha \text{ for all } \alpha \in \mathrm{End}(E_d) \otimes \mathbb{Q}\}. \tag{4.1}$$

This induces a decomposition $\mathrm{ST}_k(E_d) = \mathrm{ST}(E_d,1) \cup \mathrm{ST}(E_d,\tau)$ that can be explicitly determined. For the case $C_d = C_1$, we have

$$\begin{aligned} \mathrm{L}(E_1,1)(\mathbb{C}) &= \{A \in \mathrm{M}_2(\mathbb{C}) | A^t J_2 A = J_2,\ A^{-1} J_2 A = J_2,\ \det(A) = 1\} \\ &= \left\{ \begin{pmatrix} c & b \\ -b & c \end{pmatrix} \mid c,b \in \mathbb{C},\ c^2 + b^2 = 1 \right\}. \end{aligned}$$

Then, a maximal compact subgroup of $\mathrm{L}(E_1,1)(\mathbb{C})$ is

$$\mathrm{ST}(E_1,1) = \left\{ \begin{pmatrix} \cos(2\pi r) & \sin(2\pi r) \\ -\sin(2\pi r) & \cos(2\pi r) \end{pmatrix} \mid r \in [0,1] \right\}.$$

Analogously,

$$\begin{aligned} \mathrm{L}(E_1,\tau)(\mathbb{C}) &= \{A \in \mathrm{M}_2(\mathbb{C}) | A^t J_2 A = J_2,\ A^{-1} J_2 A = -J_2,\ \det(A) = 1\} \\ &= \left\{ \begin{pmatrix} ic & ib \\ ib & -ic \end{pmatrix} \mid c,b \in \mathbb{C},\ c^2 + b^2 = 1 \right\}. \end{aligned}$$

Then, a maximal compact subgroup of $\mathrm{L}(E_1,\tau)(\mathbb{C})$ is

$$\mathrm{ST}(E_1,\tau) = \mathrm{ST}(E_1,1) \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} i & -i \\ i & -i \end{pmatrix}.$$

Notice that given the twit $\phi : C'_d \to C_d$ we have $\phi_* : \mathrm{J}(C'_d) \to \mathrm{J}(C_d)$ and then $L(\mathrm{J}(C'_d),\tau) = \phi_*^{-1} L(\mathrm{J}(C_d),\tau)^{\tau}\phi_*$. That is conjugated by ϕ_* to $L(\mathrm{J}(C_d),\tau)^{\tau}\phi_*\phi_*^{-1} = L(\mathrm{J}(C_d),\tau)\iota(\xi_\tau^{-1})$. Then, we have

$$\mathrm{AST}_k(C'_d) = \mathrm{AST}_k(E^3)\cdot\iota(H).$$

from which follows

$$\begin{aligned}
\mathrm{ST}(C'_d) &= (\mathrm{ST}(E_1))_3\cdot\iota(H)\\
&= (\mathrm{ST}(E_1,1))_3\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}_3 \cup \frac{1}{\sqrt{2}}\begin{pmatrix} i & i\\ i & -i\end{pmatrix}_3\right)\cdot\iota(\mathrm{Gal}(L/K_d))\\
&= (\mathrm{ST}(E_1,1))_3\cdot\iota(\mathrm{Gal}(L/k))\\
&= (\mathrm{ST}(E_1,1))_3\cdot\iota(H)\,.
\end{aligned}$$

For the case $C_d = C_7$, we have

$$\begin{aligned}
\mathrm{L}(E_7,1)(\mathbb{C}) &= \{A \in \mathrm{M}_2(\mathbb{C}) | A^t J_2 A = J_2,\ A^{-1}K_2A = K_2,\ \det(A) = 1\}\\
&= \left\{\begin{pmatrix} c-b & 4b\\ -2b & c+b\end{pmatrix} | \, c,b\in\mathbb{C},\ c^2+7b^2 = 1\right\}.
\end{aligned}$$

Thus, a maximal compact subgroup of $\mathrm{L}(E_7,1)(\mathbb{C})$ is

$$\mathrm{ST}(E_7,1) = \left\{\begin{pmatrix}\cos(2\pi r) - \frac{1}{\sqrt{7}}\sin(2\pi r) & \frac{4}{\sqrt{7}}\sin(2\pi r)\\ -\frac{2}{\sqrt{7}}\sin(2\pi r) & \cos(2\pi r) + \frac{1}{\sqrt{7}}\sin(2\pi r)\end{pmatrix} | \, r \in [0,1]\right\}.$$

Analogously,

$$\begin{aligned}
\mathrm{ST}(E_7,\tau) &= \{A \in \mathrm{M}_2(\mathbb{C}) | A^t J_2 A = J_2,\ A^{-1}K_2A = -I_2 - K_2,\ \det(A) = 1\}\\
&= \left\{\begin{pmatrix} ic-ib & 4ib\\ \frac{ic}{2}+\frac{3ib}{2} & ib-ic\end{pmatrix} | \, c,b\in\mathbb{C},\ c^2+7b^2 = 1\right\}.
\end{aligned}$$

Thus, a maximal compact subgroup of $\mathrm{L}(E_7,\tau)(\mathbb{C})$ is

$$\mathrm{ST}(E_7,\tau) = \mathrm{ST}(E_7,1)\cdot\begin{pmatrix} i & -i\\ 0 & -i\end{pmatrix}.$$

Hence, again

$$\begin{aligned}
\mathrm{ST}(C'_d) &= (\mathrm{ST}(E_7))_3\cdot\iota(H)\\
&= (\mathrm{ST}(E_7,1))_3\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}_3 \cup \begin{pmatrix} i & -i\\ 0 & -i\end{pmatrix}_3\right)\cdot\iota(\mathrm{Gal}(L/K_d))\\
&= (\mathrm{ST}(E_7,1))_3\cdot\iota(\mathrm{Gal}(L/k))\\
&= (\mathrm{ST}(E_7,1))_3\cdot\iota(H)\,.
\end{aligned}$$

□

Remark 4.2.4. *The Sato-Tate group only depends on the pair (G, H) associated to the twists, and not on the field of definition. Hence, the Sato-Sate distributions depends also only on the pair (G, H).*

4.3 The Sato-Tate distributions

Since we know that the Generalized Sato-Tate conjecture holds for the twists of the Fermat and Klein quartics and we have computed the Sato-Tate groups we can compute the sequence of moments of the Sato-Tate distributions computing the sequence of moments of the distribution of the characteristic polynomials of the Sato-Tate groups, because both coincide by corollary (4.1.2). In [21] is also directly computed the Sato-Tate distribution of these twists via the study of the representation afforded by the $G_{\bar{\mathbb{Q}}}$–module $\mathrm{Hom}(E_d, \mathrm{Jac}(C_d))$.

The moments of a closed subgroup $G \subseteq \mathrm{USp}(6)$ are defined by

$$\mathrm{M}_{n,i}[G] = \int_{g\in G} a_i(g)^n d\mu(g)\,,$$

where $a_i(g)$ is the ith coefficient of the characteristic polynomial of g and $d\mu$ denotes the Haar measure of G. If the connected component G^0 of G is conjugate to a certain embedding

$$\iota : \mathrm{U}(1) = \{e^{2\pi i r} | r \in [0,1]\} \hookrightarrow \mathrm{USp}(6)$$

then

$$\mathrm{M}_{n,i}[G] = \frac{1}{[G\colon G^0]} \sum_{g\in G/G^0} \int_0^1 a_i(h_g(r))^n dr\,, \tag{4.2}$$

where

$$h_g\colon [0,1] \to gG^0\,, \qquad h_g(r) := g\iota(e^{2\pi i r})\,.$$

We have performed numerical integration on the expression (4.2) for each of the groups of theorem (4.2.3) corresponding to the possibilities for the pairs (G, H). Also notice that, by [35] the moments of a Sato-Tate distribution take values that are interger numbers, so via numerical integration we can obtain exact values of the moments.

Finally, we find 48 different distributions for the twists of the Fermat quartic, among them, only 27 can be realize by twists over $\mathbb{Q}$. For the Klein quartic we find 22 different distributions, where only 9 can be realize by twists given by equations defined over $\mathbb{Q}$. See the obstruction for getting equations over $\mathbb{Q}$ in sections (3.1) and (3.3). In the Apendix, in tables (5.6) and (5.8), we show the first terms of the moments sequences obtained for this distributions.

4.4 Example curves

In the Apendix, in tables (5.7) and (5.9), we show examples curves for each of the pairs (G,H) and then example curves of each of the distributions. In (5.7) we show, for the Fermat quartic, the pairs (G,H) by generators as in section 3 because in that case only the isomorphism classes of the groups G and H do not completly determine the pair. We also show the equation of an example twist for each pair defined over a field k, that we take equal to $\mathbb{Q}$ when is possible, and the Sato-Tate distributions of the twist when we consider it defined over k or $k(i)$. We have enumerated the distributions in (5.6). The field L of definition of the twist can be computed comparing the example curves with the equations in theorems (3.1.7), (3.1.8) and (3.1.9).

In (5.9) we show, for the Klein quartic, the isomorphism class of the groups G and H for each pair, that in this case it is enought for identifying a pair (G,H). We also show example twists with equations over $\mathbb{Q}$ when it is possible that we computed using the classification of the twists of the Klein quartic in section 3.3. The field L of definition of the twists is especified in each case.

For the last case of the Klein quartic, the pair $(<336,>,<168,>)$, we did not computed the twists in section 3.3, but even in this case we can provide an example curve using the results in [29].

Proposition 4.4.1. *(Theorem 2.1, [29]) Given an elliptic curve $E: y^2 = x^3 + ax + b$ defined over a number field k one has the twists $X_E(7)$ of the Klein quartic:*

$$ax^4 + 7bx^3z + 3x^3y^2 - 3a^2x^2z^2 - 6bxyz^2 - 5abxz^3 + 2y^3z + 3ay^2z^2 + 2a^2yz^3 - 4b^2z^4 = 0.$$

Moreover, the minimal field of definition of any isomorphism from the Klein quartic to $X_E(7)$ is the field of definition of the $7th-$torsion of the elliptic curve E.

In [45] is proven that the Galois representation corresponding to the $7th-$torsion of the elliptic curve $y^2 = x^3 - 2x + 1$ with conductor 40 is surjective, and then we get an example curve for the pair $(<336,>,<168,>)$ using this curve and previous proposition.

Unfortunately, this nice parametrization of the twists $X_E(7)$ does not cover all the twists of the Klein quartic, since the twists of the Klein quartic are in correspondence with projective Galois representations $\rho : G_k \to \mathrm{PGL}_2(\mathbb{F}_7)$ (continuous and with cyclotomic determinant, [14]) and not all of such representations come from the $7-$torsion of an elliptic curve.

Chapter 5

The Sato-Tate conjecture for the Fermat hypersurfaces

In this chapter we prove the generalize Sato-Tate conjecture for the Fermat hypersurfaces $X_n^m : x_0^m + x_1^m + \ldots + x_{n+1}^m = 0 \subseteq \mathbb{P}^{n+1}$ when we consider them defined over the number field $\mathbb{Q}(\zeta_m)$. Moreover, we compute the Sato-Tate groups $\mathrm{ST}_{\mathbb{Q}}(X_n^m)$. For this purpose we use a strong result of Delinge about the action of the Frobenius elements in the étale cohomoly of these varieties, [11], and an interpretation due to Weil of the Jacobi sums as grossencharakters, [61]. Up to our knowledge, these are the first cases for which the generalize Sato-Tate conjecture is proven for varieties of dimension greater than 1, that are not abelian varieties. Finally, as an example, we study the case with $n = 1$ and $m = 6$, that is a genus 10 curve.

5.1 Étale cohomology

All the results in this section are well-known and reproduced here for completness. They can be found in, [7], [11],[27], [28], [60].

Let $X_n^m : x_0^m + x_1^m + \ldots + x_{n+1}^m = 0 \subseteq \mathbb{P}^{n+1}$ be a Fermat hypersurface of dimension equal to n. Let us denote $A := \mathbb{P}_{\mu_m}^{n+1}$ where μ_m is the set of $m-$th roots of the unity, then $\tilde{A} := A \rtimes S_{n+2}$ is isomorphic in a natural way to the automorphisms group of X_n^m. Let us fix $\zeta_m := e^{2\pi i/m} \in \mu_m \subseteq \mathbb{C}$ and let us define the group of characters of A as:

$$\check{A} := \left\{ a = (a_0, \ldots, a_{n+1}) \in (\mathbb{Z}/m\mathbb{Z})^{n+2} \mid \sum_{i=0}^{n+1} a_i = 0 \bmod m \right\},$$

where $(a,\ (\zeta_m^{r_0}, \ldots, \zeta_m^{r_{n+1}})) \longrightarrow \prod_{i=0}^{n+1} \zeta_m^{a_i r_i}$. Consider the subset:

$$A_n^m := \left\{ a \in \check{A} \mid a_i \neq 0 \,\forall i \in \{0, \ldots, n+1\} \right\}.$$

Fix $k = \mathbb{F}_p$ with $p \equiv 1 \bmod m$ and a prime number $l \equiv 1 \bmod m$. Let χ be a character of $k^\times$ of exact order m. Given $a \in A_n^m$ we define the Jacobi sum:

$$J^{(m)}(a) = (-1)^n \sum_{\substack{(v_1,\dots,v_{n+1}) \in (k^\times)^{n+1} \\ 1+v_1+\dots+v_{n+1}=0}} \chi(v_1)^{a_1}\dots\chi(v_{n+1})^{a_{n+1}} \in \mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}_l.$$

When it is clear from the context we omit the subcript m. We have $|J(a)| = p^{n/2}$.

Remark 5.1.1. *This Jacobi sum actually is the one defined in [27] as*

$$J(\chi^{a_1},\dots,\chi^{a_{n+1}}).$$

Notice that the definition that we gave of a Jacobi sum depends on the choice of the character χ. This ambiguity is clarified with the next alternative definition given in [61]. Since $p \equiv 1 \bmod m$, it is completly split in $\mathbb{Q}(\zeta_m)$, so $p = \mathfrak{p}_1\mathfrak{p}_2...\mathfrak{p}_{\phi(m)}$, if we fix a prime, say $\mathfrak{p}_1$, we take the only character $\chi_{\mathfrak{p}_1}$ such that for every integer x prime to $\mathfrak{p}_1$ in $\mathbb{Q}(\zeta_m)$, $\chi_{\mathfrak{p}_1}(x)$ is the only root of the unity in $\mathbb{Q}(\zeta_m)$ satisfying:

$$\chi_{\mathfrak{p}_1}(x) \equiv x^{(p-1)/m} (\bmod\ \mathfrak{p}_1).$$

So, make a choice of the character χ is equivalent to make a choice of the a prime $\mathfrak{p}_i$.

Theorem 5.1.2. *(Deligne) Let be $V_\omega := H_{et}^\omega(X_n^m, \mathbb{Q}_l)$. Then:*

$$dim_{\mathbb{Q}_l} V_\omega = \begin{cases} 0 & \text{if } \omega \neq n \text{ and } \omega \text{ is odd} \\ 1 & \text{if } \omega \neq n \text{ and } \omega \text{ is even} \\ |A_n^m| = \frac{(m-1)^{n+2}-(m-1)}{m} & \text{if } \omega = n \text{ and } \omega \text{ is odd} \\ 1+|A_n^m| = 1+\frac{(m-1)^{n+2}+(m-1)}{m} & \text{if } \omega = n \text{ and } \omega \text{ is even} \end{cases}$$

Moreover, in the case $\omega = n$ one has the descomposition in $1-$dimensional vector spaces:

$$V_n = \left(\oplus_{a \in A_n^m} V_a\right) \oplus \begin{cases} 0 & \text{for } n \text{ odd} \\ \mathbb{Q}_l & \text{for } n \text{ even} \end{cases}$$

And the arithmetic Frobenius of a prime $p \equiv 1 \bmod m$ acts on V_a as multiplication by the Jacobi sum $J(a)$. When n is even the action in the 1-dimensional extra vector space is trivial. If $p \equiv t \bmod m$ then $\rho_l(\mathrm{Frob}_p)(V_a) = V_{ta}$.

Proposition 5.1.3. *If $\sigma \in S_{n+2}$ is a permutation and $a \in A_n^m$, then $J(\sigma(a)) = J(a)$.*

Lemma 5.1.4. *If $a \in A_0^m$, then $J(a) = \pm 1$. If m is odd, it is always equal to 1, and if m is even it is equal to 1 if and only if $p \equiv 1 \bmod 2m$ or a_0 is even.*

Theorem 5.1.5. *Assume $n \geq 2$ and $s, t \geq 1$ with $s + t = n$. Put*

$$A^r_{s,t} := \left\{ (b, c) \in A^r_s \times A^r_t \mid b_{s+1} + c_{t+1} = 0 \right\},$$

and define the maps

$$\begin{aligned} A^r_{s,t} \longrightarrow A^r_n : (b, c) \longrightarrow b\#c := (b_0, \ldots b_s, c_0, \ldots c_t) \\ A^r_{s-1} \times A^r_{t-1} \longrightarrow A^r_n : (b', c') \longrightarrow b' * c' := ((b'_0, \ldots, b'_s, c'_0, \ldots c'_t)). \end{aligned}$$

Then,

i) Let $a \in A^r_n$ and $t \in (\mathbb{Z}/r\mathbb{Z})^\times$ be arbitrary elements, and let σ be the automorphism of $\mathbb{Q}(\zeta)$ defined by $\zeta \longrightarrow \zeta^t$. Then $J(ta) = \sigma(J(a))$.

ii) It has $J(b\#c) = \chi(-1)^{b_{s+1}} J(b) J(c)$.

iii) And $J(b' * c') = qJ(b') J(c')$.

