On the projective geometry of curves of genus one, and an algorithm for the jacobian of such a curve

Alexander R. Perlis

A Dissertation Submitted to the Faculty of the

Department of Mathematics

In Partial Fulfillment of the Requirements
For the Degree of

Doctor of Philosophy

In the Graduate College

The University of Arizona

2 0 0 4

Document composed and printed using the LaTeX document preparation system.
Text set in the Computer Modern typeface designed by Donald Knuth.
Bound by Wyvern Bookbinders, Tucson, Arizona.

Statement by Author

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at The University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be obtained from the author (who is the copyright holder).

Acknowledgments

The idea of the algorithm was presented by Minhyong Kim in a series of informal lectures when we were working on [AKM$^+$01]. Much of the material in this dissertation was worked out in extensive conversations with Minhyong Kim and William McCallum, both of whom I owe a great debt of gratitude.

Both throughout this dissertation and in other material related to [AKM$^+$01], there are contributions from conversations with Greg Anderson, John Brillhart, John Cremona, Larry Grove, William Hoffman, Hermann Karcher, Kirti Joshi, Benjamin Levitt, Klaus Lux, David Marshall, Susan Marshall, Barry Mazur, Jorge Morales, Catherine O'Neil, Robert Perlis, Christopher Rasmussen, Nicholas Shepherd-Barron, Dinesh Thakur, and Douglas Ulmer, among others—my sincere apologies to anyone whose name I have forgotten to mention. I thank everyone for their time, encouragement, and words of wisdom.

Abstract

Given equations with k-rational coefficients that define a curve C of genus 1 over a perfect field k, can we find equations that define its jacobian J_C? The problem is trivial when the degree n of a k-rational divisor on C is equal to 1. For the cases $2 \leq n \leq 4$, certain standard forms for C appear classically, and the classical invariant theory of those forms turns out to contain equations that define J_C. This modern interpretation of classical results was explained for $n = 2$ in 1954, for $n = 3$ in 2001, and for $n = 4$ in 1996. A standard form for C and its invariant theory was worked out by Tom Fisher for $n = 5$ in 2003, again leading to equations for J_C.

In the present work, the problem is solved *algorithmically* for all $n \geq 3$. (As in the classical approach, we must assume the characteristic of k does not divide n.) The basic idea, given to us by Minhyong Kim, is to embed C in $\mathbf{P}_k^{n-1}$ using the divisor of degree n, then to explicitly describe as matrices the finite Heisenberg group that corresponds to the n-torsion $\mathrm{J}_C[n]$ on the jacobian, and then to determine equations for the quotient of C by the Heisenberg group, giving us the sought jacobian: $C/\mathrm{J}_C[n] \cong \mathrm{J}_C$. The Heisenberg matrices also allow us to compute the points of hyperosculation on C, which is a k-rational orbit under the action of $\mathrm{J}_C[n]$ and thus gives the origin for the group law on J_C. Our algorithm relies on techniques from the theory of Gröbner bases, and on techniques from the invariant theory of finite groups.

In presenting the background material to our algorithm, we develop the theory of curves of genus 1 with an attached k-rational divisor class, and the theory of non-degenerate degree n curves in $\mathbf{P}_k^{n-1}$ of genus 1. We thus state in a more general context results that appeared previously in more specialized contexts in work of Klaus Hulek and work of Catherine O'Neil. We give an elementary proof that the commutator pairing on the Heisenberg group corresponds to the Weil pairing on $\mathrm{J}_C[n]$. We describe intriguing hyperplane configurations and relate them to the points of hyperosculation on the curve of genus 1.

Contents

CHAPTER I

Introduction

I.1. The motivating problem

The motivation behind this work is the following arithmo-geometric problem: *given equations defining a curve C of genus 1 over a perfect field k, find equations defining the jacobian curve* J_C. The arithmetic nature of the problem is reflected in its triviality when k is algebraically closed, for in that case we have $C \cong \mathrm{J}_C$. (The problem also turns out to be trivial when k is a finite field—see §I.2f.)

This problem is in some sense the opposite or inverse of the following problem, which occurs in the theory of descent: *given an elliptic curve, produce its principal homogeneous spaces.*

I.1a. Previous work and related work

Let n be the degree of a k-rational divisor on C. The $n = 1$ case of the motivating problem is trivial: we have $C \cong \mathrm{J}_C$.

For $n \geq 2$, it turns out the curve C always admits a non-degenerate degree n map to $\mathbf{P}_k^{n-1}$, so without loss of generality we may assume that C is given that way to begin with. For $n \geq 3$ that map is an embedding, so we are essentially assuming that C is given to us as a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1.

The classical approach. The cases $n = 2$, $n = 3$, $n = 4$, and $n = 5$ of the motivating problem, or slight variants thereof, have been solved, under the hypothesis $\mathrm{char}(k) \nmid n$ (in some cases also $\mathrm{char}(k) \neq 2, 3$), using techniques of classical invariant theory: [Wei54], [MSS96], [AKM+01], [VT], and [Fis]. The first four references rely on results from invariant theory worked out in the 19th century, and thus amount to establishing interesting modern interpretations of classical results. The work [Fis], on the other hand, does quite a bit more: it develops from scratch the relevant invariant theory—which does not appear classically—and then gives the interpretation in terms of jacobians.

This "classical approach" requires one to work with a suitable *family* of curves of genus 1. The classical invariant theory of the generic equations defining the family describes a fundamental system of covariants and their relations, called *syzygies*. In the cases considered so far, there has always been one Weierstrass-like syzygy (I am not aware of a satisfactory explanation for that), which turns out to define the jacobian J_C of each member C of the family.

However, we know of a family $\mathcal{F}$ (see §I.2a), for which the classical approach appears to go through without a hitch, yet the Weierstrass-like syzygy turns out to define a *quadratic twist* of the jacobian, not the jacobian itself! A little extra work then identifies *which* twist occurred, thereby leading to the actual jacobian.

Because the classical approach works with a *family* of curves, it ends up producing *formulas* for the coefficients of J_C in terms of the coefficients of C. The approach itself does not apply to individual curves, but once the formulas are known, they can of course be applied to individual curves, giving us an *algorithm* (namely: substitution) of trivial computational complexity for solving a *restricted version* of the motivating problem; namely, its restriction to the particular curves that occur in the family under consideration.

The O'Neil approach. With additional assumptions on the starting curves and the ground field k, the motivating problem is treated by an intriguing approach in [O'N01]: the jacobian J_C, together with a level-n structure (this is part of the extra data on C), is expressed as a point on the modular curve $\mathrm{X}_1(n)$. For $n = 3$ and $n = 5$, [O'N01] exhibits formulas for $\mathrm{J}_C \in \mathrm{X}_1(n)$ in terms of C.

The Anderson approaches. A related problem has been studied by Greg Anderson: given a curve of genus g defined over an *algebraically closed* field, find equations defining its jacobian (an abelian variety of dimension g). One approach to this problem, which may lead to an algorithm, is given in [And02]. A different, and algorithmic, approach is given in [And]. By assuming the ground field to contain symbols that are algebraically independent over the prime subfield, this approach can treat a *family* of curves of genus 1, which then leads to *formulas* for the jacobian (which can then be applied to individual curves). Even though the formulas are defined over the prime subfield, it is unclear whether they always give the jacobian over that field—certainly they do so over the field's algebraic closure. As shown in [And], when the Anderson algorithm is applied over $\mathbf{Q}$ to two of the cases considered in [AKM$^+$01], it produces the *same* equations for the jacobian as exhibited in [AKM$^+$01], and thus gives the correct answer over $\mathbf{Q}$.

I.1b. Present contribution

In the present work, again assuming $\mathrm{char}(k) \nmid n$ (cf. §I.2e), we develop an *algorithm* (a computational process guaranteed to complete in a finite number of computational steps), based on ideas given to us by Minhyong Kim, that solves the motivating problem in *all* degrees $n \geq 3$.

Unlike the approaches mentioned previously, this algorithm can be applied directly to individual curves. Of course, it can then also be applied to a *family*, serving as an alternate approach for obtaining *formulas* for J_C. (For example, in chapter V we apply the algorithm to the individual curve $3x^3+4y^3+5z^3 = 0$, and then show in §V.7 how to tackle the family $ax^3+by^3+cz^3+mxyz = 0$.)

After applying our algorithm, if one desires a Weierstrass model for J_C, one could apply the usual Riemann–Roch algorithm (cf. §V.7c): find functions x, y with poles of orders 2 and 3 at the origin of J_C, then use linear algebra to find the relation between $1, x, y, x^2, xy, y^2, x^3$.

The mere *existence* of an algorithm is not surprising, at least when k is countable, for there certainly exists the following type of *exhaustive search*: given C, one enumerates all varieties defined over k (there are countably many); for each such variety V, one enumerates all k-rational points in the ambient space; for each such pair (V, P), one enumerates all algebraic maps from the ambient space of C to the ambient space of V; for each such triple (V, P, ϕ), one checks whether V is a curve of genus 1, whether P lies on V, and whether ϕ has degree n^2 and the difference of any pair of points in $\phi^{-1}(P)$ is a divisor class of order dividing n in the divisor class group; all of this can be done algorithmically, and once all the conditions are met, by [AKM$^+$01, Prop. 4.5], one has found J_C. (This also shows that the motivating problem lies in the computational complexity class NP: a nondeterministic polynomial-time algorithm is to guess and then verify the certificate data indicated above.) But exhaustive search is completely useless: even in the simplest of cases, it exhausts our patience, and it has the philosophical drawback that its description relies only peripherally on the mathematics of the motivating problem.

In contrast to exhaustive search, the algorithm in the present work relies heavily on the mathematics of the motivating problem, and the algorithm can be successfully applied in practice (as we demonstrate in chapters V and VI). However, on multiple occasions in the algorithm, we need to find all solutions to a 0-dimensional intermediate problem; unfortunately, today we know how to complete those steps algorithmically only by appealing to the theory of Gröbner bases, and thus the overall algorithm, in its present form, has seemingly unbounded computational complexity.

In summary, our present algorithm has the advantage over the previous approaches of being applicable both to families and to individual curves, and of course the advantage that it can be applied in all degrees $n \geq 3$. On the other hand, from a practical perspective, on a current desktop-class computer (3 GHz Pentium processor, 2 GB RAM), we have been successful only with particular instances in the $n = 3$ and $n = 4$ cases of the motivating problem.

I.1c. Roadmap for the algorithm

As described below in the chapter-by-chapter overview (see §I.3), this dissertation contains more than just the algorithm that solves the motivating problem. If the reader's only goal is to understand that algorithm, then the summary below in §I.3d may be a good starting point, and the more detailed roadmap is as follows.

In chapter II, the only crucial material is: §II.2 on the map $j_{\mathcal{D}}$ and the isomorphism $C/\mathrm{J}_C[n] \xrightarrow{\sim} \mathrm{J}_C$, and §II.2a on the points of hyperosculation. In chapter III, the only crucial material is: §III.8 on classifying linear automorphisms, §III.11 on the fixpoints and hyperplane configurations associated to generators of J_n, and §III.12 on lifting $J_n \subset \mathbf{PGL}_n(\bar{k})$ to $H_n \subset \mathbf{SL}_n(\bar{k})$. Of course, all of chapter IV (description of the algorithm) is crucial, and the examples from chapter V and VI serve as concrete illustrations of the steps.

I.2. Future research projects

I.2a. The family $\mathcal{F}$

Consider the family $\mathcal{F}\colon Z^3 = U(X,Y)$, where U is a generic binary cubic form with distinct roots. When we look at the classical invariant theory of binary cubic forms (cf. [Stu93, 3.7.6, 3.7.7]), we find a Weierstrass-like syzygy. Let E be the elliptic curve over $\mathbf{Q}$ defined by that syzygy, and let C be a member of the family $\mathcal{F}$ with coefficients in $\mathbf{Q}$. The syzygy leads to a map $C \to E$ of degree 3. Thus E cannot be J_C, for a map $C \to \mathrm{J}_C$ defined over $\mathbf{Q}$ must have degree a square: its pullback is multiplication-by-m for some m. It turns out E is the quadratic twist of J_C over $\mathbf{Q}(\sqrt{-3})$, which is the field over which J_C has complex multiplication. Further investigations into $\mathcal{F}$ may give additional insight into the classical approach: *when* it works, and *why* it works when it does. (I intend to continue this research and publish the results in the future.)

I.2b. The "j-invariant" approach

An entirely different approach to finding J_C, not discussed elsewhere in this dissertation, goes as follows: starting with C defined over k, move to a finite field extension K/k over which C_K admits a point, then apply the Riemann–Roch algorithm (cf. §V.7c) to obtain a Weierstrass model W for C_K that has k-rational coefficients. (From this we can read off the j-invariant of C—my original motivation for this approach—whence the name.) Thus C, W, and J_C (as an abstract curve) are all defined over k, and all three are isomorphic over K. But W and J_C are elliptic curves over k, whence either $W \cong \mathrm{J}_C$, or W is a quadratic twist of J_C over one of the quadratic extensions lying inside K/k. By writing down the possibilities, we obtain a finite list of Weierstrass models that are candidates for J_C (and one of them must actually be J_C). Next repeat the procedure with a *different* field extension K/k, hopefully obtaining a *different* finite list of candidates that necessarily contains J_C. Repeat this process until the various finite lists intersect in a single candidate, which must then be J_C. (I have successfully applied this approach in the case $n = 2$. I intend to continue this research and publish the results in the future.)

Compared to the classical approach, or to the Anderson algorithm, or to the algorithm in this dissertation, the "j-invariant" approach has the following disadvantage: it does not give you a map $C \to \mathrm{J}_C$.

I.2c. Arithmetic complexity bounds

Any systematic approach to the jacobian might lead to relations between the arithmetic height (or other suitable notion of complexity) of J_C and the height of C. (A preliminary investigation of the "j-invariant" approach led to rough height relations. I intend to continue this line of research in the future.)

I.2d. Elucidating the hyperplane configurations

We feel that more can be said about fixpoints and fixed hyperplanes of elements of $\mathbf{PGL}_n(\bar{k})$ that preserve C (cf. §III.9 and §III.11). For example, what can be said about the hyperplanes fixed by the $[-1]$-automorphisms? For another example, we discover in chapter V that the $[-1]$-automorphisms have eigenvalue $+1$ at one fixpoint but eigenvalue -1 at the other three fixpoints. Why does this happen, and what happens in general? Many such questions are easily formulated from the examples worked out in chapters V and VI.

It would also be nice to have a formula, or at least an algorithm more elegant than brute force, for determining the osculating hyperplane at a point (thus also for determining the hyperosculating hyperplanes at the points of hyperosculation).

A better understanding of these matters may lead to further simplifications of the elementary proof in §III.10 that the commutator pairing is the Weil pairing, or at least some kind of insight into what is happening geometrically in each step of the proof.

I.2e. Handling the modular case

Our algorithm for the jacobian exploits the isomorphism $(*)$ (from §I.3b below), which holds in general. Even the recasting of $C/\mathrm{J}_C[n]$ as C/H_n (cf. §I.3d below) holds in general. However, to compute C/H_n in practice, we start by finding the $\bar{k}$-valued points of the group scheme H_n. When $\mathrm{char}(k) \mid n$ (known as the *modular* case), we have $\#H_n \neq \#H_n(\bar{k})$, and our algorithm breaks down. (Note that the invariant theory of finite groups itself is not an obstacle: algorithms for the modular case appear in [Kem96] and [DHS98].) However, since we do determine equations defining the group scheme H_n, even in the modular case there may be a method for determining equations for C/H_n.

I.2f. Examples in characteristic $p > 0$

It would be interesting to apply our algorithm to examples in characteristic $p > 0$. For example, whereas working over function fields in characteristic 0 may be computationally out of reach on today's computers, it may turn out that something similar is feasible in characteristic p.

It is worth remarking that the motivating problem is actually trivial when k is the finite field $\mathbf{F}_q$, where q is a power of p. By the *Riemann hypothesis* for curves (cf. [Har77, Ex. V.1.10]), we can easily see that a curve of genus g defined over $\mathbf{F}_q$ necessarily admits a rational point when q exceeds a bound expressible in terms of g. For $g = 1$, the condition is $q \geq 2$. Therefore, our curve C of genus 1 always admits an $\mathbf{F}_q$-rational point, whence $C \cong \mathrm{J}_C$. But this isomorphism is not canonical; in particular, given a *family* of curves of genus 1, it is unclear whether we can pick out the rational point in a consistent manner across the family. In other words, a non-canonical isomorphism $C \cong \mathrm{J}_C$ exists for each individual members of the family, but there may be no single such isomorphism for the entire family. Our algorithm, on the other hand, always produces J_C in a canonical fashion. Thus, it is still interesting to apply the algorithm even when working over a finite field.

I.3. Chapter-by-chapter overview

I.3a. Chapter I: Introduction

You're reading that chapter right now!

I.3b. Chapter II: Background on quasi-elliptic curves

Interest in the motivating problem led us to study an object we call a **quasi-elliptic curve** defined over k: a pair $(C, \mathcal{D})$, where C is a curve of genus 1 defined over k, and $\mathcal{D}$ is a k-rational divisor class on C. Each quasi-elliptic curve admits precisely n^2 (when $\mathrm{char}(k) \nmid n$) **points of hyperosculation**, which are $\bar{k}$-valued points P such that $nP \in \mathcal{D}$. They compose a k-rational orbit under the action of the n-torsion $\mathrm{J}_C[n]$ on C. This action respects the fibers of the map $j_{\mathcal{D}} \colon C \to \mathrm{J}_C$, $P \mapsto [nP] - \mathcal{D}$,

and we get an isomorphism of curves

$$\frac{C}{\mathrm{J}_C[n]} \xrightarrow{\sim} \mathrm{J}_C. \qquad (*)$$

The hyperosculation orbit on C is the k-rational point on the left that goes to the origin of J_C on the right.

Remark. Our algorithm for J_C will in fact find equations for $C/\mathrm{J}_C[n]$; it will find coordinates for the points of hyperosculation on C, and thus obtain the coordinates of the origin on $C/\mathrm{J}_C[n]$.

Chapter II proceeds with a description of morphisms between quasi-elliptic curves, and in particular establishes

$$\mathrm{Aut}(C_{\bar{k}}, \mathcal{D}) = \mathrm{J}_C[n](\bar{k}) \rtimes \mathrm{Aut}(C_{\bar{k}}, O), \qquad (**)$$

where $O \in C(\bar{k})$ is a point of hyperosculation.

We next give an alternative description of a quasi-elliptic curve, namely as a map $C \to \mathrm{J}_C$, such as $j_{\mathcal{D}}$ above, with the property that the induced pullback map $\mathrm{J}_C \to \mathrm{J}_C$ is multiplication-by-n. While working on the paper [AKM$^+$01], such maps occurred when we were considering new ways of describing principal homogeneous spaces and n-coverings of an elliptic curve. We briefly give those descriptions here.

Finally, when the class $\mathcal{D}$ admits a k-rational representative D, so that we are working with a pair (C, D), there is always the associated non-degenerate degree n map to the projective space bundle $\mathbf{P}\big(\mathrm{H}^0(C, \mathcal{O}(D))\big)$, which upon choosing coordinates is just $\mathbf{P}^{n-1}_k$. (The map is an embedding for $n \geq 3$.) We show that automorphisms of (C, D) extend to automorphisms of $\mathbf{P}^{n-1}_k$.

I.3c. Chapter III: Projective quasi-elliptic curves $C \overset{n}{\hookrightarrow} \mathbf{P}^{n-1}_k$

This chapter generalizes material on "elliptic normal curves" from [Hul86] and on "n-prepared curves" from [O'N01].

We study pairs (C, D) with $n \geq 3$ (cf. the last paragraph in the previous section), but identify them with their image in $\mathbf{P}^{n-1}_k$; thus, we study "non-degenerate degree n curves in $\mathbf{P}^{n-1}_k$ of genus 1" (it turns out, as we show, that none of these words is superfluous), and denote such a curve $C \overset{n}{\hookrightarrow} \mathbf{P}^{n-1}_k$.

We show that $C \overset{n}{\hookrightarrow} \mathbf{P}^{n-1}_k$ is projectively normal, we compute its Hilbert function and Hilbert polynomial, and we show that each generating set for the saturated ideal defining the curve contains $n(n-3)/2$ linearly independent quadratic forms. Furthermore, when $\mathrm{char}(k) \neq 2$, for $n \geq 4$ each minimal generating set comprises precisely $n(n-3)/2$ quadratic forms; that is, C is cut out scheme-theoretically by quadrics.

Combining $(**)$ with the last paragraph in §I.3b, we obtain

$$\big\{\, \phi \in \mathbf{PGL}_n(\bar{k}) \,:\, \phi(C_{\bar{k}}) = C_{\bar{k}} \,\big\} \cong \mathrm{J}_C[n](\bar{k}) \rtimes \mathrm{Aut}\big((C_{\bar{k}}, O)\big), \qquad (***)$$

and from this we conclude: the subgroup $J_n \subset \mathbf{PGL}_n(\bar{k})$ of elements that preserve C and act fixpoint-free on C is a faithful and Galois equivariant representation of the action of $\mathrm{J}_C[n](\bar{k})$ on C.

No matter the characteristic of k or the j-invariant of C, the part of $(***)$ that always exists is $J_n \rtimes \{\pm 1\}$. The non-trivial coset of J_n is characterized as the subset of $\mathbf{PGL}_n(\bar{k})$ whose elements preserve C, have a fixpoint on C, and have order 2. When n is odd, each point of hyperosculation on C occurs as the fixpoint of an element of that coset. When n is even, either all or none of the fixpoints of an element of that coset are points of hyperosculation. We can identify whether a given fixpoint is a point of hyperosculation by searching for a hyperplane that meets C with multiplicity n at the given point. Thus we have a practical procedure for finding the points of hyperosculation on C.

By choosing lifts from $\mathbf{PGL}_n(\bar{k})$ to $\mathbf{GL}_n(\bar{k})$, we define the commutator pairing

$$\begin{aligned} J_n \times J_n &\longrightarrow \bar{k}^\times, \\ \big([M], [N]\big) &\longmapsto M\,N\,M^{-1}N^{-1}. \end{aligned}$$

Using the points of hyperosculation as a crutch, we give an elementary proof that the commutator pairing on J_n corresponds to the Weil pairing on $\mathrm{J}_C[n](\bar{k})$. To even discuss the Weil pairing, we must assume $\mathrm{char}(k) \nmid n$, and this assumption now occurs repeatedly as we appeal to the commutator pairing and the fact that J_n has two generators: we show that lifts of generators M and N for J_n have distinct eigenvalues, that each generator cyclically permutes the fixpoints (eigenspaces) of the other, and the same is true of the fixed hyperplanes (eigenspaces of the transposed matrices).

For n odd, this leads to the following hyperplane configuration: the hyperplanes fixed by M intersect C in the n^2 points of hyperosculation, and the same is true of the hyperplanes fixed by N. Furthermore, each point of hyperosculation lies in the intersection of a unique hyperplane fixed by M with a unique hyperplane fixed by N. (This gives yet another procedure for finding the points of hyperosculation on C.)

For n even, the hyperplanes fixed by M intersect C in a collection of n^2 points that, under the isomorphism $(*)$, correspond to a non-trivial point of 2-torsion on J_C, while the hyperplanes fixed by N do the same thing, but for a *different* point of 2-torsion on J_C.

Next, we define $H_n \subset \mathbf{SL}_n(\bar{k})$ to be the preimage of J_n under the map $\mathbf{SL}_n \to \mathbf{PGL}_n$, giving us the exact sequence

$$1 \longrightarrow \boldsymbol{\mu}_n(\bar{k}) \longrightarrow H_n \longrightarrow J_n \longrightarrow 1.$$

This is a central extension of J_n by $\boldsymbol{\mu}_n(\bar{k})$, of order n^3 (when $\mathrm{char}(k) \nmid n$). We characterize the different lifts of J_n to $\mathbf{GL}_n(\bar{k})$ of order n^3, and establish that H_n is essentially the only lift we would want to work with.

We finish the chapter by describing Schrödinger-like representations for H_n and how they relate to the Galois module structure of $\mathrm{J}_C[n]$.

I.3d. Chapter IV: An algorithm for the jacobian

We assume C to be smooth and given as in §I.3c: a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1. We furthermore assume $\mathrm{char}(k) \nmid n$ (cf. §I.2e). Actually, the algorithm takes arbitrary equations as input, and then verifies that the input meets the assumptions. Thus

$$C = \mathrm{Proj}\, \frac{k[x_0, \ldots, x_{n-1}]}{I},$$

where the generators of I were given in the input.

Now we exploit $(*)$. As explained in §I.3c, the action of $\mathrm{J}_C[n](\bar{k})$ on $C(\bar{k})$ is given by the group $J_n \subset \mathbf{PGL}_n(\bar{k})$, which we lift to $H_n \subset \mathbf{SL}_n(\bar{k})$. We find H_n as follows: using a Gröbner basis for the ideal of C, we easily write down the conditions for a generic matrix to preserve C and have determinant 1. In finding the finitely many solutions, we obtain a finite field extension K/k over which each solution is defined. We can then check which matrices have no fixpoints on C, and which have fixpoints and are of order 2 in $\mathbf{PGL}_n(\bar{k})$. Thus we can find matrices representing the elements of $J_n \rtimes \{\pm 1\}$. We identify two generators M, N for H_n by searching for a pair of matrices whose commutator is a primitive nth root of unity.

By finding eigenvectors for each matrix and its transpose, we obtain the fixpoints and fixed hyperplanes under the action of the induced element of $\mathbf{PGL}_n(\bar{k})$. As explained in §I.3c, this information gives us the coordinates of the points of hyperosculation.

We identify H_n with the K-valued points of a finite group scheme, again denoted H_n, which is defined over k. Then $(*)$ becomes

$$\begin{aligned} \mathrm{J}_C \cong \frac{C}{H_n} &= \mathrm{Proj}\left(\Big(\frac{K[x_0, \ldots, x_{n-1}]}{K\,I}\Big)^{H_n(K)} \right)^{\mathrm{Gal}(K/k)} \\ &= \mathrm{Proj}\, \frac{k[x_0, \ldots, x_{n-1}] \cap K[x_0, \ldots, x_{n-1}]^{H_n(K)}}{I \cap K[x_0, \ldots, x_{n-1}]^{H_n(K)}}. \end{aligned}$$

Algorithms in the invariant theory of finite groups (cf. [Stu93]) tell us how to find the invariants under $H_n(K)$. Because H_n itself is invariant under $\mathrm{Gal}(K/k)$, these algorithms already give us the correct answer over k.

Finally, substituting the coordinates of one of the points of hyperosculation on C gives us the coordinates of the k-rational origin on J_C.

I.3e. Chapter V: Example: a Selmer cubic

To illustrate our theory in the case $n = 3$, we apply the algorithm from chapter IV to the Selmer cubic

$$C = \operatorname{Proj} \frac{\mathbf{Q}[x, y, z]}{\langle 3x^3 + 4x^3 + 5z^3 \rangle}.$$

We show how to carry out each step of the algorithm by hand (but also include computer code in some cases), showing in moderate detail how to apply the well-known intermediate algorithms that were referenced in chapter IV.

At the end of the chapter, we rely on the earlier results in this chapter to tackle the family

$$\operatorname{Proj} \frac{k[x, y, z]}{\langle ax^3 + bx^3 + cz^3 + mxyz \rangle},$$

where k is a perfect field with $\operatorname{char}(k) \neq 3$.

We include example code for the computer systems we used: *GP/Pari* [BBB+00], *Macaulay 2* [GS], *Mathematica* [Wol03], *mwrank* [Cre], and *Singular* [GPS01].

I.3f. Chapter VI: Example: a pair of quadrics

To illustrate the case $n = 4$, we carry out some of the steps of applying the algorithm from chapter IV to

$$C = \operatorname{Proj} \frac{\mathbf{Q}[w, x, y, z]}{\langle w^2 + x^2 + y^2 + z^2, w^2 + 2x^2 + 3y^2 + 4z^2 \rangle}.$$

We include computer code that is easily adapted to arbitrary values of n.

Compared to the example from the previous chapter, the current example is interesting for at least two reasons: it illustrates how the algorithm works when n is even, and the finite Heisenberg group H_4 looks even less Schrödinger-like.

I.3g. Appendix A: Facts about curves of genus 1

We state facts about curves of genus 1 that we reference in other parts of this dissertation.

I.3h. Appendix B: Maps to projective space: a coordinate-free approach

Well known from the theory of smooth projective curves is that a divisor D on a curve X leads to the map $X \to \mathbf{P}^n$ given by $P \mapsto [s_0(P) : \ldots : s_n(P)]$, where the s_i are elements of $\mathrm{L}(D) = \mathrm{H}^0\big(X, \mathcal{O}(D)\big)$.

In this appendix, for lack of a suitable reference, we give a coordinate-free description of such maps. (For the same material described in terms of coordinates, see [Har77, §II.7].)

We describe projective space bundles, how to think of their points as certain types of rank 1 quotients, and how they behave under base change. For X a noetherian scheme over a noetherian ring A, and $\mathcal{L}$ an invertible sheaf on X that is generated by global sections and such that $\mathrm{H}^0(X, \mathcal{L})$ is a free A-module of finite rank, we obtain a canonical morphism

$$\phi\colon X \longrightarrow \mathbf{P}\big(\mathrm{H}^0(X, \mathcal{L}) \otimes_A \mathcal{O}_A\big),$$

from X to the displayed projective space bundle. When A is a field k, and K is a field extension of k, the map ϕ has a nice description in terms of K-valued points:

$$\begin{aligned} \phi_V\colon X(K) &\longrightarrow \mathbf{P}\big(\mathrm{H}^0(X, \mathcal{L})\big)(K), \\ P &\longmapsto \{\, s \in \mathrm{H}^0(X, \mathcal{L}) \otimes_k K \;:\; s_P = 0 \,\}. \end{aligned}$$

In other words, ϕ carries the K-valued point P to the hyperplane, in the vector space $\mathrm{H}^0(X, \mathcal{L}) \otimes_k K$, of global sections that vanish at P.

