Models of Genus One Curves

Mohammad Sadek
Fitzwilliam College, Cambridge

This dissertation is submitted for the degree of
Doctor of Philosophy

December 2009

Declaration

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration. No part of this dissertation has been submitted for any other qualification.

Acknowledgements

I am indebted to my supervisor, Tom Fisher, for encouragement, guidance, inspiration, and for suggesting the topic of the thesis to me.

I acknowledge with gratitude the financial support of Cambridge Overseas Trust. I also wish to thank the Department of Pure Mathematics and Mathematical Statistics of the University of Cambridge for funding my research trips.

Finally, I would like to thank my parents and sisters for all their love, support, and patience.

Models of Genus One Curves

Mohammad Sadek

Summary

In this thesis we give insight into the minimisation problem of genus one curves defined by equations other than Weierstrass equations. We are interested in genus one curves given as double covers of $\mathbb{P}^1$, plane cubics, or complete intersections of two quadrics in $\mathbb{P}^3$. By minimising such a curve we mean making the invariants associated to its defining equations as small as possible using a suitable change of coordinates. We study the non-uniqueness of minimisations of the genus one curves described above. To achieve this goal we investigate models of genus one curves over Henselian discrete valuation rings. We give geometric criteria which relate these models to the minimal proper regular models of the Jacobian elliptic curves of the genus one curves above. We perform explicit computations on the special fibers of minimal proper regular models of elliptic curves. Then we use these computations to count the number of minimisations of a genus one curve defined over a Henselian discrete valuation field. This number depends only on the Kodaira symbol of the Jacobian and on an auxiliary rational point. Finally, we consider the minimisation problem of a genus one curve defined over $\mathbb{Q}$.

Contents

Chapter 1

Introduction

Let E be an elliptic curve defined over a number field K. The problem of finding the Mordell-Weil group $E(K)$ has been a target for an enormous amount of research. It is known that $E(K)$ is a finitely generated abelian group. Furthermore, to determine $E(K)$ we only need to find $E(K)/nE(K)$ for any integer $n \geq 2$. The method of n-descent is one of the methods which enable us to get a bound on $E(K)/nE(K)$, $n \geq 2$. Indeed, the n-descent computes the n-Selmer group of E which contains $E(K)/nE(K)$. The difference between the two groups is the n-torsion of the Tate-Shafarevich group of E/K.

An element of the n-Selmer group can be represented as a geometric object, namely as a double cover of $\mathbb{P}^1$ ramified in four points when $n = 2$, a plane cubic curve when $n = 3$, an intersection of two quadrics in $\mathbb{P}^3$ when $n = 4$. It follows from the definition of the n-Selmer group that each of these curves has points everywhere locally. The equations defining these genus one curves will be called *genus one equations of degree n*. See §2.1 for the precise definitions of genus one equations and their invariants.

For using n-descent to search for points on E, we need the coefficients of the genus one equations described above to be small. The solution has two parts: Reduction and Minimisation. By reducing genus one equations, we mean reducing the size of the coefficients by a unimodular linear change of coordinates, which does not change the invariants. The problem of reduction is treated in [9] when $n = 2$, and in [11] when $n = 2, 3, 4$. To minimise genus one equations, we need to make the associated invariants smaller. The minimisation problem has been investigated intensively, for example see [4] and [29] for $n = 2$, [14] for $n = 3$, and [30] for $n = 4$. An algorithmic approach to the minimisation problem can be found in [11]. In this thesis we will be interested in the minimisation question.

The question of minimisation has a local nature. More precisely, we minimise genus one equations of degree n over local fields. Usually, there are many further details to consider when the residue field is not algebraically closed. Therefore, we prefer studying genus one equations over strict Henselisations of local fields because these fields have algebraically closed residue fields. Thus we assume that our base field K is a Henselian discrete valuation field with ring of integers $\mathcal{O}_K$ and algebraically closed residue field k. Moreover, since our genus one curves represent elements in n-Selmer groups, they have rational points everywhere locally. Therefore, when we treat a genus one curve C over K, we will assume that $C(K) \neq \emptyset$. It has been shown in [11] that if C is defined by a genus one equation ϕ of degree n, and $C(K) \neq \emptyset$, then the minimal discriminant associated to ϕ has the same valuation as the minimal discriminant associated to the Jacobian elliptic curve.

Unlike elliptic curves, the minimisations of the genus one curves described above are not unique under the action of the group $\mathcal{G}_n(\mathcal{O}_K)$ defined in §2.1. We give the following example to illustrate that a genus one equation of degree 2 might have more than one minimisation. We consider the elliptic curve $E : y^2 + y = x^3 + x^2 - 83x + 244$. We use MAGMA, see [6], to perform 2-descent on E. We obtain the following genus one equation $\phi : y^2 = f(x) = 5x^4 + 20x^3 + 10x^2 - 40x + 25$. We apply the $\mathcal{G}_2(\mathbb{Z}_5)$-transformation

$$(1, A), \text{ where } A = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix},$$

to move the zeros of $f(x)/5$ to 0 and ∞. Then we are able to apply the $\mathcal{G}_2(\mathbb{Q}_5)$-transformations given by $(1/25, \mathrm{diag}(5, 1))$ and $(1/25, \mathrm{diag}(1, 5))$, so that we have the following three minimal genus one equations which lie in the same $\mathcal{G}_2(\mathbb{Q}_5)$-equivalence class.

$$\begin{aligned} y^2 &= 27500x^4 + 17000x^3 + 4000x^2 + 416x + 16, \\ y^2 &= 1100x^4 + 3400x^3 + 4000x^2 + 2080x + 400, \\ y^2 &= 44x^4 + 680x^3 + 4000x^2 + 10400x + 10000. \end{aligned}$$

It can be shown that the transformations stated above are the only ones relating these genus one equations. Therefore, the genus one equations written above lie in three distinct $\mathcal{G}_2(\mathbb{Z}_5)$-equivalence classes. In this thesis we study the non-uniqueness of minimisation by considering the problem geometrically. In fact, since E has reduction of type IV* over $\mathbb{Q}_5$, Corollary 8.1.4 tells us that the number of $\mathcal{G}_2(\mathbb{Z}_5)$-equivalence classes lying in the $\mathcal{G}_2(\mathbb{Q}_5)$-equivalence class containing ϕ is exactly 3.

The knowledge of all possible minimisations of a genus one curve can be exploited to find rational points on elliptic curves. In fact, rational points on genus one curves, defined by minimal genus one equations of degree n, can be expected to be reasonably of smaller height, and therefore will be found more easily. Our results on the number of minimisations will be used to study heights on such genus one curves in [26].

In Chapter 3 we generalise the terminology of minimal Weierstrass models for elliptic curves to *minimal degree-n-models* for genus one curves. In fact, we define a degree-n-model for a genus one curve $C \to \mathbb{P}_K^{n-1}$ to be a pair $(\mathcal{C}, \alpha)$ consisting of a $\operatorname{Spec} \mathcal{O}_K$-scheme $\mathcal{C}$ defined by an integral genus one equation of degree n, and an isomorphism α from the generic fiber $\mathcal{C}_K$ of $\mathcal{C}$ onto C, where α is defined by an element in $\mathcal{G}_n(K)$. Now we show why we insist on remembering the isomorphism α in our definition of a degree-n-model. In the case $C(K) \neq \emptyset$, we pick $P \in C(K)$. Then we identify the group structure on (C, P) with the group structure on the Jacobian elliptic curve E. The automorphism group $\operatorname{Aut}(C)$ of C fits in an exact sequence

$$0 \to E \to \operatorname{Aut}(C) \to \operatorname{Aut}(E, 0) \to 0.$$

The first map is $Q \mapsto \tau_Q$, where τ_Q is the translation by Q. Let H be a hyperplane section on C. We are interested in automorphisms λ of C such that $\lambda^* H \sim H$. But $\tau_Q^* H \sim H$ if and only if $nQ = 0$. Hence the elements of $\mathrm{PGL}_n(K)$ that act fixed-point-free on C correspond precisely to $E[n](K)$. Therefore, we can have more than one K-isomorphism between $\mathcal{C}_K$ and C.

For example, we consider the elliptic curve $E : y^2 = x^3 - x^2 - 113x + 516$ which has a non-trivial 2-torsion point $(-12, 0)$. Performing 2-descent on E will yield the genus one equation $\phi : y^2 = -3x^4 - 56x^3 - 399x^2 - 1274x - 1519$. We notice that $\phi' : y^2 = -147x^4 - 392x^3 - 399x^2 - 182x - 31$ is a genus one equation which lies in the $\mathcal{G}_2(\mathbb{Q}_7)$-equivalence class containing ϕ. The following two $\mathcal{G}_2(\mathbb{Q}_7)$-transformations carry ϕ to ϕ'.

$$T_1 = (1/7^2, \operatorname{diag}(7, 1)), \text{ and, } T_2 = (1, A) \text{ where } A = \begin{pmatrix} -7 & 1 \\ -6 & 1 \end{pmatrix}.$$

Moreover, the transformation T_1 is an element in $\mathcal{G}_2(\mathbb{Q}_7) \setminus \mathcal{G}_2(\mathbb{Z}_7)$ while T_2 is in $\mathcal{G}_2(\mathbb{Z}_7)$. The genus one equations ϕ and ϕ' lie in the same $\mathcal{G}_2(\mathbb{Z}_7)$-equivalence class because they are related via the transformation T_2. Let $\mathcal{C}'$ be the $\operatorname{Spec} \mathcal{O}_K$-scheme defined by ϕ'. We distinguish between the two degree-2-models $(\mathcal{C}', \alpha_1)$ and $(\mathcal{C}', \alpha_2)$, where α_1 and α_2 are defined by T_1 and T_2 respectively. The reason is that the special fibers of these two models have different representatives in the special fiber of the minimal proper regular model of the Jacobian.

It is known that an integral Weierstrass equation defining a Weierstrass model W for an elliptic curve E is minimal if the minimal desingularisation of W is isomorphic to the minimal proper regular model of E. The analogous result for the case $n = 2$ has been proved by Liu in [18]. Liu obtained his results using hyperelliptic involutions defined on double covers of the projective line. We use our knowledge of invariant theory of genus one curves to give geometric criteria for the minimality of genus one equations of degree n for $n \leq 4$, see Chapter 4.

In what follows we try to describe briefly how Liu obtained his results, and why we did not use the hyperelliptic involution method to obtain our results. We suppose C is a smooth curve defined by a minimal genus one equation. Let C^{min} be the minimal proper regular model of C. Since we assume $C(K) \neq \emptyset$, there exists a divisor of degree 2 on C. This divisor defines a separable morphism $C \to \mathbb{P}^1_K$ of degree 2. The generator of $\mathrm{Gal}(K(C)/K(\mathbb{P}^1_K))$ induces an automorphism σ of order 2 on C. We call σ a hyperelliptic involution. Now σ extends to an automorphism $\tilde{\sigma}$ on C^{min}. If Γ is an irreducible component of multiplicity-1 in the special fiber of $C^{min}/\langle\tilde{\sigma}\rangle$, then we can find a model $\mathbb{P}^1$ of $\mathbb{P}^1_K$ which is birational to $C^{min}/\langle\tilde{\sigma}\rangle$ in a neighborhood of the generic point of Γ. Liu produced models for C by taking the normalisation of $\mathbb{P}^1$ in C. The reason why we could not use this method to construct minimal degree-n-models for C, when $n = 3, 4$, is that it only gives models for $C \to \mathbb{P}^1_K$, i.e., it gives models for C when C is viewed as a double cover of the projective line. Moreover, even if we consider the models produced as $\mathrm{Spec}\,\mathcal{O}_K$-schemes, then the special fibers of these models either consist of one irreducible component of multiplicity-m, $m \leq 2$, or two irreducible components of multiplicity-1. So, for example, we can not recover degree-n-models which contain irreducible components of multiplicity-3 in their special fibers. But when $n = 3, 4$, there are degree-n-models whose special fibers contain irreducible components of multiplicity-3.

In Chapter 5 we give a necessary and sufficient condition for degree-n-models to be isomorphic. In Chapter 6 we perform some explicit computations on the minimal proper regular model of an elliptic curve. These computations are used to count minimal degree-n-models for a soluble smooth genus one curve $C \to \mathbb{P}^{n-1}_K$, up to isomorphism, in Chapter 7. Liu proved that there is a bijection between minimal degree-2-models for $C \to \mathbb{P}^1_K$, up to isomorphism, and the multiplicity-1 irreducible components in the special fiber of the quotient of the minimal proper regular model by a hyperelliptic involution, see ([18], Corollaire 5). Our results relate the number of minimal degree-n-models for $C \to \mathbb{P}^{n-1}_K$ when $n \in \{2, 3, 4\}$, up to isomorphism, to the cardinality of a finite set which depends only on the Kodaira Symbol of the Jacobian of C and on an auxiliary rational point, see Theorem 7.1.1.

Finding all integral genus one equations of degree 2 which have the same invariants, up to $\mathcal{G}_2(\mathbb{Q})$-equivalence, is an essential part of the 2-descent algorithm described by

Birch and Swinnerton-Dyer in [4]. The algorithm makes use of the fact that each $\mathcal{G}_2(\mathbb{Q})$-equivalence class contains at least one reduced genus one equation of degree 2. Theorem 1 of [4] proves that reduced genus one equations of degree 2 are finite in number. The problem of counting all the binary forms

$$f(x,z) = a_0x^n + a_1x^{n-1}z + \ldots + a_nz^n,$$

with $\mathbb{Z}$-coefficients and the same invariants, up to $\mathrm{GL}_2(\mathbb{Z})$-equivalence, is a classical problem. For example, Theorem 1 of ([23], Chapter 18) asserts that the number of such equivalence classes is finite. In a series of papers Bhargava studied the number of many forms and tuples of forms, up to some equivalence relations defined over $\mathbb{Z}$. He presented interesting counting results for these equivalence classes. Moreover, he defined composition laws on the equivalence classes of these objects. See [3] for some of Bhargava's results.

Our work contributes to the problem of counting forms and pairs of forms up to relations defined over $\mathbb{Z}$. In fact, we fix a $\mathcal{G}_n(\mathbb{Q})$-equivalence class of genus one equations of degree n, whose invariants are as small as possible, then we count the number of $\mathcal{G}_n(\mathbb{Z})$-equivalence classes within this $\mathcal{G}_n(\mathbb{Q})$-equivalence class. We use arithmetic-geometric methods to tackle this problem.

In Chapter 8 we get rid of the assumption that the residue field is algebraically closed, and count the number of minimal degree-n-models for genus one curves defined over p-adic fields. When the reduction of the Jacobian is split, we show that the number of minimal degree-n-models for a genus one curve defined over a p-adic field is the same as that number over the maximal unramified extension of the p-adic field. But maximal unramified extensions are Henselian discrete valuation fields with algebraically closed residue fields, and the number of models in this case is obtained in Chapter 7. Then we work out how this number changes when the reduction of the Jacobian is non-split. This step is a basic ingredient in counting minimal global degree-n-models for genus one curves defined over $\mathbb{Q}$. Our methods can be generalised easily to find the number of minimal global degree-n-models for genus one curves defined over number fields with class number one, as the problem reduces to considering genus one curves locally over completions of number fields at non-archimedean places.

In Appendix A we work over complete discrete valuation fields with algebraically closed residue fields. We treat the case when the genus one curve has no rational point on it. We prove, using explicit computations, that the number of minimal degree-n-models for such a curve is n when $n \in \{2, 3\}$. Then we give an example to show that the number of minimal degree-4-models for insoluble genus one curves can become arbitrarily large.

We have to mention that we proved our counting results only when the residue field has characteristic greater than 3. We believe that similar results hold when the residue characteristic is 3 but we have not checked the details. When the residue characteristic is 2, we believe that our counting results hold for minimal degree-n-models, when $n = 3, 4$, but the problem needs deeper analysis. When the residue characteristic is 2 and $n = 2$, we have to consider generalised genus one equations of degree 2, i.e., genus one equations of the form $\phi : y^2 + g(x)y = f(x)$, where $\deg g \leq 2$ and $\deg f \leq 4$. Moreover, the invariants associated to ϕ are more complicated. When $n = 2$, Liu's treatment of the problem provided him with results when the residue characteristic is 2, see [18].

Chapter 2

Preliminaries

2.1 Genus one equations of degree n

In this section we will give a brief description of several genus one curves and the equations defining them. We work over a perfect field K with algebraic closure $\overline{K}$. We write $G_K = \mathrm{Gal}(\overline{K}/K)$. We assume further that $\mathrm{char}(K) \neq 2, 3$.

By a *K-curve*, or a *curve over K*, we mean a proper K-scheme that is geometrically connected and of dimension 1.

Let C be a smooth curve of genus one over K. The function field of C will be denoted by $K(C)$. By a closed point $P \in C$ we mean the G_K-orbit of P considered as a geometric point in $C(\overline{K})$. The *divisor group* of C, called $\mathrm{Div}(C)$, is the free abelian group generated by the closed points of C, i.e., a divisor $D \in \mathrm{Div}(C)$ is a formal sum

$$D = \sum_{P \in C} n_P(P)$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many closed points $P \in C$. The divisor D is said to be *effective* if $n_P \geq 0$ for every $P \in C$. The degree of D is defined by

$$\deg D = \sum_{P \in C} n_P[K(P) : K].$$

Let $C_{\overline{K}} = C \times_K \overline{K}$. If we assume that the G_K-orbit of P is $\{P_1, \ldots, P_{d_P}\}$, where $d_P = [K(P) : K]$, then we get a map

$$\mathrm{Div}(C) \to \mathrm{Div}(C_{\overline{K}}),\ \sum n_P(P) \mapsto \sum n_P(\sum_{i=1}^{d_P} P_i).$$

We define an action of G_K on $\mathrm{Div}(C_{\overline{K}})$ in the following way:

$$\sigma : \sum_{P\in C(\overline{K})} n_P(P) \mapsto \sum_{P\in C(\overline{K})} n_P(P^\sigma).$$

Now we obtain $\mathrm{Div}(C)$ as the subgroup of G_K-invariant divisors of $\mathrm{Div}(C_{\overline{K}})$. In other words, we have

$$\mathrm{Div}(C) = \mathrm{Div}(C_{\overline{K}})^{G_K}.$$

We will call a divisor $D \in \mathrm{Div}(C)$ a *K-rational divisor on C*.

The local ring of C at P will be denoted by $\mathcal{O}_{C,P}$. The ring $\mathcal{O}_{C,P}$ is a discrete valuation ring with maximal ideal $\mathfrak{m}_P$ and valuation ν_P.

Let $f \in K(C)^*$. Then we can associate to f the divisor

$$\mathrm{div}(f) = \sum_{P\in C} \nu_P(f)(P).$$

A divisor $D \in \mathrm{Div}(C)$ is said to be *principal* if $D = \mathrm{div}(f)$ for some $f \in K(C)^*$. Two divisors D_1, D_2 are *linearly equivalent*, denoted $D_1 \sim D_2$, if $D_1 - D_2$ is principal. The *divisor class* $[D]$ of a divisor $D \in \mathrm{Div}(C)$ is the set of all divisors linearly equivalent to D. The quotient of $\mathrm{Div}(C)$ by the subgroup of principal divisors is the *Picard group* of C, denoted $\mathrm{Pic}(C)$.

Let $D \in \mathrm{Div}(C)$ be of degree $n > 0$. Set

$$\mathcal{L}(D) = \{f \in K(C)^* | \, \mathrm{div}(f) + D \text{ is effective}\} \cup \{0\}.$$

Then Riemann-Roch Theorem implies that $\dim_K \mathcal{L}(D) = \deg D$.

In what follows we aim to write explicit equations for the pair $(C, [D])$ when $n = 1, 2, 3, 4$, see [1]. We assume A is a Dedekind domain.

Genus one equations of degree 1

If $\deg D = 1$, then any effective rational divisor linearly equivalent to D is a rational point $P \in C(K)$. Let $x, y \in K(C)$ be such that $\mathcal{L}(2(P))$ and $\mathcal{L}(3(P))$ have bases $\{1, x\}$ and $\{1, x, y\}$ respectively. Note that x has a pole of exact order 2 at P, and y has a pole of exact order 3 at P. There is a linear dependence relation between the 7 elements $1, x, y, x^2, xy, x^3, y^2$ in the 6-dimensional space $\mathcal{L}(6(P))$. Furthermore, the coefficients of x^3 and y^2 are non-zero. Rescaling x and y this linear dependence relation can be assumed to be

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \; a_i \in K. \tag{2.1}$$

We will call the Weierstrass equation (2.1) a *genus one equation of degree* 1.

Two genus one equations of degree 1 with coefficients in A are A-*equivalent*, sometimes we will write $\mathcal{G}_1(A)$-equivalent, if they are related by the substitutions

$$x' = u^2x + r,\ y' = u^3y + su^2x + t,\ r, s, t \in A,\ u \in A^*.$$

The group $\mathcal{G}_1(A)$ is the group of all such transformations $[u; r, s, t]$. We define $\det([u; r, s, t]) = u^{-1}$.

We will write down the standard notations $b_2, b_4, b_6, b_8, c_4, c_6$, and the *discriminant* Δ associated to equation (2.1), see ([27], Chapter III).

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned} \tag{2.2}$$

It is easy to verify that $1728\Delta = c_4^3 - c_6^2$.

Genus one equations of degree 2

If $\deg D = 2$, then we pick $x, y \in K(C)$ such that $\mathcal{L}(D)$ and $\mathcal{L}(2D)$ have bases $\{1, x\}$ and $\{1, x, y, x^2\}$. The 9 elements $1, x, x^2, y, x^3, xy, x^4, x^2y, y^2$ in the 8-dimensional space $\mathcal{L}(4D)$ satisfy a linear dependence relation. Moreover, the coefficient of y^2 is non-zero. Therefore, $(C, [D])$ has equation

$$y^2 + (\alpha_0x^2 + \alpha_1x + \alpha_2)y = ax^4 + bx^3 + cx^2 + dx + e. \tag{2.3}$$

We will always assume that $\operatorname{char}(K) \neq 2$. Therefore, by completing the square it suffices to consider equations of the form

$$y^2 = ax^4 + bx^3 + cx^2 + dx + e. \tag{2.4}$$

Equation (2.4) is called a *genus one equation of degree* 2.

Two genus one equations of degree 2 with coefficients in A are A-*equivalent*, or $\mathcal{G}_2(A)$-equivalent, if they are related by the substitutions

$$x' = (m_{11}x + m_{21})/(m_{12}x + m_{22}),\ y' = \mu^{-1}y$$

where $\mu \in A^*$, $M = (m_{ij}) \in \mathrm{GL}_2(A)$. The group $\mathcal{G}_2(A)$ is the group of all such transformations $[\mu, M]$. We define $\det([\mu, M]) = \mu \det(M)$.

We associate the classical invariants I and J to equation (2.4), where

$$\begin{aligned} I &= 12ae - 3bd + c^2, \\ J &= 72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3. \end{aligned} \tag{2.5}$$

We set $c_4 = 2^4 I, c_6 = 2^5 J$, and $\Delta = (c_4^3 - c_6^2)/1728$.

Genus one equations of degree 3

If $\deg D = 3$, then we pick $x, y, z \in K(C)$ such that $\{x, y, z\}$ is a basis for $\mathcal{L}(D)$. We write a linear dependence relation between the 10 elements $x^3, y^3, z^3, x^2y, x^2z, y^2x, y^2z, z^2x, z^2y, xyz$ in the 9-dimensional space $\mathcal{L}(3D)$. Therefore, $(C, [D])$ has a homogeneous ternary cubic equation

$$ax^3 + by^3 + cz^3 + a_2x^2y + a_3x^2z + b_1y^2x + b_3y^2z + c_1z^2x + c_2z^2y + mxyz = 0. \tag{2.6}$$

Equation (2.6) is called *a genus one equation of degree* 3.

Two genus one equations of degree 3 with coefficients in A are A-*equivalent*, or $\mathcal{G}_3(A)$-equivalent, if they are related by multiplying by $\mu \in A^*$ and then substituting

$$x' = m_{11}x + m_{21}y + m_{31}z,\ y' = m_{12}x + m_{22}y + m_{32}z, z' = m_{13}x + m_{23}y + m_{33}z,$$

where $M = (m_{ij}) \in \mathrm{GL}_3(A)$. The group $\mathcal{G}_3(A)$ is the group of all such transformations $[\mu, M]$. We define $\det([\mu, M]) = \mu \det(M)$.

We define the *Hessian* of a genus one equation $\phi(x, y, z) = 0$ of degree 3 to be

$$H(\phi) = -1/2 \times \det \begin{pmatrix} \phi_{xx} & \phi_{xy} & \phi_{xz} \\ \phi_{yx} & \phi_{yy} & \phi_{yz} \\ \phi_{zx} & \phi_{zy} & \phi_{zz} \end{pmatrix}.$$

Then we have

$$H(\lambda\phi + \mu H(\phi)) = 3(c_4\lambda^2\mu + 2c_6\lambda\mu^2 + c_4^2\mu^3)\phi + (\lambda^3 - 3c_4\lambda\mu^2 - 2c_6\mu^3)H(\phi).$$

Moreover, we put $\Delta = (c_4^3 - c_6^2)/1728$, see [14].

Genus one equations of degree 4

If $\deg D = 4$, then we pick $x_1, x_2, x_3, x_4 \in K(C)$ such that $\{x_1, x_2, x_3, x_4\}$ is a basis for $\mathcal{L}(D)$. Now we consider the 10 elements $x_1^2, x_2^2, x_3^2, x_4^2, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4$ in the 8-dimensional space $\mathcal{L}(2D)$. Therefore, $(C, [D])$ has equations

$$F_1(x_1, x_2, x_3, x_4) = F_2(x_1, x_2, x_3, x_4) = 0, \quad \text{where } F_1, F_2 \text{ are quaternary quadratic forms.} \tag{2.7}$$

We will call the equations (2.7) a *genus one equation of degree* 4.

Two genus one equations of degree 4 with coefficients in A are *A-equivalent*, or $\mathcal{G}_4(A)$-equivalent, if they are related by

$$F_1' = m_{11}F_1 + m_{12}F_2, F_2' = m_{21}F_1 + m_{22}F_2, \; M = (m_{ij}) \in \mathrm{GL}_2(A),$$

and then substituting

$$x_j' = \sum_{i=1}^{4} n_{ij}x_i, \; N = (n_{ij}) \in \mathrm{GL}_4(A).$$

The group $\mathcal{G}_4(A)$ is the group of all such transformations $[M, N]$. We define $\det([M, N]) = \det(M)\det(N)$.

Let M_1 and M_2 be the 4×4 symmetric matrices of second partial derivatives of F_1 and F_2 respectively. We associate a genus one equation ϕ of degree 2 to the genus one equation $\{F_1 = F_2 = 0\}$, where $\phi : y^2 = F(x, z) := \det(M_1x + M_2z)$. Then we set $c_4 = I, c_6 = J/2$ where I, J are the invariants associated to ϕ, see (2.5). We put $\Delta = (c_4^3 - c_6^2)/1728$.

Definition 2.1.1. Let K_n be the polynomial ring in the coefficients of a genus one equation ϕ of degree $n = 1, 2, 3, 4$. A polynomial $G \in K_n$ is an *invariant of weight* k if $G \circ g = \det(g)^k G$ for all $g \in \mathcal{G}_n(\overline{K})$.

The following theorem indicates the properties of the invariants c_4, c_6, and Δ defined above.

Theorem 2.1.2. *Let ϕ be a genus one equation of degree $n = 1, 2, 3, 4$. Let c_4, c_6, and Δ be the associated invariants.*

(i) The polynomials $c_4, c_6, \Delta \in K_n$ are invariants of weight $4, 6$ and 12 respectively.

(ii) The equation ϕ defines a smooth curve C_ϕ of genus one if and only if $\Delta \neq 0$.

(iii) If $\operatorname{char}(K) \neq 2, 3$, *and* $\Delta \neq 0$, *then the Jacobian of* C_ϕ *has equation*

$$y^2 = x^3 - 27c_4x - 54c_6.$$

Proof: See [15]. □

Definition 2.1.3. Let R be a Dedekind ring with fraction field K. A genus one equation ϕ of degree n with discriminant $\Delta \neq 0$ is

(i) *integral* if the defining polynomials have coefficients in R.

If R is a discrete valuation ring with normalised valuation ν, then ϕ is

(ii) *minimal* if it is integral and $\nu(\Delta)$ is minimal among all the valuations of the discriminants of the integral genus one equations of degree n which are K-equivalent to ϕ.

2.2 Models of curves and contraction

In this section we recall the definition of a model of a curve, introduce some well-known models of smooth curves and record their basic properties. Then we define contraction morphisms and give some results on their existence and uniqueness. References for this are [5], [8] and [20].

2.2.1 Models of curves

Let R be a Dedekind domain with fraction field K. Put $S = \operatorname{Spec} R$.

We recall that an S-scheme X is *reduced at* $x \in X$ if the local ring $\mathcal{O}_{X,x}$ has no nilpotent elements. X is *reduced* if it is reduced at all its points. X is said to be *integral* if it is reduced and irreducible. X is *normal at* $x \in X$ if $\mathcal{O}_{X,x}$ is integrally closed in $\operatorname{Frac}(\mathcal{O}_{X,x})$. We say X is *normal* if it is irreducible and normal at all of its points. The scheme X is said to be regular at $x \in X$ if $\mathcal{O}_{X,x}$ is regular, i.e., $\dim \mathcal{O}_{X,x} = \dim_k \mathfrak{m}_x/\mathfrak{m}_x^2$, where $\mathfrak{m}_x$ is the maximal ideal corresponding to x. X is regular if it is regular at all of its points.

Definition 2.2.1. An S-*curve* is an integral, projective, flat, normal S-scheme $f : X \to S$ of dimension 2.

We define what an S-model for a smooth curve over K is.

Definition 2.2.2. Let C be a smooth projective curve over K. An *S-model for C* is a pair $(\mathcal{C}, i)$, where $\mathcal{C} \to S$ is an S-curve and $i : \mathcal{C}_K \cong C$ is an isomorphism. A *morphism* of S-models $(\mathcal{C}, i) \to (\mathcal{C}', i')$ is an S-morphism $\alpha : \mathcal{C} \to \mathcal{C}'$ such that $i' \circ \alpha_K = i$. An S-model $(\mathcal{C}, i)$ for C *dominates* another model $(\mathcal{C}', i')$ if there exists a morphism $\mathcal{C} \to \mathcal{C}'$ of S-models. We generally omit the explicit mention of i unless there is a danger of confusion.

Now we introduce two of the most interesting models of smooth curves.

Definition 2.2.3. Let C be a smooth projective curve over K. A *minimal proper regular model* for C is a regular S-model C^{min} for C such that any domination map $C^{min} \to \mathcal{C}$ to another regular S-model $\mathcal{C}$ for C is an isomorphism.

Theorem 2.2.4. *Let C be a smooth projective curve over K. If C has positive genus, then a minimal proper regular model C^{min} for C exists and is unique up to unique isomorphism. In particular, C^{min} is dominated by all regular S-models for C.*

Proof: See ([8], Theorem 3.9). □

Definition 2.2.5. Let $\mathcal{C}$ be an S-model for a smooth curve C over K. A proper morphism $f : \mathcal{C}' \to \mathcal{C}$ of S-models for C with $\mathcal{C}'$ regular is called a *desingularisation* of $\mathcal{C}$. We call a desingularisation morphism $\widetilde{\mathcal{C}} \to \mathcal{C}$ such that every other desingularisation morphism $\mathcal{C}' \to \mathcal{C}$ factors uniquely through $\mathcal{C}' \to \widetilde{\mathcal{C}} \to \mathcal{C}$ a *minimal desingularisation* of $\mathcal{C}$. Moreover, $\widetilde{\mathcal{C}}$ is an S-model for C. By definition, if a minimal desingularisation exists, then it is unique up to unique isomorphism.

Theorem 2.2.6. *Let $\mathcal{C}$ be an S-model for a smooth curve C over K. If C has positive genus, then a minimal desingularisation $\widetilde{\mathcal{C}} \to \mathcal{C}$ exists and is unique up to unique isomorphism.*

Proof: See ([20], Proposition 9.3.36 (b)). □

2.2.2 Contraction

Let K be a discrete valuation field with normalised valuation ν. We write $\mathcal{O}_K$ for its ring of integers. Fix a uniformiser $t \in K$ and write $k = \mathcal{O}_K/t\mathcal{O}_K$ for the residue field. Put $S = \operatorname{Spec} \mathcal{O}_K$. If X is an S-scheme, then we will denote its generic fiber by X_K and its special fiber by X_k.

Definition 2.2.7. Let $\mathcal{C}$ be an S-curve. Let $(\Gamma_i)_{i\in I}$ be the family of irreducible components of the special fiber $\mathcal{C}_k$. For a strict subset $J \subset I$, a *contraction* of the components Γ_j, $j \in J$, in $\mathcal{C}$ consists of an S-morphism $u : \mathcal{C} \to \mathcal{C}^J$ of S-schemes such that

(a) For each $j \in J$, the image $u(\Gamma_j)$ consists of a single point $x_j \in \mathcal{C}^J$, and

(b) u defines an isomorphism $\mathcal{C} - \bigcup_{j\in J} \Gamma_j \xrightarrow{\sim} \mathcal{C}^J - \bigcup_{j\in J} x_j$.

Theorem 2.2.8. *Assume that $\mathcal{O}_K$ is Henselian. Let $\mathcal{C}$ be an S-curve. Let $(\Gamma_i)_{i\in I}$ be the family of irreducible components of $\mathcal{C}_k$. For a strict subset $J \subset I$, the contraction $u : \mathcal{C} \to \mathcal{C}^J$ of the components Γ_j, $j \in J$, exists. Moreover, the morphism u is unique up to unique isomorphism.*

Proof: For the existence of $u : \mathcal{C} \to \mathcal{C}^J$, see ([20], Theorem 8.3.36) or ([5], §6.7, Proposition 4). For the uniqueness of $u : \mathcal{C} \to \mathcal{C}^J$, see ([20], Proposition 8.3.28). □

Let X be a scheme over S. We recall that a *Cartier divisor* D is a system $\{(U_i, f_i)_i\}$, where the U_i are covering open subsets of X, f_i is the quotient of two regular elements of $\mathcal{O}_X(U_i)$, and $f_i|_{U_i\cap U_j} \in f_j|_{U_i\cap U_j}\mathcal{O}_X(U_i \cap U_j)^*$ for every i, j. Two systems $\{(U_i, f_i)_i\}$ and $\{(V_j, g_j)_j\}$ represent the same Cartier divisor if on $U_i \cap V_j$, f_i and g_j differ by a multiplicative factor in $\mathcal{O}_X(U_i \cap V_j)^*$.

To a Cartier divisor D we associate an invertible sheaf $\mathcal{O}_X(D)$ defined by $\mathcal{O}_X(D)|_{U_i} = f_i^{-1}\mathcal{O}_X|_{U_i}$. We define the *support of* D to be the set of points $x \in X$ such that $\mathcal{O}_X(D)_x \neq \mathcal{O}_{X,x}$, we denote it by $\operatorname{Supp} D$. The set $\operatorname{Supp} D$ is a closed subset of X.

The Cartier divisor D is *effective* if it can be represented by $\{(U_i, f_i)_i\}$ with $f_i \in \mathcal{O}_X(U_i)$. It is *principal* if it can be represented by a system $\{(X, f)\}$. An *effective relative Cartier divisor* on X is an effective Cartier divisor on X which is flat over S when considered as a closed subscheme of X. Linear equivalence is defined in the obvious way. The group of isomorphism classes of Cartier divisors modulo linear equivalence is denoted by $\operatorname{CaCl}(X)$.

A *prime divisor* on X is a closed integral subscheme of codimension one. A *Weil divisor* is an element of the free abelian group generated by the prime divisors, i.e., we write a Weil divisor D as $\sum n_i Y_i$, where the Y_i are prime divisors, the n_i are integers, and only finitely many n_i are different from zero. If $n_i \geq 0$ for every i, then D is *effective.* A Weil divisor is said to be *principal* if it can be written as $\sum \nu_Y(f).Y$, where $f \in K(X)^*$, and the sum is over all prime divisors of X and hence is finite. A Weil divisor D is *locally principal* if X can be covered by open sets U such that $D|_U$ is principal for each U. We define the linear equivalence as usual, and denote the group of isomorphism classes of Weil divisors modulo linear equivalence by $\operatorname{Cl}(X)$.

Remark 2.2.9. If $\mathcal{C}$ is an S-curve, then $\mathrm{CaCl}(\mathcal{C})$ is isomorphic to the group $\mathrm{Pic}(\mathcal{C})$ of isomorphism classes of invertible sheaves on $\mathcal{C}$, see ([20], Corollary 7.1.19). Moreover, the group of Cartier divisors on $\mathcal{C}$ is isomorphic to the group of locally principal Weil divisors on $\mathcal{C}$, see ([16], Chapter II, Proposition 6.11 and Remark 6.11.2).

If $\mathcal{C}$ is regular, then the group of Cartier divisors on $\mathcal{C}$ is isomorphic to the group of Weil divisors on $\mathcal{C}$, and $\mathrm{CaCl}(\mathcal{C})$ is isomorphic to $\mathrm{Cl}(\mathcal{C})$, see ([20], Proposition 7.2.16).

Proposition 2.2.10. *Let $\mathcal{C}$ be an S-curve. Let $\mathcal{L}$ be an invertible sheaf on $\mathcal{C}$ generated by global sections $s_0, \ldots, s_n$. Let us consider the morphism $f : \mathcal{C} \to \mathbb{P}^n_S$ associated to these sections. Let Γ be an irreducible component of $\mathcal{C}_k$. Then $f(\Gamma)$ is reduced to a point if and only if $\mathcal{L}|_\Gamma \simeq \mathcal{O}_\Gamma$.*

Proof: See ([20], Lemma 8.3.29). □

The following theorem describes the contraction morphism explicitly. In fact, we use it repeatedly in this thesis.

Theorem 2.2.11. *Let $\mathcal{C}$ be an S-curve. Let $(\Gamma_i)_{i\in I}$ be the family of irreducible components of $\mathcal{C}_k$. Let D be a non-trivial effective relative Cartier divisor on $\mathcal{C}$. Let J be the set of all indices $j \in I$ such that $\mathrm{Supp}(D) \cap \Gamma_j = \emptyset$. Then the canonical morphism*

$$u : \mathcal{C} \to \mathcal{C}^J := \mathrm{Proj}(\bigoplus_{m=0}^{\infty} H^0(\mathcal{C}, \mathcal{O}_\mathcal{C}(mD)))$$

is a contraction of the components $\Gamma_j, j \in J$, and $\mathcal{C}^J$ is an S-curve.

Proof: Theorem 1 of ([5], §6.7) proves that the morphism u is a contraction of the components $\Gamma_j, j \in J$, and that $\mathcal{C}^J$ is projective and normal. The proof that $\mathcal{C}^J$ is integral is similar to the proof that $\mathcal{C}^J$ is normal with replacing the integral closeness property with being an integral domain, see the proof of Lemma 2 of ([5], §6.7) and ([20], Proposition 2.4.17). The flatness is a direct consequence of the integrality of $\mathcal{C}^J$ and that $J \neq I$, see ([20], Corollary 4.3.10). □

Definition 2.2.12. Let $\mathcal{C} \to S$ be a regular S-curve. Let Γ be an irreducible component of $\mathcal{C}_k$. Γ is called an *exceptional divisor* (or *(-1)-curve*) if there exist a regular S-curve $\mathcal{C}^\Gamma \to S$ and a morphism $u : \mathcal{C} \to \mathcal{C}^\Gamma$ of S-schemes such that $u(\Gamma)$ is reduced to a point, and that $u : \mathcal{C} - \Gamma \xrightarrow{\sim} \mathcal{C}^\Gamma - u(\Gamma)$ is an isomorphism, i.e., Γ can be contracted to a regular point.

Example 2.2.13. Let C be a smooth curve defined over K. Assume that C has positive genus. Let C^{min} be the minimal proper regular model for C. Let $\mathcal{C}$ be an S-model for C with minimal desingularisation $\widetilde{\mathcal{C}} \to \mathcal{C}$.

Theorem 2.2.4 implies that there exists a unique morphism $\widetilde{\mathcal{C}} \to C^{min}$ as S-models for C. Indeed, this morphism is the contraction morphism of the exceptional divisors in $\widetilde{\mathcal{C}}$, see ([20], §10.1).

2.3 Canonical sheaves

In this section we define what a canonical sheaf is, and review some of its properties. For a reference see ([20], Chapter 6).

Let $f : X \to Y$ be a morphism of schemes. Let $\Delta : X \to X \times_Y X$ be the diagonal morphism. The morphism Δ gives an isomorphism of X onto its image $\Delta(X)$. Moreover, $\Delta(X)$ is a closed subscheme of an open subset U of $X \times_Y X$.

Definition 2.3.1. Let $\mathcal{I}$ be the sheaf of ideals of $\Delta(X)$ in U. We define the *sheaf of relative differentials of degree 1 of* X *over* Y to be $\Omega^1_{X/Y} := \Delta^*(\mathcal{I}/\mathcal{I}^2)$ on X. For any $r \geq 1$, we call the quasi-coherent sheaf $\Omega^r_{X/Y} := \wedge^r \Omega^1_{X/Y}$ the *sheaf of differentials of order* r.

Recall that an *immersion* of schemes is a morphism which is an open immersion followed by a closed immersion.

Definition 2.3.2. Let $f : X \to Y$ be a morphism of schemes. Assume that there exists an open subscheme V of Y such that f factors through a closed immersion $i : X \to V$. Let $\mathcal{J}$ be the sheaf of ideals defining $i(X)$. The sheaf $i^*(\mathcal{J}/\mathcal{J}^2)$ on X is called the *conormal sheaf of* X *in* Y, and we denote it by $\mathcal{C}_{X/Y}$. This sheaf does not depend on the choice of V.

Definition 2.3.3. Let $\mathcal{F}$ be a quasi-coherent sheaf on a scheme X. Assume moreover that $\mathcal{F}$ is of constant rank r_i on each connected component X_i of X. We define the invertible sheaf $\det \mathcal{F}$ by setting $(\det \mathcal{F})|_{X_i} = \wedge^{r_i}(\mathcal{F}|_{X_i})$.

Example 2.3.4. Let $X = \operatorname{Spec} A[T_1, \dots, T_n]$, where A is a Noetherian ring. Then $\Omega^1_{X/\operatorname{Spec} A}$ is locally free on X, and $\det \Omega^1_{X/\operatorname{Spec} A} = \Omega^n_{X/\operatorname{Spec} A}$ is free over $\mathcal{O}_X$, generated by $dT_1 \wedge \ldots \wedge dT_n$.

Definition 2.3.5. Let Y be a locally Noetherian scheme, and let $f : X \to Y$ be a quasi-projective local complete intersection. Let $i : X \to Z$ be an immersion into a scheme Z that is smooth over Y. We define the *canonical sheaf* of $X \to Y$ to be the invertible sheaf

$$\omega_{X/Y} := \det(\mathcal{C}_{X/Y})^{\vee} \otimes_{\mathcal{O}_X} i^*(\det \Omega^1_{Z/Y}).$$

This sheaf is independent of the choice of the decomposition $X \to Z \to Y$, up to isomorphism.

Let $f : X \to Y$ be a smooth morphism of relative dimension d, i.e., for $x \in X, \dim_x X_{f(x)} = d$. It is known that $\omega_{X/Y} = \wedge^d \Omega^1_{X/Y}$.

The reason we are interested in canonical sheaves and not in sheaves of differentials is that we are dealing with non-smooth schemes most of the time.