5.2 Jacobi sums

We fix $n \geq 1$, $m \geq 3$ and $p \equiv 1 \bmod m$ if m is odd and $p \equiv 1 \bmod 2m$ if m is even. We say that $a, b \in A^m_n$ are conjugate if up to permutation $a_j + b_j = m$ with $j \in \{0, 1, ..., n+1\}$, and in this case $J(a)$ and $J(b)$ are complex conjugate numbers. For $i \in \left\{1, 2, ..., k = \left\lfloor \frac{m-1}{2} \right\rfloor \right\}$, we define $N_i(a)$ as the number of a_j's equal to i minus the number of a_j's equal to $m - i$. We fix the notation $J_i = J(1, i, m-1-i)$, however, sometimes we do an abuse of notation and we will write $J_{m-1-i} = J_i$, and we set $J_0 = \sqrt{p}$. It is well-known that $J(a)$ can be writen as a product of Jacobi sums (up to p factors and a sign ±1) of elements in A^m_1, [53], [54]. But next lemma is a little bit stronger because it proves that actually is enough with consider the J_i that we have alredy defined.

Lemma 5.2.1. *Given $a \in A^m_n$ there exist integers $b_1, ..., b_k \in \mathbb{Z}$ such that*

$$J(a) = p^{\frac{n - b_1 - \ldots - b_k}{2}} J_1^{b_1} \cdot \ldots \cdot J_k^{b_k}.$$

Proof. Let us first suppose $m = 2k + 1$ is odd. Then, using the relations $ii)$ and $iii)$ in theorem 5.1.5 we will need integers $b_1, ..., b_k$ such that

$$2b_1 + b_2 + \ldots + b_k = N_1(a) \tag{5.1}$$

$$-b1 + b_2 = N_2(a)$$

$$-b2 + b_3 = N_3(a)$$

$$\ldots$$

$$-b_{k-2} + b_{k-1} = N_{k-1}(a)$$

$$-b_{k-1} + 2b_k = N_k(a).$$

Then, we can write

$$b_{k-1} = 2b_k - N_k(a)$$
$$b_{k-2} = 2b_k - N_k(a) - N_{k-1}(a)$$
$$...$$
$$b_2 = 2b_k - N_{k-1}(a) - N_{k-2}(a) - ... - N_3(a)$$
$$b_1 = 2b_k - N_{k-1}(a) - N_{k-2}(a) - ... - N_3 - N_2(a)$$

and if we substitute in (5.1):

$$\sum_{j=1}^{k} jN_j(a) = mb_k,$$

since $\sum_{j=1}^{k} jN_j(a) = \sum_{i=0}^{n+1} a_i \equiv 0 \bmod m$ we get an unique solution with all $b_i \in \mathbb{Z}$.

If $m = 2k+2$ is even, we look for integers $b_1, ..., b_k$ such that

$$2b_1 + b_2 + ... + b_k = N_1(a) \tag{5.2}$$
$$-b1 + b_2 = N_2(a)$$
$$-b2 + b_3 = N_3(a)$$
$$...$$
$$-b_{k-2} + b_{k-1} = N_{k-1}(a)$$
$$-b_{k-1} + b_k = N_k(a)$$
$$b_k \equiv N_{k+1}(a) \bmod 2$$

Then, we can write

$$b_{k-1} = b_k - N_k(a)$$
$$b_{k-2} = b_k - N_k(a) - N_{k-1}(a)$$
$$...$$
$$b_2 = b_k - N_{k-1}(a) - N_{k-2}(a) - ... - N_3(a)$$
$$b_1 = b_k - N_{k-1}(a) - N_{k-2}(a) - ... - N_3(a) - N_2(a)$$

and if we substitute in (5.2):

$$\sum_{j=1}^{k} jN_j(a) = (k+1)b_k,$$

since $\sum_{j=1}^{k} jN_j(a) + (k+1)N_{k+1}(a) = \sum_{i=0}^{n+1} a_i \equiv 0 \bmod (2k+2)$ we get an unique solution with all $b_i \in \mathbb{Z}$ and $b_k \equiv N_{k+1}(a) \bmod 2$. □

Then, we can write

$$J(a) = \pm p^{\frac{n-b_1-\ldots-b_k}{2}} J_1^{b_1} \ldots J_k^{b_k} = \pm p^{\frac{n-b_1-\ldots-b_k}{2}} f_a(J_1, \ldots, J_k)$$

where the sing is computed using lemma (5.1.4) and $f_a \in \mathbb{Z}[x_1, \ldots, x_k]$ is a monomial where the b_i's can be computed from the previous linear system.

Lemma 5.2.2. *For all $i \in \{1, \ldots, k\}$ there exists $a \in A_n^m$ such that $J(a) = \pm p^{\frac{n-1}{2}} J_i$ if n is odd or $J(a) = \pm p^{\frac{n-2}{2}} J_i J_{i+1}$ if $i \neq k$ or J_k^2 when n is even.*

Proof. If n is odd we use the relation $iii)$ of the theorem 5.1.5 and the lemma 5.1.4 for $a = (1, i, m-1-i, 1, m-1, \ldots, 1, m-1)$. If n is even we use the former argument and then we only need to prove the case for $n = 2$. For $i \neq k$ we take $a = (1, i, 1, m-i-2)$ and for $i = k$ we take $a = (1, k, 1, k)$. □

Next lemma is a consequence of the results in [61].

Lemma 5.2.3. *The J_i's, where $i \in \{1, 2, \ldots, k\}$, are nontrivial grössencharakters.*

A grössencharakteres is a character on K in the sense of Hecke, that is a character of the set of fractional ideals of $\mathbb{Q}(\zeta_m)$ that are prime to m,

$$J_i : I_{\mathbb{Q}(\zeta_m)}(m) \longrightarrow \mathbb{C}^*. \tag{5.3}$$

In [61] is also proven that

$$J_i(\mathfrak{a})\mathcal{O}_K = \mathfrak{a}^{\omega((1,i,m-1-i))}$$

where

$$\omega(1, i, m-1-i) := \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} c_t(i) \sigma_{-t}^{-1} =$$

$$= \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} (\left\{\frac{t}{m}\right\} + \left\{\frac{it}{m}\right\} + \left\{\frac{(m-1-i)t}{m}\right\} - 1) \sigma_{-t}^{-1} \tag{5.4}$$

and where $\{\cdot\}$ denotes the fractional part.

However, formula (5.3) is only an equality of ideals, next lemma (theorem 2.1.14, [5]) will be useful for explicity evaluating Jacobi sums.

Lemma 5.2.4. *One has the next congruence modulo $\bar{\mathfrak{p}}$:*

$$J_i(\mathfrak{p}) \equiv (-1)^f \chi_{\mathfrak{p}}^{m+i}(-1) \binom{(i+1)f}{f} \operatorname{mod} \bar{\mathfrak{p}},$$

where $f = \frac{p-1}{m}$.

Theorem 5.2.5. *Given d a positive divisor of m and $l \in \{0, 1, ..., \frac{m}{d} - 2\}$, then we have the equality:*

$$\chi_{\mathfrak{p}}(d^d) J_l(\mathfrak{p}) J_{\frac{m}{d}+l}(\mathfrak{p}) J_{\frac{2m}{d}+l}(\mathfrak{p}) ... J_{\frac{(d-1)m}{d}+l}(\mathfrak{p}) = \chi_{\mathfrak{p}}^{\frac{(d-1)(m-d)}{2}}(-1) J_{dl}(\mathfrak{p}) J_{dl+1}(\mathfrak{p}) ... J_{dl+d-1}(\mathfrak{p}).$$

Proof. We will first prove using relation (5.4) the equality of ideals:

$$J_l(\mathfrak{p}) J_{\frac{m}{d}+l}(\mathfrak{p}) J_{\frac{2m}{d}+l}(\mathfrak{p}) ... J_{\frac{(d-1)m}{d}+l}(\mathfrak{p}) \mathcal{O}_K = J_{dl}(\mathfrak{p}) J_{dl+1}(\mathfrak{p}) ... J_{dl+d-1}(\mathfrak{p}) \mathcal{O}_K.$$

The exponent in which a prime ${}^{\sigma_{-t}^{-1}}\mathfrak{p}$ appear in the left-hand size is:

$$\begin{gathered}
\left\{\frac{t}{m}\right\} + \left\{\frac{lt}{m}\right\} + \left\{\frac{(m-l-1)t}{m}\right\} + \\
+ \left\{\frac{t}{m}\right\} + \left\{\frac{lt}{m} + \frac{t}{d}\right\} + \left\{\frac{(m-l-1)t}{m} - \frac{t}{d}\right\} + \\
\cdots\cdots\cdots \\
+ \left\{\frac{t}{m}\right\} + \left\{\frac{lt}{m} + \frac{(d-1)t}{d}\right\} + \left\{\frac{(m-l-1)t}{m} - \frac{(d-1)t}{d}\right\} = \\
d\left\{\frac{t}{m}\right\} + \left\{\frac{dlt}{m}\right\} + \frac{d-1}{2} + \left\{\frac{d(m-l-1)t}{m}\right\} + \frac{d-1}{2},
\end{gathered}$$

while in the right-hand size:

$$\begin{gathered}
\left\{\frac{t}{m}\right\} + \left\{\frac{dlt}{m}\right\} + \left\{\frac{(m-dl-1)t}{m}\right\} + \\
+ \left\{\frac{t}{m}\right\} + \left\{\frac{(dl+1)t}{m}\right\} + \left\{\frac{(m-dl-2)t}{m}\right\} + \\
\cdots\cdots\cdots \\
+ \left\{\frac{t}{m}\right\} + \left\{\frac{(dl+d-1)t}{m}\right\} + \left\{\frac{(m-dl-d)t}{m}\right\} = \\
d\left\{\frac{t}{m}\right\} + d - 1 + \left\{\frac{dlt}{m}\right\} + \left\{\frac{d(m-l-1)t}{m}\right\},
\end{gathered}$$

since the second term in each row and the third in the one above sum 1. And then both ideals are equal.

Now we use lemma (5.2.4) for computing the equality in the statement of the theorem. The left-hand size is congruent modulo $\bar{\mathfrak{p}}$ with:

$$d^{df}(-1)^{df} \chi_{\mathfrak{p}}^{dm+dl+\frac{m}{d}\frac{d(d-1)}{2}}(-1) \binom{(l+1)f}{f} \cdots \binom{(\frac{d-1}{d}m + l + 1)f}{f} \equiv$$

$$d^{df}(-1)^{df}\chi_{\mathfrak{p}}^{dm+dl+\frac{m}{d}\frac{d(d-1)}{2}}(-1)\frac{1}{(f!)^d}\frac{((l+1)f)!}{(lf)!}\frac{((\frac{m}{d}+l+1)f)!}{((\frac{m}{d}+l)f)!}\cdots\frac{((\frac{(d-1)m}{d}+l+1)f)!}{((\frac{(d-1)m}{d}+l)f)!}\equiv$$

$$(-1)^{df}\chi_{\mathfrak{p}}^{dm+dl+\frac{m}{d}\frac{d(d-1)}{2}}(-1)\frac{d^{df}}{(f!)^d}\frac{((l+1)f)!}{(lf)!}\frac{(\frac{p-1}{d}+(l+1)f)!}{(\frac{p-1}{d}+lf)!}\cdots\frac{(\frac{(d-1)(p-1)}{d}+(l+1)f)!}{(\frac{(d-1)(p-1)}{d}+lf)!}\equiv$$

$$(-1)^{df}\chi_{\mathfrak{p}}^{dm+dl+\frac{m}{d}\frac{d(d-1)}{2}}(-1)\frac{d^{df}}{(f!)^d}\frac{((l+1)f)!}{(lf)!}\frac{(\frac{-1}{d}+(l+1)f)!}{(\frac{-1}{d}+lf)!}\cdots\frac{(-\frac{(d-1)}{d}+(l+1)f)!}{(-\frac{(d-1)}{d}+lf)!}\equiv$$

$$(-1)^{df}\chi_{\mathfrak{p}}^{dm+dl+\frac{m}{d}\frac{d(d-1)}{2}}(-1)\frac{1}{(f!)^d}\frac{((dl+d)f)!}{(dlf)!}\equiv$$

$$(-1)^{df}\chi_{\mathfrak{p}}^{dm+dl+\frac{m}{d}\frac{d(d-1)}{2}}(-1)\binom{(dl+1)f}{f}\cdots\binom{(dl+d)f}{f},$$

that is just the right-hand size of the equality of the theorem. □

Remark 5.2.6. *For $d=1$ and $d=m$ we just get $J_l(\mathfrak{p})=J_l(\mathfrak{p})$ for all $l=0,...,k$. For considering all these relations for the different divisors d is enough with taken d equal to the different primes that divide m.*

Given a grössencharakter $J: I_{\mathbb{Q}(\zeta_m)}(m)\longrightarrow\mathbb{C}^*$ we can see the unitarized character $X:=\frac{J}{|J|}: I_{\mathbb{Q}(\zeta_m)}(m)\longrightarrow \mathrm{U}(1)$ as a random variable from the set of prime ideals of $\mathbb{Q}(\zeta_m)$ not dividing m on the unitary group $\mathrm{U}(1)$.

Next lemma gives the distribution of this random variables. It is corollary 1.9 in [16] and it is a consequence of the Tauberian theorem of Wiener-Ikehara, [48] and of the theorem of Hecke that states that the L−function of a nontrivial Hecke character if holomorphic and does not vanish for $\Re(s)\geq 1$, [30].

Lemma 5.2.7. *For a nontrivial grossencharacter J, the $X(\mathfrak{p}):=\frac{J(\mathfrak{p})}{|J(\mathfrak{p})|}$ are $\mu-$equidistributed on $U(1)$, where μ is the Haar measure on $U(1)$.*

Remark 5.2.8. *At most there can be $\phi(m)/2$ independent random variables among the k characters $X_i(\mathfrak{p})=\frac{J_i(\mathfrak{p})}{|J_i(\mathfrak{p})|}$ for $i\in\{1,2,...,k\}$, because $|(\mathbb{Z}/m\mathbb{Z})^\times|=\phi(m)$ and $c_t(i)+c_{m-t}(i)=1$ for all $i\in\{1,2,...,k\}$ and $t\in(\mathbb{Z}/m\mathbb{Z})^\times$. Notice, that in fact, the rank of the matrix $C:=\{c_t(i)\}i,t=1..k,(t,m)=1$ plus 1 is equal to r, the number of independent random variables among the characters X_i. At the end of the appendix we show these matrix for $m=5,...,25$.*

Definition 5.2.9. *We say that a natural number $m\geq 3$ is maximal if $r=\phi(m)/2$. And we say that m good if we can choose r of the characters X_i: $X_{i_1},...,X_{i_r}$ such that the rows of the matrix C are integer linear combination of the rows $C(i_1),...,C(i_r)$, so we can write $X_i=\Psi_i X_{i_1}^{\beta_1}...X_{i_r}^{\beta_r}$ for some $\beta_i\in\mathbb{Z}$ and Ψ_i an order m character.*

Remark 5.2.10. *If m is a prime number and is maximal then it is good. And if p is a prime that is maximal, then $2p$ is maximal and good by theorem (5.2.5) with $d = 2$.*

Example 5.2.11. *Let us take $m = 6$, then, see table for $m = 6$ at the end of the appendix, we have $J_1\mathcal{O}_K = J_2\mathcal{O}_K$, so $r = \phi(m)/2$ and 6 is a maximal number and a good number. Now we can apply theorem (5.2.5) with $d = 2$ and we get: $J_2(\mathfrak{p}) = \chi(-4)J_1(\mathfrak{p})$.*

Example 5.2.12. *Let us take $m = 9$, then, see table for $m = 9$ at the end of the appendix, we get that there are $3 = \phi(9)/2$ independent random variables: J_1, J_2 and J_4, and we have $J_1\mathcal{O}_K = J_3\mathcal{O}_K$. We apply theorem (5.2.5) with $d = 3$ and we get: $J_1(\mathfrak{p}) = \chi(3^3)J_3(\mathfrak{p})$.*

Conjecture 5.2.13. *Every natural number $m \geq 3$ is maximal and good. And all the characters Ψ_i in definition (5.2.9) have the form $\chi_{\mathfrak{p}}(N_i)$ for some $N_i \in \mathbb{Z}$.*

We checked using magma that until $m = 1000$ every natural number is *maximal.*

Some evidences of the conjecture (5.2.13).