I.4. Table of notation

Symbol	Explanation
k, $\bar{k}$, G_k	perfect field, algebraic closure, absolute Galois group $\mathrm{Gal}(\bar{k}/k)$
K	field extension of k, often a finite and/or Galois extension in $\bar{k}$
$\mathbf{P}_k^{n-1}$	projective $(n-1)$-space over $k \equiv \mathrm{Proj}\big(k[X_0, \dots, X_{n-1}]\big)$
$\mathbf{P}(\cdot)$	projective space bundle $\equiv$ space of hyperplanes
X	a k-scheme, often a k-curve of arbitrary genus
X_K	the K-scheme $X \times_k K$
$X(K)$	the K-valued points of $X \equiv$ morphisms $\mathrm{Spec}(K) \to X$
C	a k-curve of genus 1
$k(C)$	field of k-rational rational functions on $C(\bar{k})$
J_C	the jacobian of C
$\mathcal{D}$	k-rational divisor class on C of positive degree
n	degree of $\mathcal{D}$
p	$\mathrm{char}(k)$
e	when $\mathrm{char}(k) \mid n$, we have $p^e \mid n$ but $p^{e+1} \nmid n$
$j_{\mathcal{D}}$	the map $C \to \mathrm{J}_C$, $P \mapsto [nP] - \mathcal{D}$
$\mathcal{H}$	hyperosculation packet on C (see II.2a)
D	k-rational divisor on C of positive degree
$[D]$	set of all divisors linearly equivalent to D
$[D]_k$	set of k-rational divisors linearly equivalent to D
(C, O)	elliptic curve with group law origin $O \in C(k)$
$(C, \mathcal{D})$	quasi-elliptic curve (see II.2)
$C \xrightarrow{(n)} \mathrm{J}_C$	map whose pullback $\mathrm{J}_C \to \mathrm{J}_C$ is multiplication-by-n (see II.3)
$C \overset{n}{\hookrightarrow} \mathbf{P}_k^{n-1}$	non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1 (see III.1)
I	saturated homogeneous ideal of C (see III.3)
J_n	$\mathrm{J}_C[n](\bar{k})$ disguised as a certain subgroup of $\mathbf{PGL}_n(\bar{k})$ (see III.10)
H_n	finite Heisenberg group in $\mathbf{SL}_n(\bar{k})$ covering J_n (see III.12)
$\mathfrak{G}$	Gröbner basis for an ideal

Table I.1. Notation used throughout this dissertation.

CHAPTER II

Background on quasi-elliptic curves

II.1. Assumptions

Let k be a perfect field, and throughout let $\bar{k}$ denote an algebraic closure. Without further context or qualification, use of "Galois" refers to the absolute Galois group $\mathrm{G}_k := \mathrm{Gal}(\bar{k}/k)$.

A **k-variety** is a separated, geometrically integral, finite-type k-scheme, and a **curve** is a variety of dimension 1. If X is a k-scheme, and $K \supseteq k$ is a field extension, then X_K denotes the K-scheme

$$X_K := X \times_k K := X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(K).$$

Thus a k-variety may be defined as a finite-type k-scheme X such that the base change $X_{\bar{k}}$ is a variety in the sense of classical algebraic geometry carried out over algebraically closed fields.

Throughout, C is a k-curve of genus 1, and J_C denotes the jacobian of C. Basic facts about curves of genus 1 appear in appendix A. Crucial among them is the fact, which follows from Riemann–Roch, that each K-rational divisor class of degree 1 admits a *unique* K-rational point as representative (for details, see §A.1d); from this, we can give an elementary definition both of the canonical group law on an elliptic curve (see §A.2) and of the canonical action of J_C on C (see §A.3). Familiarity with these facts is assumed.

II.2. Definition of a quasi-elliptic curve $(C, \mathcal{D})$

Recall that an **elliptic k-curve** is a pair

$$(C, O),$$

where C is a k-curve of genus 1 and O is a k-rational point on C. A morphism of elliptic curves $(C, O) \to (C', O')$ is a morphism of curves $\phi\colon C \to C'$ so that $\phi(O) = O'$. In fact, (C, O) can be given a canonical group scheme structure; in particular, for any field extension $K \supseteq k$, the set $C(K)$ is a group with identity element O, and any morphism of elliptic curves is necessarily a group homomorphism on K-valued points. Associated with (C, O) is the canonical k-morphism $j_O\colon C \to \mathrm{J}_C$ of degree 1, determined on $\bar{k}$-valued points by

$$\begin{aligned} j_O\colon C(\bar{k}) &\xrightarrow{\sim} \mathrm{J}_C(\bar{k}), \\ P &\longmapsto [P - O]. \end{aligned}$$

Via this map, which evidently takes the group law origin on C to the group law origin on J_C, we have: every elliptic curve is canonically isomorphic to its jacobian.

Note that a given k-curve C of genus 1 need not occur as an elliptic k-curve, since C need not admit a k-valued point.

In analogy with the above, we define a **quasi-elliptic k-curve** to be a pair

$$(C, \mathcal{D}),$$

where C is a k-curve of genus 1 and $\mathcal{D}$ is a k-rational divisor class on C of positive degree. (In §II.4, and throughout chapter III, we'll further assume that $\mathcal{D}$ admits a k-rational representative, but for now it is only the *class* that is k-rational.) A morphism of quasi-elliptic curves $(C, \mathcal{D}) \to (C', \mathcal{D}')$ is a morphism of curves $\phi\colon C \to C'$ so that $\phi_*\mathcal{D} = \mathcal{D}'$. We define the **degree** of $(C, \mathcal{D})$ to be the

degree of $\mathcal{D}$. Let n be that degree. Associated with $(C,\mathcal{D})$ is the canonical k-morphism $j_{\mathcal{D}}\colon C \to \mathrm{J}_C$ of degree n^2, determined on $\bar{k}$-valued points by

$$\begin{aligned} j_{\mathcal{D}}\colon C(\bar{k}) &\longrightarrow \mathrm{J}_C(\bar{k}),\\ P &\longmapsto [nP]-\mathcal{D}. \end{aligned}$$

Note that each k-curve C of genus 1 does occur as a quasi-elliptic k-curve: simply define a k-rational divisor class on C by taking the Galois orbit of any $\bar{k}$-valued point of C.

On a curve of genus 1, since each k-rational divisor class of degree 1 has a *unique* k-rational point as representative, *a quasi-elliptic curve of degree* 1 *is the same thing as an elliptic curve.*

II.2a. Osculating divisors and points of hyperosculation

On a curve C of genus 1, the canonical action of J_C on C induces, for each integer $n \geq 1$, an action of $\mathrm{J}_C[n](\bar{k})$ on $C(\bar{k})$. The orbits under this action are called **n-torsion packets**. Here are the basic facts (explained in more detail in §A.3a):

- An n-torsion packet is a maximal collection of points in $C(\bar{k})$ so that, if P,Q are any two of them, then there is a linear equivalence $nP \sim nQ$.
- The set of n-torsion packets on C is in one-to-one correspondence with the set $\big(C/\mathrm{J}_C[n]\big)(\bar{k})$.
- Given an n-torsion packet $\mathcal{P} \subset C(\bar{k})$, we can pick $O \in T$ and consider the elliptic curve $E = (C_{\bar{k}}, O)$. Then $\mathcal{P}$ comprises the points of n-torsion: $\mathcal{P} = E[n](\bar{k})$. Thus an n-torsion packet is a collection of points which *would* be the (usual) n-torsion *were* we to choose one of them as group law origin.
- The Galois conjugate of an n-torsion packet is again an n-torsion packet.

Definition. Let $(C,\mathcal{D})$ be a quasi-elliptic curve of degree n. A point $P \in C(\bar{k})$ such that $nP \in \mathcal{D}$ is called a **point of hyperosculation**. For each $P \in C(\bar{k})$, the unique divisor of the form $(n-1)P+Q$ that lies in $\mathcal{D}$ is called the **osculating divisor at** P.

The uniqueness is explained as follows: since the divisor class $\mathcal{D}-(n-1)[P]$ has degree 1, it is represented by a unique point $Q \in C(\bar{k})$. Observe that a point of hyperosculation may be characterized as one whose osculating divisor involves that point more than usual.

Remark. The terms "osculation" and "hyperosculation" have a geometric interpretation for $n \geq 3$. Identify C with its image in $\mathbf{P}^{n-1}_k$ via the embedding given by $\mathcal{D}$ (see §II.4). Associated with each $P \in C(\bar{k})$ is the hyperplane meeting C to maximal order at P, called the osculating hyperplane. For most P, we have just seen that the osculating hyperplane meets C to order $n-1$ at P. For certain points P, the osculating hyperplane meets C to order n at P, and that phenomenon is called hyperosculation. A point whose osculating plane hyperosculates is called a point of hyperosculation. For a cubic curve in $\mathbf{P}^2_k$, the osculating hyperplane at each point is simply the tangent line. The 9 points of hyperosculation are simply the flex points—they are the points where the tangent line meets the curve to order 3.

Proposition II.2.1. *On a quasi-elliptic curve $(C,\mathcal{D})$, the points of hyperosculation compose an n-torsion packet. There are precisely $\#\mathrm{J}_C[n](\bar{k})$ distinct points of hyperosculation in $C(\bar{k})$. (Therefore, when* $\mathrm{char}(k) \nmid n$*, there are n^2 such points.)*

Proof. It is easy to check that the points of hyperosculation are one orbit under the action of $\mathrm{J}_C[n](\bar{k})$ on $C(\bar{k})$. □

Corollary II.2.2. *Every quasi-elliptic curve has at least one point of hyperosculation. (It might not be k-rational, but see II.2.3.)*

Definition. The n-torsion packet $\mathcal{H}$ comprising points of hyperosculation is called the **hyperosculation packet**.

Proposition II.2.3. *The hyperosculation packet $\mathcal{H}$ is Galois stable.*

Proof. If P is such that $nP \in \mathcal{D}$, then it is easy to see that P^σ has the same property: $nP^\sigma = (nP)^\sigma \in \mathcal{D}^\sigma = \mathcal{D}$. □

The space of n-torsion packets is $\big(C/\mathrm{J}_C[n]\big)(\bar{k})$. If C is an arbitrary k-curve of genus 1, then $C/\mathrm{J}_C[n]$ need not admit a k-rational point; but, by II.2.3, when C is part of a quasi-elliptic curve $(C, \mathcal{D})$ of degree n, then $C/\mathrm{J}_C[n]$ always admits a canonical k-rational point, namely the hyperosculation packet $\mathcal{H}$. In other words, $(C/\mathrm{J}_C[n], \mathcal{H})$ is an elliptic curve.

Theorem II.2.4. *The k-morphism $j_\mathcal{D}$ of degree n^2, given on $\bar{k}$-valued points by*

$$\begin{aligned} j_\mathcal{D} \colon C(\bar{k}) &\longrightarrow \mathrm{J}_C(\bar{k}) \\ P &\longmapsto [nP] - \mathcal{D}, \end{aligned}$$

descends to a k-isomorphism of elliptic curves

$$j_\mathcal{D} \colon C/\mathrm{J}_C[n] \xrightarrow{\sim} \mathrm{J}_C.$$

(When $n = 1$, this is just the usual isomorphism $C \xrightarrow{\sim} \mathrm{J}_C$.)

Proof. To see this, observe merely that the map has degree 1, and that the fibers of $j_\mathcal{D}$ are the same as the orbits under the action of $\mathrm{J}_C[n]$; in particular, the hyperosculation packet is $j_\mathcal{D}^{-1}(0)$. □

II.2b. Structure of morphisms

The definition of a morphism between two quasi-elliptic curves was given in §II.2. For there to exist such a morphism, it is of course necessary that the two quasi-elliptic curves have the same degree. We will now give descriptions of the set of morphisms between two quasi-elliptic curves, of the monoid of endomorphisms of a quasi-elliptic curve, and of the group of automorphisms of a quasi-elliptic curve. These particular descriptions require the choice of a point of hyperosculation. Since there may be no such choice that is k-rational, these descriptions may not be useful for describing k-rational homomorphisms, k-rational endomorphisms, and k-rational automorphisms.

Proposition II.2.5. *Let $(C, \mathcal{D})$ and $(C', \mathcal{D}')$ be two quasi-elliptic curves of the same degree n. Fix points of hyperosculation $O \in C(\bar{k})$ and $O' \in C'(\bar{k})$. Each morphism*

$$\psi \in \mathrm{Hom}\big((C_{\bar{k}}, \mathcal{D}), (C'_{\bar{k}}, \mathcal{D}')\big)$$

can be written uniquely in the form

$$\psi = \tau \circ \phi, \qquad \text{where } \tau \in \mathrm{J}_{C'}[n](\bar{k}),\ \phi \in \mathrm{Hom}\big((C_{\bar{k}}, O), (C'_{\bar{k}}, O')\big).$$

Moreover, vice versa, each such $\tau \circ \phi$ defines a ψ.

Proof. By A.4.1, we certainly can write $\psi = \tau \circ \phi$ with ϕ as above and $\tau \in \mathrm{J}_{C'}(\bar{k})$. Then $\psi_*(nO) = \tau_*\phi_*(nO) = \tau_*(nO') = n\tau(O')$, and we have $n\tau(O') \sim nO'$ if and only if $n(\tau(O') - O') \sim 0$, i.e., if and only if τ has order n. □

Corollary II.2.6. *Let $(C, \mathcal{D})$ be a quasi-elliptic curve of degree n. Fix a point of hyperosculation $O \in C(\bar{k})$. Each endomorphism*

$$\psi \in \mathrm{End}\big((C_{\bar{k}}, \mathcal{D})\big)$$

can be written uniquely in the form

$$\psi = \tau \circ \phi, \quad \tau \in \mathrm{J}_C[n](\bar{k}),\ \phi \in \mathrm{End}\big((C_{\bar{k}}, O)\big).$$

Proposition II.2.7. *Let $(C, \mathcal{D})$ be a quasi-elliptic curve of degree n. Fix a point of hyperosculation $O \in C(\bar{k})$. The automorphism group of $(C_{\bar{k}}, \mathcal{D})$ has the structure*

$$\mathrm{Aut}\big((C_{\bar{k}}, \mathcal{D})\big) = \mathrm{J}_C[n](\bar{k}) \rtimes \mathrm{Aut}\big((C_{\bar{k}}, O)\big).$$

Proof. As in II.2.5, this time by A.4.5. □

II.3. Quasi-elliptic curves as maps $C \xrightarrow{(n)} \mathrm{J}_C$

Associated with the quasi-elliptic curve $(C, \mathcal{D})$ is the map $j_{\mathcal{D}}\colon P \longmapsto [nP] - \mathcal{D}$, which has the property:

$$\text{the induced map } (j_{\mathcal{D}})_*\colon \mathrm{J}_C \longrightarrow \mathrm{J}_C \text{ is multiplication-by-}n.$$

We will now classify maps with that property and thereby obtain another description of quasi-elliptic curves.

To get started, forget $\mathcal{D}$ for the time being, and let $\phi\colon C \to \mathrm{J}_C$ be any morphism whatsoever. For each integer $n \geq 1$, we associate with ϕ the map

$$\phi_n\colon C \longrightarrow \mathrm{Pic}^n_C$$

whose behavior on $\bar{k}$-valued points is

$$\phi_n\colon P \mapsto \text{unique class } \mathcal{D}_P \text{ so that } \phi(P) = [nP] - \mathcal{D}_P.$$

Proposition II.3.1. *We have $\phi_* = [n]$ if and only if ϕ_n is constant; when that is the case, ϕ is defined over k if and only if the value of the constant map ϕ_n in Pic^n_C is a k-rational class.*

Proof. If ϕ_n is constant, say with value $\mathcal{D}$, then $\phi(P) = [nP] - \mathcal{D}$ for all $P \in C(\bar{k})$, whence ϕ_* is immediately seen to be $[n]$. Now assume $\phi_* = [n]$. Let $P, Q \in C(\bar{k})$ be arbitrary. Then $[nP - nQ] = n[P - Q] = \phi_*[P - Q] = \phi(P) - \phi(Q) = \big([nP] - \mathcal{D}_P\big) - \big([nQ] - \mathcal{D}_Q\big) = [nP - nQ] - (\mathcal{D}_P - \mathcal{D}_Q)$, so $\mathcal{D}_P = \mathcal{D}_Q$.

Now assume $\phi(P) = [nP] - \mathcal{D}$ for all $P \in C(\bar{k})$. Then $\phi^\sigma(P) = (\phi(P^{\sigma^{-1}}))^\sigma = \big([nP^{\sigma^{-1}}] - \mathcal{D}\big)^\sigma = [nP] - \mathcal{D}^\sigma$, so $\phi = \phi^\sigma$ for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$ if and only if $\mathcal{D} = \mathcal{D}^\sigma$ for all $\sigma \in \mathrm{Gal}(\bar{k}/k)$, i.e., if and only if the class $\mathcal{D}$ is k-rational. □

Let us write

$$C \xrightarrow{(n)} \mathrm{J}_C \tag{II.1}$$

for a k-morphism with the property that the induced map ϕ_* on jacobians is multiplication-by-n. Given two diagrams

$$C \xrightarrow{(n)} \mathrm{J}_C \quad \text{and} \quad C' \xrightarrow{(n)} \mathrm{J}_{C'},$$

a morphism between them is a curve morphism $\phi\colon C \to C'$ fitting into a commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{(n)} & \mathrm{J}_C \\ \big\downarrow{\scriptstyle \phi} & & \big\downarrow{\scriptstyle \phi_*} \\ C' & \xrightarrow{(n)} & \mathrm{J}_{C'}. \end{array}$$

By the proof of II.3.1, each (II.1) is equal to $j_{\mathcal{D}}$ for a unique $\mathcal{D} \in \mathrm{Pic}^n(C)(k)$, whence the two horizontal arrows in the diagram are of the form $j_{\mathcal{D}}$ and $j_{\mathcal{D}'}$. Commutativity of the diagram is easily seen to correspond to the condition $\phi_*\mathcal{D} = \mathcal{D}'$.

Thus there is an isomorphism between the category of quasi-elliptic curves and the category of morphisms of the form (II.1), which goes as follows: to a quasi-elliptic curve $(C, \mathcal{D})$ we associate the morphism $j_{\mathcal{D}}$, while to a morphism (II.1), which must equal $j_{\mathcal{D}}$ for a unique $\mathcal{D} \in \mathrm{Pic}^n(C)(k)$, we associate the quasi-elliptic curve $(C, \mathcal{D})$.

De-emphasizing the divisor class by thinking of a quasi-elliptic curve as being a morphism (II.1) is analogous to de-emphasizing the origin by thinking of an elliptic curve as being a curve together with an isomorphism to its jacobian.

II.3a. Relationship with n-coverings of an elliptic curve

Let (E, O) be a fixed elliptic k-curve. Associated with E is the Kummer sequence

$$0 \to \frac{E(k)}{nE(k)} \to \mathrm{H}^1\big(\mathrm{G}_k, E[n](\bar{k})\big) \to \mathrm{H}^1\big(\mathrm{G}_k, E(\bar{k})\big)[n] \to 0. \tag{$*$}$$

Elements of the Weil–Châtelet group $\mathrm{WC}(E) := \mathrm{H}^1\big(\mathrm{G}_k, E(\bar{k})\big)$ are classically described as equivalence classes of torsors (= principal homogeneous spaces) over E: a k-curve C together with a simply transitive action of E on C. Elements of $\mathrm{WC}(E)$ may instead be described (see [AKM$^+$01, §4]) as equivalence classes of pairs

$$(C, \mathrm{J}_C \xrightarrow{\sim} E),$$

where $\mathrm{J}_C \xrightarrow{\sim} E$ is a k-isomorphism of elliptic curves.

Elements of $\mathrm{H}^1\big(\mathrm{G}_k, E[n](\bar{k})\big)$ are classically described (following [Cas60, §1] and [Cas62, §2]) as equivalence classes of n-coverings: diagrams

$$\begin{array}{ccc} C & \longrightarrow & E \\ {\scriptstyle\sim}\downarrow & \nearrow_{[n]} & \\ E & & \end{array} \tag{$**$}$$

in which C and the morphism $C \longrightarrow E$ are each defined over k, but the isomorphism $C \xrightarrow{\sim} E$ need not be defined over k. Elements of $\mathrm{H}^1\big(\mathrm{G}_k, E[n](\bar{k})\big)$ may instead be described as equivalence classes of pairs

$$(C \xrightarrow{(n)} \mathrm{J}_C, \mathrm{J}_C \xrightarrow{\sim} E),$$

where $C \xrightarrow{(n)} \mathrm{J}_C$ is a quasi-elliptic k-curve (in the sense of §II.3), and $\mathrm{J}_C \xrightarrow{\sim} E$ is a k-isomorphism of elliptic curves; two pairs $(C \xrightarrow{(n)} \mathrm{J}_C, \mathrm{J}_C \xrightarrow{\sim} E)$ and $(C' \xrightarrow{(n)} \mathrm{J}_{C'}, \mathrm{J}_{C'} \xrightarrow{\sim} E)$ are *equivalent* when there is a k-morphism $\phi\colon C \to C'$ so that the following diagram commutes:

$$\begin{array}{ccccc} C & \xrightarrow{(n)} & \mathrm{J}_C & \xrightarrow{\sim} & E \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\phi_*} & & \| \\ C' & \xrightarrow{(n)} & \mathrm{J}_{C'} & \xrightarrow{\sim} & E. \end{array}$$

We now establish this alternate description. Given a pair $(C \xrightarrow{(n)} \mathrm{J}_C, \mathrm{J}_C \xrightarrow{\sim} E)$, we immediately obtain the corresponding classical n-covering $(**)$. On the other hand, given $(**)$, $C \to E$ induces the pullback morphism $\mathrm{J}_E \to \mathrm{J}_C$ whose kernel is $\mathrm{J}_E[n]$. Thus $\mathrm{J}_E/\mathrm{J}_E[n] \cong \mathrm{J}_C$, but also $\mathrm{J}_E/\mathrm{J}_E[n] \cong \mathrm{J}_E \cong E$, whence there is a canonical k-isomorphism $\mathrm{J}_C \xrightarrow{\sim} E$.

With these descriptions, the first map in $(*)$ sends a point $P \in E(k)$ to the map $Q \mapsto nQ + P$, or more precisely,

$$\begin{aligned} [P] \quad \longmapsto \quad & (E \xrightarrow{(n)} \mathrm{J}_E, \mathrm{J}_E \xrightarrow{\sim} E) \\ & \big(Q \longmapsto [nQ + P - (n+1)O], [P - O] \mapsto P\big), \end{aligned}$$

while the second map in $(*)$ is simply the forgetful map

$$(C \xrightarrow{(n)} \mathrm{J}_C, \mathrm{J}_C \xrightarrow{\sim} E) \quad \longmapsto \quad (C, \mathrm{J}_C \xrightarrow{\sim} E).$$

II.4. Mapping a quasi-elliptic curve to projective space

Consider a quasi-elliptic curve $(C, \mathcal{D})$, of degree n, for which the divisor class $\mathcal{D}$ admits a k-rational representative D. Such a quasi-elliptic curve, together with the additional data of the choice of

representative, is denoted simply (C, D). Associated with (C, D) is the k-morphism ι_D of degree n to the canonical projective space bundle arising from D, which is given on $\bar{k}$-valued points by

$$\begin{aligned} \iota_D \colon C(\bar{k}) &\longrightarrow \mathbf{P}\big(\mathrm{H}^0(C, \mathcal{O}(D))\big)(\bar{k}), \\ P &\longmapsto \big\{\, s \in \mathrm{H}^0(C_{\bar{k}}, \mathcal{O}(D)) \;:\; s(P) = 0 \,\big\}. \end{aligned}$$

Remark. For V any k-vector space, the $\bar{k}$-valued points of the projective space bundle $\mathbf{P}(V)$ are simply the hyperplanes in the $\bar{k}$-vector space $V \otimes_k \bar{k}$. (See appendix B for details on projective space bundles.) The map ι_D takes a point to the hyperplane of sections that vanish at that point, but one must interpret this correctly: $\mathcal{O}(D)$ is a subsheaf of the constant sheaf induced by the function field, so it is common to think of a section of $\mathcal{O}(D)$ as a rational function f; the section vanishes at P precisely when the order of vanishing of f at P is at least one higher than what is allowed/required by the coefficient of P in D.

The map ι_D is an embedding precisely for $n \geq 3$, because that is the precise condition for D to be very ample (see [Har77, IV.3.3.3]). We will study such embedded curves in chapter III. For now, however, we make no assumption on n.

By choosing a basis $\mathcal{B} = \{\, x_0, \ldots, x_{n-1} \,\}$ for $\mathrm{H}^0\big(C, \mathcal{O}(D)\big)$, our map becomes

$$\begin{aligned} \iota_{\mathcal{B}} \colon C(\bar{k}) &\longrightarrow \mathbf{P}_k^{n-1}(\bar{k}), \\ P &\longmapsto [x_0(P) : \ldots : x_{n-1}(P)]. \end{aligned}$$

The image of $\iota_{\mathcal{B}}$ is non-degenerate (meaning: it does not lie in a hyperplane), because otherwise we would contradict the linear independence of the basis elements. Each choice of basis leads to such a map, and two different choices lead to two maps that differ by an automorphism of $\mathbf{P}_k^{n-1}$, namely by the element of $\mathbf{PGL}_n(k)$ induced by the change-of-basis matrix. Replacing D with $D' \in [D]_k$, and choosing a basis $\mathcal{B}'$ for $\mathrm{H}^0\big(C, \mathcal{O}(D')\big)$, we obtain a map $\iota_{\mathcal{B}'} \colon C \to \mathbf{P}_k^{n-1}$ as before, and it, too, differs from the original $\iota_{\mathcal{B}}$ by an automorphism of $\mathbf{P}_k^{n-1}$. (To see this, note that $\mathcal{O}(D)$ and $\mathcal{O}(D')$ are isomorphic, whence by B.3b we have $\mathbf{P}\big(\mathrm{H}^0(C, \mathcal{O}(D))\big) \cong \mathbf{P}\big(\mathrm{H}^0(C, \mathcal{O}(D'))\big)$. Now apply [Har77, II.7.1.1].)

In short, given a quasi-elliptic curve $(C, \mathcal{D})$ with the property that $\mathcal{D}$ admits a k-rational representative but *without* the data of a choice of such representative, there is a maximal family $\mathcal{F}$ of k-morphisms $\iota \colon C \to \mathbf{P}_k^{n-1}$ of degree n with non-degenerate image such that any two members of $\mathcal{F}$ differ by a k-rational automorphism of $\mathbf{P}_k^{n-1}$. Given the pair $(C, \mathcal{F})$, we recover the pair $(C, \mathcal{D})$ by letting $\mathcal{D}$ be the class of divisors of hyperplane sections (= pullbacks of hyperplanes) for any (and all) maps in $\mathcal{F}$.

II.4a. Extending a morphism between quasi-elliptic curves to a morphism between projective spaces

Isomorphisms between quasi-elliptic curves induce compatible morphisms between the projective spaces to which they map. More precisely, if (C, D) is a quasi-elliptic curve with a k-rational divisor of degree n, and if (C', D') is a quasi-elliptic curve with a k-rational divisor of the same degree n, and if we choose a basis $\mathcal{B}$ for $\mathrm{H}^0\big(C, \mathcal{O}(D)\big)$ and a basis $\mathcal{B}'$ for $\mathrm{H}^0\big(C', \mathcal{O}(D')\big)$, and if we have a morphism $\phi \colon C \to C'$ with $\phi_* D \sim D'$, then we can ask about the existence of a map in the indicated position:

$$\begin{array}{ccc} C & \xrightarrow{\;\iota_{\mathcal{B}}\;} & \mathbf{P}_k^{n-1} \\ \big\downarrow{\scriptstyle \phi} & & \vdots\,{\scriptstyle ?} \\ C' & \xrightarrow{\;\iota_{\mathcal{B}'}\;} & \mathbf{P}_k^{n-1} \end{array} \qquad (*)$$

Proposition II.4.1. *If ϕ is an isomorphism, then the map in question in $(*)$ exists (and is an automorphism of $\mathbf{P}_k^{n-1}$).*

Proof. We have $\phi^* D' \sim D$. The desired map is obtained by composing the maps in the following commutative diagram:

$$\begin{array}{ccc}
C & \longrightarrow & \mathbf{P}\big(\mathrm{H}^0(C, \mathcal{O}(D))\big) \\
\| & & \sim\downarrow \quad \text{(by B.3b)} \\
C & \longrightarrow & \mathbf{P}\big(\mathrm{H}^0(C, \mathcal{O}(\phi^* D'))\big) \\
\| & & \sim\downarrow \quad \text{(by B.3b)} \\
C & \longrightarrow & \mathbf{P}\big(\mathrm{H}^0(C, \phi^* \mathcal{O}(D'))\big) \\
\sim\downarrow \phi & & \| \quad \text{(by B.3a)} \\
C' & \longrightarrow & \mathbf{P}\big(\mathrm{H}^0(C', \mathcal{O}(D'))\big).
\end{array}$$

□

It is natural to wonder, when ϕ is not an isomorphism, whether the map in question in $(*)$ exists. We now show this is in general *not* the case.

