On the Model Theory of Function Fields

Charlie Conneen
April 22, 2022

A thesis submitted to

the Department of Mathematics at
The University of Virginia

in partial fulfillment for the degree of

Master of Science

Faculty Advisor: Professor Thomas Koberda

Contents

Chapter 1

Introduction

Model theory and algebraic geometry are deeply connected areas of mathematics; so connected, in fact, that model theorist W. Hodges has described model theory as "algebraic geometry minus fields," a modern twist on a quote from Chang and Keisler's text, in which they refer to model theory as "universal algebra plus logic" [10]. It is often the case that the objects of interest in algebraic geometry, such as varieties and rational maps between them, are described by first-order formulae. It is for this reason that model-theoretic results (such as the Lefschetz transfer principle and quantifier elimination in ACF) appear naturally in geometric settings. On the other hand, when investigating first-order theories in the language $\mathcal{L} = \{0, 1, +, \cdot\}$ of rings, such as the theory ACF of algebraically closed fields, it is not surprising that the robust nature of existing results in algebraic and arithmetic geometry will be invaluable. The contents of this thesis concern two problems of the latter kind: those which are model-theoretic in nature, but wield the tools and techniques from algebraic and arithmetic geometry.

The first goal of this thesis is to tackle certain problems of definability, namely, the definability of the field of constants and the genus of a given function field. These two problems, which are results of Duret [5], are discussed in Chapter 3. In Section 3.1, we show the following:

Theorem (1) *Let k be an algebraically closed field, K a function field of dimension 1 over k. There exists a first-order formula $\varphi(x)$ in the language $\mathcal{L} = \{0, 1, +, \cdot\}$ such that, for all $a \in K$,*

$$K \models \varphi(a) \text{ if and only if } a \in k.$$

This is to say that k is *defined by* a first-order formula $\varphi(x)$. The definability of genus is a slightly different problem: usually, definability problems are concerned with whether a particular *subset* is "cut out" by a first-order formula. When we say that the genus is definable, we mean this in the following sense:

Theorem (2) *There exists a set $\{\varphi_m\}_{m\in\mathbb{N}}$ of $\mathcal{L}$-sentences such that, for any algebraically closed field k and any function field K of dimension 1 over k, the following hold:*

1. *$K \models \neg\varphi_m$ for all $m \in \mathbb{N}$ if and only if its genus $\gamma(K/k)$ is zero;*
2. *If $g \neq 0$, then $K \models \varphi_g$ and $K \models \neg\varphi_m$ for all $m > g$ if and only if $\gamma(K/k) = g$.*

By the *genus* of K, we mean the genus of the associated curve. It is also worth mentioning that, while the above theorem is slightly weaker than saying that each φ_g is satisfied if and only if $\gamma(K/k) = g$, it is strong enough to conclude that the first-order properties of a function field uniquely determine its genus. The details of this result are the focus of Section 3.2.

Our second goal is the problem of first-order rigidity for function fields. By a rigidity problem, we mean a question of whether a certain class consists of objects which are uniquely determined by a smaller amount of information than expected.

In model theory, there is a very natural notion of equivalence of objects, that of elementary equivalence. This is a kind of equivalence between objects which is given by their relationship to the syntactic properties described by a given first-order language. In brief, elementary equivalence is an equivalence of two structures $\mathcal{M}, \mathcal{N}$ in a given language $\mathcal{L}$, written $\mathcal{M} \equiv_{\mathcal{L}} \mathcal{N}$, which states that all of their first-order properties (those statements which can be formalized in the language $\mathcal{L}$) agree. This is always true when $\mathcal{M}$ and $\mathcal{N}$ are isomorphic, but is, in general, weaker than isomorphism. For instance, $\overline{\mathbb{Q}}$ and $\mathbb{C}$ are certainly not isomorphic, as they differ in cardinality, but they satisfy the same complete first-order theory ACF_0, the theory of characteristic 0 algebraically closed fields. This gives that they are elementarily equivalent; one might also consider $\overline{\mathbb{Q}}$ as a subfield of $\mathbb{C}$, and from this perspective, $\overline{\mathbb{Q}}$ is an "elementary substructure" of $\mathbb{C}$.

However, there do exist circumstances in which the affirmative holds, that is, the *elementary classes* (that is, those equivalence classes of $\mathcal{L}$-structures up to elementary equivalence) do correspond precisely to the isomorphism classes. But when precisely does elementary equivalence imply isomorphism? Or to ask the converse: if two $\mathcal{L}$-structures are not isomorphic, must they disagree on some $\mathcal{L}$-sentence?

One of the main goals of this thesis is to discuss this problem for function fields over an algebraically closed ground field, as structures in the language $\mathcal{L} = \{0, 1, +, \cdot\}$ of rings. This is detailed in Chapter 4, where we present results of Duret [6], which address certain cases of the following conjectures:

Conjecture 1.1 Let K, L be function fields over an algebraically closed field k. If $K \equiv_{\mathcal{L}} L$, then $K \cong L$.

Conjecture 1.2 Let K, L be function fields over an algebraically closed field k. There exists a finite subset $A \subseteq k$ such that, if $K \equiv_{\mathcal{L}(A)} L$, then $K \cong_k L$, that is, K and L are isomorphic as k-algebras.

In other words, the conjectures state that equivalence of the first-order properties of K and L give that they are isomorphic as abstract fields (1.1) or as k-algebras (1.2). We will exhibit these in the following setting:

Theorem (3) *Let k be algebraically closed, and let K, L be function fields of dimension 1 over k. Suppose one of the following hold:*

- *L is not of genus 1;*
- *k is characteristic 0, and L is genus 1 without complex multiplication.*

If $K \equiv_{\mathcal{L}} L$, then $K \cong L$. Furthermore, there exists a finite subset $A \subseteq k$ such that, if $K \equiv_{\mathcal{L}(A)} L$, then $K \cong_k L$; that is, K and L are isomorphic as k-algebras.

Our proofs will make use of the definability results contained in Chapter 3. It is also worth noting that the case where L is genus 1 *with* complex multiplication is still an open problem. Some of the "state-of-the-art" results on elementary equivalence and isomorphism of function fields will be discussed at the end of Chapter 4.

Structure of this Text

The content of Chapter 2 constitutes a review of content from the relevant areas: algebra, algebraic geometry, number theory, and model theory. The associated background from algebraic geometry and number theory is covered in Sections 2.2 and 2.3. For a more thorough treatment of this content, [8, 9, 19] serve as references. For related background on Riemann surfaces, including the analytic content relevant in the case of genus one, see e.g. [7] or [12].

The content of Section 2.4 is model-theoretic background. To ensure that this thesis is as self-contained and accessible as possible, the discussion on this content is more detailed. There are many well-written, accessible expositions on introductory model theory; the author learned this content from [11], but other useful references include [2, 10, 14]. The main results are contained in Chapters 3 and 4.

Acknowledgements

There are many people to whom I wish to extend my gratitude. First and foremost, I would like to thank my advisor, Thomas Koberda. This work would not be possible if it were not for his incredibly patient guidance and support. He served as an outstanding guide as I learned the language of model theory, both through my independent study, and the course he taught this past Fall semester. I am forever in his debt for instilling in me the passion I have for the content of this thesis, and for the subject of model theory as a whole.

I would also like to extend my thanks to all my friends in the UVA math department and beyond. To the many PhD students and all others with whom I have undergone this intense year of graduate coursework, I thank you all for your camaraderie, and for making the math department such a lively environment. To Spencer Martin and Zach Baugher, I would like to thank you both in particular for your support as I dove headfirst into the theory of elliptic curves. Your assistance has made a substantial impact on the quality of this work, and I am incredibly grateful for your academic support and your friendship.

This project marks the end of my final year as a math student at UVA. My journey through my undergraduate and master's degrees would not have been possible without the aid of those mentioned above, as well as many others, including my many great professors over the years.

Chapter 2

Background

2.1 Preliminaries from Algebra

We begin with some elementary background and recall some definitions from field theory.

Definition 2.1.1 Let K be a field. The *prime subfield of* K, denoted K^{abs}, is the subfield generated by $1 \in K$.

Any field is either of characteristic $p \in \mathbb{N}$ where p is prime, or characteristic zero. If $\operatorname{Char} K = p$, then $K^{\text{abs}} \cong \mathbb{F}_p$, the field with p elements. Otherwise, $\operatorname{Char} K = 0$, and $K^{\text{abs}} \cong \mathbb{Q}$.

Definition 2.1.2 A *field extension* of a field K is a field L with an inclusion $K \hookrightarrow L$ of K as a subfield of L. We will write L/K to denote the field extension of K by L.

Some familiar examples of field extensions include $\mathbb{R}/\mathbb{Q}, \mathbb{C}/\mathbb{R}$, and $\mathbb{A}/\mathbb{Q}$, where $\mathbb{A} \subseteq \mathbb{C}$ is the field of algebraic numbers. That is, $\mathbb{A}$ is the subfield of $\mathbb{C}$ given by

$$\mathbb{A} = \{\alpha \in \mathbb{C} \mid \exists\, p(X) \in \mathbb{Q}\,[X], p(\alpha) = 0\}.$$

Definition 2.1.3 A field K is called *algebraically closed* if every non-constant polynomial $p(X) \in K[X]$ has a root in K.

Definition 2.1.4 Let K be a field. An *algebraic closure of* K, denoted $\overline{K}$, is a field extension of K such that every element of $\overline{K}$ is the root of a polynomial in K, and $\overline{K}$ is algebraically closed.

It is a standard fact from algebra that every field is contained in an algebraically closed field, and that the algebraic closure is unique up to isomorphism. See e.g. [4,

§ 13.4] for a proof. For this reason, we may refer to *the* algebraic closure of a field. $\mathbb{A}$ is the algebraic closure of $\mathbb{Q}$, and $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

An equivalent characterization of algebraically closed fields is that every such polynomial splits into linear factors. A third characterization will be given shortly, which will be of use when discussing the model-theoretic content of algebraically closed fields. For now, we will continue to describe important kinds of field extensions.

Definition 2.1.5 A field extension L/K is called

1. *proper* if $L \neq K$;
2. *finitely generated* if L is finitely generated as a K-algebra;
3. *algebraic* if every $\alpha \in L$ is the root of some polynomial $p(X) \in K[X]$, that is, every element of L is algebraic over K;
4. *purely transcendental* if there exists an algebraically independent set $S \subseteq L$ such that $K(S) = L$, i.e. there exists a transcendence base which spans L;
5. *separable* if it is either an algebraic extension such that the minimal polynomial[1] of each $\alpha \in L$ has *distinct* roots in the algebraic closure $\overline{K}$ of K, or there exists an intermediary field $K \subseteq F \subseteq L$ such that F/K is purely transcendental and L/F is algebraic and separable.
6. *normal* if it is an algebraic extension such that the minimal polynomial of each $\alpha \in L$ splits into linear factors over L.
7. *simple* if $L = K(\alpha)$ for some $\alpha \in K$.

Proposition 2.1.6 *Let L/K be an field extension, and suppose* $\operatorname{Char} K = 0$. *Then L/K is separable.*

Proof The case for finite extensions is given by [4, p. 551, Corollary 39]. The general case follows readily by taking a transcendence base $S \subseteq L$ and observing that any $\alpha \in L$ is algebraic over $K(S)$, a characteristic zero field. So its minimal polynomial is separable. □

A field is called *perfect* if every finite extension of it is separable. In this language, the above proposition gives that every characteristic zero field is perfect.

Proposition 2.1.7 (Primitive Element Theorem) *Let L/K be a finite separable field extension. Then L/K is a simple extension.*

Proof See [4, p. 595, Theorem 25]. □

[1] the *minimal polynomial* of $\alpha \in L$ over K, where L/K is an algebraic field extension, is the monic polynomial $\mu_{\alpha,K}(X) \in K[X]$ of minimal degree such that $\mu_{\alpha,K}(\alpha) = 0$. For proofs involving existence and uniqueness of $\mu_{\alpha,K}$, see [4, §3.2].

2.2 Algebraic Geometry

Curves

Definition 2.2.1 Let k be an algebraically closed field. By an *algebraic curve over* k, we mean an (irreducible) algebraic variety of Krull dimension 1 over k. Similarly, by a *projective curve over* k, we mean an (irreducible) projective variety of dimension 1 over k.

The two relevant kinds of maps between varieties are rational maps and regular maps. Rational maps are maps which are, in the affine case, expressible as rational functions in each coordinate (elements of $k(x_1, \ldots, x_n)$), and are defined as functions outside of the set of poles of the expression. In the projective case, rational maps are, at every point, expressible in an affine chart around that point as a rational function in each coordinate. Two curves (or varieties in general) are called *birationally equivalent* if there is a rational map between them with rational inverse. Regular maps are rational maps which are everywhere defined on the specified domain, and a regular map whose inverse is regular is an isomorphism of varieties. For this reason (and to not overburden the terminology "regular") we will refer to regular maps as *morphisms*.

We will now make note of a few relevant conventions and results about algebraic curves.

Definition 2.2.2 A plane curve is called *generic* if any singularity of it is a node.[2]

Theorem 2.2.3 *Any curve over an algebraically closed field is birationally equivalent to a generic affine plane curve.*

Proof See [9, p. 314, Corollary 3.11]. □

While the above theorem is essential, we will also require a refinement of it: namely, that we may place a bound on the degree of the generic curve we obtain, where this bound is dependent only on the genus of the initial curve. This is formulated as follows:

Theorem 2.2.4 ([5], p. 952, Proposition 18) *Let $g \geq 2$. Then there is some $D(g) \in \mathbb{N}$ such that any curve C of genus g over an algebraically closed field k is birationally equivalent to a generic affine plane curve C' of degree at most $D(g)$.*

[2] A *node* of a curve C is a singular point such that the Hessian matrix of the polynomials defining C has nonzero determinant.

Proof The proof of this follows the same route as the proof of Theorem 2.2.3, but all the while keeping track of the data used to construct the curve C'. If $C \subseteq \mathbb{P}^n$ has genus g, then the map which determines a birational equivalence between C and some $C_0 \subseteq \mathbb{P}^3$ (using [9, p. 310, Corollary 3.6]) has degree determined by a choice of divisor of degree at least $2g+1$. From this, birational equivalence with some $C' \subseteq \mathbb{P}^2$ is obtained with degree determined by the Riemann-Hurwitz formula, which reduces to an expression for d in terms of g (via [9, pp. 312-314]). □

Function Fields

Suppose that k is field. A function field over k is a kind of field extension K/k whose elements can be interpreted as rational functions acting on a variety defined over k.

Definition 2.2.5 Let k be a field. An *algebraic function field* is a finitely generated field extension K of k.

The transcendence degree of a function field K/k will correspond to the dimension of the variety we will associate to it. For this reason, we refer to a function field with transcendence degree n as one of *dimension* n over k.

Example 2.2.6 $\mathbb{C}(x)$ is a function field of dimension 1 over $\mathbb{C}$. It is also a function field of dimension 1 over $\mathbb{R}$.

Example 2.2.7 Let $\mathbb{F}_p$ be a finite field, p prime. Then $\mathbb{F}_q(t_1, \ldots, t_m)$ (where $q = p^n$ and $n \in \mathbb{N}$, and t_i transcendental over $\mathbb{F}_p$) is a function field over $\mathbb{F}_p$.

Example 2.2.8 More generally, let $R = k[X_1, \ldots, X_n]$ be the ring of polynomials in n variables over a field k, and let $P \subseteq R$ be a prime ideal. Then R/P is an integral domain, and we may take its fraction field $K = \mathrm{Frac}(R/P)$. Then K is a finitely generated extension of k, with generators given by the image of the set $\{X_1, \ldots, X_n\}$ under $R \twoheadrightarrow R/P \hookrightarrow \mathrm{Frac}(R/P)$.

If $\overline{k}$ is the algebraic closure of k, given a function field K/k, we can construct a function field $K(\overline{k})$ over $\overline{k}$ by simply adjoining $\overline{k}$ to K. If $t \in K$ is transcendental over k, then $t \in K(\overline{k})$ will be transcendental over $\overline{k}$. This shows that $\mathrm{trdeg}_{\overline{k}}(K(\overline{k})) = \mathrm{trdeg}_k(K)$. In particular, if K is the function field for a curve over k (the case of $\mathrm{trdeg}_k(K) = 1$), then $K(\overline{k})$ will be the function field of a curve over $\overline{k}$.

The study of these field extensions is motivated by the study of algebraic curves; Given a curve C, the rational functions $C \to k$ on C form a field, the *function field* of C. We denote this field by $k(C)$.

Example 2.2.9 $K = \mathbb{R}(x)$ is a function field over $k = \mathbb{R}$. Then $\overline{k} = \mathbb{C}$, and $K(\overline{k}) = \mathbb{C}(x)$.

We may also go from function fields to curves: a function field of dimension 1 over $\overline{k}$ is (isomorphic to) the function field of some nonsingular projective curve C defined over $\overline{k}$, unique up to isomorphism. If K/k is a function field of dimension 1 over an arbitrary field k, then $\gamma(K/k)$ will refer to the genus $g(C)$ of the nonsingular projective curve C defined over the algebraic closure $\overline{k}$ of k, which we associate to our field K.

Theorem 2.2.10 *Let k be a field, $\overline{k}$ its algebraic closure. Then there is a contravariant equivalence of categories between*

1. *Function fields of dimension 1 over $\overline{k}$ with $\overline{k}$-algebra homomorphisms, and*
2. *Nonsingular projective curves over $\overline{k}$ with dominant morphisms.*[3]

Proof See [9], p. 45, Corollary 6.12. □

In the case that the base field is $\mathbb{C}$, we have a further result, relating the algebraic category with the analytic category. A third equivalent category to the above two in this setting is that of compact Riemann surfaces with non-constant holomorphic maps.

2.3 Elliptic Curves

Lattices in the Complex Domain

Definition 2.3.1 A *lattice* is an additive subgroup $\Lambda \subseteq \mathbb{C}$ of the complex plane of the form $\langle w_1, w_2 \rangle$ where w_1, w_2 are linearly independent over $\mathbb{R}$.

Definition 2.3.2 Let $\Lambda, \Lambda' \subseteq \mathbb{C}$ be lattices. Then we say that Λ, Λ' are *similar* if there exists an action by $\alpha \in \mathbb{C}$ on $\mathbb{C}$ such that $\alpha(\Lambda) = \Lambda'$.[4]

This is an equivalence relation. Also observe that any lattice $\Lambda = \langle w_1, w_2 \rangle$, is similar to a lattice of the form $\langle 1, \tau \rangle$, where $\tau \in \mathbb{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$.

Definition 2.3.3 The *modular group* is the group $\mathrm{PSL}_2(\mathbb{Z})$ of 2×2 square matrices with entries in $\mathbb{Z}$ of determinant 1, equivalent up to a sign ($A \sim -A$).

In particular, the modular group is realized as acting on the upper half-plane $\mathbb{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\}$ by linear fractional transformations in the following way:

[3] A dominant morphism $\varphi : X \to Y$ between curves is a regular map with dense image, i.e. $\varphi(X) \subseteq Y$ is a dense subspace in the Zariski topology. In fact, any such map is surjective.

[4] The terminology *homothety* also occurs in the literature describing this equivalence.

given $\tau \in \mathbb{H}$, we have an associated lattice $\Lambda = \langle 1, \tau \rangle$. Given some matrix $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, the equivalence class $[T] \in \mathrm{PSL}_2(\mathbb{Z})$ acts by the map $z \mapsto \frac{az+b}{cz+d}$.