1. Every $m \geq 3$ is maximal: the cases already proven and the shape of the matrix $C = \{c_t(i)\}$, see these matrices at the end of the appendix for $m = 5, ..., 25$. Moreover, we expect that all the relations among the J_i come from theorem (5.2.5).For each prime q dividing m we get aproximately $\frac{m}{2q}$ relations (notice that $J_i = J_{m-i-1}$) and we would need $k - \frac{\phi(m)}{2} \sim \frac{1}{2}(m - \phi(m)) = \frac{m}{2}(1 - \prod \frac{q-1}{q}) \sim \frac{m}{2}\sum\frac{1}{q}$ relations.

2. Every $m \geq 3$ is good: if $J_i^n = \prod_1^r J_{i_s}^{a_s}$ it seems natural to figure out that $n \mid a_s$ and then $J_i = \Psi\prod_1^r J_{i_s}^{a_s/n}$ for some character that could be computed using lemma (5.2.4).

3. The character Ψ_i in definition (5.2.9) have the form $\chi_{\mathfrak{p}}(N_i)$ for some $N_i \in \mathbb{Z}$ if effectively all the relations among the J_i come from the ones described in theorem (5.2.5).

4. If m is prime the conjecture agrees with the results in [17].

If m is *good* we fix next notation. Let us call I_s for $s \in \{1, ..., r\}$ to r of the J_i that are independent and generate the others. Then there will be exist monic monomials $h_i \in \mathbb{Z}[x_1, ..., x_r]$ such that $J_i = h_i(I_1, ..., I_r)$. Then, given any $a \in A_n^m$ one has

$$J_a = f_a(J_1, ..., J_k) = f_a(h_1(I_1, ..., I_r), ..., h_k(I_1, ..., I_r)) = g_a(I_1, ..., I_r).$$

We define

$$B_n^m = \begin{cases} A_n^m \text{ if } n \text{ is odd} \\ A_n^m \cup \mathbf{0} \text{ if } n \text{ is even} \end{cases}$$

where $\mathbf{0} = (0, .., 0)$ and put $J_{\mathbf{0}} = g_{\mathbf{0}}(I_1, ..., I_{\phi(m)/2}) = p^{n/2}$.

5.3 Sato-Tate groups

Given a prime l and a number field k over which X_n^m is defined, the Sato-Tate group $\mathrm{ST}_k(X_n^m)$ is defined ([16], [51]) as a maximal compact subgroup of $G_l^1 \otimes_\iota \mathbb{C}$ where $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$ is an embedding and G_l^1 is the Zariski clousure of $\rho_l(G_k1)$, where G_k^1 is the kernel of the of the $l-$adic cyclotomic character in $G_k = \mathrm{Gal}(\bar{k}/k)$ and ρ_l is the Galois representation

$$\rho_l : G_k \longrightarrow \mathrm{Aut}(H_{et}^n(X_n^m, \mathbb{Q}_l)) \subseteq GL_d(\mathbb{Q}_l),$$

where $d = dim_{\mathbb{Q}_l}(H_{et}^n(X_n^m, \mathbb{Q}_l))$.

Let $\mathfrak{p}$ be a prime of k lying over a prime number p. For equidistribution results we can forget a finite number of primes, so we can assume that p is not ramified. Moreover, the set of primes in k such that the prime in $\mathbb{Q}$ over it lies has inert degree different from 1, has density zero. Hence, we can assume $\mathfrak{p}$ is completly splitting. If $k = \mathbb{Q}(\zeta_m)$, the a prime $\mathfrak{p}$ is completly splitting if and only if $p \equiv 1 \bmod m$. Therefore, we can use the results in the last sections for computing the image of the Frobenius element $Frob_{\mathfrak{p}}$ (the inverse of the geometric Frobenius) by the representatioln ρ_l for a prime $l \equiv 1 \bmod m$.

Proposition 5.3.1. *The following Sato-Tate groups are isomorphic:*

$$\mathrm{ST}_{\mathbb{Q}}(X_n^m) \simeq \mathrm{ST}_{\mathbb{Q}}(X_n^m).$$

Proof. By lemma (5.2.2) we have the isomorphism over $\mathbb{Q}(\zeta_m)$. Now, applying last part of theorem (5.1.2) and proposition (11.4) in [7] we get:

$$\mathrm{ST}_{\mathbb{Q}}(X_n^m) \simeq \mathrm{ST}_{\mathbb{Q}(\zeta_m)}(X_n^m) \rtimes \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq \mathrm{ST}_{\mathbb{Q}(\zeta_m)}(X_1^m) \rtimes \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq \mathrm{ST}_{\mathbb{Q}}(X_n^m).$$

□

Proposition 5.3.2. *If m is good, then the connected component $(\mathrm{ST}_{\mathbb{Q}}(X_n^m))_0$ is isomorphic to:*

$$(\mathrm{ST}_{\mathbb{Q}}(X_n^m))_0 \simeq \mathrm{U}(1)^r.$$

More precisely, as a subgroup of USp_d or O_d, it is conjugated to

$$\left\{ diag((g_a(\theta_1, ..., \theta_r))_{a \in B_n^m}) | \theta_i \in S^1 \right\}.$$

.

Proof. By theorem (5.1.2) and lemma (5.2.7), the Zariski clousure of G_l^1 is

$$G_l^{1,Zar} = \left\{ diag((g_a(x_1, ..., x_r))_{a \in B_n^m}) | x_i \in \mathbb{Q}_l^*,\ x_i \bar{x}_i = 1 \right\}$$

A maximal compact subgroup of $G_l^{1,Zar} \otimes_{\mathbb{Q}_l} \mathbb{C}$ is given by

$$\left\{ diag((g_a(\theta_1, ..., \theta_r))_{a \in B_n^m}) | \theta_i \in S^1 \right\}.$$

And lemma 5.2.2 ensure that all the θ_i appear. □

Proposition 5.3.3. *If conjecture (5.2.13) holds and all the characters in definition (5.2.9) come from the relations in theorem (5.2.5), then:*

$$\mathrm{ST}_{\mathbb{Q}}(X_n^m) \simeq \mathrm{U}(1)^r \rtimes \mathrm{Gal}(L/\mathbb{Q})$$

where $L = K(\sqrt[m]{(-1)^{\frac{(q-1)(m-q)}{2}} q^q} : q \mid m \text{ and } \frac{m}{q} > 2)$ *and* $K = \mathbb{Q}(\zeta_m)$ *if* m *is odd and* $K = \mathbb{Q}(\zeta_{2m})$ *if* m *is even. Moreover* $r = \phi(m)/2$*. More precisely,*

$$\mathrm{ST}_{\mathbb{Q}}(X_n^m) \simeq (\mathrm{U}(1)^r \times \prod_{q|m,\, \frac{m}{q}>2} C_{\frac{m}{q}}) \rtimes \mathrm{Gal}(K/\mathbb{Q}).$$

Proof. First we will prove that the minimal field L over which $\mathrm{ST}_L(X_n^m)$ is connected is the one given in the statement of the proposition. Notice that $K \subset L$ by theorem (5.1.2) and lemma (5.1.4). Then, for $\mathrm{ST}_L(X_n^m)$ to be connected with $K \subset L$, we need $\chi_{\mathfrak{p}}(q^q) = 1$ for all primes $q \mid m$ and such that $\frac{m}{q} > 2$ (see theorem (5.2.5)) and for all primes $\mathfrak{p}$ that lie over a prime p that is completely splitting in L. The minimal field extension $L/\mathbb{Q}(\zeta_m)$ such that all the primes p that are completly splitting satisfy $q^{q\frac{p-1}{m}} \equiv 1 \bmod p$ is that one in which q is a m/q–th power. Then L is the one specified above and we have:

$$\mathrm{ST}_K(X_n^m) \simeq \mathrm{U}(1)^r \times \prod_{q|m,\, \frac{m}{q}>2} C_{\frac{m}{q}}.$$

Finally, proposition (11.4) in [7] implies:

$$\mathrm{ST}_{\mathbb{Q}}(X_n^m) \simeq \mathrm{ST}_K(X_n^m) \rtimes \mathrm{Gal}(K/\mathbb{Q}).$$

□

Notice that even in the case in which conjecture (5.2.13) does not hold we can compute the Sato-Tate group of any Fermat hypersurface $X_n^m : x_0^m + ... + x_{n+1}^m = 0$ using the results in previous sections. For computing the Sato-Tate group $\mathrm{ST}_{\mathbb{Q}(\zeta_m)}(X_n^m)$ we just have to use theorem (5.1.2) of Deligne that describes the action of the arithmetic Frobenius on $H_{et}^1(X_n^m, \mathbb{Q}_l)$ via Jacobi sums. And then apply lemmas (5.1.5) and (5.2.4) and relation (5.4) for computing all the relation among the Jacobi sums. Finally, for computing $\mathrm{ST}_{\mathbb{Q}}(X_n^m)$ we can just apply last part of theorem (5.1.2) that is proposition (11.4) in [7]. In section (5.5) we show an example of the computation of the Sato-Tate groups of the Fermat hypersurfaces X_1^6 and X_2^6.

Moreover, from the computation of the Sato-Tate groups via the method described above and when the conjecture holds, see next section, it is easy to compute the Sato-Tate distributions for the Fermat hypersurfaces X_n^m. In section (5.5) we show also an example of how to compute the Sato-Tate distributions.

5.4 Proof of the conjecture

First at all, notice that the Sato-Tate conjecture for the Fermat hypersurfaces X_n^m with $n = 1$ follows by proposition (4.1.1) due to Johansson, [34], and the fact that the Jacobian of a Fermar curve X_1^m is isogenous to the product of some simple abelian varieties with complex multiplication, [36], [47], [52].

Theorem 5.4.1. *The Generalized Sato-Tate Conjecture holds for the Fermat curves* $X_1^m : x_0^m + x_1^m + x_2^m = 0$ *over* $\mathbb{Q}$.

But we can provide another proof, if we consider X_1^m defined over $\mathbb{Q}(\zeta_m)$, that is generalizable for $n \geq 1$ when m is a *good* number, see definition (5.2.9).
Proof. If m is good then the equidistribution part of the conjecture over $\mathbb{Q}(\zeta_m)$ holds by the description of the Sato-Tate group done in previous section and lemma (5.2.7). Moreover we have that the algebraic Sato-Tate conjecture holds since we have write $G_l^{1,Zar}$ as an algebraic group, then by the remark in definition 2.4 in [2] we get the independence on the prime l. □

Corollary 5.4.2. *If m is a good number then the generalize Sato-Tate conejcture holds for the Fermat hypersurfaces* $X_n^m/\mathbb{Q}(\zeta_m)$.

5.5 An example

Let us consider first the case with $n = 1$ and $m = 6$. Then $X_1^6 : x_0^6 + x_1^6 + x_2^6 = 0$ is a genus 10 curve. We will compute the Sato-Tate group $\mathrm{ST}_{\mathbb{Q}}(X_1^6)$ and we will check that in this case the Munford-Hodge conjecture and the Algebraic Sato-Tate conjecture hold for it.

We have that the dimension $\dim(\mathrm{H}^1_{\mathrm{et}}(X_1^6, \mathbb{Q}_l)) = 20$ and we have that:

$$\begin{aligned} A_1^6 = \{ & a_1 = (1,1,4),\ a_3 = (1,4,1),\ a_5 = (4,1,1),\\ & a_7 = (1,2,3),\ a_9 = (1,3,2),\ a_{11} = (2,1,3), a_{13} = (2,3,1),\ a_{15} = (3,1,2), a_{17} = (3,2,1),\\ & a_{19} = (2,2,2),\ a_{20} = (4,4,4),\\ & a_8 = (5,4,3),\ a_{10} = (5,3,4),\ a_{12} = (4,5,3),\ a_{14} = (4,3,5),\ a_{16} = (3,5,4),\ a_{18} = (3,4,5),\\ & a_2 = (5,5,2),\ a_4 = (5,2,5),\ a_6 = (2,5,5)\} \end{aligned}$$

Applying theorem 5.1.5, we have: $J(a_0,a_1,a_2) = J(\sigma(a_0,a_1,a_2))$ for all $\sigma \in S_3$ and if $J_1 = J(1,1,4)$ and $J_2 = J(1,2,3)$, we have $J(2,2,2) = \chi(-1)J_2^2J_1^{-1}$ where χ is a character of $\mathbb{F}_p^\times$ of exact order 6, so $\chi(-1) = 1$ if $p \equiv 1 \bmod 12$ and $\chi(-1) = -1$ if $p \equiv 7 \bmod 12$. Now, example (5.2.11) gives us $J_2 = \chi(-4)J_1$. Then,

$$\mathrm{ST}_{\mathbb{Q}(\zeta_6)}(X_1^6) = \{\mathrm{diag}((\theta,\bar{\theta})_3, (\pm\zeta_6^a\theta, \pm\zeta_6^{-a}\bar{\theta})_6, \pm\zeta_6^{2a}\theta, \pm\zeta_6^{-2a}\bar{\theta}) \mid \theta \in S_1,\, a \in \{0,2,4\}\} \simeq$$

$$\simeq \mathrm{U}(1) \times C_2 \times C_3 \subseteq \mathrm{Sp}_{20}(\mathbb{Q}_l).$$

This group is symplectic with respect to the matrix $J = (J_2)_{10}$ where $J_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. We will see that the minimal field L over which the Sato-Tate group is connected is $\mathbb{Q}(\zeta_{12}, \sqrt[3]{2})$. As in the proof of proposition (5.3.3) and by lemma (5.2.5) we get $a = 0$ if and only if $\chi(4) = \chi^2(2) = 1$, that is, if 2 is a cube modulo p, because χ has exact order 6. And 2 is a cube modulo p, if and only if p is completly split in $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$. If we joint the condition $p \equiv 1 \bmod 12$, for getting $\chi(-1) = 1$, we get that the minimal field L over which $\mathrm{ST}_L(X_1^6)$ is connected is $L = \mathbb{Q}(\zeta_{12}, \sqrt[3]{2}) = \mathbb{Q}(i, \zeta_3, \sqrt[3]{2})$, hence

$$\mathrm{ST}_{\mathbb{Q}(\zeta_{12}, \sqrt[3]{2})}(X_1^6) = \{\mathrm{diag}((\theta,\bar{\theta})_{10}) \mid \theta \in S_1\} \simeq \mathrm{U}(1) \subseteq \mathrm{Sp}_{20}(\mathbb{Q}_l),$$

where we have $\phi(6)/2 = 1$ copies of U(1).

For computing the Sato-Tate group over $\mathbb{Q}$, we fix a basis $\{v_1, v_2, ..., v_{20}\}$ of $\mathrm{H}^1_{\mathrm{et}}(X_1^6, \mathbb{Q}_l)$ such that $v_i \in V_{a_i}$ as in theorem 5.1.2 and such that in this basis the Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(\mathrm{H}^1_{\mathrm{et}}(X_1^6, \mathbb{Q}_l)) \subseteq \mathrm{Sp}_{20}(\mathbb{Q}_l)$ is symplectic respect to the matrix J. Then, for computing $\mathrm{ST}_{\mathbb{Q}}(X_1^6)$ is enough to compute the image by ρ of an element $\tau \in \mathrm{Ker}(\chi_l)$ such that $\tau(\zeta_3) \neq \zeta_3$. By theorem 5.1.2, we have:

$$\rho(\tau) = \begin{pmatrix} 0 & \eta_2 & & & \\ \eta_1 & 0 & & & \\ & & \ddots & & \\ & & & 0 & \eta_{20} \\ & & & \eta_{19} & 0 \end{pmatrix},$$

and since it has to be symplectic with respect to the matrix J we have $\eta_{2i} = -\bar{\eta}_{2i-1} \in \mathrm{U}(1)$ for all $i \in \{1, ..., 10\}$. So, finally, $\mathrm{ST}_{\mathbb{Q}}(X_1^6) \simeq \mathrm{U}(1) \times C_2 \times S_3$. And for this Sato-Tate group we have:

$$\det(T \cdot Id - \rho(Frob_p)) =$$

$$\begin{cases} (T^2 - (\theta+\bar{\theta})T + 1)^3(T^2 - \chi(-1)(\chi(4)\theta + \bar{\chi}(4)\bar{\theta})T + 1)^6(T^2 - \chi(-1)(\chi^2(4)\theta + \bar{\chi}^2(4)\bar{\theta})T + 1) & \text{if} \quad p \equiv 1 \bmod 6 \\ (T^2+1)^{10} & \text{if} \quad p \equiv 5 \bmod 6 \end{cases}$$

Notice that if $\theta = \cos(2\pi r) + i\sin(2\pi r)$ then $\theta + \bar{\theta} = 2\cos(2\pi r)$ and $\zeta_3^a\theta + \zeta_3^{-a}\bar{\theta} = \cos(2\pi r - a\frac{2\pi}{3})$ with $a = \pm 1$. Then, by Chebotarev's density theorem we can compute the $n-$th moment of the trace as follows:

$$\mathrm{M}_n(a_1) = \frac{-1}{12}\sum_{a=0}^{2}\int_0^1 \Big[(6\cos(2\pi r) + 12\cos(2\pi r + a\frac{2\pi}{3}) + 2\cos(2\pi r - a\frac{2\pi}{3}))^n$$

$$+(6\cos(2\pi r) - 12\cos(2\pi r + a\frac{2\pi}{3}) - 2\cos(2\pi r - a\frac{2\pi}{3}))^n\Big]\,\mathrm{d}\,r.$$

We can compute in a similar fashion the moment sequence of the other random variables a_i with $i \in \{1, ..., 10\}$. We only have to expand the above polynomials and integrate the corresponding terms.