Assume it exists. By pulling back $\mathcal{O}(1)$ from the lower right corner of $(*)$ to the upper left corner in two different ways, we obtain $\mathcal{O}(\ell D) \cong \phi^* \mathcal{O}(D')$ for some $\ell \in \mathbf{Z}$, which forces $\ell = \deg(\phi)$, and we have obtained a simple necessary condition:

$$\phi^* D' \sim \deg(\phi) \cdot D.$$

Example. The necessary condition need not hold. Let (C, O) be an elliptic curve with a k-rational point P of order 2. Let Φ be the subgroup $\{ O, P \}$. The quotient map $C \to C/\Phi$ may be viewed as a degree 2 morphism between quasi-elliptic curves of degree 3:

$$\phi\colon (C, 3O) \longrightarrow (C/\Phi, 3O/\Phi).$$

Then $\phi^*(3O/\Phi) = 3O + 3P$, while $\deg(\phi) \cdot 3O = 6O$, but $[3]O \oplus [3]P \neq [6]O$, whence $3O + 3P \not\sim 6O$. Therefore, if C and C/Φ are embedded in $\mathbf{P}^2_k$ via $3O$ and $3O/\Phi$, then ϕ does *not* extend to a morphism $\mathbf{P}^2_k \to \mathbf{P}^2_k$.

CHAPTER III

Projective quasi-elliptic curves $C \overset{n}{\hookrightarrow} \mathbf{P}_k^{n-1}$

In this chapter, we study arithmo-geometric aspects of k-curves of genus 1 that are embedded as non-degenerate degree n curves in $\mathbf{P}_k^{n-1}$, where k is a perfect field. Obviously $n \geq 3$. Such a curve C will be denoted

$$C \overset{n}{\hookrightarrow} \mathbf{P}_k^{n-1}. \tag{III.1}$$

Remark. Together with the additional data of a choice of k-valued point on $\mathrm{J}_C[n]$, and the assumption $\mathrm{char}(k) \nmid n$, (III.1) is called an "n-prepared curve" in [O'N01]. When $k = \mathbf{C}$, (III.1) is called an "elliptic normal curve".

Let $\mathcal{D}$ be the class of hyperplane sections on C. Then (III.1) gives us a quasi-elliptic curve $(C, \mathcal{D})$ of degree at least 3 and such that $\mathcal{D}$ admits a k-rational representative. Call such a quasi-elliptic curve **projective**. Conversely, given a k-curve C of genus 1 and a divisor class $\mathcal{D}$ on C of degree $n \geq 3$ that admits a k-rational representative D, a choice of basis for $\mathrm{H}^0\big(C, \mathcal{O}(D)\big)$ gives an embedding to projective space (cf. §II.4), recovering the description (III.1). In summary, "projective quasi-elliptic curve of degree n" means essentially the same thing as "non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1".

Note that each k-curve C of genus 1 occurs as a projective quasi-elliptic curve: simply define a k-rational divisor on C by taking the Galois orbit of any $\bar{k}$-valued point on C.

III.1. Attempting to simplify the description

In this section, we answer the question: *are any of the words in "non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1" superfluous?* After all, we are familiar with the fact: a degree 3 smooth curve in $\mathbf{P}_k^2$ necessarily has genus 1 and necessarily is non-degenerate.

Proposition III.1.1. *If $X \subset \mathbf{P}_k^{n-1}$ is a non-degenerate curve, then* $\deg(X) \geq n - 1$.

Proof. Choosing $n-1$ distinct points in $X(\bar{k})$, there exists a hyperplane $H \subset \mathbf{P}_{\bar{k}}^{n-1}$ containing those points. If $\deg(X) < n-1$, then $X_{\bar{k}}$ is contained in H. □

Proposition. *If $X \subset \mathbf{P}_k^{n-1}$ is a non-degenerate curve, and D is a hyperplane section, then $\ell(D) \geq n$.*

Proof. The dimension $\ell(D)$ is the same for every hyperplane section, so let D be the section determined by $X_0 = 0$. Then $1, X_1/X_0, \ldots, X_{n-1}/X_0$ lie in $\mathrm{H}^0\big(X, \mathcal{O}(D)\big)$, and they are linearly independent since X is non-degenerate. Thus $\ell(D) \geq n$. □

Corollary. *If $C \subset \mathbf{P}_k^{n-1}$ is a non-degenerate curve of genus 1, then* $\deg(C) \geq n$.

Proof. By Riemann–Roch (see §A.1), we have $\ell(D) = \deg(D)$ for any divisor of positive degree. Now let D be any hyperplane section. Then $\deg(D) = \deg(C)$. □

Example. We show that a non-degenerate curve in $\mathbf{P}_k^{n-1}$ of genus 1 can have degree strictly larger than n. In [Har77, §IV.3] it is shown that every projective k-curve can be embedded in $\mathbf{P}_k^3$. The procedure goes like this: if the curve already lies in $\mathbf{P}_k^2$ or $\mathbf{P}_k^3$, we're done; otherwise, we repeatedly project from points off the curve to decrease the dimension. We can always get as far as $\mathbf{P}_k^3$ without

introducing singularities. Thus we can start with a projective quasi-elliptic curve $C \overset{5}{\hookrightarrow} \mathbf{P}^4_k$ of degree 5 in $\mathbf{P}^4_k$, and then project it to $\mathbf{P}^3_k$, giving us a non-degenerate degree 5 curve in $\mathbf{P}^3_k$ of genus 1.

Example. We show that a degree n curve in $\mathbf{P}^{n-1}_k$ of genus 1 can be degenerate. Take the non-degenerate degree 5 curve in $\mathbf{P}^3_k$ of genus 1 from the previous example, and inject it into $\mathbf{P}^4_k$. This gives a degenerate degree 5 curve in $\mathbf{P}^4_k$ of genus 1.

Example. We show that a non-degenerate degree n curve in $\mathbf{P}^{n-1}_k$ can have genus $\neq 1$. Consider a rational normal curve (generalization of the twisted cubic) of degree n in $\mathbf{P}^n_k$ and project it to $\mathbf{P}^{n-1}_k$. It has genus 0.

In summary, no words in "non-degenerate degree n curve in $\mathbf{P}^{n-1}_k$ of genus 1" are superfluous.

III.2. Basic facts about $C \overset{n}{\hookrightarrow} \mathbf{P}^{n-1}_k$

Let $C \overset{n}{\hookrightarrow} \mathbf{P}^{n-1}_k$ be a projective quasi-elliptic curve.

Proposition III.2.1. *Given $n-1$ points $P_1, \ldots, P_{n-1} \in C(\bar{k})$, they lie in the support of a* unique *hyperplane section.*

Proof. By §A.1d, there is a unique $Q \in C(\bar{k})$ so that $P_1 + \ldots + P_{n-1} + Q \in \mathcal{D}$, where $\mathcal{D}$ is the divisor class comprising hyperplane sections on C. □

Corollary III.2.2. *Given $n-1$* distinct *points $P_1, \ldots, P_{n-1} \in C(\bar{k})$, their linear span in $\mathbf{P}^{n-1}_k$ is a hyperplane.*

Proof. If their linear span had codimension ≥ 2, then $P_1, \ldots, P_{n-1}$ would be contained in more than one hyperplane, contradicting III.2.1. □

Corollary III.2.3. *Any $n-1$ or fewer* distinct *points in $C(\bar{k})$ are independent.*

Corollary III.2.4. *The linear span of any $n-2$ or fewer points in $C(\bar{k})$ misses the rest of C.*

Proof. Let ℓ be the number of distinct points in the given collection. By III.2.3, they span a $\mathbf{P}^\ell_{\bar{k}}$. If that $\mathbf{P}^\ell_{\bar{k}}$ were to meet C in another point, then, again by III.2.3, the points would have to instead span a $\mathbf{P}^{\ell+1}_{\bar{k}}$. □

III.3. The saturated homogeneous ideal of C

From the scheme viewpoint, our projective quasi-elliptic curve C is a closed subscheme of

$$\mathbf{P}^{n-1}_k = \mathrm{Proj}(S), \qquad \text{where } S = k[X_0, \ldots, X_{n-1}],$$

and thus, by [Har77, II.5.16], we have

$$C = \mathrm{Proj}(S/I),$$

where I is a homogeneous ideal in S. However, if I and I' are homogeneous ideals of S such that the rings S/I and S/I' are *not* isomorphic, it can nonetheless be the case (see [Har77, Ex. II.2.14c]) that

$$\mathrm{Proj}(S/I) \cong \mathrm{Proj}(S/I'). \tag{III.2}$$

Fortunately, by [Har77, Ex. II.5.10], we have (III.2) if and only if I and I' have the same saturation. Recall that the **saturation** of an ideal I is

$$\bar{I} = \{\, s \in S \,:\, \text{for each } i, \text{ there exists } n_i \text{ so that } X_i^{n_i} \cdot s \in I \,\}.$$

We always have $\mathrm{Proj}(S/I) \cong \mathrm{Proj}(S/\bar{I})$, and the correspondence between closed subschemes of $\mathbf{P}^{n-1}_k$ and saturated homogeneous ideals in S is one-to-one. Whenever we speak of *the ideal of C*, we always mean the unique saturated homogeneous ideal in S that defines C.

More generally, by [Har77, II.5.9], closed subschemes (of any scheme, not just projective space) correspond to quasi-coherent sheaves of ideals. Let $\mathcal{I}_C$ denote the ideal sheaf of C on $\mathbf{P}_k^{n-1}$. It is defined by the exactness of the following sequence of $\mathcal{O}_{\mathbf{P}_k^{n-1}}$-modules:

$$0 \to \mathcal{I}_C \to \mathcal{O}_{\mathbf{P}_k^{n-1}} \to \iota_* \mathcal{O}_C \to 0. \tag{III.3}$$

The relationship between $\mathcal{I}_C$ and the ideal of C is given by [Har77, Ex. II.5.10c]:

$$I = \bigoplus_{m \in \mathbf{Z}} \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(m)\big). \tag{III.4}$$

It is worth recording that the (saturated homogeneous) ideal of $C_{\bar{k}}$ is simply

$$I_{\bar{k}} = I \otimes_k \bar{k}.$$

Certainly $I_{\bar{k}}$ is *an* ideal of $C_{\bar{k}}$, and one can easily check that it is saturated; alternatively, start with the description

$$I_{\bar{k}} := \bigoplus_{m \in \mathbf{Z}} \mathrm{H}^0\big(\mathbf{P}_{\bar{k}}^{n-1}, \mathcal{I}_{C_{\bar{k}}}(m)\big),$$

and apply [Har77, III.9.3], which tells us

$$\mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(m)\big) \otimes_k \bar{k} = \mathrm{H}^0\big(\mathbf{P}_{\bar{k}}^{n-1}, \mathcal{I}_{C_{\bar{k}}}(m)\big), \quad \text{for all } m \in \mathbf{Z},$$

whence we recover $I_{\bar{k}} = I \otimes_k \bar{k}$.

III.4. Projective normality

By twisting (III.3), we obtain, for each $m \in \mathbf{Z}$, the following exact sequence of $\mathcal{O}_{\mathbf{P}_k^{n-1}}$-modules:

$$0 \to \mathcal{I}_C(m) \to \mathcal{O}_{\mathbf{P}_k^{n-1}}(m) \to (\iota_* \mathcal{O}_C)(m) \to 0. \tag{III.5}$$

Taking global sections, we obtain

$$\begin{aligned} 0 \to \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(m)\big) \to \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{O}_{\mathbf{P}_k^{n-1}}(m)\big) \to \mathrm{H}^0\big(C, \mathcal{O}_C(mD)\big) \\ \to \mathrm{H}^1\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(m)\big) \to \mathrm{H}^1\big(\mathbf{P}_k^{n-1}, \mathcal{O}_{\mathbf{P}_k^{n-1}}(m)\big) \to \mathrm{H}^1\big(C, \mathcal{O}_C(mD)\big) \to \dots, \end{aligned} \tag{III.6}$$

where D is any choice of k-rational hyperplane section on C. (We used $\mathrm{H}^0\big(\mathbf{P}_k^{n-1}, (\iota_* \mathcal{O}_C)(m)\big) = \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \iota_*(\mathcal{O}_C(mD))\big) = \mathrm{H}^0\big(C, \mathcal{O}_C(mD)\big)$, which follow from [Har77, Ex. III.4.1, II.5.12c].)

It is of interest to determine for which m the map

$$\mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{O}_{\mathbf{P}_k^{n-1}}(m)\big) \to \mathrm{H}^0\big(C, \mathcal{O}_C(mD)\big) \tag{III.7}$$

from (III.6) is surjective. This gives us information about the dimension of the first term in (III.6), which, by (III.4), is information about the mth graded piece of the ideal I of C.

For $m < 0$, surjectivity of (III.7) follows from $\ell(mD) = 0$ (see [Har77, IV.1.2]). For $m = 0$, surjectivity follows from the fact that C is connected. For $m = 1$, surjectivity is sometimes called *linear normality*, and holds because we can view (III.1) as the embedding associated with a choice of basis for $\mathrm{H}^0\big(C, \mathcal{O}_C(D)\big)$, whence the homogeneous coordinates on $\mathbf{P}_k^{n-1}$ pull back to that basis. We now establish surjectivity for all m, which is sometimes called *projective normality* (cf. [Har77, Ex. II.5.14]).

Theorem III.4.1. *Let C be a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1. For each $m \in \mathbf{Z}$, the short exact sequence* (III.5) *remains exact upon taking global sections. In other words, the map* (III.7) *is surjective.*

Proof. Since $\mathrm{H}^1\big(\mathbf{P}_k^{n-1}, \mathcal{O}_{\mathbf{P}_k^{n-1}}(m)\big) = 0$ (see [Har77, III.5.1]), the surjectivity of (III.7) is equivalent, by (III.6), to

$$\mathrm{H}^1\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(m)\big) = 0, \quad \text{for all } m \in \mathbf{Z}.$$

The cases $m < 2$ were established preceding the theorem statement. Now we mimic the proof in [Hul86].

By [Har77, III.9.3], $\mathrm{H}^1\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(m)\big) \otimes_k \bar{k} \cong \mathrm{H}^1\big(\mathbf{P}_{\bar{k}}^{n-1}, \mathcal{I}_{C_{\bar{k}}}(m)\big)$, whence we may assume $k = \bar{k}$. By Bertini (see [Har77, II.8.18]), there exists a hyperplane H so that the scheme $D = C \cap H$ comprises n distinct points, call them $P_1, \ldots, P_n$.

$$\begin{array}{ccc} D & \xrightarrow{s} & H \\ \downarrow & & \downarrow{\scriptstyle j} \\ C & \xrightarrow{\iota} & \mathbf{P}_k^{n-1} \end{array}$$

We will now consider various sheaves of $\mathcal{O}_{\mathbf{P}_k^{n-1}}$-modules on $\mathbf{P}_k^{n-1}$, which fit together into the following diagram:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{I}_C(m) & \longrightarrow & \mathcal{O}_{\mathbf{P}_k^{n-1}}(m) & \longrightarrow & (\iota_*\mathcal{O}_C)(m) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{I}_C(m+1) & \longrightarrow & \mathcal{O}_{\mathbf{P}_k^{n-1}}(m+1) & \longrightarrow & (\iota_*\mathcal{O}_C)(m+1) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & (j_*\mathcal{I}_{D/H})(m+1) & \longrightarrow & (j_*\mathcal{O}_H)(m+1) & \longrightarrow & (j_*s_*\mathcal{O}_D)(m+1) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Multiplication by the linear form $\ell \in \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{O}_{\mathbf{P}_k^{n-1}}(1)\big)$ that defines H gives the exact sequence

$$0 \to \mathcal{I}_C(m) \xrightarrow{\ell} \mathcal{I}_C(m+1) \to (j_*\mathcal{I}_{D/H})(m+1) \to 0,$$

where $\mathcal{I}_{D/H}$ denotes the ideal sheaf of D on H. Taking global sections, we obtain

$$\begin{aligned} \ldots \to \mathrm{H}^1\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(m)\big) & \\ \to \mathrm{H}^1\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(m+1)\big) & \to \mathrm{H}^1\big(\mathbf{P}_k^{n-1}, (j_*\mathcal{I}_{D/H})(m+1)\big) \to \ldots, \end{aligned}$$

and the theorem is reduced, by induction on $m \geq 1$, to establishing

$$\mathrm{H}^1\big(\mathbf{P}_k^{n-1}, (j_*\mathcal{I}_{D/H})(m+1)\big) = 0, \quad \text{for } m \geq 1. \tag{$*$}$$

If we now start with the exact sequence of sheaves of $\mathcal{O}_H$-modules

$$0 \to \mathcal{I}_{D/H} \to \mathcal{O}_H \to s_*\mathcal{O}_D \to 0,$$

we can apply j_* and then twist $m+1$ times to obtain

$$0 \to (j_*\mathcal{I}_{D/H})(m+1) \to (j_*\mathcal{O}_H)(m+1) \to (j_*s_*\mathcal{O}_D)(m+1) \to 0.$$

Note that j_* is exact here because j is a closed immersion (see [Har77, III.3.7, III.8.1]). Taking global sections gives

$$\begin{aligned} \ldots \to \mathrm{H}^0\big(H, \mathcal{O}_H(m+1)\big) \to \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, (j_*s_*\mathcal{O}_D)(m+1)\big) & \\ \to \mathrm{H}^1\big(\mathbf{P}_k^{n-1}, (j_*\mathcal{I}_{D/H})(m+1)\big) \to \mathrm{H}^1\big(H, \mathcal{O}_H(m+1)\big) \to \ldots. & \end{aligned}$$

We now claim $\mathrm{H}^1\big(H, \mathcal{O}_H(m+1)\big)$ vanishes for $m \geq 1$; in other words, since $H \cong \mathbf{P}_k^{n-2}$, we are claiming $\mathrm{H}^1\big(\mathbf{P}_k^{n-2}, \mathcal{O}_{\mathbf{P}_k^{n-2}}(m+1)\big) = 0$ for $m \geq 1$. For $n \geq 4$, the claim follows immediately from [Har77, III.5.1b]. For $n = 3$, the claim follows from the existence of a perfect pairing (see [Har77, III.5.1d])

$\mathrm{H}^0\big(\mathbf{P}_k^1, \mathcal{O}_{\mathbf{P}_k^1}(-m-3)\big) \times \mathrm{H}^1\big(\mathbf{P}_k^1, \mathcal{O}_{\mathbf{P}_k^1}(m+1)\big) \to k$ and the fact that the first term in this pairing vanishes when $m \geq 1$ (see [Har77, II.5.13]). Having established the claim, we see that $(*)$ is equivalent to showing the map

$$\mathrm{H}^0\big(H, \mathcal{O}_H(m+1)\big) \to \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, (j_* s_* \mathcal{O}_D)(m+1)\big)$$

to be surjective for $m \geq 1$. Since the codomain is simply the direct sum of one-dimensional skyscraper sheaves supported on the P_i, we are done if we can exhibit an $(m+1)$-form on H that vanishes at all P_i except, say, P_1. Since some projective coordinate does not vanish at P_1, we are reduced to finding a *quadratic* form on H that vanishes at all P_i except P_1.

By lemma III.2.4, the points $P_3, \ldots, P_n$ span a linear space in $\mathbf{P}_k^{n-1}$ that misses the rest of C, and thus they define a hyperplane inside H that misses P_1 and P_2. Reasoning instead with $P_2, \ldots, P_{n-1}$, we obtain a hyperplane that misses P_1 and P_n. The product of the associated linear forms gives a quadratic form on H that vanishes at all P_i except P_1. □

III.5. The Hilbert function of C

To describe I explicitly for particular values of n, we will start by determining the dimension of each graded piece. Set

$$d_I(s) := \dim_k I_s = \dim_k \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(s)\big).$$

By III.4.1, taking global sections of the exact sequence

$$0 \to \mathcal{I}_C(s) \to \mathcal{O}_{\mathbf{P}_k^{n-1}}(s) \to (i_* \mathcal{O}_C)(s) \to 0$$

gives the exact sequence

$$0 \to \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(s)\big) \to \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{O}_{\mathbf{P}_k^{n-1}}(s)\big) \to \mathrm{H}^0\big(C, \mathcal{O}(sD)\big) \to 0,$$

whence

$$d_I(s) = \dim_k \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{O}_{\mathbf{P}_k^{n-1}}(s)\big) - \ell(sD).$$

By counting monomials of degree s, and by Riemann–Roch, we obtain

$$d_I(s) = \binom{n-1+s}{n-1} - ns.$$

Recall that the Hilbert function of C is $\phi_C(s) := \dim_k (S/I)_s$. By what we determined above, we immediately obtain:

$$\begin{aligned} \phi_C(s) &= \dim_k S_s - \dim_k I_s \\ &= \binom{n-1+s}{n-1} - d_I(s) \\ &= ns. \end{aligned}$$

For sufficiently large s, the Hilbert function agrees with a polynomial function (see [Har77, I.7.5]), called the Hilbert polynomial of C. But $\phi_C(s)$ is itself polynomial in s, whence $\phi_C(s)$ is both the Hilbert function and the Hilbert polynomial. (Since C is a degree n curve of genus 1, we can independently see, by [Har77, I.7.6, Ex. I.7.2], that its Hilbert polynomial is $P_C(s) = ns$.) We have proved:

Theorem III.5.1. *On a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1, the Hilbert polynomial and Hilbert function are the same, namely $\phi_C(s) = P_C(s) = ns$.*

III.6. C is a complete intersection for $n = 3$ and $n = 4$

We ask: *for which n is a projective quasi-elliptic curve C a complete intersection?*

Recall, for X a closed subscheme of $\mathbf{P}_k^{n-1}$, each generating set for the ideal of X has cardinality $\geq n - 1 - \dim(X)$; if there exists a generating set of cardinality $= n - 1 \dim(X)$, then X is said to be a *complete intersection*, in which case the degree of X is the product of the degrees of the $n - 1 - \dim(X)$ generators (see [HAR77, I.7.7]).

Our curve (III.1), whose degree n is ≥ 3, is a complete intersection if and only if its ideal can be generated by $n - 2$ elements. Since no hyperplane contains C, each generator has degree ≥ 2, whence, to be a complete intersection, C must have degree $\geq 2^{n-2}$. From $2^{n-2} \leq n$ we conclude $n \leq 4$.

Theorem III.6.1. *Let C be a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1. Then C is a complete intersection if and only if $n = 3$ or $n = 4$.*

Proof. We already saw that $n = 3$ or $n = 4$ is necessary. Let $n = 3$. From our calculation in §III.5, we have

$$d_I(s) := \dim_k I_s = \binom{s+2}{s} - 3s = \frac{(s-2)(s-1)}{2}.$$

In particular, $d_I(3) = 1$, so there is a cubic form $F \in I$. Since $\langle F \rangle \subseteq I$, we obtain $\langle F \rangle = I$ by showing $\dim_k \langle F \rangle_s = \dim_k I_s$ for each degree s. But the dimension of $\langle F \rangle$ in degree s is the same as the dimension of $S = k[x, y, z]$ in degree $s - 3$. Since $\dim_k S_s = \binom{s+2}{2}$, we have $\dim_k \langle F \rangle_s = \binom{s-1}{2}$, which is just $d_I(s)$.

Now let $n = 4$. Then

$$d_I(s) = \binom{s+3}{s} - 4s = \frac{(s-1)(s^2+7s-6)}{6}.$$

In particular, $d_I(2) = 2$, so there are two linearly independent quadratic forms $Q_1, Q_2 \in I$. As before, we will show $\dim_k I_s = \dim_k \langle Q_1, Q_2 \rangle_s$, and thus obtain $I = \langle Q_1, Q_2 \rangle$. Since there are relations between Q_1 and Q_2, we have to work a bit harder to determine $\dim_k \langle Q_1, Q_2 \rangle_s$. Let N be the free module $S \oplus S$, where $S = k[w, x, y, z]$. Consider the Koszul complex for $(Q_1, Q_2) \in N$ (cf. [EIS95, §17.2]),

$$0 \longrightarrow S \longrightarrow N \longrightarrow \bigwedge^2 N \longrightarrow 0,$$

where the maps are just wedge-multiplication on the left by the element (Q_1, Q_2). In terms of the basis $e_1 = (1, 0)$ and $e_2 = (0, 1)$ for N, and the basis $e_1 \wedge e_2$ for $\bigwedge^2 N$, the complex is

$$0 \longrightarrow S \xrightarrow{\binom{Q_1}{Q_2}} S^2 \xrightarrow{(-Q_2, Q_1)} S \longrightarrow 0. \qquad (*)$$

By [EIS95, 17.5], the complex $(*)$ is *exact* everywhere except at the right since Q_1, Q_2 compose a regular sequence; indeed, since C is not contained in a plane, Q_1 is irreducible whence $\langle Q_1 \rangle$ is prime, and since Q_2 is not a multiple of Q_1, it is nonzero in the integral domain $S/\langle Q_1 \rangle$. We thus obtain the exact sequence

$$0 \longrightarrow S \xrightarrow{\binom{Q_1}{Q_2}} S^2 \xrightarrow{(-Q_2, Q_1)} \langle Q_1, Q_2 \rangle \longrightarrow 0. \qquad (**)$$

From this we can determine $\dim_k \langle Q_1, Q_2 \rangle_s$. Since $\dim_k S_s = \binom{s+3}{3}$, the dimension of the middle term of $(**)$ in degree s is $2\binom{s+3}{3}$. The map $\binom{Q_1}{Q_2}$ shifts degrees by 2, whence the dimension of the cokernel in degree s is $2\binom{s+3}{3} - \binom{(s-2)+3}{3}$. But the quotient map $(-Q_2, Q_1)$ again shifts degrees by 2, so

$$\dim_k \langle Q_1, Q_2 \rangle_s = 2\binom{(s-2)+3}{3} - \binom{(s-4)+3}{3},$$

which is the same as $d_I(s)$. □

Remark. For $n = 4$, an alternate argument appears at the end of §18.2 in [EIS95].

III.7. Cutting C out by quadrics when $n \geq 4$ and $\mathrm{char}(k) \neq 2$

We ask: *is C cut out scheme-theoretically by quadrics (equivalently, is I generated by quadratic forms)? If so, how many quadrics are needed?* In the previous section, we saw that C is *not* cut out by quadrics when $n = 3$, while it is cut out by a pair of quadrics when $n = 4$.

Proposition III.7.1. *Let C be a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1. Then each minimal generating set for I contains $n(n-3)/2$ quadratic forms.*

Proof. From our work in §III.5, we have

$$\dim_k\{\text{ quadratic forms in } I\} = d_I(2) = \dim_k \mathrm{H}^0\big(\mathbf{P}_k^{n-1}, \mathcal{I}_C(2)\big) = \frac{n(n-3)}{2}.$$

Since there are no linear forms in I, each generating set for I must contain $n(n-3)/2$ linearly independent quadratic forms, whence each *minimal* generating set contains precisely $n(n-3)/2$ quadratic forms (and possibly also forms of higher degree—indeed, such is the case when $n = 3$). □

Theorem III.7.2. *Assume $\mathrm{char}(k) \neq 2$. Let C be a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1. Then C is cut out scheme-theoretically by quadrics if and only if $n \geq 4$, in which case each minimal generating set for I comprises $n(n-3)/2$ elements, all of them quadratic forms.*

Proof. In light of III.7.1, it remains to show, when $n \geq 4$ and $\mathrm{char}(k) \neq 2$, that I is generated by quadratic forms—we do this below, in III.7.4. □

We recall (cf. [Har77, Ex. 5.12] and [Har95, Lec. 3, Lec. 22]) basic facts about quadrics in $\mathbf{P}_k^{n-1}$ when $\mathrm{char}(k) \neq 2$. Thinking of the variables $(X_0, \ldots, X_{n-1})$ as a column vector X, each quadratic form $Q(X) \in k[X_0, \ldots, X_{n-1}]$ can be written in the form $Q(X) = X^{\mathrm{t}}AX$, where A is an $n \times n$ symmetric matrix with entries in k. The **rank** of the quadric defined by Q is, by definition, simply the rank of the matrix A. A rank 1 quadric is a hyperplane of multiplicity 2, while a rank 2 quadric is a union of two distinct hyperplanes. A quadric is irreducible if and only if its rank r satisfies $r \geq 3$, and a quadric is smooth if and only if r is maximal: $r = n$. For $2 \leq r \leq n-1$, the quadric may be described as a cone, with vertex a $\mathbf{P}_k^{n-1-r}$, over a smooth (rank r) quadric in $\mathbf{P}_k^{r-1}$. Given any two distinct quadrics Q_A and Q_B, with (scheme-theoretic) intersection $X = Q_A \cap Q_B$, each member of the pencil

$$\lambda_0 Q_A + \lambda_1 Q_B, \quad \text{where } [\lambda_0 : \lambda_1] \in \mathbf{P}_k^1(\bar{k}), \tag{III.8}$$

also contains X. The pencil (III.8) may be recovered by any two distinct members of that pencil. The singular members correspond to the roots $[\lambda_0 : \lambda_1] \in \mathbf{P}_k^1(\bar{k})$ of the equation

$$\det(\lambda_0 A + \lambda_1 B) = 0, \tag{III.9}$$

where A and B are the $n \times n$ symmetric matrices corresponding to Q_A and Q_B.

We return now to our curve C. Since C is non-degenerate, each quadric containing C has rank ≥ 3, and we will show that $C_{\bar{k}}$ is in fact the (scheme-theoretic) intersection of the rank 3 quadrics containing it. (We had to go to $\bar{k}$ for the following reason: since the roots of (III.9) need not be k-rational, the singular quadrics in $\mathbf{P}_{\bar{k}}^{n-1}$ containing $C_{\bar{k}}$ need not be defined over k.)

For $n = 4$, we already know from §III.6 that $C = Q_A \cap Q_B$, where Q_A and Q_B are any two distinct quadrics containing C, and we know from III.7.1 that *every* quadric containing C lies in the pencil (III.8). (Both facts hold even when $\mathrm{char}(k) = 2$, but henceforth we assume $\mathrm{char}(k) \neq 2$.)