Theorem 2.3.4 *Let $\Lambda = \langle 1, \tau \rangle, \Lambda' = \langle 1, \tau' \rangle$ be lattices. Then Λ, Λ' are similar if and only if they are in the same orbit of the action on the set of lattices by the modular group of $\mathbb{H}$.*

Proof See [3, § 26]. □

Definition 2.3.5 If Λ is a lattice containing a lattice Λ', we write

$$\mathscr{R}(\Lambda, \Lambda') = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \supseteq \Lambda'\}.$$

If $\Lambda = \langle 1/n, \tau \rangle$ and $\Lambda' = \langle 1, \tau \rangle$, then we write $\mathscr{R}(\Lambda, \Lambda') = \mathscr{R}(n, \tau)$. One may regard elements of $\mathscr{R}(\Lambda, \Lambda')$ as morphisms between lattices. So if $\Lambda = \langle 1, \tau \rangle$ with $\tau \in \mathbb{H}$, then $\mathscr{R}(1, \tau)$ may be considered as the endomorphism ring of the lattice Λ.

Proposition 2.3.6 *If $\Lambda \subseteq \Lambda'$ are lattices, there exists a basis $\langle w_1', w_2' \rangle$ for Λ' and a pair of natural numbers m, n such that $\langle w_1'/mn, w_2'/m \rangle$ is a basis for Λ.*

Proof See [18, p. 81, Proposition 2]. □

Proposition 2.3.7 ([6, p. 811, Proposition 12]) *If τ is not quadratic over $\mathbb{Q}$, then $\mathscr{R}(n, \tau) = 1/\mathbb{Z} = \{1/k \mid k \in \mathbb{Z}, k \neq 0\}$.*

Proof Let $\alpha \in \mathscr{R}(n, \tau)$ and let $a, b, c, d \in \mathbb{Z}$ so that $1 = a\alpha/n + b\alpha\tau$ and $\tau = c\alpha/n + d\alpha\tau$. Then we obtain

$$\frac{1}{\alpha} = \frac{a}{n} + b\tau$$
$$\frac{\tau}{\alpha} = \frac{c}{n} + d\tau$$

By substitution, we have $\frac{a\tau}{n} + b\tau^2 = \frac{c}{n} + d\tau$, and thus

$$b\tau^2 + \left(\frac{a}{n} - d\right)\tau - \frac{c}{n} = 0.$$

Since τ is not quadratic over $\mathbb{Q}$, we obtain $b = 0$, $\frac{c}{n} = 0$, and $\frac{a}{n} = d$. But then $\frac{1}{\alpha} = d$, which shows $\mathscr{R}(n, \tau) \subseteq 1/\mathbb{Z}$. The other inclusion follows readily. □

Proposition 2.3.8 ([6, p. 811, Proposition 13]) *If τ is quadratic over $\mathbb{Q}$, then writing $\tau = r + is\sqrt{d}$ where $r \in \mathbb{Q}, s \in \mathbb{Q}^*, d \in \mathbb{N}$, d being square-free, we have*

$$\mathscr{R}(n, \tau) = \left\{(a/n + b\tau)^{-1} \mid a, b \in \mathbb{Z}, a \neq 0 \text{ or } b \neq 0, \text{and } bn(r^2 + ds^2), a/n + 2rb \in \mathbb{Z}\right\}.$$

Proof We first compute the following:

$$\begin{aligned}\tau^2 &= r^2 - ds^2 - 2r\tau = 2r^2 + 2irs\sqrt{d} - r^2 - s^2 d \\ &= 2r\left(r + is\sqrt{d}\right) - r^2 - s^2 d = 2r\tau - r^2 - s^2 d.\end{aligned}$$

From this, we obtain:

$$\begin{aligned}\alpha \in \mathscr{R}(n,\tau) &\iff 1, \tau \in \langle \alpha/n, \alpha\tau \rangle \\ &\iff \exists a, b \in \mathbb{Z}\left(\frac{1}{\alpha} = \frac{a}{n} + b\tau \text{ and } \tfrac{\tau}{\alpha} \in \left\langle \tfrac{1}{n}, \tau \right\rangle\right) \\ &\iff \exists a, b \in \mathbb{Z}\left(\frac{1}{\alpha} = \frac{a}{n} + b\tau \text{ and } \frac{-n\left(r^2 + s^2 d\right)}{n} + \left(\tfrac{a}{n} + 2rb\right)\tau \in \left\langle \tfrac{1}{n}, \tau \right\rangle\right) \\ &\iff \exists a, b \in \mathbb{Z}\left(\frac{1}{\alpha} = \frac{a}{n} + b\tau \text{ and } n\left(r^2 + s^2 d\right), \frac{a}{n} + 2rb \in \mathbb{Z}\right).\end{aligned}$$

□

Proposition 2.3.9 ([6, p. 811, Proposition 15]) *Let $d \in \mathbb{N}$ be square-free, $m \in \mathbb{N}, \ell \in \mathbb{Z}\backslash\{0\}$, $k \in \mathbb{Z}$, and let $\tau = \frac{1}{m}\left(k + i\ell\sqrt{d}\right)$. Then for all $n \in \mathbb{N}$ coprime to m, $\mathscr{R}(n,\tau) = \mathscr{R}(1,\tau)$.*

Proof Let $(a/n + b\tau)^{-1} \in \mathscr{R}(n,\tau)$. Since m, n are coprime, we have

$$n\frac{k^2 + d\ell^2}{m^2} b \in \mathbb{Z} \iff \frac{k^2 + d\ell^2}{m^2} b \in \mathbb{Z}$$

Then

$$\begin{aligned}\frac{a}{n} + 2\frac{k}{m}b = \frac{am + 2kbn}{mn} \in \mathbb{Z} &\iff mn \mid (am + 2kbn) \\ &\iff m \mid (am + 2kbn) \text{ and } n \mid (am + 2kbn) \\ &\iff m \mid 2kbn \text{ and } n \mid am \\ &\iff 2kb/m \in \mathbb{Z} \text{ and } a/n \in \mathbb{Z}\end{aligned}$$

But then $\mathscr{R}(n,\tau)$ is given by elements of the form $(a' + b\tau)^{-1}$ by setting $a' = a/n$. This shows $\mathscr{R}(n,\tau) = \mathscr{R}(1,\tau)$, as required. □

Elliptic Curves and the Modular Invariant

Definition 2.3.10 An *elliptic curve* over $\mathbb{C}$ is a nonsingular projective curve of genus 1 over $\mathbb{C}$ with a specified base point $O \in E$.

There are many equivalent definitions of elliptic curves over $\mathbb{C}$. However, when studying their function fields, it is natural to consider them as a special case of varieties with additional structure. It should be noted that every elliptic curve is naturally an algebraic group (varieties which are group objects), with $O \in E$ the identity in the group law.

Theorem 2.3.11 *Let E be an elliptic curve over $\mathbb{C}$. Then E is isomorphic to the projective closure of an affine plane curve cut out by an equation of the form*

$$y^2 = 4x^3 - ax - b.$$

Proof See [19, p. 49, Proposition III.1.7]. □

Definition 2.3.12 Let E be an elliptic curve over $\mathbb{C}$, and let C be a curve over $\mathbb{C}$ isomorphic to E given by the equation $y^2 = 4x^3 - ax - b$, as in the prior theorem. The *modular invariant of E*, or the *j-invariant of E*, is the element $j \in \mathbb{C}$ given by

$$j = 1728\frac{a^3}{a^3 - 27b^2}$$

For the modular invariant to be well-defined as stated, it must be invariant under the choice of nonsingular plane curves of the form $C : y^2 = 4r^3 - ax - b$ for which E has a Zariski-open subset isomorphic to C. This is discussed in [19, III.1].

Theorem 2.3.13 *Let E, E' be elliptic curves over $\mathbb{C}$. Then E and E' are isomorphic if and only if they have the same modular invariant.*

Proof See [19, p. 45, Proposition 1.4(b)]. □

Proposition 2.3.14 *For any $j \in \mathbb{C}$, there exists an elliptic curve over $\mathbb{C}$ for which j is the modular invariant, whose associated affine plane curve is definable*[5] *over $\mathbb{Q}(j)$.*

Proof Given $j \in \mathbb{C}$, we define an affine plane curve $C(j)$ over $\mathbb{C}$ by casework on j: if $j = 0$, let $C(j) : y^2 = 4x^3 - 1$, and if $j = 1728$, let $C(j) : y^2 = 4x^3 - x$. Otherwise let $C(j) : y^2 = 4x^3 - 3j(j - 1728)x - j(j - 1728)^2$. In each case, the projective closure $\widetilde{C(j)}$ of $C(j)$ is an elliptic curve isomorphic to $C(j)$ whose modular invariant is j. Furthermore, the coefficients in the Weierstrass equation defining $C(j)$ used only constant symbols from $\mathbb{Q}(j)$. So $C(j) \subseteq \mathbb{C}^2$ is definable over $\mathbb{Q}(j)$. □

Definition 2.3.15 Let E, E' be elliptic curves over $\mathbb{C}$. We say that E and E' are *isogenous* if there exists a dominant morphism $\varphi : E \to E'$ which preserves the base points, i.e. $\varphi(O) = O'$.[6] Any such map φ is called an *isogeny*.

[5] What "definability" means precisely (in the model-theoretic sense) will be postponed until Section 2.4.

[6] It is often the case that isogenies are introduced as certain group homomorphisms, but this definition is indeed sufficient, as any morphism of curves which preserves base points must also respect the group law.

Given an isogeny $\varphi : E \to E'$, there exists a *dual isogeny* $\widehat{\varphi} : E' \to E$ [19, p. 81, Theorem III.6.1] which is a dominant morphism in the other direction. Importantly, this gives that isogeny of elliptic curves is an equivalence relation. Furthermore, we have the following relationship between the j-invariants of isogenous curves:

Proposition 2.3.16 *Let E, E' be isogenous elliptic curves over $\mathbb{C}$, and let j, j' be their respective modular invariants. Then j' is integral over $\mathbb{Z}[j]$.*

Proof See [16, p. 201, Theorem 3.10]. □

Elliptic Functions

Definition 2.3.17 Let $\Lambda = \langle 1, \tau \rangle$ be a lattice in $\mathbb{C}$. A meromorphic function f on $\mathbb{C}$ is called *elliptic in* Λ if for all $z \in \mathbb{C}$, $f(z+1) = f(z)$ and $f(z+\tau) = f(z)$. In other words, f is elliptic if it is periodic in Λ.

If $\Lambda \subseteq \mathbb{C}$ is a lattice, we will denote by $\mathscr{E}(\Lambda)$ the set of all meromorphic functions which are elliptic in Λ. Observe that if f and g are elliptic in Λ, then $f+g$, fg, and f/g are also elliptic in Λ. So we see that $\mathscr{E}(\Lambda)$ is a subfield of $\mathcal{M}(\mathbb{C})$, the field of meromorphic functions on $\mathbb{C}$.

We will now give some well-known facts about elliptic functions.

Theorem 2.3.18 (Liouville) *Let $\Lambda \subseteq \mathbb{C}$ be a lattice, and let $f \in \mathscr{E}(\Lambda)$. The following are true:*

1. *If f is holomorphic, then f is constant.*
2. *Let $X = \mathbb{C}/\Lambda$ be the associated complex torus. Then f descends to a meromorphic function F on X, and $\sum_{p \in X} \operatorname{Res}(F; p) = 0$.*

Proof See [19, Proposition VI.2.1 and Theorem VI.2.2]. □

The above theorem allows us to further see $\mathscr{E}(\Lambda)$ as a subfield of $\mathcal{M}(X)$, the field of meromorphic functions on the complex torus $X = \mathbb{C}/\Lambda$.

Theorem 2.3.19 *Let $\Lambda \subseteq \mathbb{C}$ be a lattice. There exists an element $\wp \in \mathscr{E}(\Lambda)$ and a pair $a, b \in \mathbb{C}$ satisfying $a^3 - 27b^3 \neq 0$ such that $(\wp')^2 = 4\wp^3 - a\wp - b$ and $\mathscr{E}(\Lambda) = \mathbb{C}(\wp, \wp')$. Conversely, if $a, b \in \mathbb{C}$ satisfy $a^3 - 27b^3 \neq 0$, then there exists a lattice $\Lambda \subseteq \mathbb{C}$ such that $\mathscr{E}(\Lambda)$ is isomorphic to the function field of the affine plane curve given by $y^2 = 4x^3 - ax - b$.*

Proof This theorem summarizes a few results from [19, Chapter VI]. In particular, this includes the Uniformization Theorem [19, p. 173, Theorem VI.5.1]. □

The element $\wp \in \mathscr{E}(\Lambda)$ described in the above theorem is called the *Weierstrass function* associated to the complex torus $X = \mathbb{C}/\Lambda$. Note in particular that, because $\wp$ satisfies the following differential equation:

$$\left(\wp'\right)^2 = 4\wp^3 - a\wp - b \tag{2.1}$$

for any $z_0 \in \mathbb{C}$ outside of the poles of $\wp, \wp'$, the point $(\wp(z_0), \wp'(z_0)) \in \mathbb{C}^2$ lies on the affine plane curve $C(\Lambda) : y^2 = 4x^3 - ax - b$. Its projective closure may be described by the homogenized coordinate version of this equation:

$$\widetilde{C(\Lambda)} : y^2 z = 4x^3 - axz^2 - bz^3 \tag{2.2}$$

Precisely, we may define a map $F : X \to \widetilde{C(\Lambda)}$ given by

$$F(w) = \left[\wp(w) : \wp'(w) : 1\right] \tag{2.3}$$

Note that Λ-periodicity of $\wp, \wp'$ gives that this is well-defined, and furthermore, it is a holomorphic map of Riemann surfaces. In fact, it is bijective, and has nowhere zero derivative; this is because $z \mapsto (\wp(z), \wp'(z))$ has derivative given by $z \mapsto (\wp'(z), \wp''(z))$, and $\wp''(z) \neq 0$ on all of $\mathbb{C}$, as all of the zeroes of $\wp'$ are simple. Hence F is bi-holomorphic. Put another way, we have an analytic isomorphism $F : X \cong \widetilde{C(\Lambda)}$ between complex manifolds. In this way, we realize the torus X as an elliptic curve, where the specified base point of X is the image of $0 \in \mathbb{C}$ under the quotient $\mathbb{C} \twoheadrightarrow \mathbb{C}/\Lambda$. We also obtain an equivalence between the fields associated to these objects: we have already seen that $\mathscr{E}(\Lambda)$ is naturally a subfield of $\mathcal{M}(X)$, but it in fact constitutes the entire field.

Theorem 2.3.20 *There is a covariant equivalence of categories between:*

1. *Elliptic curves over $\mathbb{C}$ with isogenies;*
2. *Elliptic curves over $\mathbb{C}$ with basepoint-preserving complex-analytic maps;*
3. *Lattices in $\mathbb{C}$ up to similarity, with* $\mathrm{Mor}(\Lambda, \Lambda') = \mathscr{R}(\Lambda', \Lambda) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda'\}$.

Proof See [19, p. 175, Theorem VI.5.3]. □

Note in particular that any two elliptic curves are isomorphic as algebraic groups if and only if they are isomorphic as complex manifolds, if and only if the underlying lattices are similar. Combining this with Theorem 2.2.10 yields the following:

Corollary 2.3.21 *The elliptic function fields $\mathscr{E}(\Lambda)$ and $\mathscr{E}(\Lambda')$ are isomorphic as $\mathbb{C}$-algebras if and only if Λ and Λ' are similar lattices. Furthermore, a given $\mathbb{C}$-algebra homomorphism $\Phi : \mathscr{E}(\Lambda) \to \mathscr{E}(\Lambda')$ is an isomorphism if and only if there exists a pair $\alpha, \beta \in \mathbb{C}$ with $\alpha \neq 0$ such that $\alpha\Lambda = \Lambda'$ and the following holds:*

$$\forall f \in \mathscr{E}(\Lambda), \forall z \in \mathbb{C}, \Phi(f)(z) = f(z/\alpha + \beta).$$

Proof The first statement is immediate from the above theorem, and the derivation of the expression for $\Phi(f)$ is the content of [19, p. 171, Theorem VI.4.1]. □

Definition 2.3.22 Let E be an elliptic curve over $\mathbb{C}$, and let $\mathbb{C}/\Lambda$ be a complex torus isomorphic to E. We say that E has *complex multiplication* if $\mathscr{R}(\Lambda, \Lambda) \neq 1/\mathbb{Z}$. That is, E has complex multiplication if the underlying lattice Λ has self-coverings which are not given simply by integer scaling.

The Story for Different Base Fields

Much of our discussion thus far concerns curves over $\mathbb{C}$, which is a relatively well-behaved setting. It is clear that $\mathbb{C}$ has the comfort of being algebraically closed of characteristic zero. However, it also benefits from the analytic techniques available via the theory of Riemann surfaces. Because of this, whenever the analytic techniques are applied, the results detailed for elliptic curves thus far will require alternative justification over other algebraically closed fields of characteristic zero.

For one important example, consider the modular invariant j of an elliptic curve

$$E : y^2 = 4x^3 - ax - b$$

defined over $\mathbb{C}$, as given in Definition 2.3.12. If $\Lambda = \langle 1, \tau \rangle$ is a lattice with $\tau \in \mathbb{H}$ such that $E \cong \mathbb{C}/\Lambda$, we are able to recover the isomorphism class of the elliptic curve, just from the lattice Λ. But then, Theorem 2.3.13 allows us to recover the j-invariant from Λ, since it yields the isomorphism class of E. Put another way, given some $\tau \in \mathbb{H}$, we may assign some $j \in \mathbb{C}$ which will be the j-invariant of the elliptic curve associated to the lattice $\Lambda = \langle 1, \tau \rangle$. In fact, we can say more: we may realize the assignment of the j-invariant as a holomorphic function $j : \mathbb{H} \to \mathbb{C}$, which is given by the following formula:

$$j(\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2} \tag{2.4}$$

where $g_2(\tau)$ and $g_3(\tau)$ are holomorphic in τ and are determined uniquely by the The analytic structure of j is a powerful tool, but is by no means necessary to define the modular invariant over another base field.

Let k be an algebraically closed field of characteristic zero. If $\mathrm{trdeg}_{\mathbb{Q}} k \leq 2^{\aleph_0}$, then k embeds into $\mathbb{C}$ as a subfield, and we may interpret the j-invariant just the

same as in the case of $\mathbb{C}$. Otherwise, $\mathrm{trdeg}_{\mathbb{Q}} k > 2^{\aleph_0}$, and there is not the same analytic description. However, the characterization of the modular invariant given in Definition 2.3.12 will still make sense over k (since it is simply a rational function) so long as there is still a cubic curve given by a Weierstrass equation isomorphic to any elliptic curve E over k, and the value of $j(E)$ is independent of the choice of such a curve. Indeed, this is the case, and the proof contained in [19, III.1] is given in this generality. The same results also hold in positive characteristic (other than 2), but we will contain our discussion of elliptic curves to the case of characteristic zero.

2.4 Model Theory

We will now take some time to build the model-theoretic framework in which we will discuss the problems of interest, regarding function fields of curves.