If A is a ring and $\{a_1, \ldots, a_n\}$ is a sequence of elements of A. We say that it is a *regular sequence* if a_1 is not a zero divisor and for any $i \geq 2,\ a_i$ is not a zero divisor in $A/(a_1, \ldots, a_{i-1})$. Now we state a lemma which enables us to compute the canonical sheaves of S-curves.

Lemma 2.3.6. *Let $Y = \operatorname{Spec} A$ be a Noetherian integral scheme, and let X be an integral closed subscheme of $Z = \operatorname{Spec} A[T_1, \ldots, T_n]$ defined by an ideal generated by a regular sequence $F_1, \ldots, F_r$ with $r \leq n$. Let us suppose that*

$$\Delta := \det(\frac{\partial F_i}{\partial T_j})_{1 \leq i,j \leq r}$$

is non-zero in $K(X)$. Let ξ be the generic point of X.

(i) Let t_i be the image of T_i in $\mathcal{O}_X(X)$. Then

$$\omega_{X/Y,\xi} = (dt_{r+1} \wedge \ldots \wedge dt_n)\mathcal{O}_{X,\xi}.$$

(ii) As a subsheaf of $\omega_{X/Y,\xi}$, we have

$$\omega_{X/Y} = \Delta^{-1}.(dt_{r+1} \wedge \ldots \wedge dt_n)\mathcal{O}_X.$$

Proof: See ([20], Corollary 6.4.14). □

Chapter 3

Degree-n-models

In this chapter we define what we mean by a degree-n-model for a smooth genus one curve C over a discrete valuation field K. Then we prove that if such a model is minimal, then it is an S-model for C, see Definition 2.2.2. We conclude by describing the singular loci of these models.

3.1 Definitions

Let R be a Dedekind domain with fraction field K. Put $S = \operatorname{Spec} R$.

The S-scheme defined by an integral genus one equation ϕ of degree 1 is simply the S-scheme $\mathcal{C} \subset \mathbb{P}^2_S$ defined as follows

$$\operatorname{Proj} R[x, y, z]/(\phi : y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3)),\ a_i \in R.$$

Definition 3.1.1. Let ϕ be a genus one equation of degree 1. Let C be the elliptic curve over K defined by ϕ. A *degree-*1*-model* for C is a pair $(\mathcal{C}, \alpha)$ where $\mathcal{C} \subset \mathbb{P}^2_S$ is an S-scheme defined by an integral genus one equation of degree 1, and $\alpha : \mathcal{C}_K \cong C$ is an isomorphism defined by a K-equivalence of genus one equations of degree 1, i.e., α is defined by an element of $\mathcal{G}_1(K)$, see §2.1 for the definition of $\mathcal{G}_n(K)$.

An isomorphism $\beta : (\mathcal{C}_1, \alpha_1) \cong (\mathcal{C}_2, \alpha_2)$ of degree-1-models is an isomorphism $\beta : \mathcal{C}_1 \cong \mathcal{C}_2$ of S-schemes defined by an R-equivalence of genus one equations of degree 1, i.e., β is defined by an element of $\mathcal{G}_1(R)$, with $\beta_K = \alpha_2^{-1}\alpha_1$, see §2.1.

Note that our definition of a degree-1-model for an elliptic curve C is the definition of a Weierstrass model for C as given in ([20], §9.4.4).

The S-scheme $\mathcal{C}$ defined by an integral genus one equation $\phi : y^2 = F(x, z)$ of degree 2 is the scheme obtained by glueing $\{y^2 = F(x, 1)\} \subset \mathbb{A}^2_S$ and $\{v^2 = F(1, u)\} \subset \mathbb{A}^2_S$ via

$x = 1/u$ and $y = x^2v$. It comes with a natural morphism $\mathcal{C} \to \mathbb{P}^1_S$ given on these affine pieces by $(x, y) \mapsto (x : 1)$ and $(u, v) \mapsto (1 : u)$.

The S-scheme defined by an integral genus one equation ϕ of degree $n = 3, 4$, is simply the subscheme $\mathcal{C} \subset \mathbb{P}^{n-1}_S$ defined by ϕ.

Definition 3.1.2. (i) Let ϕ be a genus one equation of degree $n \in \{2, 3, 4\}$. Let $C \to \mathbb{P}^{n-1}_K$ be the genus one curve defined by ϕ, where this morphism is a double cover when $n = 2$, and it is an embedding when $n \geq 3$.

A *degree-n-model* for C is a pair $(\mathcal{C}, \alpha)$ where $\mathcal{C} \to \mathbb{P}^{n-1}_S$ is an S-scheme defined by an integral genus one equation of degree n, and $\alpha : \mathcal{C}_K \cong C$ is an isomorphism defined by a K-equivalence of genus one equations of degree n, i.e., α is defined by an element of $\mathcal{G}_n(K)$.

(ii) An *isomorphism* of degree-n-models $(\mathcal{C}_1, \alpha_1) \cong (\mathcal{C}_2, \alpha_2)$ is an isomorphism $\beta : \mathcal{C}_1 \cong \mathcal{C}_2$ of S-schemes defined by an R-equivalence of genus one equations of degree n, i.e., β is defined by an element of $\mathcal{G}_n(R)$, with $\beta_K = \alpha_2^{-1}\alpha_1$.

If there is no confusion, then we will omit mentioning the isomorphism α in the degree-n-model $(\mathcal{C}, \alpha)$ and write $\mathcal{C}$ instead.

Definition 3.1.3. Let R be a discrete valuation ring. A degree-n-model $(\mathcal{C}, \alpha)$ for a smooth genus one curve over K is said to be *minimal* if the defining genus one equation of degree n of $\mathcal{C}$ is minimal, see Definition 2.1.3.

3.2 Normality

We will fix the following notations for the rest of this section unless otherwise stated. K is a Henselian discrete valuation field with normalised valuation ν. We write $\mathcal{O}_K$ for its ring of integers. Fix a uniformiser $t \in K$ and write $k = \mathcal{O}_K/t\mathcal{O}_K$ for the residue field. We will assume moreover that k is algebraically closed and that $\mathrm{char}(k) \neq 2$. Set $S = \mathrm{Spec}\, \mathcal{O}_K$

In this section we find necessary and sufficient conditions for a degree-n-model for a smooth genus one curve C to be normal, and hence to be an S-model for C.

If $f(x_1, \ldots, x_n) = \sum_{i=1}^{m} a_i x_1^{l_{1i}} \ldots x_n^{l_{ni}} \in \mathcal{O}_K[x_1, \ldots, x_n]$, then $\tilde{f}(x_1, \ldots, x_n)$ will denote its image in $k[x_1, \ldots, x_n]$. Moreover, $\nu(f) = \min\{\nu(a_i) : 1 \leq i \leq m\}$.

A Noetherian S-scheme X is said to be *Cohen-Macaulay* if $\mathcal{O}_{X,x}$ is a Cohen-Macaulay ring for every $x \in X$.

Let $(A, \mathfrak{m})$ be a regular Noetherian local ring of dimension d. Any system of generators of $\mathfrak{m}$ with d elements is called a *coordinate system* for A.

Lemma 3.2.1. *Let $(A, \mathfrak{m})$ be a regular Noetherian local ring.*

(i) Suppose that $f \in \mathfrak{m}\backslash\{0\}$. Then A/fA is regular if and only if $f \notin \mathfrak{m}^2$.

(ii) Suppose that I is a proper ideal of A. Then A/I is regular if and only if I is generated by r elements of a coordinate system for A, with $r = \dim A - \dim A/I$. In other words, if and only if I is generated by r elements of $\mathfrak{m}$ which are linearly independent $\bmod \mathfrak{m}^2$.

Proof: See ([20], Corollary 4.2.12 and Corollary 4.2.15). □

We state the following lemma which we use throughout this section.

Lemma 3.2.2. *Let $\mathcal{C} \to S$ be a local complete intersection. Assume that $\mathcal{C}_K$ is normal. Then the following statements are true.*

(i) $\mathcal{C}$ is normal if and only if $\mathcal{C}$ is regular at the generic points of $\mathcal{C}_k$.

(ii) If $\mathcal{C}_k$ is reduced, then $\mathcal{C}$ is normal.

Proof: (i) Since $\mathcal{C}$ is a local complete intersection, it follows that it is a Cohen-Macaulay scheme, see ([20], Corollary 8.2.18). Therefore, as a consequence of Serre's criterion for normality, it follows that $\mathcal{C}$ is normal if and only if it is normal at its points of codimension 1, i.e., either closed points of the generic fiber, or the generic points of the special fiber, see for example ([20], Corollary 8.2.24). Since $\mathcal{C}_K$ is normal, we have that $\mathcal{C}$ is normal if and only if $\mathcal{C}$ is normal at the generic points of its special fiber and that is equivalent to regularity at these generic points.

(ii) See ([20], Lemma 4.1.18). □

It is known that if C is a curve over K, then the normality of C coincides with the regularity.

We need to define the concept of multiplicity of an irreducible component. Let X be a locally Noetherian scheme over k. Let Γ be an irreducible component of X with generic point ξ. Let $\mathfrak{m}_\xi$ be the maximal ideal corresponding to ξ. Then the *multiplicity* of Γ in X is the dimension d of $\mathcal{O}_{X,\xi}/\mathfrak{m}_\xi$ as a k-vector space. Moreover, $d = 1$ if and only if $\mathcal{O}_{X,\xi}$ is reduced (or, equivalently, if X is reduced on a non-empty open subset containing ξ), see ([20], Definition 7.5.6).

If $\mathcal{C}$ is an S-curve, then there is a normalised valuation ν_Γ of $K(\mathcal{C})$ corresponding to each irreducible component Γ of $\mathcal{C}_k$. The multiplicity of Γ in $\mathcal{C}_k$ is equal to $\nu_\Gamma(t)$, see ([20], Exercise 8.3.3 (a)).

Let C be a genus one curve defined by a genus one equation ϕ of degree $n = 1, 2$, and let $\mathcal{C}$ be the degree-n-model for C defined by ϕ.

If $n = 1$, then $\mathcal{C}_k$ is one of the following

(1) smooth cubic (2) nodal cubic (3) cuspidal cubic.

If $n = 2$, i.e., $\phi : y^2 = f(x)$, then we can classify $\mathcal{C}_k$ according to the repeated roots of $f(x)$. Therefore, $\mathcal{C}_k$ is one of the following

(1) smooth quartic (2) nodal quartic (3) cuspidal quartic

(4) two intersecting lines (5) two tangent conics (6) double line.

The forms (1), (2), (3), (4), (5) and (6) above correspond to $f(x)$ having no repeated roots, one and only one double root, a cubic root, two double roots, a root of order 4, and $f(x) = 0 \bmod t$ respectively.

Now we state the conditions for $\mathcal{C}$ to be normal in the following two propositions.

Proposition 3.2.3. *Let C be a smooth genus one curve over K defined by an integral genus one equation ϕ of degree* 1. *Let $\mathcal{C}$ be the degree-*1*-model for C given by ϕ. Then the model $\mathcal{C}$ is normal.*

PROOF: Since $\mathcal{C}_k$ consists of one irreducible component of multiplicity-1, in particular $\mathcal{C}_k$ is reduced, and C is smooth, it follows that $\mathcal{C}$ is normal, see Lemma 3.2.2 (*ii*). □

The following normality condition, when $n = 2$, can be found in ([18], Lemme 5).

Proposition 3.2.4. *Let C be a smooth genus one curve over K defined by an integral genus one equation $\phi : y^2 = f(x)$ of degree* 2. *Let $\mathcal{C}$ be the degree-*2*-model for $C \to \mathbb{P}^1_K$ given by ϕ. The model $\mathcal{C}$ is normal if and only if $\nu(f) \leq 1$.*

PROOF:

(i) If $t \nmid f(x)$, then the defining equation $y^2 - \tilde{f}(x) = 0$ of $\mathcal{C}_k$ has no square factor, and so $\mathcal{C}_k$ is reduced, see ([20], Exercise 2.4.1). Since C is smooth, and hence it is normal, and $\mathcal{C}_k$ is reduced, it follows that $\mathcal{C}$ is normal, see Lemma 3.2.2 (*ii*).

(ii) If $t \mid f(x)$, then the maximal ideal corresponding to the generic point ξ of $\mathcal{C}_k$ is $\mathfrak{m}_\xi = \langle t, y \rangle$. Lemma 3.2.2 (*i*) implies that $\mathcal{C}$ is normal if and only if $\mathcal{C}_k$ is regular at ξ, and Lemma 3.2.1 (*i*) shows that the latter statement is equivalent to $y^2 - f(x) \notin \mathfrak{m}_\xi^2$. Since $y^2 \in \mathfrak{m}_\xi^2$ and $t \mid f(x)$, whence $\mathcal{C}$ is normal if and only if $t \mid\mid f(x)$, i.e., $\nu(f) = 1$.

□

When C is a genus one curve defined by a genus one equation ϕ of degree $n = 3, 4$, and $\mathcal{C}$ is the degree-n-model for $C \to \mathbb{P}^{n-1}_K$ defined by ϕ, the combinatorial possibilities for the special fiber $\mathcal{C}_k$ increase.

We start with $\phi : F(x, y, z) = 0$ of degree 3, then the special fiber $\mathcal{C}_k$ is one of the following, see ([25], p. 266).

(1) smooth cubic
(2) nodal cubic
(3) cuspidal cubic
(4) conic + line
(5) conic + tangent
(6) line + double line
(7) three lines
(8) three concurrent lines
(9) triple line.

When $\phi : F(x_1, x_2, x_3, x_4) = G(x_1, x_2, x_3, x_4) = 0$ is of degree 4, we will assume that $\mathcal{C}_k$ is a curve, hence $\tilde{F}$ and $\tilde{G}$ are coprime. The special fiber $\mathcal{C}_k$ is in one of the forms given below, see [12] or ([7], p. 46).

(1) smooth quartic
(2) nodal quartic
(3) cuspidal quartic
(4) two secant conics
(5) two tangent conics
(6) four lines (skew quadrilateral)
(7) four concurrent lines
(8) cubic + secant line
(9) cubic + tangent line
(10) conic + two lines not crossing on it
(11) conic + two lines crossing on it
(12) conic + double line
(13) double conic
(14) double line + two lines
(15) triple line + line
(16) two double lines
(17) quadruple line.

Remark 3.2.5. Let $\mathcal{C}$ be a degree-4-model for a smooth genus one curve. We will need explicit defining equations for $\mathcal{C}_k$ when $\mathcal{C}_k$ contains a component of multiplicity greater than one. These equations can be obtained after applying transformations in $\mathcal{G}_4(k)$. For the whole list of defining equations for the special fiber $\mathcal{C}_k$, see [12] or ([7], p. 46).

$\mathcal{C}_k$	Defining equations
conic + double line	$x_1x_3 = x_1x_4 + x_2^2 = 0$
double conic	$x_1^2 = x_2^2 + x_3^2 + x_4^2 = 0$ which is k-equivalent to $x_1^2 = x_2^2 + x_3x_4 = 0$
double line + two lines	$x_1^2 + x_2^2 = x_1x_3 + \mu x_2x_4 = 0,\ \mu \in k$
triple line + line	$x_1x_2 = x_1^2 + x_2x_4 = 0$
two double lines	$x_1^2 = x_2x_4 + \mu x_1x_3 = 0,\ \mu \in k$
quadruple line	$x_1^2 = x_2^2 + \mu x_1x_3 = 0,\ \mu \in k$

Consider a genus one equation ϕ of degree 3 given by

$$\phi : by^3 + f_1(x,z)y^2 + f_2(x,z)y + f_3(x,z) = 0, \tag{3.1}$$

where $f_1(x,z) = b_1x + b_3z, f_2(x,z) = a_2x^2 + mxz + c_2z^2, f_3(x,z) = ax^3 + a_3x^2z + c_1z^2x + cz^3$.

Let $\mathcal{C}$ be the degree-3-model defined by ϕ. Assume that its special fiber $\mathcal{C}_k$ contains an irreducible component of multiplicity-m, $m \geq 2$. Using a matrix in $\mathrm{GL}_3(\mathcal{O}_K)$ we can assume that the defining equation of this multiplicity-m component is $y = 0$. This means that $\min\{\nu(f_2), \nu(f_3)\} \geq 1, \nu(f_1) = 0$ when $m = 2$, and $\min\{\nu(f_1), \nu(f_2), \nu(f_3)\} \geq 1, \nu(b) = 0$ when $m = 3$.

Proposition 3.2.6. *Let C be the smooth genus one curve over K defined by the integral equation $\phi : F(x,y,z) = 0$ given in (3.1). Let $\mathcal{C}$ be the degree-3-model for $C \to \mathbb{P}^2_K$ given by the same equation.*

(i) If $\mathcal{C}_k$ contains only multiplicity-1 components, then $\mathcal{C}$ is normal.

(ii) If $\mathcal{C}_k$ contains a multiplicity-m component, $m \geq 2$, whose defining equation is $y = 0$, then $\mathcal{C}$ is normal if and only if $\nu(f_3) = 1$.

PROOF: *(i)* Since C is normal and $\mathcal{C}_k$ is reduced, then $\mathcal{C}$ is normal, see Lemma 3.2.2 *(ii)*.

(ii) Assume that $\mathcal{C}_k$ contains an irreducible component $\Gamma : \{y = 0\}$ of multiplicity $m = 2$. Using a matrix in $\mathrm{GL}_3(\mathcal{O}_K)$ we can assume that $\mathcal{C}_k$ is defined by $y^2x = 0$. The maximal ideal corresponding to the generic point ξ of Γ is $\mathfrak{m}_\xi = \langle t, y\rangle$, and the maximal ideal corresponding to the generic point ξ' of $\{x = 0\}$ is $\mathfrak{m}_{\xi'} = \langle t, x\rangle$. Lemma 3.2.1 and Lemma 3.2.2 imply that $\mathcal{C}$ is normal if and only if $F(x,y,z) \notin \mathfrak{m}_\xi^2$ and $F(x,y,z) \notin \mathfrak{m}_{\xi'}^2$. Since $\nu(f_2) \geq 1$, we have $y^3, y^2, f_2(x,z)y \in \mathfrak{m}_\xi^2$. Therefore, $F(x,y,z) \notin \mathfrak{m}_\xi^2$ if and only if $t \mid\mid f_3(x,z)$, i.e., $\nu(f_3) = 1$. Moreover, it is always true that $F(x,y,z) \notin \mathfrak{m}_{\xi'}^2$ because $\nu(by^3 + b_3y^2z + c_2yz^2 + cz^3) = 0$. Hence $\mathcal{C}$ is normal if and only if $\nu(f_3) = 1$.

Assume that $\mathcal{C}_k$ consists of a multiplicity-3 irreducible component $\Gamma : \{y = 0\}$. The maximal ideal corresponding to the generic point ξ of $\mathcal{C}_k$ is $\mathfrak{m}_\xi = \langle t, y\rangle$. Since $\nu(f_2) \geq 1$, it follows that $\mathcal{C}$ is normal if and only if $\nu(f_3) = 1$. □

Now we study the normality of degree-4-models for smooth genus one curves. Consider a genus one equation ϕ of degree 4 given by $F(x_1, x_2, x_3, x_4) = G(x_1, x_2, x_3, x_4) = 0$, where F and G are given by the following two integral equations respectively

$$\begin{aligned} &a_1x_1^2 + a_2x_1x_2 + a_3x_1x_3 + a_4x_1x_4 + a_5x_2^2 + a_6x_2x_3 + a_7x_2x_4 + a_8x_3^2 + a_9x_3x_4 + a_{10}x_4^2, \\ &b_1x_1^2 + b_2x_1x_2 + b_3x_1x_3 + b_4x_1x_4 + b_5x_2^2 + b_6x_2x_3 + b_7x_2x_4 + b_8x_3^2 + b_9x_3x_4 + b_{10}x_4^2, \end{aligned} \tag{3.2}$$

where $\tilde{F}, \tilde{G}$ are coprime, and do not define coplanar lines.

Proposition 3.2.7. *Let C be the smooth genus one curve over K defined by the integral equation ϕ given in (3.2). Let $\mathcal{C}$ be the degree-4-model for $C \to \mathbb{P}^3_K$ given by the same equation.*

(i) If $\mathcal{C}_k$ contains a multiplicity-1 component Γ, then $\mathcal{C}$ is normal at Γ.

(ii) If $\mathcal{C}_k$ is a conic and a double line with $\tilde{F} = x_1x_3$ and $\tilde{G} = x_1x_4 + x_2^2$, then $\mathcal{C}$ is normal if and only if

$$\nu(x_4F(0,0,x_3,x_4) - x_3G(0,0,x_3,x_4)) = 1.$$

(iii) Assume that $\mathcal{C}_k$ is a double conic with $\tilde{F} = x_1^2$ and $\tilde{G} = x_2^2 + x_3x_4$. Then $\mathcal{C}$ is normal unless $F(0,x_2,x_3,x_4) \equiv \mu(x_2^2 + x_3x_4) \mod t^2$, for some $\mu \in \mathcal{O}_K$.

(iv) Assume that $\mathcal{C}_k$ contains a line $\Gamma : \{x_1 = x_2 = 0\}$ of multiplicity-m, $m \geq 2$, with $\tilde{F} = q(x_1, x_2)$ and $\tilde{G} = x_1x_3 + \mu x_2x_4 + q'(x_1, x_2)$, $\mu \in k$. If $\nu(F(0,0,x_3,x_4)) = 1$, then $\mathcal{C}$ is normal at Γ.

Proof: (i) If $\mathcal{C}_k$ contains a multiplicity-1 component Γ, then $\mathcal{C}_k$ is reduced at the generic point ξ of Γ, but C is normal, hence $\mathcal{C}$ is normal at ξ, see ([20], Lemma 4.1.18).

Now we use Lemma 3.2.1 (ii) and Lemma 3.2.2 (i) to study the normality of $\mathcal{C}$ at components of multiplicity greater than 1. The model $\mathcal{C}$ is normal if and only if $F, G \notin \mathfrak{m}_\xi^2$, and F, G are linearly independent mod $\mathfrak{m}_\xi^2$, for every generic point ξ of $\mathcal{C}_k$. Note that the linear independence condition for $F, G \mod \mathfrak{m}_\xi^2$, $\xi \in \mathcal{C}$, is: for $\lambda_1, \lambda_2 \in \mathcal{O}_K[x_1, \ldots, x_4]_\xi$, if $\lambda_1F + \lambda_2G \in \mathfrak{m}_\xi^2$, then $\lambda_1, \lambda_2 \in \mathfrak{m}_\xi$.

(ii) Let ξ be the generic point of the double line $\{x_1 = x_2 = 0\}$ in $\mathcal{C}_k$, then $\mathfrak{m}_\xi = \langle x_1, x_2, t\rangle$. It is clear that $F, G \notin \mathfrak{m}_\xi^2$. Now we consider the linear independence of F and G. If $\lambda_1F + \lambda_2G \in \mathfrak{m}_\xi^2$, then the fact that x_1 and t are linearly independent mod $\mathfrak{m}_\xi^2$ implies that $\lambda_1x_3 + \lambda_2x_4 \in \mathfrak{m}_\xi$, i.e., $\lambda_1 \equiv \mu x_4 \mod \mathfrak{m}_\xi$ and $\lambda_2 \equiv -\mu x_3 \mod \mathfrak{m}_\xi$ for some $\mu \in \mathcal{O}_K$. Therefore, $\mathcal{C}$ is normal if and only if $\nu(f) = 1$, where

$$f = x_4(a_8x_3^2 + a_9x_3x_4 + a_{10}x_4^2) - x_3(b_8x_3^2 + b_9x_3x_4 + b_{10}x_4^2).$$

(iii) Let $\mathfrak{m}_\xi = \langle x_1, x_2^2 + x_3x_4, t\rangle$ be the maximal ideal corresponding to the generic point ξ of the conic. We have $G \notin \mathfrak{m}_\xi^2$. If $a_5x_2^2 + a_9x_3x_4 = tu(x_2^2 + x_3x_4), u \in \mathcal{O}_K$, then $F \notin \mathfrak{m}_\xi^2$ if and only if $\nu(a_6x_2x_3 + a_7x_2x_4 + a_8x_3^2 + a_{10}x_4^2) = 1$, otherwise $F \notin \mathfrak{m}_\xi^2$ if and only if $\nu(a_5x_2^2 + a_6x_2x_3 + a_7x_2x_4 + a_8x_3^2 + a_9x_3x_4 + a_{10}x_4^2) = 1$.

To investigate the linear independence of F and G, we note that if $\lambda_1F + \lambda_2G \in \mathfrak{m}_\xi^2$, then $\lambda_2 \in \mathfrak{m}_\xi$. The reason is t and $x_2^2 + x_3x_4$ are linearly independent mod $\mathfrak{m}_\xi^2$. Therefore, the condition we obtained from $F \notin \mathfrak{m}_\xi^2$ implies that $\lambda_1 \in \mathfrak{m}_\xi$, and hence we get linear independence.

(iv) Assume that ξ is the generic point of $\Gamma : \{x_1 = x_2 = 0\}$. The ideal $\mathfrak{m}_\xi$ is given by $\langle x_1, x_2, t\rangle$. Since $\tilde{F} = q(x_1, x_2)$, and $\nu(a_8x_3^2 + a_9x_3x_4 + a_{10}x_4^2) = 1$, we have $F \notin \mathfrak{m}_\xi^2$. Since $\tilde{G} = x_1x_3 + \mu x_2x_4 + q'(x_1, x_2)$, where $\mu \in k$, we have $G \notin \mathfrak{m}_\xi^2$ because $x_1x_3 \notin \mathfrak{m}_\xi^2$. Therefore, we need to check the linear independence only. Let $\lambda_1, \lambda_2 \in \mathcal{O}_K[x_1, \dots, x_4]_\xi$ be such that $\lambda_1F + \lambda_2G \in \mathfrak{m}_\xi^2$. Since x_1, x_2 and t are linearly independent mod $\mathfrak{m}_\xi^2$, it follows that $\lambda_2 \in \mathfrak{m}_\xi$. Moreover, as $\nu(a_8x_3^2 + a_9x_3x_4 + a_{10}x_4^2) = 1$, we get $\lambda_1 \in \mathfrak{m}_\xi$, hence F and G are linearly independent mod $\mathfrak{m}_\xi^2$. □

The proof of the following lemma can be found in §2.5.1 of [30].

Lemma 3.2.8. *Let C be the smooth genus one curve over K defined by the integral equation ϕ given in (3.2). Let $\mathcal{C}$ be the degree-4-model for $C \to \mathbb{P}^3_K$ given by the same equation.*

(i) Assume that $\tilde{F}$ and $\tilde{G}$ have a common factor. Then ϕ is not minimal.

(ii) Assume that $\mathcal{C}_k$ is a quadruple line with $\tilde{F} = x_1^2$ and $\tilde{G} = x_2^2$. Then either ϕ is not minimal, or $C(K) = \emptyset$.

Proof: (i) Applying a transformation in $\mathrm{GL}_4(\mathcal{O}_K)$ we can assume that $x_1 \mid \tilde{F}, \tilde{G}$. Now we deduce that ϕ is not minimal by applying the transformation

$$\frac{1}{t}F(tx_1, x_2, x_3, x_4) = \frac{1}{t}G(tx_1, x_2, x_3, x_4) = 0.$$

(ii) If $\nu(F(0, 0, x_3, x_4)) > 1$, then ϕ is not minimal as we can apply the following transformation

$$\frac{1}{t^2}F(tx_1, tx_2, x_3, x_4) = \frac{1}{t}G(tx_1, tx_2, x_3, x_4) = 0.$$

Similarly, if $\nu(G(0, 0, x_3, x_4)) > 1$, then ϕ is not minimal.

Now we assume that $\nu(F(0, 0, x_3, x_4)) = \nu(G(0, 0, x_3, x_4)) = 1$. Consider the pair of quadrics

$$F' = \frac{1}{t}F(tx_1, tx_2, x_3, x_4) \text{ and } G' = \frac{1}{t}G(tx_1, tx_2, x_3, x_4).$$

If $\tilde{F}'$ and $\tilde{G}'$ have a common factor, then the genus one equation $F' = G' = 0$ is not minimal by (i). So we assume that $\tilde{F}'$ and $\tilde{G}'$ have no common factor. Let $(x_1, x_2, x_3, x_4) \in C(K)$. Clearing denominators, we can assume that $\min_{1 \le i \le 4} \nu(x_i) = 0$. Reducing $F, G \mod t$, we have $t \mid x_1, x_2$. Reducing $F, G \mod t^2$, we get $t \mid x_3, x_4$, which is a contradiction. Therefore, $C(K) = \emptyset$. □

Theorem 3.2.9. *Let ϕ be an integral genus one equation of degree $n \in \{1, 2, 3, 4\}$ defining a genus one smooth curve C over K. Let $\mathcal{C}$ be the degree-n-model defined by ϕ. When $n = 4$, assume that $\mathcal{C}$ is not isomorphic to a degree-4-model whose special fiber is of the form $\{x_1^2 = x_2^2 = 0\}$. If ϕ is minimal, then $\mathcal{C}$ is normal. In particular, $\mathcal{C}$ is an S-model for C.*

PROOF: If $\mathcal{C}_k$ consists only of multiplicity-1 components, then $\mathcal{C}_k$ is reduced and hence $\mathcal{C}$ is normal, see Lemma 3.2.2 (*ii*). Therefore, we only need to assume that ϕ is of degree n, $n \geq 2$, and $\mathcal{C}_k$ contains a component of multiplicity greater than 1.

For $n = 2$, let $\phi : y^2 = f(x)$ be minimal with $t \mid f(x)$. Then $\mathcal{C}$ is normal, since otherwise $\nu(f) \geq 2$, see Proposition 3.2.4 (*ii*), and ϕ is not minimal as we can apply the transformation $y^2 = \frac{1}{t^2} f(x)$.

For $n = 3$, let $\phi : F(x, y, z) = 0$ be a minimal genus one equation of degree 3 as in equation (3.1). Let $\mathcal{C}_k$ contain a multiplicity-m component, $m \geq 2$. It follows that after using a matrix in $\mathrm{GL}_3(\mathcal{O}_K)$, we can assume that $\nu(f_2), \nu(f_3) \geq 1$. We claim that $\nu(f_3) = 1$, and hence $\mathcal{C}$ is normal, see Proposition 3.2.6 (*ii*), since otherwise $\nu(f_3) \geq 2$ and ϕ is not minimal because we can apply the transformation $\frac{1}{t^2} F(x, ty, z)$.

For $n = 4$, let ϕ be a minimal genus one equation of degree 4 given by $F = G = 0$, where F and G are given as in equation (3.2). Let $\mathcal{C}_k$ contain a multiplicity-m component, $m \geq 2$. We will go through the different cases of Proposition 3.2.7.

If $\mathcal{C}_k : \{x_1x_3 = x_1x_4 + x_2^2 = 0\}$, then we claim that $\nu(x_4F(0, 0, x_3, x_4) - x_3G(0, 0, x_3, x_4)) = 1$, and hence $\mathcal{C}$ is normal. To prove that claim, we assume on the contrary that the latter valuation is greater than 1. We use a matrix in $\mathrm{GL}_4(\mathcal{O}_K)$ to get rid of the x_1^2, x_1x_2 and x_1x_4-terms in F and of the x_1^2, x_1x_2 and x_1x_3-terms in G. We notice that in the equation

$$x_4F(0, 0, x_3, x_4) - x_3G(0, 0, x_3, x_4) = -b_8x_3^3 + (a_8 - b_9)x_3^2x_4 + (a_9 - b_{10})x_3x_4^2 + a_{10}x_4^3,$$

we have $\min\{\nu(b_8), \nu(a_8 - b_9), \nu(a_9 - b_{10}), \nu(a_{10})\} \geq 2$. We apply the transformation $x_1 \mapsto x_1 - a_8x_3 - a_9x_4, x_i \mapsto x_i, i = 2, 3, 4$, to get rid of the terms $a_8x_3^2$ and $a_9x_3x_4$. Thereafter, we obtain the genus one equation $\phi' : F' = G' = 0$, where

$$\begin{aligned} F' &= x_1x_3 + a_5x_2^2 + a_6x_2x_3 + a_7x_2x_4 + a_{10}x_4^2, \\ G' &= x_1x_4 + x_2^2 + b_6x_2x_3 + b_7x_2x_4 + b_8x_3^2 + (b_9 - a_8)x_3x_4 + (b_{10} - a_9)x_4^2. \end{aligned}$$

We deduce that ϕ' is not minimal by applying the transformation

$$\frac{1}{t^2} F'(t^2x_1, tx_2, x_3, x_4) = \frac{1}{t^2} G'(t^2x_1, tx_2, x_3, x_4) = 0.$$

Assume that $\mathcal{C}_k : \{x_1^2 = x_2^2 + x_3x_4 = 0\}$. If $\mathcal{C}$ is not normal, then $\nu(F(0, x_2, x_3, x_4) - \mu(x_2^2 + x_3x_4)) \geq 2$ for some $\mu \in \mathcal{O}_K$, see Proposition 3.2.7 (*iii*). But then ϕ is not minimal as we can apply the transformation

$$\frac{1}{t^2}(F(tx_1,x_2,x_3,x_4)-\mu G(tx_1,x_2,x_3,x_4)) = G(tx_1,x_2,x_3,x_4) = 0.$$

Now assume that $\mathcal{C}_k$ contains a line $\Gamma : \{x_1 = x_2 = 0\}$ of multiplicity-m, $m \geq 2$, with $\tilde{F} = q(x_1,x_2)$ and $\tilde{G} = x_1x_3 + \mu x_2x_4 + q'(x_1,x_2)$, where $\mu \in k$. We claim that $\nu(a_8x_3^2 + a_9x_3x_4 + a_{10}x_4^2) = 1$, and hence $\mathcal{C}$ is normal at Γ, see Proposition 3.2.7 (*iv*), since otherwise ϕ is not minimal because we can apply the transformation

$$\frac{1}{t^2}F(tx_1,tx_2,x_3,x_4) = \frac{1}{t}G(tx_1,tx_2,x_3,x_4) = 0.$$

□

The following corollary is a direct consequence of Lemma 3.2.8 and Theorem 3.2.9.

Corollary 3.2.10. *Let ϕ be an integral genus one equation of degree $n \in \{1,2,3,4\}$ defining a genus one smooth curve C over K. Assume that $C(K) \neq \emptyset$. Let $\mathcal{C}$ be the degree-n-model defined by ϕ. If ϕ is minimal, then $\mathcal{C}$ is normal.*

3.3 Singular Loci

Let $\mathcal{C}$ be an S-curve with a smooth generic fiber. Then it is known that the normality of $\mathcal{C}$ implies that there are only finitely many non-regular points on $\mathcal{C}$, and all these points are closed points in the special fiber, see for example ([8], p. 8). The set of non-regular points of $\mathcal{C}$ will be called the *singular locus* of $\mathcal{C}$, and we will denote it by $\mathrm{Sing}(\mathcal{C})$.

In this section we will compute the singular locus $\mathrm{Sing}(\mathcal{C})$ of a normal degree-n-model $\mathcal{C}$ for a smooth genus one curve where $n \in \{1,2,3,4\}$.

The set of zeros of a polynomial $f \in \mathcal{O}_K[x_1,\ldots,x_n]$ will be denoted $V(f)$. If $f \in \mathcal{O}_K[x_1,\ldots,x_n]$, then we will write $f_i(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)/t^i$.

Proposition 3.3.1. *Let C be a smooth genus one curve over K defined by an integral genus one equation ϕ of degree* 1. *Let $\mathcal{C}$ be the degree-*1*-model for C given by ϕ. Then* $\mathrm{Sing}(\mathcal{C})$ *consists of one point at most.*

Proof: This point is the node of $\mathcal{C}_k$ if C has multiplicative reduction, and it is the cusp of $\mathcal{C}_k$ if C has additive reduction. □

Proposition 3.3.2. *Let C be a smooth genus one curve over K defined by an integral genus one equation $\phi : y^2 = f(x)$ of degree 2. Assume that ϕ defines a normal degree-2-model $\mathcal{C}$ for $C \to \mathbb{P}^1_K$. Then*

$$\mathrm{Sing}(\mathcal{C}) = \begin{cases} \{(x_0, 0) : (x - x_0)^2 | \tilde{f}(x)\} & \textit{if } \nu(f) = 0 \\ \{(x_0, 0) : x_0 \in V(\tilde{f}_1)\} & \textit{if } \nu(f) = 1 \end{cases}$$

Proof: Assume that $\nu(f) = 0$. Lemma 3.2.1 (i) implies that the singular locus of $\mathcal{C}$ consists of points $P = (x_0, 0) \in \mathcal{C}$ such that $y^2 - f(x) \in \mathfrak{m}_P^2 = \langle x - x_0, y, t\rangle^2$. Therefore, if $\nu(f) = 0$, then $\mathrm{Sing}(\mathcal{C})$ is the set $\{(x_0, 0) : (x - x_0)^2 \mid \tilde{f}(x)\}$.

Now assume that $\nu(f) = 1$. The maximal ideal corresponding to the generic point ξ of $\mathcal{C}_k$ is $\mathfrak{m}_\xi = \langle t, y\rangle$. Therefore, $\mathrm{Sing}(\mathcal{C})$ consists of the points $P = (x_0, 0)$ such that $\tilde{f}_1(x_0) = 0$. □

Remark 3.3.3. Keep the notations of Proposition 3.3.2. If $\nu(f) = 0$, then there are at most two points in the singular locus of $\mathcal{C}$. If $\nu(f) = 1$, then there are at most four points in the singular locus of $\mathcal{C}$ corresponding to the zeros of $\tilde{f}_1(x)$.

Proposition 3.3.4. *Let C be a smooth genus one curve over K defined by an integral genus one equation ϕ of degree 3 given by*

$$F(x, y, z) := by^3 + f(x, z)y^2 + g(x, z)y + h(x, z) = 0.$$

Assume that ϕ defines a normal degree-3-model $\mathcal{C}$ for $C \to \mathbb{P}^2_K$.

- *(i) If $\mathcal{C}_k$ consists of l multiplicity-1 irreducible components, then* $\mathrm{Sing}(\mathcal{C})$ *consists of one point at most when $l = 1$, and is contained in the set of intersection points of these components when $l \geq 2$.*
- *(ii) If* $\min\{\nu(g), \nu(h)\} \geq 1$, *then* $\mathrm{Sing}(\mathcal{C}) = \{(x_0 : 0 : z_0) : (x_0, z_0) \in V(\tilde{h}_1(x, z))\}$.

Proof: (i) If $\mathcal{C}_k$ is a nodal cubic or a cuspidal cubic, then $\mathrm{Sing}(\mathcal{C})$ consists of the node or the cusp respectively. If $\mathcal{C}_k$ consists of more than one multiplicity-1 component, then each point of $\mathcal{C}_k$ is regular except possibly the intersection points of these components.

(ii) Now assume that $\min\{\nu(g), \nu(h)\} \geq 1$. The normality implies that $\nu(h) = 1$, see Proposition 3.2.6. The maximal ideal corresponding to the generic point of the multiplicity-m component, $m \geq 2$, is $\langle y, t\rangle$. We dehomogenise by setting $z = 1$. Let $P = (x_0 : 0 : 1) \in \mathcal{C}$. The maximal ideal corresponding to P is $\mathfrak{m}_P = \langle x - x_0, y, t\rangle$. Lemma 3.2.1 (i) implies that $P \in \mathcal{C}$ is non-regular if and only if $F(x, y, 1) \in \mathfrak{m}_P^2$. Since $y^3, y^2, g(x, 1)y \in \mathfrak{m}_P^2$ and $\nu(h) = 1$, it follows that P is non-regular if and only $\tilde{h}_1(x_0, 1) = 0$. □

Remark 3.3.5. Keep the notations of Proposition 3.3.4. If $\mathcal{C}_k$ consists only of multiplicity-1 components, then the number of points in the singular locus of $\mathcal{C}$ is three points at most.

If $\mathcal{C}_k$ contains a multiplicity-m component, $m \geq 2$, then the fact that $h(x,z)$ is a homogeneous polynomial of degree 3 implies that $\mathcal{C}_k$ has at most three points in its singular locus corresponding to the factors of $\tilde{h}_1(x,z)$.

Proposition 3.3.6. *Let C be a smooth genus one curve over K defined by an integral genus one equation $\phi : F = G = 0$ of degree 4 given as in equation (3.2). Assume that ϕ defines a normal degree-4-model $\mathcal{C}$ for $C \to \mathbb{P}^3_K$.*

(i) If $\mathcal{C}_k$ consists of l multiplicity-1 irreducible components, then $\operatorname{Sing}(\mathcal{C})$ *consists of one point at most when $l = 1$, and is contained in the set of intersection points of these components when $l \geq 2$.*

(ii) If $\mathcal{C}_k$ is a conic and a double line with $\tilde{F} = x_1x_3$ and $\tilde{G} = x_1x_4 + x_2^2$, then

$$\operatorname{Sing}(\mathcal{C}) = \{(0:0:x:y) : (x,y) \in V(\tilde{h}_1(x_3,x_4))\},$$

where $h(x_3,x_4) = x_4F(0,0,x_3,x_4) - x_3G(0,0,x_3,x_4)$.

(iii) If $\mathcal{C}_k$ is a double conic with $\tilde{F} = x_1^2$ and $\tilde{G} = x_2^2 + x_3x_4$, then

$$\operatorname{Sing}(\mathcal{C}) = \{(0:xy:-x^2:y^2) : (x,y) \in V(\tilde{h}_1(x_2,x_4))\},$$

where $h(x_2,x_4) = F(0,x_2x_4,-x_2^2,x_4^2)$.

(iv) Assume that $\mathcal{C}_k$ contains a line $\Gamma : \{x_1 = x_2 = 0\}$ of multiplicity-m, $m \geq 2$, with $\tilde{F} = q(x_1,x_2)$ and $\tilde{G} = x_1x_3 + \mu x_2x_4 + q'(x_1,x_2)$ where $\mu \in k$. Then

$$S' \subseteq \operatorname{Sing}(\mathcal{C}) \cap \Gamma \subseteq S' \cup \{(0:0:0:1)\},$$

where $S' = \{(0:0:x:y) : (x,y) \in V(\tilde{F}_1(0,0,x_3,x_4))\}$.

Proof: *(i)* If $\mathcal{C}_k$ is a nodal or a cuspidal quartic, then $\operatorname{Sing}(\mathcal{C})$ consists of the node or the cusp respectively. If $\mathcal{C}_k$ consists of more than one multiplicity-1 component, then each point of $\mathcal{C}_k$ is regular except possibly the intersection points of these components.

Therefore, we assume that $\mathcal{C}_k$ contains a component of multiplicity greater than 1, we want to find the points of $\operatorname{Sing}(\mathcal{C})$ which lie on this multiple component. Let $P \in \mathcal{C}$. Then Lemma 3.2.1 *(ii)* implies that $P \in \mathcal{C}$ is non-regular if and only if either $F \in \mathfrak{m}_P^2$, or $G \in \mathfrak{m}_P^2$, or F, G are linearly dependent mod $\mathfrak{m}_P^2$.

(ii) The maximal ideal corresponding to the generic point of the double line is $\langle x_1, x_2, t\rangle$. Let P be a closed point on the double line. Since x_1 and t are linearly independent, we have $F \in \mathfrak{m}_P^2$ if and only if $x_3(P) = 0$ and $\nu(a_{10}) \geq 2$, in other words $F \in \mathfrak{m}_P^2$ if and only if $P = (0 : 0 : 0 : 1)$ and $\nu(a_{10}) \geq 2$.

Similarly, $G \in \mathfrak{m}_P^2$ if and only if $P = (0 : 0 : 1 : 0)$ and $\nu(b_8) \geq 2$.