We can compute the Sato-Tate group, following a different approach, as in subsection (4.2).

Lemma 5.5.1. *The jacobian of the Fermat curve* $X_1^6 : x_0^6 + x_1^6 + x_2^6 = 0$ *is isogenous over* $\mathbb{Q}$ *to the next product of elliptic curves:*

$$\mathrm{Jac}(X_1^6) \sim_{\mathbb{Q}} E_1^6 \times E_2^3 \times E_3,$$

where

$$E_1 : y^2 = x^3 - 1,\ E_2 : y^2 = x^3 - 4,\ E_3 : y^2 = 4x^3 + 1.$$

Those elliptic curves are isomorphic to the first one and all of them have complex multiplication by $\mathbb{Q}(\sqrt{-3})$. *In particular, the endomorphism algebra* $\mathrm{End}_0(\mathrm{J}(X_1^6)) := \mathrm{End}(\mathrm{J}(X_1^6))\otimes\mathbb{Q} \simeq \mathrm{GL}_3(\mathbb{Q}(\sqrt{-3}))$ *and it is defined over* $\mathbb{Q}(\zeta_{12}, \sqrt[3]{2})$.

Proof. Let us consider the morphisms:

$$X_1^6 \to E_1 : (x : y : z) \to (-x^2 z : y^3 : z^3),$$

$$X_1^6 \to E_2 : (x : y : z) \to (xyz^4 : 2x^6 + z^6 : x^3y^3),$$

$$X_1^6 \to E_3 : (x : y : z) \to (-x^2y^2z^2 : 2x^6 + z^6 : z^6).$$

Now it is easy to check that the pullback of the regular differential of each of these elliptic curves by these morphism and the ones coming from permuting the variables x, y, z generate the full vector space $\Omega^1(X_1^6)$. We can check it for example with magma, [6]:

```
R<x,y,z>:=ProjectiveSpace(Rationals(),2);
F:=x^6+y^6+z^6;
C:=Curve(R,F);
G:=y^2*z-x^3+z^3;
```

```
E:=Curve(R,G);
phi:=map<C->E|[-x^2*z,y^3,z^3]>;
Omega:=BasisOfHolomorphicDifferentials(E)[1];
W:=Pullback(phi,Omega);
W;
```

And we have the isomorphisms:

$$\phi_2 : E_2 \to E_1 : (x,y) \to (x/\sqrt[3]{4}, y/2),$$

$$\phi_3 : E_3 \to E_1 : (x,y) \to (\sqrt[3]{4}x, iy),$$

and we fix $\phi_1 = id : E_1 \to E_1$. □

It is easy to check as in (4.2) that the two components of the Lefschetz group of E_1 are:

$$\mathrm{L}(E_1,1) = \left\{ \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix} \mid a^2+b^2-ab=1,\ a,b\in\mathbb{R} \right\},$$

$$\mathrm{L}(E_1,\tau) = \left\{ \begin{pmatrix} ia & ib \\ ib-ia & -ia \end{pmatrix} \mid a^2+b^2-ab=1,\ a,b\in\mathbb{R} \right\}.$$

If we conjugate by the matrix $\mathcal{M} = \begin{pmatrix} -\zeta_3^2 & 1 \\ 1 & -\zeta_3 \end{pmatrix}$, we get:

$$\mathcal{M}\,\mathrm{ST}_{\mathbb{Q}}(E_1,1)\mathcal{M}^{-1} = \left\{ \begin{pmatrix} \theta & 0 \\ 0 & \bar\theta \end{pmatrix} \mid \theta\in S^1 \right\},\ \mathcal{M}\,\mathrm{ST}_{\mathbb{Q}}(E_1,\tau)\mathcal{M}^{-1} = \left\{ \begin{pmatrix} 0 & -\bar\theta \\ \theta & 0 \end{pmatrix} \mid \theta\in S^1 \right\}.$$

Hence, we can take:

$$\mathrm{ST}_{\mathbb{Q}}(E_1^{10}) = \left\{ \begin{pmatrix} \theta & 0 \\ 0 & \bar\theta \end{pmatrix}_{10}, \begin{pmatrix} 0 & -\bar\theta \\ \theta & 0 \end{pmatrix}_{10} \mid \theta\in S^1 \right\}.$$

We have that $\mathrm{J}(X_1^6)$ is isogenous over $\mathbb{Q}$ to a twists of E_1^{10}. And by corolary 4.1 in [2] we have that the Mumford-tate conjecture holds for $\mathrm{J}(X_1^6)$. Then we are under the hypothesis in theorem 6.1 in [2] so by remark 6.2 also in [2] we have that the algebraic Sato-Tate conjecture holds for $\mathrm{J}(X_1^6)$ with $\mathrm{AST}_{\mathbb{Q}}(\mathrm{J}(X_1^6)) = \mathrm{L}(\mathrm{J}(X_1^6))$. Then we have:

$$\mathrm{ST}_{\mathbb{Q}}(\mathrm{J}(X_1^6)) = \mathrm{ST}_{\mathbb{Q}}(E_1^{10})\iota(H),$$

where $H = \xi(\mathrm{Gal}(\mathbb{Q}(i,\zeta_3,\sqrt[3]{2})/\mathbb{Q}(\zeta_3)))$, here $\xi_\sigma = \phi^\sigma\phi^{-1}$ stands for the cocycle associated to the twists:

$$\phi = ((\phi_1)_3, (\phi_2)_6, \phi_3) : E_1^3 \times E_2^6 \times E_3 \longrightarrow E_1^{10},$$

and

$$\iota : \mathrm{Aut}(E_1^{10}) \to \mathrm{End}(E_1^{10}) \to \mathrm{GL}_{10}(\mathbb{Q}(\sqrt{-3})) \to \mathrm{GL}(T_l(E_1^{10})) = \mathrm{GL}_{10}(T_l(E_1)) \subseteq \mathrm{Sp}_{20}(\mathbb{Q}_l)$$

is given by the composition of the natural previous morphisms and where the third one is defined by:

$$1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sqrt{-3} \to \begin{pmatrix} -1 & -2 \\ 2 & 1 \end{pmatrix}.$$

Then we obtain the same Sato-Tate group previously computed. The advantage of the first method is that allows us to compute the Sato-Tate groups of all the Fermat hypersurfaces X_n^6. So, for example, for $n = 2$ we have that the dimension $\dim(\mathrm{H}^1_{\mathrm{et}}(X_2^6, \mathbb{Q}_l)) = 106$ and up to permutation the jacobi sums that appear are:

$$J(1,1,1,3) = \chi(-4)J_1^2, \ J(5,5,5,3) = \bar{\chi}(-4)\bar{J}_1^2$$
$$J(1,1,2,2) = \chi(-1)\chi^2(-4)J_1^2 \ J(5,5,4,4) = \bar{\chi}(-1)\bar{\chi}^2(-4)\bar{J}_1^2$$
$$J(1,1,5,5) = 1$$
$$J(1,2,4,5) = \chi(-1)$$
$$J(2,2,3,5) = \chi(-4) \ J(4,4,3,1) = \bar{\chi}(-4)$$
$$J(2,2,4,4) = 1$$
$$J(2,3,3,4) = \chi(-1)$$
$$J(1,3,3,5) = 1$$
$$J(3,3,3,3) = 1$$
$$J(0,0,0,0) = 1$$

And then, we have:

$$\mathrm{ST}_{\mathbb{Q}(\zeta_6)}(X_2^6) = \{\mathrm{diag}((\theta,\bar{\theta})_4, (\pm\zeta_6^a\theta, \pm\zeta_6^{-a}\bar{\theta})_6, (\zeta_6^a, \zeta_6^{-a})_{12}, (\pm 1)_{36}, (1)_{26}) \mid \theta \in S_1, \ a \in \{0,2,4\}\} \simeq$$
$$\simeq \mathrm{U}(1) \times C_2 \times C_3.$$

Notice that this time we can see the Sato-Tate group like a subgroup of the orthogonal group $\mathrm{O}_{53}(\mathbb{Q}_l)$ if we do the change of basis that send the blocks:

$$\mathrm{diag}(\theta,\bar{\theta}) \to \begin{pmatrix} \cos(2\pi r) & \sin(2\pi r) \\ -\sin(2\pi r) & \cos(2\pi r) \end{pmatrix},$$

where $\theta = \cos(2\pi r) + i\sin(2\pi r)$ and

$$\mathrm{diag}(\pm\zeta_6^a\theta, \pm\zeta_6^{-a}\bar{\theta}) \to \pm \begin{pmatrix} \cos(2\pi r + \frac{2\pi}{3}) & \sin(2\pi r + \frac{2\pi}{3}) \\ -\sin(2\pi r + \frac{2\pi}{3}) & \cos(2\pi r + \frac{2\pi}{3}) \end{pmatrix},$$

$$\mathrm{diag}(\zeta_6^a, \zeta_6^{-a}) \to \begin{pmatrix} \cos(\frac{2\pi}{3}) & \sin(+\frac{2\pi}{3}) \\ -\sin(\frac{2\pi}{3}) & \cos(\frac{2\pi}{3}) \end{pmatrix}.$$

Appendix

The method described in chapter 1 for computing the twists of curves is not completely explicit in the sense that we need to solve a Galois emebdding problem for each fixed curve. And there is not known method for computing these solutions.

In this apendix we show an approach for computing such solutions. Instead of trying to solve the Galois embedding problem:

$$\begin{tikzcd}
 & G_k \arrow[dl, dashed, "\Psi"'] \arrow[d] & \\
\Gamma \arrow[r, "\pi"'] & \mathrm{Gal}(K/k) \arrow[r] & 1
\end{tikzcd} \tag{5.5}$$

we can try to solve the Inverse Galois problem $\mathrm{Gal}(L/k) \simeq G$ for each subgroup G of Γ such that $[G : G \cap \mathrm{Ker}(\pi)] =\mid \mathrm{Gal}(K/k) \mid$ and then check what of these solutions provide also a solution to (5.5). Neither there exists an algorithm for solving inverse Galois problems, but this problem has been more considerably studied. Here, we show a correspondence that can be useful in general for solving these problems. We establish a correspondence between the solutions to a given Galois inverse problem and the set of rational points of a certain variety that we show how to built.

Inverse Galois problems

The Inverse Galois problem, first proposed in the 19th century, is still unsolved, (see [33] for a classical introduction to the subject):

Inverse Galois problem (IGP): *"given a finite group G, determine when there exists a Galois finite extension $K/\mathbb{Q}$ such that is Galois group $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$".*

The expected answer is: always. E. Noether deeply studied the problem and formulated it in the following terms:

Noether problem (NP): *"Let $M = \mathbb{Q}(x_1, ..., x_n)$ be the field of rational functions in n indeterminates. The symmetric group S_n acts on M by permuting the indeterminates. Let G be a transitive subgroup of S_n, and let $K = ^G M$ be the subfield of $G-$invariant rational functions of M. Is K a rational extension of $\mathbb{Q}$? I.e., is K isomorphic to a field of rational functions over $\mathbb{Q}$?".*

Roughly speaking, the Noether problem ask for the existence of a generic polynomial given by parameters such that parametrizes all the extensions over $\mathbb{Q}$ such that its Galois group is isomorphic to G. Clearly, if the Noether Problem has an affirmative answer, G can be realised as a Galois group over $\mathbb{Q}$, and in fact over any Hilbertian field of characteristic 0, such as a number field. However a negative answer does not imply a negative one for the (IGP). For example, it is known that the (NP) has a negative answer for the cyclic group C_8, while the answer to the (IGP) is affirmative by the Kroneker-Weber theorem. Some groups for which (IGP) has been studied:

- for abelian groups (Kroneker-Weber),
- symmetric and alternate groups (Hilbert),
- $p-$ groups with p an odd prime (Reichardt, Scholz),
- solvable groups (Shafarevic), however in this case the proof is not constructive,
- four of the Mathieu groups (Matzat & Al.)
- the monster group (Thompsom) and
- some linear groups (Arias-de-Reyna, Belyi, Dieulefait, Malle, Matzat, Shih, Vila, Wiese...).

The Noether's strategy is based on invariant theory, she looks for invariants of polynomials whose splitting field has Galois groups isomorphic to the finite group G given. On the other hand, we will attack the problem via a different perspective. We study the relations that should satisfy the coefficients of a polynomial for having G as the Galois groups of its splitting field.

The algorithm

Let G be a finite group, and let n be an integer such that there exists an embedding $G \hookrightarrow S_n$, with the property that the image is a transitive subgroup of S_n. The algorithm will be more efficient as we take n smaller as we can. From now on, we will see all the groups G like transitive subgroups of permutations of some S_n. Let us consider the polynomial:

$$P(x) = x^n - s_1x^{n-1} + s_2x^{n-2} + ... + (-1)^n s_n \in L := \mathbb{Q}(s_1, s_2, ..., s_n),$$

and let be $x_1, ...x_n$ its roots. Let us call $\tilde{L} = L\,(x_1, ..., x_n)$, G defines a natural left action on $\tilde{L}$. Then $\mathrm{Gal}(\tilde{L}/L) \simeq S_n$. And since $\mathbb{Q}$ is hilbertian, for almost all rational values that we give to $s_1, .., s_n$ we get $P(x)$ to be an irreducible polynomial with Galois group of its splitting field isomorphic to S_n. We look for necesarly and sufficient conditions on the $s_i's$ in such a way that the polynomial $P(x)$ has splitting field with Galois group over $\mathbb{Q}$ isomorphisc to G and not to S_n.

Since $\tilde{L}$ is separable and by the primitive element theorem, there exists $f \in \tilde{L}$ such that $\tilde{L} = \mathbb{Q}\,(s_1, ..., s_n, f)$. Let $P_f(s_1, ..., s_n, T) \in L[T]$ the minimal polynomial of f over the field L. On the other hand, we have that $\tilde{L}/{}^G\tilde{L}$ is a Galois extension, and $\mathrm{Gal}(\tilde{L}/{}^G\tilde{L}) \simeq G$.

Proposition 5.5.2. *Let $Q_1, ..., Q_n, Q_{n+1} \in \mathbb{Q}$ be rational numbers such that $P_f(Q_1, .., Q_n, Q_{n+1}) = 0$, then the splitting field of the polynomial*

$$P(x) = x^n - Q_1x^{n-1} + ... + (-1)^n Q_n,$$

has Galois group over $\mathbb{Q}$ isomorphic to a subgroup of G.

Proof. Since $\mathrm{Gal}(\tilde{L}/{}^G\tilde{L}) \simeq G$ and $\mathbb{Q}$ is hilbertian the proposition follows. □

Remark 5.5.3. *The Galois group is isomorphisc to G if and only if for all maximal subgroups $H < G$ there is not a rational number Q_{n+2} such that $P_g(Q_1, ..., Q_n, Q_{n+1}, Q_{n+2}) = 0$ where $P_g(s_1, .., s_n, f, T)$ is the minimal polynomial over ${}^G\tilde{L}$ of a primitive element g of the field extension ${}^H\tilde{L}/{}^G\tilde{L}$, because in that case the Galois group will be isomorphic to a subgroup of H.*

Proposition 5.5.4. *Given a Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$, there exists a polynomial $x^n - a_1x^{n-1} + ... + (-1)^n a_n$, such that the splitting field is K and such that $P_f(a_1, .., a_n, T) = 0$ has a rational solution.*

Proof. Let be the composition $\iota : \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\sim} G \hookrightarrow S_n$. And let us define $G_i = \{g \in \mathrm{Gal}(K/\mathbb{Q}) : \iota(g)(i) = i\}$. As G is a transitive subgroup of S_n all these groups are conjugated. Let be $\alpha_1 \in {}^{G_1}K$ a primitive element of the extension ${}^{G_1}K/\mathbb{Q}$, and let be $\alpha_i \in {}^{G_i}K$ the conjugates of α_1. Then, the minimal polynomial of α_1: $x^n - a_1x^{n-1} + ... + (-1)^n a_n = 0$ has as splitting field K and $P_f(a_1, .., a_n, f(\alpha_1, ..., \alpha_n)) = 0$ with $f(\alpha_1, ..., \alpha_n) \in \mathbb{Q}$. □

Corollary 5.5.5. *There is a correspondece between Galois field extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) < G$ and rational solutions to the equation $P_f(y_1, .., y_n, y_{n+1}) = 0$.*

The algorithm
Input: G

- Find n such that there exists an embedding $G \hookrightarrow S_n$ is a transitive way.
- Find a primitive element f. For example $f = \sum_{g\in G} {}^g x_2 x_3^2 ... x_n^{n-1}$ always works.
- Find the minimal polynomial P_f: compute the conjugates of f and then the symmetric functions on it.
- Find the maximal subgroups of G up to conjugacy.
- Find a primitive element g_i for each one.
- Find the minimal polynomials P_{g_i}.