Languages, Theories, and Models

Definition 2.4.1 A *language* $\mathcal{L}$ consists of the following data:

- A set $\mathcal{C}_{\mathcal{L}}$ of *constant symbols*,
- A set $\mathcal{F}_{\mathcal{L}}$ of *function symbols*, such that each $f \in \mathcal{F}_{\mathcal{L}}$ has an assigned *arity*, a natural number n_f, and
- A set $\mathcal{R}_{\mathcal{L}}$ of *relation symbols*, such that each $R \in \mathcal{R}_{\mathcal{L}}$ has an assigned arity $n_R \in \mathbb{N}$.

The arity of a function or relation symbol is the number of arguments it takes in. If the arity of a relation symbol is 2, then it is a binary relation symbol.[7]

If $\mathcal{L}$ is a finite language, we will often write our language simply as a tuple of all of its constituent symbols; that is, we will often write $\mathcal{L} = \left\{\dot{c}_1, \ldots, \dot{c}_n, \dot{f}_1, \ldots, \dot{f}_m, \dot{R}_1, \ldots, \dot{R}_\ell\right\}$, where $\mathcal{C}_{\mathcal{L}} = \{\dot{c}_1, \ldots, \dot{c}_n\}, \mathcal{F}_{\mathcal{L}} = \left\{\dot{f}_1, \ldots, \dot{f}_m\right\}$, and $\mathcal{R}_{\mathcal{L}} = \left\{\dot{R}_1, \ldots, \dot{R}_\ell\right\}$.

Example 2.4.2 $\mathcal{L}_{\mathbf{Grp}} = \{e, \pi, \iota\}$ is the language of groups, where e is a constant symbol (the identity), π is a binary function symbol (the product map), and ι is a unary function symbol (the inverse map).

Example 2.4.3 $\mathcal{L}_{\mathbf{Ring}} = \{0, 1, +, \cdot\}$ is the language of rings (with unity), where $0, 1$ are the constant symbols and $+, \cdot$ are binary function symbols.

[7] Constant symbols are sometimes regarded instead as 0-ary function symbols, that is, function symbols corresponding to functions of the form $M^0 \to M$. Since M^0 is a singleton (its only element being the empty function $\emptyset \to M$), these correspond to elements of M.

In both of the above examples, we have symbols which are intended to correspond to well-known functions. In $\mathcal{L}_{\mathbf{Ring}}$, 0 and 1 are intended to be the elements of a ring corresponding to the additive and multiplicative identities, and $+, \cdot$ are meant to be the binary operations of addition and multiplication, respectively. However, as it stands, they are only symbols. How these symbols are interpreted will correspond to their assignments in an $\mathcal{L}$-*structure*:

Definition 2.4.4 Let $\mathcal{L}$ be a language. An $\mathcal{L}$-*structure* $\mathcal{M}$ consists of the following data:

- A *universe* M of $\mathcal{M}$, which is a set;
- For each constant symbol $\dot{c} \in \mathcal{C}_{\mathcal{L}}$, an element $c = \dot{c}^{\mathcal{M}} \in M$;
- For each n-ary function symbol $\dot{f} \in \mathcal{F}_{\mathcal{L}}$, a function $f = \dot{f}^{\mathcal{M}} : M^n \to M$;
- For each n-ary relation symbol $\dot{R} \in \mathcal{R}_{\mathcal{L}}$, an n-ary relation $R = \dot{R}^{\mathcal{M}} \subseteq M^n$.

Example 2.4.5 $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are all $\mathcal{L}_{\mathbf{Ring}}$-structures, with the usual interpretations.

Observe in particular that an $\mathcal{L}_{\mathbf{Ring}}$-structure need not be a ring (since $\mathbb{N}$ is an $\mathcal{L}_{\mathbf{Ring}}$-structure, for instance). In fact, none of the intended properties of $0, 1, +, \cdot$ need to hold in a given $\mathcal{L}_{\mathbf{Ring}}$-structure. To restrict ourselves to only those structures which satisfy certain rules, we need to formalize *theories* in a given language. Informally, a theory is a set of rules about how the symbols from $\mathcal{L}$ must behave, and the things which satisfy those rules are *models* of that theory.

To formalize what those rules are, we define $\mathcal{L}$-terms, $\mathcal{L}$-formulae, and $\mathcal{L}$-sentences. $\mathcal{L}$-terms are symbolic representations for elements. No matter the language $\mathcal{L}$, we allow ourselves a countable collection $\{v_1, v_2, \ldots\}$ of variable symbols. Each variable v_n is a term, and each constant symbol $c \in \mathcal{C}_{\mathcal{L}}$ is a term. If $\dot{f} \in \mathcal{F}_{\mathcal{L}}$ is an n-ary function symbol, and $t_1, \ldots, t_n$ are terms, then $\dot{f}(t_1, \ldots, t_n)$ is a term.

Now we may define $\mathcal{L}$-formulae and $\mathcal{L}$-sentences:

Definition 2.4.6 The set $\mathrm{Fm}_{\mathcal{L}}$ of $\mathcal{L}$-*formulae* is defined recursively as follows:

1. For any pair of $\mathcal{L}$-terms t_1, t_2, $(t_1 = t_2) \in \mathrm{Fm}_{\mathcal{L}}$;
2. For any n-placed relation symbol $\dot{R} \in \mathcal{R}_{\mathcal{L}}$ and $\mathcal{L}$-terms $t_1, \ldots, t_n$, $\dot{R}(t_1, \ldots, t_n) \in \mathrm{Fm}_{\mathcal{L}}$;
3. For any $\varphi, \psi \in \mathrm{Fm}_{\mathcal{L}}$, $\neg\varphi, \varphi \wedge \psi, \varphi \vee \psi \in \mathrm{Fm}_{\mathcal{L}}$ (where $\wedge, \vee, \neg$ are the logical symbols AND, OR, and NOT, respectively);
4. For any $\varphi \in \mathrm{Fm}_{\mathcal{L}}$ and any variable x, $(\forall x\, \varphi) \in \mathrm{Fm}_{\mathcal{L}}$ and $(\exists x\, \varphi) \in \mathrm{Fm}_{\mathcal{L}}$.

An $\mathcal{L}$-*sentence* is an $\mathcal{L}$-formula with no free variables, that is, an $\mathcal{L}$-formula φ is a sentence if any variable x occurring in φ is bounded by a quantifier: either $\forall x$ or $\exists x$ must occur before x in the formula for it to be a sentence.

Example 2.4.7 Let $\mathcal{L} = \{0, 1, +, \cdot\}$. Then the following are $\mathcal{L}$-sentences:

$$1 + 1 = 0 \qquad \forall y \exists x \left(x^2 = y\right) \qquad \exists x \left(x^3 + 2 = 0\right)$$

where x^2 is notation for $x \cdot x$ and 2 is notation for $1 + 1$. On the other hand, the following are $\mathcal{L}$-formulae which are not $\mathcal{L}$-sentences:

$$y^2 = 4x^3 - ax - b \qquad \neg (x = 0) \to \exists y \, (x \cdot y = 1)$$

where $\varphi \to \psi$ is notation for $\psi \vee \neg\varphi$.

The above example illustrates a few important facts about formulae: we may make use of logical notation such as implication and bi-implication, even though they are not among the logical symbols allowed initially.

Definition 2.4.8 Let $\mathcal{M}$ be an $\mathcal{L}$-structure, and let φ be an $\mathcal{L}$-sentence. We say that $\mathcal{M}$ *satisfies* φ, written $\mathcal{M} \models \varphi$, if φ is true in $\mathcal{M}$.

Example 2.4.9 If $\mathcal{L} = \{e, \cdot, \iota\}$ is the language of groups, consider any group G as an $\mathcal{L}$-structure by interpreting the constant symbol e as the identity element of G, the binary function symbol $\cdot$ as the group operation $G \times G \to G$, and the unary relation symbol ι as the inverse map $G \to G$. Consider the following $\mathcal{L}$-sentences:

$$\varphi : \forall x \exists y \, (x \cdot y = e) \qquad \psi : \forall x \, (x \cdot e = x)$$

Then any group G has $G \models \varphi \wedge \psi$. However, if $\theta : \forall x \forall y \, (x \cdot y = y \cdot x) \in \mathrm{Sent}_{\mathcal{L}}$, then $G \models \theta$ if and only if G is abelian.

With the above definitions at hand, we may describe what first-order theories are, and how they relate to structures.

Definition 2.4.10 Let $\mathcal{L}$ be a language. An $\mathcal{L}$-*theory* is a set $T \subseteq \mathrm{Sent}_{\mathcal{L}}$ of sentences which is closed under implication; that is, T satisfies the condition that for any $\varphi \in \mathrm{Sent}_{\mathcal{L}}$, if $T \vdash \varphi$ (there exists a proof of φ under the assumption that T holds), then $\varphi \in T$.[8]

Given a set $\Delta \subseteq \mathrm{Sent}_{\mathcal{L}}$, we may consider the set $T(\Delta) = \{\varphi \in \mathrm{Sent}_{\mathcal{L}} \mid \Delta \vdash \varphi\}$. Then $T(\Delta)$ is an $\mathcal{L}$-theory, the $\mathcal{L}$-theory *generated by* Δ, and we say that Δ is a set of *axioms* for $T(\Delta)$.

Example 2.4.11 Let $\mathcal{L}_{\mathbf{Ring}} = \{0, 1, +, \cdot\}$ be the language of rings. We may formalize the axioms for additive abelian groups as the following $\mathcal{L}$-sentences:

[8] Some authors use the convention that a theory is simply *any* collection of $\mathcal{L}$-sentences. However, it will be useful to think of theories as consisting of all the statements which they imply, as well. A set of sentences which is not closed under entailment will be called a set of axioms.

$\forall x \forall y \forall z\,((x+y)+z = x+(y+z))$,
$\forall x \forall y\,(x+y = y+x)$,
$\forall x\,(x+0 = x)$,
$\forall x \exists y\,(x+y = 0)$.

To introduce commutative ring structure, we may add the following sentences:

$\forall x\,(x \cdot 0 = 0)$,
$\forall x \forall y \forall z\,(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$,
$\forall x \forall y\,(x \cdot y = y \cdot x)$,
$\forall x\,(x \cdot 1 = x)$,
$\forall x \forall y \forall z\,(x \cdot (y+z) = x \cdot y + x \cdot z)$.

These axiomatize the $\mathcal{L}$-theory CR of commutative rings with unity. If we add to this list the following axioms:

$\forall x\,(\neg\,(x = 0) \rightarrow \exists y\,(x \cdot y = 1))$,
$\neg\,(0 = 1)$,

then the theory generated is the $\mathcal{L}$-theory Fld, the theory of fields.

Definition 2.4.12 Let T be an $\mathcal{L}$-theory. An $\mathcal{L}$-structure $\mathcal{M}$ is called a *model of* T if $\mathcal{M} \models \varphi$ for every $\varphi \in T$; that is to say, $\mathcal{M}$ satisfies all of the sentences of T. If $\mathcal{M}$ is a model of T, we write $\mathcal{M} \models T$.

Example 2.4.13 Models of the $\mathcal{L}_{\mathbf{Ring}}$-theory CR are commutative rings with unity. Models of Fld are fields.

Definition 2.4.14 Let T be an $\mathcal{L}$-theory. T is called:

1. *consistent* if T does not prove a contradiction, i.e. there does not exist an $\mathcal{L}$-sentence φ such that $T \vdash \varphi \wedge \neg\varphi$;
2. *satisfiable* if T has a model;
3. *complete* if for every $\varphi \in \mathrm{Sent}_{\mathcal{L}}$, one of $T \vdash \varphi$ or $T \vdash \neg\varphi$ holds.

Definition 2.4.15 If $\mathcal{M}$ is an $\mathcal{L}$-structure, the *$\mathcal{L}$-theory of $\mathcal{M}$*, written $\mathrm{Th}\,(\mathcal{M})$, is the set of all sentences $\varphi \in \mathrm{Sent}_{\mathcal{L}}$ such that $\mathcal{M} \models \varphi$.

Theorem 2.4.16 (Compactness Theorem) *Let $\mathcal{L}$ be a language, If T is an $\mathcal{L}$-theory, T is satisfiable if and only if every finite subset of T is satisfiable.*

Proof See Chapter 2 of [11]. □

The compactness theorem is a fundamental result in model theory. One of the standard proofs of compactness[9] relies upon Gödel's completeness theorem:

[9] See [11] for said proof. There are two other proofs worth mentioning: one is due Henkin, and is also contained in [11]. The other involves the compactness of the Lindenbaum algebra of a theory with the Stone topology, and is the origin of the theorem's name. See [14] for this proof.

Theorem 2.4.17 (Gödel's Completeness Theorem) *Let $\mathcal{L}$ be a language, T an $\mathcal{L}$-theory. Then T is consistent if and only if T is satisfiable.*

The completeness theorem allows us to restate the compactness theorem as such: T is consistent if and only if every finite subset of T is consistent. This is perhaps a more initially believable statement, as it reduces to saying that, if T proves a contradiction, then T proves a contradiction using only finitely many axioms. The completeness theorem also says that any consistent theory has a model, and any $\mathcal{L}$-structure has a consistent $\mathcal{L}$-theory.

Theories of Fields

Let $\mathcal{L} = \mathcal{L}_{\mathbf{Ring}} = \{0, 1, +, \cdot\}$ be the language of rings. We already discussed in Example 2.4.11 the $\mathcal{L}$-theory Fld of fields. This theory is consistent since it has a model (take your favourite field as proof of this). However, it is not complete: for instance, the $\mathcal{L}$-sentence

$$\psi : 1 + 1 = 0$$

is satisfied by $\mathbb{F}_2$, the field with two elements, but not by $\mathbb{Q}$. There are a plethora of complete theories which contain Fld. Take, for example, the theory $\mathrm{Th}(\mathbb{Q})$, the complete theory of the rational numbers. This is distinct from $\mathrm{Th}(\mathbb{F}_2)$ by the above example, since $\psi \in \mathrm{Th}(\mathbb{F}_2)$ but $\neg\psi \in \mathrm{Th}(\mathbb{Q})$. Other distinct theories are $\mathrm{Th}(\mathbb{R})$ and $\mathrm{Th}(\mathbb{C})$; $\mathbb{R}$ and $\mathbb{C}$ disagree on the $\mathcal{L}$-sentence $\exists x \left(x^2 + 1 = 0\right)$, whereas $\mathbb{R}$ and $\mathbb{Q}$ (or $\mathbb{C}$ and $\mathbb{Q}$) disagree on the $\mathcal{L}$-sentence $\exists x \left(x^2 = 2\right)$.

To actually characterize these theories, it is easier to start with a list of axioms, and refine those axioms until the theory generated by it is complete. By a *theory of fields*, we mean a theory in the language $\mathcal{L}$ of rings which contains Fld. Completions of this theory correspond to the elementary classes of fields. We will now discuss some of the relevant examples.

Consider the set of $\mathcal{L}$-sentences obtained by appending to the axioms of Fld the set of $\mathcal{L}$-sentences of the form

$$\forall a_0 \forall a_1 \ldots \forall a_{n-1} \exists x \left(x^n + a_{n-1}x^{n-1} + \cdots + a_0\right) = 0$$

for all $n \in \mathbb{N}$. The theory generated by these sentences is ACF, the theory of algebraically closed fields.

This theory is still not complete, since there are algebraically closed fields of prime characteristic, and of characteristic 0, so some models of ACF will still disagree on the sentence $1 + 1 = 0$. However, this can be amended – if p is prime, let ϕ_p be the $\mathcal{L}$-sentence

$$\underbrace{1 + \ldots + 1}_{p \text{ times}} = 0.$$

Then appending the axiom ϕ_p to ACF gives the theory ACF_p of algebraically closed fields of characteristic p. If $p = 0$, appending $\{\neg\phi_p\}_p$ (where p ranges over all primes) as axioms gives ACF_0, the theory of algebraically closed fields of characteristic 0.

Theorem 2.4.18 *Let p be prime or 0. Then ACF_p is complete.*

Proof By Vaught's test [11, p. 42, Theorem 2.2.6], any consistent theory with no finite models which is uncountably categorical[10] is complete. ACF_p is consistent since it has a model, there are no finite algebraically closed fields, and uncountable categoricity holds by recalling that isomorphism classes of algebraically closed fields are uniquely determined by characteristic and absolute transcendence degree (transcendence degree over the prime subfield). Since the absolute transcendence degree is the same for any two algebraically closed fields of the same *uncountable* cardinality, the theorem follows. □

Remark. Note that categoricity fails in the countable case. For example, $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}(\pi)}$ are both countable and algebraically closed, but not isomorphic, since $\mathrm{trdeg}_{\mathbb{Q}}\,\overline{\mathbb{Q}} = 0$ but $\mathrm{trdeg}_{\mathbb{Q}}\,\overline{\mathbb{Q}(\pi)} = 1$.

The reader familiar with algebraic geometry may recognize the characteristic zero case of the above theorem as the first-order formulation of the *Lefschetz transfer principle*. Often, the Lefschetz principle is introduced informally as a way of using analytic techniques over $\mathbb{C}$ to prove results about other characteristic zero fields.[11] Indeed, we will make use of this in Chapter 4, but we can in fact say quite a bit more about the properties of ACF and ACF_p; in particular, note the following theorem:

Theorem 2.4.19 (Quantifier Elimination in ACF) *For any formula $\phi(\overline{x}) \in \mathrm{Fm}_{\mathcal{L}}$, there exists a formula $\psi(\overline{x}) \in \mathrm{Fm}_{\mathcal{L}}$ which contains no quantifiers*[12] *such that* $\mathrm{ACF} \models \phi \leftrightarrow \psi$.

Proof See [11, p. 85, Theorem 3.2.2]. □

Definability

We now discuss the main tool which allows us to be quite expressive in a language, which is definability.

For a concrete example, consider the language $\mathcal{L} = \mathcal{L}_{\mathbf{Ring}}$ of rings, and the $\mathcal{L}$-theory T of commutative rings (with unity). Despite subtraction not having a

[10] This condition says that any models of the same uncountable cardinality are isomorphic.
[11] See [17] for a more detailed, historical discussion.
[12] This means ψ does not contain the symbols $\forall$ or $\exists$.

symbol in $\mathcal{L}$, the function $a \mapsto -a$ is *definable* in a ring; that is, given a ring R, the set of all $(x, -x) \subseteq R^2$ can be described by a first-order formula:

$$\left\{(x,-x) \;\middle|\; x \in R^2\right\} = \left\{(x,y) \in R^2 \;\middle|\; x+y=0\right\}$$

If a function $f : R^n \to R^m$ is definable in the above sense, then we may use it freely in formulae. For this reason, the language $\{0, 1, +, \cdot, -\}$ is not "more expressive" than the language $\{0, 1, +, \cdot\}$, at least in the context of rings.

Properly, a subset $A \subseteq R^n$ is *definable* if there exists an $\mathcal{L}$-formula $\varphi(x_1, \ldots, x_n)$ in n free variables such that

$$A = \{(a_1, \ldots, a_n) \in R^n \mid R \models \varphi(a_1, \ldots, a_n)\}.$$

In this case, we are allowed to quantify over elements of A; that is, if $\varphi(x_1, \ldots, x_n)$ is the formula defining A, and $\psi(x_1, \ldots, x_n)$ is any other formula, the statements

$$\exists\, \overline{a} \in A \text{ such that } \psi(\overline{a}) \qquad\qquad \exists\, \overline{a} \in A^c \text{ such that } \psi(\overline{a})$$

may be written in the language $\mathcal{L}$ as

$$\exists\, \overline{x}\,(\varphi(\overline{x}) \wedge \psi(\overline{x})) \qquad\qquad \exists\, \overline{x}\,(\neg\varphi(\overline{x}) \wedge \psi(\overline{x}))$$

The same statements with universal instead of existential quantifications. Note that a function $f : R^n \to R^m$ is definable (in the informal sense above) if and only if its graph as a subset of R^{n+m} is definable.