Now for a point $P = (0 : 0 : x : y)$ on the double line of $\mathcal{C}_k$, we have F and G are linearly dependent if and only if $(x, y) \in V(\tilde{h}_1(x_3, x_4))$, where $h(x_3, x_4) = x_4F(0, 0, x_3, x_4)-x_3G(0, 0, x_3, x_4)$, see Proposition 3.2.7 (ii). Note that if a point P makes either F or G lie in $\mathfrak{m}_P^2$, then it is a point at which F and G are linearly dependent.

(iii) Let $l(x_2, x_3, x_4) = F(0, x_2, x_3, x_4)-\mu(a_5x_2^2+a_9x_3x_4)$, where $\mu = 1$ if $a_5 = a_9$, and $\mu = 0$ otherwise. We have $F \in \mathfrak{m}_p^2$ if and only if $P \in V(\tilde{l}_1(x_2, x_3, x_4))\cap V(x_2^2+x_3x_4)$, i.e., $P = (0 : xz : -x^2 : z^2)$ where $(x, z) \in V(\tilde{h}_1(x_2, x_4))$ and $h(x_2, x_4) = F(0, x_2x_4, -x_2^2, x_4^2)$.

For any $P \in \mathcal{C}$, we have $G \notin \mathfrak{m}_P^2$ because $x_3x_4(P) \notin \mathfrak{m}_P^2$ for any $P \in \mathcal{C}$. There are no new non-regular points which can cause linear dependence because $x_2^2(P) + x_3x_4(P) \notin \mathfrak{m}_P^2$ for any $P \in \mathcal{C}$.

(iv) Now let P be a point on the multiple line Γ. $F \in \mathfrak{m}_P^2$ if and only if $P = (0 : 0 : x : y)$, where $(x, y) \in V(\tilde{F}_1(0, 0, x_3, x_4)$.

Consider $\tilde{G} = x_1x_3 + \mu x_2x_4 + q'(x_1, x_2)$ where $\mu \in k$. If $\mu \neq 0$, then $G \notin \mathfrak{m}_P^2$ for any $P \in \Gamma$. If $\mu = 0$, then the linear independence of t and x_1 implies that $G \in \mathfrak{m}_P^2$ if and only if $x_3(P) = 0$ and $\tilde{G}_1(0, 0, x_3(P), x_4(P)) \in \mathfrak{m}_P$. Therefore, $G \in \mathfrak{m}_P^2$ if and only if $P = (0 : 0 : 0 : 1)$ and $\nu(b_{10}) \geq 2$. We have no new non-regular points which can cause linear dependence. □

Remark 3.3.7. Assume that the special fiber $\mathcal{C}_k$ is given by $x_2^2 = x_1x_3+\mu x_2x_4 = 0,\ \mu \in k$. We have

$$S' \cup S'' \subseteq \mathrm{Sing}(\mathcal{C}) \subseteq S' \cup S'' \cup \{(0 : 0 : 0 : 1)\},$$

where S' is as in Proposition 3.3.6 and $S'' = \{(x : 0 : 0 : y) : (x, y) \in V(\tilde{F}_1(x_1, 0, 0, x_4)\}$. Hence $\mathrm{Sing}(\mathcal{C})$ consists of five points at most.

In any other case, the above proposition implies that a degree-4-model for a smooth genus one curve has at most four points in its singular locus. Indeed, if C_k consists of multiplicity-1 components, then the number of points in $\mathrm{Sing}(\mathcal{C})$ is bounded by the number of these components. If $\mathcal{C}_k$ is a conic and a double line as in (ii), then the number of points in $\mathrm{Sing}(\mathcal{C})$ is at most three points corresponding to the factors of the degree-3 polynomial $\tilde{h}_1$ given in (ii). If $\mathcal{C}_k$ is a double conic as in (iii), then $\mathrm{Sing}(\mathcal{C})$ consists of at most four points corresponding to the factors of the degree-4 polynomial $\tilde{h}_1$ of (iii). If $\mathcal{C}_k$ consists of a double line and two simple lines, then $\mathrm{Sing}(\mathcal{C})$ consists at most of three points on the double line plus the intersection point of the simple lines.

Chapter 4

Criteria for minimality

In this chapter we will assume that K is a Henselian discrete valuation field with normalised valuation ν. We write $\mathcal{O}_K$ for the ring of integers. We fix a uniformiser t. The residue field $k = \mathcal{O}_K/t\mathcal{O}_K$ is not necessarily algebraically closed. Set $S := \operatorname{Spec} \mathcal{O}_K$. When we are dealing with degree-2-models for smooth genus one curves, we are going to assume that $\operatorname{char} k \neq 2$.

In this chapter we give geometric criteria for the minimality of normal degree-n-models for smooth genus one curves. The main result introduced in this chapter is stated in the following theorem.

Theorem 4.0.1. Let ϕ be an integral genus one equation of degree $n = 1, 2, 3, 4$. Assume that ϕ defines a smooth genus one curve C over K, and that $C(K) \neq \emptyset$. Assume moreover that ϕ defines a normal degree-n-model $\mathcal{C}$ for C. Let E/K be the Jacobian elliptic curve of C, and E^{min} be the minimal proper regular model of E.

Then ϕ is minimal, see Definition 2.1.3, if and only if $\widetilde{\mathcal{C}} \cong E^{min}$, where $\widetilde{\mathcal{C}} \to \mathcal{C}$ is the minimal desingularisation of $\mathcal{C}$.

Theorem 4.0.1 is known for the case $n = 1$, see ([20], §9.4) or [8]. Moreover, Liu gave a proof for the case $n = 2$, see ([18], Proposition 8 (b)). We will give a proof which works for $n = 1, 2, 3, 4$.

4.1 Canonical sheaves of degree-n-models

Let ϕ be an integral genus one equation of degree $n = 1, 2, 3, 4$. Assume that ϕ defines a smooth genus one curve C/K whose Jacobian elliptic curve is E. Assume moreover that $C(K) \neq \emptyset$. Then $C \cong_K E$, whence the minimal proper regular model C^{min} of C

is isomorphic to the minimal proper regular model E^{min} of E. For this reason we will dispense with C^{min} and write E^{min} from here on.

The following proposition describes the canonical sheaf $\omega_{E^{min}/S}$ of E^{min}.

Proposition 4.1.1. *Let E/K be an elliptic curve. Let E^{min} be its minimal proper regular model. Then the canonical sheaf $\omega_{E^{min}/S}$ of E^{min} is a trivial line bundle on E^{min}. In other words, there exists $\omega_0 \in H^0(E^{min}, \omega_{E^{min}/S})$ such that $\omega_{E^{min}/S} = \omega_0 \mathcal{O}_{E^{min}}$.*

Proof: See ([8], Example 7.7). □

If $\mathcal{C}$ is an S-model for a smooth genus one curve C, then the canonical sheaf $\omega_{\mathcal{C}/S}$ of $\mathcal{C}$ satisfies $\omega_{\mathcal{C}/S}|_C = \omega_{C/K}$, see ([20], Theorem 6.4.9 (b)). Moreover, the restriction of the canonical sheaf $\omega_{\mathcal{C}/S}$ on C gives a canonical injection $H^0(\mathcal{C}, \omega_{\mathcal{C}/S}) \hookrightarrow H^0(C, \omega_{C/K})$, see ([20], Corollary 9.2.25 (a)).

Lemma 4.1.2. *Let $\mathcal{C}$ be a normal degree-n-model for a smooth genus one curve C/K with minimal desingularisation $g : \widetilde{\mathcal{C}} \to \mathcal{C}$. Assume that $C(K) \neq \emptyset$. Let E^{min} be the minimal proper regular model of the Jacobian E of C. Then*

$$H^0(E^{min}, \omega_{E^{min}/S}) = H^0(\widetilde{\mathcal{C}}, \omega_{\widetilde{\mathcal{C}}/S}) \subseteq H^0(\mathcal{C}, \omega_{\mathcal{C}/S}).$$

Proof: Since $\widetilde{\mathcal{C}}$ and E^{min} are two regular S-curves with a contraction map $\widetilde{\mathcal{C}} \to E^{min}$, we have $H^0(E^{min}, \omega_{E^{min}/S}) = H^0(\widetilde{\mathcal{C}}, \omega_{\widetilde{\mathcal{C}}/S})$ as subgroups of $H^0(E, \omega_{E/K})$, see ([20], Corollary 9.2.25 (b)).

Let F be the divisor such that $\widetilde{\mathcal{C}} \setminus F \cong \mathcal{C} \setminus g(F)$. Then we have the following relations in $H^0(E, \omega_{E/K})$:

$$H^0(\widetilde{\mathcal{C}}, \omega_{\widetilde{\mathcal{C}}/S}) \subseteq H^0(\widetilde{\mathcal{C}} \setminus F, \omega_{\widetilde{\mathcal{C}}/S}) = H^0(\mathcal{C} \setminus g(F), \omega_{\mathcal{C}/S}) = H^0(\mathcal{C}, \omega_{\mathcal{C}/S}),$$

the second equality holds because $g(F)$ has codimension 2 in $\mathcal{C}$, see ([20], Lemma 9.2.17 (a)). □

In the following proposition we compute the canonical sheaf of a degree-n-model for a smooth genus one curve.

Proposition 4.1.3. *Let ϕ be an integral genus one equation of degree $n = 1, 2, 3, 4$. Assume that ϕ defines a smooth genus one curve C/K. Assume moreover that ϕ defines a normal degree-n-model $\mathcal{C}$ for C. Then $\omega_{\mathcal{C}/S} = \omega \mathcal{O}_{\mathcal{C}}$, where $\omega \in H^0(C, \omega_{C/K})$ is*

(i) if $n = 1$ and $\phi : y^2 + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$, then

$$\omega = \frac{du}{2v + (a_1u + a_3)}, \text{ where } u = x/z, v = y/z \in K(\mathcal{C}),$$

(ii) if $n = 2$ *and* $\phi : y^2 = f(x, 1)$, *then*

$$\omega = \frac{dx}{2y},$$

(iii) if $n = 3$ *and* $\phi : F(x, y, z) = 0$, *then*

$$\omega = \frac{du}{\partial F/\partial v}, \text{ where } u = x/z, v = y/z \in K(\mathcal{C}),$$

(iv) if $n = 4$ *and* $\phi : F_1(x_1, x_2, x_3, x_4) = F_2(x_1, x_2, x_3, x_4) = 0$, *then*

$$\omega = \frac{du}{\frac{\partial F_1}{\partial w}\frac{\partial F_2}{\partial v} - \frac{\partial F_1}{\partial v}\frac{\partial F_2}{\partial w}}, \text{ where } u = x_2/x_1,\ v = x_3/x_1,\ w = x_4/x_1 \in K(\mathcal{C}).$$

PROOF: According to the definition of the canonical sheaf, see Definition 2.3.5, we have to check first that $\mathcal{C}$ is a local complete intersection. In fact, $\mathcal{C}$ is a global complete intersection over S. That follows directly from the fact that $\mathcal{C}$ can be embedded in $\mathbb{P}^2_S$ for $n = 1, 2, 3$, and it can be embedded in $\mathbb{P}^3_S$ as an intersection of a pair of quadrics for $n = 4$.

For $n = 1, 3$, let V_1 be the open affine subset of $\mathcal{C}$ obtained by setting $z = 1$. Then we can write $\mathcal{O}_{\mathcal{C}}(V_1)$ as

$$\mathcal{O}_{\mathcal{C}}(V_1) = \mathcal{O}_K[u, v]/(bv^3 + f_1(u, 1)v^2 + f_2(u, 1)v + f_3(u, 1)),$$

where $b = 0$ and $f_1(u, 1) = 1$ when $n = 1$. Therefore, $\omega_{V_1/S} = \omega\mathcal{O}_{V_1}$, see Lemma 2.3.6. Let V_2 be the open affine subset of $\mathcal{C}$ given by setting $y = 1$. Set $r = x/y, s = z/y$. Then $\mathcal{O}_{\mathcal{C}}(V_2) = \mathcal{O}_K[r, s]/(g(r, s))$ where

$$g(r, s) = b + f_1(r, s) + f_2(r, s) + f_3(r, s).$$

Hence $\omega_{V_2/S} = \omega'\mathcal{O}_{V_2}$, where $\omega' = \frac{ds}{\partial g/\partial r}$.

We note that $r = u/v,\ s = 1/v$ in $K(\mathcal{C})$, and $ds = -\frac{1}{v^2}dv$ in $H^0(C, \omega_{C/K})$. Therefore, $\omega' = \omega$.

For $n = 2$, the first affine piece V_1 satisfies $\mathcal{O}_{\mathcal{C}}(V_1) = \mathcal{O}_K[x, y]/(y^2 - f(x, 1))$ and therefore $\omega_{V_1/S} = \omega\mathcal{O}_{V_1}$. Let V_2 be the open affine subset of $\mathcal{C}$ given by $s^2 = f(1, r)$, where $r = 1/x, y = x^2 s$. Then $\mathcal{O}_{\mathcal{C}}(V_2) = \mathcal{O}_K[r, s]/(s^2 - f(1, r))$ and $\omega_{V_2/S} = \omega'\mathcal{O}_{V_2}$, where $\omega' = \frac{dr}{2s}$. Since $r = 1/x \in K(\mathcal{C})$ and $dr = -\frac{1}{x^2}dx \in H^0(C, \omega_{C/K})$, it follows that $\omega' = \omega$.

Now as $\mathcal{C} = V_1 \cup V_2$, we have $\omega_{\mathcal{C}/S} = \omega\mathcal{O}_{\mathcal{C}}$.

The proof is similar for $n = 4$. Let V_1 be the open subset of $\mathcal{C}$ given by $x_1 = 1$. We have

$$\mathcal{O}_{\mathcal{C}}(V_1) = \mathcal{O}_K[u, v, w]/(F_1(1, u, v, w), F_2(1, u, v, w)),$$

hence $\omega_{V_1/S} = \omega\mathcal{O}_V$ by Lemma 2.3.6.

Now let V_2 be the open subset of $\mathcal{C}$ given by $x_2 = 1$. Set $q = x_1/x_2,\ r = x_3/x_2,\ s = x_4/x_2$. Then $\mathcal{O}_{\mathcal{C}}(V_2) = \mathcal{O}_K[q, r, s]/(F_1(q, 1, r, s), F_2(q, 1, r, s))$.
Therefore, $\omega_{V_2/S}$ is generated by the rational differential

$$\omega' := \frac{dq}{\frac{\partial F_1}{\partial s}\frac{\partial F_2}{\partial r} - \frac{\partial F_1}{\partial r}\frac{\partial F_2}{\partial s}}.$$

Using the relations

$$q = 1/u,\ r = v/u,\ s = w/u,\ dq = -\frac{1}{u^2}du \text{ in } K(\mathcal{C}) \text{ and } H^0(C, \omega_{C/K}),$$

we find that $\omega' = \omega$. As $\mathcal{C} = V_1 \cup V_2$, we have $\omega_{\mathcal{C}/S} = \omega\mathcal{O}_{\mathcal{C}}$. □

Recall the definitions of the groups $\mathcal{G}_n(K)$ from §2.1. Now we state the following corollary of Proposition 5.19 in [15].

Corollary 4.1.4. *Let ϕ_1, ϕ_2 be two K-equivalent integral genus one equations of degree $n = 1, 2, 3, 4$, where $\phi_1 = g.\phi_2, g \in \mathcal{G}_n(K)$. Assume that ϕ_1, ϕ_2 define smooth genus one curves whose Jacobian elliptic curve is E/K. Assume moreover that ϕ_1, ϕ_2 define two normal degree-n-models $\mathcal{C}_1, \mathcal{C}_2$. If $\omega_{\mathcal{C}_i/S} = \omega_i\mathcal{O}_{\mathcal{C}_i}, i = 1, 2$, where ω_i is defined as in Proposition 4.1.3, then $\omega_2 = \alpha(\det g)\omega_1$ as elements in $H^0(E, \omega_{E/K})$, where $\alpha \in \mathcal{O}_K^*$.*

Proof: The genus one equation ϕ_i defines a smooth genus one curve $C_i,\ i = 1, 2$. The element $g \in \mathcal{G}_n(K)$ defines an isomorphism $\gamma : C_1 \cong C_2$. The isomorphism γ satisfies $\gamma^*\omega_2 = (\det g)\omega_1$, see ([15], Proposition 5.19). □

Corollary 4.1.5. *Let ϕ_1, ϕ_2 be two K-equivalent integral genus one equations of degree $n = 1, 2, 3, 4$, with corresponding discriminants Δ_1, Δ_2. Assume that ϕ_1, ϕ_2 define smooth genus one curves whose Jacobian elliptic curve is E. Assume moreover that ϕ_1, ϕ_2 define two normal degree-n-models $\mathcal{C}_1, \mathcal{C}_2$. If $\omega_{\mathcal{C}_i/S} = \omega_i\mathcal{O}_{\mathcal{C}_i}, i = 1, 2$, then*

$$\Delta_1\omega_1^{\otimes 12} = \lambda\Delta_2\omega_2^{\otimes 12} \in H^0(E, \omega_{E/K})^{\otimes 12}, \textit{ where } \lambda \in \mathcal{O}_K^*.$$

Proof: Assume that $\phi_1 = g.\phi_2$ where $g \in \mathcal{G}_n(K)$. Since $\Delta_1 = (\det g)^{12}.\Delta_2$, see Theorem 2.1.2 (i), and $\omega_1 = \alpha(\det g)^{-1}\omega_2$, where $\alpha \in \mathcal{O}_K^*$, see Corollary 4.1.4, we have $\Delta_1\omega_1^{\otimes 12} = \alpha^{12}\Delta_2\omega_2^{\otimes 12}$. □

Let ϕ_1 be a minimal genus one equation of degree $n = 1, 2, 3, 4$. Let ϕ_2 be a genus one equation K-equivalent to ϕ_1. Let ω_1, ω_2 be as in Corollary 4.1.4. We will call the integer m such that $\omega_2 = ut^{-m}\omega_1, u \in \mathcal{O}_K^*$, the *level* of ϕ_2, and denote it by $\mathrm{level}(\phi_2)$.

Corollary 4.1.5 implies that the level of an integral genus one equation of degree n does not depend on the choice of the minimal genus one equation ϕ_1. It follows immediately that an integral genus one equation ϕ of degree n is minimal if and only if $\mathrm{level}(\phi) = 0$.

Note that according to Corollary 4.1.5, we have $\nu(\Delta_2) = \nu(\Delta_1) + 12\,\mathrm{level}(\phi_2)$. Hence $\Delta_2 = u^{-1}t^{12\,\mathrm{level}(\phi_2)}\Delta_1$.

Lemma 4.1.6. *Let $\mathcal{C}$ be an S-model for a smooth genus one curve C. Then we have $H^0(\mathcal{C}, \mathcal{O}_\mathcal{C}) = \mathcal{O}_K$. In particular, if $\omega_{\mathcal{C}/S} = \omega\mathcal{O}_\mathcal{C}$, then $H^0(\mathcal{C}, \omega_{\mathcal{C}/S}) = \omega\mathcal{O}_K$.*

PROOF: The $\mathcal{O}_K$-module $H^0(\mathcal{C}, \mathcal{O}_\mathcal{C})$ is integral over $\mathcal{O}_K$, see ([20], Proposition 3.3.18). Moreover, $H^0(\mathcal{C}, \mathcal{O}_\mathcal{C})$ is contained in $\mathcal{O}_\mathcal{C}(C)$, but $\mathcal{O}_\mathcal{C}(C) = K$ as C is geometrically integral, see ([20], Corollary 3.3.21). □

Lemma 4.1.7. *Assume that ϕ_1, ϕ_2 are two genus one equations of degree n defining two normal degree-n-models $\mathcal{C}_1, \mathcal{C}_2$ for a smooth genus one curve C. Let E be the Jacobian elliptic curve of C. Then we have $H^0(\mathcal{C}_1, \omega_{\mathcal{C}_1/S}) \subseteq H^0(\mathcal{C}_2, \omega_{\mathcal{C}_2/S})$ as sub-$\mathcal{O}_K$-modules of $H^0(E, \omega_{E/K})$ if and only if $\nu(\Delta(\phi_1)) \leq \nu(\Delta(\phi_2))$. Moreover, the equality of the two submodules holds if and only if ϕ_1 and ϕ_2 have the same level.*

PROOF: Let $\omega_{\mathcal{C}_i/S} = \omega_i\mathcal{O}_{\mathcal{C}_i}$, $\omega_i \in H^0(E, \omega_{E/K})$, $i = 1, 2$. The assumption $H^0(\mathcal{C}_1, \omega_{\mathcal{C}_1/S}) \subseteq H^0(\mathcal{C}_2, \omega_{\mathcal{C}_2/S})$ is equivalent to $\omega_1\mathcal{O}_K \subseteq \omega_2\mathcal{O}_K$, by Lemma 4.1.6, i.e., $\omega_1 \in \omega_2\mathcal{O}_K$. Since $\Delta(\phi_1)\omega_1^{\otimes 12} = \lambda\Delta(\phi_2)\omega_2^{\otimes 12}$ for some $\lambda \in \mathcal{O}_K^*$, see Corollary 4.1.5, it follows that $\omega_1 \in \omega_2\mathcal{O}_K$ is equivalent to $\Delta(\phi_2) \in \Delta(\phi_1)\mathcal{O}_K$, i.e., $\nu(\Delta(\phi_1)) \leq \nu(\Delta(\phi_2))$.

The equality of the sub-$\mathcal{O}_K$-modules $H^0(\mathcal{C}_1, \omega_{\mathcal{C}_1/S}) = H^0(\mathcal{C}_2, \omega_{\mathcal{C}_2/S})$ means that $\omega_1\mathcal{O}_K = \omega_2\mathcal{O}_K$ as $\mathcal{O}_K$-modules, i.e., $\omega_1 \in \omega_2\mathcal{O}_K^*$. The latter statement means that ϕ_1 and ϕ_2 have the same level. □

The following lemma compares the generators of the canonical sheaves of E^{min} and $\mathcal{C}$ when $E^{min} \cong \widetilde{\mathcal{C}}$.

Lemma 4.1.8. *If $f : E^{min} \to \mathcal{C}$ is a contraction morphism, where $\mathcal{C}$ is a degree-n-model for a smooth genus one curve, then $f_*\omega_{E^{min}/S} = \omega_{\mathcal{C}/S}$. In other words, if $\omega_{E^{min}/S} = \omega_0\mathcal{O}_{E^{min}}$ and $\omega_{\mathcal{C}/S} = \omega\mathcal{O}_\mathcal{C}$, then $\omega_0 \in \omega\mathcal{O}_K^*$.*

PROOF: See ([20], Corollary 9.4.18 (b)). □

Now we will prove the first part of Theorem 4.0.1.

Proposition 4.1.9. *Let ϕ be an integral genus one equation of degree $n = 1, 2, 3, 4$. Assume that ϕ defines a smooth genus one curve C over K, and that $C(K) \neq \emptyset$. Assume moreover that ϕ defines a normal degree-n-model $\mathcal{C}$ for C. Let E/K be the Jacobian elliptic curve of C, and E^{min} be the minimal proper regular model of E.*

If $\widetilde{\mathcal{C}} \cong E^{min}$, where $\widetilde{\mathcal{C}} \to \mathcal{C}$ is the minimal desingularisation of $\mathcal{C}$, then ϕ is minimal.

Proof: The assumption $\widetilde{\mathcal{C}} \cong E^{min}$ means that $\mathcal{C}$ is obtained from E^{min} by contracting the components different from those of $\mathcal{C}_k$, thus we have a contraction morphism $f : E^{min} \to \mathcal{C}$.

We are going to prove that if $\mathcal{C}'$ is another normal degree-n-model for C given by a genus one equation ϕ' of degree n, then

$$H^0(\mathcal{C}, \omega_{\mathcal{C}/S}) \subseteq H^0(\mathcal{C}', \omega_{\mathcal{C}'/S}), \tag{4.1}$$

hence $\nu(\Delta(\phi)) \leq \nu(\Delta(\phi'))$, see Lemma 4.1.7, therefore ϕ is minimal.

To prove (4.1), let $\widetilde{\mathcal{C}'} \to \mathcal{C}'$ be the minimal desingularisation of $\mathcal{C}'$. According to Lemma 4.1.2, we have

$$H^0(E^{min}, \omega_{E^{min}/S}) = H^0(\widetilde{\mathcal{C}'}, \omega_{\widetilde{\mathcal{C}'}/S}) \subseteq H^0(\mathcal{C}', \omega_{\mathcal{C}'/S}).$$

The fact that $\mathcal{C}$ is obtained from E^{min} by contraction implies that $f_*\omega_{E^{min}/S} = \omega_{\mathcal{C}/S}$, see Lemma 4.1.8. Therefore, we have $H^0(\mathcal{C}, \omega_{\mathcal{C}/S}) = H^0(E^{min}, \omega_{E^{min}/S})$, and (4.1) holds. □

4.2 Constructing minimal degree-n-models

Let ϕ be a genus one equation of degree $n \in \{1, 2, 3, 4\}$ defining a smooth genus one curve C/K. Assume that $C(K) \neq \emptyset$. Let E be the Jacobian elliptic curve of C with minimal proper regular model E^{min}. If $P \in C(K)$, then $\overline{\{P\}}$ will denote the Zariski closure of $\{P\}$ in E^{min}.

When $n = 1$, set $D_1 = 3.\overline{\{P\}}$ where $P \in C(K)$. When $n \geq 2$, let $\sum(P_i) \in \mathrm{Div}(C)$ be a K-rational divisor of a hyperplane section on C. In particular, the degree of this divisor is n. Assume moreover that $\overline{\{P_i\}} \cap E_k^{min}$ is contained in one and only one irreducible component of E_k^{min}. Consider the following Weil divisor on E^{min}

$$D_n = \sum \overline{\{P_i\}}.$$

Since E^{min} is regular, the divisor D_n is a Cartier divisor, see Remark 2.2.9.

We define an S-model $\mathcal{C}_n$ for C as follows

$$\mathcal{C}_n := \mathrm{Proj}(\bigoplus_{m=0}^{\infty} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n))).$$

There is a canonical morphism $u : E^{min} \longrightarrow \mathcal{C}_n$ contracting all the irreducible components of E_k^{min} apart from the ones having nonempty intersection with D_n, see Theorem 2.2.11.

Lemma 4.2.1. *Let D_n, $n \in \{1,2,3,4\}$, be as above. Then $H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n)), m \geq 1$, is a free $\mathcal{O}_K$-module of rank $3m$ if $n = 1$, and of rank mn if $n \geq 2$.*

Proof: It is known that $H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n)) \otimes_{\mathcal{O}_K} K \cong H^0(C, \mathcal{O}_C(mD_n|_C))$, see for example ([20], Corollary 5.2.27). Moreover, by virtue of Riemann-Roch Theorem, $H^0(C, \mathcal{O}_C(mD_n|_C))$ is a $3m$-dimensional K-vector space when $n = 1$, and an mn-dimensional K-vector space when $n \geq 2$.

Since $\mathcal{O}_{E^{min}}(mD_n)$ is an invertible sheaf on E^{min}, it follows that $H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n))$ is a flat $\mathcal{O}_K$-module, see ([20], Lemma 5.2.31). But since $\mathcal{O}_K$ is a principal ideal domain, an $\mathcal{O}_K$-module is flat if and only if it is torsion-free over $\mathcal{O}_K$. Therefore, $H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n))$ is torsion-free over $\mathcal{O}_K$.

Since $\mathcal{O}_K$ is a local ring, it is a general fact that a finitely generated flat $\mathcal{O}_K$-module is free. Hence $H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n))$ is free over $\mathcal{O}_K$. Thus $H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n))$ is a free $\mathcal{O}_K$-module of rank $3m$ if $n = 1$, and of rank mn if $n \geq 2$. □

Lemma 4.2.2. *Let E be an elliptic curve over K with minimal proper regular model $\pi : E^{min} \rightarrow S$. Let D_n be the divisor on E^{min} defined above. Then the following are true.*

(i) $H^1(E^{min}, \mathcal{O}_{E^{min}})$ is a free $\mathcal{O}_K$-module of rank 1.

(ii) For any $m \geq 2$, there exists an exact sequence

$$0 \rightarrow H^0(E^{min}, \mathcal{O}_{E^{min}}((m-1)D_n)) \rightarrow H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n)) \rightarrow A^{\otimes m} \rightarrow 0,$$

where A is a free $\mathcal{O}_K$-module.

Proof: (i) Since $\mathcal{O}_{E^{min}}$ is invertible on E^{min}, we have $H^1(E^{min}, \mathcal{O}_{E^{min}})$ is a finitely generated $\mathcal{O}_K$-module, see ([20], Theorem 5.3.2). Moreover, since $\mathcal{O}_K$ is a local ring, it follows that $H^1(E^{min}, \mathcal{O}_{E^{min}})$ is free.

We have $H^1(E^{min}, \mathcal{O}_{E^{min}}) \otimes_{\mathcal{O}_K} K = H^1(E, \mathcal{O}_E) \cong K$ and $H^1(E^{min}, \mathcal{O}_{E^{min}}) \otimes_{\mathcal{O}_K} k = H^1(E_k^{min}, \mathcal{O}_{E_k^{min}}) \cong k$, see ([20], Lemma 9.4.28).

Let $\mathcal{L} := R^1\pi_*\mathcal{O}_{E^{min}}$ be the first higher direct image of $\mathcal{O}_{E^{min}}$. By definition we have $H^0(S,\mathcal{L}) = H^1(E^{min},\mathcal{O}_{E^{min}})$, see ([20], Proposition 5.2.28). Now we have $\mathcal{L}$ is locally free of rank 1 and hence $H^0(S,\mathcal{L})$ is a flat $\mathcal{O}_K$-module, see ([20], Lemma 5.2.31), which implies that it is torsion-free over $\mathcal{O}_K$. It follows that $H^1(E^{min},\mathcal{O}_{E^{min}})$ is free of rank 1.

(ii) Let $i : D_n \to E^{min}$ be the canonical closed immersion. For any $m \geq 1$, we have a canonical isomorphism $\mathcal{O}_{E^{min}}(mD_n) \otimes_{\mathcal{O}_{E^{min}}} i_*\mathcal{O}_{D_n} \to i_*i^*\mathcal{O}_{E^{min}}(mD_n)$, see ([20], Exercise 5.1.1). But $\mathcal{O}_{D_n}$ fits in

$$0 \to \mathcal{O}_{E^{min}}(-D_n) \to \mathcal{O}_{E^{min}} \to \mathcal{O}_{D_n} \to 0.$$

Therefore, $i_*i^*\mathcal{O}_{E^{min}}(mD_n) \cong \mathcal{O}_{E^{min}}(mD_n) \otimes_{\mathcal{O}_{E^{min}}} \mathcal{O}_{E^{min}}/\mathcal{O}_{E^{min}}(-D_n)$, and thus we have the following short exact sequence

$$0 \to \mathcal{O}_{E^{min}}((m-1)D_n) \to \mathcal{O}_{E^{min}}(mD_n) \to i_*i^*\mathcal{O}_{E^{min}}(mD_n) \to 0. \tag{4.2}$$

Consider the morphism $E^{min} \to \mathbb{P}^d_S$ determined by D_n. We note that

$$(\pi i)_*(i^*\mathcal{O}_{E^{min}}(mD_n)) \cong (\pi i)_*(i^*\mathcal{O}_{\mathbb{P}^d_S}(m)|_{E^{min}}) \cong (\pi i)_*(\mathcal{O}_{D_n}(m)) \cong ((\pi i)_*\mathcal{O}_{D_n})(m),$$

see ([20], Lemma 7.1.29 (b) and Exercise 5.1.16 (c)) for the second and last isomorphisms respectively. Thus we have the following exact sequence by applying π_* to sequence (4.2)

$$0 \to \pi_*\mathcal{O}_{E^{min}}((m-1)D_n) \to \pi_*\mathcal{O}_{E^{min}}(mD_n) \to \mathcal{L}'^{\otimes m} \to 0, \tag{4.3}$$

where $\mathcal{L}' = ((\pi i)_*\mathcal{O}_{D_n})(1)$. Taking global sections in (4.3) we have

$$\begin{aligned} 0 \quad &\to \quad H^0(E^{min},\mathcal{O}_{E^{min}}((m-1)D_n)) \to H^0(E^{min},\mathcal{O}_{E^{min}}(mD_n)) \to H^0(S,\mathcal{L}'^{\otimes m}) \\ &\to \quad H^1(E^{min},\mathcal{O}_{E^{min}}((m-1)D_n)) \to \dots \end{aligned} \tag{4.4}$$

For $m \geq 1$, we have $H^1(E^{min},\mathcal{O}_{E^{min}}(mD_n)) \otimes K = H^1(E,\mathcal{O}_E(mD_n|_K)) = 0$, see for example ([24], Chapter III). Therefore, we have $H^1(E^{min},\mathcal{O}_{E^{min}}(mD_n)) = 0$ when $m \geq 1$. Therefore, taking $m \geq 2$ in sequence (4.4) we have

$$0 \to H^0(E^{min},\mathcal{O}_{E^{min}}((m-1)D_n)) \to H^0(E^{min},\mathcal{O}_{E^{min}}(mD_n)) \to H^0(S,\mathcal{L}'^{\otimes m}) \to 0.$$

Taking $m = 1$ in sequence (4.4) we will have

$$0 \to \mathcal{O}_K \to H^0(E^{min},\mathcal{O}_{E^{min}}(D_n)) \to H^0(S,\mathcal{L}') \to H^1(E^{min},\mathcal{O}_{E^{min}}) \to 0. \tag{4.5}$$

Now $\mathcal{L}'$ is an invertible sheaf over $\mathcal{O}_S$, therefore $H^0(S,\mathcal{L}')$ is a finitely generated torsion-free $\mathcal{O}_K$-module over a local ring, and hence it is free. □

The following theorem is classical for $n = 1, 2$, see for example ([20], §9.4) and [18]. Recall that when $n = 2$, we assume that $\operatorname{char} k \neq 2$.

Theorem 4.2.3. *Let $\mathcal{C}_n$ and D_n, $n \in \{1,2,3,4\}$, be as above. Then there exists an integral genus one equation ϕ_n of degree n defining $\mathcal{C}_n$. Moreover, ϕ_n is minimal.*

Proof: For $n = 1$, Lemma 4.2.2 (ii) allows us to pick a basis $\{1, x, y\}$ of the free module $H^0(E^{min}, \mathcal{O}_{E^{min}}(3D_1))$ such that $\{1, x\}$ is a basis of $H^0(E^{min}, \mathcal{O}_{E^{min}}(2D_1))$. Now proceed as in §2.1 to write a genus one equation $\phi_1 : f(x, y) = 0$ of degree 1, where f is some dependence relation in $H^0(E^{min}, \mathcal{O}_{E^{min}}(6D_1))$. The morphism

$$\lambda_1 : \mathcal{C}_1 := \operatorname{Proj}(\bigoplus_{m\geq 0} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_1))) \longrightarrow \mathbb{P}^2_S$$

associated to the basis $\{1, x, y\}$ of $H^0(E^{min}, \mathcal{O}_{E^{min}}(3D_1))$ sends $\mathcal{C}_1$ into the cubic $\mathcal{C}_1'$ defined by $f(x, y) = 0$. We know that both $\mathcal{C}_1$ and $\mathcal{C}_1'$ are normal and integral, hence $\lambda_1 : \mathcal{C}_1 \to \mathcal{C}_1'$ is a birational morphism, see ([20], Exercise 3.2.6). Since the special fibers of both $\mathcal{C}_1$ and $\mathcal{C}_1'$ are irreducible, it follows that $\lambda_1 : \mathcal{C}_1 \to \mathcal{C}_1'$ is an isomorphism, see ([20], Exercise 8.3.8 (b)).

For $n = 2$, we pick a basis $\{1, x\}$ of $H^0(E^{min}, \mathcal{O}_{E^{min}}(D_2))$. Let λ_2 be the morphism

$$\lambda_2 : \mathcal{C}_2 := \operatorname{Proj}(\bigoplus_{m\geq 0} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_2))) \to \mathbb{P}^1_S = \operatorname{Spec}\mathcal{O}_K[x] \cup \operatorname{Spec}\mathcal{O}_K[1/x]$$

associated to the basis $\{1, x\}$. Let $U = \lambda_2^{-1}(\operatorname{Spec}\mathcal{O}_K[x])$, $V = \lambda_2^{-1}(\operatorname{Spec}\mathcal{O}_K[1/x])$. We have $\mathcal{C}_2 = U \cup V$. Taking the integral closure of $\mathcal{O}_K[x]$ in $K(\mathcal{C}_2)$, we have

$$\mathcal{O}_{\mathcal{C}_2}(U) = \mathcal{O}_K[x] \oplus y\mathcal{O}_K[x], \text{ for some } y \in \mathcal{O}_{\mathcal{C}_2}(U),$$

moreover there exist $g(x), f(x) \in \mathcal{O}_K[x]$ such that $\deg g \leq 2$, $\deg f \leq 4$ and $y^2 + g(x)y = f(x)$, see ([18], Lemme 1). As 2 is invertible in $\mathcal{O}_K$, we can complete the square and assume that $g = 0$. The surjective homomorphism

$$\mathcal{O}_K[x, y]/(y^2 - f(x)) \to \mathcal{O}_{\mathcal{C}_2}(U),\ y \mapsto y,$$

is an isomorphism because the left-hand term is integral of dimension 2, see ([20], Remark 8.3.25). Following the same argument we have $\mathcal{O}_K[w, z]/(z^2 - h(w)) \cong \mathcal{O}_{\mathcal{C}_2}(V)$, where $w = 1/x$, $z = y/x^2$, and $h(w) = w^4 f(1/w)$. Therefore, $\mathcal{C}_2$ is the union of the two affine open schemes

$$U = \operatorname{Spec}\mathcal{O}_K[x, y]/(y^2 - f(x)),\ V = \operatorname{Spec}\mathcal{O}_K[w, z]/(z^2 - w^4 f(1/w)).$$

For $n = 3, 4$, we pick a basis $\{x_1, \ldots, x_n\}$ of $H^0(E^{min}, \mathcal{O}_{E^{min}}(D_n))$. Let $\lambda_n : E^{min} \to \mathbb{P}^{n-1}_S$ be the morphism associated to the basis $\{x_1, \ldots, x_n\}$. Let Z_n be the closed subset

$\lambda_n(E^{min}) \subset \mathbb{P}_S^{n-1}$ endowed with the reduced scheme structure. We are going to show that Z_n is defined by an integral genus one equation of degree n. Then we show that $\mathcal{C}_n \cong Z_n$, where $\mathcal{C}_n := \mathrm{Proj}(\bigoplus_{m\geq 0} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n)))$.

When $n = 3$, the free $\mathcal{O}_K$-module $H^0(E^{min}, \mathcal{O}_{E^{min}}(3D_3))$ is of rank-9, see Lemma 4.2.1, but it contains the 10 elements $x_1^3, x_2^3, x_3^3, x_1^2x_2, x_1^2x_3, x_2^2x_1, x_2^2x_3, x_3^2x_1, x_3^2x_2, x_1x_2x_3$. It follows that there are $a_i \in \mathcal{O}_K$ such that

$$F := a_1x_1^3+a_2x_2^3+a_3x_3^3+a_4x_1^2x_2+a_5x_1^2x_3+a_6x_2^2x_1+a_7x_2^2x_3+a_8x_3^2x_1+a_9x_3^2x_2+a_{10}x_1x_2x_3 = 0.$$

Rescaling x, y and z, we can assume that there is at least one $a_i \in \mathcal{O}_K^*$. Hence Z_3 is contained in $\mathrm{Proj}\,\mathcal{O}_K[x_1, x_2, x_3]/(F)$.

When $n = 4$, we consider the 10 elements $x_1^2, x_1x_2, x_1x_3, x_1x_4, x_2^2, x_2x_3, x_2x_4, x_3^2, x_3x_4, x_4^2$ in the rank-8 free $\mathcal{O}_K$-module $H^0(E^{min}, \mathcal{O}_{E^{min}}(2D_4))$. They satisfy two linearly independent quadrics Q and R. Therefore, Z_4 is contained in the intersection of Q and R.

We want to show that $Z_n = \mathrm{Proj}\,\mathcal{O}_K[x_1, \ldots, x_n]/I_n$, where $I_3 = (F)$ and $I_4 = (Q, R)$. Since $Z_n \subseteq \mathrm{Proj}\,\mathcal{O}_K[x_1, \ldots, x_n]/I_n$, we have $\mathrm{Proj}\,\mathcal{O}_K[x_1, \ldots, x_n]/I_n = Z_n \cup Z_n'$, for some closed subscheme $Z_n' \subset \mathbb{P}_S^{n-1}$, $Z_n' \neq \mathrm{Proj}\,\mathcal{O}_K[x_1, \ldots, x_n]/I_n$. Recall that C is the generic fiber of E^{min}. Since $D_n|_C$ is a divisor of degree n, $n \in \{3, 4\}$, on C, it follows that $\mathrm{Proj}(\mathcal{O}_K[x_1, \ldots, x_n]/I_n \otimes K)$ is irreducible, see ([24], Chapter III). Hence, $\mathrm{Proj}\,\mathcal{O}_K[x_1, \ldots, x_n]/I_n$ is irreducible itself, see for example ([2], Lemma 2.2). It follows from the definition of irreducibility that $Z_n' = \emptyset$, and the closed subscheme Z_n is $\mathrm{Proj}\,\mathcal{O}_K[x_1, \ldots, x_n]/I_n$.

According to the description of the contraction morphism included in the proof of ([20], Proposition 8.3.30), the morphism $\lambda_n : E^{min} \to Z_n \subseteq \mathbb{P}_S^{n-1}$, $n = 3, 4$, factors into $u_n : E^{min} \to \mathcal{C}_n$ followed by $v_n : \mathcal{C}_n \to Z_n$, where v_n is the normalisation morphism. It is understood that v_n is a finite morphism, hence for an irreducible component Γ of E_k^{min}, $\lambda_n(\Gamma)$ is a point if and only if $u_n(\Gamma)$ is a point. In other words, the special fibers of $\mathcal{C}_n$ and Z_n have the same number of irreducible components. We have shown that Z_n is integral of dimension 2. Hence both $\mathcal{C}_n$ and Z_n have dimension 2, their generic fibers are isomorphic, and their special fibers have the same number of irreducible components. By virtue of ([20], Remark 8.3.25), $v_n : \mathcal{C}_n \to Z_n$ is an isomorphism.

Since $\mathcal{C}_n$ is obtained by contracting components in E^{min}, i.e., the minimal desingularisation of $\mathcal{C}_n$ is isomorphic to E^{min}, we have that $\mathcal{C}_n$ is minimal, see Proposition 4.1.9. □

4.3 Geometric criteria

In this section we will prove Theorem 4.0.1 and state some direct corollaries.

Lemma 4.3.1. *Let ϕ be an integral genus one equation of degree $n = 1, 2, 3, 4$. Assume that ϕ defines a smooth genus one curve C over K, and that $C(K) \neq \emptyset$. Assume moreover that ϕ defines a normal degree-n-model $\mathcal{C}$ for C. Let E/K be the Jacobian elliptic curve of C, and E^{min} be the minimal proper regular model of E. Then we have $H^0(E^{min}, \omega_{E^{min}/S}) = H^0(\mathcal{C}, \omega_{\mathcal{C}/S})$ as sub-$\mathcal{O}_K$-modules of $H^0(E, \omega_{E/K})$ if and only if ϕ is minimal.*

Proof: Assume that $H^0(E^{min}, \omega_{E^{min}/S}) = H^0(\mathcal{C}, \omega_{\mathcal{C}/S})$. Let $\mathcal{C}'$ be another degree-n-model for C. Let $\widetilde{\mathcal{C}'} \to \mathcal{C}'$ be the minimal desingularisation of $\mathcal{C}'$. Then we have

$$H^0(\mathcal{C}, \omega_{\mathcal{C}/S}) = H^0(E^{min}, \omega_{E^{min}}/S) = H^0(\widetilde{\mathcal{C}'}, \omega_{\widetilde{\mathcal{C}'}/S}) \subseteq H^0(\mathcal{C}', \omega_{\mathcal{C}'/S}),$$

see Lemma 4.1.2. Therefore, ϕ is minimal by virtue of Lemma 4.1.7.