Output: $P_f(s_1, ..., s_n, f)$ and the $P_{g_i}(s_1, ..., s_n, f, g_i)$.

Example 5.5.6. *Let us consider $G = \langle (123) \rangle < S_3$. Let us take $f = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1$. Then:*

$$P_f(s_1, s_2, s_3, T) = T^2 - (s_1 s_2 - 3s_3)T + 9s_3^2 + s_2^3 + s_1^3 s_3 - 6s_1 s_2 s_3.$$

Moreover, we can assume $s_1 = 0$ and we get $P_f = T^2 + 3s_3 T + 9s_3^2 + s_2^3 = 0$, that can be rewrite in the well-known condition: $4(-s_2)^3 - 27s_3^2 = (2T + 3s_3)^2$ is a square in $\mathbb{Q}$.

For exactly having Galois group isomorphic to C_3 and not 1 we just have to ask to $P(x) = x^3 + s_2 x - s_3$ to not split completly in $\mathbb{Q}$, because in this case the only maximal subgroup is the trivial one and we can take $g_1 = x_1$ and we get

$$P_{g_1}(s_1, s_2, s_3, f, T) = T^3 - s_1 T^2 + s_2 T - s_3.$$

Example 5.5.7. *Let us consider $G =< (1234), (13) >< S_4$. Let us take $f = x_1 x_3 + x_2 x_4$. Then:*

$$P_f(s_1, s_2, s_3, s_4, T) = T^3 - s_2 T^2 + (s_1 s_3 - 4s_4)T - (s_4 s_1^2 - 4s_2 s_4 + s_3^2).$$

Up to conjugacy the only maximal subgroups of G are $< (1234) >$ and $< (13), (24) >$. Then, we take $g_1 = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_4 + x_4^2 x_1$ and $g_2 = x_1 x_3$. And after assume $s_1 = 0$ we get:

$$P_{g_1}(s_1, s_2, s_3, s_4, f, T) = T^2 + 2s_3 T + 20s_2 s_4 + f s_2^2 - 2s_2 f^2 + 4f s_4 + s_2^3 - 2s_3^2, \text{ and}$$

$$P_{g_2}(s_1, s_2, s_3, s_4, f, T) = T^2 - fT + s_4.$$

Notice that in this case we can isolate for example the variable s_2 from the equation and then we can also solve the problem (NP) for $G = D_4$. Next polynomial has generic Galois group isomorphic to D_4 and moreover parametrize all the extensions over $\mathbb{Q}$ with Galois group isomorphisc to D_4:

$$x^4 + s_3 x^2 - \frac{T^3 - 4s_4 T - s_3^2}{T^2 - 4s_4} x + s_4 = 0.$$

The algorithm does not look to be very efficient, so by hand we cannot compute much more examples. We are waitting for an implementation of the algorithm to trying to solve the Galois inverse problem for $G =< 336, 208 >$ and in that way compute the remaining twists of the Klein quartic. In fact, this group is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_7)$ and some generic polynomials that have it like Galois group are known, see [39]. But not all such extensions are known.

Even if we have not been still able of implementing the algorithm, it gives rise to the following interesting questions:

- What about taking different primitive elements?
- If with one f we can isolate one of the variables s_i, that is, there is a parametrization of all the extensions with Galois group G, then with any other choice of a primitive element do we get the same property?
- What kind of varieties do we get with this algorithm? Notice that the set of rational points is not empty because all non-trivial groups contain a non-trivial cyclic one and the inverse Galois problem $\mathrm{Gal}(K/\mathbb{Q}) \simeq C_r$ has solutions for all r.
- Can we recover the group G from the variety defined by $P_f(s_1, ..., s_n, T) = 0$?

Tables

Case	$Aut\,(C)$	generators in $\mathrm{PGL}_3\,(\mathbb{C})$
I	C_2	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
II	V_4	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
III	C_3	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi \end{pmatrix}$ with $\xi^2 + \xi = -1$
IV	S_3	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \xi & 0 & 0 \\ 0 & \xi^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
V	D_4	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{pmatrix}$
VI	C_6	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi \end{pmatrix}$
VII	$GAP\,(16, 13)$	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

VIII	S_4	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
IX	C_9	$\begin{pmatrix} \xi & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{pmatrix}$ with $\omega^3 = \xi$
X	GAP $(48, 33)$	$\begin{pmatrix} \frac{i\xi^2\sqrt{3}}{3} & 0 & \frac{i\xi\sqrt{3}}{3} \\ 0 & \xi^2 & 0 \\ \frac{2\sqrt{3}\xi^2}{3} & 0 & \frac{-i\xi\sqrt{3}}{3} \end{pmatrix}, \begin{pmatrix} \frac{\xi\sqrt{3}}{3} & 0 & \frac{\xi^2\sqrt{3}}{3} \\ 0 & \xi & 0 \\ \frac{2\sqrt{3}\xi}{3} & 0 & \frac{-\sqrt{3}\xi^2}{3} \end{pmatrix}$
XI	$GAP\,(96, 64)$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i & 0 \\ 1 & 0 & 0 \\ 0 & 0 & i \end{pmatrix}$
XII	$\mathrm{PSL}_2(\mathbb{F}_7)$	$\frac{-1}{\sqrt{-7}}\begin{pmatrix} \zeta - \zeta^6 & \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 \\ \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 & \zeta - \zeta^6 \\ \zeta^4 - \zeta^3 & \zeta - \zeta^6 & \zeta^2 - \zeta^5 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} \zeta^4 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta \end{pmatrix}$ with $\zeta^7 = 1$ and $\zeta \neq 1$

Table 5.1: Automorphisms Henn classification

Case	$Aut\,(C)$	generators in $\mathrm{PGL}_3\,(\mathbb{C})$
I	C_2	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
II	V_4	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
III	C_3	$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi \end{pmatrix}$ with $\xi^2+\xi=-1$
IV	S_3	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} \xi & 0 & 0 \\ 0 & \xi^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
V	D_4	$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{pmatrix}$
VI	C_6	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \xi \end{pmatrix}$
VII	$GAP\,(16,13)$	$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

VIII	S_4	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$
IX	C_9	$\begin{pmatrix} \xi & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \omega \end{pmatrix}$ with $\omega^3 = \xi$
X	GAP $(48, 33)$	$\begin{pmatrix} \frac{i\xi^2\sqrt{3}}{3} & 0 & \frac{i\xi\sqrt{3}}{3} \\ 0 & \xi^2 & 0 \\ \frac{2\sqrt{3}\xi^2}{3} & 0 & \frac{-i\xi\sqrt{3}}{3} \end{pmatrix}, \begin{pmatrix} \frac{\xi\sqrt{3}}{3} & 0 & \frac{\xi^2\sqrt{3}}{3} \\ 0 & \xi & 0 \\ \frac{2\sqrt{3}\xi}{3} & 0 & \frac{-\sqrt{3}\xi^2}{3} \end{pmatrix}$
XI	$GAP\,(96, 64)$	$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i & 0 \\ 1 & 0 & 0 \\ 0 & 0 & i \end{pmatrix}$
XII	$\mathrm{PSL}_2\,(\mathbb{F}_7)$	$\frac{-1}{\sqrt{-7}} \begin{pmatrix} \zeta - \zeta^6 & \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 \\ \zeta^2 - \zeta^5 & \zeta^4 - \zeta^3 & \zeta - \zeta^6 \\ \zeta^4 - \zeta^3 & \zeta - \zeta^6 & \zeta^2 - \zeta^5 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} \zeta^4 & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta \end{pmatrix}$ with $\zeta^7 = 1$ and $\zeta \neq 1$

Table 5.2: Automorphisms Modified Henn classification

Invariant	Value
I_3	0
I_6	0
I_9	$3(65a^4 + 2520a^2 + 11664)$
I_{12}	$(5a^4 - 1800a^2 - 3888)$
I_{15}	0
I_{18}	0
I_{27}	0
J_9	0
J_{12}	$2^5 3^5 a^2(a^2 + 12)(5a^2 + 108)(5a^2 + 252)$
J_{15}	$2^5 3^2 a^2(a^2 + 12)(5a^2 - 324)(5a^2 + 108)$
J_{18}	0
I_{21}	0
J_{21}	$2^8(a - 2)^4(a + 2)^4$

Table 5.3: Dixmier-Ohno Invariants. Case VI

Invariant	Value
I_3	1
I_6	$a^3(a - 6)^2(a + 3)(a^3 + 9a^2 + 36)^{-2}$
I_9	$a^2(a + 3)(a + 18)^2(a^2 + 3a + 18)^2(a^3 + 9a^2 + 36)^{-3}$
I_{12}	$a^2(a + 18)(a^2 - 9a - 6)(a^2 + 3a + 18)^2(a^3 + 9a^2 + 36)^{-3}$
I_{15}	$a^3(a + 18)^3(a^2 + 3a + 18)^3 2^{-1}(a^3 + 9a^2 + 36)^{-4}$
I_{18}	$2a^2(a + 3)(a + 18)(a^2 - 9a - 6)(a^2 + 3a + 18)^2(5a^2 + 12a + 36)(a^3 + 9a^2 + 36)^{-4}$
I_{27}	$2^4a^3(a + 3)^3(a + 18)^3(a^2 + 3a + 18)^3(a^3 + 9a^2 + 36)^{-5}$
J_9	$2^4a^3(a^2 - 9a - 6)^3(a^2 + 3a + 18)^3(a^3 + 9a^2 + 36)^{-5}$
J_{12}	$2^3a^4(a + 3)^2(a + 18)^4(a^2 + 3a + 18)^4(a^3 + 9a^2 + 36)^{-6}$
J_{15}	$2^3a^4(a + 18)^2(a^2 - 9a - 6)^2(a^2 + 3a + 18)^4(a^3 + 9a^2 + 36)^{-6}$
J_{18}	$2^2a^3(a^2 - 9a - 6)^3(a^2 + 3a + 18)^3(5a^2 + 12a + 36)^3(a^3 + 9a^2 + 36)^{-7}$
I_{21}	$2^5a^3(a + 18)(a^2 - 9a - 6)^2(a^2 + 3a + 18)^3(5a^2 + 12a + 36)^2(a^3 - 9a^2 - 18a - 6)(a^3 + 9a^2 + 36)^{-7}$
J_{21}	$2^2(a - 2)^{14}(a + 1)^4(a + 2)^6(a^3 + 9a^2 + 36)^{-9}$

Table 5.4: Dixmier-Ohno Invariants. Case VIII

Here, we show the implemented code in MAGMA for computing the pairs (G, H) for the Fermat quartic. It is easily adaptable for any other curve. Moreover, it computes tha cardinality of expresion (1.7), that is, the number of solutions to the Galois embedding problem (1.3) corresponding to a pair (G, H) with same splitting field L.

```
Gamma:=SmallGroup(192,956);
lat:=SubgroupLattice(Gamma);
AutC:=lat[81];

OrderAut2:=function(G,H,AutC)
A:=AutomorphismGroup(G);
D:=[];
f,B:=PermutationRepresentation(A);
for b in B do
        if H @ (b@@f) eq H then
                D:=Append(D,b);
        end if;
end for;
A2:=sub<B|D>;
return Order(A2);
end function;

OrderInner:=function(G,AutC)
D:=[];
for a in AutC do
    h:=hom<Gamma->Gamma|x:->axa^(-1)>;
    if G@h eq G then
        g:=hom<G->G|x:->axa^(-1)>;
        D:=Append(D,g);
    end if;
end for;
A:=AutomorphismGroup(G);
Inn:=sub<A|D>;
return Order(Inn);
end function;

B:=[];
for i in [2..#lat] do
    G:=lat[i];
    T:=[];
    for g in G do
        if g in AutC then
            T:=Append(T,g);
        end if;
    end for;
    H:=sub<G|T>;
    if Index(G,H) eq 2 then
        B:=Append(B, <i,IdentifyGroup(G),IdentifyGroup(H),
        OrderAut2(G,H,AutC)/OrderInner(G,AutC)>);
    end if;
end for;

print "The number of pairs (G,H) is:", #B;

for i:=1 to #B do
    print "(iteration,(G,H), times)=", B[i];
end for;
```

Table 5.5: Magma code for computing the pairs (G,H)

#	a_i	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9
#1	a_1	0	9	0	243	0	7290	0	229635	0
	a_2	6	54	621	7938	106191	1454355	20212254	283815738	4016375199
	a_3	0	82	0	23574	0	7727410	0	2680982990	0
#2	a_1	0	18	0	486	0	14580	0	459270	0
	a_2	9	99	1215	15795	212139	2907981	40422321	567624915	8032730715
	a_3	0	164	0	47148	0	15454820	0	5361965980	0
#3	a_1	0	5	0	123	0	3650	0	114835	0
	a_2	2	26	305	3954	53047	727031	10105678	141906506	2008183463
	a_3	0	42	0	11798	0	3863850	0	1340493518	0
#4	a_1	0	10	0	246	0	7300	0	229670	0
	a_2	5	51	611	7907	106095	1454061	20211357	283813011	4016366927
	a_3	0	84	0	23596	0	7727700	0	2680987036	0
#5	a_1	0	5	0	123	0	3650	0	114835	0
	a_2	4	30	319	3994	53169	727395	10106772	141909786	2008193305
	a_3	0	42	0	11798	0	3863850	0	1340493518	0
#6	a_1	0	3	0	81	0	2430	0	76545	0
	a_2	2	18	207	2646	35397	484785	6737418	94605246	1338791733
	a_3	0	28	0	7860	0	2575810	0	893661020	0
#7	a_1	0	6	0	162	0	4860	0	153090	0
	a_2	3	33	405	5265	70713	969327	13474107	189208305	2677576905
	a_3	0	56	0	15720	0	5151620	0	1787322040	0
#8	a_1	0	3	0	81	0	2430	0	76545	0
	a_2	3	21	216	2673	35478	485028	6738147	94607433	1338798294
	a_3	0	28	0	7860	0	2575810	0	893661020	0
#9	a_1	0	3	0	63	0	1830	0	57435	0
	a_2	3	18	168	2022	26658	363915	5054031	70956810	1004102358
	a_3	0	22	0	5910	0	1932070	0	670248782	0
#10	a_1	0	6	0	126	0	3660	0	114870	0
	a_2	3	27	309	3963	53073	727101	10105875	141907059	2008185033
	a_3	0	44	0	11820	0	3864140	0	1340497564	0
#11	a_1	0	5	0	99	0	2450	0	68355	0
	a_2	2	22	221	2546	31367	405547	5422370	74233722	1033431575
	a_3	0	34	0	7222	0	2086690	0	689426766	0
#12	a_1	0	10	0	198	0	4900	0	136710	0
	a_2	5	43	443	5091	62735	811093	10844741	148467443	2066863151
	a_3	0	68	0	14444	0	4173380	0	1378853532	0
#13	a_1	0	5	0	99	0	2450	0	68355	0
	a_2	4	26	235	2586	31489	405911	5423464	74237002	1033441417
	a_3	0	34	0	7222	0	2086690	0	689426766	0
#14	a_1	0	3	0	63	0	1830	0	57435	0
	a_2	2	16	161	2002	26597	363733	5053484	70955170	1004097437
	a_3	0	22	0	5910	0	1932070	0	670248782	0