We will see later (in §III.13) that there exists a linear change-of-coordinates, defined over $\bar{k}$, so that the group $H_4' \subset \mathbf{GL}_4(\bar{k})$ of order 64 generated by

$$M = \begin{bmatrix} 1 & & & \\ & i & & \\ & & -1 & \\ & & & -i \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} & 1 & & \\ & & 1 & \\ & & & 1 \\ 1 & & & \end{bmatrix}$$

preserves $C_{\bar{k}}$ in its action on $\mathbf{P}^3_{\bar{k}}$, where $i^2 = -1$. (We use the notation H'_4 because, in §III.12, we reserve "H_4" to mean the order 64 subgroup of $\mathbf{SL}_4(\bar{k})$ that has the same image in $\mathbf{PGL}_4(\bar{k})$ as H'_4.) We assume the change-of-coordinates to have been applied.

Since H'_4 preserves $C_{\bar{k}}$, it also preserves the set (III.8) of all quadrics that contain $C_{\bar{k}}$. As discussed in [Hul86, §III.2], the H'_4-module $\mathrm{H}^0\big(\mathbf{P}^3_{\bar{k}}, \mathcal{O}(2)\big)$ can be expressed as a direct sum of irreducible submodules in the form

$$\mathrm{H}^0\big(\mathbf{P}^3_{\bar{k}}, \mathcal{O}(2)\big) = (V_1 \oplus V_2) \oplus V_3 \oplus V_4 \oplus V_5,$$

where

$$\begin{aligned}
V_1 &= \langle x_0^2 + x_2^2,\, x_1^2 + x_3^2 \rangle, \\
V_2 &= \langle x_1 x_3,\, x_0 x_2 \rangle, \\
V_3 &= \langle x_0^2 - x_2^2,\, x_1^2 - x_3^2 \rangle, \\
V_4 &= \langle x_0 x_1 + x_2 x_3,\, x_1 x_2 + x_0 x_3 \rangle, \\
V_5 &= \langle x_0 x_1 - x_2 x_3,\, x_1 x_2 - x_0 x_3 \rangle.
\end{aligned}$$

One can check that $V_1 \cong V_2$ as H'_4-modules, while no other two of the direct summands are isomorphic. Therefore, either our pencil (III.8) lies in $V_1 \oplus V_2$, or it is equal to one of V_3, V_4, V_5. It cannot be V_3 since $C_{\bar{k}}$ does not lie in a plane, while it can be neither V_4 nor V_5 since those pencils define singular curves. Thus, our pencil lies in $V_1 \oplus V_2$. As an H'_4-module, it must be isomorphic to V_1 and V_2, whence it must have a $\bar{k}$-vector space basis on which H'_4 acts in the same manner as it does on the bases for V_1 and V_2 exhibited above; in short, our pencil must have a $\bar{k}$-vector space basis of the form

$$\big\langle a(x_0^2 + x_2^2) + b(x_1 x_3),\, a(x_1^2 + x_3^2) + b(x_0 x_2) \big\rangle.$$

Some pairs of values for a, b cannot occur, but we need not identify them all: certainly $(a, b) \neq (0, 0)$, and it is easy to check that (III.9) has at least two distinct roots. In summary, $C_{\bar{k}}$ is an intersection of a pair of quadrics of rank 3, whence it is also the intersection of all rank 3 quadrics containing it.

Theorem III.7.3. *Assume $k = \bar{k}$ and $\mathrm{char}(k) \neq 2$. For $n \geq 4$, each non-degenerate degree n curve in $\mathbf{P}^{n-1}_k$ of genus 1 is cut out scheme-theoretically by the rank 3 quadrics containing it; that is, the rank 3 quadratic forms in I compose a generating set for I.*

Proof. The proof for $k = \mathbf{C}$ in [Hul86, §IV.1] goes through unaltered. For the convenience of the reader, we repeat it here. It proceeds by induction on n. The case $n = 4$ was explained preceding the theorem.

Assume $n \geq 5$. We shall first show that C is a *set-theoretic* intersection of rank 3 quadrics. To do this, let $P \in \mathbf{P}^{n-1}_k(k) \setminus C(k)$ be an arbitrary point not lying on C. We can choose a point $P_0 \in C(k)$ such that the line PP_0 is neither a secant nor a tangent of C. (Otherwise, projection from P would map C onto a non-degenerate curve $C' \subset \mathbf{P}^{n-2}_k$ of degree $\leq n/2$, so by III.1.1 we would have $n/2 \geq n - 2$, which is never the case for $n \geq 5$.) Projection from P_0 maps C onto a non-degenerate degree $n-1$ curve $C' \subset \mathbf{P}^{n-2}_k$ of genus 1, and the image P' of P does not lie on C'. By the induction hypothesis, there is a rank 3 quadric Q' through C' that does not contain P'. Let Q be the cone over Q' with vertex P_0. Then $C \subset Q$ but $P \notin Q(k)$.

It remains to show that the intersection is *scheme-theoretic*; equivalently, we must show that the rank 3 quadrics separate tangents. Let $P \in C(k)$ be an arbitrary point on C and let L be a line through P that is not tangent to C at P. Next choose a point $P_0 \in C(k)$ that does not lie on L. Projecting from P_0 we get a non-degenerate degree $n-1$ curve C' in $\mathbf{P}^{n-2}_k$ of genus 1. Let P' and L' be the images of P and L. By the induction hypothesis, there is a rank 3 quadric Q' through C' such that Q' and the line L' intersect transversally at P'. The cone Q over Q' with vertex P_0 therefore intersects the line L at P transversally. □

The following corollary to the theorem completes the proof of III.7.2.

Corollary III.7.4. *Assume* $\mathrm{char}(k) \neq 2$. *For* $n \geq 4$, *each non-degenerate degree* n *curve in* $\mathbf{P}_k^{n-1}$ *of genus* 1 *is cut out scheme-theoretically by quadrics; that is, the ideal* I *of* C *is generated by quadratic forms. (Moreover, in any generating set for* I, *the subset of quadratic forms is itself a generating set.)*

Proof. By the theorem, certainly $I \otimes_k \bar{k}$ is generated by quadratic forms. Let $\{ p_1, \ldots, p_r \}$ be a finite set of homogeneous forms that generate I. Any element of $I \otimes_k \bar{k}$ can also be expressed in terms of the p_i. Certainly none of the p_i is linear, so by degree considerations, elements of a quadratic generatoring set for $I \otimes_k \bar{k}$ can be expressed in terms of those p_i that are quadratic, whence the quadratic p_i themselves compose a quadratic generating set for $I \otimes_k \bar{k}$. Multiplying them by all possible powers of the variables leads to a generating set for $I \otimes_k \bar{k}$ as a vector space over $\bar{k}$. Thus there is a $\bar{k}$-basis for $I \otimes_k \bar{k}$ of vectors that are defined over k, whence, by linear descent (see [Sil99, II.5.8.1]), the same vectors compose a k-basis for I. Therefore, the quadratic p_i compose a quadratic generating set for I. □

III.8. Classifying linear automorphisms of $C \overset{\subset n}{\hookrightarrow} \mathbf{P}_k^{n-1}$

Let $C \overset{\subset n}{\hookrightarrow} \mathbf{P}_k^{n-1}$ be a projective quasi-elliptic curve of degree n, and let $\mathcal{D}$ be the class of hyperplane sections on C.

The automorphism group of $\mathbf{P}_{\bar{k}}^{n-1}$ is $\mathbf{PGL}_n(\bar{k})$. Since elements of $\mathbf{PGL}_n(\bar{k})$ send hyperplanes in $\mathbf{P}_{\bar{k}}^{n-1}$ to hyperplanes, if such an element also preserves $C_{\bar{k}}$, then it will induce an automorphism of $(C_{\bar{k}}, \mathcal{D})$. Automorphisms of $C_{\bar{k}}$ that are induced by automorphisms of the ambient projective space are called **linear automorphisms of** $C_{\bar{k}}$.

It turns out that all automorphisms of $(C_{\bar{k}}, \mathcal{D})$ are linear. We saw in II.4.1 that each automorphism of $(C_{\bar{k}}, \mathcal{D})$ extends to an automorphism of the ambient $\mathbf{P}_{\bar{k}}^{n-1}$. Furthermore, the extension is unique: since each point in $\mathbf{P}_{\bar{k}}^{n-1}(\bar{k})$ is an intersection of hyperplanes in $\mathbf{P}_{\bar{k}}^{n-1}$, an element of $\mathbf{PGL}_n(\bar{k})$ is determined by its behavior on hyperplanes, which are in one-to-one correspondence with hyperplane sections on $C_{\bar{k}}$; thus, if two elements of $\mathbf{PGL}_n(\bar{k})$ move a given hyperplane to two different places, then they move the associated hyperplane section to two different places, and thus cannot induce the same automorphism of $C_{\bar{k}}$. We have shown:

$$\mathrm{Aut}\big((C_{\bar{k}}, \mathcal{D})\big) = \big\{ \text{linear automorphisms of } C_{\bar{k}} \big\} \cong \big\{ \phi \in \mathbf{PGL}_n(\bar{k}) \colon \phi(C_{\bar{k}}) = C_{\bar{k}} \big\}.$$

Note that the isomorphism above is $\mathrm{Gal}(\bar{k}/k)$-equivariant. In other words: *any group of matrix classes in* $\mathbf{PGL}_n(\bar{k})$ *that acts on* C *necessarily does so in a faithful and Galois equivariant manner.* By II.2.7, the largest such group has structure

$$\big\{ \phi \in \mathbf{PGL}_n(\bar{k}) \,:\, \phi(C_{\bar{k}}) = C_{\bar{k}} \big\} \cong \mathrm{J}_C[n](\bar{k}) \rtimes \mathrm{Aut}\big((C_{\bar{k}}, O)\big),$$

where $O \in C(\bar{k})$ is a point of hyperosculation.

Proposition III.8.1. *In the above identification, the elements of* $\mathbf{PGL}_n(\bar{k})$ *that act fixpoint-free on* C *correspond precisely to* $\mathrm{J}_C[n](\bar{k})$. *Thus, when* $\mathrm{char}(k) \nmid n$, *there are precisely* n^2 *elements of* $\mathbf{PGL}_n(\bar{k})$ *that act fixpoint-free on* C.

Proof. The first part is a special case of A.4.3. The second part follows from $\#\mathrm{J}_C[n](\bar{k}) = n^2$ when $\mathrm{char}(k) \nmid n$. □

Corollary III.8.2. *Let* C *be a non-degenerate degree* n *curve in* $\mathbf{P}_k^{n-1}$ *of genus* 1. *Let* $J_n \subset \mathbf{PGL}_n(\bar{k})$ *be the subgroup of elements that preserve* C *and act fixpoint-free on* C. *Then* J_n *is a faithful and Galois equivariant representation of the action of* $\mathrm{J}_C[n](\bar{k})$ *on* C.

III.9. Concerning the $[-1]$-automorphisms of $C \overset{\subset n}{\hookrightarrow} \mathbf{P}_k^{n-1}$

This section is about those linear automorphisms of $C_{\bar{k}}$ that are of order 2 and have a fixpoint in $C(\bar{k})$.

Proposition III.9.1. *Let ϕ be an order 2 curve automorphism of $C_{\bar{k}}$ that has a fixpoint $P \in C(\bar{k})$. Then ϕ is the* unique *order 2 automorphism of the elliptic curve $(C_{\bar{k}}, P)$, more commonly known as $[-1]$. Thus the fixpoints of ϕ are the points of 2-torsion on $(C_{\bar{k}}, P)$; furthermore, if Q is such a point, then ϕ is also the $[-1]$-automorphism on the elliptic curve $(C_{\bar{k}}, Q)$.*

Proof. See A.4.8. □

Let $O \in C(\bar{k})$ be a point of hyperosculation. By $[-1]$ we mean the unique order 2 automorphism of the elliptic curve $(C_{\bar{k}}, O)$. In the previous section, we identified the linear automorphisms of $C_{\bar{k}}$ with $\mathrm{J}_C[n](\bar{k}) \rtimes \mathrm{Aut}\big((C_{\bar{k}}, O)\big)$.

Proposition III.9.2. *Inside $\mathrm{J}_C[n](\bar{k}) \rtimes \mathrm{Aut}\big((C_{\bar{k}}, O)\big)$, the order 2 linear automorphism of $C_{\bar{k}}$ with a fixpoint are precisely the elements of the form $\tau \circ [-1]$, where $\tau \in \mathrm{J}_C[n](\bar{k})$.*

Proof. Follows immediately from A.4.9. □

It is easy to verify (cf. the proof of A.4.9) that $\tau_{Q \oplus Q} \circ [-1]$ is the unique order 2 automorphism of $C_{\bar{k}}$ that fixes $Q \in C(\bar{k})$, where the group law is on the elliptic curve $(C_{\bar{k}}, O)$, and $\tau_{Q \oplus Q}$ is the translation-by-$(Q \oplus Q)$ map. We therefore see a relationship between points of hyperosculation and fixpoints of order 2 linear automorphisms, but due to the presence of $Q \oplus Q$, that relationship depends on the parity of n:

- Assume n is odd. For $P \in C(\bar{k})$ a point of hyperosculation, there is a unique point of hyperosculation $Q \in C(\bar{k})$ so that $[2]Q = P$. Therefore, for each linear automorphism of order 2 with a fixpoint in $C(\bar{k})$, precisely one of its fixpoints is a point of hyperosculation.
- Assume n is even. For $P \in C(\bar{k})$ a point of hyperosculation, either all the solutions of $[2]Q = P$ are points of hyperosculation, or none of them are. (The two cases are determined by whether P is a point of $(n/2)$-torsion.) Therefore, for each linear automorphism of order 2 with a fixpoint in $C(\bar{k})$, either all of its fixpoints are points of hyperosculation, or none of them are.

In either case, we see: *each point of hyperosculation occurs as the fixpoint of a unique order 2 linear automorphism.*

III.9a. Procedure for finding the points of hyperosculation

By the work in §III.8, we may identify the order 2 linear automorphisms of C that have a fixpoint with the elements of $\mathbf{PGL}_n(\bar{k})$ that: act on C, have order 2, and admit a fixpoint. In fact, as the following proposition shows, if we find one of them, and if we have found all the elements of $\mathbf{PGL}_n(\bar{k})$ that act fixpoint-free on C, then this gives us all the order 2 elements with fixpoints.

Proposition III.9.3. *Let C be a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1. Let $\bar{T} \in \mathbf{PGL}_n(\bar{k})$ be an element of order 2 that preserves C and has at least one fixpoint on C. The remaining such automorphisms have the form $\bar{M} \otimes \bar{T}$, where $\bar{M} \in \mathbf{PGL}_n(\bar{k})$ acts on C without fixpoints.*

Proof. If one of the fixpoints of $\bar{T}$ is a point of hyperosculation, then this proposition is just a repeat of III.9.2. In fact, by III.9.2, we know that $\bar{T} = \tau \circ [-1]$ for some $\tau \in \mathrm{J}_C[n](\bar{k})$. It is clear that each $\bar{M} \circ \bar{T}$ also has that form. □

To find the points of hyperosculation, we first find all the order 2 elements of $\mathbf{PGL}_n(\bar{k})$ that preserve C and have a fixpoint on C. The points of hyperosculation lie among the finitely many fixpoints. For each fixpoint, the osculating hyperplane can be determined by brute force: parameterize all hyperplanes that go through the given point, and then impose the conditions that maximize the intersection multiplicity of the hyperplane with C. The unique solution is the osculating hyperplane. If the hyperplane does not meet C elsewhere, then the point in question is a point of hyperosculation.

Remark. When n is odd, a simpler way for finding the points of hyperosculation is given in III.11.8.

III.10. The commutator pairing is the Weil pairing

Let $J_n \subset \mathbf{PGL}_n(\bar{k})$ denote the subgroup of elements that act fixpoint-free on C. In the previous section, we saw that there is a canonical isomorphism of Galois modules

$$J_n \cong \mathrm{J}_C[n](\bar{k}). \tag{III.10}$$

We will establish that the "commutator pairing" (defined below) on J_n corresponds, under (III.10), to the inverse of the Weil pairing on $\mathrm{J}_C[n](\bar{k})$.

III.10a. Commutator pairings on abelian projective linear groups

Consider an abelian subgroup $G \subset \mathbf{PGL}_n(\bar{k})$. For matrix classes $[A], [B] \in G$, the usual commutator

$$\big[[A],[B]\big] := [A]\,[B]\,[A]^{-1}[B]^{-1}$$

is of course trivial. But if we first lift the classes $[A], [B]$ to representing matrices $A, B \in \mathbf{GL}_n(\bar{k})$, then the commutator $[A, B]$ might be nontrivial, and all we can say for certain is that $[A, B]$ lies in $\bar{k}^\times$. It is easy to check that $[A, B]$ is independent of the choice of representing matrices. Thus we obtain a well-defined **commutator pairing**

$$\begin{aligned} G \times G &\longrightarrow \bar{k}^\times, \\ \big([A],[B]\big) &\longmapsto A\,B\,A^{-1}B^{-1}. \end{aligned}$$

The commutator pairing is immediately seen to be alternating (whence also skew-symmetric), and can be easily verified to be bilinear. If G is Galois stable, then the pairing is a map between Galois modules, and it is easily seen to be equivariant with respect to that action.

Remark. The commutator pairing could easily be degenerate, indeed trivial, as is seen by considering the matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3^2 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3 \end{bmatrix},$$

which generate a $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ in $\mathbf{PGL}_3(\bar{\mathbf{Q}})$.

III.10b. The Weil pairing on an elliptic curve (E, O)

Let (E, O) be an elliptic curve, defined over k, and let n be such that $\mathrm{char}(k) \nmid n$. Then as a group, $E[n](\bar{k}) \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, although as a Galois module the structure can be more complicated. The well-known Weil pairing is usually defined by one of the procedures for computing it, such as the one in [Sil99, III.8]. We will instead work with the description given below in III.10.1, and connect that with the commutator pairing below in III.10.3.

Theorem. *Assume* $\mathrm{char}(k) \nmid n$. *The Weil pairing*

$$\mathrm{e}_n \colon E[n](\bar{k}) \times E[n](\bar{k}) \longrightarrow \boldsymbol{\mu}_n(\bar{k})$$

has the following properties:

- *bilinear*
- *alternating, whence skew-symmetric;*
- *perfect:* $E[n](\bar{k}) \cong \mathrm{Hom}\big(E[n](\bar{k}), \boldsymbol{\mu}_n(\bar{k})\big)$, *whence non-degenerate and surjective;*
- *Galois equivariant;*
- *compatible:* $\mathrm{e}_{mn}(P, Q) = \mathrm{e}_n(mP, Q)$;
- *admits dual isogenies as adjoints:* $\mathrm{e}_n(P, \phi Q) = \mathrm{e}_n(\hat{\phi}P, Q)$.

Proof. All properties except "perfect" are established in [Sil99, III.8.1, III.8.1.1, III.8.2]. As for "perfect", observe that non-degeneracy gives an injection $E[n](\bar{k}) \hookrightarrow \mathrm{Hom}\big(E[n](\bar{k}), \boldsymbol{\mu}_n(\bar{k})\big)$, which must be an isomorphism since the two sets have the same cardinality. □

$E[n](\bar{k})$ admits other pairings with all the properties listed above: simply post-compose the Weil pairing with an automorphism of $\boldsymbol{\mu}_n(\bar{k})$. Among these pairings, it isn't so obvious which of them should be considered the true Weil pairing. For example, the pairing as defined in [SIL99, III.8] is actually the *inverse* of the pairing as described in [MUM70]. The latter agrees with the description of the pairing in terms of function-on-divisor evaluation given in [SIL99, Ex. 3.16], which we now recall.

Theorem III.10.1. *Assume* $\mathrm{char}(k) \nmid n$. *Let* (E, O) *be an elliptic curve, and let* e_n *denote the Weil pairing on* $E[n](\bar{k})$. *Given* $P, Q \in E[n](\bar{k})$, *we may compute* $\mathrm{e}_n(P, Q)$ *as follows. Choose divisors* D_P *and* D_Q *with disjoint support so that* $D_P \sim P - O$ *and* $D_Q \sim Q - O$. *Choose rational functions* f_P *and* f_Q *so that* $(f_P) = nD_P$ *and* $(f_Q) = nD_Q$. *Then*

$$\mathrm{e}_n(P, Q) = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

Proof. See [SIL99, Ex. 3.16]. □

Proposition III.10.2. *Two points* $P, Q \in E[n](\bar{k})$ *are generators for* $E[n](\bar{k})$ *if and only if* $\mathrm{e}_n(P, Q)$ *is a generator for* $\boldsymbol{\mu}_n(\bar{k})$, *i.e., if and only if* $\mathrm{e}_n(P, Q)$ *is a primitive* n*th root of unity.*

Proof. Let the pair (P, Q) generate. Since the Weil pairing is surjective, $\mathrm{e}_n(P, Q)$ is a primitive nth root of unity. Each pair of elements in $E[n](\bar{k})$ can be written in the form $(aP + bQ, cP + dQ)$, with $a, b, c, d \in \mathbf{Z}/n\mathbf{Z}$. Such a pair generates $E[n](\bar{k})$ if and only if there is a group automorphism of $E[n](\bar{k})$ carrying (P, Q) to that pair; in other words, the matrix

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

must lie in $\mathbf{GL}_2(\mathbf{Z}/n\mathbf{Z})$, which is equivalent to the condition: $ad - bc$ is a unit in $\mathbf{Z}/n\mathbf{Z}$. On the other hand, $\mathrm{e}_n(aP + bQ, cP + dQ)$ is easily seen to be $\mathrm{e}_n(P, Q)^{ad-bc}$, which is a primitive nth root of unity under precisely the same condition: $ad - bc$ is a unit in $\mathbf{Z}/n\mathbf{Z}$. □

III.10c. The commutator pairing on J_n is the Weil pairing

We return to the subgroup $J_n \subset \mathbf{PGL}_n(\bar{k})$ and the canonical isomorphism (III.10). Since J_n is abelian, it admits the commutator pairing

$$J_n \times J_n \longrightarrow \bar{k}^\times.$$

If $\mathrm{char}(k) \nmid n$, then $\mathrm{J}_C[n](\bar{k})$ admits the Weil pairing

$$\mathrm{J}_C[n](\bar{k}) \times \mathrm{J}_C[n](\bar{k}) \longrightarrow \boldsymbol{\mu}_n(\bar{k}).$$

We ask: *in light of* (III.10)*, what is the relationship between the two pairings?*

The following theorem is sketched in [O'N01, Thm. 2.5], and appears for the case $k = \mathbf{C}$ in [HUL86]. We give here an elementary proof.

Theorem III.10.3. *Assume* $\mathrm{char}(k) \nmid n$. *Let* C *be a non-degenerate degree* n *curve in* $\mathbf{P}_k^{n-1}$ *of genus* 1. *Then, under the isomorphism* (III.10)*, the commutator pairing on* J_n *corresponds to the* inverse *of the Weil pairing on* $\mathrm{J}_C[n](\bar{k})$.

Remark. If one defines the Weil pairing as done in [SIL99, III.8], then one must eliminate "the inverse of" from the theorem statement. (Cf. discussion preceding III.10.1.

Proof. Let $\bar{P}_0, \ldots, \bar{P}_{n^2-1} \in C(\bar{k})$ be the points of hyperosculation on C. For each $\bar{P}_i$, there exists a hyperplane $\bar{H}_i$ meeting C to order n at $\bar{P}_i$, and an element $\bar{M}_i \in J_n$ whose action on C (given by matrix multiplication) is translation-by-$\bar{P}_i$ on the elliptic curve $(C, \bar{P}_0)$:

$$\bar{M}_i \bar{P}_0 = \bar{P}_i.$$

We wish to compute $\mathrm{e}_n(\bar{M}_i, \bar{M}_j)$. By III.10.1, we need disjoint divisors D_i and D_j linearly equivalent, respectively, to $\bar{P}_i - \bar{P}_0$ and $\bar{P}_j - \bar{P}_0$. We set

$$D_i := \bar{P}_i - \bar{P}_0,$$
$$D_j := (\bar{P}_j \oplus \bar{P}_\ell) - \bar{P}_\ell,$$

where $\oplus$ denotes addition on the elliptic curve $(C, \bar{P}_0)$, and ℓ is such that

$$\bar{P}_\ell \notin \{\, \bar{P}_0, \bar{P}_i, \ominus\bar{P}_j, \bar{P}_i \ominus \bar{P}_j \,\}.$$

This is the precise condition for the divisors to be disjoint, and such ℓ exists because $n \geq 3$.

In what follows, the following notation will be useful: $\bar{P}_{i\oplus j}$ is the point $\bar{P}_i \oplus \bar{P}_j$, $\bar{H}_{i\oplus j}$ is the hyperplane associated to $\bar{P}_{i\oplus j}$, and $\bar{M}_{i\oplus j}$ is the matrix class giving translation-by-$\bar{P}_{i\oplus j}$.

Now we lift everything to row vectors, column vectors, and matrices: choose row vectors H_i representing $\bar{H}_i$, column vectors P_i representing $\bar{P}_i$, and matrices M_i representing $\bar{M}_i$. By $P_{i\oplus j}$, $H_{i\oplus j}$, and $M_{i\oplus j}$ we mean the row vector, column vector, and matrix chosen to represent $\bar{P}_{i\oplus j}$, $\bar{H}_{i\oplus j}$, and $\bar{M}_{i\oplus j}$.

Observe that H_i/H_0 is a function on $C(\bar{k})$ with divisor nD_i, while $H_{j\oplus\ell}/H_\ell$ is a function on $C(\bar{k})$ with divisor nD_j. By III.10.1, we have

$$\mathrm{e}_n(\bar{M}_i, \bar{M}_j) = \frac{(H_i/H_0)(D_j)}{(H_{j\oplus\ell}/H_\ell)(D_i)} = \frac{H_iP_{j\oplus\ell}}{H_iP_\ell}\frac{H_0P_\ell}{H_0P_{j\oplus\ell}}\frac{H_{j\oplus\ell}P_0}{H_{j\oplus\ell}P_i}\frac{H_\ell P_i}{H_\ell P_0}.$$

Since each vector appears once in the numerator and once in the denominator, everything we have done is independent of our choice of lifts. Since $\bar{M}_i$ corresponds to translation-by-$\bar{P}_i$, we see that M_iP_0 represents $\bar{P}_i$, but M_iP_0 need not equal P_i: they differ by a scalar. We can nonetheless apply the substitution $P_i \leftarrow M_iP_0$, so long as we do so simultaneously in the numerator and in the denominator. We can similarly apply $H_i \leftarrow H_0M_i^{-1}$, since $H_0M_i^{-1}$ represents $\bar{H}_i$. Applying these types of substitutions gives us

$$\mathrm{e}_n(\bar{M}_i, \bar{M}_j) = \frac{H_0M_i^{-1}M_{j\oplus\ell}P_0}{H_0M_i^{-1}M_\ell P_0}\frac{H_0M_\ell P_0}{H_0M_{j\oplus\ell}P_0}\frac{H_0M_{j\oplus\ell}^{-1}P_0}{H_0M_{j\oplus\ell}^{-1}M_iP_0}\frac{H_0M_\ell^{-1}M_iP_0}{H_0M_\ell^{-1}P_0}.$$

Since $M_{i\oplus j}$ and M_iM_j each represent $\bar{M}_i\bar{M}_j$, we apply $M_{i\oplus j} \leftarrow M_iM_j$ to obtain

$$\mathrm{e}_n(\bar{M}_i, \bar{M}_j) = \frac{H_0M_i^{-1}M_jM_\ell P_0}{H_0M_i^{-1}M_\ell P_0}\frac{H_0M_\ell P_0}{H_0M_jM_\ell P_0}\frac{H_0M_\ell^{-1}M_j^{-1}P_0}{H_0M_\ell^{-1}M_j^{-1}M_iP_0}\frac{H_0M_\ell^{-1}M_iP_0}{H_0M_\ell^{-1}P_0}.$$

By §III.9, the $[-1]$ automorphism of the elliptic curve $(C, \bar{P}_0)$ lies in $\mathbf{PGL}_n(\bar{k})$. Let T be a matrix representing this automorphism. Then TP_0 and P_0 differ by a scalar, similarly H_0T and H_0 differ by a scalar, and the same can be said for M_iT and TM_i^{-1}. Paying attention that each of the following moves in the numerator is matched by a corresponding move in the denominator, the pesky scalars will never make an appearance. We insert T appropriately, and then walk it to the left one step at a time until it disappears again:

$$\begin{aligned}
&\frac{H_0M_i^{-1}M_jM_\ell P_0}{H_0M_i^{-1}M_\ell P_0}\frac{H_0M_\ell P_0}{H_0M_jM_\ell P_0} = \frac{H_0M_i^{-1}M_jM_\ell TP_0}{H_0M_i^{-1}M_\ell TP_0}\frac{H_0M_\ell TP_0}{H_0M_jM_\ell TP_0}\\
&= \frac{H_0M_i^{-1}M_jTM_\ell^{-1}P_0}{H_0M_i^{-1}TM_\ell^{-1}P_0}\frac{H_0TM_\ell^{-1}P_0}{H_0M_jTM_\ell^{-1}P_0} = \frac{H_0M_i^{-1}TM_j^{-1}M_\ell^{-1}P_0}{H_0M_i^{-1}TM_\ell^{-1}P_0}\frac{H_0TM_\ell^{-1}P_0}{H_0TM_j^{-1}M_\ell^{-1}P_0}\\
&= \frac{H_0TM_iM_j^{-1}M_\ell^{-1}P_0}{H_0TM_iM_\ell^{-1}P_0}\frac{H_0M_\ell^{-1}P_0}{H_0M_j^{-1}M_\ell^{-1}P_0} = \frac{H_0M_iM_j^{-1}M_\ell^{-1}P_0}{H_0M_iM_\ell^{-1}P_0}\frac{H_0M_\ell^{-1}P_0}{H_0M_j^{-1}M_\ell^{-1}P_0}.
\end{aligned}$$

Inserting this equation already leads to some cancellation:

$$\mathrm{e}_n(\bar{M}_i, \bar{M}_j) = \frac{H_0M_iM_j^{-1}M_\ell^{-1}P_0}{H_0M_iM_\ell^{-1}P_0}\frac{H_0M_\ell^{-1}M_j^{-1}P_0}{H_0M_j^{-1}M_\ell^{-1}P_0}\frac{H_0M_\ell^{-1}M_iP_0}{H_0M_\ell^{-1}M_j^{-1}M_iP_0}.$$

Now we would like to swap adjacent pairs of matrices. Although we have not yet shown matrix commutators to be the Weil pairing, those commutators nonetheless are scalars, so we must merely be careful to match each swap above and below.

$$\begin{aligned}\mathrm{e}_n(\bar{M}_i, \bar{M}_j) &= \frac{H_0 M_i M_j^{-1} M_\ell^{-1} P_0}{H_0 M_i M_\ell^{-1} P_0} \frac{H_0 M_j^{-1} M_\ell^{-1} P_0}{H_0 M_j^{-1} M_\ell^{-1} P_0} \frac{H_0 M_\ell^{-1} M_i P_0}{H_0 M_j^{-1} M_\ell^{-1} M_i P_0} \\ &= \frac{H_0 M_i M_j^{-1} M_\ell^{-1} P_0}{H_0 M_i M_\ell^{-1} P_0} \frac{H_0 M_i M_\ell^{-1} P_0}{H_0 M_j^{-1} M_i M_\ell^{-1} P_0} \\ &= [M_i, M_j^{-1}] \frac{H_0 M_j^{-1} M_i M_\ell^{-1} P_0}{H_0 M_j^{-1} M_i M_\ell^{-1} P_0} = [M_i, M_j^{-1}] = [M_i, M_j]^{-1}.\end{aligned}$$

The final equality of commutators holds because the commutator is a scalar. □

III.11. The configuration of hyperplanes fixed by J_n

We return to the subgroup of $\mathbf{PGL}_n(\bar{k})$ that preserves C (see §III.8), especially the subgroup J_n—corresponding to $\mathrm{J}_C[n](\bar{k})$—that preserves C and has no fixpoints on C. The reader may easily verify the following facts about fixpoints and fixed hyperplanes:

- Let $\bar{M} \in \mathbf{PGL}_n(\bar{k})$, and let $M \in \mathbf{GL}_n(\bar{k})$ represent $\bar{M}$. A fixpoint of $\bar{M}$ corresponds to an eigenvector of M.
- $\bar{M}$ fixes a linear subspace of $\mathbf{P}^{n-1}_{\bar{k}}$ pointwise if and only if the corresponding linear subspace of $\mathbf{A}^n_{\bar{k}}$ is an eigenspace of M.
- For a row vector $\bar{\ell}$ of homogeneous coordinates, let $H_\ell := \{\, \bar{P} \in \mathbf{P}^{n-1}_k(\bar{k}) \,:\, \bar{\ell} \cdot \bar{P} = 0 \,\}$ be the corresponding hyperplane. The action of $\mathbf{PGL}_n(\bar{k})$ on points is $\bar{P} \mapsto \bar{M}\bar{P}$, but its action on hyperplanes is $\bar{\ell} \mapsto \bar{\ell}\bar{M}^{-1}$:
$$\bar{M} H_\ell = \{\, \bar{M}\bar{P} \,:\, \bar{\ell} \cdot \bar{P} = 0 \,\} = \{\, \bar{P} \,:\, \bar{\ell}\bar{M}^{-1}\bar{P} = 0 \,\} = H_{\ell \bar{M}^{-1}}.$$
- $\bar{M}$ fixes a hyperplane H_ℓ if and only if ℓ is an eigenvector of M^{t}.