Now assume that ϕ is minimal. Let H be the K-rational hyperplane section divisor defined by ϕ, see §2.1. If $n = 1$, then $H = 3(P)$ for some $P \in C(K)$. Set $D_1 = 3\overline{\{P\}}$, where $\overline{\{P\}}$ is the Zariski closure of $\{P\}$ in E^{min}. If $n \geq 2$, then pick $x \in E_k^{min}$ such that x lies on a multiplicity-1 component and on no other component, and x is defined over k. Hensel's Lemma allows us to lift x to a point $P \in C(K)$. Set $Q \in C(K)$ to be such that $(Q) \sim H - (n-1).(P)$. Set $D_n = (n-1).\overline{\{P\}} + \overline{\{Q\}}$.

Consider the S-model $\mathcal{C}'$ for C given by

$$\mathcal{C}' = \mathrm{Proj}(\bigoplus_{m=0}^{\infty} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_n))).$$

Let ϕ' be the minimal genus one equation of degree n defining $\mathcal{C}'$, see Theorem 4.2.3. Since H_n and $D_n|_C$ have the same degree and sum, they are linearly equivalent and the genus one equations ϕ and ϕ' are K-equivalent, see for example [10].

Moreover, since $\mathcal{C}'$ is obtained from E^{min} by contraction, Lemma 4.1.8 shows that $\omega_{E^{min}/S} = \omega'\mathcal{O}_{E^{min}}$ where $\omega' \in H^0(E, \omega_{E/K})$ is such that $\omega_{\mathcal{C}'/S} = \omega'\mathcal{O}_{\mathcal{C}'}$.

Since the genus one equations ϕ and ϕ' are both minimal, in particular they have the same level, Lemma 4.1.7 implies the second equality of the following

$$H^0(E^{min}, \omega_{E^{min}/S}) = H^0(\mathcal{C}', \omega_{\mathcal{C}'/S}) = H^0(\mathcal{C}, \omega_{\mathcal{C}/S}).$$

□

Proof of Theorem 4.0.1: We proved one of the implications of the theorem in Proposition 4.1.9.

Assume that ϕ is minimal and that $\omega_{\mathcal{C}/S} = \omega\mathcal{O}_{\mathcal{C}}$ for some $\omega \in H^0(E, \omega_{E/K})$.

We assume on the contrary that $\widetilde{\mathcal{C}} \ncong E^{min}$, and therefore $\mathcal{C}_k$ contains an exceptional divisor Γ.

Let $\mathcal{B}$ be the set of points $x \in \widetilde{\mathcal{C}}$ where $\omega_{\widetilde{\mathcal{C}}/S}$ is not generated by its global sections. Since Γ is an exceptional divisor, we have $\deg \omega_{\widetilde{\mathcal{C}}/S}|_\Gamma < 0$, see ([20], Proposition 9.3.10), it follows that $H^0(\Gamma, \omega_{\widetilde{\mathcal{C}}/S}|_\Gamma) = 0$, therefore $\Gamma \subseteq \mathcal{B}$. But we have

$$\omega_{\widetilde{\mathcal{C}}/S}|_\Gamma = \omega_{\mathcal{C}/S}|_\Gamma = \omega\mathcal{O}_{\mathcal{C}}|_\Gamma,$$

and the global sections of $\omega_{\widetilde{\mathcal{C}}/S}$ are

$$H^0(\widetilde{\mathcal{C}}, \omega_{\widetilde{\mathcal{C}}/S}) = H^0(E^{min}, \omega_{E^{min}/S}) = H^0(\mathcal{C}, \omega_{\mathcal{C}/S}) = \omega\mathcal{O}_K,$$

where the second equality is justified by $\mathcal{C}$ being minimal, see Lemma 4.3.1. Therefore, $\omega_{\widetilde{\mathcal{C}}/S}$ is generated by its global sections at every $x \in \Gamma$, whence a contradiction. Thus $\mathcal{C}_k$ contains no exceptional divisors and $\widetilde{\mathcal{C}} \cong E^{min}$. □

Now we state more criteria for normal degree-n-models to be minimal.

Corollary 4.3.2. *Let $\phi, C, \mathcal{C}, E, \widetilde{\mathcal{C}}$ and E^{min} be as in Theorem 4.0.1. Assume that $\omega_{\mathcal{C}/S} = \omega\mathcal{O}_{\mathcal{C}}$ for some $\omega \in H^0(E, \omega_{E/K})$. Then the following statements are equivalent.*

(i) *ϕ is minimal.*

(ii) $\omega_{\widetilde{\mathcal{C}}/S} = \omega\mathcal{O}_{\widetilde{\mathcal{C}}}$.

(iii) $H^0(\widetilde{\mathcal{C}}, \omega_{\widetilde{\mathcal{C}}/S}) = H^0(\mathcal{C}, \omega_{\mathcal{C}/S}) = \omega\mathcal{O}_K$.

Proof: $(i) \Rightarrow (ii)$: Since ϕ is minimal, we have $\widetilde{\mathcal{C}} \cong E^{min}$. But $\omega_{E^{min}/S} = \omega\mathcal{O}_{E^{min}}$, see Lemma 4.1.8. Whence (ii).

$(ii) \Rightarrow (iii)$ follows directly from Lemma 4.1.6.

$(iii) \Rightarrow (i)$: Since $H^0(\widetilde{\mathcal{C}}, \omega_{\widetilde{\mathcal{C}}/S}) = H^0(E^{min}, \omega_{E^{min}/S})$, see Lemma 4.1.2, then ϕ is minimal, see Lemma 4.3.1. □

In §3.2 we stated all the combinatorial possibilities for the special fiber of a degree-n-model $\mathcal{C}$ for a smooth genus one curve C. Theorem 4.0.1 allows us to find out which of these possibilities occur for minimal degree-n-models for C according to the Kodaira symbol of the Jacobian elliptic curve E of C. That can be done by looking at the pull-back of the irreducible components of $\mathcal{C}_k \setminus \mathrm{Sing}(\mathcal{C})$ under the contraction morphism

$u : E^{min} \to \mathcal{C}$, where $\mathrm{Sing}(\mathcal{C})$ is the singular locus of $\mathcal{C}$. The pull-back of an irreducible component Γ of $\mathcal{C}_k \setminus \mathrm{Sing}(\mathcal{C})$ in E^{min}_k is called the *strict transform* of Γ. It is understood that the strict transform of an irreducible component Γ has the same multiplicity as Γ. For example, if $\mathcal{C}_k$ consists of a conic and a double line, then the strict transform of $\mathcal{C}_k$ in E^{min}_k consists of a multiplicity-1 irreducible component corresponding to the conic, and a multiplicity-2 irreducible component corresponding to the double line.

We set
$T_1 = \{$nodal cubic, conic + line, three lines$\}$,
$T_2 = \{$cuspidal cubic, conic + tangent, three concurrent lines$\}$,
$T_3 = \{$line + double line, triple line$\}$,

$$T_4 = \left\{ \begin{array}{c} \text{nodal quartic, secant conics, conic + two lines not crossing on it, four lines,} \\ \text{cubic + secant line} \end{array} \right\},$$

$$T_5 = \left\{ \begin{array}{c} \text{cuspidal quartic, tangent conics, conic + two lines crossing on it,} \\ \text{four concurrent lines, cubic + tangent line} \end{array} \right\},$$

$T_6 = \{$two lines + double line, conic + double line, double conic, two double lines$\}$,
$T_7 = \{$triple line + line, quadruple line$\}$.

In the following corollary we assume that k is algebraically closed.

Corollary 4.3.3. *Let ϕ be a minimal genus one equation of degree $n = 1, 2, 3, 4$. Assume that ϕ defines a smooth genus one curve C, $C(K) \neq \emptyset$. Let E be the Jacobian elliptic curve of C with Kodaira symbol T. Assume that $\mathcal{C}$ is a minimal degree-n-model for C defined by ϕ. Then $\mathcal{C}_k$ lies in one of the sets determined by the following tables.*

T	*n=1*	*n=2*
I_0	$\{$*smooth cubic*$\}$	$\{$*smooth quartic*$\}$
$\mathrm{I}_m, m \geq 1$	$\{$*nodal cubic*$\}$	$\{$*nodal quartic, intersecting lines*$\}$
II	$\{$*cuspidal cubic*$\}$	$\{$*cuspidal quartic*$\}$
$\mathrm{III}, \mathrm{IV}$	$\{$*cuspidal cubic*$\}$	$\{$*cuspidal quartic, tangent conics*$\}$
$\mathrm{I}^*_m, m \geq 0, \mathrm{IV}^*, \mathrm{III}^*$	$\{$*cuspidal cubic*$\}$	$\{$*cuspidal quartic, tangent conics, double line* $\}$
II^*	$\{$*cuspidal cubic*$\}$	$\{$*cuspidal quartic, double line*$\}$

T	*n=3*	*n=4*
I_0	$\{$*smooth cubic*$\}$	$\{$*smooth quartic*$\}$
$\mathrm{I}_m, m \geq 1$	T_1	T_4
II	$\{$*cuspidal cubic*$\}$	$\{$*cuspidal quartic*$\}$
III	$\{$*cuspidal cubic, conic+tangent*$\}$	$\{$*cubic+tangent*$\}\cup$ $\{$*cuspidal quartic, tangent conics*$\}$
IV	T_2	$T_5 \setminus \{$*four concurrent lines*$\}$
$\mathrm{I}_m^*, m \geq 0$	$T_2\cup\{$*line+double line*$\}$	$T_5 \cup T_6$
IV^*	$T_2 \cup T_3$	$T_6\cup$ $\{$*triple line+line*$\}\cup$ $T_5\setminus$ $\{$*four concurrent lines*$\}$
III^*	$T_3\cup$ $\{$*cuspidal cubic, conic+tangent*$\}$	$T_6 \cup T_7\cup\{$*cuspidal quartic*$\}\cup$ $\{$*tangent conics, cubic+tangent*$\}$
II^*	$T_3\cup\{$*cuspidal cubic*$\}$	$\{$*cuspidal quartic*$\}\cup T_7\cup$ $T_6\setminus\{$*two lines+double line*$\}$

PROOF: The case $n = 1$ is already known, see ([27], Chapter III, Proposition 1.4).

In order to classify which of these forms of the special fibers occur when E has multiplicative reduction and which occur when E has additive reduction, we need to compute the valuations of the invariants c_4, c_6, and Δ corresponding to ϕ. For explicit formulae for c_4, c_6, and Δ see ([11], Lemma 2.9).

For $n = 2$, if $\mathcal{C}_k$ is either a nodal quartic or two intersecting lines, then $\nu(c_4) = 0$, and $\nu(\Delta) \geq 1$, hence E has multiplicative reduction. Similarly, for $n = 3, 4$, if $\mathcal{C}_k$ lies in T_1, T_4 respectively, then E has multiplicative reduction. The remaining forms of $\mathcal{C}_k$ force $\nu(c_4) \geq 1, \nu(\Delta) \geq 1$, therefore E has additive reduction.

Now since ϕ is minimal, it follows that $E^{min} \cong \widetilde{\mathcal{C}}$, where $\widetilde{\mathcal{C}} \to \mathcal{C}$ is the minimal desingularisation of $\mathcal{C}$, see Theorem 4.0.1. The strict transforms of the irreducible components of $\mathcal{C}_k$ are irreducible components in E_k^{min} with the same multiplicities. We consider the multiplicities of the irreducible components of $\mathcal{C}_k$, and the number l_m of irreducible components with multiplicity-m in $\mathcal{C}_k$. If the graph associated to E_k^{min} has components with the same multiplicities as those of $\mathcal{C}_k$, and E_k^{min} contains at least l_m components with multiplicity-m, then the strict transform of $\mathcal{C}_k$ can lie in E_k^{min}, hence we obtain the classification given above. For a reference for the graphs associated to E_k^{min} see ([28], Chapter IV, Table 9.4.1). □

Chapter 5

Isomorphisms of degree-n-models

For this chapter we assume that K is a Henselian discrete valuation field with ring of integers $\mathcal{O}_K$. The residue field k is algebraically closed, t is a uniformiser, and $S = \operatorname{Spec} \mathcal{O}_K$.

In the first section of this chapter we see the conditions under which two minimal degree-n-models are isomorphic. In fact, we show that two minimal degree-n-models are isomorphic if and only if they have the same special fiber, see Theorem 5.1.4 below. In the second section we assume that Γ is an irreducible component of multiplicity-1 in E_k^{min}, then we count the number of minimal degree-n-models with special fibers containing a multiplicity-1 irreducible component whose strict transform in E_k^{min} is Γ. The results obtained in the second section will not be used elsewhere in this thesis.

5.1 Isomorphic degree-n-models

Let $(\mathcal{C}, \alpha)$ be a minimal degree-n-model for a smooth genus one curve C over K. Assume that $C(K) \neq \emptyset$. Let E be the Jacobian elliptic curve of C, and E^{min} be the minimal proper regular model of E. Let $P \in C(K)$. Fix an isomorphism $\beta : C \to E$ such that $\beta(P) = 0_E$. The isomorphism β identifies the group structure on the elliptic curve (C, P) with the group structure on $(E, 0_E)$, hence β extends to an isomorphism between the minimal proper regular model of C and E^{min}.

Let $\mathcal{C}$ be a degree-n-model for a smooth genus one curve over K. Let Γ be an irreducible component of $\mathcal{C}_k$. We will write $\deg_k(\Gamma)$ for the degree of Γ. By the *type* of Γ we mean the ordered pair $(\operatorname{mult}_k(\Gamma), \deg_k(\Gamma))$, where $\operatorname{mult}_k(\Gamma)$ is the multiplicity of Γ defined in §3.2.

Remark 5.1.1. Let $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ be two isomorphic minimal degree-n-models for a smooth genus one curve C over K. Assume that $C(K) \neq \emptyset$. Let E be the Jacobian of C with minimal proper regular model E^{min}. Let $\alpha := \alpha_2^{-1}\alpha_1 : (\mathcal{C}_1)_K \to (\mathcal{C}_2)_K$. By the definition of isomorphic degree-n-models, the map α extends to an S-isomorphism $\tilde{\alpha} : \mathcal{C}_1 \to \mathcal{C}_2$ which is defined by an element in $\mathcal{G}_n(\mathcal{O}_K)$. Therefore, if Γ is an irreducible component of $(\mathcal{C}_2)_k$, then $\tilde{\alpha}^*\Gamma$ is an irreducible component of $(\mathcal{C}_1)_k$ with the same type as Γ. Moreover, after identifying the minimal proper regular model of C with E^{min}, $(\mathcal{C}_1)_k$ and $(\mathcal{C}_2)_k$ have the same strict transform in E_k^{min}.

In this section we show that the converse of Remark 5.1.1 holds. More precisely, if the strict transforms of the special fibers of two minimal degree-n-models coincide in the sense given in Theorem 5.1.4, then these degree-n-models are isomorphic.

Let x be a generator of $K(\mathbb{P}_K^1)$ over K. We define the S-scheme $\mathbb{P}_x^1$ to be

$$\mathbb{P}_x^1 := \operatorname{Spec} \mathcal{O}_K[x] \cup \operatorname{Spec} \mathcal{O}_K[1/x].$$

We have $\mathbb{P}_x^1 \cong \mathbb{P}_S^1$ as S-schemes and $\mathbb{P}_x^1$ is an S-model for $\mathbb{P}_K^1$. Furthermore, every smooth S-model for $\mathbb{P}_K^1$ is obtained that way, see ([18], §4). Two S-models $\mathbb{P}_x^1, \mathbb{P}_u^1$ for $\mathbb{P}_K^1$ are isomorphic if and only if there exists a matrix

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K)$$

such that $x = (au + b)/(cu + d)$.

Now we use models of projective lines to describe isomorphic degree-2-models for smooth genus one curves over K.

Theorem 5.1.2. *Let $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ be two minimal degree-n-models, $n = 1, 2$, for a smooth genus one curve C over K. Assume that $C(K) \neq \emptyset$. Set $\alpha : \alpha_2^{-1}\alpha_1$. Then the following statements are equivalent.*

(i) The map α extends to an isomorphism $\tilde{\alpha} : \mathcal{C}_1 \to \mathcal{C}_2$ of S-schemes.

(ii) The curves $(\mathcal{C}_1)_k$ and $(\mathcal{C}_2)_k$ have the same strict transform in E_k^{min}.

(iii) $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ are isomorphic as degree-n-models for C.

Proof: This is clear for the case $n = 1$ as there is a unique minimal degree-1-model for C. So we will assume that $n = 2$.

(i) $\Leftrightarrow$ *(ii)* : It is known that a birational map induces an S-isomorphism if and only if it establishes a bijection between the generic points of the special fibers, see for example

([20], Remark 8.3.25). Hence (i) is equivalent to the statement that any irreducible component of $(\mathcal{C}_2)_k$ is carried to an irreducible component of $(\mathcal{C}_1)_k$ under $\tilde{\alpha}^*$. The latter occurs if and only if the strict transforms of $(\mathcal{C}_1)_k$ and $(\mathcal{C}_2)_k$ coincide in E_k^{min} because $\tilde{\alpha}$ extends to the identity on E^{min}.

$(i) \Leftrightarrow (iii)$: The degree-2-model $\mathcal{C}_i, i = 1, 2$, is obtained from E^{min} by a contraction morphism, see Theorem 4.0.1. Let D_i be a Cartier divisor on E^{min} such that

$$\mathcal{C}_i := \mathrm{Proj}(\bigoplus_{m \geq 0} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_i))).$$

Let $\{1, x_i\}$ be a basis for the free module $H^0(E^{min}, \mathcal{O}_{E^{min}}(D_i))$. Now consider the morphism $\mathcal{C}_i \xrightarrow{x_i} \mathbb{P}^1_{x_i}$, we have the commutative diagram

$$\begin{tikzcd}
\mathcal{C}_1 \arrow[r, "x_1"] \arrow[d, "\tilde{\alpha}"'] & \mathbb{P}^1_{x_1} \arrow[d, "\tilde{\alpha}"'] \\
\mathcal{C}_2 \arrow[r, "x_2"] & \mathbb{P}^1_{x_2}
\end{tikzcd}$$

Therefore, $\mathcal{C}_1$ and $\mathcal{C}_2$ are S-isomorphic if and only if $\mathbb{P}^1_{x_1}$ and $\mathbb{P}^1_{x_2}$ are S-isomorphic. The latter occurs if and only if $\tilde{\alpha} : \mathbb{P}^1_{x_1} \to \mathbb{P}^1_{x_2}$ is defined by an element in $\mathrm{GL}_2(\mathcal{O}_K)$ which means that $\mathcal{C}_1$ and $\mathcal{C}_2$ are isomorphic degree-2-models for C. □

The following example, shown to me by T. Fisher, illustrates that Theorem 5.1.2 does not hold for $n = 4$.

Example 5.1.3. Consider the following forms

$$F_1 = tx_1^2 - x_2x_4 + x_3^2,\ F_2 = tx_4^2 - x_1x_3 + x_2^2,$$
$$F_1' = x_1^2 - x_2x_4 + tx_3^2,\ F_2' = x_4^2 - x_1x_3 + tx_2^2.$$

The genus one equations $\phi : F_1 = F_2 = 0$ and $\phi' : F_1' = F_2' = 0$ are minimal of degree 4. The genus one equation ϕ defines a smooth genus one curve C. Let $(\mathcal{C}, \mathrm{id}_4)$ and $(\mathcal{C}', \alpha')$ be two minimal degree-4-models for C, where $\mathcal{C}$ is given by ϕ, $\mathcal{C}'$ is given by ϕ', and α' is multiplying x_2 and x_3 by t and dividing through by t. Now $\mathcal{C}_k$ consists of the line $\Gamma_1 : \{x_2 = x_3 = 0\}$ and the twisted cubic Γ_2 parameterised by $[u : v] \mapsto [u^3 : u^2v : uv^2 : v^3]$. Similarly, $\mathcal{C}_k'$ consists of $\Gamma_1' : \{x_1 = x_4 = 0\}$ and the twisted cubic $\Gamma_2' : [u : v] \mapsto [u^2v : u^3 : v^3 : uv^2]$. The morphism α' carries the generic point of Γ_1 to the generic point of Γ_2' and the generic point of Γ_2 to the generic point of Γ_1'. But $(\mathcal{C}, \mathrm{id}_4)$ and $(\mathcal{C}', \alpha')$ are not isomorphic degree-4-models.

The above example shows that we need to modify Theorem 5.1.2 when $n = 3, 4$.

Let $(\mathcal{C}_i, \alpha_i), i = 1, 2$, be a minimal degree-$n$-model for a smooth genus one curve $C \to \mathbb{P}^{n-1}_K$, $n = 3, 4$. Let D_i be a divisor on E^{min} which defines $\mathcal{C}_i$, more precisely $\mathcal{C}_i$ is obtained from E^{min} by contraction using D_i. What we are going to do next is to compare the divisors $D_1|_{E^{min}_k}$ and $D_2|_{E^{min}_k}$.

Recall that the degree map $\deg_k : \mathrm{Pic}(\mathbb{P}^1_k) \to \mathbb{Z}$ is an isomorphism. Moreover, $\mathrm{Pic}^0(\mathbb{P}^1_k) = 1$, see for example ([20], Proposition 9.3.16). Therefore, two effective divisors D_1, D_2 on $\mathbb{P}^1_k$ are linearly equivalent if and only if they have the same degree.

Let X be a projective curve over k. Let $X_1, \ldots, X_m$ be its irreducible components with respective multiplicities $d_1, \ldots, d_m$. We give each X_i the reduced subscheme structure. If $\mathcal{L}$ is an invertible sheaf on X, then we define the *partial degree* of $\mathcal{L}$ on X_i to be $\deg(\mathcal{L}|_{X_i})$. Then we have

$$\deg \mathcal{L} = \sum_{i=1}^{m} d_i \deg(\mathcal{L}|_{X_i}),$$

see for example ([20], Proposition 7.5.7) or ([5], §9.1, Proposition 5).

We consider the families of invertible sheaves of degree 0 on X, $\mathrm{Pic}^0(X)$. Since k is algebraically closed, Corollary 13 of ([5], §9.3) shows that $\mathrm{Pic}^0(X)$ consists of all elements of $\mathrm{Pic}(X)$ whose partial degree on each irreducible component X_i is zero.

Now we are in a place to generalise Theorem 5.1.2. Recall that the type of an irreducible component Γ is the pair $(\mathrm{mult}_k(\Gamma), \deg_k(\Gamma))$.

Theorem 5.1.4. *Let $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ be two minimal degree-n-models, $n = 1, 2, 3, 4$, for a smooth genus one curve C over K. Assume that $C(K) \neq \emptyset$. Set $\alpha = \alpha_2^{-1}\alpha_1$ and denote its extension $\mathcal{C}_1 \dashrightarrow \mathcal{C}_2$ by $\tilde{\alpha}$. Then the following statements are equivalent.*

(i) $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ are isomorphic as degree-n-models for C.

(ii) For every irreducible component Γ of $(\mathcal{C}_2)_k$, $\tilde{\alpha}^*\Gamma$ is an irreducible component of $(\mathcal{C}_1)_k$ with the same type as Γ.

Proof: The cases $n = 1, 2$ have been done in Theorem 5.1.2.

Let $n = 3, 4$. That (i) implies (ii) follows from Remark 5.1.1.

$(ii) \Rightarrow (i)$: We want to show that $\tilde{\alpha}$ is defined by an element in $\mathcal{G}_n(\mathcal{O}_K)$.

Let E^{min} be the minimal proper regular model of the Jacobian E of C. Statement (ii) implies that both $(\mathcal{C}_1)_k$ and $(\mathcal{C}_2)_k$ have the same strict transform in E^{min}_k.

Let D_i be a defining divisor of $\mathcal{C}_i$ as a contraction in E^{min}, i.e.,

$$\mathcal{C}_i = \mathrm{Proj}(\bigoplus_{m \geq 0} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD_i))).$$

Set $\mathcal{L}_i = \mathcal{O}_{E^{min}}(D_i)$, $D_{i,k} = D_i|_{E_k^{min}}$ and $\mathcal{L}_{i,k} = \mathcal{L}_i|_{E_k^{min}}$.

Let Γ be an irreducible component of $(\mathcal{C}_2)_k$. Consider the strict transform $\tilde{\Gamma}$ of the irreducible components Γ and $\tilde{\alpha}^*\Gamma$ in E_k^{min}. Since Γ and $\tilde{\alpha}^*\Gamma$ have the same type, it follows that $\deg_k \mathcal{L}_{1,k}|_{\tilde{\Gamma}} = \deg_k \mathcal{L}_{2,k}|_{\tilde{\Gamma}}$. For any irreducible component Λ which is not a strict transform of a component of $(\mathcal{C}_i)_k$, we have $\deg_k \mathcal{L}_{i,k}|_\Lambda = 0$. Since each irreducible component of E_k^{min} is isomorphic to $\mathbb{P}_k^1$ and $D_{1,k}, D_{2,k}$ have the same degree on each irreducible component of E_k^{min}, we have $D_{1,k} \sim D_{2,k}$ and $\mathcal{L}_{1,k} \cong \mathcal{L}_{2,k}$.

Now we know that $C(K) \neq \emptyset$, $\mathcal{L}_1|_{(\mathcal{C}_1)_K} \cong \mathcal{L}_2|_{(\mathcal{C}_2)_K}$, and we have established the isomorphism $\mathcal{L}_{1,k} \cong \mathcal{L}_{2,k}$, these imply that $\mathcal{L}_1 \cong \mathcal{L}_2$, see ([20], Exercise 9.1.13 (b)). Therefore, $H^0(E^{min}, \mathcal{L}_1)$ and $H^0(E^{min}, \mathcal{L}_2)$ are isomorphic as $\mathcal{O}_K$-modules, and $\tilde{\alpha}$ is a change of basis of a free $\mathcal{O}_K$-module of rank n, hence $\tilde{\alpha}$ is defined by an element in $\mathcal{G}_n(\mathcal{O}_K)$. □

In the following corollary we assume that $\operatorname{char} k \neq 2$ when $n = 2$.

Corollary 5.1.5. *Let C a smooth genus one curve. Assume that $C(K) \neq \emptyset$. Assume moreover that the Jacobian E of C has either reduction types* I_0 *or* I_1. *Then there is a unique minimal degree-n-model for C.*

Proof: There is always a unique minimal degree-1-model for C. So assume $n \geq 2$. Let E^{min} be the minimal proper regular model of E. According to Theorem 4.0.1, any minimal degree-n-model for C is obtained from E^{min} via contraction. Therefore, the special fiber of a minimal degree-n-model for C consists of one irreducible component of multiplicity-1 because E_k^{min} consists of a unique irreducible component of multiplicity-1. By virtue of Theorem 5.1.4, if there are two minimal degree-n-models for C, then they are isomorphic as they have the same strict transform in E_k^{min}. □

5.2 Degree-n- and degree-$(n-1)$-models, $n \geq 3$

In this section we will count minimal degree-n-models with a specific property.

Let $\mathcal{C}$ be an S-model for a curve C/K. Let x be a closed point of $\mathcal{C}_k$. Set

$$C_+(x) := \{P \in C : \overline{\{P\}} \cap \mathcal{C}_k = \{x\}\},$$

where $\overline{\{P\}}$ is the Zariski closure of $\{P\}$ in $\mathcal{C}$. $C_+(x)$ depends on the choice of the model $\mathcal{C}$. By $K(P)$ we mean the field of definition of P. We state the following lemma which plays an essential rule in the way we construct divisors on minimal proper regular models.

Proposition 5.2.1. *Let C/K be a curve of genus $g \geq 1$ with minimal proper regular model C^{min}. Fix a closed point $x \in C_k^{min}$ such that x lies on one and only one irreducible component Γ of C_k^{min}, of multiplicity $r \geq 1$. Then there exists a point $P \in C_+(x)$ such that $[K(P) : K] = r$.*

PROOF: See ([20], Exercise 9.2.11 (c)) or ([19], Lemma 5.1 (b)). □

Now we investigate finite field extensions of K.

Proposition 5.2.2. *If $[L : K] = m$, where $m \in \{2, 3, 4\}$, then $L = K(\sqrt[m]{t})$, and L/K is a Galois tamely ramified extension.*

PROOF: If $a \in L$, we will denote its image in k by $\tilde{a}$.
Since $k = \overline{k}$, it follows that L is a totally ramified extension of K. The fact that $2, 3 \nmid \mathrm{char}(k)$ implies that this extension is tame. Let t_L be a uniformiser for the ring of integers $\mathcal{O}_L$ of L. Then $t = ut_L^m$ for some $u \in \mathcal{O}_L^*$. Hensel's Lemma implies that there is a $v \in \mathcal{O}_L^*$ such that $v^m = u$.

Therefore, $L = K[x]/(x^m - t)$, which is clearly Galois for $m = 2$. For $m = 3, 4$, k has a full set μ_m of m-th roots of unity, and we lift them to $\mathcal{O}_K$ using Hensel's Lemma. Thus L is Galois. □

Let C be a smooth genus one curve given by a minimal genus one equation of degree $n = 2, 3, 4$ over K. Assume moreover that $C(K) \neq \emptyset$. Let E be the Jacobian elliptic curve of C.

Let $P \in C(K)$. Again we fix an isomorphism $\beta : C \to E$ such that $\beta(P) = 0_E$. So we can dispense with C and write E instead. If D is an effective K-rational divisor of degree n on E, then Riemann-Roch theorem implies that there exists a point $Q \in E(K)$ such that $D \sim (n-1).0_E + Q$. Therefore, the equation defining C is an equation for the double cover of the projective line $E \to \mathbb{P}^1_K$ given by the divisor class $[0_E + Q]$ when $n = 2$, or the image of E when it is embedded in $\mathbb{P}^{n-1}_K$ by the divisor class $[(n-1).0_E + Q]$ when $n = 3, 4$.

Consider the smooth genus one curve $E \xrightarrow{[(n-1).0_E+Q]} \mathbb{P}^{n-1}_K$, $n \geq 2$. Let Γ be an irreducible component of E_k^{min}. We set

$$S_\Gamma := \left\{ \begin{array}{c} \text{minimal degree-}n\text{-models } (\mathcal{C}, \alpha) \text{ for } E \xrightarrow{[(n-1).0_E+Q]} \mathbb{P}^{n-1}_K \text{ such that } \Gamma \text{ is} \\ \text{the strict transform of an irreducible component of } \mathcal{C}_k \end{array} \right\}.$$

The following lemma shows that S_Γ is not empty if the multiplicity of Γ is less than n.

Lemma 5.2.3. *Let $n \geq 2$. Let Γ be a multiplicity-m irreducible component of E_k^{min}. If $1 \leq m < n$, then $S_\Gamma \neq \emptyset$.*

PROOF: Let $x \in E_k^{min}$ be a closed point on Γ. Let $P \in E_+(x)$ be a closed point, i.e., P is identified with its Galois orbit $\{P_1, \ldots, P_m\}$, where $K(P) = K(t^{1/m})$. Now set

$$\begin{array}{ll} Q_2 = Q - (n-1).P,\ D = (n-1).\overline{\{P\}} + \overline{\{Q_2\}} & \text{if } m = 1, \\ Q_2 = Q - \sum_{i=1}^{n-1} P_i,\ D = \overline{\{P\}} + \overline{\{Q_2\}} & \text{if } m = n-1, n \geq 3, \\ Q_2 = Q - (P_1 + P_2),\ D = \overline{\{P\}} + \overline{\{Q_2\}} + \overline{\{0_E\}} & \text{if } m = 2, n = 4. \end{array}$$

Now consider the following minimal degree-n-model for $E \xrightarrow{[(n-1).0_E+Q]} \mathbb{P}_K^{n-1}$

$$\mathcal{C}' = \mathrm{Proj}(\bigoplus_{m \geq 0} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD))),$$

see Theorem 4.0.1 and Theorem 4.2.3. We have $x \in D \cap \Gamma$, and hence Γ is an irreducible component of $\mathcal{C}'_k$. Since $D|_E \sim (n-1).0_E + Q$, it follows that there exists an isomorphism $\alpha : \mathcal{C}'_K \cong E$ defined by an element in $\mathcal{G}_n(K)$. Thus $(\mathcal{C}', \alpha) \in S_\Gamma$. □

In what follows we compute the cardinality of S_Γ when the multiplicity of Γ is 1.

Theorem 5.2.4. *Consider the smooth genus one curve $E \xrightarrow{[(n-1).0_E+Q]} \mathbb{P}_K^{n-1}$, $n \geq 3$, with a rational point on it. Let Γ be a multiplicity-1 irreducible component of E_k^{min}. Let $x \in \Gamma$ and $P \in E_+(x)$. Then there is a bijection between the set S_Γ and the set of minimal degree-$(n-1)$-models for $E \xrightarrow{[(n-2).0_E+(Q-P)]} \mathbb{P}_K^{n-2}$.*

To prove Theorem 5.2.4 we have to establish a bijection between the two sets in the statement. Let $(\mathcal{C}, \alpha) \in S_\Gamma$. Let D be a defining divisor of $\mathcal{C}$ as a contraction in E^{min}. The restriction $D|_E$ satisfies $D|_E \sim (n-1).0_E + Q$. Let $P_1 \in \mathrm{Supp}\, D|_E$ be such that $\overline{\{P_1\}} \cap E_k^{min} \in \Gamma$. After applying a transformation in $\mathcal{G}_n(\mathcal{O}_K)$, we can assume that $P_1 = P$.

Now the bijection map is

$$\begin{array}{rcl} \lambda_\Gamma : S_\Gamma & \rightarrow & \{\text{degree-}(n-1)\text{-models for } E \xrightarrow{[(n-2).0_E+(Q-P)]} \mathbb{P}_K^{n-2}\} \\ (\mathcal{C}, \alpha) & \mapsto & \left(\mathrm{Proj}(\bigoplus_{m \geq 0} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD'))),\ \beta \right), \end{array}$$

where $D' = D - \overline{\{P\}}$, and β is obtained from the linear equivalence $D|_E - (P) \sim (n-2).0_E + (Q-P)$. The model on the right is a minimal degree-$(n-1)$-model for $E \xrightarrow{[(n-2).0_E+(Q-P)]} \mathbb{P}_K^{n-2}$, see Theorem 4.0.1 and Theorem 4.2.3.

PROOF OF THEOREM 5.2.4: The map λ_Γ is well defined: Assume that $(\mathcal{C}_i, \alpha_i)$, $i = 1, 2$, are two isomorphic minimal degree-n-models in S_Γ. Remark 5.1.1 shows that the special fibers of both models have the same irreducible components with the same types, therefore the irreducible components of the special fibers of $\lambda_\Gamma((\mathcal{C}_i, \alpha_i))$, $i = 1, 2$, coincide and have the same types. Thus $\lambda_\Gamma((\mathcal{C}_1, \alpha_1))$ and $\lambda_\Gamma((\mathcal{C}_2, \alpha_2))$ are isomorphic as degree-$(n-1)$-models for $E \xrightarrow{[(n-2).0_E+(Q-P)]} \mathbb{P}_K^{n-2}$, see Theorem 5.1.4.

To prove that the map λ_Γ is injective: Assume that the images of $(\mathcal{C}_i, \alpha_i) \in S_\Gamma$, $i = 1, 2$, under λ_Γ are isomorphic degree-$(n-1)$-models, hence the special fibers of $\lambda_\Gamma((\mathcal{C}_i, \alpha_i))$ consist of the same irreducible components with the same types. It follows that the special fibers of both $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same irreducible components with the same types, because they both have the same irreducible components as the special fiber of $\lambda_\Gamma((\mathcal{C}_i, \alpha_i))$ with the degree of Γ being increased by 1. Therefore, Theorem 5.1.4 implies that $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ are isomorphic.

Now we prove that λ_Γ is surjective. Let $(\mathcal{C}, \alpha)$ be a degree-$(n-1)$-model for $E \xrightarrow{[(n-2).0_E+(Q-P)]} \mathbb{P}_K^{n-2}$ with D being a divisor defining $\mathcal{C}$ as a contraction in E^{min}. Consider the model $(\mathcal{C}', \alpha') \in S_\Gamma$ defined by

$$\mathrm{Proj}(\bigoplus_{m \geq 0} H^0(E^{min}, \mathcal{O}_{E^{min}}(m(D + \overline{\{P\}})))),$$

and α' is obtained from the linear equivalence $D|_E + (P) \sim (n-1).0_E + (Q)$. The model $\mathcal{C}'$ is defined by a minimal genus one equation of degree n, see Theorem 4.2.3. The surjectivity follows by noting that $\lambda_\Gamma((\mathcal{C}', \alpha')) = (\mathcal{C}, \alpha)$. □

Chapter 6

Computing in E^{min}

In this chapter K will be a perfect Henselian discrete valuation field with algebraic closure $\overline{K}$, ring of integers $\mathcal{O}_K$, normalised valuation ν, and a uniformiser t. We assume that the residue field k is algebraically closed with $\operatorname{char} k \neq 2, 3$.

Let E be an elliptic curve over K, with minimal proper regular model E^{min}. Let $E^0(K)$ be the group of rational points of E with non-singular reduction. In this chapter we define a map $\delta_m : \Phi_K^m(E) \to \Phi_K(E)$, where $\Phi_K^m(E)$ is the set of multiplicity-m irreducible components of E_k^{min}, and $\Phi_K(E) := \Phi_K^1(E)$ is the group of components $E(K)/E^0(K)$.

Since k is algebraically closed, it follows that the reduction of E is always split.

6.1 The components group

In this section we will study the components group $\Phi_K(E) = E(K)/E^0(K)$. We start by describing this group.

Proposition 6.1.1 ([28], Chapter IV, Corollary 9.2)**.** *Let E be an elliptic curve over K. Let $j(E)$ be the j-invariant of E. Then the group $E(K)/E^0(K)$ is finite. More precisely, if E has multiplicative reduction, then $E(K)/E^0(K)$ is a cyclic group of order $-\nu(j(E))$; otherwise, $E(K)/E^0(K)$ has order $1, 2, 3,$ or 4.*

Assume E has reduction of type $\mathrm{I}_n, n \geq 0$. Then E_k^{min} is a non-singular smooth curve of genus one when $n = 0$. E_k^{min} is a rational curve with a node when $n = 1$. E_k^{min} consists of n multiplicity-1 irreducible components arranged in the shape of an n-gon when $n \geq 2$.

We will denote the extension of the normalised valuation ν on K to $\overline{K}$ by $\nu_{\overline{K}} : \overline{K} \to \mathbb{Q} \cup \{\infty\}$. Let $p = \operatorname{char} k$. Denote by $|*| = 1/p^{\nu_{\overline{K}}(*)}$ an associated absolute value. Tate's uniformisation of E, see ([28], Chapter V, §3), implies that there exists a $q \in K^*$ with $\nu(q) = \nu(\Delta) = n$ such that

$$\overline{K}^*/q^{\mathbb{Z}} \cong E(\overline{K}).$$

For $z \in \overline{K}^*$, we denote by $\tilde{z}$ the image of z in $E(\overline{K})$. For $z \in \overline{K}^*$, there exists an integer i such that $|t|^{i+1} < |z| \leq |t|^i$.

Consider the reduction map $r : E(\overline{K}) \to E(k)$. Any isomorphism $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \Phi_K(E)$ enables us to number the irreducible components Γ_i's of E_k^{min}, with $\bar{i} \in \mathbb{Z}/n\mathbb{Z}$ where $\bar{i}$ denotes the class of the integer i in $\mathbb{Z}/n\mathbb{Z}$. There exists such a numbering such that if $|z| = |t|^i$, then $r(\tilde{z})$ belongs to the i-th component Γ_i, and if $|t|^{i+1} < |z| < |t|^i$, then $r(\tilde{z})$ is an intersection point of the irreducible components Γ_i and Γ_{i+1}. This intersection point is unique when $n \geq 3$. For the above discussion see ([21], p. 503).

Assume that E has additive reduction. We fix an isomorphism $\alpha : \Phi_K(E) \cong \mathbb{Z}/n\mathbb{Z}, n = 1, 2, 3, 4$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ when E has reduction of type I_{2m}^*, $m \geq 0$. Let Λ be a multiplicity-1 irreducible component of E_k^{min}. By Hensel's Lemma we can lift any closed point x of Λ which lies on no other component to a rational point $P \in E(K)$. Now consider the image $\bar{i}$ of P under α. We give the component Λ the number i, and denote it by Γ_i.

The map $\delta_1 : \Phi_K^1(E) \to \Phi_K(E)$ will be viewed as the identification of multiplicity-1 components with their images in $\mathbb{Z}/n\mathbb{Z}$ when the reduction is of type I_n, and with their images under the isomorphism α defined above when the reduction is additive. In other words, $\delta_1(\Gamma_i) = \bar{i}$.

We note that if E has one of the reduction types $\mathrm{I}_n, n \geq 0, \mathrm{II}, \mathrm{III}$, or IV, then E_k^{min} consists only of multiplicity-1 components, hence $\Phi_K^m(E) = \emptyset$ when $m \geq 2$ and we do not need to define δ_m for $m \geq 2$.

6.2 The set $\Phi_K^m(E)$, $m \geq 2$

In this section we assume that E has one of the reduction types $\mathrm{I}_m^*, m \geq 0, \mathrm{IV}^*, \mathrm{III}^*$, or II^*. Then the special fiber of the minimal proper regular model E^{min} contains irreducible components of multiplicities greater than one. In other words, there exists an integer $m \geq 2$ such that $\Phi_K^m(E) \neq \emptyset$.

We define the map $\delta_m : \Phi_K^m(E) \to \Phi_K(E)$, $m \geq 2$, as follows: Let x be a k-point of $\Theta \in \Phi_K^m(E)$. Recall that k is algebraically closed and hence x is a closed point. Assume moreover that x lies on no other component. Let $P \in E(\overline{K})$ be a point which reduces to x such that $[K(P) : K] = m$, see Proposition 5.2.1. Let σ be a generator of $\mathrm{Gal}(K(P)/K)$. The sum of the Galois orbit $\mathrm{sum}\, P := P + \ldots + P^{\sigma^{m-1}}$ of P is a point in $E(K)$. The image $\delta_m(\Theta)$ is the image of sum P in $\Phi_K(E) = E(K)/E^0(K)$. It will be clear from the description of the map δ_m that $\delta_m(\Theta)$ does not depend on x nor on P.

Since $K(P)/K$ is a totally tamely ramified extension, see Proposition 5.2.2, the Galois group $\mathrm{Gal}(K(P)/K)$ is the inertia group of $K(P)/K$. In other words, $\mathrm{Gal}(K(P)/K)$ fixes every irreducible component of E_k^{min}.

In what follows we are going to follow two strategies to determine the image of each $\Theta \in \Phi_K^m(E)$ under δ_m. When the reduction type is I_n^*, we use Tate's algorithm to write down explicit equations for the components in $\Phi_K^2(E)$. For reduction types IV^*, III^* and II^*, the defining equations of the components in $\Phi_K^m(E)$, $m \geq 2$, are complicated. Therefore, we use the projection formula to exploit the symmetry of the graphs associated to E_k^{min}.

6.2.1 Reduction type I_n^*, $n \geq 0$

Assume that E/K has reduction of type I_n^*, $n \geq 0$. The special fiber E_k^{min} contains a sequence of multiplicity-2 components and no components of higher multiplicities. Therefore, $\Phi_K^m(E) = \emptyset$ when $m \geq 3$. The strategy we will follow to compute δ_2 in this case is as follows: We desingularise a minimal Weierstrass model for E using a sequence of blow-ups, then we determine conditions for points in E defined over $K(\sqrt{t})$ to lie on one of the produced multiplicity-2 irreducible components, and use that to compute the sums of the Galois orbits of these points.