In Chapter 3, we will prove the definability of the field of constants k of a function field K, under certain conditions about the ground field. Along with solving this question of definability, this result will also allow us to write sentences of the form $(\exists x \in k)\varphi(x)$ and $(\exists x \notin k)\varphi(x)$ (for example), where $\varphi(x)$ is an $\mathcal{L}$-formula. this will be particularly helpful in Chapter 4 to show that certain elements of K are not contained in the base field.

Elementary Equivalence

Fix a language $\mathcal{L}$. We have that the relevant objects over $\mathcal{L}$ are $\mathcal{L}$-structures, but we have yet to describe what the morphisms are. There are two kinds of morphisms which are relevant: $\mathcal{L}$-embeddings, and elementary embeddings.

Definition 2.4.20 Let $\mathcal{M}, \mathcal{N}$ be $\mathcal{L}$-structures. an *$\mathcal{L}$-embedding* from $\mathcal{M}$ to $\mathcal{N}$ is an injective function $\iota : M \hookrightarrow N$ satisfying the following conditions:

1. For every $a_1, \ldots, a_n \in M$ and every n-ary function symbol $\dot{f} \in \mathcal{F}_{\mathcal{L}}$, we have $\iota\left(\dot{f}^{\mathcal{M}}(a_1, \ldots, a_n)\right) = \dot{f}^{\mathcal{M}}(\iota(a_1), \ldots, \iota(a_n))$;
2. For every constant symbol $c \in \mathcal{C}_{\mathcal{L}}$, we have $\iota\left(c^{\mathcal{M}}\right) = c^{\mathcal{N}}$.

In other words, the interpretations of all constant symbols are preserved under $\mathcal{L}$-embeddings, and they respect applications of function symbols. An *$\mathcal{L}$-isomorphism* is a bijective $\mathcal{L}$-embedding.

It might seem fairly restrictive to only allow ourselves to consider injective maps, but recall that we are interested in function fields over an algebraically closed field k, and any k-algebra homomorphism of fields must be injective. So the relevant maps will end up being those desired.[13]

Example 2.4.21 Let $\mathcal{L} = \{0, 1, +, \cdot\}$ be the language of rings, and suppose R, S are two rings (with unity). Then an $\mathcal{L}$-embedding $R \hookrightarrow S$ must be an injective ring homomorphism (sending 1_R to 1).

Example 2.4.22 Let R be a ring and consider the language $\mathcal{L} = \{0, 1, +, \cdot\}$ and the language $\mathcal{L}(R) = \mathcal{L} \cup \{\dot{x} \mid x \in R\}$ obtained by adjoining to $\mathcal{L}$ constant symbols from R. Now if A, B are two R-algebras, an $\mathcal{L}$-embedding is simply an injective ring homomorphism. However, an $\mathcal{L}(R)$-embedding must preserve the interpretations of the constant symbols appended. In other words, it fixes R pointwise as a substructure of A and B. Hence, an $\mathcal{L}(R)$-embedding is a genuine R-algebra inclusion $A \hookrightarrow B$. For this reason, the language $\mathcal{L}(R)$ may be thought of as the "language of R-algebras." Accordingly, we will write $A \cong_R B$ to say that A, B are $\mathcal{L}(R)$-isomorphic.

Definition 2.4.23 Let $\mathcal{M}, \mathcal{N}$ be $\mathcal{L}$-structures. An *elementary embedding* of $\mathcal{M}$ into $\mathcal{N}$ is an $\mathcal{L}$-embedding $j : \mathcal{M} \hookrightarrow \mathcal{N}$ such that, for any $\mathcal{L}$-formula $\varphi(\overline{x})$, $\mathcal{M} \models \varphi(\overline{x})$ if and only if $\mathcal{N} \models \varphi(j(\overline{x}))$. If $\mathcal{M}$ is a substructure of $\mathcal{N}$, then we say that $\mathcal{M}$ is an *elementary substructure* of $\mathcal{N}$, written $\mathcal{M} \preccurlyeq \mathcal{N}$, if the inclusion map $\iota : \mathcal{M} \hookrightarrow \mathcal{N}$ is an elementary embedding.

The language of the above definitions will help when discussing the details of *elementary equivalence*, a kind of semantic equivalence between structures, which is described as follows:

Definition 2.4.24 Let $\mathcal{L}$ be a language, $\mathcal{M}, \mathcal{N}$ two $\mathcal{L}$-structures. $\mathcal{M}$ and $\mathcal{N}$ are called *elementarily equivalent*, written $\mathcal{M} \equiv_{\mathcal{L}} \mathcal{N}$, if for all $\varphi \in \mathrm{Sent}_{\mathcal{L}}$,

$$\mathcal{M} \models \varphi \text{ if and only if } \mathcal{N} \models \varphi.$$

Put another way, two $\mathcal{L}$-structures are elementarily equivalent if they have the same $\mathcal{L}$-theory, i.e. $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$. The equivalence classes of $\mathcal{L}$-structures up to elementary equivalence are called *elementary classes*.

[13] There are settings in which non-injective maps of $\mathcal{L}$-structures still makes sense, and one may talk about relevant algebraic things such as quotients; see e.g. [11, pp. 24-28] for an elementary discussion of interpretability.

Remark. The substance of Example 2.4.22 justifies the way in which we structure the two main questions about elementary equivalence addressed in Chapter 4. Namely, we concern ourselves with showing certain cases of the following:

- $\mathcal{L}$-equivalence implies $\mathcal{L}$-isomorphism, and
- $\mathcal{L}(k)$-equivalence implies $\mathcal{L}(k)$-isomorphism.

$\mathcal{L}$-isomorphism of k-algebras is the same as isomorphism as abstract fields, but an $\mathcal{L}(k)$-isomorphism of k-algebras is an isomorphism *as k-algebras*.

It is important to see that the definition of elementary equivalence is not stated in terms of how $\mathcal{M}$ and $\mathcal{N}$ interact with respect to the relevant first-order maps ($\mathcal{L}$-embeddings and elementary embeddings) between them. It is thus unclear what the relationship between the existence of mutual embeddings and elementary equivalence is, in general. However, the model-theoretic technique known as a back-and-forth argument is one which will allow us to show elementary equivalence between two $\mathcal{L}$-structures analogous to taking a direct limit, where the objects are isomorphisms of certain substructures, and the transition maps between these isomorphisms will be function inclusions. Since we only use this technique in the proof of Lemma 4.2.6, we will save the exposition until then.

The relationship between elementary equivalence and $\mathcal{L}$-embeddings is still unclear, but the fundamental relationship between elementary equivalence and isomorphism is not so complicated:

Theorem 2.4.25 (Isomorphism theorem) *Let $\mathcal{L}$ be a language, and let $\mathcal{M},\mathcal{N}$ be two $\mathcal{L}$-structures such that $\mathcal{M} \cong \mathcal{N}$. Then $\mathcal{M} \equiv_{\mathcal{L}} \mathcal{N}$.*

The idea is straightforward: take some isomorphism $j : \mathcal{M} \cong \mathcal{N}$. It is already an elementary embedding in the forward direction, by definition. So it is left to verify that the inverse of j is an elementary embedding. The proof of this follows readily by formula induction; for details, see [11, p.13, Theorem 1.1.10].

It is also worth mentioning the following theorem, which details the precise relationship between elementary equivalence and isomorphism:

Theorem 2.4.26 (Keisler-Shelah Isomorphism Theorem) *Let $\mathcal{L}$ be a language. two $\mathcal{L}$-structures $\mathcal{M},\mathcal{N}$ are elementarily equivalent if and only if there exists a set I and an ultrafilter $\mathcal{U}$ on I such that $\mathcal{M}^{\mathcal{U}} \cong \mathcal{N}^{\mathcal{U}}$; in other words, $\mathcal{L}$-structures have the same $\mathcal{L}$-theory if and only if they have isomorphic ultrapowers.*

Proof See [2, p. 398, Theorem 6.1.15]. □

The proof is by no means elementary, despite the fact that the condition is fairly natural to state.[14] In fact, the original proof by Keisler was one which proved a stricter statement, but did so assuming the generalized continuum hypothesis.

We now have the language to properly describe the main question of interest in Chapter 4: given two elementarily equivalent $\mathcal{L}$-structures $\mathcal{M} \equiv_{\mathcal{L}} \mathcal{N}$, when is it the case that $\mathcal{M} \cong \mathcal{N}$? In particular, we will concern ourselves with the case where $\mathcal{L} = \mathcal{L}_{\mathbf{Ring}}$ is the language of rings, and our $\mathcal{L}$-structures are function fields over an algebraically closed field k.

We will simultaneously consider whether elementary equivalence in $\mathcal{L}(k)$ induces a k-algebra isomorphism, or to use the terminology from Example 2.4.22, an $\mathcal{L}(k)$-isomorphism. A partial answer to the affirmative will be given, and we will weaken the assumed condition by controlling the size of the specified language. Namely, we will exhibit k-isomorphism under the condition of $\mathcal{L}(A)$-equivalence, where $A \subseteq k$ is finite. In the case of function fields for elliptic curves over k of characteristic zero, our results will consider the case where $A = \{j\}$, where j is the modular invariant of the elliptic curve. This is a fairly natural choice, since the modular invariant determines the isomorphism class of elliptic curves.

Consider the case of two elliptic curves E, E' over k which are isogenous but not isomorphic. If their function fields are K and K', respectively, then isogeny gives that there is a pair of k-algebra inclusions $K \hookrightarrow K'$ and $K' \hookrightarrow K$, but K and K' are not isomorphic as k-algebras. In particular, it is important to observe that *a priori*, the precise relationship between the following conditions is not clear:

1. $K \cong_k K'$;
2. There exists a pair of k-algebra homomorphisms $K \hookrightarrow K'$ and $K' \hookrightarrow K$;
3. $K \equiv_{\mathcal{L}(j)} K'$, where j is the j-invariant of K;
4. $K \equiv_{\mathcal{L}} K'$;

As of right now, the only implications which are clear are (1) $\Rightarrow$ (2), (3) $\Rightarrow$ (4), and (1) $\Rightarrow$ (3), where the last of these follows by the isomorphism theorem.

We will see in Section 4.2 that elliptic curves whose function fields have the same $\mathcal{L}(j)$-theory (where j is one of their j-invariants) are isogenous; that is, we will show that (3) $\Rightarrow$ (2). In this setting, we may shift the perspective of our question to one regarding the actual curves: is elementary equivalence between their function fields strong enough to get from isogeny to isomorphism? Or, to ask the contrapositive: if two elliptic curves are isogenous but not isomorphic, is there an $\mathcal{L}$-sentence which their function fields must disagree on?[15]

[14] For the reader interested in the connections between model theory and ultraproducts, see [1].
[15] This question is answered by Theorem 4.2.8.

Chapter 3

Definability in Function Fields

Let $\mathcal{L}$ be the language of rings. In Section 2.4, we discussed the notion of definability in structures. Our current goal is to highlight some important definability results: the definability of the *field of constants* and the *genus* of a function field for a curve. Definability of the field of constants will allow us to ensure, using first-order properties, that an element of a function field is, or is not, contained in the base field. As for the latter result, the definability of genus will ensure that two function fields of curves cannot be elementarily equivalent if they are of distinct genus. This will make the structure of results contained in Chapter 4 much simpler.

3.1 The Fields of Constants

When K is an algebraic function field over some field k, we would like to consider the elements of $K \setminus k$ as the non-constant rational functions on some curve over k, and treat the elements of k as constant rational functions. However, these field extensions might not behave as we expect. Consider $\mathbb{C}(x)$ as a function field over $\mathbb{R}$. The elements of $\mathbb{C}(x)$ act as rational functions on $\mathbb{C}$ (treated as an affine curve) or on the projective curve $\mathbb{P}^1$, which we might treat as a curve over $\mathbb{C}$. However, the base field is $\mathbb{R}$, which conflicts with the desire to view the base field sitting inside of the function field as the associated constant maps.

Indeed, given an algebraic function field K/k, there may be elements of $K \setminus k$ which we might want to treat as though they are elements of the base field, since they behave like constant maps. This motivates the following definition.

Definition 3.1.1 Let K be an algebraic function field over k. The *field of constants* of K/k is the relative algebraic closure of k in K, that is, the intermediate subfield of K given by $\{\alpha \in K \mid \alpha \text{ algebraic over } k\}$.

Example 3.1.2 The field of constants of $\mathbb{C}(x)/\mathbb{R}$ is $\mathbb{C}$.

In model-theoretic terms, the field of constants of K/k is given by $\mathrm{acl}^K(k)$, the union of all finite subsets of K which are definable with parameters from k.[1] Note, then, that the condition $\mathrm{acl}^K(k) = k$ is precisely the same as saying that the field of constants is the base field. In fact, by taking the relative algebraic closure of our base field, we can consider more kinds of field extensions as though they are function fields.

For another example, consider any field K, without a specified base field. If we take the relative algebraic closure $\mathrm{acl}^K(F)$ of the prime subfield $F \subseteq K$, if K is a finitely generated extension of $\mathrm{acl}^K(F)$, we may treat K as an algebraic function field over $\mathrm{acl}^K(F)$.

Definition 3.1.3 We say that a field extension K/k is *regular* if $\mathrm{acl}^K(k) = k$. That is, a field extension is regular if the base field k contains all elements of the ambient field which are algebraic over k. We say that K is a *regular function field* over k if K is an algebraic function field over k and K/k is a regular field extension.

A natural question arises when considering the field of constants from the model-theoretic perspective: when are we able to describe such a subfield in first-order? Our goal now will be to answer that question, that is, to describe the conditions under which the field of constants is 0-definable.[2] To this end, we will make extensive use of the properties of a particularly useful curve, the so-called *Fermat curve* defined by the equation

$$Z_0^d + Z_1^d = Z_2^d$$

for a certain value of $d \in \mathbb{N}$, which will be described shortly.

Let $n \in \mathbb{N}$ be a natural number and let $\mathbb{P}^n$ be projective n-space over the field $\overline{k}$. For $1 \leq i \leq n$, let $U_i \subseteq \mathbb{P}^n$ be the basic open set given by $U_i = \{[Z_0 : \cdots : Z_n] \in \mathbb{P}^n \mid Z_i \neq 0\}$. Now let $C \subseteq \mathbb{P}^n$ be a projective curve over $\overline{k}$, and let $F_1, \ldots, F_q$ be the homogeneous polynomial generators of C. For each i, let $C_i = C \cap U_i$. Then at least one of $C_1, \ldots, C_n$ is nonempty, and each C_i is either empty or dense in C. Let $1 \leq i \leq n$ such that C_i is nonempty. Then C_i is an affine curve over $\overline{k}$, and is generated by the polynomials $f_1, \ldots, f_q$, where each $f_i \in \overline{k}\,[X_1, \ldots, X_n]$ is the local expression for F_i.[3]

In our discussion of function fields K/k, whenever k is not relatively algebraically closed in K (that is, $\mathrm{acl}^K(k) \neq k$), we will replace our base field with the more appropriate field of constants. For this reason, in the results to follow, we will append the condition that K is a regular function field over k.

[1] In fact, if k is algebraically closed with prime subfield $F = k^{\mathrm{abs}}$, then for any $A \subseteq k$, $\mathrm{acl}^k(A)$ is the algebraic closure of $F(A)$.

[2] If $\mathcal{L}$ is a language, $\mathcal{M}$ an $\mathcal{L}$-structure, we say that $X \subseteq M^n$ is 0-*definable* if it is definable by a formula $\varphi(x_1, \ldots, x_n)$ in the base language $\mathcal{L}$. If X is definable in the language $\mathcal{L}(A)$ for some $A \subseteq M$, we say X is A-*definable*, or *definable with parameters from* A.

[3] See e.g. [9] for a more detailed discussion.

Proposition 3.1.4 ([5, p.948, Lemma 1]) *Let k be a field, K a regular function field of dimension 1 over k, and let $C \subseteq \mathbb{P}^n(\overline{k}), C' \subseteq \mathbb{P}^m(\overline{k}), C'' \subseteq \mathbb{P}^\ell(\overline{k})$ be projective curves over $\overline{k}$ such that the following conditions hold:*

1. *The function field of C is $K(\overline{k})$;*
2. *C' is birationally equivalent to C''.*

Let $\{F_1, \ldots, F_q\}$ be a generating set for the ideal of $C_i' \neq \emptyset$ for some $1 \leq i \leq m$. Suppose there exists some $P = (x_1, \ldots, x_m) \in K^m \setminus k^m$ such that $\forall 1 \leq j \leq q, F_j(P) = 0$. Then there exists a dominant morphism $\varphi : C \to C''$ of curves.

Proof Consider $L = \overline{k}(x_1, \ldots, x_m) \subseteq K(\overline{k})$. Since $F_j(x_1, \ldots, x_m) = 0$ for each $1 \leq j \leq q$, L is isomorphic to the function field $\overline{k}(C_i')$ of the affine curve $C_i' = \{[Z_0 : \cdots : Z_m] \in C' \mid Z_i \neq 0\}$. Since C_i' is dense in C', there is an isomorphism $\overline{k}(C_i') \cong \overline{k}(C')$ of their function fields. As C' and C'' are birationally equivalent, we have an isomorphism $\overline{k}(C'') \cong \overline{k}(C')$. So consider the chain $\overline{k}(C'') \cong \overline{k}(C') \cong L \hookrightarrow K(\overline{k}) = \overline{k}(C)$ of k-algebra homomorphisms. By Theorem 2.2.10, this induces a dominant morphism $\varphi : C \to C''$. □

Indeed, we can say more about how these curves relate to each other once we have a dominant morphism between them: in particular, any such morphism exhibits the relationship $g(C) \geq g(C'')$ between their genera, by application of the Riemann-Hurwitz formula (where, without loss of generality, $g(C'') \neq 0$):

$$g(C) = g(C'') + (\deg \varphi - 1)(g(C'') - 1) + \frac{1}{2} \deg R \geq g\left(C''\right)$$

where R is the ramification divisor of φ [9, p. 303, example 2.5.4].

Corollary 3.1.5 ([5, p. 949, Lemma 2]) *Let k be a field, K a regular function field of dimension 1 over k. Suppose $C' \subseteq \mathbb{P}^m$ is a nonsingular projective curve over $\overline{k}$ with genus $g(C') > \gamma(K/k)$. For some $1 \leq i \leq m$ with $C_i' \neq \emptyset$, let $\{F_1, \ldots, F_q\}$ generate the ideal $I(C_i') \subseteq k[X_1, \ldots, X_m]$, and suppose that $x_1, \ldots, x_m \in K$ satisfies $\forall 1 \leq j \leq q$,*

$$F_j(x_1, \ldots, x_m) = 0.$$

Then $x_1, \ldots, x_m \in k$.

Proof By way of contradiction, suppose that for some $x_1, \ldots, x_m \in K$ we have $F_j(x_1, \ldots, x_m) = 0$ for all $1 \leq j \leq q$ but not all of $x_1, \ldots, x_m$ are in k. Then $(x_1, \ldots, x_m) \in K^m \setminus k^m$. But then by Proposition 3.1.4, writing $C = K(\overline{k})$, there exists a dominant rational map $C \to C'$, which forces $\gamma(K/k) = g(C) \geq g(C')$, contradicting the assumption that $g(C') > \gamma(K/k)$. □

With this result at our disposal, we will be able to start discussing the first-order formula which will determine our field of constants. This formula is exhibited in the following result.