Concerning the structure of things related to J_n, there are often three cases to consider:

- $\#J_n = n^2$, which happens if and only if $\mathrm{char}(k) \nmid n$, in which case we have $J_n \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ (as $\mathbf{Z}$-modules);
- $\#J_n = n^2/p^e$ where $p = \mathrm{char}(k)$ and $p^e \mid n$ but $p^{e+1} \nmid n$, which can happen when $\mathrm{char}(k) \mid n$, in which case we have $J_n \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/(n/p^e)\mathbf{Z}$ (as $\mathbf{Z}$-modules);
- $\#J_n = n^2/p^{2e}$, which is the other possibility when $\mathrm{char}(k) \mid n$, in which case we have $J_n \cong \mathbf{Z}/(n/p^e)\mathbf{Z} \times \mathbf{Z}/(n/p^e)\mathbf{Z}$ (as $\mathbf{Z}$-modules).

As we will see, we can often make a general statement—without restricting to a particular case above—in terms of an element of J_n of order n. Implicitly, of course, such a statement applies only to the first two cases given above.

Proposition III.11.1. *Let $\bar{M} \in \mathbf{PGL}_n(\bar{k})$ be an element that preserves C. For each hyperplane H fixed by $\bar{M}$, the corresponding hyperplane section $H \cap C$ is a union of orbits under the action of $\bar{M}$ on C.*

Proof. Obvious. □

Corollary III.11.2. *Let $\bar{M} \in J_n$ have order n. Then each hyperplane H fixed by $\bar{M}$ meets C transversally: $H \cap C$ comprises n distinct points.*

Proof. Each orbit of $\bar{M}$ on C comprises n distinct points. On the other hand, $H \cap C$ comprises at most n points. Now apply the proposition. □

Proposition III.11.3. *Assume that n is odd. Let $\bar{M} \in J_n$ have order n. The orbit of $Q \in C(\bar{k})$ is a hyperplane section if and only if Q is a point of hyperosculation.*

Proof. Fix a point of hyperosculation $O \in C(\bar{k})$ to obtain a group law. Then points of n-torsion coincide with points of hyperosculation. The orbit of Q is a hyperplane section if and only if $Q+\bar{M}Q+\bar{M}^2Q+\ldots+\bar{M}^{n-1}Q \sim nO$. But $\bar{M}$ is just translation-by-P for some point of hyperosculation P. Thus the condition is $Q+(Q\oplus P)+(Q\oplus[2]P)+\ldots+(Q\oplus[n-1]P)\sim nO$, which is equivalent to $[n]Q\oplus[n(n-1)/2]P=O$, which reduces to: Q is a point of hyperosculation. □

To obtain a version of the proposition for n even, we need the notion of a dyadic packet. By the isomorphism $C/\mathrm{J}_C[n]\cong \mathrm{J}_C$ from II.2.4, the n-torsion packets on C correspond to the $\bar{k}$-valued points on J_C, and the hyperosculation packet on C corresponds to the origin on J_C. We will call an n-torsion packet on C **dyadic** if it corresponds to a point of 2-torsion on J_C.

Proposition III.11.4. *Fix a point of hyperosculation $O \in C(\bar{k})$ to obtain a group law on $C_{\bar{k}}$. The multiplication-by-n map $C \longrightarrow C$ gives a one-to-one correspondence between the dyadic packets and the* 2*-torsion on $(C_{\bar{k}}, O)$. Thus the dyadic packets* partition *the $(2n)$-torsion on $(C_{\bar{k}}, O)$; furthermore, this partition is independent of the choice of O.*

Proof. It is easy to check that the group law on J_C is induced by the group law on $(C_{\bar{k}}, O)$, where O is any choice of point of hyperosculation. The preimages under multiplication-by-n of the 2-torsion on $(C_{\bar{k}}, O)$ are easily seen to be n-torsion packets, with the property that multiplying them by 2 sends them into the hyperosculation packet; in short, they are the 2-torsion on the quotient J_C. □

Proposition III.11.5. *Assume that n is even. Let $\bar{M} \in J_n$ have order n. Let a point of hyperosculation $O \in C(\bar{k})$ define a group law, so that $\bar{M}$ corresponds to translation-by-P, whence $\bar{M}^{n/2}$ is translation by $[n/2]P$, which is a point of order* 2 *on $(C_{\bar{k}}, O)$. Then the orbit of $Q \in C(\bar{k})$ is a hyperplane section if and only if $[n]Q = [n/2]P$, i.e., if and only if Q lies in the dyadic packet corresponding to $[n/2]P$.*

Proof. By the proof of III.11.3, the orbit of Q is a hyperplane section if and only if $[n]Q\oplus[n(n-1)/2]P=O$, which reduces to: $[n]Q=[n/2]P$. □

Combining III.11.3 and III.11.5, we obtain: *if $\bar{M} \in J_n$ has order n, then the orbit of $Q \in C(\bar{k})$ is a hyperplane section if and only if Q lies in a certain n-torsion packet that depends only on $\bar{M}$.* From this we obtain the following result.

Corollary III.11.6. *Let $\bar{M} \in J_n$ have order n, and let $M \in \mathbf{GL}_n(\bar{k})$ represent $\bar{M}$.*

- *Each eigenvalue of M has a* 1*-dimensional eigenspace.*
- *M has $\#J_n/n$ distinct eigenvalues.*

Proof. There are only finitely many points in an n-torsion packet, so there can be only finitely many hyperplanes fixed by $\bar{M}$. If an eigenspace of M were 2-dimensional or larger, then there would be infinitely many hyperplanes fixed by $\bar{M}$.

The n-torsion packet has cardinality $\#J_n$. That set is partitioned into collections of size n by the hyperplanes fixed by $\bar{M}$. The fixed hyperplanes correspond to the eigenspaces of M, which in turn correspond to the eigenvalues. □

Corollary III.11.7. *Let $\bar{M} \in J_n$ have order n, and let $M \in \mathbf{GL}_n(\bar{k})$ represent $\bar{M}$.*

- *If $\mathrm{char}(k) \nmid n$ (i.e., $\#J_n = n^2$), then M has n distinct eigenvalues, whence there are precisely n distinct fixpoints of $\bar{M}$ (not on C), and precisely n distinct fixed hyperplanes. The fixed hyperplanes intersect C in the n^2 points of either the hyperosculation packet (when n is odd) or a non-hyperosculation dyadic packet (when n is even).*
- *If $\mathrm{char}(k) \mid n$ (i.e., $\#J_n = n^2/p^e$ where $p = \mathrm{char}(k)$ and $p^e \mid n$ but $p^{e+1} \nmid n$), then M has n/p^e unique eigenvalues, whence there are precisely n/p^e distinct fixpoints of $\bar{M}$ (not on C), and precisely n/p^e distinct fixed hyperplanes. The fixed hyperplanes intersect C in the n/p^e points of either the hyperosculation packet (when n is odd) or a non-hyperosculation dyadic packet (when n is even).*

- *Special case: if $n = p$ is prime and* $\mathrm{char}(k) = p$ *(i.e., $\#J_n = p$), then M has a unique eigenvalue (algebraic multiplicity n, but geometric multiplicity 1), thus a unique fixpoint (not on C), and a unique fixed hyperplane. The fixed hyperplane intersects C in the p points of either the hyperosculation packet (when p is odd) or the unique non-hyperosculation dyadic packet (when $p = 2$).*

Remark III.11.8. When n is odd, this gives an easy procedure to find the points of hyperosculation on C: find an element of $\mathbf{PGL}_n(\bar{k})$ that preserves C, has no fixpoints, and has order n; next, find its fixed hyperplane(s); finally, compute their intersection with C. (When $\mathrm{char}(k) \mid n$ and furthermore $\#J_n = n^2/p^{2e}$ where $p = \mathrm{char}(k)$ and $p^e \mid n$ but $p^{e+1} \nmid n$, then this procedure can't be used. Instead, one can follow the procedure in §III.9a.)

III.11a. Hyperplane configurations when $\mathrm{char}(k) \nmid n$

For the rest of this section, we will assume $\mathrm{char}(k) \nmid n$, whence $J_n \cong \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ (as $\mathbf{Z}$-modules). Our goal is to describe the configuration of hyperplanes fixed by generators for J_n.

We already know, by III.11.6, that (a representative for) $\bar{M} \in J_n$ of order n has distinct eigenvalues. Now we can say a bit more.

Proposition III.11.9. *Assume* $\mathrm{char}(k) \nmid n$. *Let $\bar{M} \in J_n$ be an element of order n, and let $M \in \mathbf{GL}_n(\bar{k})$ be any matrix representating $\bar{M}$. If $\lambda \in \bar{k}^\times$ is an eigenvalue of M, then also $\zeta\lambda$ is an eigenvalue of M for each $\zeta \in \boldsymbol{\mu}_n(\bar{k})$. In other words, M has distinct eigenvalues, and they compose a coset of $\boldsymbol{\mu}_n(\bar{k})$ inside $\bar{k}^\times$.*

Proof. Since $\bar{M}$ has order n, there exists $\bar{N} \in J_n$ so that $\bar{M}$ and $\bar{N}$ are generators. Let N be any lift of $\bar{N}$ to $\mathbf{GL}_n(\bar{k})$. By III.10.2 and III.10.3, $MNM^{-1}N^{-1}$ is a primitive nth root of unity, which we'll call ζ_n. Now let $\lambda \in \bar{k}^\times$ be an eigenvalue of M, and let x be a corresponding eigenvector. Then

$$Mx = \lambda x, \quad \text{and} \quad M(Nx) = MNx = \zeta_n NMx = \zeta_n \lambda Nx = (\zeta_n\lambda)(Nx),$$

so $\zeta_n\lambda$ is an eigenvalue of M (with corresponding eigenvector Nx). □

Proposition III.11.10. *Assume* $\mathrm{char}(k) \nmid n$. *Let $\bar{M}, \bar{N} \in J_n$ be generators. Then $\bar{M}$ cyclically permutes the hyperplane sections preserved by $\bar{N}$, and vice versa.*

Proof. In the proof of III.11.9, we saw that if x is an eigenvector of M, also Nx is an eigenvector of M. Thus $\bar{N}$ cyclically permutes the fixpoints of $\bar{M}$, whence also $\bar{N}$ cyclically permutes the hyperplanes preserved by $\bar{M}$. □

Theorem III.11.11. *Assume* $\mathrm{char}(k) \nmid n$. *Further assume that n is odd. If $\bar{M}, \bar{N}$ generate J_n, then there is a one-to-one correspondence*

$$\left\{\begin{matrix}\textit{hyperplane sections}\\ \textit{preserved by } \bar{M}\end{matrix}\right\} \times \left\{\begin{matrix}\textit{hyperplane sections}\\ \textit{preserved by } \bar{N}\end{matrix}\right\} \longleftrightarrow \{\, \textit{points of hyperosculation}\,\}$$
$$(H, H') \longmapsto H \cap H',$$

which is equivariant with respect to the action of J_n; thus, if we fix a point of hyperosculation as origin to obtain a group law, this correspondence is an isomorphism of J_n-modules.

Proof. Obvious from the preceding material. □

Instead of intersecting hyperplane sections to obtain points in $C(\bar{k})$, we could instead intersect the actual hyperplanes to obtain points in a Grassmannian. When n is even, the hyperplanes fixed by M cover a non-hyperosculation dyadic packet on C, while the hyperplanes fixed by N cover a *different* non-hyperosculation dyadic packet on C. There is again an intersection pairing taking values in a Grassmannian, but not one taking values in $C(\bar{k})$. (In other words, when n is even, the $(n-3)$-dimensional linear space obtained by intersecting a hyperplane fixed by M with a hyperplane fixed by N does not meet C.)

III.12. Lifting $J_n \subset \mathbf{PGL}_n(\bar{k})$ to $H_n \subset \mathbf{GL}_n(\bar{k})$

We now consider the problem of lifting the subgroup $J_n \subset \mathbf{PGL}_n(\bar{k})$, which corresponds to $\mathrm{J}_C[n](\bar{k})$, from $\mathbf{PGL}_n(\bar{k})$ to $\mathbf{GL}_n(\bar{k})$. In other words, we seek a *finite* subgroup $H_n \subset \mathbf{GL}_n(\bar{k})$ so that, under the canonical projection $\mathbf{GL}_n \to \mathbf{PGL}_n$, the image of H_n is J_n. We furthermore require H_n to be a $\mathrm{Gal}(\bar{k}/k)$-module.

Of course we would like H_n to be as small as possible; in fact, we would be delighted if H_n could be isomorphic, as a Galois module, to J_n. Unfortunately, as we will see below, this is too much to ask in general.

Remark. One reason for wanting H_n to be $\mathrm{Gal}(\bar{k}/k)$-stable is that it may then be viewed as the set of $\bar{k}$-valued points of a finite group scheme defined over k. This will be relevant in chapter IV, where we will be interested in computing a quotient by J_n, which we will express in terms of invariants of H_n. This also explains why we would like H_n to be as small as possible: the computational expense for finding the elements of H_n and then working out its invariant theory is likely to increase with the size of H_n.

We always have available the following canonical lift: we define H_n by taking the preimage of J_n under the canonical projection $\mathbf{SL}_n \to \mathbf{PGL}_n$:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \boldsymbol{\mu}_n(\bar{k}) & \longrightarrow & \mathbf{SL}_n(\bar{k}) & \longrightarrow & \mathbf{PGL}_n(\bar{k}) & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & \boldsymbol{\mu}_n(\bar{k}) & \longrightarrow & H_n & \longrightarrow & J_n & \longrightarrow & 1 \end{array}$$

In other words:

$$H_n := \left\{ A \in \mathbf{GL}_n(\bar{k}) \,:\, \bar{A} \in J_n \text{ and } \det(A) = 1 \right\}.$$

Note $\#H_n = \#\boldsymbol{\mu}_n(\bar{k}) \cdot \#J_n$. (Thus, when $\mathrm{char}(k) \nmid n$, we have $\#H_n = n^3$.) Since the determinant 1 condition is preserved when matrices are moved by elements of $\mathrm{Gal}(\bar{k}/k)$, the canonical lift H_n is $\mathrm{Gal}(\bar{k}/k)$-stable. We will see below that H_n is always a central extension of J_n by $\boldsymbol{\mu}_n(\bar{k})$.

III.12a. Case: $\mathrm{char}(k) \nmid n$ (i.e., $\#J_n = n^2$)

We saw that taking commutators of arbitrary lifts of elements in J_n corresponds to the Weil pairing (see III.10.3). Since the Weil pairing is surjective, any lift of J_n to $\mathbf{GL}_n(\bar{k})$ must contain the constant matrices $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$. Therefore, any lift of J_n has cardinality $\geq n^3$, while the canonical lift H_n has cardinality $= n^3$.

Now that we know lifts of order n^3 exist, we can classify them all. Let H_n' be a fixed but unknown lift of J_n to $\mathbf{GL}_n(\bar{k})$ of order n^3. For $\bar{M} \in J_n$, let $M \in H_n$ and $M' \in H_n'$ denote a choice of representatives for $\bar{M}$. Since both H_n and H_n' admit only elements of $\boldsymbol{\mu}_n(\bar{k})$ as scalar matrices, we have $(M')^n = \alpha M^n$ for some $\alpha \in \boldsymbol{\mu}_n(\bar{k})$, and α is independent of our choices. Thus we obtain a well-defined homomorphism

$$\begin{aligned} \phi\colon J_n &\longrightarrow \boldsymbol{\mu}_n(\bar{k}) \\ \bar{M} &\longmapsto (M')^n M^{-n} \end{aligned}$$

On the other hand, if $\phi \in \mathrm{Hom}\big(J_n, \boldsymbol{\mu}_n(\bar{k})\big)$, then we can define a lift H_n' as follows: take generators $\bar{M}, \bar{N}$ for J_n, choose representatives $M, N \in H_n$, set $M' = \sqrt[n]{\phi(\bar{M})}M$ and $N' = \sqrt[n]{\phi(\bar{N})}N$ for some choice of nth roots, and let H_n' be the group of order n^3 generated by M', N'. It is easy to check that we have established a one-to-one correspondence between $\mathrm{Hom}\big(J_n, \boldsymbol{\mu}_n(\bar{k})\big)$ and lifts of J_n to $\mathbf{GL}_n(\bar{k})$ of order n^3; in fact, the correspondence respects the Galois action, in the following sense: if ϕ is the homomorphism associated to H_n', then ϕ^σ is the homomorphism associated to $(H_n')^\sigma$. Thus the lifts that are Galois stable correspond to the elements of $\mathrm{Hom}\big(J_n, \boldsymbol{\mu}_n(\bar{k})\big)$ that are Galois invariant. The canonical lift H_n corresponds to the trivial homomorphism.

Proposition. *Assume* $\mathrm{char}(k) \nmid n$. *There exist precisely* n^2 *lifts of* J_n *to* $\mathbf{GL}_n(\bar{k})$ *of order* n^3.

Proof. The cardinality of $\mathrm{Hom}\big(J_n, \boldsymbol{\mu}_n(\bar{k})\big)$ is n^2. □

If we fix generators $\bar{M}, \bar{N}$ for J_n, and a generator ζ_n for $\boldsymbol{\mu}_n(\bar{k})$, and choose representatives $M', N' \in H'_n$, then each element of H'_n has a unique expression in the form

$$\zeta_n^a (M')^b (N')^c, \quad \text{where } a, b, c \in \mathbf{Z}/n\mathbf{Z}. \tag{III.11}$$

Proposition. *Assume* $\mathrm{char}(k) \nmid n$. *Each of the lifts* H'_n *is a central extension of* J_n *by* $\boldsymbol{\mu}_n(\bar{k})$.

Proof. Using commutators, we can express a product of elements in the form (III.11) in the same form. It is easy to check that an element lies in the center if and only if $b \equiv c \equiv 0 \pmod{n}$. □

III.12b. Case: $\mathrm{char}(k) \mid n$ and $\#J_n = n^2/p^e$

Let $p := \mathrm{char}(k)$, and define e by $p^e \mid n$ but $p^{e+1} \nmid n$. Since $\#\boldsymbol{\mu}_n(\bar{k}) = n/p^e$, the canonical lift H_n has order n^3/p^{2e}. If $M, N \in H_n$ are such that $\bar{M}, \bar{N}$ generate J_n, and furthermore $\bar{M}$ has order n while $\bar{N}$ has order n/p^e, then each element of H_n has a unique expression in the form $\zeta_{n/p^e}^a M^b N^c$ with $a \in \mathbf{Z}/(n/p^e)\mathbf{Z}$, $b \in \mathbf{Z}/n\mathbf{Z}$, and $c \in \mathbf{Z}/(n/p^e)\mathbf{Z}$. We see easily that H_n is a central extension of J_n by $\boldsymbol{\mu}_n(\bar{k})$.

III.12c. Case: $\mathrm{char}(k) \mid n$ and $\#J_n = n^2/p^{2e}$

Set p and e as in §III.12b. The canonical lift H_n has order n^3/p^{3e}. If $M, N \in H_n$ are such that $\bar{M}, \bar{N}$ generate J_n, then each element of H_n has a unique expression in the form $\zeta_{n/p^e}^a M^b N^c$ with $a, b, c \in \mathbf{Z}/(n/p^e)\mathbf{Z}$. We again see easily that H_n is a central extension of J_n by $\boldsymbol{\mu}_n(\bar{k})$.

III.13. Schrödinger-like representations of H_n when $\mathrm{char}(k) \nmid n$

Assume $\mathrm{char}(k) \nmid n$. We show in this section that there exist nice matrix representations over $\bar{k}$ of both the canonical lift $H_n \subset \mathbf{SL}_n(\bar{k})$ and the non-canonical lifts $H'_n \subset \mathbf{GL}_n(\bar{k})$ of $J_n \subset \mathbf{PGL}_n(\bar{k})$, which were introduced in §III.12. We will see that the classical Schrödinger representation occurs for H_n when n is odd, while it occurs for one of the H'_n when n is even.

We first consider the canonical lift H_n. Fix choices $\bar{M}, \bar{N} \in J_n$ and $M, N \in H_n$ as in the discussion in §III.12a. We saw in III.11.9 that the eigenvalues of M, N are each a coset of $\boldsymbol{\mu}_n(\bar{k})$ inside $\bar{k}^\times$. By the definition of H_n, the product of the eigenvalues is 1. Therefore, when n is odd, both M and N have eigenvalues

$$\{\, 1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1} \,\},$$

while when n is even, both M and N have eigenvalues

$$\{\, \zeta_{2n}, \zeta_{2n}^3, \zeta_{2n}^5, \ldots, \zeta_{2n}^{2n-1} \,\}.$$

Over $\bar{k}$, we can choose an eigenvector x for M corresponding to the first eigenvalue, and then use the basis $\{\, x, Nx, N^2x, \ldots, N^{n-1}x \,\}$ of eigenvectors for M (cf. proof of III.11.9) to obtain a new coordinate system for $\mathbf{P}_{\bar{k}}^{n-1}$. (Even though, when n is odd, x itself can be chosen to be defined over k, the remaining eigenvectors need not be defined over k.) For n odd, H_n will then have the **classical Schrödinger representation**

$$M = \begin{bmatrix} 1 & & & & \\ & \zeta_n & & & \\ & & \zeta_n^2 & & \\ & & & \ddots & \\ & & & & \zeta_n^{n-1} \end{bmatrix}, \quad N = \begin{bmatrix} & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \\ 1 & & & & \end{bmatrix},$$

while for n even we obtain

$$M = \begin{bmatrix} \zeta_{2n} & & & \\ & \zeta_{2n}^3 & & \\ & & \ddots & \\ & & & \zeta_{2n}^{2n-1} \end{bmatrix}, \quad N = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ -1 & & & \end{bmatrix}.$$

We now consider one of the lifts $H_n' \subset \mathbf{GL}_n(\bar{k})$. For generators $M', N' \in H_n'$, if we define $\alpha, \beta \in \boldsymbol{\mu}_n(\bar{k})$ by $(M')^n = \alpha M^n$ and $(N')^n = \beta N^n$ (cf. §III.12a), then in terms of the same basis used just now above, for n odd we obtain

$$M' = \begin{bmatrix} \sqrt[n]{\alpha} & & & \\ & \sqrt[n]{\alpha}\zeta_n & & \\ & & \ddots & \\ & & & \sqrt[n]{\alpha}\zeta_n^{n-1} \end{bmatrix}, \quad N' = \begin{bmatrix} & \sqrt[n]{\beta} & & \\ & & \ddots & \\ & & & \sqrt[n]{\beta} \\ \sqrt[n]{\beta} & & & \end{bmatrix},$$

while for n even we obtain

$$M' = \begin{bmatrix} \sqrt[n]{\alpha}\zeta_{2n} & & & \\ & \sqrt[n]{\alpha}\zeta_{2n}^3 & & \\ & & \ddots & \\ & & & \sqrt[n]{\alpha}\zeta_{2n}^{2n-1} \end{bmatrix}, \quad N' = \begin{bmatrix} & \sqrt[n]{\beta} & & \\ & & \ddots & \\ & & & \sqrt[n]{\beta} \\ -\sqrt[n]{\beta} & & & \end{bmatrix}.$$

We could instead scale the basis so that it is $\{ x, N'x, \ldots, (N')^{n-1}x \}$. Then $(N')^n x$ is either βx (when n is odd) or $-\beta x$ (when n is even), so for n odd we obtain

$$M' = \begin{bmatrix} \sqrt[n]{\alpha} & & & \\ & \sqrt[n]{\alpha}\zeta_n & & \\ & & \ddots & \\ & & & \sqrt[n]{\alpha}\zeta_n^{n-1} \end{bmatrix}, \quad N' = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \beta & & & \end{bmatrix},$$

while for n even we obtain

$$M' = \begin{bmatrix} \sqrt[n]{\alpha}\zeta_{2n} & & & \\ & \sqrt[n]{\alpha}\zeta_{2n}^3 & & \\ & & \ddots & \\ & & & \sqrt[n]{\alpha}\zeta_{2n}^{2n-1} \end{bmatrix}, \quad N' = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ -\beta & & & \end{bmatrix}.$$

Thus, when n is even, we obtain the classical Schrödinger representation for the particular H_n' corresponding to $(\alpha, \beta) = (-1, -1)$.

Our use of a pair $\alpha, \beta \in \boldsymbol{\mu}_n(\bar{k})$ to "measure" how a lift H_n' deviates from H_n required us to then separately treat the cases n odd and n even in looking at Schrödinger-like representations. We can treat all values of n simultaneously by instead working with a pair $\alpha', \beta' \in \boldsymbol{\mu}_n(\bar{k})$ that measures how far we deviate from the classical Schrödinger representation.

Theorem III.13.1. *Assume* $\mathrm{char}(k) \nmid n$. *Let* $\alpha', \beta' \in \boldsymbol{\mu}_n(\bar{k})$. *Over* $\bar{k}$, *there always exists a coordinate system so that the matrix group of order* n^3 *generated by*

$$\begin{bmatrix} \sqrt[n]{\alpha'} & & & \\ & \sqrt[n]{\alpha'}\zeta_n & & \\ & & \ddots & \\ & & & \sqrt[n]{\alpha'}\zeta_n^{n-1} \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ \beta' & & & \end{bmatrix}$$

represents one of the lifts H_n'. *The classical Schrödinger representation occurs when* $(\alpha', \beta') = (1, 1)$. *For* n *odd, it has determinant* 1 *throughout and thus represents the canonical lift* H_n; *for* n *even, it has determinant* ± 1 *throughout and thus does* not *represent* H_n.

III.14. Concerning the Galois module structure of $\mathrm{J}_C[n]$

Theorem III.14.1. *Assume* $\mathrm{char}(k) \nmid n$. *If there exists a change-of-coordinates, defined over* k, *in which the canonical lift* H_n *has a Schrödinger-like representation (cf. §III.13), then there exists an isomorphism* $\mathrm{J}_C[n] \cong \boldsymbol{\mu}_n \times \mathbf{Z}/n\mathbf{Z}$.