We will use the data given by the proof of Tate's algorithm to write the defining equations of $\Theta \in \Phi_K^2(E)$, see ([28], Chapter IV, §9). We start with a homogenised minimal genus one equation of degree 1, i.e., a minimal Weierstrass equation of the form

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,\ a_i \in \mathcal{O}_K,$$

for E/K. We will write $a_{i,r}$ for $t^{-r}a_i$, and x_r, y_r for $t^{-r}x, t^{-r}y$ respectively.

The proof of Tate's algorithm shows that if E has additive reduction of one of the types I_n^*, $n \geq 0$, IV^*, III^* or II^*, then we can assume $t \mid a_1, a_2, t^2 \mid a_3, a_4$, and $t^3 \mid a_6$. Now blowing-up the singularity $t = x = y = 0$, by making the substitutions $x = tx_1$ and $y = ty_1$ we will have

$$V : y_1^2z + ta_{1,1}x_1y_1z + ta_{3,2}y_1z^2 = tx_1^3 + ta_{2,1}x_1^2z + ta_{4,2}x_1z^2 + ta_{6,3}z^3,$$

and its special fiber $y_1^2z = 0$ consists of the double line $y_1^2 = 0$ and the multiplicity-1 line $z = 0$. We next blow-up the line $t = y_1 = 0$. Putting $z = 1$ and recalling the definitions of x_i and y_i above, we obtain

$$V_0 : ty_2^2 + ta_{1,1}x_1y_2 + ta_{3,2}y_2 = x_1^3 + a_{2,1}x_1^2 + a_{4,2}x_1 + a_{6,3},$$

and the special fiber of the total blow-up consists of

$$\tilde{V} : y_1^2 z = 0,\ \tilde{V}_0 : x_1^3 + \tilde{a}_{2,1}x_1^2 + \tilde{a}_{4,2}x_1 + \tilde{a}_{6,3} = 0.$$

For type I_0^*, the special fiber $\tilde{V}_0$ consists of three distinct lines. Hence E_k^{min} consists of the double line $y_1^2 = 0$ together with four distinct lines of multiplicity 1 intersecting it.

Now we assume that $h(x) = x^3 + \tilde{a}_{2,1}x^2 + \tilde{a}_{4,2}x + \tilde{a}_{6,3}$ has one double root. We may assume that this root is $x = 0$, which implies that $t^2 \nmid a_2, t^3 \mid a_4$, and $t^4 \mid a_6$. Now we have

$$\tilde{V}_0 : x_1^2(x_1 + \tilde{a}_{2,1}) = 0,$$

so we blow up the double line $t = x_1 = 0$. Therefore, we make the substitution $x_1 = tx_2$ and divide by t to get

$$V_1 : y_2^2 + ta_{1,1}x_2y_2 + a_{3,2}y_2 = t^2x_2^3 + ta_{2,1}x_2^2 + ta_{4,3}x_2 + a_{6,4}.$$

The total special fiber consists now of the simple lines $z = 0$ and $x_1 + \tilde{a}_{2,1} = 0$, the double lines $y_1^2 = 0$ and $x_1^2 = 0$, and the special fiber of V_1 which is given by

$$\tilde{V}_1 : y_2^2 + \tilde{a}_{3,2}y_2 - \tilde{a}_{6,4} = 0.$$

If this quadratic equation has distinct roots in k, then $\tilde{V}_1$ consists of two distinct simple lines, and the reduction of E is of type I_1^*. Otherwise, it has a double root and after a translation on y_2 we can take this double root to $y_2 = 0$, i.e., $t^3 \mid a_3$ and $t^5 \mid a_6$, and the special fiber $\tilde{V}_1$ of V_1 is the double line $y_2^2 = 0$. We blow-up V_1 along this double line via the substitution $y_2 = ty_3$ and divide by t to get

$$V_2 : ty_3^2 + ta_{1,1}x_2y_3 + ta_{3,3}y_3 = tx_2^3 + a_{2,1}x_2^2 + a_{4,3}x_2 + a_{6,5}.$$

The special fiber is

$$\tilde{V}_2 = \tilde{a}_{2,1}x_2^2 + \tilde{a}_{4,3}x_2 + \tilde{a}_{6,5} = 0.$$

If this quadratic equation has distinct roots, then E has reduction type I_2^*. Otherwise, we continue the blowing-up process which will terminate eventually.

We note that at each step we have a new scheme V_l of the form

$$\begin{aligned} &y_u^2 + ta_{1,1}x_uy_u + a_{3,u}y_u = t^ux_u^3 + ta_{2,1}x_u^2 + ta_{4,u+1}x_u + a_{6,2u} && \text{if } l = 2u-3 \text{ is odd,}\\ &ty_{u+1}^2 + ta_{1,1}x_uy_{u+1} + ta_{3,u+1}y_{u+1} = t^{u-1}x_u^3 + a_{2,1}x_u^2 + a_{4,u+1}x_u + a_{6,2u+1} && \text{if } l = 2u-2 \text{ is even.}\end{aligned}$$

The special fiber of V_l is given by

$$\tilde{V}_l : \begin{cases} y_u^2 + \tilde{a}_{3,u}y_u - \tilde{a}_{6,2u} = 0 & \text{if } l = 2u-3 \text{ is odd,}\\ \tilde{a}_{2,1}x_u^2 + \tilde{a}_{4,u+1}x_u + \tilde{a}_{6,2u+1} = 0 & \text{if } l = 2u-2 \text{ is even.}\end{cases}$$

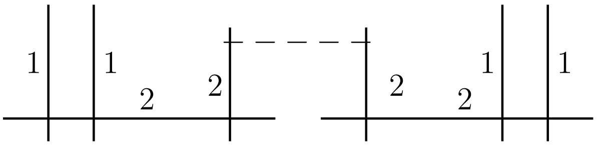
After each two blowing-ups the coefficients a_3 and a_4 are forced to be divisible by an additional power of t. The special fiber $\tilde{V}_l$ consists of two distinct lines precisely when $l = n = \nu(\Delta) - 6$. Thus if E has reduction of type $\mathrm{I}_n^*, n \geq 0$, we can assume that E has coefficients with valuations as in the following table.

Table 6.1:

	a_1	a_2	a_3	a_4	a_6
$n = 0$	≥ 1	≥ 1	≥ 2	≥ 2	≥ 3
$n \geq 2$ even	≥ 1	$= 1$	$\geq \frac{n}{2} + 2$	$= \frac{n}{2} + 2$	$\geq n + 3$
n odd	≥ 1	$= 1$	$= \frac{n-1}{2} + 2$	$\geq \frac{n-1}{2} + 2$	$\geq n + 3$

The inequalities in the second, third, and fourth line relate to the valuation of the coefficient in the first line.

The special fiber E_k^{min} is as in the following figure. The numbers on the components refer to the multiplicities.



The number of multiplicity-2 components in E_k^{min} is $n + 1$. Let $L = K(\sqrt{t})$ be the unique quadratic tame Galois extension of K. A point lying above a k-point on $\tilde{V}_l$, where $l = 2u - 2$ is even, and on no other component is a point in $E(L)$ of the form $(\alpha t^{u+1} + \beta t^{u+1/2}, y)$, where $y \in L$, $t^{u+1} \mid y$ and $\alpha, \beta \in \mathcal{O}_K$ with $\nu(\alpha) \geq \nu(\beta) = 0$. We have $\beta \in \mathcal{O}_K^*$, since otherwise this point would reduce to a point on $\tilde{V}_{l+1}$.

A point lying above a k-point on $\tilde{V}_l$, where $l = 2u - 3$ is odd, and on no other component is a point in $E(L)$ of the form $(x, \alpha t^{u+1} + \beta t^{u+1/2})$, where $x \in L$, $t^u \mid x$ and $\alpha, \beta \in \mathcal{O}_K$ with $\nu(\alpha) \geq \nu(\beta) = 0$. We have $\beta \in \mathcal{O}_K^*$, since otherwise this point would reduce to a point on $\tilde{V}_{l+1}$.

We recall the addition formula on elliptic curves. Let $P_1, P_2 \in E(\overline{K})$. If $P_1 \neq \pm P_2$, then

$$x(P_1+P_2) = \lambda^2+a_1\lambda-a_2-x(P_1)-x(P_2), \text{ and, } y(P_1+P_2) = -(\lambda+a_1)x(P_1+P_2)-\mu-a_3,$$

where

$$\lambda = \frac{y(P_2) - y(P_1)}{x(P_2) - x(P_1)},\ \mu = \frac{y(P_1)x(P_2) - y(P_2)x(P_1)}{x(P_2) - x(P_1)}.$$

Lemma 6.2.1. *Assume E has one of the reduction types I_n^*, $n \geq 0$, IV^*, III^* or II^*. Let $L = K(\sqrt{t})$ with $\mathrm{Gal}(L/K) = \langle\sigma\rangle$. Let $P \in E(L)$ be a point which lies above the the multiplicity-2 component $\Theta_0 : y_1^2 = 0$. Then $P + P^\sigma \in E^0(K)$. In particular, $\delta_2(\Theta_0) = \bar{0}$.*

Proof: We can assume that $P = (x, \alpha t^2 + \beta t^{3/2})$, where $x \in L, t \mid x$ and $\alpha, \beta \in \mathcal{O}_K$, with $\nu(\alpha) \geq \nu(\beta) = 0$. If $P^\sigma = -P$, then $P + P^\sigma = 0 \in E^0(K)$ and we are done. Since $t \mid x(P)$, we assume $x(P) = \alpha' t + \beta' t^{3/2}$, where $\alpha', \beta' \in \mathcal{O}_K$. Therefore, we have in the addition formula given above that

$$\lambda := \frac{y(P) - y(P^\sigma)}{x(P) - x(P^\sigma)} = \frac{\beta}{\beta'} \in K.$$

If $\nu(\beta') = 0$, then $\nu(x(P + P^\sigma)) = 0$ because $t \mid a_1, a_2$, see Table 6.1. Hence $P + P^\sigma$ is not a singular point, i.e., $P + P^\sigma \in E^0(K)$. If $\nu(\beta') > 0$, then we have $\nu(x(P + P^\sigma)) < 0$, in particular $P + P^\sigma \in E^0(K)$, and we are done. □

Now we state our main result of this subsection in the following proposition.

Proposition 6.2.2. *Assume that E/K has reduction type I_n^*, $n \geq 0$. Let $L = K(\sqrt{t})$ with $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.*

(i) The multiplicity-1 component Γ given by $x_1 + \tilde{a}_{2,1} = 0$ is of order 2 in $\Phi_K(E)$.

(ii) Let $P \in E(L)$ be a point lying above the double line $y_1^2 = 0$. Then $P + P^\sigma \in E^0(K)$.

(iii) Let $P \in E(L)$ be a point lying above $\tilde{V}_l$ where $l = 2u - 2$ is even. Then $P + P^\sigma$ reduces to a point on Γ.

(iv) Let $P \in E(L)$ be a point lying above $\tilde{V}_l$ where $l = 2u - 3$ is odd. Then $P + P^\sigma \in E^0(K)$.

Proof: We note first that the identity component, i.e., points in $E^0(K)$, is given by the linear equation $z = 0$.

(i) If $P \in E(K)$, then $x(-P) = x(P)$. If moreover P lies above $\Gamma : x_1 + \tilde{a}_{2,1} = 0$, then $-P$ lies above Γ as well. It follows that the inverse of Γ when considered as an element of $\Phi_K(E)$ is itself, i.e., Γ has order 2 as an element in $\Phi_K(E)$.

(ii) This is Lemma 6.2.1.

(iii) We can assume that $P = (\alpha t^{u+1} + \beta t^{u+1/2}, y)$, where $y \in L$, $t^{u+1} \mid y$ and $\alpha, \beta \in \mathcal{O}_K$ with $\nu(\alpha) \geq \nu(\beta) = 0$. Therefore, we have $\nu(\lambda) > 0$ where $\lambda := \frac{y(P) - y(P^\sigma)}{x(P) - x(P^\sigma)}$.

Following the addition formula we have $x(P+P^\sigma) = \lambda^2 + a_1\lambda - a_2 - x(P) - x(P^\sigma)$, dividing by t and using that $t \mid a_1, a_2$, see Table 6.1, we get that $x_1(P+P^\sigma) = -\tilde{a}_{2,1} \mod t$, and we are done.

(iv) We can assume that $P = (x, \alpha t^{u+1} + \beta t^{u+1/2})$, where $x \in L, t^u \mid x$ and $\alpha, \beta \in \mathcal{O}_K$, with $\nu(\alpha) \geq \nu(\beta) = 0$. If $P^\sigma = -P$, then $P + P^\sigma = 0 \in E^0(K)$ and we are done. Thus we assume $x(P) = \alpha' t^u + \beta' t^{u+1/2}$, where $\alpha', \beta' \in K$ with $\nu(\alpha') \geq \nu(\beta') \geq 0$. Therefore, we have in the addition formula given above that $\lambda = \frac{\beta}{\beta'} \in K$. If $\nu(\beta') = 0$, then $\nu(x(P+P^\sigma)) = 0$, hence $P + P^\sigma$ is not a singular point, i.e., $P + P^\sigma \in E^0(K)$. If $\nu(\beta') > 0$, then we have $\nu(x(P+P^\sigma)) < 0$, in particular $P + P^\sigma \in E^0(K)$. □

In Proposition 6.2.2 we note that since $\Gamma : x_1 + \tilde{a}_{2,1} = 0$ has order 2, we have that $\delta_1(\Gamma) = \bar{2} \in \Phi_K(E) \cong \mathbb{Z}/4\mathbb{Z}$, when n is odd. When n is even, we know that $\alpha : \Phi_K(E) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, therefore every non-identity irreducible component has order 2. From now on, we will fix α such that $\delta_1(\Gamma) = (\bar{1}, \bar{1})$. We obtain the following direct consequence.

Corollary 6.2.3. *Assume that E/K has reduction type I_n^*, $n \geq 0$. Let*

$$\Phi_K^2(E) = \{\tilde{V}_{-1} : y_1^2 = 0, \tilde{V}_0, \ldots, \tilde{V}_{n-1}\}$$

be as above. Then $\delta_2 : \Phi_K^2(E) \to \Phi_K(E)$ is determined according to the following.

$$\delta_2(\Theta) = \begin{cases} \bar{0} & \text{if } \Theta = \tilde{V}_l, \text{ where } l \text{ is odd and } n \text{ is odd,} \\ \bar{2} & \text{if } \Theta = \tilde{V}_l, \text{ where } l \text{ is even and } n \text{ is odd,} \\ (\bar{0}, \bar{0}) & \text{if } \Theta = \tilde{V}_l, \text{ where } l \text{ is odd and } n \text{ is even,} \\ (\bar{1}, \bar{1}) & \text{if } \Theta = \tilde{V}_l, \text{ where } l \text{ is even and } n \text{ is even.} \end{cases}$$

While treating elliptic curves with reduction type III^*, see below, we will need more information on the reduction type I_0^*. If E/K is an elliptic curve given by a minimal Weierstrass equation with reduction type I_0^*, then the special fiber of the minimal proper regular model of E consists of the single line $z = 0$, a double line $y_1^2 = 0$, and the three distinct lines of

$$\tilde{V}_0 : x_1^3 + \tilde{a}_{2,1}x_1^2 + \tilde{a}_{4,2}x_1 + \tilde{a}_{6,3} = 0.$$

Using Hensel's Lemma we can lift the simple zeros of this cubic polynomial to α_1, α_2, and α_3 in $\mathcal{O}_K$ such that

$$x^3 + a_2x^2 + a_4x + a_6 = (x - t\alpha_1)(x - t\alpha_2)(x - t\alpha_3).$$

Let $P_i = (t\alpha_i, 0)$. We conclude that the reduction map $\{0, P_1, P_2, P_3\} \to \Phi_K(E)$ is surjective as each of these points lies on a different multiplicity-1 component. Note that these points are the elements of $E(K)[2]$.

6.2.2 Reduction types IV^*, III^* and II^*

Let E/K be an elliptic curve with either reduction types IV^* or III^*. We start by investigating the new reduction type of E over Galois tame extensions.

Lemma 6.2.4. *Let E/K be an elliptic curve. Let $L_m = K(t_m)$, where $t_m = t^{1/m}$, $m \in \{2,3,4\}$. The following statements are true.*

(i) If E/K has reduction type IV^*, then E/L_3 has good reduction.

(ii) Assume that E/K has reduction type III^*. Then E/L_2 has reduction type I_0^*, E/L_3 has reduction type III, and E/L_4 has good reduction.

Proof: Let ν_{L_m} denote the normalised discrete valuation on L_m.

(i) We recall from ([28], Chapter IV, §9) that if E has reduction type IV^*, then $\nu(c_4) \geq 3$, $\nu(c_6) = 4$, and $\nu(\Delta) = 8$. Therefore, $\nu_{L_3}(c_4) \geq 9$, $\nu_{L_3}(c_6) = 12$, and $\nu_{L_3}(\Delta) = 24$. Since $\operatorname{char} K \neq 2, 3$, a Weierstrass equation for E/L_3 with good reduction is now given by

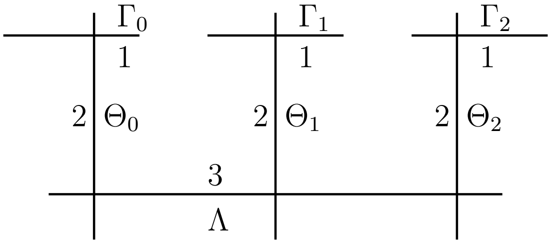
$$y^2 = x^3 - 27t_3^{-8}c_4x - 54t_3^{-12}c_6.$$

(ii) Recall from [28] that if E has reduction type III^*, then $\nu(c_4) = 3$, $\nu(c_6) \geq 5$, and $\nu(\Delta) = 9$. Therefore, $\nu_{L_m}(c_4) = 3m$, $\nu_{L_m}(c_6) \geq 5m$, and $\nu_{L_m}(\Delta) = 9m$. The following Weierstrass equation for E/L_m has reduction type I_0^* when $m = 2$, reduction type III when $m = 3$, and good reduction when $m = 4$

$$y^2 = x^3 - 27t_m^{-4(m-1)}c_4x - 54t_m^{-6(m-1)}c_6.$$

□

Now we assume that E/K has additive reduction of type IV^*. The minimal proper regular model E^{min} has special fiber as in the following figure. Again the numbers on the components refer to the multiplicities.



According to the proof of Tate's algorithm, the blowing-up process will yield that the multiplicity-1 identity component Γ_0 is given by the equation $z = 0$, and the multiplicity-2 component Θ_0 is given by the equation $y_1^2 = 0$. The multiplicity-3 component Λ has equation $x_1^3 = 0$, see ([28], Chapter IV, §9). The multiplicity-1 component Γ_i will correspond as usual to $\bar{i} \in \Phi_K(E)$.

Proposition 6.2.5. *Assume that E/K has reduction type* IV*. *Let $L_m = K(t_m)$, where $t_m = t^{1/m}$, $m \in \{2, 3\}$. Let* $\mathrm{Gal}(L_m/K) = \langle \sigma_m \rangle$.

*(i) Let $P \in E(L_2)$ lie above a multiplicity-*2 *component Θ_i, $i \in \{0, 1, 2\}$. The following table relates the component Θ_i to the multiplicity-*1 *component above which $P + P^{\sigma_2}$ lies, and the image $\delta_2(\Theta_i)$.*

$\tilde{P} \in$	Θ_0	Θ_1	Θ_2
$(P + P^{\sigma_2})^\sim \in$	Γ_0	Γ_2	Γ_1
δ_2	$\bar{0}$	$\bar{2}$	$\bar{1}$

(ii) Let $P \in E(L_3)$ be a point lying above Λ. Then we have $\sum_{i=0}^{2} P^{\sigma_3^i} \in E^0(K)$. In particular, $\delta_3(\Lambda) = \bar{0}$.

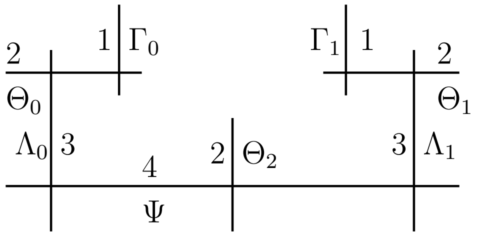
Proof: (*i*) If $P \in E(L_2)$ lies above $\Theta_0 : y_1^2 = 0$, then $P + P^{\sigma_2} \in E^0(K)$, see Lemma 6.2.1.

Let $P \in E(L_2)$ be a point lying above Θ_1 and above no other component. Now let $Q \in E(K)$ be a point lying above Γ_2. Consider the translation-by-Q automorphism $\tau_Q : E \to E$. This K-automorphism extends to give an $\mathcal{O}_K$-automorphism $\tau'_Q : E^{min} \to E^{min}$, see e.g. ([28], Chapter IV, Proposition 4.6). Moreover, $\tau'^*_Q(\Gamma_1) = \Gamma_0$, and the projection formula implies that $\tau'^*_Q(\Gamma_1).\tau'^*_Q(\Theta_1) = \Gamma_1.\Theta_1$, see ([20], Theorem 9.2.12), therefore $\tau'^*_Q(\Theta_1) = \Theta_0$. Therefore, $\tau_Q(P)$ lies above Θ_0, hence the first part of the proof shows that $\tau_Q(P) + \tau_Q(P)^{\sigma_2} \in E^0(K)$, but $\tau_Q(P)^{\sigma_2} = P^{\sigma_2} + Q$. Whence $P + P^{\sigma_2} + 2Q \in E^0(K)$, in other words $P + P^{\sigma_2} \in Q + E^0(K)$, i.e., $P + P^{\sigma_2}$ lies above Γ_2.

If $P \in E(L_2)$ lies above Θ_2 and above no other component, then we choose $Q \in E(K)$ to lie above Γ_1 and we follow the same argument to get $P + P^{\sigma_2} \in Q + E^0(K)$, i.e., $P + P^{\sigma_2}$ lies above Γ_1.

(*ii*) Since E/L_3 has good reduction, see Lemma 6.2.4, it follows that $E(L_3) = E_0(L_3)$. Moreover, since $\bar{k} = k$, and $\mathrm{char}\, k \neq 3$, the theory of formal groups implies that $E_0(L_3)/3E_0(L_3) = 0$, see ([27], Chapter VII, Exercise 7.8). This means that the multiplication-by-3 map is surjective on $E(L_3)$. Therefore, $P = 3Q$, for some $Q \in E(L_3)$, and hence $\sum_{i=0}^{2} P^{\sigma_3^i} = 3\sum_{i=0}^{2} Q^{\sigma_3^i} \in 3E(K)$. Hence $\sum_{i=0}^{2} P^{\sigma_3^i} \in E^0(K)$ because $\Phi_K(E) \cong \mathbb{Z}/3\mathbb{Z}$. □

Now assume that E/K has reduction type III*. The special fiber of the minimal proper regular model is as follows.



The multiplicity-1 identity component Γ_0 is given by $z = 0$, the multiplicity-2 component Θ_0 is given by $y_1^2 = 0$, and the multiplicity-3 component Λ_0 is given by $x_1^3 = 0$, see ([28], Chapter IV, §9).

Proposition 6.2.6. *Assume that E/K has reduction type* III*. *Let $L_m = K(t_m)$, where $t_m = t^{1/m}$, $m \in \{2, 3, 4\}$. Let $\mathrm{Gal}(L_m/K) = \langle\sigma_m\rangle$.*

- *(i) Let $P \in E(L_2)$ lie above a multiplicity-2 component Θ_i, $i \in \{0, 1, 2\}$. Then $P + P^{\sigma_2} \in E^0(K)$ when $i = 0, 1$, and $P + P^{\sigma_2} \notin E^0(K)$ when $i = 2$.*
- *(ii) Let $P \in E(L_3)$ be a point lying above Λ_i, $i \in \{0, 1\}$. Then we have $\sum_{l=0}^{2} P^{\sigma_3^l} \in E^0(K)$ when $i = 0$, and $\sum_{l=0}^{2} P^{\sigma_3^l} \notin E^0(K)$ when $i = 1$.*
- *(iii) Let $P \in E(L_4)$ be a point lying above Ψ. Then we have $\sum_{l=0}^{3} P^{\sigma_4^l} \in E^0(K)$.*

Proof: Let $Q \in E(K)$ be a point lying above Γ_1. Let $\tau'_Q : E^{min} \to E^{min}$ be the extension of the translation-by-Q automorphism τ_Q.

(*i*) Let $P \in E(L_2)$. If P lies above $\Theta_0 : y_1^2 = 0$, then $P + P^{\sigma_2} \in E^0(K)$, see Lemma 6.2.1.

So let $P \in E(L_2)$ lie above Θ_1. We have $\tau'^*_Q(\Gamma_1) = \Gamma_0$, and $\tau'^*_Q(\Gamma_1).\tau'^*_Q(\Theta_1) = \Gamma_1.\Theta_1$, so $\tau'^*_Q(\Theta_1) = \Theta_0$. Therefore, $\tau_Q(P) + \tau_Q(P)^{\sigma_2} \in E^0(K)$, i.e., $P + P^{\sigma_2} + 2Q \in E^0(K)$. In other words, $P + P^{\sigma_2} \in E^0(K)$.

Now let $P \in E(L_2)$ lie above Θ_2. By virtue of Lemma 6.2.4, the reduction type of E/L_2 is I_0^*. We showed in the last paragraph of the previous subsection that E/L_2 has a minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathcal{O}_{L_2},$$

where $x^3 + a_2x^2 + a_4x + a_6 = (x - t\alpha_1)(x - t\alpha_2)(x - t\alpha_3),\ \alpha_i \in \mathcal{O}_{L_2}$. Now σ_2 fixes one of the α_i's and swaps the other two because $E[2] \not\subset E(K)$, see ([28], p. 390), so we can assume without loss of generality that $\alpha_1 \in \mathcal{O}_K$ and $\alpha_2, \alpha_3 \in \mathcal{O}_{L_2} \setminus \mathcal{O}_K$, moreover we know $P_1 = (t\alpha_1, 0) \notin E^0(K)$.

Since the reduction map

$$\{0, P_i = (t\alpha_i, 0) | i = 1, 2, 3\} \to \Phi_{L_2}(E)$$

is surjective, it follows that P_1 lies above a non-identity multiplicity-1 component Γ' of $\mathcal{E}_k$, where $\mathcal{E}$ is the minimal proper regular model of E/L_2. Moreover, σ_2 fixes the components $\Gamma_{(0,0)}$ and Γ' of $\mathcal{E}$ and swaps the other two multiplicity-1 irreducible components $\Gamma_*,\ \Gamma_*^{\sigma_2}$. Note that $\Gamma_{(0,0)}$ and Γ' lie above Γ_0 and Γ_1 respectively.

Since $[L_2 : K]$ divides the multiplicities of Θ_2 and Ψ, it is a known fact that Γ_* and $\Gamma_*^{\sigma_2}$ are lying above Θ_2 under the following morphism

$$\widetilde{N} \to N := \mathrm{Norm}(E^{min} \times_{\mathcal{O}_K} \mathcal{O}_{L_2}) \to E^{min},$$

where N is the normalisation of $E^{min} \times_{\mathcal{O}_K} \mathcal{O}_{L_2}$, and $\widetilde{N}$ is the minimal desingularisation of N, see for example ([20], §10.4) and ([22], pp. 10-11). The model $\mathcal{E}$ is obtained from $\widetilde{N}$ by contracting the exceptional divisors, see Definition 2.2.12.

Therefore, if P lies above Θ_2 in E^{min}, then it lies on either Γ_* or $\Gamma_*^{\sigma_2}$ in $\mathcal{E}$. Since $\Phi_{L_2}(E) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we have $P + P^{\sigma_2}$ lies above Γ' in $\mathcal{E}_k$, and hence it lies above Γ_1 in E_k^{min}.

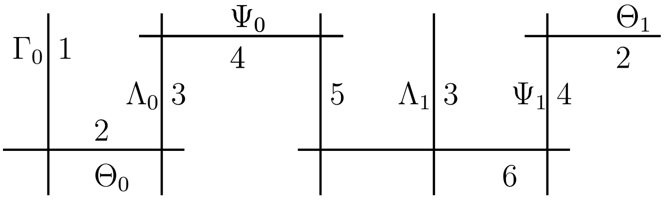
(ii) If $P \in E(L_3)$ lies above the multiplicity-3 component $\Lambda_0 : x_1^3 = 0$, then $\sum_{l=0}^{2} P^{\sigma_3^l}$ is a non-singular point. This follows from Proposition 6.2.5 (ii).

Let $P \in E(L_3)$ be a point lying above Λ_1. Since $\tau_Q'^*(\Theta_1) = \Theta_0$, see (i), and $\tau_Q'^*(\Theta_1).\tau_Q'^*(\Lambda_1) = \Theta_1.\Lambda_1$, therefore $\tau_Q'^*(\Lambda_1) = \Lambda_0$. Thus $\sum_{l=0}^{2} \tau_Q(P)^{\sigma_3^l} \in E^0(K)$. In other words, $\sum_{l=0}^{2} P^{\sigma_3^l} + 3Q \in E^0(K)$, which means $\sum_{l=0}^{2} P^{\sigma_3^l} \notin E^0(K)$.

(iii) Lemma 6.2.4 shows that E/L_4 has good reduction. It follows that $E(L_4) = E_0(L_4)$. Moreover, since $\overline{k} = k$, and $\mathrm{char}\, k \neq 2$, the theory of formal groups implies that $E_0(L_4)/4E_0(L_4) = 0$, see ([27], Chapter VII, Exercise 7.8). Therefore, $P = 4Q$, for some $Q \in E(L_4)$ and hence $\sum_{l=0}^{3} P^{\sigma_4^l} = 4\sum_{l=0}^{3} Q^{\sigma_4^l} \in 4E(K)$, and we are done because $\Phi_K(E) \cong \mathbb{Z}/2\mathbb{Z}$. □

Remark 6.2.7. When E/K has reduction type III*, the above Proposition implies that $\delta_2(\Theta_i) = \bar{0}$ when $i \in \{0, 1\}$, and $\delta_2(\Theta_2) = \bar{1}$. Moreover, $\delta_3(\Lambda_i) = \bar{i},\ i \in \{0, 1\}$, and $\delta_4(\Psi) = \bar{0}$.

Now assume that E/K has reduction type II*. The special fiber of the minimal proper regular model is as follows.



Proposition 6.2.8. *Assume that E/K has reduction type* II*. *Let $L_m = K(t_m)$, where $t_m = t^{1/m}$. Let $\mathrm{Gal}(L_m/K) = \langle \sigma_m \rangle$. Let $P \in E(L_m)$ lie above a component of multiplicity m. Then $\sum_{i=0}^{m-1} P^{\sigma_m^i} \in E^0(K)$. In particular, $\delta_m(\Gamma) = \bar{0}$, for every multiplicity-m irreducible component Γ of E_k^{min}, $m \in \{1, 2, 3, 4\}$.*

Proof: That is straightforward because $\sum_{i=0}^{m-1} P^{\sigma_m^i} \in E(K)$, and $E(K) = E^0(K)$ for reduction type II*. □

We conclude this chapter by stating the following direct corollary.

Corollary 6.2.9. *Let E/K be an elliptic curve with minimal proper regular model E^{min}. Let L_m, σ_m and δ_m, where $m \in \{1, 2, 3, 4\}$, be as above. Let $Q \in E(K)$. Assume that there exists a multiplicity-m irreducible component Θ in E_k^{min} such that $\delta_m(\Theta) = \psi_E(Q)$. Then there exists a point $P \in E(L_m)$ lying above Θ such that $Q = \sum_{i=0}^{m-1} P^{\sigma_m^i}$.*

Proof: The statement is clear for $m = 1$ by taking $P = Q$.

So assume $m \geq 2$. Let $P' \in E(L_m)$ be a point above Θ, see Proposition 5.2.1. Then $\sum_{i=0}^{m-1} P'^{\sigma_m^i}$ reduces to the same multiplicity-1 irreducible component as Q because $\delta_m(\Theta) = \psi_E(Q)$. Therefore, $R := Q - \sum_{i=0}^{m-1} P'^{\sigma_m^i} \in E^0(K)$. Since $\operatorname{char} k \neq 2, 3$ and $\overline{k} = k$, we have $E^0(K) = mE^0(K)$, see ([27], Chapter VII, Exercise 7.8). Thus $R = mT$ for some $T \in E^0(K)$.

Now consider the extension $\tau_T' : E^{min} \to E^{min}$ of the translation-by-T automorphism τ_T. The multiplicity-1 irreducible components of E_k^{min} are fixed under τ_T', the projection formula then implies that τ_T' fixes every irreducible component of E_k^{min}. Set $P := \tau_T(P') = T + P'$. Then $\sum_{i=0}^{m-1} P^{\sigma_m^i} = mT + \sum_{i=0}^{m-1} P'^{\sigma_m^i} = Q$. □

Chapter 7

Counting minimal degree-n-models

Let K be a Henselian discrete valuation field with ring of integers $\mathcal{O}_K$. We fix a uniformiser t. We denote the normalised valuation on K by ν. We assume that the residue field k is algebraically closed and that $\operatorname{char} k \neq 2, 3$.

Let C be a smooth genus one curve over K defined by a genus one equation ϕ of degree n. We assume that $C(K) \neq \emptyset$. In this chapter we count the number of minimal degree-n-models for $C \to \mathbb{P}^{n-1}_K$ up to isomorphism, where $n \in \{2, 3, 4\}$.

7.1 Counting results

Let E be the Jacobian of C. Since $E \cong_K C$, we can assume that ϕ is the defining equation of a morphism $E \to \mathbb{P}^{n-1}_K$ determined by a divisor class $[H]$, where H is a hyperplane section divisor on E. The divisor H is linearly equivalent to $(n-1).0_E + P$ for some $P \in E(K)$.

The homomorphism ψ_E is the surjective homomorphism in the following short exact sequence

$$0 \to E^0(K) \to E(K) \xrightarrow{\psi_E} \Phi_E(K) \to 0.$$

We recall that $\Phi^m_K(E)$, $m \geq 1$, is the set of multiplicity-m components in the special fiber of the minimal proper regular model E^{min} of E. The main result of this chapter is the following theorem.

Theorem 7.1.1. *Let E/K be an elliptic curve and let $P \in E(K)$. Let $E \to \mathbb{P}^{n-1}_K$ be the morphism determined by the divisor class $[(n-1).0_E + P]$, $n \in \{2, 3, 4\}$. Let $\delta_m : \Phi^m_K(E) \to \Phi_K(E)$ be the function defined in Chapter 6. Then there is a bijection between the set of minimal degree-n-models for $E \to \mathbb{P}^{n-1}_K$ up to isomorphism and the disjoint union of the following sets.*

(i) The set of unordered n-tuples

$$S_1(n) = \{(a_1, \ldots, a_n) : a_i \in \Phi_K(E) \mid a_1 + \ldots + a_n = \psi_E(P)\},$$

(ii) the set $S_n = \{a \in \Phi_K^n(E) \mid \delta_n(a) = \psi_E(P)\}$,

and

if $n \geq 3$

(iii) the set $S_{(n-1,1)} = \{(a, b) \in \Phi_K^{n-1}(E) \times \Phi_K(E) \mid \delta_{n-1}(a) + b = \psi_E(P)\}$,

and

if $n = 4$

(iv) the set $S_{(2,1,1)} = \{(a, b, c) \in \Phi_K^2(E) \times \Phi_K(E) \times \Phi_K(E) \mid \delta_2(a) + b + c = \psi_E(P)\}$, where the order of b and c is immaterial,

(v) the set of unordered pairs

$$S_{(2,2)} = \{(a, b) \in \Phi_K^2(E) \times \Phi_K^2(E) \mid \delta_2(a) + \delta_2(b) = \psi_E(P)\}.$$

The proof will follow directly from Theorem 7.2.3 stated below.

The sets defined in the theorem above depend on the point $P \in E(K)$. Now we get the following corollaries as direct consequences of Theorem 7.1.1

Corollary 7.1.2. *Let E/K be an elliptic curve and let $P \in E(K)$. Let $E \to \mathbb{P}_K^{n-1}$ be the morphism determined by the divisor class $[(n-1).0_E + P]$, $n \in \{2, 3, 4\}$. Assume that E has one of the reduction types $\mathrm{I}_m, m \geq 0, \mathrm{II}, \mathrm{III}$, or IV. Let $m = \#\Phi_K(E)$. The number of minimal degree-n-models for $E \to \mathbb{P}_K^{n-1}$ is N_n where*

(i) if $n = 2$

$$N_2 = \begin{cases} (m+1)/2 & \textit{if } 2 \nmid m \\ m/2 + 1 & \textit{if } 2 \mid m \textit{ and } \psi_E(P) \in 2\Phi_K(E) \\ m/2 & \textit{if } 2 \mid m \textit{ and } \psi_E(P) \notin 2\Phi_K(E) \end{cases}$$

(ii) if $n = 3$

$$N_3 = \begin{cases} (m+1)(m+2)/6 & \textit{if } 3 \nmid m \\ m(m+3)/6 + 1 & \textit{if } 3 \mid m \textit{ and } \psi_E(P) \in 3\Phi_K(E) \\ m(m+3)/6 & \textit{if } 3 \mid m \textit{ and } \psi_E(P) \notin 3\Phi_K(E) \end{cases}$$

(iii) if $n = 4$

$$N_4 = \begin{cases} (m+1)(m+2)(m+3)/24 & \textit{if } 2 \nmid m \\ 3 & \textit{if } m = 2 \textit{ and } \psi_E(P) = \bar{0} \\ m(m+2)(m+4)/24 + 2 & \textit{if } 2 \mid m,\ m \neq 2 \textit{ and } \psi_E(P) \in 4\Phi_K(E) \\ m(m+2)(m+4)/24 + 1 & \textit{if } 2 \mid m \textit{ and } \psi_E(P) \in 2\Phi_K(E) \setminus 4\Phi_K(E) \\ m(m+2)(m+4)/24 & \textit{if } 2 \mid m \textit{ and } \psi_E(P) \notin 2\Phi_K(E). \end{cases}$$

Proof: Since for the given reduction types we have $\Phi_K^m(E) = \emptyset$ when $m \geq 2$, the sets $S_n,\ S_{(n-1,1)}, S_{(2,1,1)}$ and $S_{(2,2)}$ of Theorem 7.1.1 are empty. In other words, $N_n = \#S_1(n)$. The numbers stated above are the possible cardinalities of $S_1(n)$. □

For $a \in \Phi_K^2(E)$ we set

$$S_{(2,1,1)}(a) = \{(b, c) : b, c \in \Phi_K(E) \mid b + c = \psi_E(P) - \delta_2(a)\}.$$

Lemma 7.1.3. *The following equalities hold*

(i) $\#S_{(n-1,1)} = \#\Phi_K^{n-1}(E)$ *when* $n \geq 3$.

(ii) $\#S_{(2,1,1)} = \sum_{a \in \Phi_K^2(E)} S_{(2,1,1)}(a)$.

Proof: (i) We consider the projection map $S_{(n-1,1)} \to \Phi_K^{n-1}(E)$ which sends an element $(a, b) \in \Phi_K^{n-1}(E) \times \Phi_K(E)$ to a. It is surjective and we want to show the injectivity. Let $(a_1, b_1), (a_2, b_2)$ be two elements in $S_{(n-1,1)}$ with the same image, i.e., $a_1 = a_2$. From the definition of $S_{(n-1,1)}$ we have $\delta_{n-1}(a_1) + b_1 = \delta_{n-1}(a_2) + b_2 = \psi_E(P)$. Therefore, $b_1 = b_2$, and the two sets are in bijection.

(ii) Direct calculation by computing the number of triples in which each $a \in \Phi_K^2(E)$ lies. □

Corollary 7.1.4. *Let E/K be an elliptic curve and let $P \in E(K)$. Assume that E has reduction type $T \in \{\mathrm{I}_m^*,\ m \geq 0, \mathrm{IV}^*, \mathrm{III}^*, \mathrm{II}^*\}$. Let $E \to \mathbb{P}_K^{n-1}$ be the morphism determined by the divisor class $[(n-1).0_E + P]$, $n \in \{2, 3, 4\}$. Let N_n denote the number of minimal degree-n-models for $E \to \mathbb{P}_K^{n-1}$. Then N_n is determined according to the following tables*

(i) if E has reduction type $\mathrm{I}_{2m}^*, m \geq 0$, then

$\psi_E(P)$	$(\bar{0},\bar{0})$	$(\bar{1},\bar{1})$	$(\bar{0},\bar{1})$	$(\bar{1},\bar{0})$
N_2	$m+5$	$m+2$	2	2
N_3	$2m+6$			
N_4	$(m+4)^2$	$(m+2)(m+5)$	$4m+10$	

(ii) if E has reduction type $\mathrm{I}^*_{2m+1}, m \geq 0$, *then*

$\psi_E(P)$	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\bar{3}$
N_2	$m+4$		2	
N_3	$2m+7$			
N_4	$(m+3)(m+6)$	$(m+4)^2$	$4m+12$	

(iii) if E has reduction type IV^*, *then*

$\psi_E(P)$	$\bar{0}$	$\bar{1}$	$\bar{2}$
N_2	3		
N_3	8	6	6
N_4	14		

(iv) if E has reduction type III^*, *then*

$\psi_E(P)$	$\bar{0}$	$\bar{1}$
N_2	4	2
N_3	6	6
N_4	15	10

(v) if E has reduction type II^*, *then*

N_2	3
N_3	5
N_4	10

PROOF: We recall that the number of minimal degree-2-models for $E \to \mathbb{P}^1_K$ is the cardinality of the disjoint union of the sets $S_1(2)$ and S_2. The number of minimal degree-3-models for $E \to \mathbb{P}^2_K$ is the cardinality of the disjoint union of $S_1(3), S_{(2,1)}$, and S_3. The number of minimal degree-4-models for $E \to \mathbb{P}^3_K$ is the cardinality of the disjoint union of $S_1(4), S_{(3,1)}, S_{(2,2)}, S_{(2,1,1)}$, and S_4. So we have to find the cardinality of each set when E has one of the reduction types $\mathrm{I}^*_m, \mathrm{IV}^*, \mathrm{III}^*$, or II^*.

(i) When E has reduction type $\mathrm{I}^*_{2m}, m \geq 0$, the components group $\Phi_K(E)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We have $\#S_1(2) = 4$ when $\psi_E(P) = (\bar{0}, \bar{0})$ and $\#S_1(2) = 2$ otherwise. We have $\#S_1(3) = 5$, moreover $\#S_1(4) = 11$ when $\psi_E(P) = (\bar{0}, \bar{0})$, and $\#S_1(4) = 8$ otherwise. Moreover, $\#S_{(2,1)} = \#\Phi^2_K(E) = 2m + 1$, see Lemma 7.1.3. The sets $S_i, i = 3, 4$, and $S_{(3,1)}$ are empty.

To compute the size of $S_2, S_{(2,1,1)}$, and $S_{(2,2)}$ we need to recall some results from Chapter 6. The multiplicity-2 components of E^{min}_k consists of a sequence $V_{-1} : \{y_1^2 = 0\}, V_0, V_1, \ldots, V_{2m-1}$, where $\delta_2(V_i) = (\bar{0}, \bar{0})$ if i is odd and it is equal to $(\bar{1}, \bar{1})$ otherwise, see Corollary 6.2.3. Therefore, $S_2 = \emptyset$ if $\psi_E(P) = (\bar{0}, \bar{1})$ or $(\bar{1}, \bar{0})$, and $\#S_2 = m + 1$ if $\psi_E(P) = (\bar{0}, \bar{0})$, and $\#S_2 = m$ if $\psi_E(P) = (\bar{1}, \bar{1})$.