#	a_i	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9
#15	a_1	0	3	0	63	0	1830	0	57435	0
	a_2	2	14	155	1982	26537	363551	5052938	70953530	1004092517
	a_3	0	22	0	5910	0	1932070	0	670248782	0
#16	a_1	0	2	0	42	0	1220	0	38290	0
	a_2	2	12	112	1348	17772	242610	3369354	47304540	669401572
	a_3	0	15	0	3941	0	1288050	0	446832533	0
#17	a_1	0	4	0	84	0	2440	0	76580	0
	a_2	2	18	206	2642	35382	484734	6737250	94604706	1338790022
	a_3	0	30	0	7882	0	2576100	0	893665066	0
#18	a_1	0	3	0	51	0	1230	0	34195	0
	a_2	2	12	113	1278	15697	202809	2711284	37117138	516716573
	a_3	0	18	0	3622	0	1043490	0	344715406	0
#19	a_1	0	6	0	102	0	2460	0	68390	0
	a_2	3	23	225	2555	31393	405617	5422567	74234275	1033433145
	a_3	0	36	0	7244	0	2086980	0	689430812	0
#20	a_1	0	3	0	51	0	1230	0	34195	0
	a_2	3	16	126	1318	15818	203173	2712377	37120418	516726414
	a_3	0	18	0	3622	0	1043490	0	344715406	0
#21	a_1	0	3	0	51	0	1230	0	34195	0
	a_2	2	14	119	1298	15757	202991	2711830	37118778	516721493
	a_3	0	18	0	3622	0	1043490	0	344715406	0
#22	a_1	0	3	0	51	0	1230	0	34195	0
	a_2	2	14	119	1298	15757	202991	2711830	37118778	516721493
	a_3	0	18	0	3618	0	1043400	0	344713838	0
#23	a_1	0	6	0	102	0	2460	0	68390	0
	a_2	3	23	225	2555	31393	405617	5422567	74234275	1033433145
	a_3	0	36	0	7236	0	2086800	0	689427676	0
#24	a_1	0	2	0	33	0	920	0	28735	0
	a_2	2	10	86	1016	13342	181993	2527114	35478682	502051964
	a_3	0	12	0	2966	0	966180	0	335126414	0
#25	a_1	0	4	0	66	0	1840	0	57470	0
	a_2	2	15	158	1991	26562	363621	5053134	70954083	1004094086
	a_3	0	24	0	5932	0	1932360	0	670252828	0
#26	a_1	0	2	0	33	0	920	0	28735	0
	a_2	2	11	89	1026	13372	182084	2527387	35479502	502054424
	a_3	0	12	0	2966	0	966180	0	335126414	0
#27	a_1	0	3	0	51	0	1230	0	34195	0
	a_2	3	16	126	1318	15818	203173	2712377	37120418	516726414
	a_3	0	18	0	3618	0	1043400	0	344713838	0
#28	a_1	0	1	0	21	0	610	0	19145	0
	a_2	1	6	56	674	8886	121305	1684677	23652270	334700786
	a_3	0	8	0	1972	0	644030	0	223416284	0
#29	a_1	0	2	0	42	0	1220	0	38290	0
	a_2	1	9	103	1321	17691	242367	3368625	47302353	669395011
	a_3	0	16	0	3944	0	1288060	0	446832568	0

#	a_i	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9
#30	a_1	0	1	0	21	0	610	0	19145	0
	a_2	1	7	58	681	8906	121366	1684859	23652817	334702426
	a_3	0	8	0	1972	0	644030	0	223416284	0
#31	a_1	0	3	0	45	0	930	0	22575	0
	a_2	3	15	105	966	10398	122802	1541550	20202222	273038442
	a_3	0	16	0	2478	0	599200	0	181948718	0
#32	a_1	0	6	0	90	0	1860	0	45150	0
	a_2	3	21	183	1851	20553	244875	3080913	40397883	546057201
	a_3	0	32	0	4956	0	1198400	0	363897436	0
#33	a_1	0	2	0	27	0	620	0	17115	0
	a_2	2	9	65	664	7922	101622	1356287	18560486	258363992
	a_3	0	10	0	1818	0	521800	0	172358158	0
#34	a_1	0	4	0	54	0	1240	0	34230	0
	a_2	2	13	116	1287	15722	202879	2711480	37117691	516718142
	a_3	0	20	0	3636	0	1043600	0	344716316	0
#35	a_1	0	2	0	27	0	620	0	17115	0
	a_2	2	9	65	664	7922	101622	1356287	18560486	258363992
	a_3	0	10	0	1822	0	521890	0	172359726	0
#36	a_1	0	4	0	54	0	1240	0	34230	0
	a_2	2	13	116	1287	15722	202879	2711480	37117691	516718142
	a_3	0	20	0	3644	0	1043780	0	344719452	0
#37	a_1	0	3	0	45	0	930	0	22575	0
	a_2	2	12	95	936	10307	122529	1540730	20199762	273031061
	a_3	0	16	0	2478	0	599200	0	181948718	0
#38	a_1	0	2	0	27	0	620	0	17115	0
	a_2	2	10	68	674	7952	101713	1356560	18561306	258366452
	a_3	0	10	0	1818	0	521800	0	172358158	0
#39	a_1	0	2	0	27	0	620	0	17115	0
	a_2	2	10	68	674	7952	101713	1356560	18561306	258366452
	a_3	0	10	0	1822	0	521890	0	172359726	0
#40	a_1	0	1	0	12	0	310	0	9590	0
	a_2	1	5	33	352	4486	60779	842710	11827232	167353638
	a_3	0	5	0	997	0	322160	0	111710165	0
#41	a_1	0	2	0	24	0	620	0	19180	0
	a_2	1	6	55	670	8871	121254	1684509	23651730	334699075
	a_3	0	10	0	1994	0	644320	0	223420330	0
#42	a_1	0	2	0	24	0	470	0	11305	0
	a_2	2	9	56	493	5227	61482	771010	10101798	136521236
	a_3	0	9	0	1248	0	299700	0	90975598	0
#43	a_1	0	4	0	48	0	940	0	22610	0
	a_2	2	12	95	935	10302	122508	1540653	20199495	273030170
	a_3	0	18	0	2496	0	599400	0	181951196	0

#	a_i	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9
#44	a_1	0	1	0	15	0	310	0	7525	0
	a_2	1	5	34	319	3456	40904	513759	6733801	91011994
	a_3	0	6	0	828	0	199740	0	60649596	0
#45	a_1	0	2	0	30	0	620	0	15050	0
	a_2	1	7	61	617	6851	81625	1026971	13465961	182019067
	a_3	0	12	0	1656	0	399480	0	121299192	0
#46	a_1	0	1	0	15	0	310	0	7525	0
	a_2	1	5	35	322	3466	40934	513850	6734074	91012814
	a_3	0	6	0	828	0	199740	0	60649596	0
#47	a_1	0	1	0	9	0	160	0	3780	0
	a_2	1	4	21	171	1761	20548	257160	3367724	45508422
	a_3	0	4	0	423	0	99970	0	30326037	0
#48	a_1	0	2	0	18	0	320	0	7560	0
	a_2	1	5	34	318	3451	40883	513682	6733534	91011103
	a_3	0	8	0	846	0	199940	0	60652074	0

Table 5.6: The 48 moment sequences that arise for twists of the Fermat quartic.

<table>
<tr><th>Gen(H)</th><th>h</th><th>ID(G)</th><th>ID(H)</th><th>k</th><th>#/k</th><th>#/$k(i)$</th></tr>
<tr><td>id</td><td>id</td><td>$\langle 2,1\rangle$</td><td>$\langle 1,1\rangle$</td><td>$\mathbb{Q}$</td><td>#1</td><td>#2</td></tr>
<tr><td colspan="7">$x^4+y^4+z^4=0$</td></tr>
<tr><td>id</td><td>$u_1^2t_1$</td><td>$\langle 2,1\rangle$</td><td>$\langle 1,1\rangle$</td><td>$\mathbb{Q}$</td><td>#1</td><td>#2</td></tr>
<tr><td colspan="7">$2x^4-12x^2y^2+2y^4+z^4=0$</td></tr>
<tr><td>id</td><td>$t_1^3u_1t_1u_1$</td><td>$\langle 2,1\rangle$</td><td>$\langle 1,1\rangle$</td><td>$\mathbb{Q}$</td><td>#1</td><td>#2</td></tr>
<tr><td colspan="7">$-4x^4+y^4+z^4=0$</td></tr>
<tr><td>t_1^2</td><td>t_1</td><td>$\langle 4,1\rangle$</td><td>$\langle 2,1\rangle$</td><td>$\mathbb{Q}(\sqrt{-5})$</td><td>#3</td><td>#4</td></tr>
<tr><td colspan="7">$-2x^4-32x^3y+12x^2y^2+32xy^3-2y^4+z^4=0$</td></tr>
<tr><td>t_1^2</td><td>$t_1^3u_1t_1u_1$</td><td>$\langle 4,2\rangle$</td><td>$\langle 2,1\rangle$</td><td>$\mathbb{Q}$</td><td>#5</td><td>#4</td></tr>
<tr><td colspan="7">$9x^4+9y^4-4z^4=0$</td></tr>
<tr><td>t_1^2</td><td>$u_1^2t_1$</td><td>$\langle 4,2\rangle$</td><td>$\langle 2,1\rangle$</td><td>$\mathbb{Q}$</td><td>#5</td><td>#4</td></tr>
<tr><td colspan="7">$-14x^4-192x^3y+84x^2y^2+192xy^3-14y^4+z^4=0$</td></tr>
<tr><td>t_1^2</td><td>id</td><td>$\langle 4,2\rangle$</td><td>$\langle 2,1\rangle$</td><td>$\mathbb{Q}$</td><td>#5</td><td>#4</td></tr>
<tr><td colspan="7">$9x^4+y^4+z^4=0$</td></tr>
<tr><td>t_1^2</td><td>u_1</td><td>$\langle 4,2\rangle$</td><td>$\langle 2,1\rangle$</td><td>$\mathbb{Q}$</td><td>#5</td><td>#4</td></tr>
<tr><td colspan="7">$9x^4-4y^4+z^4=0$</td></tr>
<tr><td>$u_1^2t_1$</td><td>id</td><td>$\langle 4,2\rangle$</td><td>$\langle 2,1\rangle$</td><td>$\mathbb{Q}$</td><td>#5</td><td>#4</td></tr>
<tr><td colspan="7">$2x^4+36x^2y^2+18y^4+z^4=0$</td></tr>
<tr><td>$u_1^2t_1$</td><td>$t_1^3u_1t_1u_1$</td><td>$\langle 4,2\rangle$</td><td>$\langle 2,1\rangle$</td><td>$\mathbb{Q}$</td><td>#5</td><td>#4</td></tr>
<tr><td colspan="7">$-8x^4-144x^2y^2-72y^4+z^4=0$</td></tr>
<tr><td>s_1</td><td>id</td><td>$\langle 6,2\rangle$</td><td>$\langle 3,1\rangle$</td><td>$\mathbb{Q}$</td><td>#6</td><td>#7</td></tr>
<tr><td colspan="7">$3x^4+14(6x^2y^2+4x^3z)-21(12x^2yz+4xy^3)+98(6x^2y^2+12xy^2z+y^4)-$
$-245(4y^3z+12xyz^2)+4998y^2z^2-9604yz^3+7546z^4=0$</td></tr>
<tr><td>s_1</td><td>$u_1^2t_1$</td><td>$\langle 6,1\rangle$</td><td>$\langle 3,1\rangle$</td><td>$\mathbb{Q}$</td><td>#8</td><td>#7</td></tr>
<tr><td colspan="7">$3x^4-12(6x^2y^2+4x^3z)-12(12x^2yz+4xy^3)+72(6x^2y^2+12xy^2z+y^4)+$
$+120(4y^3z+12xyz^2)-2304y^2z^2-4032yz^3+1824z^4=0$</td></tr>
<tr><td>t_1^2,u_1^2</td><td>id</td><td>$\langle 8,5\rangle$</td><td>$\langle 4,2\rangle$</td><td>$\mathbb{Q}$</td><td>#9</td><td>#10</td></tr>
<tr><td colspan="7">$9x^4+25y^4+z^4=0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1$</td><td>t_1</td><td>$\langle 8,4\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}(\sqrt{-2})$</td><td>#11</td><td>#12</td></tr>
<tr><td colspan="7">$-24x^3y+24xy^3+z^4=0$</td></tr>
<tr><td>t_1^2,u_1^2</td><td>u_1</td><td>$\langle 8,5\rangle$</td><td>$\langle 4,2\rangle$</td><td>$\mathbb{Q}$</td><td>#9</td><td>#10</td></tr>
<tr><td colspan="7">$9x^4+25y^4-4z^4=0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1$</td><td>$u_1^2t_1$</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#13</td><td>#12</td></tr>
<tr><td colspan="7">$6x^4-36x^2y^2+6y^4+z^4=0$</td></tr>
<tr><td>$u_1^2t_1,t_1^2$</td><td>$t_1^3u_1t_1u_1$</td><td>$\langle 8,5\rangle$</td><td>$\langle 4,2\rangle$</td><td>$\mathbb{Q}$</td><td>#9</td><td>#10</td></tr>
<tr><td colspan="7">$-28x^4-240x^3y-840x^2y^2-1200xy^3-700y^4+z^4=0$</td></tr>
<tr><td>t_1</td><td>u_1^2</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#9</td><td>#10</td></tr>
<tr><td colspan="7">$10x^4+800x^3y-300x^2y^2-4000xy^3+250y^4+z^4=0$</td></tr>
</table>

<table>
<tr><th>Gen(H)</th><th>h</th><th>ID(G)</th><th>ID(H)</th><th>k</th><th>#/k</th><th>#/$k(i)$</th></tr>
<tr><td>t_1</td><td>$t_1^3u_1t_1u_1^3$</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#9</td><td>#10</td></tr>
<tr><td colspan="7">$-10x^4 + 800x^3y + 300x^2y^2 - 4000xy^3 - 250y^4 + z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1$</td><td>u_1</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#13</td><td>#12</td></tr>
<tr><td colspan="7">$3x^4 - 4y^4 + z^4 = 0$</td></tr>
<tr><td>$u_1^2t_1, t_1^2$</td><td>$t_1^3u_1t_1u_1^3$</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,2\rangle$</td><td>$\mathbb{Q}$</td><td>#14</td><td>#10</td></tr>
<tr><td colspan="7">$-22x^4 - 160x^3y - 1320x^2y^2 - 1600xy^3 - 2200y^4 + z^4 = 0$</td></tr>
<tr><td>t_1^2, u_1^2</td><td>$u_1^2t_1$</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,2\rangle$</td><td>$\mathbb{Q}$</td><td>#14</td><td>#10</td></tr>
<tr><td colspan="7">$-2x^4 - 32x^3y + 12x^2y^2 + 32xy^3 - 2y^4 + z^4 = 0$</td></tr>
<tr><td>$u_1^2t_1, t_1^2$</td><td>id</td><td>$\langle 8,5\rangle$</td><td>$\langle 4,2\rangle$</td><td>$\mathbb{Q}$</td><td>#9</td><td>#10</td></tr>
<tr><td colspan="7">$28x^4 + 240x^3y + 840x^2y^2 + 1200xy^3 + 700y^4 + z^4 = 0$</td></tr>
<tr><td>t_1</td><td>$t_1^3u_1t_1u_1$</td><td>$\langle 8,2\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#14</td><td>#10</td></tr>
<tr><td colspan="7">$-60x^4 - 400x^3y - 1800x^2y^2 - 2000xy^3 - 1500y^4 + z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1^3$</td><td>u_1</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#9</td><td>#10</td></tr>
<tr><td colspan="7">$9x^4 + 3y^4 - 4z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1^3$</td><td>id</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#9</td><td>#10</td></tr>
<tr><td colspan="7">$9x^4 + 3y^4 + z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1^3$</td><td>$u_1^2t_1$</td><td>$\langle 8,2\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#14</td><td>#10</td></tr>
<tr><td colspan="7">$14x^4 - 192x^3y - 84x^2y^2 + 192xy^3 + 14y^4 + z^4 = 0$</td></tr>
<tr><td>$u_1^2t_1, t_1^2$</td><td>u_1^2</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,2\rangle$</td><td>$\mathbb{Q}$</td><td>#14</td><td>#10</td></tr>
<tr><td colspan="7">$22x^4 + 160x^3y + 1320x^2y^2 + 1600xy^3 + 2200y^4 + z^4 = 0$</td></tr>
<tr><td>t_1</td><td>id</td><td>$\langle 8,2\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#14</td><td>#10</td></tr>
<tr><td colspan="7">$60x^4 + 400x^3y + 1800x^2y^2 + 2000xy^3 + 1500y^4 + z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1^3$</td><td>t_1u_1</td><td>$\langle 8,1\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}(\sqrt{6})$</td><td>#15</td><td>#10</td></tr>
<tr><td colspan="7">$6x^4 - 40x^3y - 36x^2y^2 + 40xy^3 + 6y^4 + z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1$</td><td>id</td><td>$\langle 8,3\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>#13</td><td>#12</td></tr>
<tr><td colspan="7">$3x^4 + y^4 + z^4 = 0$</td></tr>
<tr><td>$s_1, u_1^2t_1$</td><td>id</td><td>$\langle 12,4\rangle$</td><td>$\langle 6,1\rangle$</td><td>$\mathbb{Q}$</td><td>#16</td><td>#17</td></tr>
<tr><td colspan="7">$3x^4 + 2(6x^2y^2 + 4x^3z) - 3(12x^2yz + 4xy^3) + 2(6x^2y^2 + 12xy^2z + y^4)-$
$-5(4y^3z + 12xyz^2) + 30y^2z^2 - 28yz^3 + 10z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1, u_1^2$</td><td>u_1t_1</td><td>$\langle 16,6\rangle$</td><td>$\langle 8,2\rangle$</td><td>$\mathbb{Q}(\sqrt{-5})$</td><td>#18</td><td>#19</td></tr>
<tr><td colspan="7">$2x^4 - 16x^3y - 12x^2y^2 + 16xy^3 + 2y^4 + z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1, u_1^2$</td><td>u_1</td><td>$\langle 16,11\rangle$</td><td>$\langle 8,2\rangle$</td><td>$\mathbb{Q}$</td><td>#20</td><td>#19</td></tr>
<tr><td colspan="7">$9x^4 + 5y^4 - 4z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1, u_1^2$</td><td>$u_1^2t_1$</td><td>$\langle 16,13\rangle$</td><td>$\langle 8,2\rangle$</td><td>$\mathbb{Q}$</td><td>#21</td><td>#19</td></tr>
<tr><td colspan="7">$6x^4 - 32x^3y - 36x^2y^2 + 32xy^3 + 6y^4 + z^4 = 0$</td></tr>
<tr><td>$t_1^3u_1t_1u_1, u_1^2$</td><td>id</td><td>$\langle 16,11\rangle$</td><td>$\langle 8,2\rangle$</td><td>$\mathbb{Q}$</td><td>#20</td><td>#19</td></tr>
<tr><td colspan="7">$9x^4 + 5y^4 + z^4 = 0$</td></tr>
<tr><td>$u_1^2t_1u_1$</td><td>u_1</td><td>$\langle 16,8\rangle$</td><td>$\langle 8,1\rangle$</td><td>$\mathbb{Q}$</td><td>#22</td><td>#23</td></tr>
<tr><td colspan="7">$16x^3y + 32xy^3 + z^4 = 0$</td></tr>
</table>