Proof. The change-of-coordinates does not affect the abstract Galois module structure, so let H_n be the matrix group of order n^3 generated by the two Schrödinger-like matrices M and N, as in §III.13. (Thus, if n is odd, the diagonal entries of M are $1, \zeta_{2n}^2, \zeta_{2n}^4, \ldots$, while if n is even, the diagonal entries of M are $\zeta_{2n}, \zeta_{2n}^3, \zeta_{2n}^5, \ldots$.) Each element of H_n has a unique expression in the form $\zeta_n^a M^b N^c$ with $a, b, c \in \mathbf{Z}/n\mathbf{Z}$, and each element of $\mathrm{J}_C[n](\bar{k}) \cong J_n$ has a unique expression in the form $\bar{M}^b \bar{N}^c$.

We can write down an isomorphism $J_n \to \boldsymbol{\mu}_n \times \mathbf{Z}/n\mathbf{Z}$ on $\bar{k}$-valued points as follows: $\bar{M}^b \bar{N}^c \mapsto (\zeta_{2n}^{2b}, c)$. We already know this to be an isomorphism of groups; as for Galois modules, we need worry only about the first coordinate. The result follows easily from the observation that ζ_{2n}^{2b} is always the same as the ratio of the first two diagonal entries of M^b. □

CHAPTER IV

An algorithm for the jacobian

Let k be a perfect field. As we saw in chapter III, every curve C of genus 1, defined over k, occurs as a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1. In this chapter, under the assumption $\mathrm{char}(k) \nmid n$ (regarding this, see §I.2e), we describe how to find equations for the jacobian J_C of C.

IV.1. An algorithm for the jacobian

Theorem IV.1.1. *There exists an algorithm (described in this chapter) that takes as input a finite set of homogeneous equations; the algorithm checks whether the input defines a non-degenerate degree n curve in $\mathbf{P}_k^{n-1}$ of genus 1, where $n-1$ is the number of variables and n is coprime to $\mathrm{char}(k)$; if not, the algorithm terminates with an error; otherwise, it produces as output:*

- *coordinates of the n^2 points of hyperosculation on C;*
- *equations describing the jacobian J_C;*
- *coordinates of the k-rational origin on J_C;*
- *polynomials describing the map $j_{\mathcal{D}}\colon C \to \mathrm{J}_C$ of degree n^2 that carries $P \mapsto [nP] - \mathcal{D}$, where $\mathcal{D}$ is the divisor class of hyperplane sections on C.*

Proof. The rest of this chapter is the proof. □

Remarks. (1) To do all of this on a computer, we must of course have an encoding for elements of k and have algorithms for the field operations. In other words, k must be a *computable field* (cf. [BW93, §4.6]). In this chapter, we will not concern ourselves with such implementation-level details.

(2) More generally, we could take as input a finite set of homogeneous or inhomogeneous equations, not requiring them to define a non-degenerate degree n (smooth) curve in $\mathbf{P}_k^{n-1}$ or $\mathbf{A}_k^{n-1}$ of genus 1, and it is clear in principle that we would then need to do the following (but it is unclear how practical some of the steps are): we homogenize the equations and check that they define a variety of dimension is 1; then we blow up all the singularities to obtain a smooth curve of some degree n embedded in $\mathbf{P}_k^m$ for some m; we check that the genus is 1 and that n is coprime to $\mathrm{char}(k)$; then we intersect with a k-rational hyperplane to obtain a k-rational divisor D of degree n, then compute the map to projective space (cf. §II.4) determined by $\mathcal{O}(D)$. If $n = 2$, this map gives us a double cover of $\mathbf{P}_k^1$, and we apply the formulas from [Wei54] (also in [AKM+01]) to output everything stated in the theorem (the 4 points of hyperosculation correspond to the 4 points of ramification of the double cover, and these are easily determined). If $n \geq 3$, the map to projective space gives us a new set of equations that meet the conditions of the theorem, and so we proceed with the algorithm described in this chapter.

IV.2. Vetting the input

The input to the algorithm is a finite set of homogeneous equations in a finite number of variables. There exist algorithms (see, e.g., [BS92]) for determining the dimension, genus, and degree of the scheme defined by the equations, as well as algorithms for determining whether a variety is smooth

(by determining the dimension of the singular locus), and they are implemented in *Macaulay 2* [GS] (cf. the code in table V.1).

If the dimension is $\neq 1$, then the algorithm terminates with the message "input does not define a curve".

If the genus is $\neq 1$, then the algorithm terminates with the message "input curve does not have genus 1".

If $\mathrm{char}(k) \mid n$, where n is the degree, then the algorithm terminates with the message "degree of input curve is divisible by ground field characteristic".

If the number of variables in the input equations is $\neq n-1$, then the algorithm terminates with the message "input curve is not of degree one higher than dimension of ambient projective space".

If one of the input equations is linear, then the algorithm terminates with the message "input curve is degenerate (it lies in a hyperplane)".

If the curve has a non-empty singular locus, then the algorithm terminates with the message "input curve is singular".

IV.3. Describing all matrices that preserve the curve

Let I be the ideal generated by the input equations. Our curve is

$$C = \mathrm{Proj}\,\frac{k[x_0,\ldots,x_{n-1}]}{I},$$

but note that I may not be *the* ideal of the curve because I might not be saturated. (There exists algorithms for computing the saturation. We do not care whether I is saturated.) Let $\mathfrak{G}$ be a Gröbner basis for I with respect to some arbitrary (but fixed) monomial order on $k[x_0,\ldots,x_{n-1}]$.

Let A be an $n \times n$ matrix of variables a_{ij}. If $\mathbf{x} = [x_0 : \ldots : x_{n-1}]$ is a $\bar{k}$-valued point of $\mathbf{P}^{n-1}_k$ that lies on C, then $A\mathbf{x}$ may or may not lie on C. The condition for A to preserve C is that, for each $f(\mathbf{x}) \in I$, where $\mathbf{x}$ is now a tuple of variables, also $f(A\mathbf{x}) \in I$. It is sufficient for this condition to hold on a set of generators for I. The ideal membership problem $f(A\mathbf{x}) \in I$ is solved computationally using the Gröbner basis: we have $f(A\mathbf{x}) \in I$ if and only if $f(A\mathbf{x})$ reduces to 0 upon division by $\mathfrak{G}$.

We proceed as follows: For each of the original generators $f(\mathbf{x})$ of I given to us as part of the input, we divide $f(A\mathbf{x})$ by $\mathfrak{G}$ and, viewing the remainder as a polynomial in $k(a_{ij})[\mathbf{x}]$, set each remainder coefficient equal to 0. This process results in a system of equations in the a_{ij} whose solutions correspond to the matrices A that preserve C.

IV.4. Finding $H_n \rtimes \{\pm 1\}$

To the system of equations in the a_{ij} obtained in the last step, add in the additional equation $\det(A) = 1$. At this point, the equations define a 0-dimensional ideal. (The number of solutions will depend on the number of elliptic curve automorphisms the input curve admits over $\bar{k}$. When the j-invariant of C is neither 0 nor 1728, then there will be $2n^3$ solutions.) The elements of H_n are then characterized as those solutions that act fixpoint-free on the curve (cf. §III.8). The various $[-1]$ automorphisms (cf. §III.9) are characterized as those solutions that do have a fixpoint and have order 2 (modulo scalars).

IV.4a. Solving over a field extension

The 0-dimensional system defining the finitely many matrices must now be solved. There exist various techniques for this (cf. [CLO98, Ch. 2]). The simplest is elimination and extension. Slightly fancier is to obtain a Gröbner basis with respect to a favorite monomial order, and then use a *Gröbner basis conversion* procedure (cf. [CLO98, §2.3]) to land in the elimination/extension situation.

At any rate, a tedious but finite process will construct a normal field extension $k(\theta)/k$ and all the solution matrices, with all the entries expressed in terms of θ.

Once the solutions are in hand, we must identify H_n, and when n is even, we must also identify the $[-1]$ automorphisms (we'll need them to find the points of hyperosculation). Since fixpoints

correspond to eigenvectors, we can use linear algebra to determine the fixpoints of each matrix, and the equations for C tell us whether any of the fixpoints lie on C.

For H_n, we hold on to the matrices that have no fixpoints, while for the $[-1]$ automorphisms, we hold on to the matrices of order 2 (modulo scalars) and have a fixpoint. (In fact, by III.9.3, if we find one such matrix T, then they all have the form MT, where $M \in H_n$.)

Finally, by expanding all possible products of elements of H_n, we can find generators for H_n. In fact, since $\mathrm{char}(k) \nmid n$, we will find two generators whose commutator is a primitive nth root of unity (cf. §III.12).

IV.4b. Practical improvements for finding H_n

Since $\mathrm{char}(k) \nmid n$, the group H_n is characterized by the following properties: it admits a pair of matrices that act fixpoint-free on the curve and whose commutator is a primitive nth root of unity. Furthermore, each of the two generators admits n distinct fixpoints (not lying on the curve).

Thus, instead of solving for *all* matrices that preserve the curve, we need only solve for potentital generators of H_n. We can apply the following result to reduce the number of solutions, and then simply search for a pair of solutions whose commutator is a primitive nth root of unity, and which have no fixpoints on C.

Proposition IV.4.1. *Assume* $\mathrm{char}(k) \nmid n$. *If n is odd, and if $M \in H_n$ is such that $\bar{M} \in J_n$ has order n, then $M^n = 1$. If n is even, we instead have $M^n = -1$.*

Proof. As we saw in III.11.9, the eigenvalues of M are $\{\, \alpha, \alpha\zeta_n, \ldots, \alpha\zeta_n^{n-1} \,\}$, for some $\alpha \in \bar{k}^\times$. Thus, both the minimum and characteristic polynomials of M are $\prod_{0 \le i \le n-1}(X - \alpha\zeta_n^i) = X + (-1)^n \alpha^n \prod_i \zeta_n^i$. But the determinant is 1. Thus, for n odd, M satisfies $X^n - 1$, while for n even, M satisfies $X^n + 1$. □

Remark. In fact, when n is odd, H_n may be characterized as $\{\, A \in \mathbf{GL}_n(\bar{k}) \,:\, \bar{A} \in J_n \text{ and } A^n = 1 \,\}$. However, when n is even, we know of no such characterization.

Therefore, when n is odd, if one introduces the condition $M^n = 1$, one could leave off the $\det = 1$ condition; however, it is unclear how—or even whether—the running time is affected by doing so (cf. V.2.1).

IV.4c. Practical improvements for finding the $[-1]$ automorphisms

When n is even, we will need matrices corresponding to the $[-1]$ automorphisms to find the points of hyperosculation on C.

When n is odd, we won't need (as far as our algorithm for the jacobian is concerned) those matrices, but there may be independent interest in finding them.

We have already seen that the $[-1]$ matrices are characterized by having a fixpoint on C and having order 2 in $\mathbf{PGL}_n(\bar{k})$, i.e., modulo scalars. By the determinant 1 condition, the only possible scalars are elements of $\boldsymbol{\mu}_n(\bar{k})$.

Proposition. *When n is odd, we can choose the $[-1]$ matrices to satisfy $A^2 = 1$.*

Proof. Say we have found a matrix representing $[-1]$ but $A^2 = \zeta_n^i$. If i is odd, then we replace A with $\zeta_n^{(n-i)/2} A$. Then we will have $A^2 = 1$ and $\det A = 1$. If i is even, then we instead replace A with $\zeta_n^{(2n-i)/2} A$. □

Proposition. *When n is even, we can choose each $[-1]$ matrix to satisfy either $A^2 = 1$ or $A^2 = \zeta_n$.*

Proof. Say $A^2 = \zeta_n^i$. If i is even, we replace A with $\zeta_n^{(n-i)/2}$. If i is odd, we replace A with $\zeta_n^{(n+1-i)/2}$. □

IV.5. Finding the points of hyperosculation

For this step, what we do depends on the parity of n.

IV.5a. When n is odd

The hyperplanes fixed by M will intersect our curve in the n^2 points of hyperosculation. (The same is true for the hyperplanes fixed by N. See III.11.11.)

The hyperplanes fixed by M correspond to the eigenvectors of M^{t} (cf. §III.11). Thus, for example, if

$$M^{\mathsf{t}}[\alpha_0, \ldots, \alpha_{n-1}] = [\alpha_0, \ldots, \alpha_{n-1}],$$

then

$$[\alpha_0, \ldots, \alpha_{n-1}]^{\mathsf{t}} M^{-1} = [\alpha_0, \ldots, \alpha_{n-1}]^{\mathsf{t}},$$

whence M fixes the hyperplane

$$\alpha_0 x_0 + \ldots + \alpha_{n-1} x_{n-1} = 0.$$

Tossing the equation of a fixed hyperplane into our equations for I gives a 0-dimensional system whose solutions correspond to the points of intersection of the hyperplane with the curve. We solve this system by any convenient technique (cf. §IV.4a).

Repeating this process for each fixed hyperplane, we obtain the coordinates of the n^2 points of hyperosculation. We print these out as part of the algorithm's output.

IV.5b. When n is even

We find the points of hyperosculation by investigating the fixpoints of the $[-1]$ automorphisms (cf. §III.9a). For each matrix T representing such an automorphism, either all of its fixpoints on C (there are four of them) are points of hyperosculation, or none of them are. For a given fixpoint, we look at all hyperplanes through that fixpoint, looking for the one with maximal intersection multiplicity with C at that fixpoint (this is the osculating hyperplane at that point). In fact, it is easy to see that the osculating hyperplane must itself be fixed by T, so we can restrict our search to the fixed hyperplanes of T.

If the osculating hyperplane meets C *only* at the fixpoint in question, then we have found a point of hyperosculation, and the other fixpoints of the matrix are also points of hyperosculation.

IV.6. Finding *weighted* equations for the jacobian

The action of H_n on the curve is a non-faithful representation of the action of $\mathrm{J}_C[n]$ on the curve. We have

$$\mathrm{J}_C \cong C/\mathrm{J}_C[n] = C/H_n.$$

By basic principles of geometric invariant theory (cf. [Mum70, §II.7, §III.12] and [ABD+64, §7]), we have

$$\mathrm{J}_C \cong \operatorname{Proj}\left(\left(\frac{k(\theta)[x_0, \ldots, x_{n-1}]}{I\, k(\theta)[x_0, \ldots, x_{n-1}]}\right)^{H_n}\right)^{\mathrm{Gal}\left(k(\theta)/k\right)}.$$

Remark. In fact, since we only need to find J_C up to birational equivalence, we really only care that the Proj exhibited above has the correct function field. By the universal property of C/H_n, we can easily establish that its function field is

$$\left(K(C_K)^{H_n}\right)^{\mathrm{Gal}(K/k)}, \quad \text{where } K = k(\theta).$$

We easily check that the Proj above has the same function field.

The following lemma helps us break the monster Proj expression into bite-size pieces. (In the lemma, we are interested in the cases $G = H_n$ or $G = \mathrm{Gal}\big(k(\theta)/k\big)$.)

Lemma. *Let G be a finite group acting on a k-algebra R with trivial action on k, where k is a field and* $\mathrm{char}(k) \nmid |G|$. *If $I \subseteq R$ is an ideal with $GI = I$ (so that G acts on R/I), then*

$$(R/I)^G = R^G/I^G.$$

Proof. The averaging operator

$$*\colon R \longrightarrow R^G, \quad r \longmapsto \frac{1}{|G|}\sum_{g\in G} r^g$$

is a homomorphism of R^G-modules. Taking G-invariants on the short exact sequence $0 \to I \to R \to R/I \to 0$ gives the exact sequence

$$0 \to I^G \to R^G \to (R/I)^G.$$

If $f + I \in (R/I)^G$, then $f - f^g \in I$ for all $g \in G$. Then $\frac{1}{|G|}\big(\sum_g (f - f^g)\big) = f - f^*$ also lies in I, whence the coset $f + I$ is represented by $f^* \in R^G$. Thus we have the short exact sequence of R^G-modules

$$0 \to I^G \to R^G \to (R/I)^G \to 0.$$

□

By the lemma, we have

$$\mathrm{J}_C \cong \mathrm{Proj}\, \frac{\big(k(\theta)[x_0,\dots,x_{n-1}]^{H_n}\big)^{\mathrm{Gal}\left(k(\theta)/k\right)}}{\Big(\big(I\,k(\theta)[x_0,\dots,x_{n-1}]\big)^{H_n}\Big)^{\mathrm{Gal}\left(k(\theta)/k\right)}}.$$

(Observe the denominator may not be simply I. Certainly both H_n and $\mathrm{Gal}\big(k(\theta)/k\big)$ preserve the curve, whence I is preserved as a whole, but the individual elements in I need not be invariant.)

By work of Hilbert and Noether, $k(\theta)[x_0,\dots,x_{n-1}]^{H_n}$ is finitely generated. There exist standard algorithms in the invariant theory of finite groups (see for example [Stu93]) for finding a system of generators.

Applying one of these algorithms, we obtain finitely many polynomials p_i in $k(\theta)[x_0,\dots,x_{n-1}]$ so that $k(\theta)[x_0,\dots,x_{n-1}]^{H_n} = k(\theta)[p_i]$. Since H_n itself is $\mathrm{Gal}\big(k(\theta)/k\big)$-invariant, it is in fact the case that the algorithms cited above will produce p_i that are themselves $\mathrm{Gal}\big(k(\theta)/k\big)$-invariant, and thus

$$\big(k(\theta)[x_0,\dots,x_{n-1}]^{H_n}\big)^{\mathrm{Gal}\left(k(\theta)/k\right)}$$

is simply $k[p_i]$.

We end up with equations for J_C in terms of the generators p_i of the ring of invariants $\big(k(\theta)[x_0,\dots,x_{n-1}]^{H_n}\big)^{\mathrm{Gal}\left(k(\theta)/k\right)}$. These actually express J_C as a closed subscheme of a *weighted* projective space, since the new variables p_i need not have degree 1.

One can work with closed subschemes of weighted projective spaces quite similarly to the way one works with them in usual projective spaces (see [Dol82]). However, weighted projective spaces do admit some pathologies (cf. [Dol82, §1.5])—for example, they can be singular. Following [Dol82, §1.1, Lemma], we formally eliminate all common factors from the degrees of the p_i. For example, if we have five generators of degrees $(3; 6; 9; 9; 15)$, say, then we instead declare the degrees to be $(1; 2; 3; 3; 5)$, but otherwise make no changes.

Remark. We make this simple formal degree change because much of the theory of weighted projective spaces assumes one has done so. One could also attempt to further clean up the description of the weighted space, such as by applying [Dol82, §1.3.1, Proposition].

The algorithm now outputs the equations and the (formally adjusted) degrees of the variables of the weighted projective space.

The map $j_{\mathcal{D}}\colon C \to \mathrm{J}_C$ is simply the map $P \mapsto [p_i(P)]$. The algorithm outputs the polynomials p_i to give an explicit description of $j_{\mathcal{D}}$.

The k-rational origin on J_C is simply the image, under $j_{\mathcal{D}}$, of any one of the points of hyperosculation on C. We determined those points earlier. Picking one, and evaluating the p_i there, the algorithm outputs the coordinates of the origin of J_C.

IV.7. Obtaining non-weighted equations for J_C

Using the affine covering described in [Har77, II.2.5b], we can find an affine patch of J_C containing the origin of J_C. Homogenizing the resulting equations leads to equations for J_C as a closed subscheme of a (non-weighted) projective space. The algorithm outputs these equations and the new coordinates for the origin.

Remark. An alternate approach is to take the function field of J_C, which can be read off from the weighted projective model, and express that field in the form $k(\alpha)[\beta]/\langle f(\alpha,\beta)\rangle$, which leads to a non-weighted plane model of J_C.

Remark. If one's goal is a Weierstrass model for J_C, one could now (or even prior to finding a non-weighted model) apply the Riemann–Roch algorithm (cf. §V.7c).

IV.8. Algorithm summary

Let k be a perfect field. The input to the algorithm is a finite set of homogeneous forms with coefficients in k.

(They are supposed to scheme-theoretically define a non-degenerate curve of degree n in $\mathbf{P}_k^{n-1}$ of genus 1, where $n-1$ is the number of variables in the input, and $\mathrm{char}(k) \nmid n$. But all of this is verified in the first step of the algorithm.)

(1) Determine the dimension, genus, and degree n of the scheme defined by the equations, as well as whether the singular locus is empty. Terminate with an error if the scheme does not have dimension 1, or if the curve does not have genus 1, or if n is a multiple of $\mathrm{char}(k)$, or if the number of variables differs from $n-1$, or if the curve is singular, or if one of the equations is linear (whence the curve is degenerate).

(2) Let $\mathfrak{G}$ be a Gröbner basis (with respect to some fixed monomial order) for the ideal generated by the input equations. Let A be a generic $n \times n$ matrix. For each input equation $f(\mathbf{x}) = 0$, divide $f(A\mathbf{x})$ by $\mathfrak{G}$ and set each coefficient of the remainder to 0, thus obtaining a system of equations in the a_{ij} that describe which matrices A preserve the input curve.

(3) With the additional equation $\det(A) = 1$, solve for the finitely many solution matrices, expressing each matrix's entries as elements in $k(\theta)$, where $k(\theta)$ is a finite normal field extension of k constructed during the solution process.

(4) Among the finitely many matrices, find the ones that act fixpoint-free on the curve, and find generators for that subgroup of matrices.

(5) If n is odd, determine the hyperplanes fixed by one of the generators, and intersect those hyperplanes with the curve to find the points of hyperosculation. If n is even, instead find the $[-1]$-matrices among the solutions found earlier, write down all their fixpoints, and then determine which of the fixpoints admit osculating hyperplanes that hyperosculate.

(6) Compute k-rational generators p_i for the subring $k(\theta)[x_0,\dots,x_{n-1}]^{H_n}$, where H_n is the matrix group whose generators were found a couple steps ago. Compute k-rational generators for the ideal $\big(I\,k(\theta)[x_0,\dots,x_{n-1}]\big)^{H_n}$. These ideal generators serve as equations for J_C in a weighted projective space, whose coordinates are the p_i. Evaluating the p_i on the points of hyperosculation of C (see previous step) gives the coordinates of the origin on J_C.

(7) Grab an affine patch containing the origin of J_C and homogenize, thus obtaining equations for J_C in a (non-weighted) projective space.

CHAPTER V

Example: a Selmer cubic

Let $k = \mathbf{Q}$, and let $C \subset \mathbf{P}^2_{\mathbf{Q}}$ be the curve defined by $F(x, y, z) = 0$, where

$$F(x, y, z) = 3x^3 + 4y^3 + 5z^3.$$

That is,

$$C = \operatorname{Proj} \frac{\mathbf{Q}[x, y, z]}{\langle 3x^3 + 4y^3 + 5z^3 \rangle}. \tag{V.1}$$

In this chapter, we will apply the algorithm from chapter IV to find the jacobian of (V.1), as well as related data (such as the points of hyperosculation on C). Afterwards, in §V.6, we will find some of the other data discussed in chapter III that was not necessary for finding J_C. Finally, in §V.7, we will generalize the results to the family

$$\operatorname{Proj} \frac{k[x, y, z]}{\langle ax^3 + by^3 + cz^3 + mxyz \rangle},$$

where k is a perfect field with $\operatorname{char}(k) \neq 3$.

V.1. Vetting the input

It is easy to see that (V.1) is a smooth non-degenerate degree 3 curve in $\mathbf{P}^2_{\mathbf{Q}}$ of genus 1: we check smoothness by verifying the matrix of partial derivatives of F has full rank everywhere on C; non-degeneracy follows because the generator F is not linear; the degree can be read off from F; the genus can be read off from the genus formula $g = (d-1)(d-2)/2$ for plane curves. The code in table V.1 will give us the same information.

```
ringP2 = QQ[x,y,z]
f=3*x^3+4*y^3+5*z^3
idealC = ideal(f)
ringC = ringP2 / idealC
C = Proj ringC
dim C
codim singularLocus idealC
degree C
HH^1 OO_C
```

Table V.1. This *Macaulay 2* code vets the input.

V.2. Finding H_3

We will now go about finding the 27 matrices that are the $\bar{\mathbf{Q}}$-valued points of the Heisenberg group $H_3 \subset \mathbf{SL}_3$, which, in its action on $\mathbf{P}^2_{\mathbf{Q}}$, preserves C and corresponds to the action of $\mathrm{J}_C[3]$ on C (cf. §III.12). It is characterized by three things: it preserves C, each matrix has determinant 1, and it acts fixpoint-free on C.

First we will find conditions under which the generic matrix

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

preserves C. In other words, whenever a point $[x : y : z]$ lies on C, we require

$$\bar{A}[x : y : z] = [a_{11}x + a_{12}y + a_{13}z : a_{21}x + a_{22}y + a_{23}z : a_{31}x + a_{32}y + a_{33}z]$$

to also lie on C, where $\bar{A}$ denotes the image of A in $\mathbf{PGL}_3(\bar{\mathbf{Q}})$. That is, $F\big(\bar{A}[x : y : z]\big)$ must lie in the ideal $\big\langle F(x, y, z)\big\rangle$, where

$$F\big(\bar{A}[x : y : z]\big) = \\ 3(a_{11}x + a_{12}y + a_{13}z)^3 + 4(a_{21}x + a_{22}y + a_{23}z)^3 + 5(a_{31}x + a_{32}y + a_{33}z)^3. \quad (*)$$

This amounts to dividing $(*)$ by F and demanding the remainder to vanish, giving us 9 vanishing conditions on the coefficients of A:

$$\begin{aligned} F\big(\bar{A}[x : y : z]\big) = {} & (a_{11}^3 + \tfrac{4}{3}a_{21}^3 + \tfrac{5}{3}a_{31}^3)\, F(x, y, z) - \\ & \big(4a_{11}^3 - 3a_{12}^3 + \tfrac{16}{3}a_{21}^3 - 4a_{22}^3 + \tfrac{20}{3}a_{31}^3 - 5a_{32}^3\big)\, y^3 + \big(9a_{12}^2a_{13} + 12a_{22}^2a_{23} + 15a_{32}^2a_{33}\big)\, y^2z + \\ & \big(9a_{12}a_{13}^2 + 12a_{22}a_{23}^2 + 15a_{32}a_{33}^2\big)\, yz^2 - \big(5a_{11}^3 - 3a_{13}^3 + \tfrac{20}{3}a_{21}^3 - 4a_{23}^3 + \tfrac{25}{3}a_{31}^3 - 5a_{33}^3\big)\, z^3 + \\ & \big(9a_{11}^2a_{12} + 12a_{21}^2a_{22} + 15a_{31}^2a_{32}\big)\, x^2y + \big(9a_{11}^2a_{13} + 12a_{21}^2a_{23} + 15a_{31}^2a_{33}\big)\, x^2z + \\ & \big(9a_{11}a_{12}^2 + 12a_{21}a_{22}^2 + 15a_{31}a_{32}^2\big)\, xy^2 + \big(9a_{11}a_{13}^2 + 12a_{21}a_{23}^2 + 15a_{31}a_{33}^2\big)\, xz^2 + \\ & \big(18a_{11}a_{12}a_{13} + 24a_{21}a_{22}a_{23} + 30a_{31}a_{32}a_{33}\big)\, xyz. \end{aligned}$$

```
ring R = (0,a11,a12,a13,a21,a22,a23,a31,a32,a33),(x,y,z),dp;
poly F = 3*x^3+4*y^3+5*z^3;
ideal I = F;
I = groebner(I);
matrix A[3][3] = a11,a12,a13,a21,a22,a23,a31,a32,a33;
matrix vars[3][1] = x,y,z;
matrix newvars = A*vars;
map substitution = R,newvars[1,1],newvars[2,1],newvars[3,1];
poly substituted = substitution(F);
poly reduced = reduce(substituted, I);
matrix conditions = coef(reduced, x*y*z);
conditions;
```

Table V.2. This *Singular* code determines the conditions for a matrix to preserve the Selmer cubic.

We next put these 9 conditions, along with the extra conditions $\det(A) = 1$ and $A^3 = 1$ (cf. IV.4.1) into an ideal in $\mathbf{Q}[a_{ij}]$ with elimination (lexicographic) ordering, and find a reduced Gröbner basis. For example, the code in table V.2 finds again the 9 conditions found previously by hand, and then the code in table V.3 produces the equations shown below.

Remark V.2.1. The $A^3 = 1$ condition turns out to be crucial (this possibility is discussed in §IV.4b). Without that condition, the code would need to run an unknown amount of time—we gave up after waiting an hour. Even with $A^9 = 1$ (a trivial condition—for both n even and n odd, we certainly have $A^{n^2} = 1$, since A^n is a scalar matrix), and with or without the $\det = 1$ condition, we again gave up after an hour. But with $A^3 = 1$ in place, with or without $\det = 1$, the code runs almost instantaneously.

```
ring S = 0,(a11,a12,a13,a21,a22,a23,a31,a32,a33),lp;
ideal conditions_ideal;

int i; for (i = 1; i <= 9; i++) {
  setring R;
  poly condition = conditions[2,i];
  setring S;
  poly condition_in_S = imap(R,condition);
  condition_in_S = cleardenom(condition_in_S);
  conditions_ideal = conditions_ideal + condition_in_S;
  }

matrix AA = imap(R,A);
poly determinant_one = 1 - det(AA);
conditions_ideal = conditions_ideal + determinant_one;

LIB "matrix.lib";  // Lets us call power(), unitmat(), ...
matrix AA_cubed = power(AA,3) - unitmat(3);
int j; for (i = 1; i <= 3; i++) {
  for (j = 1; j <= 3; j++) {
    conditions_ideal = conditions_ideal + AA_cubed[i,j];
    }
  }

option(redSB); // so that ``groebner'' returns reduced result...
conditions_ideal = groebner(conditions_ideal);
conditions_ideal;
```

Table V.3. This *Singular* code (continuation from previous table) determines the conditions, in elimination order, for a matrix to satisfy three conditions: preserve the Selmer cubic, have determinant 1, and have its cube be 1.

$$
\begin{aligned}
125a_{32}^{10} - 64a_{32} = 0, \quad & a_{33}^4 - a_{33} = 0, \quad a_{32}a_{33} = 0, \quad a_{31}a_{33} = 0,\\
8000a_{31}^9 + 3375a_{32}^9 + 1728a_{33}^3 - 1728 = 0, \quad & 12a_{23}^3 - 25a_{31}^3 = 0, \quad a_{31}a_{32} = 0, \quad a_{23}a_{33} = 0,\\
125a_{21}a_{32}^9 - 64a_{21} = 0, \quad & a_{22}a_{33}^3 - a_{22} = 0, \quad a_{23}a_{32} = 0, \quad a_{22}a_{32} = 0,\\
12a_{13} - 25a_{21}^2a_{32}^5 = 0, \quad & a_{22}^3 - a_{33}^3 = 0, \quad a_{22}a_{31} = 0, \quad a_{22}a_{23} = 0,\\
9a_{12} - 20a_{23}^2a_{31}^5 = 0, \quad & 16a_{21}^3 - 15a_{32}^3 = 0, \quad a_{21}a_{33} = 0, \quad a_{21}a_{31} = 0,\\
& a_{11} - a_{22}^2a_{33}^2 = 0, \quad a_{21}a_{23} = 0, \quad a_{21}a_{22} = 0.
\end{aligned}
$$

These equations define a 0-dimensional ideal in $\mathbf{Q}[a_{ij}]$. There exist computer algorithms, such as the ones in *Singular*'s library `zeroset_lib`, that will construct a field extension containing all solutions and then list the solutions. Waiting on the computer to do this exhausted our patience, so we simply solved it by hand.