Now if $\psi_E(P) = \delta_2(V_i)$, then $\#S_{(2,1,1)}(V_i) = 4$, otherwise $\#S_{(2,1,1)}(V_i) = 2$, see Lemma 7.1.3. Therefore, if $\psi_E(P) = (\bar{0}, \bar{1})$ or $(\bar{0}, \bar{1})$, then $\#S_{(2,1,1)}(V_i) = 2$ for each i and $\#S_{(2,1,1)} = 2(2m + 1)$, see Lemma 7.1.3. If $\psi_E(P) = (\bar{0}, \bar{0})(= (\bar{1}, \bar{1})$ respectively), then $(\#S_{(2,1,1)}(V_{2i-1}), \#S_{(2,1,1)}(V_{2i})) = (4, 2), ((2, 4)$ respectively$), i = 0, \ldots, m$. Therefore, we have $\#S_{(2,1,1)} = 4(m + 1) + 2m, (2(m + 1) + 4m$ respectively), see Lemma 7.1.3.

Again if $\psi_E(P) = (\bar{0}, \bar{1})$ or $(\bar{1}, \bar{0})$, then $S_{(2,2)} = \emptyset$. If $\psi_E(P) = (\bar{0}, \bar{0})$, then $\#S_{(2,2)} = \sum_{i=1}^{m+1} i + \sum_{i=1}^{m} i = (m + 1)^2$. If $\psi_E(P) = (\bar{1}, \bar{1})$, then $\#S_{(2,2)} = m(m + 1)$.

(ii) When E has reduction type $\mathrm{I}^*_{2m+1}, m \geq 0$, the components group $\Phi_K(E) = \mathbb{Z}/4\mathbb{Z}$. We have $\#S_1(3) = 5$. Lemma 7.1.3 implies that $\#S_{(2,1)} = \#\Phi^2_K(E) = 2m+2$. Moreover, $S_i, i = 3, 4$, and $S_{3,1}$ are empty sets.

Now $S_1(2) = 3$ when $\psi_E(P) = \bar{0}$ or $\bar{2}$, and $\#S_1(2) = 2$ otherwise. We have $\#S_1(4) = 10$ when $\psi_E(P) = \bar{0}$, $\#S_1(4) = 9$ when $\psi_E(P) = \bar{2}$, and $\#S_1(4) = 8$ otherwise.

We recall that the multiplicity-2 components of E^{min}_k consists of a sequence $V_{-1} : \{y_1^2 = 0\}, V_0, V_1, \ldots, V_{2m}$, where $\delta_2(V_i) = \bar{0}$ if i is odd and it is equal to $\bar{2}$ otherwise, see Corollary 6.2.3. Therefore, if $\psi_E(P) = \bar{1}$ or $\bar{3}$, then S_2 and $S_{(2,2)}$ are empty sets. If $\psi_E(P) = \bar{0}$ or $\bar{2}$, then $\#S_2 = m + 1$.

If $\psi_E(P) - \delta_2(V_i) \in 2\Phi_K(E)$, then $\#S_{(2,1,1)}(V_i) = 3$. Otherwise, $\#S_{(2,1,1)}(V_i) = 2$. Therefore, if $\psi_E(P) = \bar{1}$ or $\bar{3}$, then $\#S_{(2,1,1)}(V_i) = 2$ for each i, hence $\#S_{(2,1,1)} = 2(2m + 2)$, see Lemma 7.1.3. If $\psi_E(P) = \bar{0}$ or $\bar{2}$, then $\#S_{(2,1,1)}(V_i) = 3$ for each i. Therefore, $\#S_{(2,1,1)} = 3(2m + 2)$.

If $\psi_E(P) = \bar{1}$ or $\bar{3}$, then $S_{(2,2)} = \emptyset$. If $\psi_E(P) = \bar{0}$, then $\#S_{(2,2)} = (m + 1)(m + 2)$. If

$\psi_E(P) = \bar{2}$, then $\#S_{(2,2)} = (m+1)^2$.

(iii) When E has reduction type IV*, we have $\Phi_K(E) = \mathbb{Z}/3\mathbb{Z}$. Therefore, $\#S_1(2) = 2$ and $\#S_1(4) = 5$, moreover $\#S_1(3) = 4$ when $\psi_E(P) = \bar{0}$ and $\#S_1(3) = 3$ otherwise.

We recall that $\#S_3 = 1$ if $\psi_E(P) = \bar{0}$, and $S_3 = \emptyset$ otherwise, see Proposition 6.2.5 (ii). Moreover, $\Phi_K^4(E) = \emptyset$ and $\Phi_K^2(E) = \{\Theta_i,\ i = 0,1,2\}$, where $\delta_2(\Theta_0) = \bar{0}$, $\delta_2(\Theta_1) = \bar{2}$, and $\delta_2(\Theta_2) = \bar{1}$, see Proposition 6.2.5. Therefore, Lemma 7.1.3 implies that $\#S_{(2,1)} = \#\Phi_K^2(E) = 3$, and $\#S_{(3,1)} = \#\Phi_K^3(E) = 1$. We have $S_4 = \emptyset$, $\#S_2 = 1$, and $\#S_{(2,2)} = 2$. Furthermore, $S_{(2,1,1)}(a) = 2$ for every $a \in \Phi_K^2(E)$, therefore $\#S_{(2,1,1)} = 6$.

(iv) When E has reduction type III*, we have $\Phi_K(E) = \mathbb{Z}/2\mathbb{Z}$. Therefore, $\#S_1(2) = 2$ if $\psi_E(P) = \bar{0}$, and $\#S_1(2) = 1$ otherwise. $\#S_1(3) = 2$, moreover we have $\#S_1(4) = 3$ when $\psi_E(P) = \bar{0}$, and $\#S_1(4) = 2$ otherwise.

Recall that $\Phi_K^2(E) = \{\Theta_i,\ i = 0,1,2\}$, where $\delta_2(\Theta_i) = \bar{0}$ when $i = 0,1$, and $\delta_2(\Theta_2) = \bar{1}$. Moreover, $\Phi_K^3(E) = \{\Lambda_1, \Lambda_2\}$, where $\delta_3(\Lambda_i) = \bar{i}$, and $\Phi_K^4(E) = \{\Psi\}$, where $\delta_4(\Psi) = \bar{0}$, see Proposition 6.2.6. By virtue of Lemma 7.1.3, we have $\#S_{(2,1)} = \#\Phi_K^2(E) = 3$, and $\#S_{(3,1)} = \#\Phi_K^3(E) = 2$. If $\psi_E(P) = \bar{0}$, then $\#S_2 = 2$, $\#S_{2,2} = 4$, $\#S_{(2,1,1)} = 5$, and $\#S_4 = 1$. Otherwise, we have $\#S_2 = 1, \#S_{2,2} = 2$, $\#S_{(2,1,1)} = 4$, and $S_4 = \emptyset$. We always have $\#S_3 = 1$.

(v) When E has reduction type II*, we have $\Phi_K(E) = (0)$. Therefore, $\#S_1(n) = 1, n \in \{2,3,4\}$, see Corollary 7.1.2.

We have that $\#S_{(n-1,1)} = \#\Phi_K^{n-1}(E) = 2, n = 3,4$, see Lemma 7.1.3. Moreover, $\#S_n = 2, n = 2,3,4$. Finally, $S_{(2,2)} = 3$ and $S_{(2,1,1)} = 2$, see Proposition 6.2.8. □

7.2 Constructing divisors and models

The aim of this section is to prove Theorem 7.1.1. Again we start with a smooth genus one curve C/K where $n \in \{2,3,4\}$. We assume that the equation of C is obtained as an equation for the morphism $E \to \mathbb{P}_K^{n-1}$ determined by $[(n-1).0_E + P]$, where E is the Jacobian of C and $P \in E(K)$. We set

$$S^2 = S_1(2) \cup S_2,\ S^3 = S_1(3) \cup S_3 \cup S_{(2,1)} \text{ and } S^4 = S_1(4) \cup S_4 \cup S_{(3,1)} \cup S_{(2,1,1)} \cup S_{(2,2)}.$$

Then we define the map

$$\lambda_n : \{\text{minimal degree-}n\text{-models for } C \text{ up to isomorphism}\} \to S^n;\ (\mathcal{C}, \alpha) \mapsto (\Gamma_1, \ldots, \Gamma_m),$$

where

(i) $(\Gamma_1, \ldots, \Gamma_m)$ consists of the irreducible components of the strict transform of $\mathcal{C}_k$ in E_k^{min}.

(ii) If $m \geq 2$, then $\text{mult}_k(\Gamma_1) \geq \ldots \geq \text{mult}_k(\Gamma_m)$.

(iii) If Γ is the strict transform of a component Γ' in $\mathcal{C}_k$, then Γ appears in $(\Gamma_1, \ldots, \Gamma_m)$ as many times as $\deg_k \Gamma'$. In particular, we have $\sum_{i=1}^m \text{mult}_k(\Gamma_i) = n$.

We will prove that the map λ_n is a bijection and hence Theorem 7.1.1 follows. Recall that the type of an irreducible component Γ of the special fiber of a degree-n-model is the pair $(\text{mult}_k \Gamma, \deg_k \Gamma)$.

Lemma 7.2.1. *The map λ_n described above is well-defined.*

Proof: We need to show that (i) if $\mathcal{C}$ and $\mathcal{C}'$ are minimal isomorphic degree-n-models for C, then $\lambda_n(\mathcal{C}) = \lambda_n(\mathcal{C}')$, and (ii) $\lambda(\mathcal{C}) \in S^n$. To prove (i) we know that the special fibers of any two isomorphic degree-n-models for C have the same irreducible components with the same types, therefore the corresponding tuples of both models are the same, see Theorem 5.1.4.

Now we want to prove (ii), in other words we want to show that if $(\Gamma_1, \ldots, \Gamma_m)$ is the tuple associated to $\mathcal{C}$, then $\sum_{i=1}^m \delta_{m_i}(\Gamma_i) = \psi_E(P)$ where $m_i = \text{mult}_k(\Gamma_i)$. Let D be a divisor on E^{min} such that $\mathcal{C}$ is obtained from E^{min} by contraction using D, see Theorem 4.0.1. The divisor D intersects the Γ_i's and no other components. We have $D.\Gamma_j = m_j \deg_k \Gamma'_j$, where Γ'_j is an irreducible component of $\mathcal{C}_k$ whose strict transform in E_k^{min} is Γ_j, in particular if $\deg_k \Gamma'_j = d_j$, then D intersects Γ_j in d_j points which might not be distinct. Let $(x_1, \ldots, x_m)$ be a tuple of all intersection points of D with the irreducible components $(\Gamma_1, \ldots, \Gamma_m)$, where $x_i \in \Gamma_i$. Note that x_i may be repeated in $(x_1, \ldots, x_m)$ if Γ_i is the strict transform of a component whose degree is greater than 1. Moreover, we have $D|_E \sim (n-1).0 + P$.

Let $m_r = \max\{m_j := \text{mult}_k \Gamma_j : 1 \leq j \leq m\}$. It is clear that for $\Gamma_j,\ j = 1, \ldots, m$, the multiplicity $m_j \in \{1, m_r\}$, since otherwise we will have $1 < m_j < m_r$ which implies that $m_r \geq 3$, hence $m_r + m_j \geq 5$ which contradicts that $\sum_{i=1}^m m_i = n \leq 4$. Let $L_j = K(t^{1/m_j})$ and $\text{Gal}(L_j/K) = \langle \sigma_j \rangle$. By virtue of Proposition 5.2.1, there exists a closed point $P_j \in E(L_j)$ such that $[K(P_j) : K] = m_j$, and $\overline{\{P_j\}} \cap \Gamma_j = \{x_j\}$. Let $\mathcal{E}$ be the minimal proper regular model of E/L_r. Since x_j lies on one and only one component of E_k^{min}, then there are exactly m_j points $\{y_1, \ldots, y_{m_j}\}$ of $\mathcal{E}$ lying above x_j, and each of these points lies on a multiplicity-1 component of $\mathcal{E}_k$, see ([20], Remark 10.4.8). Now we view D as a divisor on $\mathcal{E}$. We have

$$\tilde{P} = (\text{sum}\, D|_E)^{\sim} = \text{sum}\, D|_{\mathcal{E}_k} = \sum_{j=1}^{m} \sum_{l=1}^{m_j} y_l = \sum_{j=1}^{m} \sum_{l=1}^{m_j} \tilde{P}_j^{\sigma_j^l}.$$

The second equality holds because D intersects $\mathcal{E}_k$ only in multiplicity-1 components. Therefore, we have $P - \sum_{j=1}^{m} \sum_{l=1}^{m_j} P_j^{\sigma_j^l} \in E^0(K)$. Applying the surjective group homomorphism $\psi_E : E(K) \to \Phi_K(E)$, we get $\psi_E(P) = \sum_{j=1}^{m} \psi_E(\sum_{l=1}^{m_j} P_j^{\sigma_j^l}) = \sum_{j=1}^{m} \delta_{m_j}(\Gamma_j)$. □

Lemma 7.2.2. *Let $(\Gamma_1, \dots, \Gamma_m) \in S^n$. Then there exists a divisor D on E^{min} such that:*

(i) $D|_E$ is K-rational.

(ii) $D.\Gamma_i = d_i. \operatorname{mult}_k \Gamma_i$, where d_i is the number of times Γ_i appears in $(\Gamma_1, \dots, \Gamma_m)$.

(iii) $D|_E \sim (n-1).0 + P$.

Proof: Assume that $(\Gamma_1, \dots, \Gamma_n) \in S_1(n)$. Let $x_i \in \Gamma_i,\ i = 1, \dots, n-1$, be a point defined over k. Hensel's Lemma allows us to lift x_i to a point $P_i \in E(K),\ i = 1, \dots, n-1$. Set $P_n = P - \sum_{i=1}^{n-1} P_i \in E(K)$. Note that P_n lies above Γ_n because $\psi_E(P_n) = \psi_E(P) - \sum_{j=1}^{n-1} \psi_E(P_i) = \psi_E(P) - \sum_{i=1}^{n-1} \delta_1(\Gamma_i) = \delta_1(\Gamma_n)$, where the last equality follows from the definition of $S_1(n)$. Set the divisor D to be $\sum_{i=1}^{n} \overline{\{P_i\}}$ on E^{min}, where $\overline{\{P_i\}}$ is the Zariski closure of P_i in E^{min}.

Now let $K_m = K(t^{1/m})$ and $\mathrm{Gal}(K_m/K) = \langle \sigma_m \rangle$.

Assume that $(\Gamma_n) \in S_n$. Since $\delta_n(\Gamma_n) = \psi_E(P)$, Corollary 6.2.9 shows that there exists a point $Q \in E$ with $[K(Q) : K] = n$, $\tilde{Q} \in \Gamma_n$ and $\sum_{i=1}^{n} Q^{\sigma_n^i} = P$. Set $D = \overline{\{Q\}}$.

Assume that $(\Gamma_{n-1}, \Gamma) \in S_{(n-1,1)}$, $n \geq 3$. Let Q' be a point which reduces on Γ. We have $\delta_{n-1}(\Gamma_{n-1}) = \psi_E(P) - \delta_1(\Gamma) = \psi_E(P - Q')$. Again Corollary 6.2.9 shows that there exists a point $Q \in E$ with $[K(Q) : K] = n-1$, $\tilde{Q} \in \Gamma_{n-1}$, and $\sum_{i=1}^{n-1} Q^{\sigma_{n-1}^i} = P - Q'$. Set $D = \overline{\{Q'\}} + \overline{\{Q\}}$.

Assume that $(\Theta, \Gamma_1, \Gamma_2) \in S_{(2,1,1)}$. Let $P_i \in E(K)$ be such that $\tilde{P}_i \in \Gamma_i$. We have $\delta_2(\Theta) = \psi_E(P - P_1 - P_2)$. Again there exists a point $Q \in E$ with $[K(Q) : K] = 2$, $\tilde{Q} \in \Theta$, and $Q + Q^{\sigma_2} = P - P_1 - P_2$. Set $D = \overline{\{P_1\}} + \overline{\{P_2\}} + \overline{\{Q\}}$.

Assume that $(\Theta_1, \Theta_2) \in S_{(2,2)}$. Let $P' \in E(K)$ be such that $\delta_2(\Theta_1) = \psi_E(P')$. According to Corollary 6.2.9, there exists $Q_i \in E$ with $[K(Q_i) : K] = 2$, $\tilde{Q}_i \in \Theta_i$, $Q_1 + Q_1^{\sigma_2} = P'$, and $Q_2 + Q_2^{\sigma_2} = P - P'$. Set $D = \overline{\{Q_1\}} + \overline{\{Q_2\}}$. □

Theorem 7.2.3. *The map λ_n is a bijection.*

Proof: We proved that λ_n is well defined in Lemma 7.2.1. To prove that λ_n is injective, let $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ be two minimal degree-n-models for C. Assume that $\lambda_n(\mathcal{C}_1) = \lambda_n(\mathcal{C}_2)$. We want to show that $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ are isomorphic. The fact that they have the same corresponding tuples implies that for an irreducible component Γ of $(\mathcal{C}_2)_k$, we have $(\alpha_2^{-1}\alpha_1)^*\Gamma$ is an irreducible component of $(\mathcal{C}_1)_k$ with the same type, therefore $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ are isomorphic, see Theorem 5.1.4.

Now we will prove that λ_n is surjective. So assume that $(\Gamma_1, \ldots, \Gamma_m) \in S^n$ and we want to construct a minimal degree-n-model $(\mathcal{C}, \alpha)$ whose image under λ_n is $(\Gamma_1, \ldots, \Gamma_m)$. If Γ_i appears d_i times in $(\Gamma_1, \ldots, \Gamma_m)$, then $\mathcal{C}_k$ should contain an irreducible component Γ'_i, whose strict transform in E_k^{min} is Γ_i, such that $\deg_k \Gamma'_i = d_i$. By virtue of Lemma 7.2.2, there exists a divisor D on E^{min} such that $D|_E$ is K-rational, $D.\Gamma_i = d_i.\operatorname{mult}_k \Gamma_i$, and $D|_E \sim (n-1).0 + P$. Consider the following S-model for C

$$\mathcal{C} := \operatorname{Proj}(\bigoplus_{m=0}^{\infty} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD))).$$

The model $\mathcal{C}$ is given by a genus one equation of degree n, moreover it is minimal because it is obtained by contracting components in E^{min}, see Theorem 4.2.3. The special fiber $\mathcal{C}_k$ consists of the components in $(\Gamma_1, \ldots, \Gamma_m)$ because D intersects these components in E_k^{min} and intersects no other components. Moreover, each component of $\mathcal{C}_k$ has degree equal to the number of iterations of its strict transform in $(\Gamma_1, \ldots, \Gamma_m)$ because $D.\Gamma_i = d_i.\operatorname{mult}_k \Gamma_i$. We obtain α from the linear equivalence of $D|_E$ and $(n-1).0_E + P$. □

Chapter 8

Counting models over $\mathbb{Q}$

Let $p \geq 5$ be a prime number, and $n \in \{2, 3, 4\}$. Let $\mathbb{Q}_p^{un}$ be the maximal unramified extension of the p-adic field $\mathbb{Q}_p$. Let $\mathbb{Z}_p$ be the ring of p-adic integers and $\mathbb{Z}_p^{un}$ the ring of integers of $\mathbb{Q}_p^{un}$.

In this chapter we will be interested in attacking the global question. More precisely, let C be a smooth genus one curve over $\mathbb{Q}$ defined by an integral genus one equation of degree n, we define a *minimal global degree-n-model* $(\mathcal{C}, \alpha)$ *for* $C \to \mathbb{P}^{n-1}_{\mathbb{Q}}$ to be a degree-n-model $\mathcal{C} \to \operatorname{Spec}\mathbb{Z}$ for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}}$ such that $\mathcal{C} \to \operatorname{Spec}\mathbb{Z}_p$ is minimal for every prime p, see §3.1.

It is known that a minimal global degree-1-model for $C/\mathbb{Q}$, i.e., a Weierstrass model, exists and is unique up to isomorphism. A proof of the existence of a minimal global degree-n-model for $C/\mathbb{Q}$ when $n \in \{2, 3\}$ can be found in ([14], Theorem 2.6). An algorithm which proves the existence of minimal global degree-n-models when $n \in \{1, 2, 3, 4\}$ can be found in [11].

The problem stated above can be tackled locally by considering C as a curve over $\mathbb{Q}_p$ and looking at minimal degree-n-models for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$ up to $\operatorname{Spec}\mathbb{Z}_p$-isomorphism at each prime p. It turns out that we need only to investigate a finite set of primes. We need to overcome two obstacles: (i) the residue fields $\mathbb{F}_p$ are not algebraically closed which means that we can not use the results we obtained in the previous chapters directly (ii) collecting the local data we obtain at each prime to count minimal global models up to $\operatorname{Spec}\mathbb{Z}$-isomorphism.

We will show that the split reduction types are no different from the geometric case, i.e., when the residue field is algebraically closed. Then we move to the non-split reduction types and use the fact that after a finite unramified base change the reduction becomes split. In fact, we make use of the action of the Galois group $\operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on the irreducible components of the minimal proper regular model.

The last remark to make is that considering C as a curve over $\mathbb{Q}_p^{un}$ rather than over $\mathbb{Q}_p$, the number of degree-n-models for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_p^{un}}$ up to $\operatorname{Spec}\mathbb{Z}_p^{un}$-isomorphism is determined according to Theorem 7.1.1 because the residue field $\overline{\mathbb{F}}_p$ is algebraically closed. Thus we only need to figure out how many of these models are $\operatorname{Spec}\mathbb{Z}_p^{un}$-isomorphic to ones defined over $\mathbb{Z}_p$.

8.1 $\mathbb{F}_p$-rational divisors

We write $\mathcal{G}_p$ for $\operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. Let C be a smooth genus one curve over $\mathbb{Q}_p$, such that $C(\mathbb{Q}_p) \neq \emptyset$, with Jacobian elliptic curve E and minimal proper regular model E^{min}. Let $\mathcal{C} \to \operatorname{Spec}\mathbb{Z}_p^{un}$ be a minimal degree-n-model for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$. Set $\operatorname{Irr}_{\mathcal{C}}$ to be the tuple consisting of the irreducible components of the strict transform of $\mathcal{C}_{\overline{\mathbb{F}}_p}$ in $E^{min}_{\overline{\mathbb{F}}_p}$ such that if Γ is an irreducible component of $\mathcal{C}_{\overline{\mathbb{F}}_p}$, then the strict transform of Γ appears in $\operatorname{Irr}_{\mathcal{C}}$ as many times as $\deg_{\overline{\mathbb{F}}_p}\Gamma$. It is understood that only multiplicity-m components, where $m = 1, 2$, can have degrees greater than 1 in $\mathcal{C}_{\overline{\mathbb{F}}_p}$. The order of the tuple $\operatorname{Irr}_{\mathcal{C}}$ is immaterial. The group $\mathcal{G}_p$ acts on $\operatorname{Irr}_{\mathcal{C}}$ in the obvious way, namely $(\Gamma_1, \ldots, \Gamma_l)^\sigma = (\Gamma_1^\sigma, \ldots, \Gamma_l^\sigma)$ for $\sigma \in \mathcal{G}_p$.

We recall that $\mathcal{C}$ is obtained from $E^{min} \to \operatorname{Spec}\mathbb{Z}_p^{un}$ by contraction via a divisor D, see Theorem 4.0.1. The divisor D intersects each irreducible component of $\operatorname{Irr}_{\mathcal{C}}$ and meets no other components in $E^{min}_{\overline{\mathbb{F}}_p}$, i.e., for an irreducible component Γ of $E^{min}_{\overline{\mathbb{F}}_p}$, we have $D \cap \Gamma \neq \emptyset$ if and only if $\Gamma \in \operatorname{Irr}_{\mathcal{C}}$. The defining genus one equation ϕ of $\mathcal{C}$ is obtained as a dependence relation in a finitely generated free $\mathbb{Z}_p^{un}$-module of the form $H^0(E^{min}, \mathcal{O}_{E^{min}}(mD))$, for some $m \geq 1$, see Theorem 4.2.3.

In this section we give a necessary and sufficient condition for $\mathcal{C}$ to be $\operatorname{Spec}\mathbb{Z}_p^{un}$-isomorphic to a degree-$n$-model which is defined over $\mathbb{Z}_p$, in other words the condition under which it is possible to construct a divisor D' on $E^{min} \to \operatorname{Spec}\mathbb{Z}_p^{un}$ such that $\mathcal{O}_{E^{min}}(D) \cong \mathcal{O}_{E^{min}}(D')$ and $D'|_C$ is $\mathbb{Q}_p$-rational. In fact, this condition will turn out to be that $\operatorname{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant. The main result for counting degree-n-models over $\mathbb{Z}_p$ is the following theorem.

Theorem 8.1.1. *Let C be a smooth curve over $\mathbb{Q}_p$ defined by an integral genus one equation of degree n with $C(\mathbb{Q}_p) \neq \emptyset$. Let $E^{min} \to \operatorname{Spec}\mathbb{Z}_p^{un}$ be the minimal proper regular model of the Jacobian elliptic curve E. Let $(\mathcal{C} \to \operatorname{Spec}\mathbb{Z}_p^{un}, \alpha)$ be a minimal degree-n-model for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$. Then $(\mathcal{C}, \alpha)$ is $\operatorname{Spec}\mathbb{Z}_p^{un}$-isomorphic to a minimal degree-n-model defined over $\mathbb{Z}_p$ if and only if $\operatorname{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant.*

The next section is devoted to the proof of Theorem 8.1.1. Now we get some applications of Theorem 8.1.1. We will count minimal degree-n-models for C which are defined over $\mathbb{Z}_p$. That is the number of all the combinatorial possibilities for $\mathrm{Irr}_{\mathcal{C}}$ to be $\mathcal{G}_p$-invariant. Recall that the genus one equation defining C can be considered as an equation for a morphism $E \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$ determined by a divisor class of the form $[(n-1).0_E + P]$ for some $P \in E(\mathbb{Q}_p)$. This point P reduces to a point on a multiplicity-1 irreducible component in $E^{min}_{\overline{\mathbb{F}}_p}$ defined over $\mathbb{F}_p$.

Corollary 8.1.2. *Let $E/\mathbb{Q}_p$ be an elliptic curve and let $P \in E(\mathbb{Q}_p)$. Assume that E has split reduction. Let $E \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$ be the morphism determined by the divisor class $[(n-1).0_E + P]$, $n \in \{2,3,4\}$. Let $\delta_m : \Phi^m_{\mathbb{Q}_p^{un}}(E) \to \Phi_{\mathbb{Q}_p^{un}}(E)$ be the function defined in Chapter 6. Then there is a bijection between the set of minimal degree-n-models for $E \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$ up to isomorphism and the union of the sets given in Theorem 7.1.1.*

PROOF: If we consider E as a curve over $\mathbb{Q}_p^{un}$, then the number of minimal degree-n-models up to $\mathrm{Spec}\,\mathbb{Z}_p^{un}$-isomorphism is the cardinality of the disjoint union of the sets stated in Theorem 7.1.1. But Theorem 8.1.1 shows that each of these models is isomorphic to a minimal degree-n-model with coefficients in $\mathbb{Z}_p$ because all the components of $E^{min}_{\overline{\mathbb{F}}_p}$ are defined over $\mathbb{F}_p$. □

Remark 8.1.3. If E has one of the reduction types

$$\mathrm{I}_m, m \in \{0,1,2\}, \mathrm{II}, \mathrm{III}, \mathrm{III}^*, \mathrm{II}^*,$$

then the reduction is always split, in particular all irreducible components of $E^{min}_{\overline{\mathbb{F}}_p}$ are defined over $\mathbb{F}_p$. Therefore, the number of minimal degree-n-models for these reduction types is determined according to Corollary 8.1.2.

For the rest of this section we will be concerned with non-split reduction types. We will count the set of minimal degree-n-models $\mathcal{C} \to \mathrm{Spec}\,\mathbb{Z}_p^{un}$ for which $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant. We will denote the number of multiplicity-1 irreducible components of $E^{min}_{\overline{\mathbb{F}}_p}$ which are defined over $\mathbb{F}_p$ by c_p, this is the *Tamagawa number* of the Jacobian $E/\mathbb{Q}_p$.

Corollary 8.1.4. *Let $E/\mathbb{Q}_p$ be an elliptic curve and let $P \in E(\mathbb{Q}_p)$. Let $E \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$ be the morphism determined by the divisor class $[(n-1).0_E + P]$. Assume that E has non-split reduction. Then the number of minimal degree-n-models for $E \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$ up to isomorphism is determined according to the following table.*

	c_p	$n=2$	$n=3$	$n=4$
I_{2m+1}	1	$m+1$	$m+1$	$(m+1)(m+2)/2$
$\mathrm{I}_{2m},\ P\in E^0(\mathbb{Q}_p)$	2	$m+1$	$m+1$	$(m+1)(m+2)/2$
$\mathrm{I_{2m},\ P\notin E^0(\mathbb{Q}_p)}$	2	1	$m+1$	$m+1$
IV	1	2	2	3
I_0^*	1	2	3	4
$\mathrm{I}_{2m+1}^*,\ m\geq 0,\ P\in E^0(\mathbb{Q}_p)$	2	$m+4$	$2m+5$	$(m+3)(m+4)$
$\mathrm{I}_{2m+1}^*,\ m\geq 0,\ P\notin E^0(\mathbb{Q}_p)$	2	$m+2$	$2m+5$	$(m+2)(m+4)$
$\mathrm{I}_{2m}^*,\ m\geq 0,\ P\in E^0(\mathbb{Q}_p)$	2	$m+3$	$2m+4$	$(m+2)(m+4)$
$\mathrm{I}_{2m}^*,\ m\geq 0,\ P\notin E^0(\mathbb{Q}_p)$	2	$m+2$	$2m+4$	$(m+2)(m+3)$
IV^*	1	3	4	8

Recall that ψ_E is the surjective group homomorphism in the short exact sequence

$$0\to E^0(\mathbb{Q}_p)\to E(\mathbb{Q}_p)\xrightarrow{\psi_E}\Phi_{\mathbb{Q}_p}(E)(\mathbb{F}_p)\to 0,$$

and that we fix an isomorphism $\Phi_{\mathbb{Q}_p^{un}}(E)(\overline{\mathbb{F}}_p)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ when E has reduction I_{2m}^*, and $\Phi_{\mathbb{Q}_p^{un}}(E)(\overline{\mathbb{F}}_p)\cong\mathbb{Z}/l\mathbb{Z}$ for other reduction types.

Proof of Corollary 8.1.4:

Multiplicative reduction: It is known that if $E/\mathbb{Q}_p$ has non-split multiplicative reduction $\mathrm{I}_m,\ m\geq 3$, over $\mathbb{Q}_p$, then there exists an unramified quadratic extension $K/\mathbb{Q}_p$ such that E/K has split multiplicative reduction I_m.

For reduction type I_{2m+1} we have $c_p=1$. Therefore, the identity component Γ_0 is the only multiplicity-1 component defined over $\mathbb{F}_p$. We have $\psi_E(P)=\bar{0}$. The two intersection points of Γ_0 with the other irreducible components of $E_{\overline{\mathbb{F}}_p}^{min}$ are switched under the action of some $\sigma\in\mathcal{G}_p$. It follows that σ carries the ith component of $E_{\overline{\mathbb{F}}_p}^{min}$ to the $(2m+1-i)$th component.

For reduction type I_{2m} we have $c_p=2$. One of the two irreducible components defined over $\mathbb{F}_p$ is the identity component. Again $\mathcal{G}_p$ carries the ith component to the $(2m-i)$th component, therefore the other irreducible component defined over $\mathbb{F}_p$ is the mth component. We have $\psi_E(P)$ is either $\bar{0}$ or m.

Now the tuple $\mathrm{Irr}_{\mathcal{C}}$ corresponding to a minimal degree-n-model $\mathcal{C}$ for C is $\mathcal{G}_p$-invariant if and only if it consists of components of the form determined by the following table.

	$n=2$	$n=3$	$n=4$
$\mathrm{I}_{\mathrm{m}},\ \psi_E(P)=\bar{0}$	$(\bar{i}, m-\bar{i})$	$(\bar{0}, \bar{i}, m-\bar{i})$	$(\bar{i}, m-\bar{i}, \bar{j}, m-\bar{j})$
$\mathrm{I}_m,\ m:\text{even},\ \psi_E(P)=m/2$	$(\bar{0}, m/2)$	$(m/2, \bar{i}, m-\bar{i}).$	$(\bar{0}, m/2, \bar{i}, m-\bar{i})$

The numbers given in the statement of the corollary are the cardinalities of the sets consisting of the tuples given in the table above.

Additive reduction: Now we consider non-split additive reduction types. Let $\mathcal{C}$ be a minimal degree-n-model for $E \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$ determined by $[(n-1).0_E + P]$. Let N_n be the number of minimal degree-n-models which are defined over $\mathbb{Z}_p$, up to $\operatorname{Spec}\mathbb{Z}_p$-isomorphism, i.e., N_n is the number of minimal degree-n-models, up to $\operatorname{Spec}\mathbb{Z}_p$-isomorphism, whose corresponding tuples are $\mathcal{G}_p$-invariant.

Reduction IV**:** If E has non-split reduction of type IV, then $c_p = 1$. We have $\psi_E(P) = \bar{0}$. The group $\mathcal{G}_p$ switches the two non-identity components. When $n = 2$, the tuple $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0}, \bar{0})$ or $(\bar{1}, \bar{2})$. Therefore, $N_2 = 2$. When $n = 3$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0}, \bar{0}, \bar{0})$ or $(\bar{0}, \bar{1}, \bar{2})$. Hence $N_3 = 2$. When $n = 4$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if $\mathrm{Irr}_{\mathcal{C}} \in \{(\bar{0}, \bar{0}, \bar{0}, \bar{0}),\ (\bar{0}, \bar{0}, \bar{1}, \bar{2}),\ (\bar{1}, \bar{2}, \bar{1}, \bar{2})\}$. Hence $N_4 = 3$.

Reduction I_0^***:** If E has reduction type I_0^*, then

$$c_p = 1 + \#\{\alpha \in \mathbb{F}_p : f(\alpha) = 0\}$$

where f is a polynomial of degree 3 in the coefficients of the defining polynomial of E, see ([28], p. 367). Moreover, f has distinct roots in $\overline{\mathbb{F}}_p$. Thus if the reduction is non-split, then either $c_p = 1$ or $c_p = 2$. Moreover, the multiplicity-2 component Θ is defined over $\mathbb{F}_p$, i.e., it is isomorphic to $\mathbb{P}^1_{\mathbb{F}_p}$. In addition, $\delta_2(\Theta) = (\bar{0}, \bar{0})$, see Corollary 6.2.3.

When $c_p = 1$, we have $\psi_E(P) = (\bar{0}, \bar{0})$ and $\mathcal{G}_p$ swaps the 3 non-identity components. When $c_p = 2$, we fix an isomorphism $\Phi_{\mathbb{Q}_p^{un}}(E)(\overline{\mathbb{F}}_p) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ such that $(\bar{1}, \bar{1})$ corresponds to the non-identity component which is defined over $\mathbb{F}_p$. Then we have $\psi_E(P)$ is either $(\bar{0}, \bar{0})$ or $(\bar{1}, \bar{1})$, and $\mathcal{G}_p$ switches the two other components. The multiplicity-2 component Θ is always fixed under the action of $\mathcal{G}_p$.

Assume that $c_p = 1$. For the case $n = 2$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}))$ or the multiplicity-2 component Θ. When $n = 3$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{0}, \bar{0}))$, $((\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}))$ or $((\bar{0}, \bar{0}), \Theta)$. When $n = 4$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{0}, \bar{0}))$, $((\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}))$, $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}), \Theta)$ or (Θ, Θ). Hence $N_2 = 2$, $N_3 = 3$ and $N_4 = 4$.

Now assume that $c_p = 2$. Assume moreover that $\psi_E(P) = (\bar{0}, \bar{0})$. When $n = 2$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}))$, $((\bar{1}, \bar{1}), (\bar{1}, \bar{1}))$ or the multiplicity-2 component Θ. When $n=3$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0},\bar{0}),(\bar{0},\bar{0}),(\bar{0},\bar{0}))$, $((\bar{0},\bar{0}),(\bar{1},\bar{1}),(\bar{1},\bar{1}))$, $((\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1}))$ or $((\bar{0},\bar{0}),\Theta)$. When $n=4$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0},\bar{0}),(\bar{0},\bar{0}),(\bar{0},\bar{0}),(\bar{0},\bar{0}))$, $((\bar{0},\bar{0}),(\bar{0},\bar{0}),(\bar{1},\bar{1}),(\bar{1},\bar{1}))$, $((\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1}))$, $((\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}))$, $((\bar{1},\bar{1}),(\bar{1},\bar{1}),(\bar{1},\bar{1}),(\bar{1},\bar{1}))$, $((\bar{1},\bar{1}),(\bar{1},\bar{1}),\Theta)$, $((\bar{0},\bar{0}),(\bar{0},\bar{0}),\Theta)$ or (Θ,Θ). Hence $N_2=3$, $N_3=4$ and $N_4=8$.

Assume $\psi_E(P)=(\bar{1},\bar{1})$. When $n=2$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0},\bar{0}),(\bar{1},\bar{1}))$ or $((\bar{0},\bar{1}),(\bar{1},\bar{0}))$. When $n=3$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0},\bar{0}),(\bar{0},\bar{0}),(\bar{1},\bar{1}))$, $((\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}))$, $((\bar{1},\bar{1}),(\bar{1},\bar{1}),(\bar{1},\bar{1}))$ or $((\bar{1},\bar{1}),\Theta)$. When $n=4$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0},\bar{0}),(\bar{0},\bar{0}),(\bar{0},\bar{0}),(\bar{1},\bar{1}))$, $((\bar{0},\bar{0}),(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}))$, $((\bar{1},\bar{1}),(\bar{1},\bar{1}),(\bar{0},\bar{1}),(\bar{1},\bar{0}))$, $((\bar{0},\bar{0}),(\bar{1},\bar{1}),(\bar{1},\bar{1}),(\bar{1},\bar{1}))$, $((\bar{0},\bar{0}),(\bar{1},\bar{1}),\Theta)$ or $((\bar{0},\bar{1}),(\bar{1},\bar{0}),\Theta)$. Hence $N_2=2$, $N_3=4$ and $N_4=6$.

Reduction I_m^*, $m\ge 1$: If E has non-split reduction of type I_m^*, $m\ge 1$, then $c_p=2$. The multiplicity-1 non-identity component Γ which is defined over $\mathbb{F}_p$ is the one attached to the same multiplicity-2 component to which the identity component is attached. From the description of the irreducible component Γ, it follows that it corresponds to an element of order 2 in the components group, see Proposition 6.2.2, so it corresponds to $\bar{2}$ when m is odd. When m is even, we fix an isomorphism $\Phi_{\mathbb{Q}_p^{un}}(E)(\overline{\mathbb{F}}_p)\cong\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ such that Γ corresponds to $(\bar{1},\bar{1})$. The group $\mathcal{G}_p$ switches the two other multiplicity-1 irreducible components. All the multiplicity-2 components are defined over $\mathbb{F}_p$, i.e., each of them is isomorphic to $\mathbb{P}^1_{\mathbb{F}_p}$, and hence they are fixed under the action of $\mathcal{G}_p$.

(i) Reduction I_{2m+1}^*: We start with non-split reduction of type I_{2m+1}^*, $m\ge 0$. We recall that the multiplicity-2 components of $E_{\mathbb{F}_p}^{min}$ are $V_{-1},V_0,V_1,\ldots,V_{2m}$ where $\delta_2(V_i)=\bar{0}$ if i is odd and it is equal to $\bar{2}$ otherwise, see Corollary 6.2.3.

Assume that $\psi_E(P)=\bar{0}$. When $n=2$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0},\bar{0})$, $(\bar{2},\bar{2})$, $(\bar{1},\bar{3})$, or V_i where i is odd. When $n=3$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0},\bar{0},\bar{0})$, $(\bar{0},\bar{2},\bar{2})$, $(\bar{0},\bar{1},\bar{3})$, $(\bar{0},V_i)$ where i is odd, or $(\bar{2},V_i)$ where i is even. When $n=4$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0},\bar{0},\bar{0},\bar{0})$, $(\bar{0},\bar{0},\bar{2},\bar{2})$, $(\bar{0},\bar{0},\bar{1},\bar{3})$, $(\bar{2},\bar{2},\bar{1},\bar{3})$, $(\bar{2},\bar{2},\bar{2},\bar{2})$, $(\bar{1},\bar{3},\bar{1},\bar{3})$ or if $\mathrm{Irr}_{\mathcal{C}}$ lies in

$$S_{(2,1,1)}(V_i)=\begin{cases}\{(V_i,\bar{0},\bar{0}),(V_i,\bar{2},\bar{2}),(V_i,\bar{1},\bar{3})\} & \text{if } i \text{ is odd}\\ \{(V_i,\bar{0},\bar{2})\} & \text{if } i \text{ is even}\end{cases}$$

or if $\mathrm{Irr}_{\mathcal{C}}$ is (V_i,V_j) where $i+j$ is even. Therefore, $N_2=m+4$, $N_3=2m+5$ and $N_4=6+4(m+1)+(m+1)(m+2)=(m+3)(m+4)$.

Now assume that $\psi_E(P)=\bar{2}$. When $n=2$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0},\bar{2})$ or V_i where i is even. When $n=3$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0},\bar{0},\bar{2})$, $(\bar{2},\bar{2},\bar{2})$, $(\bar{2},\bar{1},\bar{3})$, or if it is of the form $(\bar{0},V_i)$ where i is even, or $(\bar{2},V_i)$

where i is odd. When $n = 4$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0}, \bar{0}, \bar{0}, \bar{2})$, $(\bar{2}, \bar{2}, \bar{0}, \bar{2})$, $(\bar{1}, \bar{3}, \bar{0}, \bar{2})$ or if it lies in

$$S_{(2,1,1)}(V_i) = \begin{cases} \{(V_i, \bar{0}, \bar{2}) & \text{if } i \text{ is odd} \\ \{(V_i, \bar{0}, \bar{0}), (V_i, \bar{2}, \bar{2}), (V_i, \bar{1}, \bar{3})\} & \text{if } i \text{ is even} \end{cases}$$

or if $\mathrm{Irr}_{\mathcal{C}}$ is of the form (V_i, V_j) where $i + j$ is odd. Therefore, $N_2 = m + 2$, $N_3 = 2m + 5$ and $N_4 = 3 + 4(m + 1) + (m + 1)^2 = (m + 2)(m + 4)$.

(ii) Reduction I^*_{2m}: Now we assume that E has non-split reduction of type I^*_{2m}, $m \geq 1$. The multiplicity-2 components of E_k^{min} are $V_{-1}, V_0, V_1, \ldots, V_{2m-1}$ where $\delta_2(V_i) = (\bar{0}, \bar{0})$ if i is odd and it is equal to $(\bar{1}, \bar{1})$ otherwise, see Corollary 6.2.3.

Assume that $\psi_E(P) = (\bar{0}, \bar{0})$. When $n = 2$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}))$, $((\bar{1}, \bar{1}), (\bar{1}, \bar{1}))$, or V_i where i is odd. When $n = 3$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{0}, \bar{0}))$, $((\bar{0}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{1}))$, $((\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}))$, $((\bar{0}, \bar{0}), V_i)$ where i is odd, or $((\bar{1}, \bar{1}), V_i)$ where i is even.