Theorem 3.1.6 ([5, p. 949, Lemma 3]) *Let k be a field, K a regular function field of dimension 1 over a field k. Suppose that $d \in \mathbb{N}$ satisfies the following conditions:*

1. $\operatorname{Char} k \nmid d$;
2. $\frac{1}{2}(d-1)(d-2) > \gamma(K/k)$.

Then for all pairs $x_1, x_2 \in K$, if $x_1^d + x_2^d = 1$, then $x_1, x_2 \in k$.

Proof It suffices to apply Corollary 3.1.5 to the projective curve $C' \subseteq \mathbb{P}^2(\overline{k})$ given by

$$Z_0^d + Z_1^d = Z_2^d.$$

Note that this curve is nonsingular by the assumption that $\operatorname{Char} k \nmid d$. Consider the map $\pi : C' \to \mathbb{P}^1(\overline{k})$ given by $\pi(Z_0 : Z_1 : Z_2) = [Z_0 : Z_1]$. This is well-defined, since there is no point $[x_0 : x_1 : x_2] \in C'$ with $x_0 = x_1 = 0$. Furthermore, any point $[x_0 : x_1 : x_2] \in C'$ is a ramification point of π if and only if $\frac{\partial}{\partial Z_2}\left(Z_0^d + Z_1^d - Z_2^d\right) = -dZ_2^{d-1} = 0$. Since $d \neq 0 \in k$, the ramification points of π are precisely $\{[x_0 : x_1 : x_2] \in X \mid x_2 = 0\}$. This is the same as the set of $[Z : 1 : 0] \in \mathbb{P}^2(\overline{k})$ such that $Z^d + 1 = 0$; in other words, there are d distinct ramification points, corresponding to the d^{th} roots of -1. So by application of the Riemann-Hurwitz formula, we obtain:

$$\begin{aligned} 2g\left(C'\right) - 2 &= \deg \pi \cdot \left(2g(\mathbb{P}^1) - 2\right) + \sum_{p \in C'} e_P - 1 \\ &= -2d + d(d-1) \end{aligned}$$

where e_P is the ramification index of π at p. This yields $g\left(C'\right) = \frac{1}{2}(d-1)(d-2)$, the Plücker formula for a smooth plane curve defined by a degree d polynomial [19, p. 39, Exercise II.2.7]. So direct application of Corollary 3.1.5 gives that $\forall x, y, z \in K, x^d + y^d = z^d \implies x, y, z \in k$. So fixing $z = 1$, we have that $x^d + y^d = 1 \implies x, y \in k$, as required. □

Limits of Field Extensions

In the process of utilising the machinery of algebraic geometry, we have had to accommodate the fact that many of the theorems we have applied only hold over algebraically closed fields. For algebraic function fields K/k where k is not algebraically closed, we have had to ensure at least that k was *relatively* algebraically closed in K. Furthermore, when associating a curve to such a K, we had to lift to the algebraic closure $\overline{k}$ of k, and take K along with us in the form of the function field $K(\overline{k})$ over $\overline{k}$. Now, we seek to further broaden the class of field extensions for which definability of the field of constants holds.

Recall. A *tower of fields* is a well-ordered sequence of fields, each contained in the next:

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$$

We will consider such a sequence as a family of fields $(K_\alpha)_{\alpha<\lambda}$ indexed by some ordinal λ, where $K_\alpha \subseteq K_\beta$ whenever $\alpha < \beta$.

Definition 3.1.7 Let K/k be a field extension, and suppose that there exists a countable tower $(K_n)_{n=0}^{\infty}$ of subfields of K such that the following conditions hold:

1. $K_0 = k$ and $K = \bigcup_{n=0}^{\infty} K_n$;
2. For all $n \in \mathbb{N}$, K_n is a dimension 1 regular function field over k;
3. There exists some $g \in \mathbb{N}$ such that for all $n \in \mathbb{N}$, $g \geq \gamma(K_n/k)$.

Then we say that K/k is *countably regular*.[4]

Since algebraic function fields are finite extensions of the base field, any dimension 1 regular function field K over a field k is also countably regular, by taking $K_0 = k$, $K_n = K$ for all $n > 0$, and $g = \gamma(K/k)$.

Observe that, by combining Theorem 2.2.10 with condition (3) in the above definition, we have that $(\gamma(K_n/k))_{n=1}^{\infty}$ is a bounded and increasing sequence of natural numbers, so it is eventually constant. Let $g \in \mathbb{N}$ be the least natural number such that there exists a countable tower of the form given in Definition 3.1.7. We will denote by g the *genus* of the field extension K/k, written $\Gamma(K/k)$.

Definition 3.1.8 Let K/k be a field extension, let λ be an uncountable ordinal, and suppose that there exists a tower $(K_\alpha)_{\alpha<\lambda}$ of subfields of K such that the following conditions hold:

1. $K_0 = k$ and $K = \bigcup_{\alpha<\lambda} K_\alpha$;
2. If $\beta < \lambda$ is any limit ordinal, then $K_\beta = \bigcup_{\alpha<\beta} K_\alpha$;
3. For any ordinal $\alpha < \lambda$, $K_{\alpha+1}/K_\alpha$ is countably regular;
4. There exists some $g \in \mathbb{N}$ such that, for all $\alpha < \lambda$, $g \geq \Gamma(K_{\alpha+1}/K_\alpha)$.

Then we say that K/k is *uncountably regular*.

Note in particular that any countably regular extension K/k is also uncountably regular, by extending the given countable tower $(K_n)_{n=1}^{\infty}$ to any uncountable ordinal length $(K_\alpha)_{\alpha<\lambda}$ by letting $K_\alpha = K$ for all ordinals $\omega \leq \alpha \leq \lambda$.

Again, since $(\Gamma(K_{\alpha+1}/K_\alpha))_{\alpha<\lambda}$ is an increasing sequence of natural numbers which is uniformly bounded above by g, it is eventually constant. Suppose $g \in \mathbb{N}$ is minimal such that there exists a sequence $(K_\alpha)_{\alpha<\lambda}$ satisfying the above conditions, for some infinite ordinal λ. Then $\Gamma(K/k) = g$ will denote the *genus* of K/k.

Example 3.1.9 Let $a \in \mathbb{N}$ be a fixed natural number. Let K be the field generated by adjoining $\{t^{1/a^n}\}_{n=1}^{\infty}$ to a field k, where t is transcendental over k. Then taking $K_0 = k$ and

[4] In [5], Duret refers to this condition as the $(\mathscr{F}_0)$ property for field extensions, whereas uncountable regularity is known as the $(\mathscr{F}_1)$ property.

$K_n = k\left(t^{1/a^n}\right)$, we see that each K_n is isomorphic to $k(T)$ for some T transcendental over k, and moreover we have containment $K_n \subseteq K_{n+1}$ for all $n \in \mathbb{N}$. Then K/k is countably regular, and $\Gamma(K/k) = 0$, since $\gamma(K_n/k) = 0$ for all $n \in \mathbb{N}$.

Example 3.1.10 Let K be a purely transcendental extension of k, and suppose that K has an uncountable set $S \subseteq K$ which is algebraically independent over k with $K = k(S)$. Then $S \subseteq K$ is a basis for K as a k-algebra. Taking a well-ordering $S = \{s_\alpha\}_{\alpha<\kappa}$ of S, we may construct a chain $K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$ of subfields of K as follows:

$$\begin{aligned} K_0 &= k \\ K_1 &= k(s_0) \\ K_2 &= k(s_0, s_1) \\ &\vdots \\ K_\alpha &= k(\{s_\beta : \beta < \alpha\}) \end{aligned}$$

Then K/k is uncountably regular, but is too tall to be countably regular.

Now it is left to show that uncountable regularity suffices to show definability of the field of constants k. To do so, we first prove that this condition holds in the countably regular case.

Lemma 3.1.11 ([5, p. 950, Lemma 8]) *Let K/k be a countably regular function field. If $d \in \mathbb{N}$ satisfies $\operatorname{Char} k \nmid d$ and $\frac{1}{2}(d-1)(d-2) > \Gamma(K/k)$, then for all $x, y \in K$, if $x^d + y^d = 1$, then $x, y \in k$.*

Proof Suppose $d \in \mathbb{N}$ is as given, and suppose $x, y \in K$ satisfy $x^d + y^d = 1$. Then there exists some $n \in \mathbb{N}$ such that $x, y \in K_n$. Observe that $\frac{1}{2}(d-1)(d-2) > \Gamma(K/k) \geq \gamma(K_n/k)$, so applying Theorem 3.1.6 to K_n/k suffices to complete the proof. □

Lemma 3.1.12 ([5, p. 950, Proposition 9]) *Let K/k be an uncountably regular function field. If $d \in \mathbb{N}$ satisfies $\operatorname{Char} k \nmid d$ and $\frac{1}{2}(d-1)(d-2) > \Gamma(K/k)$, then for all $x, y \in K$, if $x^d + y^d = 1$, then $x, y \in k$.*

Proof Let $d \in \mathbb{N}$ and $x, y \in K$ be as given. Let $(K_\alpha)_{\alpha<\lambda}$ be a tower of subfields of K satisfying the uncountable regularity conditions, and let $\alpha < \lambda$ be the least ordinal such that $x, y \in K_\alpha$. If α were a limit ordinal, then K_α is the union of K_β for $\beta < \alpha$. But then x, y would be contained in some K_β for $\beta < \alpha$. So α is either a successor ordinal or $\alpha = 0$. If α is a successor ordinal, write $\alpha = \sigma + 1$. Then $K_\alpha = K_{\sigma+1}$ is a countably regular function field over K_σ. But by assumption, we have that

$$\frac{1}{2}(d-1)(d-2) > \Gamma(K/k) \geq \Gamma(K_\alpha/K_\sigma)$$

so by Lemma 3.1.11, we have that $x, y \in K_\sigma$. This contradicts the assumption that α was chosen to be minimal with $x, y \in K_\alpha$. So we find that $\alpha = 0$, and thus $x, y \in K_0 = k$, as required. □

This brings us to the following theorem:

Theorem 3.1.13 ([5, p. 951, Corollary 11]) *Let K/k be an uncountably regular function field, and suppose that k is an algebraically closed field. Then k is definable in K.*

Proof Choose $d \in \mathbb{N}$ such that $\operatorname{Char} k \nmid d$, and make the choice sufficiently large so that $\frac{1}{2}(d-1)(d-2) > \Gamma(K/k)$. Then the formula $\xi_d(x)$ given by

$$\exists y \left(x^d + y^d = 1\right)$$

has the property that, for all $a \in K, K \models \xi_d(a)$ if and only if $a \in k$, by Lemma 3.1.12. So $\xi_d(x)$ defines k in K. □

3.2 The Genus of a Function Field

Proposition 3.2.1 ([5, p. 953, Proposition 19]) *For all $g, d \in \mathbb{N}$ with $d \geq 1$, there exists a formula $\chi_g^d(x_{ij}) \in \mathrm{Fm}_{\mathcal{L}}$ in the language of fields in $n = \frac{1}{2}(d+1)(d+2)$ free variables (x_{ij}) such that, for any algebraically closed k and any $(a_{ij}) \in k^n$, $k \models \chi_g^d(a_{ij})$ if and only if the following conditions hold:*

1. *The polynomial $F(X,Y) = \sum_{0 \leq i+j \leq d} a_{ij} X^i Y^j$ is an irreducible polynomial over k of degree d;*
2. *The projective closure C of the affine plane curve defined by $F(X,Y) = 0$ is a generic plane curve;*
3. *The genus of C is g.*

Proof It suffices to show that there is a formula for each of these three conditions individually, since their conjunction will then satisfy the properties of χ_g^d. For (1), for each degree $0 < \ell < d$, let $m = \frac{1}{2}(\ell+1)(\ell+2)$ and let $r = \frac{1}{2}(d-\ell+1)(d-\ell+2)$. Then in first order we may state the following:

$$\forall (b_{ij}) \in k^m \, \forall (c_{ij}) \in k^r \left(\sum_{0 \leq i+j \leq \ell} b_{ij} X^i Y^j \right) \cdot \left(\sum_{0 \leq i+j \leq d-\ell} c_{ij} X^i Y^j \right) \neq F(X,Y).$$

This says that $F(X,Y)$ cannot be decomposed into a product of a degree ℓ polynomial and a degree $d-\ell$ polynomial. The conjunction of these formulae for $0 < \ell < d$ suffices to state that $F(X,Y)$ is irreducible in first-order.

For (2), first we show that we may state that a point $(a, b) \in k^2$ on the affine curve $C = \{F(X, Y) = 0\}$ is singular. A point $(a, b) \in C$ is a singular point if and only if both of the partial derivatives F_x, F_y vanish at (a, b). Let $\rho(x, y)$ be the following formula:

$$(F(x, y) = 0 \wedge F_x(x, y) = 0 \wedge F_y(x, y) = 0)$$

This says that $x, y \in k$ form the coordinates of a singular point of C. To say that any singular point is a node, we only need to say that the Hessian determinant of F (where the Hessian matrix is the Jacobian of ∇F) is nonzero. Since the Hessian determinant is a polynomial, we may state this in first-order. Let $\eta(x, y)$ be the formula that determines this; then the formula

$$\forall x \forall y \, (\rho(x, y) \to \eta(x, y))$$

states that, if $(x, y) \in C$ is a singular point, it is a node.

For (3), since the genus of C is given by

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

where N is the number of distinct nodes [9, p. 314, Remark 3.11],[5] it suffices to state in first-order that the number of nodes is given by $g - \frac{1}{2}(d-1)(d-2)$. To do so, we make use of a standard technique in model theory: the so-called "$\exists^{(n)}$ modifier," which will allow us to state that there are precisely n distinct points for which a desired property holds. Let $s = g - \frac{1}{2}(d-1)(d-2)$. We want to say that there are precisely s distinct points $(x, y) \in C$ such that $k \models \rho(x, y)$. To say that a pair of points $(x_1, y_1), (x_2, y_2)$ are distinct, we may write

$$\neg (x_1 = x_2) \vee \neg (y_1 = y_2)$$

and we may say that these are distinct nodes of C by taking the conjunction of the above with $\rho(x_1, y_1) \wedge \rho(x_2, y_2)$. It is then easy to see that we may state that there are s distinct points $\{(x_1, y_1), \ldots, (x_s, y_s)\}$ which are all nodes of C. To say that this is all of them, we may say

$$\forall a \, \forall b \left(\rho(a, b) \to \bigvee_{i=1}^{s} (a = x_i \wedge b = y_i) \right)$$

That is to say, any other point $(a, b) \in C$ which is a node (i.e. $\rho(a, b)$ holds) must be equal to one of the points in our list. This concludes the proof. □

Lemma 3.2.2 ([5, p. 954, Lemma 20]) *Let k be an algebraically closed field, and suppose K is a function field of dimension 1 over k. Let $C' : F(X_1, X_2) = 0$ be an affine plane curve. If there exists a dominant rational map from $C(K)$ to C', then there exists a pair $(x_1, x_2) \in K^2 \setminus k^2$ such that $F(x_1, x_2) = 0$.*

[5] Observe that this equation is a modification of the Plücker formula in the setting of singular curves.

Proof Let $L = k(C')$ be the function field of C'. Then a dominant rational map $C(K) \to C'$ induces an inclusion $L \hookrightarrow K$ of k-algebras. So L is (isomorphic to) a subfield of K, and we can take $(x_1, x_2) \in L^2 \setminus k^2$ such that $F(x_1, x_2) = 0$ to conclude. □

Theorem 3.2.3 ([5, p. 954, Proposition 21]) *There exists a set of first order sentences $\{\varphi_m \mid m \in \mathbb{N}, m \geq 1\}$ in $\mathcal{L}$ such that, if K is a function field of dimension 1 over an algebraically closed field k, then the following hold:*

1. *$K \models \neg\varphi_m$ for each $m \geq 1$ if and only if $\gamma(K/k) = 0$.*
2. *If $g \in \mathbb{N} \setminus \{0\}$, $K \models \varphi_g$ and $K \models \neg\varphi_m$ for all $m > g$ if and only if $\gamma(K/k) = g$.*

Proof First we define φ_1, applying Theorem 3.1.13 to quantify over elements of k:

> "There exists a collection (x_{ij}) in k where $0 \leq i + j \leq 3$ and there exist $x, y \in K$ not both in k, such that the projective closure of the affine plane curve given by
>
> $$\sum_{0 \leq i+j \leq 3} x_{ij} X^i Y^j = 0$$
>
> is a non-singular cubic curve, and
>
> $$\sum_{0 \leq i+j \leq 3} x_{ij} y_1^i y_2^j = 0.$$"

For $m > 1$, we apply Proposition 3.2.1. For $0 \leq d \leq D(m)$ (where $D(m)$ is given by Theorem 2.2.4), let θ_d state the following:

> "There exists a collection (x_{ij}) in k where $0 \leq i+j \leq 3$ and there exist $x, y \in K$ not both in k such that the polynomial
>
> $$F(X, Y) = \sum_{0 \leq i+j \leq d} x_{ij} X^i Y^j$$
>
> is irreducible of degree d, and the projective closure of the curve it cuts out is generic of genus m, and $F(x, y) = 0$."

Now let $\varphi_m = \bigvee_{i=0}^{D(m)} \theta_d$. Then if $K \models \varphi_m$ it must be that $\gamma(K/k) \geq m$, by Proposition 3.1.4. Conversely, if $\gamma(K/k) = g$, then there are three cases. If $g \geq 2$, then applying Theorem 2.2.4 yields that $K \models \theta_d$ for some $0 \leq d \leq D(g)$, hence $K \models \varphi_g$. Otherwise, $g = 1$, and K is the function field of an elliptic curve over k. Since any elliptic curve over k is birationally equivalent to a cubic curve [19, p. 59, Proposition III.3.1], it must be that $K \models \varphi_1$. Otherwise $\gamma(K/k) = 0$, in which case there is no inclusion of a higher genus function field into K, so $K \models \neg\varphi_m$ for all m. □

Corollary 3.2.4 *Let K, L be two function fields over an algebraically closed field k, and suppose that $K \equiv_{\mathcal{L}} L$. Then $\gamma(K/k) = \gamma(L/k)$.*

Proof $K \models \varphi_m$ if and only if $L \models \varphi_m$ for all $m \in \mathbb{N}$. □

Remarks on Further Results

We have so far exhibited the definability of the field of constants, as well as definability of the genus, of a function field over an algebraically closed field. It should be noted that the definability of the base field holds over other kinds of fields satisfying the hypotheses of Lemma 3.1.12. In particular, this holds for real closed and separably closed fields [5, p. 951, Corollary 11].

Results of Pop [15] show the definability of transcendence degree. This result, along with others, will be discussed further at the end of the chapter to follow, in a context which allows their applications to be seen readily.

Chapter 4

Elementary Equivalence and Isomorphism

At the end of Section 2.4, we briefly discussed the relationship between elementary equivalence and isomorphism. While it is obvious that isomorphism is stronger than elementary equivalence, it is a very deep and natural question to ask the converse. In this chapter, we will make precise some results regarding this relationship for function fields of curves over algebraically closed fields.