Gen(H)	h	ID(G)	ID(H)	k	#/k	#/$k(i)$
$t_1^3u_1t_1u_1^3, u_1^2t_1$	u_1	$\langle 16,7\rangle$	$\langle 8,3\rangle$	$\mathbb{Q}$	#24	#25
$4x^4+32x^3y+48x^2y^2+64xy^3+16y^4+z^4=0$						
$t_1^3u_1t_1u_1^3, t_1$	id	$\langle 16,13\rangle$	$\langle 8,4\rangle$	$\mathbb{Q}$	#26	#25
$12x^4+72x^3y+216x^2y^2+216xy^3+108y^4+z^4=0$						
t_1, u_1^2	$u_1t_1u_1$	$\langle 16,11\rangle$	$\langle 8,3\rangle$	$\mathbb{Q}$	#26	#25
$-8x^4-48x^3y-144x^2y^2-144xy^3-72y^4+z^4=0$						
$t_1u_1^2t_1u_1t_1$	$t_1u_1t_1u_1^2$	$\langle 16,7\rangle$	$\langle 8,1\rangle$	$\mathbb{Q}$	#27	#23
$-16x^3y+32xy^3+z^4=0$						
$t_1, u_1t_1u_1$	u_1^2	$\langle 16,11\rangle$	$\langle 8,2\rangle$	$\mathbb{Q}$	#20	#19
$12x^4+64x^3y+144x^2y^2+128xy^3+48y^4+z^4=0$						
t_1, u_1^2	id	$\langle 16,11\rangle$	$\langle 8,3\rangle$	$\mathbb{Q}$	#26	#25
$8x^4+48x^3y+144x^2y^2+144xy^3+72y^4+z^4=0$						
$t_1^3u_1t_1u_1^3, u_1^2t_1$	id	$\langle 16,11\rangle$	$\langle 8,3\rangle$	$\mathbb{Q}$	#26	#25
$4x^4+24x^3y+72x^2y^2+72xy^3+36y^4+z^4=0$						
$t_1^3u_1t_1u_1^3, t_1$	u_1	$\langle 16,8\rangle$	$\langle 8,4\rangle$	$\mathbb{Q}$	#24	#25
$10x^4+200x^3y+300x^2y^2+1000xy^3+250y^4+z^4=0$						
$t_1, u_1t_1u_1$	id	$\langle 16,13\rangle$	$\langle 8,2\rangle$	$\mathbb{Q}$	#21	#19
$14x^4+120x^3y+420x^2y^2+600xy^3+350y^4+z^4=0$						
s_1, u_1^2	id	$\langle 24,13\rangle$	$\langle 12,3\rangle$	$\mathbb{Q}$	#28	#29
$14x^4-84x^3y+98(6x^2y^2+4x^3z)-245(12x^2yz+4xy^3)+833(6x^2y^2+12xy^2z+y^4)-$ $-2401(4y^3z+12xyz^2)+45276y^2z^2-90552yz^3+69629z^4=0$						
s_1, u_1^2	$u_1^2t_1$	$\langle 24,12\rangle$	$\langle 12,3\rangle$	$\mathbb{Q}$	#30	#29
$-12x^4-48x^3y+72(6x^2y^2+4x^3z)+120(12x^2yz+4xy^3)-384(6x^2y^2+12xy^2z+y^4)-$ $-1008(4y^3z+12xyz^2)+10944y^2z^2+30336yz^3-6912z^4=0$						
$u_1, t_1^3u_1t_1$	id	$\langle 32,34\rangle$	$\langle 16,2\rangle$	$\mathbb{Q}$	#31	#32
$3x^4+5y^4+z^4=0$						
$t_1u_1^2t_1u_1t_1, u_1^2$	id	$\langle 32,7\rangle$	$\langle 16,6\rangle$	$\mathbb{Q}$	#33	#34
$10x^4+40x^3y+300x^2y^2+200xy^3+250y^4+z^4=0$						
$t_1^3u_1t_1u_1, u_1^2, t_1$	u_1	$\langle 32,43\rangle$	$\langle 16,13\rangle$	$\mathbb{Q}$	#35	#36
$6x^4+48x^3y+72x^2y^2+96xy^3+24y^4+z^4=0$						
$u_1, u_1^2t_1u_1^3t_1$	$u_1^2t_1$	$\langle 32,11\rangle$	$\langle 16,2\rangle$	$\mathbb{Q}$	#37	#32
$2x^4-16x^3y-12x^2y^2+16xy^3+2y^4+z^4=0$						
$t_1u_1^2t_1u_1t_1, u_1^2$	u_1	$\langle 32,43\rangle$	$\langle 16,6\rangle$	$\mathbb{Q}$	#38	#34
$10x^4-80x^3y-300x^2y^2+400xy^3+250y^4+z^4=0$						
$u_1t_1u_1, u_1^2, t_1$	id	$\langle 32,49\rangle$	$\langle 16,13\rangle$	$\mathbb{Q}$	#39	#36
$8x^4+56x^3y+336x^2y^2+392xy^3+392y^4+z^4=0$						
s_1, t_1	id	$\langle 48,48\rangle$	$\langle 24,12\rangle$	$\mathbb{Q}$	#40	#41
$2x^4-12x^3y+2(6x^2y^2+4x^3z)-5(12x^2yz+4xy^3)+5(6x^2y^2+12xy^2z+y^4)-$ $-7(4y^3z+12xyz^2)+60y^2z^2-48yz^3+17z^4=0$						

Gen(H)	h	ID(G)	ID(H)	k	$\#/k$	$\#/k(i)$
t_1, u_1	id	$\langle 64, 134\rangle$	$\langle 32, 11\rangle$	$\mathbb{Q}$	#42	#43
$4x^4 + 48x^3y + 48x^2y^2 + 96xy^3 + 16y^4 + z^4 = 0$						
s_1, u_1	$u_1^2t_1$	$\langle 96, 64\rangle$	$\langle 48, 3\rangle$	$\mathbb{Q}$	#44	#45
$-48x^3y - 12(6x^2y^2 + 4x^3z) + 72(12x^2yz + 4xy^3) + 120(6x^2y^2 + 12xy^2z + y^4)-$ $-384(4y^3z + 12xyz^2) - 6048y^2z^2 + 7296yz^3 + 7584z^4 = 0$						
s_1, u_1	id	$\langle 96, 72\rangle$	$\langle 48, 3\rangle$	$\mathbb{Q}$	#46	#45
$56x^3y - 21(6x^2y^2 + 4x^3z) + 98(12x^2yz + 4xy^3) - 245(6x^2y^2 + 12xy^2z + y^4)+$ $+833(4y^3z + 12xyz^2) - 14406y^2z^2 + 30184yz^3 - 22638z^4 = 0$						
s_1, t_1, u_1	id	$\langle 192, 956\rangle$	$\langle 96, 64\rangle$	$\mathbb{Q}$	#47	#48
$8x^3y - 3(6x^2y^2 + 4x^3z) + 2(12x^2yz + 4xy^3) - 5(6x^2y^2 + 12xy^2z + y^4)+$ $+5(4y^3z + 12xyz^2) - 42y^2z^2 + 40yz^3 - 12z^4 = 0$						

Table 5.7: Generators for the pairs of groups (G, H) and example twists C of the Fermat quartic in each case. We also show the moment sequences corresponding to C/k and $C/k(i)$.

#	a_i	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9
#1	a_1	0	9	0	243	0	7290	0	229635	0
	a_2	6	54	621	7938	106191	1454355	20212254	283815738	4016375199
	a_3	0	82	0	23574	0	7727410	0	2680982990	0
#2	a_1	0	18	0	486	0	14580	0	459270	0
	a_2	9	99	1215	15795	212139	2907981	40422321	567624915	8032730715
	a_3	0	164	0	47148	0	15454820	0	5361965980	0
#3	a_1	0	5	0	123	0	3650	0	114835	0
	a_2	4	30	319	3994	53169	727395	10106772	141909786	2008193305
	a_3	0	42	0	11798	0	3863850	0	1340493518	0
#4	a_1	0	10	0	246	0	7300	0	229670	0
	a_2	5	51	611	7907	106095	1454061	20211357	283813011	4016366927
	a_3	0	84	0	23596	0	7727700	0	2680987036	0
#5	a_1	0	3	0	81	0	2430	0	76545	0
	a_2	3	21	216	2673	35478	485028	6738147	94607433	1338798294
	a_3	0	28	0	7860	0	2575810	0	893661020	0
#6	a_1	0	6	0	162	0	4860	0	153090	0
	a_2	3	33	405	5265	70713	969327	13474107	189208305	2677576905
	a_3	0	56	0	15720	0	5151620	0	1787322040	0
#7	a_1	0	3	0	81	0	2430	0	76545	0
	a_2	2	18	207	2646	35397	484785	6737418	94605246	1338791733
	a_3	0	28	0	7860	0	2575810	0	893661020	0
#8	a_1	0	3	0	45	0	1110	0	33285	0
	a_2	3	15	114	1227	15528	209202	2893449	40570779	573880632
	a_3	0	16	0	3468	0	1106710	0	383080124	0
#9	a_1	0	6	0	90	0	2220	0	66570	0
	a_2	3	21	201	2373	30813	417675	5784711	81134997	1147741581
	a_3	0	32	0	6936	0	2213420	0	766160248	0
#10	a_1	0	3	0	63	0	1830	0	57435	0
	a_2	2	14	155	1982	26537	363551	5052938	70953530	1004092517
	a_3	0	22	0	5910	0	1932070	0	670248782	0
#11	a_1	0	6	0	126	0	3660	0	114870	0
	a_2	3	27	309	3963	53073	727101	10105875	141907059	2008185033
	a_3	0	44	0	11820	0	3864140	0	1340497564	0
#12	a_1	0	3	0	63	0	1830	0	57435	0
	a_2	3	18	168	2022	26658	363915	5054031	70956810	1004102358
	a_3	0	22	0	5910	0	1932070	0	670248782	0
#13	a_1	0	2	0	42	0	1220	0	38290	0
	a_2	2	12	112	1348	17772	242610	3369354	47304540	669401572
	a_3	0	15	0	3941	0	1288050	0	446832533	0
#14	a_1	0	4	0	84	0	2440	0	76580	0
	a_2	2	18	206	2642	35382	484734	6737250	94604706	1338790022
	a_3	0	30	0	7882	0	2576100	0	893665066	0

#	a_i	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9
#15	a_1	0	1	0	15	0	370	0	11095	0
	a_2	1	5	38	409	5176	69734	964483	13523593	191293544
	a_3	0	6	0	1158	0	368910	0	127693398	0
#16	a_1	0	2	0	30	0	740	0	22190	0
	a_2	1	7	67	791	10271	139225	1928237	27044999	382580527
	a_3	0	12	0	2316	0	737820	0	255386796	0
#17	a_1	0	2	0	33	0	920	0	28735	0
	a_2	2	10	86	1016	13342	181993	2527114	35478682	502051964
	a_3	0	12	0	2966	0	966180	0	335126414	0
#18	a_1	0	4	0	66	0	1840	0	57470	0
	a_2	2	15	158	1991	26562	363621	5053134	70954083	1004094086
	a_3	0	24	0	5932	0	1932360	0	670252828	0
#19	a_1	0	1	0	6	0	70	0	1540	0
	a_2	1	3	12	77	746	9117	122243	1697735	23943936
	a_3	0	3	0	183	0	47040	0	15987279	0
#20	a_1	0	2	0	12	0	140	0	3080	0
	a_2	1	4	19	140	1451	18112	244121	3394376	47884591
	a_3	0	6	0	366	0	94080	0	31974558	0
#21	a_1	0	2	0	42	0	1220	0	38290	0
	a_2	1	9	103	1321	17691	242367	3368625	47302353	669395011
	a_3	0	16	0	3944	0	1288060	0	446832568	0
#22	a_1	0	2	0	24	0	620	0	19180	0
	a_2	1	6	55	670	8871	121254	1684509	23651730	334699075
	a_3	0	10	0	1994	0	644320	0	223420330	0

Table 5.8: The 22 moment sequences that arise for twists of the Klein quartic.

<table>
<tr><th>ID(G)</th><th>ID(H)</th><th>k</th><th>L</th><th>$\#/k$</th><th>$\#/k(\sqrt{-7})$</th></tr>
<tr><td>$\langle 2,1\rangle$</td><td>$\langle 1,1\rangle$</td><td>$\mathbb{Q}$</td><td>$\mathbb{Q}(\sqrt{-7})$</td><td>#1</td><td>#2</td></tr>
<tr><td colspan="6">$x^4+y^4+z^4+6(xy^3+yz^3+zx^3)-3(x^2y^2+y^2z^2+z^2x^2)+3xyz(x+y+z)=0$</td></tr>
<tr><td>$\langle 4,2\rangle$</td><td>$\langle 2,1\rangle$</td><td>$\mathbb{Q}$</td><td>$\mathbb{Q}(\sqrt{-7},i)$</td><td>#3</td><td>#4</td></tr>
<tr><td colspan="6">$49x^4-63x^2y^2+210x^2yz-126x^2z^2+y^4+12y^3z-51y^2z^2+66yz^3-31z^4=0$</td></tr>
<tr><td>$\langle 6,1\rangle$</td><td>$\langle 3,1\rangle$</td><td>$\mathbb{Q}$</td><td>see 3.3 with $p(x)=x^3+x+2$</td><td>#5</td><td>#6</td></tr>
<tr><td colspan="6">$768x^4+144x^2y^2-864x^2yz-48x^2z^2+336xy^3+336xyz^2-672xz^3-$
$-9y^4+108y^3z-318y^2z^2-36yz^3-z^4=0$</td></tr>
<tr><td>$\langle 6,2\rangle$</td><td>$\langle 3,1\rangle$</td><td>$\mathbb{Q}$</td><td>$\mathbb{Q}(\zeta_7)$</td><td>#7</td><td>#6</td></tr>
<tr><td colspan="6">$x^3y+y^3z+z^3x=0$</td></tr>
<tr><td>$\langle 14,1\rangle$</td><td>$\langle 7,1\rangle$</td><td>$\mathbb{Q}$</td><td>see section 3.3 with $\beta_1=\zeta_7+\zeta_7^6$</td><td>#8</td><td>#9</td></tr>
<tr><td colspan="6">$-x^4-8x^3y+5x^3z+18x^2y^2-54x^2yz+30x^2z^2-11xy^3+60xy^2z-$
$-111xyz^2+38xz^3+5y^4-16y^3z+36y^2z^2-25yz^3+3z^4=0$</td></tr>
<tr><td>$\langle 8,1\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}(\sqrt{2},\sqrt{i})$</td><td>$k(\sqrt[8]{-7})$</td><td>#10</td><td>#11</td></tr>
<tr><td colspan="6">$-7x^4+y^4+\frac{9-4\sqrt{2}}{3136}z^4-6x^2y^2-\frac{1-2\sqrt{2}}{7}z^2xy=0$</td></tr>
<tr><td>$\langle 8,3\rangle$</td><td>$\langle 4,1\rangle$</td><td>$\mathbb{Q}$</td><td>$\mathbb{Q}(\sqrt{-7},\sqrt{2+3\sqrt{2}},\sqrt{2-3\sqrt{2}})$</td><td>#12</td><td>#11</td></tr>
<tr><td colspan="6">$49x^4+504x^2y^2-3024x^2yz+1008x^2z^2+232y^4+2368y^3z-$
$-12000y^2z^2+19072yz^3-20576z^4=0$</td></tr>
<tr><td>$\langle 12,4\rangle$</td><td>$\langle 6,1\rangle$</td><td>$\mathbb{Q}$</td><td>see 3.3 with $p(x)=x^3-2x+1$</td><td>#13</td><td>#14</td></tr>
<tr><td colspan="6">$75x^4+630x^2y^2+945x^2yz+420x^2z^2-735xy^3+1470xyz^2+735xz^3-$
$-1764y^4+5292y^3z-6321y^2z^2-3528yz^3-784z^4=0$</td></tr>
<tr><td>$\langle 42,1\rangle$</td><td>$\langle 21,1\rangle$</td><td>$\mathbb{Q}$</td><td>$\mathbb{Q}(\zeta_7,\sqrt[7]{2})$</td><td>#15</td><td>#16</td></tr>
<tr><td colspan="6">$2x^3y+y^3z+z^3x=0$</td></tr>
<tr><td>$\langle 16,7\rangle$</td><td>$\langle 8,3\rangle$</td><td>$\mathbb{Q}(\sqrt{2})$</td><td>$k(i,\sqrt[8]{-7})$</td><td>#17</td><td>#18</td></tr>
<tr><td colspan="6">$-7x^4+y^4+\frac{9-4\sqrt{2}}{3136}z^4-6x^2y^2-\frac{1-2\sqrt{2}}{7}z^2xy=0$</td></tr>
<tr><td>$\langle 336,208\rangle$</td><td>$\langle 168,42\rangle$</td><td>$\mathbb{Q}$</td><td>see section 4.1</td><td>#19</td><td>#20</td></tr>
<tr><td colspan="6">$-2x^4+7x^3z+3x^2y^2-12x^2z^2-6xyz^2+10xz^3+2y^3z-6y^2z^2+8yz^3-4z^4=0$</td></tr>
<tr><td>$\langle 12,3\rangle$</td><td>$\langle 12,3\rangle$</td><td>$\mathbb{Q}(\sqrt{-7})$</td><td>$k(\sqrt{a},\sqrt{b},\sqrt{c})$ with a,b,c the roots of $x^3+x-2=0$</td><td>#21</td><td>#21</td></tr>
<tr><td colspan="6">$7x^4-84x^3y-28x^3z-(6+12\alpha)x^2y^2+(204+72\alpha)x^2yz+(114-108\alpha)x^2z^2+$
$+(32+36\alpha)xy^3-(168+84\alpha)xy^2z-(192+132\alpha)xyz^2-(200-132\alpha)xz^3+$
$+(46-27\alpha)y^4-(88+36\alpha)y^3z+(346+78\alpha)y^2z^2-$
$-(264-60\alpha)yz^3+(22-75\alpha)z^4=0$</td></tr>
<tr><td>$\langle 24,12\rangle$</td><td>$\langle 24,12\rangle$</td><td>$\mathbb{Q}(\sqrt{-7})$</td><td>$k(\sqrt{a},\sqrt{b},\sqrt{c})$ with a,b,c the roots of $x^3-2x-1=0$</td><td>#22</td><td>#22</td></tr>
<tr><td colspan="6">$56x^4+168x^3y+448x^3z+(96+192\alpha)x^2y^2+(816+288\alpha)x^2yz+(1272+108\alpha)x^2z^2+$
$+(128+144\alpha)xy^3+(564+876\alpha)xy^2z+(1536+1056\alpha)xyz^2+(648-216\alpha)xz^3+$
$+(185+27\alpha)y^4+(704+288\alpha)y^3z+(1188+948\alpha)y^2z^2+$
$+(1320+960\alpha)yz^3+(836+300\alpha)z^4=0$</td></tr>
</table>