Let $K = \mathbf{Q}(\zeta_3, \sqrt[3]{3}, \sqrt[3]{4}, \sqrt[3]{5})$, where ζ_3 is a primitive cube root of unity, i.e., $\zeta_3^2 + \zeta_3 + 1 = 0$, and each of the other symbols satisfies the obvious equation, e.g., $(\sqrt[3]{4})^3 = 4$. A symbol such as $\sqrt[3]{-4/5}$ is shorthand for $-\sqrt[3]{4}/\sqrt[3]{5}$.

When we go about finding all matrices in the solution set (the details are left to the reader), we discover that there are 9 solutions (modulo cube roots of unity): 1, M, M^2, N, MN, M^2N, N^2, MN^2, M^2N^2, where

$$
M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3^2 \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} 0 & \sqrt[3]{4/3} & 0 \\ 0 & 0 & \sqrt[3]{5/4} \\ \sqrt[3]{3/5} & 0 & 0 \end{bmatrix}.
$$

But we didn't really have to find them all. We merely need to find two generators for the Heisenberg group H_3. Thus we must find a pair of matrices that act fixpoint-free on C and whose commutator is a primitive cube root of unity.

It is easy to check that the two matrices M and N satisfy the commutator condition. The fixpoints of M and N in $\mathbf{P}^2_{\mathbf{Q}}(\bar{\mathbf{Q}})$ correspond to the eigenspaces of M and N (cf. §III.11). Using

standard linear algebra techniques for finding eigenvalues and eigenvectors, we determine that M fixes

$$[1:0:0], \quad [0:1:0], \quad [0:0:1],$$

while N fixes

$$[1:\sqrt[3]{3/4}:\sqrt[3]{3/5}],$$
$$[1:\zeta_3\sqrt[3]{3/4}:\zeta_3^2\sqrt[3]{3/5}],$$
$$[1:\zeta_3^2\sqrt[3]{3/4}:\zeta_3\sqrt[3]{3/5}].$$

Substituting these points into the equation defining C verifies that the action of M and N on C is indeed fixpoint-free.

V.3. Points of hyperosculation and the hyperplane configuration

The hyperplanes fixed by M and N correspond to the eigenvectors of M^{t} and N^{t} (cf. §III.11). We determine that M fixes the hyperplanes

$$x=0, \quad y=0, \quad z=0,$$

while N fixes the hyperplanes

$$x+\sqrt[3]{4/3}y+\sqrt[3]{5/3}z=0,$$
$$x+\zeta_3^2\sqrt[3]{4/3}y+\zeta_3\sqrt[3]{5/3}z=0,$$
$$x+\zeta_3\sqrt[3]{4/3}y+\zeta_3^2\sqrt[3]{5/3}z=0.$$

Intersecting *either* set of hyperplanes with C produces the 9 points of hyperosculation (cf. §III.11.8):

$$[0:1:\sqrt[3]{-4/5}], \quad [0:1:\zeta_3\sqrt[3]{-4/5}], \quad [0:1:\zeta_3^2\sqrt[3]{-4/5}],$$
$$[\sqrt[3]{-5/3}:0:1], \quad [\zeta_3\sqrt[3]{-5/3}:0:1], \quad [\zeta_3^2\sqrt[3]{-5/3}:0:1],$$
$$[1:\sqrt[3]{-3/4}:0], \quad [1:\zeta_3\sqrt[3]{-3/4}:0], \quad [1:\zeta_3^2\sqrt[3]{-3/4}:0].$$

The rows correspond to the hyperplanes fixed by M, while the columns correspond to the hyperplanes fixed by N. We see here the arrangement and intersection pairing described in §III.11.11.

Remark. Classically, the points of hyperosculation on a plane cubic are found using the Hessian. We say more about this in §V.6c.

V.4. The curve underlying the jacobian J_C

The matrices M and N generate an abelian group $J_n \subset \mathbf{PGL}_3(K)$ whose elements correspond to $\mathrm{J}_C[3](\bar{\mathbf{Q}})$. Thus $\mathrm{J}_C[3]$ is defined (element-wise) over K.

The same matrices generate a group of order 27 in $\mathbf{SL}_3(K)$. Let $H_3 \subset \mathbf{SL}_3$ be the subgroup with those K-valued points. By the material in §IV.6, we have

$$\mathrm{J}_C \cong \operatorname{Proj} \frac{\mathbf{Q}[x,y,z] \cap K[x,y,z]^{H_3(K)}}{I \cap K[x,y,z]^{H_3(K)}}.$$

To determine the latter more explicitly, we start by looking for an explicit description of $K[x,y,z]^{H_3(K)}$. We know from general principles (see [Stu93]) that there will be three algebraically

```
(*MonomialList generates all monomial exponent vectors
  satisfying the given degree constraints.*)
MonomialList[varcount_, minweight_, maxweight_] :=
    Module[
      {v, i, r, keepgoing},
      v = Table[maxweight, {varcount}];
      r = {};
      keepgoing = True;
      While[keepgoing,
        If[minweight <= (Plus @@ v) && (Plus @@ v) <= maxweight,
          r = Append[r, v];
          ];
        (* Subtract 1 from first index in varlist v. *)
        (* If result is negative, replace with maxweight,
           and move right. If we run out of variables, quit. *)
        i = 1;
        While[--v[[i]] < 0,
          v[[i]] = maxweight;
          ++i;
          If[i > varcount,
            keepgoing = False; Break[];];
          ];
        ];
      r
      ];

(*Reynolds averages the value of the function on the matrixgroup orbit of varlist.*)
ReynoldsOperator[matrixgroup_List, f_, varlist_List] :=
    Apply[Plus, Map[Apply[f, #.varlist] &, matrixgroup]]/Length[matrixgroup];

(*GeneratingInvariants applies Reynolds to all monomials of a given degree.*)
GeneratingInvariants[matrixgroup_List, varlist_List, degree_Integer] :=
    Module[
      {m = MonomialList[Length[varlist], degree, degree]},
      Table[
        ReynoldsOperator[matrixgroup,
          Function[varlist, Times @@ Apply[Power, {varlist, m[[i]]}]],
          varlist],
        {i, Length[m]}]
      ];

InvertedCharPoly[matrix_List, var_] :=
    Det[IdentityMatrix[Length[matrix]] - var*matrix];
MolienSeries[matrixgroup_List, var_] :=
  (1/Length[matrixgroup])*Plus @@ Map[1/InvertedCharPoly[#, var] &, matrixgroup]

HeisenbergGroup[m_List, n_List] :=
  Module[{d = Dimensions[m][[1]], z = m.n.Inverse[m].Inverse[n]},
    Flatten[Table[
        MatrixPower[z, i].MatrixPower[m, j].MatrixPower[n, k], {i, d}, {j,
          d}, {k, d}], 2]]
```

Table V.4. This *Mathematica* code defines functions we'll need in the next listing.

independent invariants (known as primary invariants), and possibly some additional dependent invariants (secondary invariants). The Molien series,

$$\begin{aligned}\Phi_{H_3}(t) &= \tfrac{1}{27}\sum_{\sigma\in H_3(K)}\frac{1}{\det(\mathsf{id}-t\sigma)}\\ &= \tfrac{1}{27}\left(\frac{1}{(1-t)^3}+\frac{1}{(1-\zeta_3 t)^3}+\frac{1}{(1-\zeta_3^2 t)^3}+\frac{24}{1-t^3}\right)=\frac{1-t^3+t^6}{(1-t^3)^3}\\ &= 1+2t^3+4t^6+7t^9+11t^{12}+16t^{15}+22t^{18}+29t^{21}+37t^{24}+\cdots,\end{aligned}$$

tells us that there are two linearly independent invariants of degree 3, four of degree 6, seven of degree 9, and so on.

(The *Mathematica* code in table V.5, relying on the functions from table V.4, will compute the Molien series above as well as what we are about to calculate.)

The three possible products of the two invariants of degree 3 do not account for all four linearly independent invariants of degree 6. Hence we start by looking in degree 3 and degree 6. Applying

```
cuberoot1 = Root[(#^2 + # + 1), 1];
cuberoot3 = Root[(#^3 - 3), 1];
cuberoot4 = Root[(#^3 - 4), 1];
cuberoot5 = Root[(#^3 - 5), 1];
vars = {x,y,z};
MM = DiagonalMatrix[Map[(cuberoot1^#) &, Range[3]]];
NN = RotateLeft[
      DiagonalMatrix[{cuberoot3/cuberoot5, cuberoot4/cuberoot3, cuberoot5/cuberoot4}]];
MM // Simplify // MatrixForm
NN // Simplify // MatrixForm

h = HeisenbergGroup[MM, NN];
ms = MolienSeries[h, t]
ms = Simplify[ms]
Series[ms, {t, 0, 30}]

Factor[Union[Simplify[GeneratingInvariants[h, vars, 3]]]]
Factor[Union[Simplify[GeneratingInvariants[h, vars, 6]]]]

P1 = x y z;
P2 = 3x^3 + 4y^3 + 5z^3;
P3 = 9x^6 + 16y^6 + 25z^6;
GroebnerBasis[{P1-y1,P2-y2,P3-y3}, {x,y,z,y1,y2,y3}, {x,y,z}]

Simplify[ms*((1 - t^3)(1 - t^3)(1 - t^6))]
GeneratingInvariants[h, vars, 9] // Simplify // Factor // Simplify // Union // Factor

P4 = 27x^9 + 64y^9 + 125z^9;
GroebnerBasis[{P1-y1,P2-y2,P3-y3,P4-y4}, {x,y,z,y1,y2,y3,y4}, {x,y,z}]

P4 = 48x^3y^6 + 45x^6z^3 + 100y^3z^6;
syzygy = GroebnerBasis[{P1-y1,P2-y2,P3-y3,P4-y4}, {x,y,z,y1,y2,y3,y4}, {x,y,z}]

gg = GroebnerBasis[{P1-y1,P2-y2,P3-y3,P4-y4}, {x,y,z,y1,y2,y3,y4}];
PolynomialReduce[3x^3 + 4y^3 + 5z^3, gg, {x,y,z,y1,y2,y3,y4}]

syzygy /. {y2 -> 0}
```

Table V.5. This *Mathematica* code (relying on functions from previous table) calculates the Molien series, the primary and secondary invariants, and the final syzygy that gives the model for J_C.

the Reynolds operator to all degree 3 and all degree 6 monomials gives the following list of invariants:

$$\begin{array}{lll} xyz, & 3x^3+4y^3+5z^3, & xyz(3x^3+4y^3+5z^3), \\ x^2y^2z^2, & 9x^6+16y^6+25z^6, & 12x^3y^3+15x^3z^3+20y^3z^3. \end{array}$$

Two invariants of degree 3 together with one invariant of degree 6 must compose a set of algebraically independent invariants. We arbitrarily choose

$$\begin{aligned} P_1 &:= xyz \\ P_2 &:= 3x^3+4y^3+5z^3 \\ P_3 &:= 9x^6+16y^6+25z^6 \end{aligned}$$

We verify their algebraic independence by introducing slack variables s_1, s_2, s_3 with an elimination ordering on monomials and compute a Gröbner basis for the ideal $\langle P_1 - s_1, P_2 - s_2, P_3 - s_3\rangle$ in $\mathbf{Q}[x, y, z, s_1, s_2, s_3]$ and then intersect with $\mathbf{Q}[s_1, s_2, s_3]$ to read off any syzygies: there are none. In other words, the ring homomorphism from $\mathbf{Q}[s_1, s_2, s_3]$ to $\mathbf{Q}[P_1, P_2, P_3]$ given by $s_i \mapsto P_i$ has trivial kernel. (All of this is explained quite nicely in [CLO97].

We can furthermore easily see that $(0, 0, 0)$ is the only solution to $P_1 = 0$, $P_2 = 0$, $P_3 = 0$; whence, by the Nullstellensatz, the radical of $\langle P_1, P_2, P_3\rangle$ is $\langle x, y, z\rangle$. Thus $K[x, y, z]$ is integral over $K[P_1, P_2, P_3]$, whence also $K[x, y, z]^{H_3(K)}$ is integral over $K[P_1, P_2, P_3]$, and therefore is finitely generated as a module over $K[P_1, P_2, P_3]$. (In fact, as explained in [Stu93], $K[x, y, z]^{H_3(K)}$ will be free over $K[P_1, P_2, P_3]$, since the subring of invariants is Cohen–Macaulay.)

Thus P_1, P_2, P_3 shall serve as primary invariants. They generate a graded subring of the subring of invariants, and their Hilbert series is

$$\frac{1}{1-t^3}\frac{1}{1-t^3}\frac{1}{1-t^6},$$

which forms the denominator of the Hironaka form of our earlier Molien series:

$$\Phi_{H_3}(t) = \frac{1+t^9}{(1-t^3)(1-t^3)(1-t^6)}.$$

Thus there is one secondary invariant, in degree 9, which we now locate. Applying the Reynolds operator to all degree 9 monomials gives us:

$$\begin{gathered} x^2y^2z^2(3x^3{+}4y^3{+}5z^3), \qquad 36x^6y^3{+}80y^6z^3{+}75x^3z^6, \\ xyz(9x^6{+}16y^6{+}25z^6), \qquad 48x^3y^6{+}45x^6z^3{+}100y^3z^6, \\ x^3y^3z^3, \qquad 27x^9{+}64y^9{+}125z^9, \qquad xyz(12x^3y^3{+}15x^3z^3{+}20y^3z^3). \end{gathered}$$

If we compute a Gröbner basis for the ideal

$$\langle P_1 - s_1, P_2 - s_2, P_3 - s_3, 27x^9 + 64y^9 + 125z^9 - s_4 \rangle$$

and intersect with $\mathbf{Q}[s_1, s_2, s_3, s_4]$, we obtain the syzygy

$$-360s_1^3 + s_2^3 - 3s_2s_3 + 2s_4;$$

since this syzygy is linear in s_4, it tells us that $27x^9 + 64y^9 + 125z^9$ is linearly dependent on other degree 9 invariants expressible in terms of our previous choices. We next try

$$P_4 := 48x^3y^6 + 45x^6z^3 + 100y^3z^6,$$

and this time the syzygy is not linear in s_4:

$$\begin{aligned} 259200s_1^6 - 960s_1^3s_2^3 + s_2^6 + 1440s_1^3s_2s_3 - 3s_2^4s_3 \\ + 3s_2^2s_3^2 - s_3^3 + 1440s_1^3s_4 - 4s_2^3s_4 + 4s_2s_3s_4 + 8s_4^2. \end{aligned}$$

In other words,

$$K[x,y,z]^{H_3(K)} \cong \frac{K[s_1,s_2,s_3,s_4]}{\left\langle \begin{array}{r} 259200s_1^6{-}960s_1^3s_2^3{+}s_2^6{+}1440s_1^3s_2s_3{-}3s_2^4s_3 \\ {+}3s_2^2s_3^2{-}s_3^3{+}1440s_1^3s_4{-}4s_2^3s_4{+}4s_2s_3s_4{+}8s_4^2 \end{array} \right\rangle},$$

where this is an isomorphism of graded rings so long as we keep in mind a weighted grading on the right: the variables s_1, s_2, s_3, s_4 have degrees $3, 3, 6, 9$ (corresponding to our choices of P_1, P_2, P_3, P_4).

Remark. Although irrelevant to our calculations, it is helpful to understand what the primary and secondary invariants have to do with the structure of the ring of invariants. As already mentioned, the ring $K[x,y,z]^{H_3(K)}$ is Cohen–Macaulay, and thus it is a finitely generated free module, generated by the secondary invariants over the subring generated by the algebraically independent primary invariants:

$$K[x,y,z]^{H_3(K)} = K[P_1,P_2,P_3] \oplus P_4K[P_1,P_2,P_3].$$

Having determined $K[x,y,z]^{H_3(K)}$, we return to the problem of finding J_C. Observe that our choices are such that the equation of the curve is given by $P_2 = 0$. Furthermore, since $H_3(K)$ is defined over $\mathbf{Q}$, the Molien series and the invariants calculated above were each $\mathrm{Gal}(K/\mathbf{Q})$-invariant. Thus we have

$$\mathbf{Q}[x,y,z] \cap K[x,y,z]^{H_3(K)} \cong \frac{\mathbf{Q}[s_1,s_2,s_3,s_4]}{\left\langle \begin{array}{r} 259200s_1^6{-}960s_1^3s_2^3{+}s_2^6{+}1440s_1^3s_2s_3{-}3s_2^4s_3 \\ {+}3s_2^2s_3^2{-}s_3^3{+}1440s_1^3s_4{-}4s_2^3s_4{+}4s_2s_3s_4{+}8s_4^2 \end{array} \right\rangle},$$

and substituting $s_2 = 0$ corresponds to working modulo I, so that we have established

$$\mathrm{J}_C \cong \mathrm{Proj}\, \frac{\mathbf{Q}[s_1,s_3,s_4]}{\langle 259200s_1^6 - s_3^3 + 1440s_1^3s_4 + 8s_4^2 \rangle}.$$

We have expressed the curve underlying J_C as a curve of degree 18 in a *weighted* projective plane $\mathbf{P}^{(3;6;9)}_{\mathbf{Q}}$. By the general theory of weighted projective planes (see the end of §IV.6), we formally relabel the weights to be $(1;2;3)$, so that J_C is now a curve of degree 6 in $\mathbf{P}^{(1;2;3)}_{\mathbf{Q}}$.

The $\mathbf{Q}$-rational group law origin on J_C corresponds to the points of hyperosculation on C. Since the functions s_1, s_3, s_4 are invariant on those n^2 points, we can obtain coordinates for the origin on J_C by picking any one of the points of hyperosculation and applying the map (cf. II.2.4)

$$j_{\mathcal{D}}\colon\ [x:y:z] \longmapsto \big[P_1(x,y,z) :: P_3(x,y,z) :: P_4(x,y,z)\big],$$

where we use the notation $[\cdot :: \cdot :: \cdot]$ on *weighted* homogeneous coordinates to remind us of the unusual equivalence relation: $[x :: y :: z] \sim [\lambda x :: \lambda^2 y :: \lambda^3 z]$.

For example, one of the points of hyperosculation is $[0:1:\sqrt[3]{-4/5}]$. Evaluating $j_{\mathcal{D}}$ at this point gives us the group law origin on J_C:

$$O_{\mathrm{J}_C} = [0 :: 2 :: 1].$$

Remark. In fact, evaluating $[P_1 :: P_3 :: P_4]$ at each of the 9 points of hyperosculation leads to $[0 :: 32 :: 64]$, $[0 :: 50 :: 125]$, and $[0 :: 18 :: 27]$. But each of those is just $[0 :: 2 :: 1]$.

In summary, we have determined the jacobian of (V.1) to be

$$\mathrm{J}_C \cong \mathrm{Proj}\,\frac{\mathbf{Q}[r,s,t]}{\langle 259200r^6 - s^3 + 1440r^3t + 8t^2\rangle}, \tag{V.2}$$

where variables r, s, t have degrees $(1;2;3)$, and the origin of the group law is the $\mathbf{Q}$-rational point $[0 :: 2 :: 1]$. We obtained J_C as an elliptic curve of degree 6 in the weighted projective plane $\mathbf{P}^{(1;2;3)}_{\mathbf{Q}} = \mathrm{Proj}\big(\mathbf{Q}[r,s,t]\big)$.

V.5. Obtaining a non-weighted model for J_C

We will now obtain a non-weighted version of (V.2) using the approach from §IV.7. The weighted projective plane $\mathbf{P}^{(1;2;3)}_{\mathbf{Q}}$ is covered by the following three affine patches (see [Har77, II.2.5b])

$$\begin{aligned}
\operatorname{Spec}\mathbf{Q}\big[\frac{s}{r^2},\frac{t}{r^3}\big] &\cong \operatorname{Spec}\mathbf{Q}[u,v] \quad \text{(open subset where } r\neq 0),\\
\operatorname{Spec}\mathbf{Q}\big[\frac{r^2}{s},\frac{rt}{s^2},\frac{t^2}{s^3}\big] &\cong \operatorname{Spec}\frac{\mathbf{Q}[u,v,w]}{\langle uw-v^2\rangle} \quad \text{(open subset where } s\neq 0),\\
\operatorname{Spec}\mathbf{Q}\big[\frac{r^3}{t},\frac{rs}{t},\frac{s^3}{t^2}\big] &\cong \operatorname{Spec}\frac{\mathbf{Q}[u,v,w]}{\langle uw-v^3\rangle} \quad \text{(open subset where } t\neq 0),
\end{aligned}$$

where u, v, w are indeterminates. Thus we have three different ways of obtaining an affine model for J_C, but only two of those models (the latter two above) contain the image of the $\mathbf{Q}$-rational origin $[0 :: 2 :: 1]$ on J_C.

Let us use the affine patch corresponding to $s \neq 0$. Dividing the defining expression in (V.2) through by s^3 leads to

$$\operatorname{Spec}\frac{\mathbf{Q}[u,v,w]}{\langle uw - v^2, 259200u^3 - 1 + 1440uv + 8w\rangle} \subset \mathbf{A}^3_{\mathbf{Q}},$$

where the $\mathbf{Q}$-rational origin is now $(0,0,1/8)$. We can of course homogenize this if we prefer a projective model for J_C.

We have finished applying the algorithm from chapter IV to $F(x,y,z) = 3x^3 + 4y^3 + 5z^3 = 0$. In the next section, we will say some additional things about that example. Then, in §V.7, we will tackle the family $ax^3 + by^3 + cz^3 + mxyz = 0$.

V.6. Musings

V.6a. Finding the 2-torsion on (C, O)

We will determine the matrix T corresponding to $[-1]$ on the elliptic curve (C, O), where O is the following point of hyperosculation:

$$O = [0:1:\sqrt[3]{-4/5}].$$

Thus we seek a matrix A of determinant 1 that preserves C and also fixes O, and furthermore its square should be a scalar matrix (so that the matrix has order 2 on the curve). But if, say, $A^2 = \zeta_3$, then $(\zeta_3 A)^2 = 1$, and $\det(\zeta_3 A) = 1$. Thus we can find an A that satisfies $A^2 = 1$. To do this, we repeat the calculations from tables V.2 and V.3, only this time we replace the condition $A^3 = 1$ with $A^2 = 1$. To preserve O, we discover we must have, among other things, the additional condition $5a_{12}^3 = 4a_{13}^3$, which already simplifies matters sufficiently to determine

$$T = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 0 & \sqrt[3]{-5/4} \\ 0 & \sqrt[3]{-4/5} & 0 \end{bmatrix}.$$

The three eigenvalues of T are $1, -1, -1$. There is one isolated fixpoint in $\mathbf{P}^2_{\mathbf{Q}}$, and one line's worth of fixpoints in $\mathbf{P}^2_{\mathbf{Q}}$, which gives us 3 fixpoints on C. Since T must have 4 fixpoints on C, the isolated fixpoint must lie on C. Indeed, by computing eigenvectors, we determine that the fixpoint corresponding to eigenvalue $+1$ is O, while the fixed line is spanned by $[1:0:0]$ and $[0:1:\sqrt[3]{4/5}]$. That line cuts C in the following three points:

$$[\sqrt[3]{-8/3}:1:\sqrt[3]{4/5}], \quad [\zeta_3\sqrt[3]{-8/3}:1:\sqrt[3]{4/5}], \quad [\zeta_3^2\sqrt[3]{-8/3}:1:\sqrt[3]{4/5}].$$

These must be the three points of non-trivial 2-torsion on (C, O). Note that they are *not* points of hyperosculation (cf. §III.9).

V.6b. Obtaining a Weierstrass model for J_C

As mentioned in §I.1b, once we have a curve of genus 1 together with a rational point (i.e., an elliptic curve), we can always apply the Riemann–Roch algorithm to obtain a Weierstrass model for that curve (cf. §V.7c). In the present example, it turns out there is an easier way.

At the start of §V.5, we chose an affine patch containing the $\mathbf{Q}$-rational origin on J_C. If we instead work with an affine patch that does *not* contain that point, then we will obtain an affine model with the origin "at infinity".

Dividing the defining expression in (V.2) through by r^6 leads to the affine model

$$\operatorname{Spec} \frac{\mathbf{Q}[u,v]}{\langle 259200 - u^3 + 1440v + 8v^2\rangle} \subset \mathbf{A}^2_{\mathbf{Q}}.$$

We knew this would give us an affine plane model, but it so happens we already ended up with a Weierstrass model! If we now apply the substitution $u \leftarrow 2X$, $v \leftarrow \frac{1}{2}(Y - 180)$, and clear off the common factor 2 from the result, we end up with

$$Y^2 = 4X^3 - 97200. \tag{V.3}$$

In the cases $n = 2, 3, 4$, formulas for a Weierstrass model of J_C appear in [AKM$^+$01]. (For $n = 5$, see [Fis].) If we apply those formulas to (V.1), we also end up with (V.3) above.

V.6c. The classical Hessian

In §V.3, we found the 9 points of hyperosculation on our plane cubic (V.1) by finding the hyperplane sections fixed by a generator for H_3.

Classically (cf. [Sil99, Ex. III.3.9]), the 9 points of hyperosculation (called *flex points*) on a plane cubic $F(x, y, z) = 0$ are obtained by intersecting the cubic with its Hessian $H(x, y, z) = 0$, where

$$H(x,y,z) := \begin{vmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x\,\partial y} & \frac{\partial^2 F}{\partial x\,\partial z} \\ \frac{\partial^2 F}{\partial y\,\partial x} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y\,\partial z} \\ \frac{\partial^2 F}{\partial z\,\partial x} & \frac{\partial^2 F}{\partial z\,\partial y} & \frac{\partial^2 F}{\partial z^2} \end{vmatrix}.$$

Even without knowing any of the general theory of the Hessian, we can see quite easily that the Hessian in our current example behaves as the theory says it must. For our F, the Hessian H is just (a scalar multiple of) of the invariant P_1 from §V.4. In calculating the origin on J_C, we saw that P_1

vanishes at the 9 points of hyperosculation; on the other hand, by Bézout's theorem (see [HAR77, I.7.8]), it cannot vanish elsewhere on C.

In fact, we saw in §V.4 that the space of cubic invariants is 2-dimensional, spanned by F and P_1. Therefore, *other than scalar multiples of F, any cubic invariant will intersect C in the points of hyperosculation.* A more enlightening way of seeing this goes as follows.

Invariants of any degree that do not vanish identically on C will necessarily intersect C in a union of 3-torsion packets. If the invariant is defined over $\mathbf{Q}$, then its intersection with C is also defined over $\mathbf{Q}$. In particular, by Bézout, a cubic invariant will intersect C in a single 3-torsion packet defined over $\mathbf{Q}$; therefore, if we can show that the hyperosculation packet is the *unique* such packet, then it follows that any cubic invariant must intersect C in the hyperosculation packet.

A change-of-variables to (V.3) yields $Y^2 = X^3 - 24300$. Feeding `[0,0,0,0,-24300]` to *mwrank* tells us that J_C has rank 0, while feeding

```
e=ellinit([0,0,0,0,-24300]);elltors(e)
```

to *GP/Pari* tells us that J_C has a single point of torsion. In short, the hyperosculation packet is the unique 3-torsion packet on C that is defined over $\mathbf{Q}$.

V.7. Tackling the family $ax^3 + by^3 + cz^3 + mxyz = 0$

Let k be a perfect field with $\mathrm{char}(k) \neq 3$ (concerning this restriction, cf. §I.2e). Set

$$C = \mathrm{Proj}\, \frac{k[x,y,z]}{\langle ax^3 + by^3 + cz^3 + mxyz \rangle}, \tag{V.4}$$

where $a, b, c, m \in k$. The condition for C to be smooth is $abc(27abc + m^3) \neq 0$.

V.7a. History

The family (V.4) has been studied extensively (often without the $mxyz$ term). It was known classically that a k-rational point on (V.4) leads to a non-trivial k-rational point on the elliptic curve

$$E = \mathrm{Proj}\, \frac{k[X,Y,Z]}{\langle X^3 + Y^3 + abcZ^3 + mXYZ \rangle}, \quad \text{with origin } O_E = [1:-1:0]. \tag{V.5}$$

Formulas for this are attributed to Sylvester in [CAL92, §3] and to Euler in [SEL51, §I.2]. See also [CAS91, §18, Lemma 1].