Throughout this chapter, $\mathcal{L} = \{0, 1, +, \cdot\}$ is the language of fields, and k is an algebraically closed field. If K is an (algebraic) function field over k of dimension 1, then there exists a nonsingular projective curve over k, which we will denote $C(K)$, such that K is (isomorphic to) the function field of $C(K)$. Such a K will be denoted simply as the *function field of a curve over* k.

If K, L are function fields of curves over k such that $K \equiv_{\mathcal{L}} L$, we will split into cases, based on the genus $\gamma(L/k)$ of the curve $C(L)$: if $\gamma(L/k) = 0$, we already have the tools to show that $K \cong_k L$, and will do so momentarily. Then we show that $K \cong L$ if $\gamma(L/k) \geq 2$, which is the most involved result outside of the genus one case. We will also show, for a sufficient choice of finite $A \subseteq k$, that $K \equiv_{\mathcal{L}(A)} L$ implies $K \cong_k L$. Once we prove a quick lemma, this will follow readily by application of Riemann-Hurwitz.

If $\gamma(L/k) = 1$, then we arrive at the case of elliptic curves. In this case, we will show that $K \cong L$ if $\operatorname{Char} k = 0$ and the elliptic curve $E(L)$ does not have complex multiplication. In principle, first-order rigidity holding when $E(L)$ is without complex multiplication corresponds to the fact that the endomorphism ring of the lattice is not "too large." In practice, the proof of this utilizes a number of nontrivial results arising from the theory of elliptic curves.

4.1 The Higher Genus Case

Proposition 4.1.1 ([6, p. 809, Theorem 4]) *Let k be algebraically closed, and let K be a function field of a curve over k. If L is a function field over k with $\gamma(L/k) = 0$ and $K \equiv_{\mathcal{L}} L$, then $K \cong_k L$.*

Proof By Corollary 3.2.4, since $K \equiv_{\mathcal{L}} L$, we have that $\gamma(K/k) = \gamma(L/k) = 0$. But any function field for a genus zero curve is k-isomorphic to the field $k(x)$ of rational functions in one variable, since any genus zero curve is birationally equivalent to $\mathbb{P}^1(k)$. So $K \cong_k L$ follows. □

Lemma 4.1.2 ([6, p. 808, Lemma 3]) *Let k be algebraically closed, K a function field for a curve over k, and let $C(K)$ be the associated non-singular projective curve. Let $A \subseteq k$ be the set of coefficients of a collection of generators of the homogeneous ideal for $C(K)$. If L is another function field for a curve over k such that $K \equiv_{\mathcal{L}(A)} L$, then there exists a k-algebra homomorphism $K \hookrightarrow L$. Equivalently, there exists a dominant morphism $C(L) \to C(K)$.*

Proof Elementary equivalence in $\mathcal{L}$ is enough to show that $\gamma(K/k) = \gamma(L/k)$. We also have by application of Theorem 3.2.3 that, if $d \in \mathbb{N}$ with $\operatorname{Char} k \nmid d$ such that $\frac{1}{2}(d-1)(d-2) > \gamma(K/k)$, the formula $\xi_d(x) = \exists y \left(x^d + y^d = 1\right)$ gives that $x \in k$. Now working in the language $\mathcal{L}(A)$, we make use of the $\mathcal{L}(A)$-sentence

$$\exists \overline{x} \left(\bigwedge_{n=1}^{m} P_n(\overline{x}) = 0 \wedge \bigvee_{n=1}^{m} \neg \xi_d(x_n) \right)$$

where $P_1, \ldots, P_m$ is a family of generators for $C(K)$ for which the constants from K occurring in the P_n are precisely the elements of A. Since the above $\mathcal{L}(A)$-sentence holds in K, it holds in L. Let $\overline{a} = a_1, \ldots, a_m \in L$ not all in k witness the above sentence. Then $k(\overline{a}) \subseteq L$ is k-isomorphic to K. This induces a k-algebra homomorphism $K \hookrightarrow L$. □

Theorem 4.1.3 ([6, p. 809, Theorem 5]) *Let K be a function field for a curve over algebraically closed k with $\gamma(K/k) \geq 2$. Let $C(K)$ be the associated curve, and let $A \subseteq k$ be the set of coefficients of a set of generators of $C(K)$. Then for any function field L for a curve over k with $K \equiv_{\mathcal{L}(A)} L$, we have $K \cong_k L$.*

Proof First, we apply Corollary 3.2.4 to see that, since $K \equiv_{\mathcal{L}(A)} L$, we have that $\gamma(K/k) = \gamma(L/k) \geq 2$. Then we apply Lemma 4.1.2 to realize K as a subfield of L. But then the Riemann-Hurwitz formula gives that the morphism $C(L) \to C(K)$ of curves must be an isomorphism, since it is a degree 1 map between smooth curves. This exhibits $K \cong_k L$. □

Theorem 4.1.4 ([6, p. 809, Theorem 6]) *Let k be algebraically closed, K a function field of a curve over k. If L is a function field of a curve over k with $\gamma(L/k) \geq 2$ and $K \equiv_{\mathcal{L}} L$, then $K \cong L$.*

Before beginning the proof, note the difference between this theorem and the previous one; the condition $K \equiv_{\mathcal{L}} L$ is weaker than $K \equiv_{\mathcal{L}(A)} L$, but the conclusion $K \cong L$ is also weaker than $K \cong_k L$. That is to say, the theorem at hand states that elementary equivalence in the language of rings gives isomorphism of abstract fields. On the other hand, to obtain a k-algebra isomorphism in the proof of Theorem 4.1.3, we needed a language large enough to satisfy the conditions of Lemma 4.1.2.

Proof The curves $C(K), C(L)$ are birationally equivalent to generic affine plane curves C and C', respectively, by Theorem 2.2.3. Let $\Pi, \Pi' \subseteq k[X,Y]$ be sets of generators for the ideals associated to C and C', respectively. Let $\mathcal{A}, \mathcal{A}' \subseteq \mathcal{P}(k)$ consist of sets of coefficients of elements of Π and Π', respectively. Identify $F = k^{\text{abs}}$ as the prime subfield of k, and define the following:

$$N(K) = \min\left\{\operatorname{trdeg}_F F(E) \mid E \in \mathcal{A}\right\}$$
$$N(L) = \min\left\{\operatorname{trdeg}_F F(E') \mid E' \in \mathcal{A}'\right\}$$

Since at the present K and L are indistinguishable (as $L \equiv_{\mathcal{L}} K \Longrightarrow \gamma(K/k) = \gamma(L/k)$), without loss of generality, we may assume $N(K) \leq N(L)$. Choose some $A \in \mathcal{A}$ such that $\operatorname{trdeg}_F F(A) = N(K)$, and write $A = \left\{a_0, \ldots, a_{N(K)}, \ldots, a_N\right\}$, where $\left(a_0, \ldots, a_{N(K)}\right)$ is a transcendence base for $F(A)$. Let $P(Z_0, \ldots, Z_N, X, Y) \in \mathbb{Z}\left[Z_1, \ldots, Z_N, X, Y\right]$ such that $P(a_0, \ldots, a_N, X, Y) \in \Pi$. By Theorem 3.1.13, k is definable in both K and L by the same formula $\xi_d(x)$ for some $d \in \mathbb{N}$, since the characteristic is fixed. Thus, by Proposition 3.2.1, there exists an $\mathcal{L}$-formula $\chi\left(z_1, \ldots, z_N\right) \in \mathrm{Fm}_{\mathcal{L}}$ such that, for $c_0, \ldots, c_N \in k$, $K \models \chi\left(c_0, \ldots, c_N\right)$ if and only if $P(c_0, \ldots, c_N, X, Y)$ is irreducible and defines an affine plane curve over k of genus $g = \gamma(K/k)$ whose projective closure is generic.

Now for $N(K) \leq i < N$, let $R_i(U_0, \ldots, U_i, X) \in \mathbb{Z}\left[U_0, \ldots, U_i, X\right]$ be some polynomial in $i+2$ variables such that $R_i(a_0, \ldots, a_i, X)$ is the minimal polynomial of the field extension $F\left(a_0, \ldots, a_{i+1}\right)/F(a_0, \ldots, a_i)$. Now we define the following $\mathcal{L}$-formulae:

$$\Phi\left(u_0, \ldots, u_N\right) : \left(\bigwedge_{i=0}^{N} \xi_d(u_i) \wedge \bigwedge_{i=N(K)}^{N-1} \left(R_i(u_0, \ldots, u_i) = 0\right) \wedge \chi\left(u_0, \ldots, u_N\right)\right)$$
$$\Psi\left(u_0, \ldots, u_N\right) : \exists x \exists y \left(P\left(u_0, \ldots, u_N, x, y\right) = 0 \wedge \left(\neg \xi_d(x) \wedge \neg \xi_d(y)\right)\right)$$

Then for any $u_0, \ldots, u_N \in K$, we have that $K \models \Phi\left(u_0, \ldots, u_N\right)$ if and only if the following conditions hold:

- $u_0, \ldots, u_N \in k$,
- each u_{i+1} is a root of $R_{i+1}\left(u_0, \ldots, u_i, X\right)$ for $N(K) \leq i < N$, and
- The polynomial $P\left(c_0, \ldots, c_N, X, Y\right)$ is irreducible, and defines a genus g affine curve whose projective closure is generic.

For any $u_0, \ldots, u_N \in K$, $K \models \Psi\left(u_0, \ldots, u_N\right)$ if and only if there exist some $x, y \in K \setminus k$ such that $P\left(u_0, \ldots, u_N, x, y\right) = 0$. Since $P(a_0, \ldots, a_N, X, Y) \in \Pi$, $K \models \exists \overline{u}\left(\Phi\left(\overline{u}\right) \wedge \Psi\left(\overline{u}\right)\right)$, and thus $K \equiv_{\mathcal{L}} L$ gives that $L \models \exists \overline{u}\left(\Phi(\overline{u}) \wedge \Psi\left(\overline{u}\right)\right)$. Let $b_0, \ldots, b_N \in L$ realize this sentence. Then the affine plane curve $X : P(b_0, \ldots, b_N, x, y) = 0$ is of the same genus $g = \gamma(L/k) \geq 2$ as the function field L, hence L is the function field of X. Consequently, $N(L) \leq N(K)$,

and thus $N(K) = N(L)$. So we may realize an isomorphism between $F\left(a_0, \ldots, a_{N(K)}\right)$ and $F\left(b_0, \ldots, b_{N(L)}\right)$ by sending each a_i to b_i, for $0 \leq i \leq N(K)$.

Now, we have that $R_{N(K)+1}\left(a_0, \ldots, a_{N(K)}, X\right)$ is irreducible over $F\left(a_0, \ldots, a_{N(K)}\right)$ and $R_{N(K)+1}\left(b_0, \ldots, b_{N(K)}\right)$ is irreducible over $F\left(b_0, \ldots, b_{N(K)}\right)$. So we may extend this isomorphism to one from $F\left(a_0, \ldots, a_{N(K)+1}\right)$ to $F\left(b_0, \ldots, b_{N(K)+1}\right)$. Iterating this argument yields an isomorphism from $F(A)$ to $F(B)$, hence an isomorphism from $\overline{F(A)}$ to $\overline{F(B)}$, hence an automorphism of k which induces an isomorphism from K to L. □

4.2 The Genus One Case

In this section, k will again be algebraically closed, and we will further suppose that $\operatorname{Char} k = 0$. If L is the function field of an elliptic curve $E(L)$ over k with modular invariant j, denote by $\mathcal{L}(j)$ the language $\mathcal{L}$ of rings with an additional constant symbol for j. Further, if $F = \overline{\mathbb{Q}(j)}$ is the algebraic closure of $\mathbb{Q}(j) \subseteq k$, let $\mathcal{L}(F)$ be the language of rings with additional constant symbols from F.

Our two main goals now will be as follows. Let L be a function field of an elliptic curve over k without complex multiplication. Given any other function field K of a curve over k, we will show that elementary equivalence in $\mathcal{L}$ is enough to show that K and L are isomorphic as abstract fields. Before doing so, we will show that, if $j \in k$ is the modular invariant of L, and $K \equiv_{\mathcal{L}(j)} L$, then K and L are isomorphic as k-algebras. The overall structure of these proofs are given by the following implications:

$$K \ncong_k L \implies K \not\equiv_{\mathcal{L}(F)} L \implies K \not\equiv_{\mathcal{L}(j)} L \tag{4.1}$$

$$K \ncong L \implies K \not\equiv_{\mathcal{L}} L \tag{4.2}$$

The hardest among these implications is in fact the first one. This is because it will require a reduction to the case that k is a subfield of $\mathbb{C}$, and to do this, we must first acquire a technical lemma via model-theoretic techniques. Once this is obtained, we will be able to implement the analytic tools at our disposal over $\mathbb{C}$.

Some Necessary Results Involving Weierstrass Equations

We saw in Section 2.3 some relevant properties of the Weierstrass $\wp$ function of an elliptic curve. In order to utilize the full strength of its properties when solving first-order problems for elliptic curves (which we will do in the genus one case), we require some results involving the algebraicity of coefficients which relate two elliptic curves and their Weierstrass functions. We have saved the presentation of these results until now because some aspects of the proofs to follow require model-theoretic tools.

Proposition 4.2.1 ([6, p. 815, Proposition 29]) *Let $\Lambda = \langle \omega_1, \omega_2 \rangle$ be a lattice, and let $\wp$ be its Weierstrass function, which satisfies*

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3.$$

Then for any $0 \neq n \in \mathbb{N}$ and any $1 \leq k \leq n-1$, $\wp(k\omega_1/n)$ and $\wp'(k\omega_1/n)$ are algebraic over $\mathbb{Q}(g_2, g_3)$.

Proof Supposing that $\wp(\omega_1/n)$ and $\wp'(\omega_1/n)$ are algebraic over $\mathbb{Q}(g_2, g_3)$, we may readily show that the other values are, by application of one of the Weierstrass addition formulae [3, p. 21, Theorem 2.2]:

$$\wp(u+v) = \frac{1}{4}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2 - \wp(u) - \wp(v) \tag{4.3}$$

Letting $u = v = \omega_1/n$ and proceeding by induction suffices to show that $\wp(k\omega_1/n)$ is algebraic over $\mathbb{Q}(g_2, g_3)$. The Weierstrass differential equation yields that $\wp'(\omega_1/n)$ is algebraic over $\mathbb{Q}(g_2, g_3, \wp(\omega_1/n))$, so we have reduced to showing that $\wp(\omega_1/n)$ is algebraic over $\mathbb{Q}(g_2, g_3)$. For this, we use quantifier elimination in ACF. First, observe by Λ-periodicity of $\wp$:

$$\wp(\omega_1/n) = \wp((n-1)\omega_1/n)$$

thus $\wp(\omega_1/n)$ is a witness to the following $\mathcal{L}(g_2, g_3)$-formula:

$$\theta(x) : \exists y \left(y^2 = 4x^3 - g_2 x - g_3 \wedge Q_k(x,y) \neq 0 \wedge xQ_k(x,y) - P_k(x,y) = 0\right) \tag{4.4}$$

where $P_k, Q_k \in \mathbb{Q}(g_2, g_3)[x, y]$ are polynomials such that the following holds:

$$\wp(ku) = \frac{P_k(\wp(u), \wp'(u))}{Q_k(\wp(u), \wp'(u))}$$

The existence of such a rational expression follows again by the addition formula given in eq. (4.3) above. Now we apply quantifier elimination to the formula $\theta(x)$ given in eq. (4.4). Since $\theta(x)$ is equivalent to some quantifier-free formula, it is equivalent to some boolean combination of formulae of the form $P(x) = 0$, where $P \in \mathbb{Q}(g_2, g_3)[x]$. So if there are only finitely many $a \in \mathbb{C}$ such that $\theta(a)$ holds, this shows that any witness to $\theta(x)$ is cut out by polynomial equations. In particular, this would entail that $\wp(\omega_1/n)$ is algebraic over $\mathbb{Q}(g_2, g_3)$.

So suppose $\mathbb{C} \models \theta(a)$, and let $b \in \mathbb{C}$ witness the existential statement in $\theta(a)$. Then

$$\wp(u) = a = \frac{P_k(a,b)}{Q_k(a,b)} = \frac{P_k(\wp(u), \wp'(u))}{Q_k(\wp(u), \wp'(u))} = \wp((n-1)u).$$

But there are only finitely many equivalence classes mod Λ for which $\wp(u) = \wp((n-1)u)$ (indeed, there are precisely $n^2 - 1$ of them). So there are only finitely many witnesses to $\theta(x)$, and we conclude that $\mathbb{C} \models \theta(\wp(\omega_1/n))$ implies that $\wp(\omega_1/n)$ is algebraic over $\mathbb{Q}(g_2, g_3)$. $\square$

Proposition 4.2.2 ([6, p. 815, Proposition 30]) *Let $\Lambda = \langle \omega_1, \omega_2 \rangle$ and $\Lambda' = \langle \omega_1/n, \omega_2 \rangle$ be lattices, and let $\wp_1, \wp_n$ be their respective Weierstrass functions. If $g_2^1, g_3^1 \in \mathbb{C}$ satisfy the following equation:*

$$\left(\wp_1'\right)^2 = 4\wp_1^3 - g_2^1\wp_1 - g_3^1$$

then there exists a rational function $F(x) \in \overline{\mathbb{Q}\left(g_2^1, g_3^1\right)}(x)$ such that $F(\wp_1) = \wp_n$.

Proof We utilize the following classical result, expressing $\wp_n$ in terms of $\wp_1$ [20, p. 456]:

$$\wp_n\left(u\right) = \wp_1\left(u\right) + \sum_{k=1}^{n-1}\left[\wp_1\left(u + \frac{k\omega_1}{n}\right) - \wp_1\left(\frac{k\omega_1}{n}\right)\right]$$

The case where $n = 2$ is given in [3, p. 135]. For $n \neq 2$, we may reduce to the case where n is odd by application of the following expression [20, p. 442]:

$$\wp_1\left(u + \frac{\omega_1}{2}\right) = e_1^1 + \frac{\left(e_1^1 - e_2^1\right)\left(e_1^1 - e_3^1\right)}{\wp_1(u) - e_1^1}$$

where e_i^1 are the values of $\wp_1$ at the half-period zeroes of $\wp_1'$, known to be algebraic over $\mathbb{Q}\left(g_2^1, g_3^1\right)$. When n is odd, it is enough to apply [20, p. 444] and Proposition 4.2.1 to conclude. □

Proposition 4.2.3 ([6, p. 816, Proposition 31]) *Let $\Lambda = \langle \omega_1, \omega_2 \rangle$ and $\Lambda' = \langle \omega_1/n, \omega_2 \rangle$ be lattices, and let $\wp_1, \wp_n$ be their respective Weierstrass functions. Let $g_2^1, g_3^1, g_2^n, g_3^n \in \mathbb{C}$ satisfy*

$$\left(\wp_1'\right)^2 = 4\wp_1^3 - g_2^1\wp_1 - g_3^1$$
$$\left(\wp_n'\right)^2 = 4\wp_n^3 - g_2^n\wp_n - g_3^n$$

and let e_1^n, e_2^n, e_3^n be given by the following:

$$e_1^n = \wp_n\left(\frac{\omega_1}{2n}\right) \qquad e_2^n = \wp_n\left(\frac{\omega_2}{2}\right) \qquad e_3^n = \wp_n\left(\frac{\omega_1/n + \omega_2}{2}\right)$$

Then $e_1^n, e_2^n, e_3^n, g_2^n, g_3^n$ are algebraic over $\mathbb{Q}\left(g_2^1, g_3^1\right)$.