When $n = 4$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{0}, \bar{0}))$, $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{1}, \bar{1}), (\bar{1}, \bar{1}))$, $((\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}))$, $((\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}))$, $((\bar{1}, \bar{1}), (\bar{1}, \bar{1}), (\bar{1}, \bar{1}), (\bar{1}, \bar{1}))$, or if it lies in

$$S_{(2,1,1)}(V_i) = \begin{cases} \{(V_i, (\bar{0}, \bar{0}), (\bar{0}, \bar{0})), (V_i, (\bar{1}, \bar{1}), (\bar{1}, \bar{1})) & \text{if } i \text{ is odd} \\ \{(V_i, (\bar{0}, \bar{0}), (\bar{1}, \bar{1})), (V_i, (\bar{0}, \bar{1}), (\bar{1}, \bar{0}))\} & \text{if } i \text{ is even} \end{cases}$$

or if $\mathrm{Irr}_{\mathcal{C}}$ is of the form (V_i, V_j) where $i + j$ is even. Therefore, $N_2 = m + 3$, $N_3 = 2m + 4$ and $N_4 = 5 + 2(2m + 1) + (m + 1)^2 = (m + 2)(m + 4)$.

Now assume that $\psi_E(P) = (\bar{1}, \bar{1})$. When $n = 2$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{1}, \bar{1}))$, $((\bar{0}, \bar{1}), (\bar{1}, \bar{0}))$, or V_i where i is even. When $n = 3$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{1}, \bar{1}))$, $((\bar{1}, \bar{1}), (\bar{1}, \bar{1}), (\bar{1}, \bar{1}))$, $((\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}))$, $((\bar{0}, \bar{0}), V_i)$ where i is even, or $((\bar{1}, \bar{1}), V_i)$ where i is odd. When $n = 4$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{1}, \bar{1}))$, $((\bar{0}, \bar{0}), (\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}))$, $((\bar{1}, \bar{1}), (\bar{1}, \bar{1}), (\bar{0}, \bar{0}), (\bar{1}, \bar{1}))$, $((\bar{1}, \bar{1}), (\bar{1}, \bar{1}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}))$, or if it lies in

$$S_{(2,1,1)}(V_i) = \begin{cases} \{(V_i, (\bar{0}, \bar{0}), (\bar{1}, \bar{1})), (V_i, (\bar{0}, \bar{1}), (\bar{1}, \bar{0})) & \text{if } i \text{ is odd} \\ \{(V_i, (\bar{0}, \bar{0}), (\bar{0}, \bar{0})), (V_i, (\bar{1}, \bar{1}), (\bar{1}, \bar{1}))\} & \text{if } i \text{ is even} \end{cases}$$

or if $\mathrm{Irr}_{\mathcal{C}}$ is of the form (V_i, V_j) where $i + j$ is odd. Therefore, $N_2 = m + 2$, $N_3 = 2m + 4$ and $N_4 = 4 + 2(2m + 1) + m(m + 1) = (m + 2)(m + 3)$.

Reduction IV^*: If E has non-split reduction of type IV^*, then $c_p = 1$. More precisely, $E_{\mathbb{F}_p}^{min}$ consists of three irreducible components Γ, Θ, Λ of multiplicities $1, 2, 3$ respectively. The group $\mathcal{G}_p$ switches the two non-identity multiplicity-1 components, and it switches the two multiplicity-2 components Θ', Θ'' which are not defined over $\mathbb{F}_p$. Moreover, $\delta_2(\Theta) = \bar{0}$, $\delta_2(\Theta') + \delta_2(\Theta'') = \bar{0}$, and $\delta_3(\Lambda) = \bar{0}$, see Proposition 6.2.5. When $n = 2$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it consists of either $(\bar{0}, \bar{0}), (\bar{1}, \bar{2})$ or Θ. When $n = 3$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0}, \bar{0}, \bar{0})$, $(\bar{0}, \bar{1}, \bar{2})$, $(\bar{0}, \Theta)$ or Λ. When $n = 4$, $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant if and only if it is either $(\bar{0}, \bar{0}, \bar{0}, \bar{0})$, $(\bar{0}, \bar{0}, \bar{1}, \bar{2})$, $(\bar{1}, \bar{2}, \bar{1}, \bar{2})$, $(\bar{0}, \bar{0}, \Theta)$, $(\bar{1}, \bar{2}, \Theta)$, (Θ, Θ), (Θ', Θ'') or $(\bar{0}, \Lambda)$. Hence $N_2 = 3$, $N_3 = 4$ and $N_4 = 8$. □

8.2 Proof of Theorem 8.1.1

Now we prove one of the implications of Theorem 8.1.1.

Proposition 8.2.1. *Let C be a smooth curve over $\mathbb{Q}_p$ defined by an integral genus one equation of degree n with $C(\mathbb{Q}_p) \neq \emptyset$. Let $E^{min} \to \operatorname{Spec} \mathbb{Z}_p^{un}$ be the minimal proper regular model of the Jacobian elliptic curve E. Let $(\mathcal{C} \to \operatorname{Spec} \mathbb{Z}_p^{un}, \alpha)$ be a minimal degree-n-model for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$. If $(\mathcal{C}, \alpha)$ is $\operatorname{Spec} \mathbb{Z}_p^{un}$-isomorphic to a minimal degree-n-model defined over $\mathbb{Z}_p$, then $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant.*

Proof: Assume that $(\mathcal{C}, \alpha)$ is isomorphic to a degree-n-model $(\mathcal{C}' \to \operatorname{Spec} \mathbb{Z}_p, \alpha')$. Set $\beta := \alpha'^{-1}\alpha$. It follows that if Γ is an irreducible component of $\mathcal{C}'_{\overline{\mathbb{F}}_p}$, then $\beta^*(\Gamma)$ is an irreducible component of $\mathcal{C}_{\overline{\mathbb{F}}_p}$ with the same degree and multiplicity as Γ, see Theorem 5.1.4, hence $\mathrm{Irr}_{\mathcal{C}'}$ coincides with $\mathrm{Irr}_{\mathcal{C}}$. Now we will show that $\mathrm{Irr}_{\mathcal{C}'}$ is $\mathcal{G}_p$-invariant.

The model $\mathcal{C}'$ is obtained from $E^{min} \to \operatorname{Spec} \mathbb{Z}_p^{un}$ by contraction via a divisor D'. Moreover, $H^0(E^{min}, \mathcal{O}_{E^{min}}(mD'))$, $m \geq 1$, is a free finitely generated $\mathbb{Z}_p$-module. Hence the divisors $D'|_{\mathcal{C}'_{\mathbb{Q}_p^{un}}}$ and $D'|_{E^{min}_{\overline{\mathbb{F}}_p}}$ are $\mathbb{Q}_p$-rational and $\mathbb{F}_p$-rational respectively. Since D' intersects irreducible components of $\mathrm{Irr}_{\mathcal{C}'}$ and no other components in $E^{min}_{\overline{\mathbb{F}}_p}$, it follows that if $\Gamma \in \mathrm{Irr}_{\mathcal{C}'}$, and hence there is an $x \in (D'|_{E^{min}_{\overline{\mathbb{F}}_p}}) \cap \Gamma \neq \emptyset$, then $\Gamma^\sigma \in \mathrm{Irr}_{\mathcal{C}'}$ for every $\sigma \in \mathcal{G}_p$, because $x^\sigma \in (D'|_{E^{min}_{\overline{\mathbb{F}}_p}})^\sigma \cap \Gamma^\sigma = (D'|_{E^{min}_{\overline{\mathbb{F}}_p}}) \cap \Gamma^\sigma$. □

The following Theorem is the main ingredient to proceed with the proof of the rest of Theorem 8.1.1.

Theorem 8.2.2. *Let $E/\mathbb{Q}_p$ be an elliptic curve with minimal proper regular model $E^{min} \to \operatorname{Spec} \mathbb{Z}_p$. Let $P \in E(\mathbb{Q}_p)$. Let $n \in \{1, 2, 3, 4\}$. Let $(\Gamma_1, \ldots, \Gamma_m)$ be a tuple of irreducible components of $E^{min}_{\overline{\mathbb{F}}_p}$ satisfying:*

(i) The tuple $(\Gamma_1, \ldots, \Gamma_m)$ is $\mathcal{G}_p$-invariant.

(ii) $\sum_{i=1}^m \operatorname{mult}_{\overline{\mathbb{F}}_p} \Gamma_i = n$.

(iii) $\sum_{i=1}^{m} \delta_{m_i}(\Gamma_i) = \psi_E(P)$ *where* $m_i = \operatorname{mult}_{\overline{\mathbb{F}}_p} \Gamma_i$.

Then there exists a divisor D on $E^{min} \to \operatorname{Spec} \mathbb{Z}_p^{un}$ such that:

(i) $(D|_E)^\sigma = D|_E$ *for every* $\sigma \in \operatorname{Gal}(\mathbb{Q}_p^{un}/\mathbb{Q}_p)$.

(ii) $D.\Gamma_i = d_i. \operatorname{mult}_{\overline{\mathbb{F}}_p} \Gamma_i$, *where d_i is the number of times Γ_i appears in* $(\Gamma_1, \ldots, \Gamma_m)$.

(iii) $D|_E \sim (n-1).0 + P$.

Remark 8.2.3. Notice that the invariance of the tuple of components under Galois action in Theorem 8.2.2, condition (i), was always satisfied when the residue field was algebraically closed, see Lemma 7.2.2.

Now we need a few lemmas to prove Theorem 8.2.2.

Lemma 8.2.4. *Let p be a prime and d an integer such that* $\gcd(d, p) = 1$. *Let K be a finite extension of $\mathbb{Q}_p$. Let E/K be an elliptic curve. Assume that E/K has additive reduction. Then the group $E^0(K)$ is divisible by d.*

Proof: Let k be the residue field of K. Recall that $E^1(K) = \{P \in E(K) : \tilde{P} = \tilde{0}_E\}$. The group $E^0(K)/E^1(K)$ is isomorphic to k^+ because E has additive reduction. In particular, $E^0(K)/E^1(K)$ is divisible by d because $(d, p) = 1$. But the group $E^1(K)$ is uniquely divisible by d, see ([17], Chapter 14, Corollary 1.3). Therefore, $E^0(K)$ is divisible by d. □

We know that $E^0(\mathbb{Q}_p^{un})/dE^0(\mathbb{Q}_p^{un}) = 0$, where $(d, p) = 1$, whatever the reduction type of E is, see ([27], Chapter VII, Exercise 7.8).

If $E/\mathbb{Q}_p$ has non-split reduction type, then there exists a finite unramified extension K over which E has split reduction. This field extension is quadratic except possibly when E has non-split reduction of type I_0^*, then it is either quadratic or cubic.

Let $d = [K : \mathbb{Q}_p] \in \{2, 3\}$. We define the norm map $\operatorname{Norm}_{K/\mathbb{Q}_p}$ to be $\operatorname{Norm}_{K/\mathbb{Q}_p} : E(K) \to E(\mathbb{Q}_p);\ Q \mapsto \sum_{i=1}^{d} Q^{\sigma^i}$, where $\operatorname{Gal}(K/\mathbb{Q}_p) = \langle \sigma \rangle$.

Lemma 8.2.5. *Let $p \geq 5$ be a prime. Assume that $E/\mathbb{Q}_p$ has non-split reduction. Let K be the smallest unramified extension over which E has split reduction. Then* $\operatorname{Norm}_{K/\mathbb{Q}_p} : E^0(K) \to E^0(\mathbb{Q}_p)$ *is surjective.*

Proof: We first treat the additive case. So assume that E has non-split additive reduction. Let $Q \in E^0(\mathbb{Q}_p)$. Since $E^0(\mathbb{Q}_p)$ is divisible by $d = [K : \mathbb{Q}_p]$, see Lemma 8.2.4, there is a $Q' \in E^0(\mathbb{Q}_p)$ with $dQ' = Q$. Now we have $\operatorname{Norm}_{K/\mathbb{Q}_p}(Q') = dQ' = Q$.

Now we treat the multiplicative case. So assume E has non-split multiplicative reduction. We have $[K : \mathbb{Q}_p] = 2$. The non-singular reduction of E will be denoted by $\tilde{E}_{ns}$. Let k be the residue field of K. We denote the image of σ under the isomorphism $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathrm{Gal}(k/\mathbb{F}_p)$ by σ again. Let $\mathrm{Norm}_{k/\mathbb{F}_p} : \tilde{E}_{ns}(k) \to \tilde{E}_{ns}(\mathbb{F}_p);\ Q \mapsto Q + Q^{\sigma}$. Consider the following diagram.

$$\begin{tikzcd}
0 \arrow[r] & E^1(K) \arrow[r] \arrow[d, "\mathrm{Norm}_{K/\mathbb{Q}_p}"'] & E^0(K) \arrow[r] \arrow[d, "\mathrm{Norm}_{K/\mathbb{Q}_p}"'] & \tilde{E}_{ns}(k) \arrow[r] \arrow[d, "\mathrm{Norm}_{k/\mathbb{F}_p}"'] & 0 \\
0 \arrow[r] & E^1(\mathbb{Q}_p) \arrow[r] & E^0(\mathbb{Q}_p) \arrow[r] & \tilde{E}_{ns}(\mathbb{F}_p) \arrow[r] & 0
\end{tikzcd}$$

To prove that $\mathrm{Norm}_{K/\mathbb{Q}_p} : E^0(K) \to E^0(\mathbb{Q}_p)$ is surjective, we only need to show the surjectivity of both $\mathrm{Norm}_{K/\mathbb{Q}_p} : E^1(K) \to E^1(\mathbb{Q}_p)$ and $\mathrm{Norm}_{k/\mathbb{F}_p} : \tilde{E}_{ns}(k) \to \tilde{E}_{ns}(\mathbb{F}_p)$. Let $Q \in E^1(\mathbb{Q}_p)$. Since $E^1(\mathbb{Q}_p)$ is divisible by 2, there is a $Q' \in E^1(\mathbb{Q}_p)$ such that $2Q' = Q$. Now $\mathrm{Norm}_{K/\mathbb{Q}_p}(Q') = 2Q' = Q$.

Now we will show the surjectivity of $\mathrm{Norm}_{k/\mathbb{F}_p}$. The isomorphism $f : \tilde{E}_{ns}(k) \cong k^*$ induces an isomorphism $\tilde{E}_{ns}(\mathbb{F}_p) \cong U := \{u \in k^* : \mathrm{Norm}_{k/\mathbb{F}_p}(u) = 1\}$. Moreover, the k-automorphism $\sigma^{-1} f \sigma f^{-1} : k^* \to k^*$ is $u \mapsto u^{-1}$, see ([20], Exercise 10.2.7). Therefore, the map $\mathrm{Norm}_{k/\mathbb{F}_p}$ induces the map $k^* \to U;\ v \mapsto v/v^{\sigma}$. Now according to Hilbert's Theorem 90, for $u \in k^*$ we have $\mathrm{Norm}_{k/\mathbb{F}_p}(u) = 1$ if and only if $u = v/v^{\sigma}$ for some $v \in k^*$. Therefore, we deduce the surjectivity of $\mathrm{Norm}_{k/\mathbb{F}_p}$. □

We need the following lemma which describes totally ramified extensions of $\mathbb{Q}_p$.

Lemma 8.2.6. *Let L be a totally ramified extension of $\mathbb{Q}_p$ with $[L : \mathbb{Q}_p] = m$, $m = 2, 3, 4$. Then the maximal unramified extension L^{un} of L is a Galois extension of $\mathbb{Q}_p^{un}$ with $[L^{un} : \mathbb{Q}_p^{un}] = m$.*

Proof: According to Corollary 3.4 of [13], since $\mathbb{Q}_p$ is complete, L^{un} is a totally ramified extension of $\mathbb{Q}_p^{un}$ with $[L^{un} : \mathbb{Q}_p^{un}] = [L : L_0]$, where $L_0 = L \cap \mathbb{Q}_p^{un}$. But since $L/\mathbb{Q}_p$ is a totally ramified extension, it follows that $L_0 = \mathbb{Q}_p$. Now by virtue of Proposition 5.2.2, since $\mathbb{Q}_p^{un}$ is a Henselian discrete valuation field with algebraically closed residue field, we have $L^{un} = \mathbb{Q}_p^{un}(\sqrt[m]{p})$, and $L^{un}/\mathbb{Q}_p^{un}$ is Galois. □

If $Q = (x, y) \in E(\overline{\mathbb{Q}}_p)$, then K$(Q)$ will denote its field of definition $\mathbb{Q}_p(x, y)$.

Proof of Theorem 8.2.2: The field k will always denote the residue field of K. The image of σ under $\mathrm{Gal}(K/\mathbb{Q}_p) \cong \mathrm{Gal}(k/\mathbb{F}_p)$ will be denoted by σ again. We will divide the proof into several subcases:

(i) Assume that $\Lambda := (\Gamma_1, \ldots, \Gamma_m)$ consists of one $\mathcal{G}_p$-orbit. Then we have the following three subcases:

(1) If Λ consists of one irreducible component of multiplicity-n, then this component Γ is defined over $\mathbb{F}_p$ and $\delta_n(\Gamma) = \psi_E(P)$. We have two subcases:

  - If $n = 1$, then set $D = \overline{\{P\}}$.
  - If $n \geq 2$, then the reduction is additive. There exists a point $x \in \Gamma$ defined over $\mathbb{F}_p$. According to ([20], Exercise 9.2.11 (c)), there exists a point $Q' \in E$ such that $\overline{\{Q'\}} \cap \Gamma = \{x\}$ and $[\mathrm{K}(Q') : \mathbb{Q}_p] = n$. Since x is defined over $\mathbb{F}_p$, it follows that the residue field of $\mathrm{K}(Q')$ is $\mathbb{F}_p$ itself. Therefore, $\mathrm{K}(Q')/\mathbb{Q}_p$ is a totally ramified extension. Let $L = \mathrm{K}(Q')$. According to Lemma 8.2.6, $L^{un} = \mathbb{Q}_p^{un}(\sqrt[n]{p})$. Let $\mathrm{Gal}(L^{un}/\mathbb{Q}_p^{un}) = \langle\lambda\rangle$. By the definition of δ_n we have $P' := \sum_{i=1}^{n} Q'^{\lambda^i} - P \in E^0(\mathbb{Q}_p)$. Since $E^0(\mathbb{Q}_p)$ is divisible by n, see Lemma 8.2.4, we have $P' = nS$ for some $S \in E^0(\mathbb{Q}_p)$. Now our divisor is $D = \overline{\{Q\}}$ where $Q = Q' - S$.

(2) If Λ consists of two irreducible components of multiplicity-m, then E has non-split reduction over $\mathbb{Q}_p$, and this reduction splits over an unramified quadratic extension K. Let $\mathrm{Gal}(K/\mathbb{Q}_p) = \langle\sigma\rangle$. We have $2m = n$, $\Lambda = (\Gamma, \Gamma^\sigma)$ and $\delta_m(\Gamma) + \delta_m(\Gamma^\sigma) = \psi_E(P)$. We have two further subcases to consider:

  - If Γ is of multiplicity-1, then we pick $x \in \Gamma$ to be defined over k. According to Hensel's Lemma, we can lift x to a point $Q' \in E(K)$. Since $\delta_m(\Gamma) + \delta_m(\Gamma^\sigma) = \psi_E(P)$, we have $P' := Q' + Q'^\sigma - P \in E^0(\mathbb{Q}_p)$. Lemma 8.2.5 shows that $P = S + S^\sigma$ for some $S \in E(K)$. Set $D = \overline{\{Q\}}$ where $Q = Q' - S$.
  - If Γ is of multiplicity-2, then E has non-split reduction of type IV* over $\mathbb{Q}_p$. Let x be a point on Γ defined over k. By virtue of ([20], Exercise 9.2.11 (c)), there exists a point $Q' \in E$ such that $\overline{\{Q'\}} \cap \Gamma = \{x\}$ and $K(Q')$ is a totally ramified extension of K with $[K(Q') : K] = 2$. Let $L = K(Q')$, then $[L^{un} : K^{un}] = [L : L \cap K^{un}] = [L : K] = 2$, see ([13], Corollary 3.4). Since K is an unramified extension of $\mathbb{Q}_p$, it follows that $K^{un} = \mathbb{Q}_p^{un}$. Let $\mathrm{Gal}(L^{un}/\mathbb{Q}_p^{un}) = \langle\lambda\rangle$. If we assume that $\delta_2(\Gamma) = \bar{1}$, then by the definition of δ_2 the point $Q' + Q'^\lambda$ reduces on the multiplicity-1 component corresponding to $\bar{1}$. Similarly, $Q'^\sigma + (Q'^\sigma)^\lambda$ reduces on the multiplicity-1 component corresponding to $\bar{2}$. Therefore, we have $P' := Q' + Q'^\lambda + Q'^\sigma + (Q'^\sigma)^\lambda - P \in E^0(\mathbb{Q}_p)$. Since $E^0(\mathbb{Q}_p)$ is divisible by 4, see Lemma 8.2.4, we have $P' = 4S$, then we set $D = \overline{\{Q\}}$ where $Q = Q' - S$.

(3) If Λ consists of three irreducible components of multiplicity-1, then E has non-split reduction of type I_0^* and $c_p = 1$. The reduction splits over an unramified cubic extension K. Let $\mathrm{Gal}(K/\mathbb{Q}_p) = \langle\sigma\rangle$. We have $\Lambda = (\Gamma, \Gamma^\sigma, \Gamma^{\sigma^2})$, where $\Gamma^{\sigma^i} \neq \Gamma^{\sigma^j}$ if $i \neq j$, and $\sum_{i=0}^{2} \delta_1(\Gamma^{\sigma^i}) = \psi_E(P)$. Let $x \in \Gamma$ be a point defined over k. Lift x to a point $Q' \in E(K)$, then we have $P' := Q' + Q'^\sigma + Q'^{\sigma^2} - P \in E^0(\mathbb{Q}_p)$. There is a point $S \in E(\mathbb{Q}_p)$ such that $P' = 3S$, see Lemma 8.2.4. Set $D = \overline{\{Q\}}$ where $Q = Q' - S$.

(ii) Assume that $\Lambda := (\Gamma_1, \ldots, \Gamma_m)$ consists of n $\mathcal{G}_p$-orbits. Then $m = n$, $\mathrm{mult}_{\mathbb{F}_p}(\Gamma_i) = 1$, for each i, and $\sum_{i=1}^{n} \delta_1(\Gamma_i) = \psi_E(P)$. On each Γ_i we pick a point x_i defined over $\mathbb{F}_p$, then we lift it to a point $Q_i \in E(\mathbb{Q}_p)$. We have $P' := \sum Q_i - P \in E^0(\mathbb{Q}_p)$. Set $D = \sum_{i=1}^{n-1} \overline{\{Q_i\}} + \overline{\{Q'_n\}}$ where $Q'_n = Q_n - P'$.

(iii) Assume that $\Lambda := (\Gamma_1, \ldots, \Gamma_m)$ consists of two $\mathcal{G}_p$-orbits and $m \neq 2$. Then we have the following three subcases:

(1) Each $\mathcal{G}_p$-orbit consists of one irreducible component. We have two further subcases:

- $\Lambda = (\Theta, \Gamma)$ where $\mathrm{mult}_{\mathbb{F}_p}(\Theta) = n - 1$ and $\mathrm{mult}_{\mathbb{F}_p}(\Gamma) = 1$. Pick $x \in \Gamma$ to be defined over $\mathbb{F}_p$, then we lift it to $P' \in E(\mathbb{Q}_p)$. According to (i)-(1), there is a divisor D' on $E^{min} \to \mathrm{Spec}\,\mathbb{Z}_p$ such that $D'|_E$ is $\mathbb{Q}_p$-rational, $D'|_E \sim (n-2).0 + (P - P')$, and $D'.\Theta = n - 1$. Set $D = D' + \overline{\{P'\}}$.
- $\Lambda = (\Theta_1, \Theta_2)$ where $\mathrm{mult}_{\mathbb{F}_p}(\Theta_i) = 2$. Let $P_1 \in E(\mathbb{Q}_p)$ be such that $\delta_2(\Theta_1) = \psi_E(P_1)$. Let $P_2 = P - P_1$. According to (i)-(1), there are two divisors D_1, D_2 on $E^{min} \to \mathrm{Spec}\,\mathbb{Z}_p$ such that $D_i|_E$ is $\mathbb{Q}_p$-rational, $D_i|_E \sim 0 + P_i$, and $D_i.\Theta_i = 2$, where $i \in \{1, 2\}$. Set $D = D_1 + D_2$.

(2) One of the $\mathcal{G}_p$-orbits consists of two components exactly. Then the reduction of E splits over K where $\mathrm{Gal}(K/\mathbb{Q}_p) = \{1, \sigma\}$. We have further two subcases:

- $\Lambda = (\Gamma_1, \Gamma_1^\sigma, \Gamma_2, \Gamma_2^\sigma)$ where $\mathrm{mult}_{\overline{\mathbb{F}}_p} \Gamma_i = 1$ and $\Gamma_i \neq \Gamma_i^\sigma$, where $i \in \{1, 2\}$. Let $P_1 \in E(\mathbb{Q}_p)$ be such that $\delta_1(\Gamma_1) + \delta_1(\Gamma_1^\sigma) = \psi_E(P_1)$. Let $P_2 = P - P_1$. According to (i)-(2), there are two divisors D_1, D_2 on $E^{min} \to \mathrm{Spec}\,\mathbb{Z}_p^{un}$ such that $D_i|_E$ is $\mathbb{Q}_p$-rational, $D_i|_E \sim 0 + P_i$, and $D_i.\Gamma_i = D_i.\Gamma_i^\sigma = 1$, where $i \in \{1, 2\}$. Set $D = D_1 + D_2$.
- $\Lambda = (\Theta, \Gamma, \Gamma^\sigma)$ where $m := \mathrm{mult}_{\mathbb{F}_p}(\Theta) \in \{1, 2\}$ and Γ is a multiplicity-1 component such that $\Gamma \neq \Gamma^\sigma$. Let $P_1 \in E(\mathbb{Q}_p)$ be such that $\delta_2(\Theta) = \psi_E(P_1)$. Let $P_2 = P - P_1$. According to (i)-(1) and (i)-(2), there are two divisors D_1, D_2 on $E^{min} \to \mathrm{Spec}\,\mathbb{Z}_p^{un}$ such that $D_i|_E$ is $\mathbb{Q}_p$-rational, $D_1|_E \sim (m-1).0 + P_1$, $D_1.\Theta = m$, $D_2|_E \sim 0 + P_2$ and $D_2.\Gamma = D_2.\Gamma^\sigma = 1$. Set $D = D_1 + D_2$.

(3) One of the $\mathcal{G}_p$-orbits consists of three components exactly. Then E has non-split reduction of type I_0^*, and the reduction splits over K where $\mathrm{Gal}(K/\mathbb{Q}_p) = \{1, \sigma, \sigma^2\}$. Moreover, we have $\Lambda = (\Gamma, \Gamma^\sigma, \Gamma^{\sigma^2}, \Gamma')$ where $\mathrm{mult}_{\mathbb{F}_p} \Gamma' = 1$ and $\Gamma^{\sigma^i} \neq \Gamma^{\sigma^j}$ if $i \neq j$. Let $P' \in E(\mathbb{Q}_p)$ be such that $\delta_1(\Gamma') = \psi_E(P')$. According to (i)-(3), there is a divisors D' on $E^{min} \to \operatorname{Spec} \mathbb{Z}_p^{un}$ such that $D'|_E$ is $\mathbb{Q}_p$-rational, $D'|_E \sim 2.0+(P-P')$ and $D'.\Gamma^{\sigma^i} = 1$. Set $D = D' + \overline{\{P'\}}$.

(iv) Assume that Λ consists of three $\mathcal{G}_p$-orbits and $m \neq 3$. We have two further subcases:

(1) Each $\mathcal{G}_p$-orbit consists of one component, and hence $\Lambda = (\Theta, \Gamma_1, \Gamma_2)$, where $\mathrm{mult}_{\mathbb{F}_p}(\Theta) = 2$ and $\mathrm{mult}_{\mathbb{F}_p}(\Gamma_i) = 1$. Let $P_i \in E(\mathbb{Q}_p)$ be such that $\delta_1(\Gamma_i) = \psi_E(P_i)$, $i \in \{1, 2\}$. Let $P' := P - P_1 - P_2$. According to (i)-(1), there is a divisor D' on $E^{min} \to \operatorname{Spec} \mathbb{Z}_p$ such that $D'|_E$ is $\mathbb{Q}_p$-rational, $D'|_E \sim 0 + P'$, and $D'.\Theta = 2$. Set $D = D' + \overline{\{P_1\}} + \overline{\{P_2\}}$.

(2) One of the $\mathcal{G}_p$-orbits consists of two components. Then the reduction of E splits over K, where $\mathrm{Gal}(K/\mathbb{Q}_p) = \{1, \sigma\}$, and $\Lambda = (\Gamma, \Gamma^\sigma, \Gamma_1, \Gamma_2)$, where $\Gamma \neq \Gamma^\sigma$ and $\mathrm{mult}_{\mathbb{F}_p}(\Gamma_i) = 1$. Let $P_i \in E(\mathbb{Q}_p)$ be such that $\delta_1(\Gamma_i) = \psi_E(P_i)$, $i \in \{1, 2\}$. Let $P' := P - P_1 - P_2$. According to (i)-(2), there is a divisor D' on $E^{min} \to \operatorname{Spec} \mathbb{Z}_p^{un}$ such that $D'|_E$ is $\mathbb{Q}_p$-rational, $D'|_E \sim 0 + P'$, and $D'.\Gamma = D'.\Gamma^\sigma = 1$. Set $D = D' + \overline{\{P_1\}} + \overline{\{P_2\}}$.

□

Now Theorem 8.1.1 follows as a direct consequence of Theorem 8.2.2.

Proof of Theorem 8.1.1: Proposition 8.2.1 shows that if $\mathcal{C}$ is isomorphic to a minimal degree-n-model defined over $\mathbb{Z}_p$, then $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant. So we assume that the tuple $\mathrm{Irr}_{\mathcal{C}}$ is $\mathcal{G}_p$-invariant. The model $\mathcal{C}$ is obtained from E^{min} by contraction via a divisor D, see Theorem 4.0.1. We want to construct a divisor D' such that $\mathcal{O}_{E^{min}}(D) \cong \mathcal{O}_{E^{min}}(D')$ and $H^0(E^{min}, \mathcal{O}_{E^{min}}(mD'))$, $m \geq 1$, is a finitely generated free $\mathbb{Z}_p$-module. Therefore, $\mathcal{C}' = \operatorname{Proj}(\bigoplus_{m=0}^{\infty} H^0(E^{min}, \mathcal{O}_{E^{min}}(mD'))) \to \operatorname{Spec} \mathbb{Z}_p$ is a minimal degree-n-model isomorphic to $\mathcal{C}$, see Theorem 4.2.3.

The tuple $\mathrm{Irr}_{\mathcal{C}} = (\Gamma_1, \ldots, \Gamma_m)$ satisfies the conditions of Theorem 8.2.2, for the condition $\sum_{i=1}^m \delta_{m_i}(\Gamma_i) = \psi_E(P)$ we follow the same argument as in the proof of Lemma 7.2.1. Therefore, there exists a divisor D' on $E^{min} \to \operatorname{Spec} \mathbb{Z}_p^{un}$ such that $(D'|_E)^\sigma = D'|_E$ for every $\sigma \in \mathrm{Gal}(\mathbb{Q}_p^{un}/\mathbb{Q}_P)$, $D'.\Gamma_i = d_i.\, \mathrm{mult}_{\overline{\mathbb{F}}_p} \Gamma_i$, where d_i is the number of iterations of Γ_i in the tuple $(\Gamma_1, \ldots, \Gamma_m)$, and $D'|_E \sim (n-1).0 + P$. It is clear that $D|_E \sim D'|_E$ and $D|_{E^{min}_{\overline{\mathbb{F}}_p}} \sim D'|_{E^{min}_{\overline{\mathbb{F}}_p}}$, hence $\mathcal{O}_{E^{min}}(D) \cong \mathcal{O}_{E^{min}}(D')$, see ([20], Exercise 9.1.13). □

8.3 Counting global models

Let $n \in \{2,3,4\}$. Now we are in a place to find the number N of minimal global degree-n-models for a smooth curve $C \to \mathbb{P}^{n-1}_{\mathbb{Q}}$ defined by a genus one equation of degree n such that $C(\mathbb{Q}_p) \neq \emptyset$ for every prime p. In the previous two sections we managed to find the number N_p of minimal degree-n-models for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$, at each prime $p \geq 5$. In this section, we relate N to the N_p's using Chinese Remainder Theorem.

If $m \in \mathbb{Z}$, then we set

$$P(m) = \{2, 3, p \mid p \geq 5 \text{ is a prime }, p^2 \mid m\}.$$

The main result of this chapter is the following Theorem.

Theorem 8.3.1. *Let $C \to \mathbb{P}^{n-1}_{\mathbb{Q}}$ be a smooth curve defined by a genus one equation of degree n. Assume that $C(\mathbb{Q}_p) \neq \emptyset$ for every prime p. Let $E/\mathbb{Q}$ be the Jacobian elliptic curve of C and let Δ be its minimal discriminant. Let N and N_p denote the numbers of minimal global degree-n-models for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}}$, up to isomorphism, and minimal degree-n-models for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$, up to isomorphism, respectively. Then*

$$N = \prod_{p \in P(\Delta)} N_p.$$

To prove Theorem 8.3.1 we will show that the map λ defined by

$$\begin{array}{ccc} \{\text{minimal global degree-}n\text{-models for } C/\mathbb{Q}\} & \longrightarrow & \displaystyle\prod_{p \in P(\Delta)} \{\text{minimal degree-}n\text{-models for } C/\mathbb{Q}_p\} \\ (\mathcal{C}, \alpha) & \mapsto & ((\mathcal{C}, \alpha), \ldots, (\mathcal{C}, \alpha)) \end{array}$$

is a bijection. Notice that the above two sets of degree-n-models are defined up to isomorphism. Theorem 8.3.1 follows immediately from the bijectivity of λ.

Notice that our work enables us to compute N_p for each prime $p \geq 5$. Before proceeding with the proof of Theorem 8.3.1 we need two Lemmas on matrices.

Lemma 8.3.2. *Let $A \in \mathrm{GL}_n(\mathbb{Q}_p) \cap \mathrm{Mat}_n(\mathbb{Z}_p)$ have coprime entries. Then there exist matrices $U \in \mathrm{GL}_n(\mathbb{Z})$ and $V \in \mathrm{GL}_n(\mathbb{Z}_p)$ such that $A = VDU$, where $D = \mathrm{diag}(p^{r_1}, \ldots, p^{r_{n-1}}, 1)$ and $r_1 \geq \ldots \geq r_{n-1}$.*

Proof: We claim that there exists a matrix $B \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathrm{Mat}_n(\mathbb{Z})$ such that $V' := BA^{-1} \in \mathrm{GL}_n(\mathbb{Z}_p)$. Granted this claim we write the Smith Normal Form for the matrix B, so we have $B = U'D'DU$ where $U, U' \in \mathrm{GL}_n(\mathbb{Z})$, D' is a diagonal matrix whose entries are not divisible by p, and $D = \operatorname{diag}(p^{r_1}, \dots, p^{r_{n-1}}, 1)$, $r_1 \geq \dots \geq r_{n-1}$. Then we set $V := V'^{-1}U'D' \in \mathrm{GL}_n(\mathbb{Z}_p)$, hence we are done.

To prove the claim, assume that $A = (a_{ij})_{i,j}$. Recall that every element in $\mathbb{Z}_p$ can be written uniquely as $\sum_{i\geq 0} a_i p^i$, where $a_i \in \mathbb{Z}$ satisfies $0 \leq a_i \leq p-1$. Let $m > 0$ be an integer large enough such that the matrix $B = (a_{ij} \mod p^m)_{i,j} \in \mathrm{GL}_n(\mathbb{Q}) \cap \mathrm{Mat}_n(\mathbb{Z})$. Now we have $BA^{-1} \equiv \mathrm{id}_n \mod p^m$ and hence $BA^{-1} \in \mathrm{GL}_n(\mathbb{Z}_p)$. □

Lemma 8.3.3. *Let $S = \{p_1, \dots, p_m\}$ be a finite set of primes. Let $U_i \in \mathrm{SL}_n(\mathbb{Z})$ and $m_i > 0$ be an integer, $1 \leq i \leq m$. Then there exists $U \in \mathrm{SL}_n(\mathbb{Z})$ such that $U \equiv U_i \mod p_i^{m_i}$ for every i, $1 \leq i \leq m$.*

Proof: That is Lemma 3.2 of [14]. □

Recall that if R is a ring, then $\mathcal{G}_n(R)$ is the group of transformations of the form $[\mu_n, A_n]$, where $A_n \in \mathrm{GL}_n(R)$, $\mu_n \in R^*$ when $n = 2, 3$, and $\mu_4 \in \mathrm{GL}_2(R)$, see §2.1.

Lemma 8.3.4. *Let ϕ and ϕ' be two minimal $\mathcal{G}_n(\mathbb{Q}_p)$-equivalent genus one equations of degree n with coefficients in $\mathbb{Z}$ and $\mathbb{Z}_p$ respectively. Then ϕ' is $\mathcal{G}_n(\mathbb{Z}_p)$-equivalent to a minimal genus one equation of degree n whose coefficients lie in $\mathbb{Z}$.*

Proof: Assume that ϕ' is obtained from ϕ via $[\mu_n, A_n]$ in $\mathcal{G}_n(\mathbb{Q}_p)$. For $r \in \mathbb{Q}_p^*$, the following transformations are identical:

$$[\mu_n, A_n] = [r^{-2}\mu_n, rA_n] \text{ when } n = 2, 4, \text{ and } [\mu_3, A_3] = [r^{-3}\mu_3, rA_3].$$

Therefore, we can assume that A_n has coprime entries in $\mathbb{Z}_p$. Lemma 8.3.2 allows us to write $A_n = V_n D_n U_n$ where $V_n \in \mathrm{GL}_n(\mathbb{Z}_p)$, $U_n \in \mathrm{GL}_n(\mathbb{Z})$, and $D_n = \operatorname{diag}(p^{r_1}, \dots, p^{r_{n-1}}, 1)$. Similarly, we can write $\mu_4 = \nu_4' \tau_4 \nu_4$ where $\nu_4' \in \mathrm{GL}_n(\mathbb{Z}_p)$, $\nu_4 \in \mathrm{GL}_n(\mathbb{Z})$, and $\tau_4 = \operatorname{diag}(p^{-m}, p^{-n})$.

Let ψ be the $\mathbb{Z}$-integral genus one equation obtained from ϕ via the transformation $[1, U_n]$ when $n = 2, 3$, and via $[\nu_4, U_4]$ when $n = 4$. Then ψ lies in the same $\mathcal{G}_n(\mathbb{Z})$-equivalence class as ϕ. Let ϕ'' be the genus one equation obtained from ψ via the transformation $[\mu_n', D_n]$, where $\mu_2' = (\det D_2)^{-2}$, $\mu_3' = (\det D_3)^{-1}$, and $\mu_4' = \tau_4$. It is clear that ϕ'' is $\mathcal{G}_n(\mathbb{Z}_p)$-equivalent to ϕ'. We claim that ϕ'' has coefficients in $\mathbb{Z}$. If it is not the case, then some of the coefficients of the polynomials defining ϕ'' would lie in $\frac{1}{p^k}\mathbb{Z} \subset \frac{1}{p^k}\mathbb{Z}_p$ for some $k > 0$. But ϕ'' is obtained from ϕ' via $[\omega_n, V_n^{-1}]$, where $\omega_n \in \mathbb{Z}_p^*$ when $n = 2, 3$, and $\omega_4 \in \mathrm{GL}_2(\mathbb{Z}_p)$, and since ϕ' is $\mathbb{Z}_p$-integral, it follows that ϕ'' should be $\mathbb{Z}_p$-integral, which is a contradiction. □

The following lemma, ([28], Chapter IV, Lemma 9.5), will be used to justify our choice of the set of prime numbers $P(\Delta)$.

Lemma 8.3.5. *Let K be a discrete valuation field with normalised valuation ν. Let E be an elliptic curve over K with discriminant Δ. If $\nu(\Delta) = 1$, then E has reduction of type* I_1.

PROOF OF THEOREM 8.3.1: First we will show that the map λ is well defined. Let $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ be two isomorphic minimal global degree-n-models for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}}$. Then $\alpha := \alpha_2^{-1}\alpha_1 : (\mathcal{C}_1)_{\mathbb{Q}_p} \to (\mathcal{C}_2)_{\mathbb{Q}_p}$ is defined by an element in $\mathcal{G}_n(\mathbb{Z}) \hookrightarrow \mathcal{G}_n(\mathbb{Z}_p)$ for every prime p, i.e., $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ have the same image under λ.

To show that λ is injective, let $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ be two minimal global degree-n-models for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}}$ with the same image under λ. We need to show that $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ are isomorphic. Let $\alpha := \alpha_2^{-1}\alpha_1$. The map α is defined by an element $[\mu, A] \in \mathcal{G}_n(\mathbb{Q})$. We can assume that $A \in \mathrm{Mat}_n(\mathbb{Z})$ has coprime entries. Since $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ have the same image under λ, hence $\operatorname{Spec}\mathbb{Z}_p$-isomorphic for every $p \in P(\Delta)$, it follows that $A \in \mathrm{GL}_n(\mathbb{Z}_p)$, and so $p \nmid \det A$. If $p \notin P(\Delta)$, then $E/\mathbb{Q}_p$ has either reduction types I_0 or I_1, see Lemma 8.3.5. But according to Corollary 7.1.2, when E has either reduction types I_0 or I_1, there is a unique degree-n-model for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$. That means that for $p \notin P(\Delta)$, $(\mathcal{C}_1, \alpha_1)$ and $(\mathcal{C}_2, \alpha_2)$ are isomorphic as degree-n-models for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_p}$. Hence $A \in \mathrm{GL}_n(\mathbb{Z}_p)$ for every prime p, in particular $p \nmid \det A$. Thus $\det A = \pm 1$ and $A \in \mathrm{GL}_n(\mathbb{Z})$.

Now we will prove the surjectivity of λ. We will assume without loss of generality that the defining genus one equation ϕ of C has coefficients in $\mathbb{Z}$ and that the associated discriminant is everywhere minimal.

Let $P(\Delta) = \{p_1, \ldots, p_m\}$ where $m \geq 2$. Let $(\mathcal{C}_i \to \operatorname{Spec}\mathbb{Z}_{p_i}, \alpha_i)$, where $1 \leq i \leq m$, be a minimal degree-n-model for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}_{p_i}}$. We want to construct a minimal global degree-n-model $(\mathcal{C}, \alpha)$ for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}}$ such that $\alpha^{-1}\alpha_i : (\mathcal{C}_i)_{\mathbb{Q}_{p_i}} \to \mathcal{C}$ is defined by an element in $\mathcal{G}_n(\mathbb{Z}_{p_i})$ for each i. Let ϕ_i be the defining genus one equation of $\mathcal{C}_i$.

By virtue of Lemma 8.3.4, ϕ_i is $\mathrm{GL}_n(\mathbb{Z}_{p_i})$-equivalent to a genus one equation ϕ'_i with coefficients in $\mathbb{Z}$. In fact, according to the proof of Lemma 8.3.4, ϕ'_i is obtained from ϕ via $[\mu_i, D_iU_i]$ where $D_i = \mathrm{diag}(p_i^{r_{i,1}}, \ldots, p_i^{r_{i,n-1}}, 1)$, $U_i \in \mathrm{GL}_n(\mathbb{Z})$, and μ_i is a scaling element. In fact, we can assume that $U_i \in \mathrm{SL}_n(\mathbb{Z})$ as if $\det U_i = -1$, then we replace ϕ'_i by the $\mathcal{G}_n(\mathbb{Z})$-equivalent genus one equation obtained by acting on ϕ'_i by $V_i = \mathrm{diag}(-1, \ldots, 1)$, and we replace U_i by U_iV_i.