Table 5.9: Examples twists for the pairs (G,H) of the Klein quartic. We show the field k over which the equation of the twist is defined and the field L of definition of the twist. In the last two rows we enumerate the Sato-Tate distribution of the twist over k and over $k(\sqrt{-7})$.

$m = 5$	1	2
1	0	0
2	0	1

$m = 6$	1
1	0
2	0

$m = 7$	1	2	3
1	0	0	0
2	0	0	1
3	0	1	0

$m = 8$	1	3
1	0	0
2	0	1
3	0	0

$m = 9$	1	2	4
1	0	0	0
2	0	0	1
3	0	0	0
4	0	1	1

$m = 10$	1	3
1	0	0
2	0	0
3	0	1
4	0	0

$m = 11$	1	2	3	4	5
1	0	0	0	0	0
2	0	0	0	1	1
3	0	0	1	0	0
4	0	0	0	0	1
5	0	1	0	1	0

$m = 12$	1	5
1	0	0
2	0	1
3	0	0
4	0	1
5	0	0

$m = 13$	1	2	3	4	5	6
1	0	0	0	0	0	0
2	0	0	0	0	1	1
3	0	0	0	1	0	0
4	0	0	1	0	0	1
5	0	0	0	0	1	0
6	0	1	0	1	0	1

$m = 14$	1	3	5
1	0	0	0
2	0	0	1
3	0	0	0
4	0	1	0
5	0	0	1
6	0	0	0

$m = 15$	1	2	4	7
1	0	0	0	0
2	0	0	0	1
3	0	0	1	0
4	0	0	0	1
5	0	0	0	0
6	0	0	0	1
7	0	1	1	0

$m = 16$	1	3	5	7
1	0	0	0	0
2	0	0	0	1
3	0	0	1	0
4	0	0	0	1
5	0	1	0	0
6	0	0	1	1
7	0	0	0	0

$m = 17$	1	2	3	4	5	6	7
1	0	0	0	0	0	0	0
2	0	0	0	0	0	1	1
3	0	0	0	0	1	0	0
4	0	0	0	1	0	0	1
5	0	0	1	0	0	1	0
6	0	0	0	0	1	0	0
7	0	0	0	0	0	0	1
8	0	1	0	1	0	1	0

$m = 18$	1	5	7
1	0	0	0
2	0	0	1
3	0	1	0
4	0	0	0
5	0	0	1
6	0	0	0
7	0	1	1
8	0	0	0

$m = 19$	1	2	3	4	5	6	7	8	9
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	1	1	1
3	0	0	0	0	1	1	0	0	0
4	0	0	0	1	0	0	0	1	1
5	0	0	0	0	0	0	1	0	0
6	0	0	1	0	0	1	0	0	1
7	0	0	0	0	1	0	0	1	0
8	0	0	0	0	0	0	1	0	1
9	0	1	0	1	0	1	0	1	0

$m = 20$	1	3	7	9
1	0	0	0	0
2	0	0	1	1
3	0	0	0	0
4	0	0	0	1
5	0	0	1	0
6	0	1	0	1
7	0	0	0	0
8	0	0	1	1
9	0	0	0	0

$m = 21$	1	2	4	5	8	10
1	0	0	0	0	0	0
2	0	0	0	0	1	1
3	0	0	0	0	0	0
4	0	0	0	1	0	1
5	0	0	1	0	1	0
6	0	0	0	0	0	1
7	0	0	0	0	1	0
8	0	0	0	1	0	1
9	0	0	0	0	0	0
10	0	1	1	0	1	1

$m = 22$	1	3	5	7	9
1	0	0	0	0	0
2	0	0	0	0	1
3	0	0	0	1	0
4	0	0	1	0	1
5	0	0	0	0	0
6	0	0	0	1	0
7	0	1	0	0	1
8	0	0	1	0	0
9	0	0	0	1	1
10	0	0	0	0	0

$m = 23$	1	2	3	4	5	6	7	8	9	10	11
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	1	1	1	1
3	0	0	0	0	0	1	1	0	0	0	0
4	0	0	0	0	1	0	0	0	0	1	1
5	0	0	0	1	0	0	0	1	1	0	0
6	0	0	0	0	0	0	1	0	0	1	1
7	0	0	1	0	0	1	0	0	1	0	0
8	0	0	0	0	0	0	0	1	0	0	1
9	0	0	0	0	1	0	1	0	0	1	0
10	0	0	0	0	0	0	0	0	1	0	1
11	0	1	0	1	0	1	0	1	0	1	0

$m = 24$	1	5	7	11
1	0	0	0	0
2	0	0	0	1
3	0	0	1	0
4	0	1	0	1
5	0	0	0	0
6	0	0	1	1
7	0	0	0	0
8	0	0	0	1
9	0	1	0	0
10	0	0	1	1
11	0	0	0	0

$m = 25$	1	2	3	4	6	7	8	9	11	12
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	1	1	1
3	0	0	0	0	0	1	1	0	0	0
4	0	0	0	0	1	0	0	0	1	1
5	0	0	0	0	0	0	0	1	0	0
6	0	0	0	1	0	0	1	0	1	1
7	0	0	0	0	0	1	0	0	0	0
8	0	0	1	0	1	0	0	1	0	1
9	0	0	0	0	0	0	1	0	1	0
10	0	0	0	0	0	1	0	0	0	1
11	0	0	0	0	0	0	0	1	1	0
12	0	1	0	1	1	0	1	0	0	1

Matrix $C = \{c_i(t)\}_{i,t=1,\ldots,k,\,(t,m)=1}$ for $m = 5, \ldots, 25$.

Bibliography

[1] S.S. Abhyankar, *Resolution of singularities of arithmetical surfaces*, Arithmetical Algebraic Geometry, Harper and Row, New York, 1965.

[2] G. Banaszak, K. Kedalaya, *An algebraic Sato-Tate group and Sato-Tate conjecture*, to appear in Indiana University Mathematics Journal.

[3] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, Publ. RIMS 47, 29-98, 2011.

[4] F. Bars, *Automorphism groups of genus 3 curves*, Notes del Seminari de teoria de Nombres (UB-UAB-UPC), 2006.

[5] B.C. Berndt, R.J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, Inc., 1998.

[6] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24, 235-265, 1997.

[7] L.Brunjes, *Forms of Fermat equations and their Zeta functions*, World Scientific Publishing, 2004.

[8] G. Cardona, *Models Racionals de Corbes de Genere 2*, thesis, 2001.

[9] G. Cardona, *Representations of G_k-groups and twists of the genus two curve $y^2 = x^5 - x$*, Journal of Algebra 303, 707-721, 2006.

[10] D. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, Inc., 1989.

[11] P. Deligne, S. Milne, A. Ogus, K.- Y. Shih, *Hodge Cycles, Motives, and Shimura Varieties*, Lecture Notes in Math. 900, Springer-Verlag, 1982.

[12] N. D. Elkies, *The Klein quartic in Number Theory*, The Eightfold Way MSRI Publications, Volume 35, 1998.

[13] J. Fernández, J. González, J.-C. Lario, *Plane quartic twists of* $X(5,3)$, Canadian Mathematical Bulletin 50, 196-205, 2007.

[14] J. Fernández, J.-C. Lario, A. Río, *On twists of the modular curves X(p)*, Bull. London Math. Soc. 37, 342-350, 2005.

[15] F. Fité, *L-functions and Artin representations attahed to twisted abelian varieties*, thesis, 2011.

[16] F. Fité, *Equidistribution, L-functions, and Sato-Tate groups*, submitted.

[17] F. Fité, J. González, J.-C. Lario, *Frobenius distribution for quotients of Fermat curves of prime exponent* , submitted.

[18] F. Fité, K. Kedalya, V. Rotger, A. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compositio Mathematica 148, n. 5, 1390-1442, 2012.

[19] F. Fité, K. Kedlaya, A. Sutherland, *Sato-Tate groups of some weight 3 motives*, submitted.

[20] F. Fité, J.-C. Lario, *The twisting representation of the L-function of a curve*, Revista MatemÃ¡tica Iberoamericana, 29 No. 3, 749-764, 2013.

[21] F. Fité, E. Lorenzo, A. Sutherland, *Sato-Tate distributions of twists of the Fermat and Klein quartics*, preprint.

[22] F. Fité, A. Sutherland, *Sato-Tate distributions of twists of* $y^2 = x^5 - x$ *and* $y^2 = x^6 + 1$, to appear in Algebra & Number Theory.

[23] J.M. Gamboa, J.M. Ruíz, *Anillos y cuerpos conmutativos*, Manual UNED, 2003.

[24] The GAP Group, GAP -Groups, *Algorithms, and Programming*, Version 4.5.7, 2012. (http://www.gap-system.org)

[25] M. Girard, D.R. Kohel, *Classification of Genus 3 Curves in Special Strata of the Moduli Space*, chapter of the book *Algorithmic Number Theory*, Springer, 2006.

[26] M. Girard, D.R. Kohel, C. Ritzenthaler, *Dixmier and Ohno Invariants of Ternary Quartics*, SAGE code, http://sage.math.washington.edu/home/wstein/www/home/kohel/shr/src/Geometry/CrvG3/dixmier_ohno.m, 2004.

[27] E. Z. Goren, *Gauss and Jacobi sums, Weil Conjectures*, Seminar on Cohomology Theories of McGill University, 2004.

[28] F. Q. Gouvêa, N. Yui, *Arithmetic of Diagonal Fermat Hypersurfaces over Finite Fields*, Cambridge University Press, 1995.

[29] E. Halberstadt, A. Kraus, *Sur la courbe modulaire* $X_E(7)$, Experiment. Math. Volume 12, Issue 1, 27-40, 2003.

[30] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehun- gen zur Verteilung der Primzahlen*, Zweite Mitteilung, Math. Zeit. 6, 11-51, 1920.

[31] P. Henn, *Die Automorphismengruppen dar algebraischen Funktionenkorpar vom Geschlecht 3*, Inaugural-dissertation, Heidelberg, 1976.

[32] A. Hurwitz, *Uber algebraische Gebilde mit Eindeutigen Transformationen in sich*, Mathematische Annalen 41 (3): 403-442, 1893.

[33] C. Jensen, A. Ledet, N. Yui, *Generic Polynomials. Constructive Aspects of the Inverse Galois Problem*, Cambrigde University Press, 2002.

[34] C. Johansson, *On the Sato-Tate Conjecture for non-generic abelian surfaces*, submitted.

[35] K. Kedlaya, A. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic Number Theory Symposium - ANTS VIII, Lecture Notes in Comp. Sci. 5011, Springer, 312-326, 2008.

[36] N. Koblitz, D. Rohrlich, *Simple Factors in the Jacobian of a Fermat curve*, Can. J. Math., Vol. XXX, No. 6, 1183-1205, 1978.

[37] J. Kollár, K.E. Smith, A. Corti, *Rational and Nearly Rational Varieties*, Cambridge studies in advances mathematics 92, Cambridge University Press, 2004.

[38] R. Lercier, C. Ritzenthaler, F. Rovetta, J. Sijsling, *Spanning the moduli space of curves and applications to smooth plane quartics over finite fields*, to appear in the proceedings of ANTS XI.

[39] G. Malle, *Multi-parameter Polynomials with Given Galois Group*, J. Symbolic Computation 30, 717-731, 2000.

[40] S. Meagher, J. Top, *Twists of genus three curves over finite fields.* Finite Fields and Their Applications 16(5): 347-368 (2010).

[41] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number fields*, Grundlehren der mathematischen Wissenschaften, vol. 323, Springer-Verlag, 2000.

[42] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. 77, 89-92, 1916.

[43] B. Poonen, E. F. Schaefer, M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$*, Duke Math. J. Volume 137, Number 1, 103-158, 2007.

[44] J. Quer, *Liftings of projective 2-dimensional Galois representations and embedding problems*, Journal of Algebra 171, 541-566, 1995.

[45] A. Reverte, N. Vila, *Images of mod p Galois representations associated to elliptic curves*, Canad. Math. Bull. Vol. 44(3), 313-322, 2001.

[46] E. Reyssat, *Quelques aspects des surfaces de Riemann*, Progress in Mathematics, 1977.

[47] D. Rohrlich, *The periods of the Fermat curve*, Appendix to B. Gross, Invent. Math. 45, 193-211, 1978.

[48] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, Research Notes in Mathematics 7, A K Peters, 1968.

[49] J.-P. Serre, *Galois Cohomology*, Springer-Velarg, 1997.

[50] J.-P. Serre, *Topics in Galois Theory*, A.K. Peters, 2008.

[51] J.-P. Serre, *Lectures on NX(p)*, A.K. Peters, 2012.

[52] G. Shimura, Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, The Mathematical Society of Japan, 1961.

[53] T. Shioda, *The Hodge conjecture for Fermat varieties*, Math. Ann., 245, 175-184, 1979.

[54] T. Shioda, *Geometry of Fermat varieties* in Number Theory Related to Fermat's Last Theorem, Progress in Math., 26, 45- 56, 1982.

[55] J.H. Silverman, *The aritmetic of elliptic curves*, Springer, 1986.

[56] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

[57] A. Sutherland, preliminar algorithm for counting points over finite fields of non-hyperelliptic curves.

[58] D. Swinarski, *Equations of Riemann surfaces of genus 4,5 and 6 with large automorphim groups*, preprint.

[59] A. M. Vermuelen, *Weierstrass pointss of weight two on curves of genus three*, thesis, 1983.

[60] A. Weil, *Number of solutions of equations in finite fields*, Bulletin if the American Mathematical Society, 55(1), 497-508, 1949.

[61] A. Weil, *Jacobi sums as Grossencharaktere*, Trans. Amer. Math. Soc. 73, 48-495, 1952.

[62] A. Weil, *The field of definition of a variety*, Am. J. of Math. 78, 509-524, 1956.