Proof By [20, p. 444], we have that the following hold:

$$e_1^n + e_2^n + e_3^n = 0$$
$$e_1^n e_2^n + e_1^n e_3^n + e_2^n e_3^n = -\frac{1}{4}g_2^n$$
$$e_1 e_2 e_3 = \frac{1}{4}g_3^n$$

The first of these yields that, if e_1^n, e_2^n are algebraic over $\mathbb{Q}\left(g_2^1, g_3^1\right)$, then so is e_3^n. The latter two equations show that algebraicity of e_1^n, e_2^n, e_3^n is enough to show algebraicity of g_2^n, g_3^n. So we reduce to showing that e_1^n, e_2^n are algebraic over $\mathbb{Q}\left(g_2^1, g_3^1\right)$. By Proposition 4.2.2, $e_1^n = F\left(\wp_1\left(\omega_1/2n\right)\right)$ and $e_2^n = F\left(\wp_1\left(\omega_2/2\right)\right)$, where F has coefficients algebraic over $\mathbb{Q}\left(g_2^1, g_3^1\right)$. So this reduces to showing that $\wp_1\left(\omega_1/2n\right)$ and $\wp_1\left(\omega_2/2\right)$ are algebraic over $\mathbb{Q}\left(g_2^1, g_3^1\right)$, which follows by application of Proposition 4.2.1. □

Proposition 4.2.4 ([6, p. 817, Proposition 32]) *Let $\Lambda, \Lambda', \wp_1, \wp_n, g_2^1$ and g_3^1 be as before, let $\Delta = \overline{\mathbb{Q}\left(g_2^1, g_3^1\right)}$, and let $\Delta \subseteq k \subseteq \mathbb{C}$ be any intermediary field. Then the following hold:*

1. *$k\left(\wp_n, \wp_n'\right) \subseteq k\left(\wp_1, \wp_1'\right)$;*
2. *$\wp_1$ is a primitive element of the field extension $k\left(\wp_1, \wp_1'\right)/k\left(\wp_n, \wp_n'\right)$;*
3. *$\mathbb{C}(\wp_1, \wp_1')$ is isomorphic to the meromorphic function field of the complex torus $\mathbb{C}/\Lambda$, and $\mathbb{C}\left(\wp_n, \wp_n'\right)$ is the meromorphic function field of $\mathbb{C}/\Lambda'$; and*
4. *There exists a polynomial $R\left(X, Y, Z\right) \in \mathbb{Z}\left[X, Y, Z\right]$ such that $R\left(\wp_n, \wp_n', Z\right)$ is the minimal polynomial of $k\left(\wp_1, \wp_1'\right)/k\left(\wp_n, \wp_n'\right)$. In particular, the minimal polynomial of $\wp_1$ over $k\left(\wp_n, \wp_n'\right)$ is independent of the choice of k.*

Proof For (1), Proposition 4.2.2 gives that $\wp_n = F(\wp_1)$ for some rational function F with coefficients in Δ, so $\wp_n \in \Delta\left(\wp_1, \wp_1'\right) \subseteq k\left(\wp_1, \wp_1'\right)$. Taking derivatives, we obtain $\wp_n' = \wp_1' F'\left(\wp_1\right)$.

For (2), it suffices to show that $\wp_1' \in \Delta\left(\wp_n, \wp_n', \wp_1\right)$. This follows again by the fact that $\wp_n' = \wp_1' F'(\wp_1)$.

The fact that (3) holds follows from the discussion in Section 2.3 on elliptic curves and complex tori. It is worth mentioning this again in this context because, in the case that $k = \mathbb{C}$, we see that $\wp_1$ is a primitive element of the field extension $\mathscr{E}\left(\Lambda\right)/\mathscr{E}\left(\Lambda'\right)$.

To show (4), observe that the ideal of $\left(\wp_n, \wp_n'\right)$ over k is defined by $Y^2 - 4X^3 + g_2^n X + g_3^n$, and thus is defined with coefficients from Δ by Proposition 4.2.3. So the subfields $\Delta\left(\wp_n, \wp_n'\right)$ and k of $k\left(\wp_n, \wp_n'\right)$ are linearly disjoint extensions of Δ (since $k \subseteq \mathbb{C}$). Furthermore, no element of $k\left(\wp_n, \wp_n'\right) \setminus \Delta\left(\wp_n, \wp_n'\right)$ can be algebraic over $\Delta\left(\wp_n, \wp_n'\right)$, since Δ is algebraically closed and k/Δ is a separable extension. Hence $\left[k\left(\wp_1, \wp_1'\right) : k\left(\wp_n, \wp_n'\right)\right] = \left[\Delta\left(\wp_1, \wp_1'\right) : \Delta\left(\wp_n, \wp_n'\right)\right]$, and the conclusion follows. □

Main Results in the Genus One Case

Lemma 4.2.5 ([6], p.818, Proposition 33) *Let K and L be function fields of elliptic curves over k, and let $j \in k$ be the modular invariant of K. Write $F = \overline{\mathbb{Q}(j)}$ to denote the algebraic closure of $\mathbb{Q}(j)$. If $K \equiv_{\mathcal{L}(j)} L$, then $K \equiv_{\mathcal{L}(F)} L$.*

Proof By contrapositive, suppose that there is a formula $\varphi\left(\overline{x}\right) = \varphi\left(x_0, \ldots, x_n\right) \in \mathrm{Fm}_{\mathcal{L}(j)}$ and a tuple $\overline{a} = a_0, \ldots, a_n \in F$ such that $K \models \varphi\left(\overline{a}\right)$ and $L \models \neg\varphi\left(\overline{a}\right)$. It suffices to show that there is a sentence $\psi \in \mathrm{Sent}_{\mathcal{L}(j)}$ such that $K \models \psi$ and $L \models \neg\psi$.

Let $M = \mathbb{Q}\left(j, \overline{a}\right)$ and choose a primitive element $\alpha \in M$ so that $M = \mathbb{Q}(j)(\alpha)$. Then take $\mu_{\alpha,\mathbb{Q}(j)}(X, Y) \in \mathbb{Z}\left[X, Y\right]$ such that $\mu_{\alpha,\mathbb{Q}(j)}(X, j)$ is the minimal polynomial of α over

$\mathbb{Q}(j)$. Observe that, by multiplying $\mu_{\alpha,\mathbb{Q}(j)}(X,j)$ by some sufficient choice of element of $\mathbb{Z}[j]$, we obtain a polynomial in $\mathbb{Z}[X,j]$. So for each $0 \leq i \leq n$, let $P_i(X,Y) \in \mathbb{Z}[X,Y]$ and $R_i \in \mathbb{Z}[Y]$ such that $a_i = P_i(\alpha,j)/R_i(j)$. Then we obtain:

$$L \models \exists x \exists \overline{y} \left(\mu_{i,\mathbb{Q}(j)}(x,j) = 0 \wedge \bigwedge_{i=0}^{n} \left(R_i(j) y_i = P_i(x,j) \right) \wedge \neg \varphi\left(\overline{y}\right) \right)$$

Observe that the above sentence is the negation of the following:

$$\forall x \forall \overline{y} \left(\mu_{i,\mathbb{Q}(j)}(x,j) = 0 \wedge \bigwedge_{i=0}^{n} \left(R_i(j) y_i = P_i(x,j) \right) \rightarrow \varphi\left(\overline{y}\right) \right) \tag{4.5}$$

Label the above sentence as $\psi \in \mathrm{Sent}_{\mathcal{L}(j)}$. Since $L \models \neg\psi$, to show that $\mathcal{L} \not\equiv_{\mathcal{L}(j)} K$, it suffices to show that $K \models \psi$.

Suppose that $\beta \in K$ satisfies $\mu_{i,\mathbb{Q}(j)}(\beta) = 0$ and $\overline{b} \in K$ satisfies $b_i = P_i(\beta,j)/R_i(j)$. Let $\sigma \in \mathrm{Aut}\left(F\right)$ such that $\sigma(\alpha) = \beta$. For all $0 \leq i \leq n$, σ satisfies the following:

$$\sigma(a_i) = \sigma\left(\frac{P_i(\alpha,j)}{R_i(j)} \right) = \frac{P_i\left(\sigma\left(\alpha\right),j\right)}{R_i(j)} = \frac{P_i\left(\beta,j\right)}{R_i\left(j\right)} = b_i.$$

Since K is the function field of a curve defined over $\mathbb{Q}(j)$, σ extends to a K-automorphism $\sigma' \in \mathrm{Aut}\left(K\right)$. Since $\sigma(a_i) = b_i$, the automorphism σ' exhibits $K \models \varphi(\overline{a}) \Longrightarrow K \models \varphi\left(\sigma'\left(\overline{a}\right)\right)$, hence $K \models \varphi\left(\overline{b}\right)$. So $K \models \psi$, completing the proof. □

Lemma 4.2.6 ([6], p.818, Proposition 34) *Let k, k' be algebraically closed fields of the same characteristic, Let $\Gamma \subseteq k \cap k'$ be algebraically closed, let $I \subseteq \Gamma\left[X_0, \ldots, X_n\right]$ be a prime ideal, and write $k\left(\overline{u}\right), k'\left(\overline{u}\right)$ to denote the function fields of the the affine varieties of the ideals $k \otimes_\Gamma I$ and $k' \otimes_\Gamma I$, respectively. If $\mathrm{trdeg}_\Gamma(k)$ and $\mathrm{trdeg}_\Gamma(k')$ are infinite, then $k\left(\overline{u}\right) \equiv_{\mathcal{L}(\Gamma)} k'\left(\overline{u}\right)$.*

To prove this, we make use of a back-and-forth argument. The idea is as follows: given any finite subset $A \subseteq k$, A is contained in an algebraically closed subfield Δ of k of finite transcendence degree over Γ. We will then realize this as isomorphic to an algebraically closed subfield $\Delta' \subseteq k'$. To realize A as having the same type as its image (that is, A will have the same first-order properties as A'), we need to ensure that their properties relating to other elements of $k\left(\overline{u}\right)$ are the same as those of A' with respect to the other elements of $k'\left(\overline{u}\right)$. To do this, we show that we can extend this isomorphism $\Delta\left(\overline{u}\right) \cong \Delta'\left(\overline{u}\right)$ to larger subfields $M\left(\overline{u}\right), M'\left(\overline{u}\right)$ where M, M' are algebraically closed, and either M contains any specified element $w \in k\left(\overline{u}\right)$, or M' contains any specified $w' \in k'\left(\overline{u}\right)$. In other words, we are showing that we may extend any of our specified isomorphisms to a larger one, which includes any specified element of either field. Explicitly, this is a sort of clever application of the following result:

Lemma 4.2.7 (Tarski-Vaught Test) *Let $\mathcal{N}$ be an $\mathcal{L}$-structure, and $\mathcal{M}$ a substructure of $\mathcal{N}$. Then $\mathcal{M}$ is an elementary substructure of $\mathcal{N}$ if and only if, for any $\mathcal{L}$-formula $\varphi\left(w, \overline{v}\right)$ and*

any $\overline{a} \in M$, if there exists some $b \in N$ such that $\mathcal{N} \models \varphi(b, \overline{a})$, then there exists some $c \in \mathcal{M}$ such that $\mathcal{N} \models \varphi(c, \overline{a})$.

Proof See [11, p. 45, Proposition 2.3.5]. □

For a more detailed discussion on back-and-forth arguments and examples, see [11, §2.4].

Proof of Lemma 4.2.6 Suppose $\Gamma \subseteq \Delta \subseteq k$ and $\Gamma \subseteq \Delta' \subseteq k'$ where Δ, Δ' are algebraically closed of finite transcendence degree over Γ. Define $\mathcal{I}(\Delta, \Delta')$ to be the set given by

$$\mathcal{I}(\Delta, \Delta') = \{ f : \Delta(\overline{u}) \cong \Delta'(\overline{u}) \mid \forall 1 \leq j \leq n, f(u_j) = u_j \}.$$

That is, $\mathcal{I}(\Delta, \Delta')$ is the set of all isomorphisms between the function fields associated to the ideals $I \otimes_\Gamma \Delta$ and $I \otimes_\Gamma \Delta'$. Let $\mathscr{F}$ be given by

$$\mathscr{F} = \bigcup_{\Delta, \Delta'} \mathcal{I}(\Delta, \Delta')$$

where the union ranges over all $\Gamma \subseteq \Delta \subseteq k$ and all $\Gamma \subseteq \Delta' \subseteq k'$ algebraically closed and of finite transcendence degree over Γ. Observe that $\mathscr{F}$ is nonempty, since $1_{\Gamma(\overline{u})} \in \mathcal{I}(\Gamma, \Gamma)$. So $\mathscr{F}$ is a nonempty family of partial elementary maps between $k(\overline{u})$ and $k'(\overline{u})$. Thus, it now suffices to show the following two conditions hold:

1. For any $f \in \mathscr{F}$ and any $w \in k(\overline{u})$, there exists some $g \in \mathscr{F}$ such that $f \subseteq g$ and w is contained in the domain of g (the "forth" direction);

2. For any $f \in \mathscr{F}$ and any $w' \in k'(\overline{u})$, there exists some $g' \in \mathscr{F}$ such that $f \subseteq g'$ and w' is contained in the image of g' (the "back" direction).

Let $f : \Delta(\overline{u}) \cong \Delta'(\overline{u}) \in \mathscr{F}$ for some Δ, Δ'. Let $w \in k(\overline{u})$, and choose a rational function $F(\overline{x}) \in k(\overline{x})$ such that $F(\overline{u}) = w$. If $A \subseteq k$ consists of the coefficients from F, let $b_1, \ldots, b_m$ be a transcendence base for $\Delta(A)$ over Δ. Since $\mathrm{trdeg}_\Gamma(k')$ is infinite and $\mathrm{trdeg}_\Gamma(\Delta')$ is finite, $\mathrm{trdeg}_{\Delta'}(k')$ is infinite. So we may choose a set $\{b'_1, \ldots, b'_m\} \subseteq k'$ which is algebraically independent over Δ', so that $f\big|_\Delta$ induces an isomorphism

$$f^* : \overline{\Delta(b_1, \ldots, b_m)} \cong \overline{\Delta'(b'_1, \ldots, b'_m)}$$

where $f^*(b_i) = b'_i$ for $0 \leq i \leq m$. Labeling the source and target of f^* as M and M' respectively, we have an isomorphism $f' : M(\overline{u}) \cong M'(\overline{u})$, where $f'(u_i) = u_i$ for each $0 \leq i \leq n$. This exhibits the "forth" direction of the argument.

Note the symmetry in this setting; as it stands, k, k' are indistinguishable in terms of their assumed properties, as are M and M'. So the argument above showing that we may extend the isomorphism f to f' applies the same in the other direction: that is, we may just as easily extend f' to some isomorphism $\widetilde{f} : N(\overline{u}) \cong N'(\overline{u})$, where $w' \in k'$ is any element of k', and the fields $M \subseteq N \subseteq k, M' \subseteq N' \subseteq k'$ are both algebraically closed such that $w' \in N'$. This exhibits the "back" direction. □

We will immediately make use of this lemma in the case that $\Gamma = \overline{\mathbb{Q}(j)}$, k is any algebraically closed field of characteristic zero, and $k' = \mathbb{C}$. This will allow us to use analytic techniques to exhibit that elementary equivalence in $\mathcal{L}(j)$ gives k-isomorphism.

Theorem 4.2.8 ([6], p.818, Theorem 35) *Let K be the function field for a curve over k, and let L be the function field of an elliptic curve over k without complex multiplication, with modular invariant $j \in k$. If $K \equiv_{\mathcal{L}(j)} L$, then $K \cong_k L$.*

Proof We perform casework on j: if $j = 0$, let $a = 0, b = 1$. If $j = 1728$, let $a = 1, b = 0$. In all other cases, let

$$a = 3j\,(j - 1728) \qquad\qquad b = j\,(j - 1728)^2$$

so that $L = k\,(\wp, \wp')$, where $\wp \in L$ is the Weierstrass equation of L, satisfying

$$(\wp')^2 = 4\wp^3 - a\wp - b.$$

Suppose $\mathrm{trdeg}_{\mathbb{Q}}\,(k) > 2^{\aleph_0}$. There exists a subfield of $\mathbb{C}$ isomorphic to $\overline{\mathbb{Q}(j)}$. By Lemma 4.2.6, since $\overline{\mathbb{Q}\,(j)}$ is realized as an algebraically closed subfield of both k and $\mathbb{C}$, we find that $L = k(\wp, \wp') \equiv_{\mathcal{L}(j)} \mathbb{C}(u, v)$ where $u, v \notin \mathbb{C}$ satisfy $v^2 = 4u^3 - au - b$. In this case, we can simply consider the elliptic function field over $\mathbb{C}$. Otherwise, $\mathrm{trdeg}_{\mathbb{Q}}(k) \leq \mathrm{trdeg}_{\mathbb{Q}}(\mathbb{C})$, and thus k embeds into $\mathbb{C}$. So without loss of generality, we may suppose that k is a subfield of $\mathbb{C}$.

Now by contrapositive: suppose $K \ncong L$. Our goal is to show that $K \not\equiv_{\mathcal{L}(j)} L$. By the $\mathcal{L}$-definability of genus, if $\gamma\,(K/k) \neq \gamma(L/k)$, then $K \not\equiv_{\mathcal{L}} L$, which implies that $K \not\equiv_{\mathcal{L}(j)} L$. So without loss of generality, we may suppose that $\gamma(K/k) = 1$, and thus K is the function field of an elliptic curve over k. Let j' be the associated modular invariant of K.

We have by Lemma 4.1.2 that, since the only parameters occurring in the Weierstrass equation for L are integers and j, if $K \equiv_{\mathcal{L}(j)} L$, then there is an inclusion $L \hookrightarrow K$ of k-algebras. Note that this gives that K and L have isogenous elliptic curves. So since L does not have complex multiplication, neither does K. In particular, we now have that the conditions placed upon K and L are equivalent.

Suppose then that K is a subfield K which is k-isomorphic to L. Applying extension of scalars, $K' \otimes_k \mathbb{C}$ is a subfield of $K \otimes_k \mathbb{C}$, and these are two function fields for elliptic curves over $\mathbb{C}$. Let Λ be a lattice whose function field $\mathscr{E}(\Lambda)$ is $\mathbb{C}$-isomorphic to $K \otimes_k \mathbb{C}$, and let its Weierstrass function be $\wp_1$. We may also choose a lattice $\Lambda' \supseteq \Lambda$ such that $K' \otimes_k \mathbb{C}$ is $\mathbb{C}$-isomorphic to $\mathscr{E}(\Lambda')$.