According to Lemma 8.3.3, given integers $m_i > 0$, there exists a matrix $U \in \mathrm{SL}_n(\mathbb{Z})$ such that $U \equiv U_i \mod p_i^{m_i}$ for every i. We note that $\prod_{i=1}^m D_iUU_j^{-1}D_j^{-1} \equiv \prod_{i\neq j} D_i \mod p_j^{m_j}$. Therefore, the genus one equation ψ obtained from ϕ via the transformation $[\prod_{i=1}^m \mu_i, \prod_{i=1}^m D_iU]$ is $\mathcal{G}_n(\mathbb{Z}_{p_j})$-equivalent to ϕ'_j, for every j.

Now we want to show that ψ is $\mathbb{Z}$-integral. This will imply that ψ defines a minimal global degree-n-model for $C \to \mathbb{P}^{n-1}_{\mathbb{Q}}$ which is $\operatorname{Spec}\mathbb{Z}_{p_j}$-isomorphic to $(\mathcal{C}_j, \alpha_j)$, for every j. Hence we will be done with the surjectivity. Assume on the contrary that ψ is not $\mathbb{Z}$-integral. Since ψ is obtained from the $\mathbb{Z}$-integral genus one equation ϕ via $[\prod_{i=1}^{m} \mu_i, \prod_{i=1}^{m} D_i U]$, it follows that some of the coefficients of the defining polynomials of ψ lie in $\frac{1}{b}\mathbb{Z}$, $b = p_1^{l_1} p_2^{l_2} \dots p_m^{l_m}$, where $l_i \geq 0$ and $l_j > 0$ for some $j \in \{1, \dots, m\}$. We have shown that ψ is $\mathcal{G}_n(\mathbb{Z}_{p_j})$-equivalent to the $\mathbb{Z}$-integral genus one equation ϕ'_j. It follows that ψ is $\mathbb{Z}_{p_j}$-integral, which is a contradiction. □

We give the following examples which show that the number of minimal global degree-n-models, up to isomorphism, for a given smooth genus one curve agrees with the result given by Theorem 8.3.1. Since our counting results work for minimal degree-n-models for genus one curves defined over $\mathbb{Q}_p$ when $p \geq 5$, we choose our examples such that the number of minimal degree-n-models defined over $\mathbb{Z}_m$, where $m \in \{2, 3\}$, is 1. Therefore, there is no contribution of the primes $2, 3$ towards the counting recipe given in Theorem 8.3.1.

Moreover, the genus one equations of degree 2 and 3 given below are not reduced. In fact, we moved the zeros of the defining polynomials to our favorite places to allow applying diagonal matrices whose entries are powers of the bad primes of the Jacobian. The calculations included in the examples below are performed using MAGMA, see [6]. $N_n(T)$ will denote the number of minimal degree-n-models when the reduction of the Jacobian is of type T, see Corollary 8.1.4.

Example 8.3.6. The elliptic curve $E : y^2 + xy = x^3 - x^2 + 6603008\, x - 1118312959$ has bad primes 5, 7, and 11. E has reduction of types II^*, non-split I_7, and III^* at these primes respectively. Consider the following minimal global genus one equation ϕ_2 of degree 2.

$$\begin{aligned} y^2 = f(x,z) = 8200182806525733 65\, x^4 \quad &+ \quad 405939973623867606\, x^3 z + \\ 75358348438862775\, x^2 z^2 \quad &+ \quad 6217537401171250\, x z^3 + 192369718165625 z^4. \end{aligned}$$

The equation ϕ_2 defines an everywhere locally soluble element C in the 2-Selmer group of E. Let $\mathcal{C}$ be the minimal global degree-2-model defined by ϕ_2.

We claim that $\mathcal{C} \to \operatorname{Spec} \mathbb{Z}_2$ is the unique minimal degree-2-model for C. Assume on the contrary that there is another minimal degree-2-model for $C/\mathbb{Q}_2$ defined by a genus one equation ϕ'. The equation ϕ' is obtained from ϕ via an element $(\alpha, A) \in \mathcal{G}_2(\mathbb{Q}_2)$. Smith Normal Forms for matrices allow us to write $A = VBU$, where $U, V \in \mathrm{GL}_2(\mathbb{Z}_2)$ and B is a diagonal matrix whose entries are powers of 2. Therefore, $f(x,z) \mod 2$ has at least one zero, and the matrix U will move this zero to either $(0,1)$ or $(1,0)$. But $f(x,z) \equiv (x^2 + xz + z^2)^2 \mod 2$, in particular $f(x,z)$ has no zeros over $\mathbb{F}_2$ which is a contradiction. We deduce that the number of minimal degree-2-models for $C/\mathbb{Q}_2$ is 1.

The model $\mathcal{C} \to \operatorname{Spec} \mathbb{Z}_3$ is smooth, and hence it is the unique degree-2-model for $C/\mathbb{Q}_3$, see Corollary 5.1.5. Hence the number of minimal global degree-2-models for C is $N_2(\mathrm{II}^*) \times N_2(\mathrm{I}_7) \times N_2(\mathrm{III}^*) = 3 \times 4 \times 2 = 24$, see Theorem 8.3.1.

The defining genus one equations of the minimal global degree-2-models for C are obtained from ϕ_2 via the following transformations in $\mathcal{G}_2(\mathbb{Q})$.

$$[1/(5^{2i} \times 7^{2j} \times 11^{2k}), \operatorname{diag}(5^i \times 7^j, 11^k)], \text{ where } 0 \leq i \leq 2,\ 0 \leq j \leq 3,\ 0 \leq k \leq 1.$$

Example 8.3.7. Consider the elliptic curve $E : y^2 + xy = x^3 - x^2 - 617x + 5916$. It has reduction of types III^* and I_2 at its bad primes 5 and 19 respectively. The following minimal global genus one equation ϕ_3 of degree 3 defines an everywhere locally soluble element C in the 3-Selmer group of E.

$$\begin{aligned} 21686353648850\, x^3 &+ 234081254700017\, x^2y + 9338329782950\, x^2z + 842219868972245\, xy^2 + \\ 67198263238095\, xyz &+ 1340388284750\, xz^2 + 1010096983050575\, y^3 + 120889031707155\, y^2z + \\ 4822691362750\, yz^2 &+ 64131409475\, z^3 = 0. \end{aligned}$$

The minimal degree-3-model $\mathcal{C} \to \operatorname{Spec} \mathbb{Z}_m,\ m = 2, 3$, defined by ϕ_3 is smooth. Therefore, according to Corollary 5.1.5, this model $\mathcal{C}$ is the unique minimal degree-3-model for $C/\mathbb{Q}_m$. Hence the number of minimal global degree-3-models for C is $N_3(\mathrm{III}^*) \times N_3(\mathrm{I}_2) = 6 \times 2 = 12$, see Theorem 8.3.1. These models have defining genus one equations obtained from ϕ_3 via the following transformations in $\mathcal{G}_3(\mathbb{Q})$.

$$\begin{array}{ccc} [1, \mathrm{id}_3], & [1/5, \operatorname{diag}(5,1,1)], & [1/5, \operatorname{diag}(1,5,1)], \\ [1/25, \operatorname{diag}(5,5,1)], & [1/25, \operatorname{diag}(5,1,5)], & [1/25, \operatorname{diag}(1,25,1)], \\ [1/19, \operatorname{diag}(1,1,19)], & [1/95, \operatorname{diag}(5,1,19)], & [1/95, \operatorname{diag}(1,5,19)], \\ [1/475, \operatorname{diag}(5,5,19)], & [1/475, \operatorname{diag}(5,1,95)], & [1/475, \operatorname{diag}(1,25,19)]. \end{array}$$

Example 8.3.8. Let $E : y^2 + xy + y = x^3 - 4\,x - 3$. The curve $C : y^2 = -3\,x^4 + 2\,x^3 + 7\,x^2 - 2\,x - 3$ represents an element in the 2-Selmer group of E. A second 2-descent on C gives the following minimal global genus one equation ϕ_4 of degree 4.

$$\begin{aligned} x_1^2 - x_1x_3 - x_2^2 + x_2x_4 + x_3^2 &= 0, \\ x_1x_4 + x_2^2 + x_2x_3 - x_2x_4 + x_3^2 - x_3x_4 &= 0. \end{aligned}$$

The equation ϕ_4 defines a smooth genus one curve $C_4/\mathbb{Q}$. The discriminant Δ of E is 185. Therefore, we have $P(\Delta) = \{2, 3\}$. But the equation ϕ_4 defines a smooth minimal degree-4-model $\mathcal{C} \to \operatorname{Spec} \mathbb{Z}_m,\ m = 2, 3$. Therefore, according to Corollary 5.1.5, this model $\mathcal{C}$ is the unique minimal degree-4-model for $C_4/\mathbb{Q}_m$. Hence the minimal global degree-4-model $\mathcal{C} \to \operatorname{Spec} \mathbb{Z}$ defined by ϕ_4 is unique, see Theorem 8.3.1.

Appendix A

Insoluble degree-n-models

In this appendix K will denote a complete discrete valuation field with ring of integers $\mathcal{O}_K$ and normalised valuation ν. We will fix a uniformiser t and write k for $\mathcal{O}_K/t\mathcal{O}_K$. We will assume that k is algebraically closed and that $\operatorname{char} k = p \neq 2, 3$. We set $S = \operatorname{Spec} \mathcal{O}_K$.

We count the number of minimal degree-n-models for a curve C given by a genus one equation of degree n when $C(K) = \emptyset$.

A.1 Special fibers

Let C be a smooth genus one curve over K given by a minimal genus one equation ϕ of degree $n = 2, 3, 4$, with $C(K) = \emptyset$. Let $\mathcal{C}$ be a degree-n-model for $C \to \mathbb{P}^{n-1}_K$. We start by classifying the possibilities of the special fiber $\mathcal{C}_k$.

Proposition A.1.1. *Let C be a smooth projective curve over K. Then $C(K) \neq \emptyset$ if and only if C admits a model $\mathcal{C}$ over S whose special fiber $\mathcal{C}_k$ contains an irreducible component of multiplicity* 1.

Proof: See ([20], Exercise 10.1.5). □

Corollary A.1.2. *Let C be a smooth curve over K given by a genus one equation of degree $n \geq 2$. Assume that $C(K) = \emptyset$. Let $\mathcal{C}$ be a degree-n-model for $C \to \mathbb{P}^{n-1}_K$. Then $\mathcal{C}_k$ is*

(i) if $n = 2$, a double line

(ii) if $n = 3$, a triple line

(iii) if $n = 4$, either a double conic, two double lines, or a quadruple line.

Proof: We consider the possibilities for $\mathcal{C}_k$ given in §3.2. Since $C(K) = \emptyset$, $\mathcal{C}_k$ must not contain multiplicity-1 components, see Proposition A.1.1. The only such forms of the special fiber are the ones given in the statement of the corollary. □

Let E be an elliptic curve over K with reduction type T, where

$$T \in \{\mathrm{I}_m, \mathrm{I}_m^*,\ m \geq 0, \mathrm{II}, \mathrm{II}^*, \mathrm{III}, \mathrm{III}^*, \mathrm{IV}, \mathrm{IV}^*\}.$$

If $l \geq 0$ is an integer, then we denote by lT the new type obtained from T by multiplying all the multiplicities of T by l.

We will state some facts which will help us determine the reduction type of C when $C(K) = \emptyset$.

Theorem A.1.3. *Let X be a smooth projective curve of genus 1 over K and let E be its Jacobian. Let $X^{min} \to S$ and $E^{min} \to S$ be the minimal proper regular models of X and E respectively. Let m denote the order of the element of $H^1(K, E)$ corresponding to the torsor X. If T denotes the type of E, then X is of type mT.*

Proof: See ([21], Theorem 6.6). □

The following proposition is Corollary 7.4 in [21].

Proposition A.1.4. *Let X be a smooth projective curve of genus 1 over K with minimal proper regular model X^{min}. Assume that the Jacobian E of X has additive reduction. Let $\Gamma_1, ..., \Gamma_n$ be the irreducible components of X_k^{min} of respective multiplicities $r_1, ..., r_n$. If $r := \gcd(r_1, ..., r_n) > 1$, then $r = p^s$ for some $s \geq 1$ where $p = \operatorname{char} k$.*

Theorem A.1.5. *Let K be a complete discrete valuation field with ring of integers $\mathcal{O}_K$ and algebraically closed residue field k with $\operatorname{char} k = p \neq 2, 3$. Let C be a smooth genus one curve given by a minimal genus one equation ϕ of degree $n = 2, 3, 4$. Assume moreover that $C(K) = \emptyset$. Then the Jacobian E of C has reduction type I_m, $m \geq 0$. Moreover, the minimal proper regular model C^{min} of C has special fiber of type*

(i) $2\mathrm{I}_m$ if ϕ is of degree 2,

(ii) $3\mathrm{I}_m$ if ϕ is of degree 3,

(iii) either $2\mathrm{I}_m$ or $4\mathrm{I}_m$ if ϕ is of degree 4.

PROOF: Theorem A.1.3 implies that C^{min} has reduction type lT where l is the order of the element of $H^1(K,E)$ corresponding to the torsor C and T is the reduction type of E. The order of an element of $H^1(K,E)$ is equal to the greatest common divisor of the degrees of K-rational divisors on C. Since $C(K)=\emptyset$, the order l of C in $H^1(K,E)$ is n when $n=2,3$, and it is either 2 or 4 when $n=4$.

Now we want to find T. Assume on the contrary that E has additive reduction. Then according to Proposition A.1.4, since l is the greatest common divisor of the irreducible components of C^{min}_k because C^{min}_k is of the form lT, we have $l=p^s$ for some $s>1$, which is a contradiction as $p\neq 2,3$. Therefore, the reduction type T of E is $\mathrm{I}_m,\ m\geq 0$.

□

A.2 Insoluble degree-n-models, $n=2,3$

Recall that if $f(x_1,\dots,x_m)\in\mathcal{O}_K[x_1,\dots,x_m]$, then we write $f_i(x_1,\dots,x_m)=f(x_1,\dots,x_m)/t^i$. We start by describing the special fiber of a minimal degree-n-model for a smooth genus one curve $C\to\mathbb{P}^{n-1}_K$, for $n=2,3$, where $C(K)=\emptyset$.

Lemma A.2.1. *Let ϕ be a minimal genus one equation of degree $n=2,3$. Assume that ϕ defines a smooth curve C over K with $C(K)=\emptyset$. Let $\mathcal{C}$ be the minimal degree-n-model for $C\to\mathbb{P}^{n-1}_K$ defined by ϕ. Assume that $\mathcal{C}_k$ contains the multiplicity-n irreducible component $\{y=0\}$. Then*

(i) if $\phi: y^2=f(x,z)$ where $\nu(f)=1$, then $f_1(x,z)=(\alpha_1x-\alpha_2z)^4 \mod t$ for some $\alpha_i\in k$,

(ii) if $\phi: by^3+f(x,z)y^2+g(x,z)y+h(x,z)$ where $\nu(b)=0,\nu(f),\nu(g)\geq 1,\nu(h)=1$, then $h_1(x,z)=(\alpha_1x-\alpha_2z)^3 \mod t$ for some $\alpha_i\in k$.

PROOF: (i) If $f_1(x,z) \mod t$ contains a linear factor, i.e., we can assume $f_1(x,z)=xf'(x,z) \mod t$ where $x\nmid f'(x,z)$, then Hensel's Lemma allows us to lift 0 to $x_0\in\mathcal{O}_K$ with $f_1(x_0,1)=0$. Therefore, $(x_0,0,1)\in C(K)$, a contradiction.

Assume $f(x,1)=ax^4+bx^3+cx^2+dx+e$. If $f_1(x,z) \mod t$ contains two quadratic factors, i.e., we can assume $f_1(x,z)=x^2z^2 \mod t$, then $t^2\mid a,b,d,e,\ t\mid\mid c$. Therefore, $\nu(c_4)=2,\nu(c_6)=3$ where c_4,c_6 are the invariants associated to ϕ, see §2.1. That contradicts the fact that the Jacobian elliptic curve $y^2=x^3-27c_4x-54c_6$ has reduction of type $\mathrm{I}_m,\ m\geq 0$, see Theorem A.1.5.

(ii) If $h_1(x,z) \mod t$ contains a linear factor, i.e., we can assume $h_1(x,z)=xh'(x,z) \mod t$ where $x\nmid h'(x,z)$, then Hensel's Lemma allows us to lift 0 to $x_0\in\mathcal{O}_K$ with $h_1(x_0,1)=0$. Therefore, $(x_0:0:1)\in C(K)$, which is a contradiction. □

Remark A.2.2. If C is given by a minimal genus one equation $y^2 = f(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$ and $C(K) = \emptyset$, then we can assume that $f_1(x,z) = x^4 \mod t$, see Lemma A.2.1 (*i*). Therefore, $\nu(a) = 1$ and $\min\{\nu(b), \nu(c), \nu(d), \nu(e)\} \geq 2$. Indeed, $\nu(e) \geq 3$ since otherwise $f_2(tx,z) \not\equiv 0 \mod t$ which contradicts Corollary A.1.2 (*i*).

If $\nu(e) \geq 4$ then $\nu(d) = 2$ otherwise $f_2(tx,z)$ is not minimal, but then $f_3(tx,z)$ has a linear factor which contradicts Lemma A.2.1 (*i*). Therefore, $\nu(e) = 3$. Moreover, if $\nu(d) = 2$ then again $f_3(tx,z)$ has a linear factor.

To summarise, we can assume that $\nu(a) = 1, \min\{\nu(b), \nu(c)\} \geq 2, \nu(d) \geq 3$, and $\nu(e) = 3$.

Let C be given by a minimal genus one equation $F(x,y,z) = by^3 + f(x,z)y^2 + g(x,z)y + h(x,z) = 0$ where $g(x,z) = a_2x^2 + mxz + c_2z^2$ and $h(x,z) = ax^3 + a_3x^2z + c_1xz^2 + cz^3$. We will assume that $C(K) = \emptyset,\ \nu(b) = 0, \nu(f), \nu(g) \geq 1$ and $\nu(h) = 1$. Then according to Lemma A.2.1 (*ii*) we can assume that $h_1(x,z) = x^3 \mod t$ and therefore $\nu(a) = 1,\ \min\{\nu(a_3), \nu(c_1), \nu(c)\} \geq 2$ and $c \neq 0$.

Indeed, we have $\nu(c) = 2$ and $\nu(c_2) \geq 2$, since otherwise the equation $F_2(tx, ty, 1) = 0$ would define a minimal degree-3-model for $C \to \mathbb{P}^2_K$ whose special fiber is a double line and a line which contradicts Corollary A.1.2 (*ii*).

A curve defined by a genus one equation with coefficients of the above valuations is called a *critical model* in [11].

Theorem A.2.3. *Assume that C is a smooth curve given by a minimal genus one equation ϕ_1 of degree $n = 2, 3$. Assume moreover that $C(K) = \emptyset$. Then the number of minimal degree-n-models for $C \to \mathbb{P}^{n-1}_K$ is n.*

PROOF: $n = 2$: The equation $\phi_1 : y^2 = f(x,1) = ax^4 + bx^3 + cx^2 + dx + e$ where $t \mid\mid f(x)$ defines a minimal degree-2-model $\mathcal{C}_1$ for C. According to Remark A.2.2 we are allowed to assume that $\nu(a) = 1, \min\{\nu(b), \nu(c)\} \geq 2, \nu(d) \geq 3$, and $\nu(e) = 3$. We claim that the models $(\mathcal{C}_1, \mathrm{id})$ and $(\mathcal{C}_2, \alpha_2)$, where $\mathcal{C}_2$ is given by $\phi_2 : y^2 = f_2(tx, 1)$ and hence α_2 is defined by the matrix $\mathrm{diag}(t, 1)$, are the only minimal degree-2-models for $C \to \mathbb{P}^1_K$. So assume that $(\mathcal{C}_3, \alpha_3)$ is another minimal degree-2-model for $C \to \mathbb{P}^1_K$. We will show that $\mathcal{C}_3$ is isomorphic to either $\mathcal{C}_1$ or $\mathcal{C}_2$. Assume that $\mathcal{C}_3$ is defined by the genus one equation $\phi_3 : y^2 = \frac{1}{(\det A)^2} f(a_1(x,z), a_2(x,z))$ where

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

and $a_i(x,z) = a_{1i}x + a_{2i}z,\ i = 1, 2$, moreover we will assume that A has coprime entries. If $t \mid \det A$, then $t^2 \mid f(a_1(x,z), a_2(x,z))$ because ϕ_3 is integral, hence $t \mid a_1(x,z)$ because

$\nu(a) = 1$. If $t^2 \mid \det A$, then $t^4 \mid f(a_1(x,z), a_2(x,z))$ and so $t \mid a_2(x,z)$ because $\nu(e) = 3$. Therefore, if $\det A$ is divisible by a power of t which is greater than 1, then t divides each entry of A which contradicts our assumption. Thus we can assume that if $t \mid \det A$, then $t \mid\mid \det A$.

Now assume that $\mathcal{C}_3$ is not isomorphic to $\mathcal{C}_1$, hence $t \mid\mid \det A$. We will show that $\mathcal{C}_3$ must be isomorphic to $\mathcal{C}_2$. Writing A in a Smith Normal Form we can assume that $A = B'TB$, where

$$B' \in \mathrm{GL}_2(\mathcal{O}_K),\ T = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix},\ \text{and } B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K).$$

We apply the matrix B'^{-1} which does not change the isomorphism class of $\mathcal{C}_3$. So we can assume without loss of generality that $A = TB$. The defining genus one equation $\phi_3 : y^2 = f'(x,z)$ of $\mathcal{C}_3$ satisfies $f'(x,z) = TBT^{-1}.f_2(tx,z)$. So we only need to show that $TBT^{-1} \in \mathrm{GL}_2(\mathcal{O}_K)$. Noting that

$$TBT^{-1} = \begin{pmatrix} b_{11} & tb_{12} \\ b_{21}/t & b_{22} \end{pmatrix},$$

we have to show that $t \mid b_{21}$. Let e' be the coefficient of the z^4-term in

$$f'(x,z) = f(t(b_{11}x + b_{21}z/t), tb_{12}x + b_{22}z)/t^2.$$

Hence $e' = f'(b_{21}, b_{22})/t^2 \equiv ab_{21}^4/t^2 \mod \mathcal{O}_K$. Since $\nu(a) = 1$, we conclude that $t \mid b_{21}$, since otherwise ϕ_3 is not integral.

$n = 3$: Let ϕ_1 be given by $F(x,y,z) = by^3 + f(x,z)y^2 + g(x,z)y + h(x,z) = 0$ where $g(x,z) = a_2x^2 + mxz + c_2z^2,\ h(x,z) = ax^3 + a_3x^2z + c_1xz^2 + cz^3$, and $\nu(f), \nu(g), \nu(h) \geq 1$. By virtue of Remark A.2.2, we can assume that $\nu(a) = 1,\ \min\{\nu(a_3), \nu(c_1), \nu(c_2)\} \geq 2, \nu(c) = 2$, and $c \neq 0$. We claim that the models $(\mathcal{C}_1, \mathrm{id}), (\mathcal{C}_2, \alpha_2)$ and $(\mathcal{C}_3, \alpha_3)$ given by the genus one equations $F(x,y,z) = 0, \phi_2 : F_1(x,ty,z) = 0$, and $\phi_3 : F_2(tx,ty,z) = 0$ respectively are the only degree-3-models for $C \to \mathbb{P}^2_K$. So assume that $(\mathcal{C}_4, \alpha_4)$ is another degree-3-model for $C \to \mathbb{P}^2_K$ and we want to prove that $\mathcal{C}_4$ is isomorphic to one of the $\mathcal{C}_i$'s, $i = 1,2,3$. Let $\mathcal{C}_4$ be given by $\phi_4 : \frac{1}{\det A}F(a_1(x,y,z), a_2(x,y,z), a_3(x,y,z)) = 0$ where

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

and $a_i(x,y,z) = a_{1i}x + a_{2i}y + a_{3i}z,\ i = 1,2,3$, moreover we assume that A has coprime entries. If $t^3 \mid \det A$, then $t \mid a_2(x,y,z)$ because ϕ_4 is integral and $\nu(b) = 0$, similarly $t \mid a_1(x,y,z)$ because $\nu(a) = 1$, and $t \mid a_3(x,y,z)$ because $\nu(c) = 2$, i.e., if $t^3 \mid \det A$, then that contradicts our assumption that A has coprime entries. Therefore, $\nu(\det A) \leq 2$. Now we assume that $\mathcal{C}_4$ is not isomorphic to $\mathcal{C}_1$, hence we can assume that A is written as TB where

$$T = \begin{pmatrix} t^{r_1} & 0 & 0 \\ 0 & t^{r_2} & 0 \\ 0 & 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \in \mathrm{GL}_3(\mathcal{O}_K),$$

and $r_1 \geq r_2, r_1 + r_2 \leq 2$. We first eliminate the possibility of $r_1 = 2, r_2 = 0$. That is because if we have a genus one equation of degree 3 which is K-equivalent to ϕ_1 and given by

$$\begin{aligned} F'(x,y,z) = Ax^3 + By^3 + Cz^3 &+ A_2X^2Y + A_3X^2Z + B_1Y^2X \\ &+ B_3Y^2Z + C_1Z^2X + C_2Z^2Y + MXYZ \end{aligned}$$

such that $F'_2(t^2x,y,z) \in \mathcal{O}_K[x,y,z]$, then we have $t^2 \mid B, C, B_3, C_2$. But the model corresponding to the integral genus one equation $F'_2(t^2x,y,z) = 0$ has a triple line special fiber, see Corollary A.1.2, and the reduction of $F'_2(t^2x,y,z) \mod t$ contains no y^3, z^3-terms, therefore $t \mid A_2, A_3, B_1, C_1, M$. Now the equation $F'(x,y,z) = 0$ is not minimal as we can minimise it using the transformation $F'_2(tx,y,z)$. So either $r_1 = 1, r_2 = 0$ or $r_1 = r_2 = 1$.

We will show that if $r_1 = r_2 = 1$, then $\mathcal{C}_4$ is isomorphic to $\mathcal{C}_3$. The case when $r_1 = 1, r_2 = 0$ is similar and we have $\mathcal{C}_4$ is isomorphic to $\mathcal{C}_2$. Let $r_1 = r_2 = 1$. We need to show that $TBT^{-1} \in \mathrm{GL}_3(\mathcal{O}_K)$. We notice that for $r_1 = r_2 = 1$ we have

$$TBT^{-1} = \begin{pmatrix} b_{11} & b_{12} & tb_{13} \\ b_{21} & b_{22} & tb_{23} \\ b_{31}/t & b_{32}/t & b_{33} \end{pmatrix},$$

so we have to prove that $t \mid b_{31}, b_{32}$. $\mathcal{C}_4$ is defined by the equation

$$TBT^{-1}.F_2(tx,ty,z) = F(t(b_{11}x+b_{21}y+b_{31}z/t), t(b_{12}x+b_{22}y+b_{32}z/t), tb_{13}x+tb_{23}y+b_{33}z)/t^2 = 0.$$

In the above polynomial the coefficient of z^3 is $c' = F(b_{31}, b_{32}, b_{33})/t^2$. If $\nu(b_{32}) = 0$, then since $\nu(b) = 0$, we would have $\nu(c') = -2$, which contradicts the integrality of the genus one equation above. Hence $\nu(b_{32}) \geq 1$. Now if $\nu(b_{31}) = 0$, then since $\nu(a) = 1$, we would have $\nu(c') = -1$, which is again a contradiction. Therefore, $t \mid b_{31}, b_{32}$. □

A.3 Insoluble degree-4-models

Let ϕ be a genus one equation of degree 4 given by $\{F(x_1,\dots,x_4)=G(x_1,\dots,x_4)=0\}$ where F and G are given by the following polynomials respectively

$$\begin{aligned} a_1x_1^2 &+ a_2x_1x_2+a_3x_1x_3+a_4x_1x_4+a_5x_2^2+a_6x_2x_3+a_7x_2x_4+a_8x_3^2+a_9x_3x_4+a_{10}x_4^2, \\ b_1x_1^2 &+ b_2x_1x_2+b_3x_1x_3+b_4x_1x_4+b_5x_2^2+b_6x_2x_3+b_7x_2x_4+b_8x_3^2+b_9x_3x_4+b_{10}x_4^2. \end{aligned} \tag{A.1}$$

Assume that ϕ defines a smooth curve C with $C(K)=\emptyset$. Then Corollary A.1.2 (*iii*) implies that the special fiber of any degree-4-model for $C\to\mathbb{P}^3_K$ is either a double conic, two double lines, or a quadruple line.

In Chapter 3 we introduced conditions for a degree-4-model for C to be normal and we determined its singular locus. We are going to investigate the singular locus of a minimal degree-4-model for $C\to\mathbb{P}^3_K$ under the assumption that $C(K)=\emptyset$. Then we show that unlike the case when $n=2,3$, the number of minimal degree-4-models for $C\to\mathbb{P}^3_K$ can be arbitrarily large.

We start by stating the following version of Hensel's Lemma.

Lemma A.3.1. *Let $f_1,\dots,f_r\in\mathcal{O}_K[x_1,\dots,x_n], r\le n$. Let $\underline{x}\in\mathcal{O}_K^n$ be such that $f_i(\underline{x})=0 \mod t$ for every i and*

$$\operatorname{rank}(\frac{\partial f_i}{\partial x_j}(\underline{x}) \mod t)\ge r.$$

Then there exists a $\underline{y}\in\mathcal{O}_K^n$ such that $\underline{y}\equiv\underline{x} \mod t$ and $f_i(\underline{y})=0$ for every i.

Again f_i will denote f/t^i.

Lemma A.3.2. *Let C be a smooth genus one curve over K defined by an integral genus one equation $\phi: F=G=0$ of degree 4 as in equation (A.1). Assume that $C(K)=\emptyset$. Assume moreover that ϕ defines a minimal degree-4-model $\mathcal{C}$ for $C\to\mathbb{P}^3_K$.*

(i) Assume that $\mathcal{C}_k$ is a double conic with $\tilde{F}=x_1^2$ and $\tilde{G}=x_2^2+x_3x_4$. Then $\tilde{F}_1(0,x_2x_4,-x_2^2,x_4^2)=(\alpha_1x_2-\alpha_2x_4)^4$ where $\alpha_i\in k$.

(ii) Assume that $\mathcal{C}_k$ is two double lines given by $\{x_1=x_2=0\}$ and $\{x_1=x_4=0\}$. Then both $\tilde{F}_1(0,0,x_3,x_4)$ and $\tilde{F}_1(0,x_2,x_3,0)$ are squares.

(iii) Assume that $\mathcal{C}_k$ is a quadruple line given by $\tilde{F}=x_1^2$ and $\tilde{G}=x_2^2+x_1x_3$. Then $\tilde{F}_1(0,0,x_3,x_4)$ is a square.

(iv) Assume that $\mathcal{C}_k$ is a quadruple line given by $\tilde{F} = x_1^2$ and $\tilde{G} = x_2^2$. Then both $\tilde{F}_1(0,0,x_3,x_4)$ and $\tilde{G}_1(0,0,x_3,x_4)$ are squares.

Proof: Set

$$\begin{aligned} f(x_2,x_3) &= F_1(0,x_2,x_3,1) = a_{5,1}x_2^2 + a_{6,1}x_2x_3 + a_{7,1}x_2 + a_{8,1}x_3^2 + a_{9,1}x_3 + a_{10,1}, \\ f'(x_2,x_3) &= G(0,x_2,x_3,1) = b_5x_2^2 + b_6x_2x_3 + b_7x_2 + b_8x_3^2 + b_9x_3 + b_{10}. \end{aligned}$$

(i) Let $h(x_2,x_4) = F(0,x_2x_4,-x_2^2,x_4^2)$. Assume that $h_1(x_2,x_4) \mod t$ has a simple factor. Using a matrix in $\mathrm{GL}_4(\mathcal{O}_K)$ we can assume that $h_1(x_2,x_4) = x_2g(x_2,x_4)$, where $x_2 \nmid g(x_2,x_4)$, therefore $\nu(a_7) = 1$ and $\nu(a_{10}) \geq 2$.

we have $f(0,0) = f'(0,0) = 0 \mod t$ and

$$J_{(f,f')} := \begin{pmatrix} \frac{\partial f}{\partial x_2} & \frac{\partial f}{\partial x_3} \\ \frac{\partial f'}{\partial x_2} & \frac{\partial f'}{\partial x_3} \end{pmatrix}(0,0) = \begin{pmatrix} a_{7,1} & a_{9,1} \\ b_7 & 1 \end{pmatrix} \equiv \begin{pmatrix} \tilde{a}_{7,1} & 0 \\ 0 & 1 \end{pmatrix} \mod t.$$

Lemma A.3.1 implies that there are $x,y \in \mathcal{O}_K$ such that $f(x,y) = f'(x,y) = 0$ which means that $(0 : x : y : 1) \in C(K)$, whence a contradiction.

When $a_5 \neq a_9$, the polynomial $h_1(x_2,x_4)$ can have two double factors mod t, in this case we can use a matrix in $\mathrm{GL}_4(\mathcal{O}_K)$ to assume that $h_1(x_2,x_4) = x_2^2x_4^2 \mod t$, in particular we assume that $\min\{\nu(a_6),\nu(a_7),\nu(a_8),\nu(a_{10})\} \geq 2$ and $\nu(a_5 - a_9) = 1$. But then the degree-4-model defined by the genus one equation

$$F_1(tx_1,x_2,x_3,x_4) = G(tx_1,x_2,x_3,x_4) = 0$$

has special fiber with equations $a_{5,1}x_2^2 + a_{9,1}x_3x_4 = l(x_2,x_4)^2 + x_3l'(x_2,x_4) = 0$, where l and l' are linear factors. The latter special fiber contradicts either Corollary A.1.2 (iii) or Theorem A.1.5 (iii).

(ii) We can assume that $\tilde{F} = x_1^2$ and $\tilde{G} = x_2x_4 + \mu x_1x_3$ where $\mu \in k$. If $\tilde{F}_1(0,0,x_3,x_4)$ consists of two distinct linear factors, then we can assume that $\nu(a_9) = 1$ and $\nu(a_8),\nu(a_{10}) \geq 2$. Now we have

$$J_{(f,f')} \equiv \begin{pmatrix} \tilde{a}_{7,1} & \tilde{a}_{9,1} \\ 1 & 0 \end{pmatrix} \mod t.$$

That implies the existence of a rational point on C which is a contradiction. We follow the same argument to prove that $\tilde{F}_1(0,x_2,x_3,0)$ is a square.

$(iii),(iv)$ Assume that $\tilde{F}_1(0,,0,x_3,x_4)$ consists of two distinct linear factors. We can use a matrix in $\mathrm{GL}_4(\mathcal{O}_K)$ to assume that $\nu(a_9) = 1$ and $\nu(a_8),\nu(a_{10}) \geq 2$. But then the degree-4-model $\mathcal{C}'$ for $C \to \mathbb{P}_K^3$ given by

$$F_1(tx_1,tx_2,x_3,x_4) = G_1(tx_1,tx_2,x_3,x_4) = 0$$

has a special fiber of the form $a_{9,1}x_3x_4 = \mu x_1 l(x_3,x_4) + \tilde{G}_1(0,0,x_3,x_4)$ where $\mu \in k$ and l is a linear factor. Therefore, $\mathcal{C}'_k$ contains a multiplicity-1 component which contradicts Corollary A.1.2 (*iii*). Similar argument works for the polynomial $\tilde{G}_1(0,0,x_3,x_4)$ of (*iv*). □

Remark A.3.3. Let $\mathcal{C}$ be as in Lemma A.3.2. Let $\mathrm{Sing}(\mathcal{C})$ be the singular locus of $\mathcal{C}$.

If $\mathcal{C}_k$ is a double conic with defining equations $x_1^2 = x_2^2 + x_3x_4 = 0$, then after a transformation in $\mathrm{GL}_4(\mathcal{O}_K)$ we can assume that $\nu(a_8) = 1$ and

$$\min\{\nu(a_5), \nu(a_6), \nu(a_7), \nu(a_9), \nu(a_{10})\} \geq 2,$$

see Lemma A.3.2. Moreover, $\mathrm{Sing}(\mathcal{C}) = \{(0:0:0:1)\}$, see Proposition 3.3.6 (*iii*).

Assume that $\mathcal{C}_k$ is two double lines with equations $x_1^2 = x_2x_4 + \mu x_1x_3 = 0$. If we assume that $\nu(a_5) = \nu(a_{10}) = 1$ and $\min\{\nu(a_6), \nu(a_8), \nu(a_9)\} \geq 2$, then the degree-4-model defined by the genus one equation

$$F_1(tx_1, x_2, x_3, x_4) = G(tx_1, x_2, x_3, x_4) = 0$$

has special fiber with equations $a_{5,1}x_2^2 + a_{7,1}x_2x_4 + a_{10,1}x_4^2 = x_2x_4 = 0$, which is a contradiction. Therefore, if $\mathcal{C}_k$ is two double lines given by the above equations, then we can assume that

$$\nu(a_8) = 1, \ \min\{\nu(a_5), \nu(a_6), \nu(a_9), \nu(a_{10})\} \geq 2,$$

and $\mathrm{Sing}(\mathcal{C}) = \{(0:1:0:0), (0:0:0:1)\}$, see Proposition 3.3.6 (*iii*).

If $\mathcal{C}_k$ is a quadruple line, then we have two possibilities according to Lemma A.3.2: (i) the defining equations of $\mathcal{C}_k$ are $x_1^2 = x_2^2 + x_1x_3 = 0$ with $\nu(a_8) = \nu(b_{10}) = 1$, $\nu(a_9), \nu(a_{10}) \geq 2$, $\mathrm{Sing}(\mathcal{C}) = \{(0:0:0:1)\}$, or $\nu(a_{10}) = 1$, $\nu(a_8), \nu(a_9) \geq 2$, $\mathrm{Sing}(\mathcal{C}) = \{(0:0:1:0)\}$. (ii) the defining equations of $\mathcal{C}_k$ are $x_1^2 = x_2^2 = 0$ with

$$\nu(a_8) = \nu(b_{10}) = 1 \text{ and } \min\{\nu(a_9), \nu(a_{10}), \nu(b_8), \nu(b_9)\} \geq 2.$$

Now we give an example to show that the number of non-isomorphic minimal degree-4-models for $C \to \mathbb{P}^3_K$ may become arbitrarily large when $C(K) = \emptyset$.

Example A.3.4. Let $i > 0$ be an integer. Let ϕ be a minimal genus one equation of degree 4 as in Equation (A.1) with the following coefficients valuations

$$\begin{array}{cccccccccccc}
x_1^2 & x_1x_2 & x_1x_3 & x_1x_4 & =0 & \geq i & \geq 1 & \geq i & \geq 1 & \geq 1 & \geq 1 & \geq 1 \\
 & x_2^2 & x_2x_3 & x_2x_4 & & \geq 2i & \geq i & \geq 2i & & =0 & \geq 1 & \geq 1 \\
 & & x_3^2 & x_3x_4 & & & =1 & \geq i & & & \geq 2 & \geq 2 \\
 & & & x_4^2 & & & & \geq 2i & & & & =1.
\end{array}$$

The equation ϕ defines a degree-4-model $\mathcal{C}$ for the curve $C \to \mathbb{P}^3_K$ defined by the same equation. We have $C(K) = \emptyset$, see ([11], Lemma 5.2). In addition, this genus one equation ϕ is minimal, see ([11], Lemma 5.3). The special fiber is a quadruple line. We define non-isomorphic degree-4-models $(\mathcal{C}_m, \alpha_m),\ 1 \leq m \leq i$, for $C \to \mathbb{P}^3_K$, where $\mathcal{C}_m$ is given by

$$F_{2m}(t^m x_1, x_2, t^m x_3, x_4) = G(t^m x_1, x_2, t^m x_3, x_4) = 0.$$

Bibliography

[1] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum, and A.R. Perlis. Jacobians of genus one curves. *J. Number Theory*, 90(2):304–315, 2001.

[2] M. Artin, F. Rodriguez-Villegas, and J. Tate. On the jacobians of plane cubics. *Adv. Math.*, 198(1):366–382, 2005.

[3] M. Bhargava. Higher composition laws I: A new view on gauss composition, and quadratic generalizations. *Annals of Mathematics*, 159:217–250, 2004.

[4] B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves I. *J. reine angew. Math.*, 212:7–25, 1963.

[5] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1990.

[6] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comb.*, 24:235–265, 1997.

[7] T. Bromwich. *Quadratic forms and their classification by means of invariant factors.* Cambridge Tracts in Mathematics and Mathematical Physics, 1906.

[8] B. Conrad. Minimal models for elliptic curves, unpublished work.

[9] J.E. Cremona. Reduction of binary cubic and quartic forms. *LMS J. Comput. Math.*, 2:64–94, 1999.

[10] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, and M. Stoll. Explicit n-descent on elliptic curves, I. Algebra. *J. reine angew. Math.*, 615:121–155, 2008.

[11] J.E. Cremona, T.A. Fisher, and M. Stoll. Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves, preprint.

[12] L. Dupont, D. Lazard, S. Lazard, and S. Petitjean. Near-optimal parametrization of the intersection of quadrics: II. A classification of pencils. *Journal of Symbolic Computation*, 43:192–215, 2008.

[13] I.B. Fesenko and S.V. Vostokov. *Local fields and their extensions*, volume 121 of *Translations of Mathematical Monographs.* American Mathematical Society, 2002.

[14] T.A. Fisher. A new approach to minimising binary quartics and ternary cubics. *Math. Res. Lett.*, 14:597–613, 2007.

[15] T.A. Fisher. The invariants of a genus one curve. *Proc. Lond. Math. Soc.*, 97(3):753–782, 2008.

[16] R. Hartshorne. *Algebraic geometry.* GTM 52. Springer, New York, 1977.

[17] D. Husemöller. *Elliptic curves.* GTM 111. Springer-Verlag, 1987.

[18] Q. Liu. Modèles entiers des courbes hyperelliptiques sur un corps de valuations discrète. *Trans. Amer. Math. Soc.*, 348(11):4577–4610, November 1996.

[19] Q. Liu. Models of curves and finite covers. *Compositio Math.*, 118:61–102, 1999.

[20] Q. Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, Oxford, 2002.

[21] Q. Liu, D. Lorenzini, and M. Raynaud. Néron models, lie algebras, and reduction of curves of genus one. *Invent. Math.*, 157:455–518, 2004.

[22] D. Lorenzini. Models of curves and wild ramification, preprint.

[23] L.J. Mordell. *Diophantine Equations.* Academic Press, London and New York, 1969.

[24] A.R. Perlis. *On the projective geometry of curves of genus one, and an algorithm for the jacobian of such a curve.* PhD thesis, The University of Arizona, 2004.

[25] B. Poonen. An explicit algebraic family of genus-one curves violating the Hasse principle. *J. Théor. Nombres Bordeaux*, 13(1):263–274, 2001.

[26] G. Sills. PhD thesis, University of Cambridge, in preparation.

[27] J. Silverman. *The arithmetic of elliptic curves.* GTM 106. Springer-Verlag, New York, 1986.

[28] J. Silverman. *Advanced topics in the arithmetic of elliptic curves.* GTM 151. Springer-Verlag, 1995.

[29] M. Stoll and J.E. Cremona. Minimal models for 2-coverings of elliptic curves. *LMS J. Comput. Math.*, 5:220–243, 2002.

[30] T.O. Womack. *Explicit descent on elliptic curves.* PhD thesis, University of Nottingham, 2003.