Write $\omega_1, \omega_2 \in \mathbb{C}$ to be a basis for Λ, and choose $m, n \in \mathbb{N}$ such that $\{\omega_1/mn, \omega_2/n\}$ is a basis for Λ'. Write $\mathscr{E}(\langle \omega_1/n, \omega_2 \rangle) = \mathbb{C}(\wp_n, \wp_n')$. We have that this is $\mathbb{C}$-isomorphic to $\mathscr{E}(\Lambda')$. By Proposition 4.2.4, $k(\wp_n, \wp_n')$ is a subfield of $k(\wp_1, \wp_1')$, and $k\,(\wp_1, \wp_1')$ is k-isomorphic to K. Moreover, $k(\wp_n, \wp_n') = k(m^2\wp_n, m^3\wp_n') \cong_k L \cong_k K'$, by application of the following homogeneity property of the Weierstrass differential equation:

$$\left(m^3\wp_n'\right)^2 = 4\left(m^2\wp_n\right)^3 - g_2(\Lambda')\left(m^2\wp_n\right) - g_3(\Lambda').$$

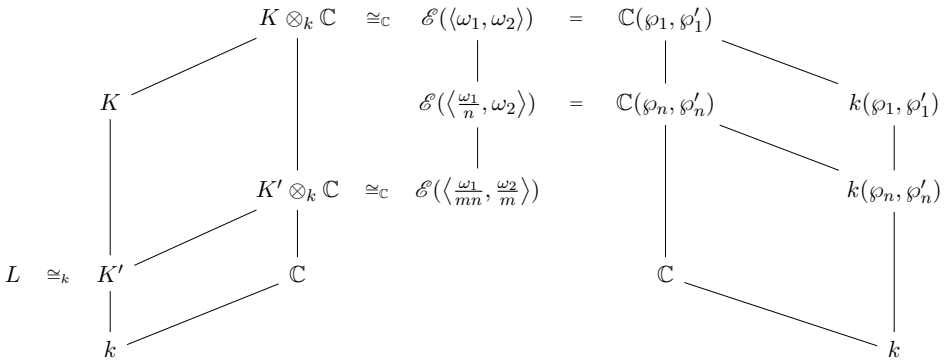

Figure 4.1: The structure of the proof of Theorem 4.2.8

Let $g_2^n = g_2\left(\langle \frac{\omega_1}{n}, \omega_2 \rangle\right)$ and $g_3^n = g_3\left(\langle \frac{\omega_1}{n}, \omega_2 \rangle\right)$ be the coefficients associated to the lattice whose elliptic function field is $\mathbb{C}(\wp_n, \wp_n')$. Let $P(X,Y,Z) \in \overline{\mathbb{Q}(j)}[X,Y,Z]$ such that $P(\wp_n, \wp_n', Z)$ is the minimal polynomial of $\wp_1$ over $\overline{\mathbb{Q}(j)}(\wp_n, \wp_n')$; note that this is also the minimal polynomial of $\wp_1$ over $k(\wp_n, \wp_n')$ by Proposition 4.2.4.

Let $\theta(x) \in \mathrm{Fm}_{\mathcal{L}}$ be the formula defining k as a subfield of $k(\wp_n, \wp_n')$; note that the same formula defines k as a subfield of $k(\wp_1, \wp_1'), \mathbb{C}(\wp_1, \wp_1')$, and $\mathbb{C}(\wp_n, \wp_n')$. Letting $x = \wp_n$ and $y = \wp_n'$, since $k(\wp_n, \wp_n') \not\cong_k k(\wp_1, \wp_1')$, we may observe the following:

$$k(\wp_n, \wp_n') \models \exists x \exists y \left(\neg\theta(x) \wedge \left(y^2 = 4x^3 - g_{2,n}x - g_{3,n}\right) \wedge \forall z \left(P(x,y,z) \neq 0\right)\right) \tag{4.6}$$

Recall that our goal is to show that $K \not\equiv_{\mathcal{L}(j)} L$. By the exhibited isomorphisms above, this is equivalent to showing that $k(\wp_1, \wp_1') \not\equiv_{\mathcal{L}(j)} k(\wp_n, \wp_n')$. Using Lemma 4.2.5, it suffices to show that $k(\wp_1, \wp_1')$ satisfies the negation of the formula in eq. (4.6), that is, it suffices to show that the following holds:

$$k(\wp_1, \wp_1') \models \forall x \forall y \left(\neg\theta(x) \wedge \left(y^2 = 4x^3 - g_{2,n}x - g_{3,n}\right) \rightarrow \exists z \left(P(x,y,z) = 0\right)\right)$$

Let $u_0, v_0 \in k(\wp_1, \wp_1')$ with $u_0 \notin k$ such that $v_0^2 = 4u_0^3 - g_{2,n}u_0 - g_{3,n}$. To show that there exists some $w_0 \in k(\wp_1, \wp_1')$ such that $P(u_0, v_0, w_0) = 0$. Observe that, if such a w_0 exists, it is algebraic over $\overline{\mathbb{Q}(j)}(u_0, v_0)$ (since it would be a root of the polynomial $P(u_0, v_0, Z)$). Since Proposition 4.2.4 gives that $k(\wp_1, \wp_1')$ is relatively algebraically closed in $\mathbb{C}(\wp_1, \wp_1')$, if such a $w_0 \in \mathbb{C}(\wp_1, \wp_1')$ exists, then it lies in in $k(\wp_1, \wp_1')$. So we have reduced to showing that there is such a $w_0 \in \mathbb{C}(\wp_1, \wp_1')$.

Let $\Phi : \mathbb{C}(\wp_n, \wp_n') \cong_{\mathbb{C}} \mathbb{C}(u_0, v_0) \subseteq \mathbb{C}(\wp_1, \wp_1')$ be the $\mathbb{C}$-isomorphism given by $\wp_n \mapsto u_0, \wp_n' \mapsto v_0$. To show that there exists some $w_0 \in \mathbb{C}(\wp_1, \wp_1')$, it suffices to exhibit some $\Psi : \mathbb{C}(\wp_1, \wp_1') \rightarrow \mathbb{C}(\wp_1, \wp_1')$ such that $\Psi\big|_{\mathbb{C}(\wp_n, \wp_n')} = \Phi$. This is because, if such a Ψ exists, since $\wp_1$ satisfies $P(\wp_n, \wp_n', \wp_1) = 0$, we would obtain that $\Psi(\wp_1) \in \mathbb{C}(\wp_1, \wp_1')$ satisfies $P(u_0, v_0, \Psi(\wp_1)) = 0$, exhibiting the desired w_0.

We now apply Corollary 2.3.21 to realize the graph of Φ as the following:

$$\left(\forall f \in \mathbb{C}(\wp_n, \wp_n')\right)\left(\forall z \in \mathbb{C}\right)\ \Phi(f)(z) = f(z/\alpha + \beta)$$

for some $\alpha, \beta \in \mathbb{C}$. Since by assumption the associated lattices do not have complex multiplication, we may write $\mathbb{C}(u_0, v_0)$ as $\mathscr{E}(\alpha\langle \omega_1/n, \omega_2 \rangle)$, where ω_1/ω_2 is not an imaginary

quadratic number and $\alpha \in 1/\mathbb{Z}$. So $\alpha\langle \omega_1/n, \omega_2\rangle$ is a lattice containing $\langle \omega_1, \omega_2\rangle = \Lambda$. So consider the $\mathbb{C}$-algebra isomorphism $\Psi : \mathbb{C}(\wp_1, \wp_1') = \mathscr{E}(\Lambda) \to \mathscr{E}(\alpha\Lambda)$ given by

$$(\forall f \in \mathbb{C}(\wp_1, \wp_1'))\,(\forall z \in \mathbb{C})\ \ \Psi(f)(z) = f(z/\alpha + \beta)$$

which extends Φ. This completes the proof. □

Theorem 4.2.9 ([6, p. 820, Theorem 36]) *Let K be the function field for a curve over k, and let L be the function field of an elliptic curve over k without complex multiplication. If $K \equiv_{\mathcal{L}} L$, then $K \cong L$.*

Before giving the proof, it is important to note the subtle differences between the proof of this theorem and the proof of Theorem 4.2.8. For one, elementary equivalence in $\mathcal{L}$ is still strong enough to conclude that K and L have the same genus, so they are both function fields for elliptic curves over k. However, it is not strong enough enough to satisfy the conditions of Lemma 4.1.2, in contrast with the proof just given. So it is not clear at all that K and L have isogenous curves, let alone that K has complex multiplication. For this reason, there is an asymmetry in assumed properties of K and L.[1] Another important distinction is that the above result yields that K and L are isomorphic only as abstract fields, not as k-algebras.[2]

Proof By contrapositive, suppose that $K \ncong L$. To show that $K \not\equiv_{\mathcal{L}} L$. Theorem 3.1.13 gives that genus of a function field over k is determined by $\mathcal{L}$, so if the genus of K and L differ, then $K \not\equiv_{\mathcal{L}} L$. So without loss of generality, $\gamma(K/k) = 1$, hence K is the function field of an elliptic curve. Let $j, j' \in k$ be the modular invariants of L and K, respectively. We will perform casework on the algebraicity of j, j'. Our three cases will be as follows: j is algebraic, j' is algebraic, or both j, j' are transcendental (where all of these conditions are over $\mathbb{Q}$).

Suppose that j is algebraic, and let $\mu_j(X) \in \mathbb{Z}[X]$ be its minimal polynomial. If $n+1 = \deg \mu_j$, write $A = \{j_0, \ldots, j_n\} \subseteq k$ to be the $n+1$ distinct roots of μ_j with $j_0 = j$. Then A is a minimal $\mathcal{L}$-definable subset of L, so for any $\varphi(x) \in \mathrm{Sent}_{\mathcal{L}}$ and any $0 \leq i, \ell \leq n$, $L \models \varphi(j_i)$ if and only if $L \models \varphi(j_\ell)$.

For each $0 \leq i \leq n$, there exists a function field L_i of an elliptic curve over k whose modular invariant is j_i, by application of Proposition 2.3.14. We may choose $L_0 = L$. Furthermore, there is an automorphism $\sigma \in \mathrm{Aut}(k)$ with $\sigma(j_i) = j_\ell$ which induces an isomorphism $\Psi_\ell^i : L_i \to L_\ell$ sending j_i to j_ℓ. Hence, each L_i is isomorphic to L by fixing $\ell = 0$. In particular, this means that each L_i satisfies $L_i \ncong K$, therefore $L \ncong_k K$, so by Theorem 4.2.8, for each $0 \leq i \leq n$, there exists a sentence $\varphi_i \in \mathrm{Sent}_{\mathcal{L}(j_i)}$ such that $L_i \models \varphi_i$ and $K \models \neg\varphi_i$. Equivalently, then, there is a formula $\psi_i(x) \in \mathrm{Fm}_{\mathcal{L}}$ in one free variable such that $L_i \models \psi_i(j_i)$ and $K \models \neg\psi_i(j_i)$. So the isomorphisms $\Psi_0^i : L_i \to L$ exhibit

[1] The distinction between 4.2.8 and 4.2.9 is analogous to the distinction between 4.1.3 and 4.1.4, in the higher genus case.

[2] This is not so much of an obstruction. Also, the more recent literature on elementary equivalence of function fields focuses primarily on classifications of isomorphism classes as abstract fields, rather than their isomorphism classes as k-algebras.

$L \models \bigwedge_{i=0}^{n} \psi_i(j)$. In terms of first-order properties, this gives that the following hold:

$$L \models \exists x \left((\mu_j(x) = 0) \wedge \bigwedge_{i=0}^{n} \psi_i(x) \right) \qquad K \models \forall x \left((\mu_j(x) = 0) \rightarrow \bigvee_{i=0}^{n} \neg \psi_i(x) \right)$$

Since the above are incompatible sentences in $\mathcal{L}$, this shows $K \not\equiv_{\mathcal{L}} L$.

Now suppose that j' is algebraic, and let $\mu_{j'}(X) \in \mathbb{Z}[X]$ be its minimal polynomial. We will use the proof of Proposition 2.3.14 to construct a formula $E(x, y, z) \in \mathrm{Fm}_{\mathcal{L}}$, conditional on the value of j':

$$E(x,y,z) = \begin{cases} \left(y^2 = 4x^3 - 1\right) & j' = 0 \\ \left(y^2 = 4x^3 - x\right) & j' = 1728 \\ \left(y^2 = 4x^3 - (3z(z-1728))\, x - \left(z(z-1728)^2\right)\right) & \text{otherwise} \end{cases}$$

Letting $z = j'$ in the above formula and $\wp_{j'} \in K$ the associated Weierstrass function, we have that $K \models E(\wp_{j'}, \wp'_{j'}, j')$, since $\wp_{j'}$ satisfies its Weierstrass differential equation. This is not a sentence in the language of rings, as it uses parameters which are not necessarily definable. However, we may translate this into $\mathcal{L}$ as the following sentence:

$$K \models \exists z \left(\mu_{j'}(z) = 0 \wedge \exists x \exists y \left(\neg \xi_d(x) \wedge E(x,y,z) \right) \right) \tag{4.7}$$

where $\xi_d(x)$ is the formula defining $k \subseteq K$, as in Theorem 3.1.13. In words, this says that there is an element $z \in K$ (witnessed by $j' \in K$) which is a root of $\mu_{j'}(X)$, and there exists a pair $(x, y) \in K^2$ with $x \notin k$ which satisfies the equation $E(x, y, z)$.

If L does not satisfy the sentence given by eq. (4.7), then $K \not\equiv_{\mathcal{L}} L$. So suppose it does. Then there is a triple $j'_0, u_0, v_0 \in L$ such that j'_0 is a root of $\mu_{j'}(X)$, $u_0 \notin k$, and the equation given by $E(u_0, v_0, j'_0)$ holds. Then $k(u_0, v_0) \subseteq L$ is a subfield which is isomorphic to $K = k\left(\wp_{j'}, \wp'_{j'}\right)$ with modular invariant j'_0. But the inclusion $K \hookrightarrow L$ induces a dominant morphism $E(L) \rightarrow E(K)$ of curves, which shows that $E(L), E(K)$ are isogenous. So j is algebraic over $\mathbb{Q}(j')$, by Proposition 2.3.16. Since j' is algebraic over $\mathbb{Q}$ by assumption, this gives that j is algebraic. This reduces to the prior case.

The third and final case is direct: suppose that j and j' are both transcendental over $\mathbb{Q}$. Then there exists some $\sigma \in \mathrm{Aut}(k)$ such that $\sigma(j) = j'$ which extends to an isomorphism $K \cong L$. □

4.3 Further Discussion

At this point, we have given a partial answer to the following fundamental question:

> If k is a given field, and K and L are two function fields over k such that $K \equiv_{\mathcal{L}} L$, must it be that $K \cong L$?

However, there are a number of cases which haven't been addressed. In particular, the following particular considerations might come to mind:

1. Function fields of elliptic curves over characteristic zero algebraically closed fields *with* complex multiplication;

2. Function fields of curves over algebraically closed fields of positive characteristic;

3. Curves over number fields or finite fields.

As it stands, the situation in (1) is still an open problem. However, there do indeed exist results in the other two cases. A natural extension of the results contained here are those of Pierce [13]. As for (3), the results of Pop [15] are relevant.

In Section 3.2, definability results contained in [15] were briefly mentioned. Of particular relevance is the following result:

Theorem 4.3.1 ([15]) *Let k be an algebraically closed field, and let K and L be function fields over k such that $K \equiv_{\mathcal{L}} L$. Then* $\operatorname{trdeg}_k K = \operatorname{trdeg}_k L$.

The proof of this is beyond the scope of this thesis, but it is worth mentioning that by applying this result, we may loosen the assumptions given in the statements of a number of theorems given in this chapter. In particular, if K is the function field of a curve over k, and L is any other function field over k with $K \equiv_{\mathcal{L}} L$, we need not further stipulate that L is the function field of a curve, since the above result gives that transcendence degree is encoded in the $\mathcal{L}$-theory of a function field. However, it is still essential to suppose that L is indeed a function field, as none of these results hold in general for arbitrary field extensions of k. Namely, the following result is crucial:

Theorem 4.3.2 ([13, Proposition 3]) *Let k be an algebraically closed field, and let $\mathscr{C}$ be any class of function fields over k. Then $\mathscr{C}$ is not an elementary class; that is, $\mathscr{C}$ is not of the form*

$$\{K \mid K \text{ is a field extension of } k \text{ such that } K \equiv_{\mathcal{L}} L\}$$

for any field extension L of k. In other words, given any function field L over k, there is a field extension of k which is not a function field over k, but is elementarily equivalent to L.

Proof Let L be any function field over k, and let $\xi_d(x)$ define $k \subseteq L$. Then the set

$$\{\neg\xi_d(x)\} \cup \left\{\exists y \left(y^{n+1} = x\right) \mid n \in \mathbb{N}\right\}$$

is a 1-type[3] which is consistent with $\operatorname{Th}(L)$, by the compactness theorem. Then there exists an elementary extension $L \prec K_0$[4] such that K_0 contains every n^{th} root of some $x \in L \setminus k$ [11, p. 116, Proposition 4.1.3]. This gives that $L \equiv_{\mathcal{L}} K_0$, but K_0 is clearly not a function field over k. □

[3] An *n-type* is a consistent set of formulae in a fixed collection of n free variables [11, p. 115, Definition 4.1.1].

[4] This means that the inclusion map $L \hookrightarrow K_0$ is an elementary embedding.

Bibliography

[1] John L. Bell and Alan B. Slomson. *Models and Ultraproducts: An Introduction*. Courier Corporation, 2006.

[2] C. C. Chang and H. Jerome Keisler. *Model Theory*, volume 73 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam, 1990.

[3] Patrick Du Val. *Elliptic Functions and Elliptic Curves*, volume 9 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1973.

[4] David S Dummit and Richard M Foote. *Abstract Algebra*. Prentice Hall Englewood Cliffs, NJ, 3rd edition, 1991.

[5] Jean-Louis Duret. Sur la théorie élémentaire des corps de fonctions. *Journal of Symbolic Logic*, 51(4):948–956, 1986.

[6] Jean-Louis Duret. équivalence élémentaire et isomorphisme des corps de courbe sur un corps algébriquement clos. *Journal of Symbolic Logic*, 57(3):808–823, 1992.

[7] Otto Forster. *Lectures on Riemann Surfaces*, volume 81 of *Graduate Texts in Mathematics*. Springer, New York, NY, 1981.

[8] Phillip Griffiths and Joseph Harris. *Principles of Algebraic Geometry*. John Wiley & Sons, 1978.

[9] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, New York, NY, 1977.

[10] Wilfrid Hodges et al. *A Shorter Model Theory*. Cambridge University Press, 1997.

[11] David Marker. *Model Theory: an Introduction*, volume 217 of *Graduate Texts in Mathematics*. Springer, New York, NY, 2006.

[12] Rick Miranda. *Algebraic Curves and Riemann Surfaces*, volume 5 of *Graduate Studies in Mathematics*. American Mathematical Society, 1995.

[13] David A Pierce. Function fields and elementary equivalence. *Bulletin of the London Mathematical Society*, 31(4):431–440, 1999.

[14] Bruno Poizat. *A Course in Model Theory: an Introduction to Contemporary Mathematical Logic*. Universitext. Springer, New York, NY, 2012.

[15] Florian Pop. Elementary equivalence versus isomophism. *Invent. math*, 150:385–408, 2002.

[16] Alain Robert. *Elliptic Curves*, volume 326 of *Lecture Notes in Mathematics*. Springer, Berlin, Heidelberg, 1973.

[17] Abraham Seidenberg. Comments on Lefschetz's principle. *The American Mathematical Monthly*, 65(9):685–690, 1958.

[18] J.P. Serre. *A Course in Arithmetic*, volume 7 of *Graduate Texts in Mathematics*. Springer, New York, NY, 1973.

[19] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, New York, NY, 2nd edition, 2009.

[20] E.T. Whittaker and G.N. Watson. *A Course of Modern Analysis*. Cambridge University Press, 4th edition, 1927.