That (V.5) is the jacobian of (V.4) has probably been known for a long time—the earliest reference I could find, for $m = 0$ and $k = \mathbf{Q}(\zeta_3)$, is [CAS91, §20, Ex. 3]. The proof outlined there works in general, and goes as follows. Over $k(\zeta_3, \sqrt[3]{a}, \sqrt[3]{b})$ we can write down the isomorphism $\phi\colon (\mathrm{V.4}) \to (\mathrm{V.5})$ given by $X = \sqrt[3]{a}\, x$, $Y = \sqrt[3]{b}\, y$, and $Z = (\sqrt[3]{ab})^{-1} z$. Then $\xi_\sigma := \phi^\sigma \circ \phi^{-1}$ is an element of $\mathrm{H}^1\bigl(\mathrm{G}_k, E(\bar{k}) \rtimes \mathrm{Aut}(E, O_E)\bigr)$. It is easy to verify that each ξ_σ is a fixpoint-free automorphism of E, whence $\xi \in \mathrm{H}^1\bigl(\mathrm{G}_k, E(\bar{k})\bigr)$. Therefore, C is a principal homogeneous space for E, and thus $E \cong \mathrm{J}_C$.

Our algorithm for the jacobian of (V.4) must therefore produce an answer isomorphic to the E given above, and we will now verify this fact. We will also relate these models for J_C to what is found in [AKM+01].

V.7b. Finding the jacobian by the algorithm

To find the jacobian J_C of (V.4), we could, in principle, repeat the earlier work in this chapter. (In fact, the computer system *Singular* is capable of performing calculations over function fields that are finitely generated over either $\mathbf{Q}$ or a finite field of small characteristic—for example, line 1 of the code in table V.2 initializes a polynomial ring over the function field $\mathbf{Q}(a_{ij})$. Thus, for suitable k, we could view C as a curve over $k(a,b,c,m)$, where the symbols a, b, c, m are algebraically independent over k. But an attempt to run the code from tables V.2 and V.3, with obvious modifications for the present situation, exhausted our patience.)

We will take a different approach. By glancing at our work in §V.2, we go ahead and form the field extension $K = k(\zeta_3, \sqrt[3]{a}, \sqrt[3]{b}, \sqrt[3]{c})$, and then guess that the two matrices

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta_3 & 0 \\ 0 & 0 & \zeta_3^2 \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} 0 & \sqrt[3]{b/a} & 0 \\ 0 & 0 & \sqrt[3]{c/b} \\ \sqrt[3]{a/c} & 0 & 0 \end{bmatrix}.$$

will generate H_3. Indeed, this is the case: it is easy to verify that they preserve C, have no fixpoints on C, and their commutator is ζ_3.

The Molien series $\Phi_{H_3}(t)$ is the same as in §V.4, and carrying out a similar procedure as given there (we will omit the details), we choose the primary invariants

$$P_1 := xyz, \quad P_2 := ax^3 + by^3 + cz^3, \quad P_3 := abx^3y^3 + acx^3z^3 + bcy^3z^3,$$

and the secondary invariant $P_4 := ab^2x^3y^6 + a^2cx^6z^3 + bc^2y^3z^6$, and obtain

$$K[x,y,z]^{H_3(K)} \cong \frac{K[s_1,s_2,s_3,s_4]}{\langle 9a^2b^2c^2s_1^6 + abcs_1^3s_2^3 - 6abcs_1^3s_2s_3 + s_3^3 + 3abcs_1^3s_4 - s_2s_3s_4 + s_4^2 \rangle}.$$

Working modulo the ideal of C corresponds to $s_2 = -ms_1$, and we obtain

$$\mathrm{J}_C \cong \operatorname{Proj} \frac{k[s_1,s_3,s_4]}{\langle abc(9abc - m^3)s_1^6 + 6abcms_1^4s_3 + s_3^3 + 3abcs_1^3s_4 + ms_1s_3s_4 + s_4^2 \rangle}.$$

We find the points of hyperosculation on C, as in §V.3, by intersecting the hyperplanes fixed by M or by N with C. For example, we find the point $[0 : 1 : \sqrt[3]{-b/c}]$. Substituting the points of hyperosculation into $[P_1 :: P_3 :: P_4]$ (cf. the end of §V.4) gives us $[0 :: -b^2 :: b^3]$, $[0 :: -c^2 :: c^3]$, $[0 :: -a^2 :: a^3]$, which are all just $[0 :: -1 :: 1]$.

In summary, the jacobian of (V.4) is

$$\mathrm{J}_C \cong \operatorname{Proj} \frac{k[r,s,t]}{\langle abc(9abc - m^3)r^6 + 6abcmr^4s + s^3 + 3abcr^3t + mrst + t^2 \rangle}, \tag{V.6}$$

where variables r, s, t have degrees $(1; 2; 3)$, and the origin of the group law is the k-rational point $[0 :: -1 :: 1]$. We obtained J_C as an elliptic curve of degree 6 in the weighted projective plane $\mathbf{P}_k^{(1;2;3)} = \operatorname{Proj}\big(k[r,s,t]\big)$. To obtain a non-weighted equation, we now proceed as in §V.6b. The affine patch

$$\operatorname{Spec} \frac{k[u,v]}{\langle v^2 + muv + 3abcv + u^3 + 6abcmu + abc(9abc - m^3) \rangle} \subset \mathbf{A}_k^2 \tag{V.7}$$

gives us a Weierstrass model for J_C.

V.7c. Applying the Riemann–Roch algorithm

We will now apply the Riemann–Roch algorithm (which we learned from an example in [Con92]) to put the elliptic curve (V.5) into Weierstrass form, so that we may compare it with (V.7).

We must find functions $\wp_x, \wp_y$ with poles of order $2, 3$ at $P = [1 : -1 : 0]$ and no poles elsewhere on $E\colon x^3 + y^3 + abcz^3 + mxyz = 0$. We go to the affine patch where $x \neq 0$. Set $Y = y/x, Z = z/x$. Then we are looking at the point $P = (-1, 0)$ on $E\colon 1 + Y^3 + abcZ^3 + mYZ = 0$. We determine Z to be a uniformizer at $(-1, 0)$, and $1/Z$ to be a uniformizer at the three points on E where $x = 0$. Thus we must have

$$\wp_x = \frac{\text{quadratic polynomial in } Y \text{ and } Z}{Z^2}, \quad \wp_y = \frac{\text{cubic polynomial in } Y \text{ and } Z}{Z^3}.$$

The bound on the numerator degree comes from looking at the pole behavior of Y at points where $x = 0$: the denominator Z^2 contributes a zero of order 2 at those points, so the numerator can contribute a pole of order at most 2, since the end result should be regular at those points.

Since $\mathrm{L}(2P) = \langle 1, \wp_x \rangle$, we can adjust $\wp_x$ by a scalar multiple of $1 = Z^2/Z^2$; that is, the coefficient of Z^2 in the numerator of $\wp_x$ can be taken to be 0. We also need the numerator of $\wp_x$ to *not* vanish at P, yet *vanish* at the other two points Q_1, Q_2 on E where Z vanishes. These

conditions immediately give some relations on the coefficients of the numerator of $\wp_x$, and tell us the Y^2 coefficient is nonzero. Scaling, we assume it to be 1. If we then use the equation of E expressed locally at Q_1, Q_2, we can expand the numerator of $\wp_x$ in a series in Z to obtain the condition for the numerator to vanish *twice* at those two points. We ultimately determine:

$$\wp_x = \frac{Y^2 + \frac{m}{3}YZ - Y + \frac{m}{3}Z + 1}{Z^2}.$$

As for $\wp_y$, the equation of E itself allows us to eliminate the Y^3 term from the numerator, and $\mathrm{L}(3P) = \langle 1, \wp_x, \wp_y \rangle$ tells us we can eliminate the Z^3 term and the Y^2Z term (by subtracting off a multiple of $\wp_x$). Repeating the previous work, this time requiring *triple* vanishing at Q_1, Q_2, we obtain:

$$\wp_y = \frac{Y^2 + \frac{m}{3}YZ - Y + \frac{m}{3}Z + 1 + \frac{m^2}{9}Z^2}{Z^3}.$$

Riemann–Roch tells us that $\ell(6P) = 6$, yet certainly $\{\, 1, \wp_x, \wp_y, \wp_x^2, \wp_x\wp_y, \wp_x^3, \wp_y^2 \,\}$ all lie in $\mathrm{L}(6P)$, and by comparing with $\mathrm{L}(5P)$, we conclude that we can express $\wp_y^2$ as a linear combination of the rest. That is, there exist a_i satisfying:

$$\wp_y^2 + a_1\wp_x\wp_y + a_3\wp_y = a_0\wp_x^3 + a_2\wp_x^2 + a_4\wp_x + a_6.$$

This equation must hold identically on E, so if we expand this using our expressions for $\wp_x, \wp_y$ and use the equation of E repeatedly to eliminate all terms containing Y^3, then the coefficients we end up with must all be 0. From this we easily determine:

$$\wp_y^2 - \tfrac{m}{3}\wp_x\wp_y + abc\wp_y = \tfrac{1}{3}\wp_x^3 + \tfrac{abcm}{3}\wp_x + \tfrac{abc}{81}(m^3 - 27abc).$$

This is E in Weierstrass form. We eliminate the denominators with a linear change-of-variables to obtain

$$E\colon y^2 - mxy + 9abcy = x^3 + 9abcmx + (abcm^3 - 27a^2b^2c^2). \tag{V.8}$$

If we now apply the substitution $x \leftarrow u$ and $y \leftarrow (v - 3abc)$, then we obtain (V.7).

V.7d. Comparing with result from classical invariant theory

If, in addition to our standing assumption $\mathrm{char}(k) \neq 3$, we also assume $\mathrm{char}(k) \neq 2$, then we can compare (V.7) with what we would obtain from the formulas in [AKM$^+$01]. There it is shown that J_C has equation

$$y^2 = 4x^3 + 108Sx - 27T, \tag{V.9}$$

where

$$S = \tfrac{1}{6}abcm - \tfrac{1}{6^4}m^4, \quad \text{and} \quad T = a^2b^2c^2 - \tfrac{20}{6^3}abcm^3 - \tfrac{8}{6^6}m^6.$$

If we scale the linear term of (V.9) by 6^4, and the constant term by 6^6 (cf. [Sil99, §III.1]), then we obtain

$$y^2 = 4x^3 + 108(216abcm - m^4)x - 216(5832a^2b^2c^2 - 540abcm^3 - m^6). \tag{V.10}$$

If we instead start with (V.7), and complete the square and the cube (cf. [Sil99, §III.1]), then after cleaning up the denominators we also end up with (V.10).

CHAPTER VI

Example: a pair of quadrics

In the previous chapter, we worked through an example of using our algorithm in the case $n = 3$. In this chapter, we work through an example for $n = 4$ far enough to find the Heisenberg group H_4 and the points of hyperosculation, which demonstrates the following points:

- The ideal of our curve is no longer principal. Thus, whereas before with $I = \langle F \rangle$ we put the condition $F(A\mathbf{x}) \equiv 0$ modulo $F(\mathbf{x})$ to find matrices that preserve the curve, now we must find a Gröbner basis $\mathfrak{G}$ for I, and for each generator F of I, we require $F(A\mathbf{x})/\mathfrak{G} \equiv 0$, where $\cdot/\mathfrak{G}$ denotes the canonical form obtained by reducing modulo $\mathfrak{G}$.
- Since the parity of n is different, we must use a different method for finding the points of hyperosculation (cf. §IV.5).
- In the previous chapter's example, the Heisenberg group H_4 admitted a Schrödinger-like representation in the given coordinate system. That will *not* be the case presently.

In contrast to the previous chapter, this time around we will rely more on the computer, and we present computer code that, although more abstract, has the advantage of being easily adapted to different values of n.

VI.1. The curve

Let C be the intersection of the two quadrics in $\mathbf{P}^3_{\mathbf{Q}}$ defined by the matrices

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}.$$

That is,

$$C = \operatorname{Proj} \frac{\mathbf{Q}[w,x,y,z]}{\langle w^2+x^2+y^2+z^2, w^2+2x^2+3y^2+4z^2 \rangle}.$$

Note that C has no $\mathbf{Q}$-rational point: it does not even have a point over $\mathbf{R}$. We will now apply our algorithm to find the points of hyperosculation, the hyperplane configuration, and the jacobian J_C.

The code in table VI.1 confirms that C is a smooth degree 4 curve in $\mathbf{P}^3_{\mathbf{Q}}$ of genus 1. It is non-degenerate because none of the ideal generators is linear.

```
n=4
nMinusOne=n-1
ringPnMinusOne = QQ[w_0..w_nMinusOne]
f1=w_0^2+w_1^2+w_2^2+w_3^2
f2=w_0^2+2*w_1^2+3*w_2^2+4*w_3^2
idealC = ideal(f1,f2)
ringC = ringPnMinusOne / idealC
C = Proj ringC
dim C
codim singularLocus idealC
degree C
HH^1 OO_C
```

Table VI.1. This *Macaulay 2* code vets the input.

Remark. We didn't really need the computer: since the two matrices are diagonal, and their λ-equation (as in (III.9)) has distinct roots, the two quadrics intersect in a smooth curve of genus 1 (see [Eis95, §18.3, Example, p.463]).

The code in table VI.2 works out the conditions for a matrix

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ a_9 & a_{10} & a_{11} & a_{12} \\ a_{13} & a_{14} & a_{15} & a_{16} \end{bmatrix}$$

to preserve the curve, have determinant 1, and satisfy $A^n = -1$. (Thus, by §IV.4b, we are describing potential generators of H_4, not H_4 itself.) Note that, for sake of speed, the code uses a non-elimination term order for the initial computations, and then uses a *Gröbner basis conversion* process (cf. [CLO98, §2.3]) to obtain a description of the ideal in elimination term order. We end up with the following conditions:

$$\begin{aligned}
a_{16}^5 + a_{16} &= 0, & a_{15}a_{16} &= 0, & a_{14}a_{16} &= 0, & a_{14}a_{15} &= 0, \\
3a_{15}^5 + a_{15} &= 0, & a_{13}a_{16} &= 0, & a_{13}a_{15} &= 0, & a_{13}a_{14} &= 0, \\
3a_{14}^5 - a_{14} &= 0, & a_{12}a_{16} &= 0, & a_{12}a_{14} &= 0, & a_{12}a_{13} &= 0, \\
a_{13}^4 - 3a_{14}^4 + 3a_{15}^4 + a_{16}^4 + 1 &= 0, & a_{11}a_{15} &= 0, & a_{11}a_{14} &= 0, & a_{11}a_{13} &= 0, \\
3a_{12}a_{15}^4 + a_{12} &= 0, & a_{11}a_{12} &= 0, & a_{10}a_{16} &= 0, & a_{10}a_{15} &= 0, \\
a_{12}^2 - 3a_{15}^2 &= 0, & a_{10}a_{14} &= 0, & a_{10}a_{12} &= 0, & a_{10}a_{11} &= 0, \\
a_{11}a_{16}^4 + a_{11} &= 0, & a_9a_{16} &= 0, & a_9a_{15} &= 0, & a_9a_{13} &= 0, \\
a_{11}^2 - a_{16}^2 &= 0, & a_9a_{12} &= 0, & a_9a_{11} &= 0, & a_9a_{10} &= 0, \\
a_{10}^2 - a_{13}^2 &= 0, & a_8a_{16} &= 0, & a_8a_{15} &= 0, & a_8a_{13} &= 0, \\
3a_9a_{14}^4 - a_9 &= 0, & a_8a_{12} &= 0, & a_8a_{11} &= 0, & a_8a_{10} &= 0, \\
a_9^2 - 3a_{14}^2 &= 0, & a_7a_{16} &= 0, & a_7a_{15} &= 0, & a_7a_{14} &= 0, \\
3a_8a_{14}^4 - a_8 &= 0, & a_7a_{12} &= 0, & a_7a_{11} &= 0, & a_7a_9 &= 0, \\
a_8^2 + 3a_{14}^2 &= 0, & a_7a_8 &= 0, & a_6a_{15} &= 0, & a_6a_{14} &= 0, \\
a_7^2 - a_{13}^2 &= 0, & a_6a_{13} &= 0, & a_6a_{12} &= 0, & a_6a_{10} &= 0, \\
a_6a_{16}^4 + a_6 &= 0, & a_6a_9 &= 0, & a_6a_8 &= 0, & a_6a_7 &= 0, \\
a_6^2 - a_{16}^2 &= 0, & a_5a_{16} &= 0, & a_5a_{14} &= 0, & a_5a_{13} &= 0, \\
3a_5a_{15}^4 + a_5 &= 0, & a_5a_{11} &= 0, & a_5a_{10} &= 0, & a_5a_9 &= 0, \\
a_5^2 + 3a_{15}^2 &= 0, & a_5a_8 &= 0, & a_5a_7 &= 0, & a_5a_6 &= 0. \\
a_4 - a_7a_{10}a_{13}^3 &= 0, & & & & & & \\
a_3 + a_8a_9a_{14}^3 &= 0, & & & & & & \\
a_2 + a_5a_{12}a_{15}^3 &= 0, & & & & & & \\
a_1 - a_6a_{11}a_{16}^3 &= 0, & & & & & &
\end{aligned}$$

```
// Lines marked ‘‘//[**]’’ are specific to the parity of n,
// or to the particular value of n, or to the particular equations
// being used in this example. Adjust these lines as necessary.

int n = 4; //[**]

ring ring_PnMinusOne = 0,(x(0..(n-1))),dp;
poly f1 = x(0)^2+x(1)^2+x(2)^2+x(3)^2; //[**]
poly f2 = x(0)^2+2*x(1)^2+3*x(2)^2+4*x(3)^2; //[**]
ideal ideal_C = f1,f2; //[**]

option(redSB); // Now ‘‘groebner’’ will reduce result...
ideal_C = groebner(ideal_C);

int n_squared = n*n;
ring ring_combined = (0,a(1..n_squared)),(x(0..(n-1))),dp;
ideal ideal_C_combined = imap(ring_PnMinusOne,ideal_C);
// Singular must be reminded it is groebner:
ideal_C_combined = groebner(ideal_C_combined);
matrix A[n][n] = a(1..(n_squared));
matrix vars[n][1] = x(0..(n-1));
matrix newvars = A * vars;
newvars;
map map_A = ring_combined,newvars[1,1],newvars[2,1],newvars[3,1],newvars[4,1]; //[**]

ideal_C_combined;

poly varprod = 1;
int i;
for (i = 0; i < n; i++) {
  varprod = varprod * x(i);
  }

ring ring_coefficients = 0,(a(1..(n_squared))),dp;
ideal ideal_conditions;

matrix AA = imap(ring_combined,A);
poly determinant_one = 1 - det(AA);
ideal_conditions = ideal_conditions + determinant_one;

// Extra (optional) conditions: (n)th power should be +1 or -1.
// Note: For n even, we won’t get a group, but we’ll find generators...
LIB "matrix.lib"; // Lets us call power(), unitmat(), ...
matrix AA_nth_power = power(AA,n) + (-1)^n * unitmat(n);
int j;
for (i = 1; i <= n; i++) {
  for (j = 1; j <= n; j++) {
    ideal_conditions = ideal_conditions + AA_nth_power[i,j];
    }
  }

setring ring_combined;
int eqn_count = ncols(ideal_C_combined);
for (i = 1; i <= eqn_count; i++) {
  setring ring_combined;
  poly generator = ideal_C_combined[i];
  poly mapped_generator = map_A(generator);
  mapped_generator;
  poly reduced = reduce(mapped_generator, ideal_C_combined);
  reduced;
  matrix coefficients = coef(reduced,varprod);
  int coef_count = ncols(coefficients);
  for (j = 1; j <= coef_count; j++) {
    setring ring_combined;
    poly coefficient = coefficients[2,j];
    setring ring_coefficients;
    poly mapped_coefficient = imap(ring_combined,coefficient);
    mapped_coefficient = cleardenom(mapped_coefficient);
    ideal_conditions = ideal_conditions + mapped_coefficient;
    }
  }

setring ring_coefficients;
ideal_conditions = groebner(ideal_conditions);
ring ring_coefficients_lex = 0,(a(1..(n_squared))),lp;
ideal ideal_conditions_lex = fglm(ring_coefficients,ideal_conditions);
ideal_conditions_lex;
```

Table VI.2. This *Singular* code find equations describing generators of H_4.

To solve the system, let $K = \mathbf{Q}(\zeta_8, \sqrt[4]{3})$, where ζ_8 is a symbol satisfying $\zeta_8^4 = -1$ and $\sqrt[4]{3}$ is a symbol satisfying $(\sqrt[4]{3})^4 = 3$. Modulo the 4th roots of unity $\{\,1, \zeta_8^2, \zeta_8^4, \zeta_8^6\,\}$, we find 12 solutions (the signs must be assigned so that the determinant is 1):

$$\begin{bmatrix} 0 & 0 & 0 & \pm\zeta_8 \\ 0 & 0 & \pm\zeta_8 & 0 \\ 0 & \pm\zeta_8 & 0 & 0 \\ \zeta_8 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & \pm\zeta_8^2/\sqrt[4]{3} & 0 \\ 0 & 0 & 0 & \pm\zeta_8^2\sqrt[4]{3} \\ \pm\sqrt[4]{3} & 0 & 0 & 0 \\ 0 & 1/\sqrt[4]{3} & 0 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & \pm\zeta_8^3/\sqrt[4]{3} & 0 & 0 \\ \pm\zeta_8^3\sqrt[4]{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & \pm\zeta_8\sqrt[4]{3} \\ 0 & 0 & \zeta_8/\sqrt[4]{3} & 0 \end{bmatrix}.$$

Their squares are the elements of order 2 in $\mathbf{PGL}_4$ (the signs must be assigned so that the determinant is 1 and so that the matrix is not a scalar):

$$\begin{bmatrix} \pm\zeta_8^2 & 0 & 0 & 0 \\ 0 & \pm\zeta_8^2 & 0 & 0 \\ 0 & 0 & \pm\zeta_8^2 & 0 \\ 0 & 0 & 0 & \zeta_8^2 \end{bmatrix}.$$

We arbitrarily choose two matrices of order 4 whose commutator is a primitive 4th root of unity:

$$M = \begin{bmatrix} 0 & 0 & 0 & -\zeta_8 \\ 0 & 0 & \zeta_8 & 0 \\ 0 & \zeta_8 & 0 & 0 \\ \zeta_8 & 0 & 0 & 0 \end{bmatrix}, \quad N = \begin{bmatrix} 0 & 0 & \zeta_8^2/\sqrt[4]{3} & 0 \\ 0 & 0 & 0 & \zeta_8^2\sqrt[4]{3} \\ -\sqrt[4]{3} & 0 & 0 & 0 \\ 0 & 1/\sqrt[4]{3} & 0 & 0 \end{bmatrix}.$$

We have $M\,N\,M^{-1}N^{-1} = \zeta_8^2$. The Heisenberg group is

$$H_4 = \{\,\zeta_8^{2a} M^b N^c \,:\, a, b, c \in \mathbf{Z}/4\mathbf{Z}\,\}.$$

VI.2. Finding the $[-1]$ matrices

By running code similar to before, but replacing the condition $A^4 = -1$ with $A^2 = 1$ and also trying again (cf. §IV.4c) with $A^2 = \zeta_8^2$ or simply $A^4 = -1$, and then checking that each matrix has 4 fixpoints on C, we find the following 16 matrices (the signs must be assigned so that the determinant is 1):

$$\begin{bmatrix} 0 & 0 & \pm\zeta_8^3/\sqrt[4]{3} & 0 \\ 0 & 0 & 0 & \pm\zeta_8^3\sqrt[4]{3} \\ \pm\zeta_8\sqrt[4]{3} & 0 & 0 & 0 \\ 0 & \zeta_8/\sqrt[4]{3} & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & \pm\zeta_8^2/\sqrt[4]{3} & 0 & 0 \\ \pm\zeta_8^2\sqrt[4]{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & \pm\sqrt[4]{3} \\ 0 & 0 & 1/\sqrt[4]{3} & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 0 & 0 & \pm\zeta_8^2 \\ 0 & 0 & \pm\zeta_8^2 & 0 \\ 0 & \pm\zeta_8^2 & 0 & 0 \\ \zeta_8^2 & 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} \pm\zeta_8 & 0 & 0 & 0 \\ 0 & \pm\zeta_8 & 0 & 0 \\ 0 & 0 & \pm\zeta_8 & 0 \\ 0 & 0 & 0 & \zeta_8 \end{bmatrix}.$$

VI.3. Finding a point of hyperosculation

Since n is even, the points of hyperosculation are the 16 fixpoints of 4 of the $[-1]$ matrices (cf. §III.9a). We simply take each matrix, look for a fixpoint, look for the osculating hyperplane at that fixpoint, and check whether it hyperosculates; if not, we move on to the next matrix.

Let us look at the matrix

$$T = \begin{bmatrix} -\zeta_8 & 0 & 0 & 0 \\ 0 & \zeta_8 & 0 & 0 \\ 0 & 0 & \zeta_8 & 0 \\ 0 & 0 & 0 & \zeta_8 \end{bmatrix}.$$

It fixes the isolated point $[1:0:0:0]$ (which is not on C) and fixes every point in the eigenspace spanned by $[0:1:0:0]$, $[0:0:1:0]$, and $[0:0:0:1]$. That eigenspace is just the hyperplane $w=0$, which intersects C in the 4 points

$$[0:1:\pm\sqrt{-2}:\pm 1].$$

Let

$$O = [0:1:\sqrt{-2}:1].$$

It is easy to see that the hyperosculating hyperplane at O (assuming it exists) must be fixed by T. The hyperplanes fixed by T correspond to the eigenvectors of T^{t}. We determine that T fixes the isolated hyperplane $w=0$ (which we just saw cannot be the hyperosculating hyperplane at O), and T also fixes all the hyperplanes spanned by $x=0$, $y=0$, $z=0$ (these are all the hyperplanes containing the point $[1:0:0:0]$).

We thus look at hyperplanes corresponding to $\ell = [0:*:*:*]^{\mathsf{t}}$ that go through O, i.e., the hyperplanes $sx+ty-(1+t\sqrt{-2})z=0$, where $[s:t]\in \mathbf{P}^1_{\mathbf{Q}}(\bar{\mathbf{Q}})$. We look for $[s:t]$ values that maximize the number of times the hyperplane meets the curve at O. We eventually discover, for $[s:t]=[1:2\sqrt{-2}]$, the hyperplane meets C only at O. Thus O is a point of hyperosculation.

VI.4. The invariant theory of H_4

To eventually describe

$$\mathrm{J}_C \cong \operatorname{Proj} \frac{\mathbf{Q}[w,x,y,z]\cap K[w,x,y,z]^{H_4(K)}}{I\cap K[w,x,y,z]^{H_4(K)}},$$

which we will not do here, we would first need to get our hands on $K[w,x,y,z]^{H_4(K)}$. We will now indicate how that calculation commences. The Molien series

$$\begin{aligned}\Phi_{H_4}(t) &= \tfrac{1}{64}\sum_{\tau\in H_4(K)} \frac{1}{\det(\mathsf{id}-t\tau)} \\ &= \frac{1-t^4+8t^2-t^{12}+t^{16}}{(t^4-1)^4(t^4+1)} \\ &= 1+2t^4+12t^8+29t^{12}+63t^{16}+112t^{20}+186t^{24}+283t^{28}+\dots\end{aligned}$$

tells us there are two linearly independent invariants in degree 4, twelve in degree 8, and so on. We can verify that the following four polynomials,

$$\begin{aligned}P_1 &= wxyz,\\ P_2 &= 3w^4-x^4+y^4-3z^4,\\ P_3 &= x^4y^4+9w^4z^4,\\ P_4 &= (x^2y^2+3w^2z^2)(w^2y^2+x^2z^2),\end{aligned}$$

are algebraically independent invariants with $(0,0,0,0)$ being the only solution to $P_1=0$, $P_2=0$, $P_3=0$, and $P_4=0$. Thus they serve as primary invariants, and we rewrite the Molien series in the form

$$\Phi_{H_4}(t) = \frac{1+7t^8+7t^{12}+t^{20}}{(1-t^4)^2(1-t^8)^2}.$$

We see that there are 7 secondary invariants in degree 8, 7 in degree 12, and 1 in degree 20. We have not carried out the calculation to find those secondary invariants.

APPENDIX A

Facts about curves of genus 1

In this appendix, we review facts concerning k-curves of genus 1, where k is a perfect field. Our results are mostly obtained from the theory of elliptic curves, as presented in [Sil99], by separating an elliptic curve into two aspects: the underlying curve of genus 1, and the curve's jacobian.

A.1. Consequences of Riemann–Roch on curves of genus 1

We recall the Riemann–Roch theorem for a curve of arbitrary genus.

Theorem (Riemann–Roch)**.** *Let X be a k-curve of genus g, let K be a canonical divisor, and let D be a k-rational divisor on X. Let $\ell_k(\cdot) = \dim_k \mathrm{L}_k(\cdot) = \dim_k \mathbf{H}^0\big(X, \mathcal{O}(\cdot)\big)$. Then*

$$\ell_k(D) - \ell_k(K - D) = \deg(D) + 1 - g.$$

Proof. Combine [Har77, IV.1.3] with [Sil99, II.5.8.1]). □

We now return to the context of C being a curve of genus 1, and explore the consequences of the above theorem.

A.1a. The canonical divisor and differential forms

Substituting $D = 0$ and $D = K$ into Riemann–Roch gives

$$\ell_k(K) = 1 \quad \text{and} \quad \deg(K) = 0, \quad \text{whence} \quad K \sim 0.$$

In words: *there exist global differential forms, any two differ by a scalar multiple, and they are nowhere vanishing.*

Any choice of nonzero global differential form is usually called "the invariant differential", referring to the fact that they are invariant under translation by the action of the jacobian J_C on C; this follows from [Sil99, III.5.1].

A.1b. Dimension of complete linear systems

Corollary (Riemann–Roch on curves of genus 1)**.** *Let C be a k-curve of genus 1, and D a k-rational divisor. Then:*

$$\ell_k(D) - \ell_k(-D) = \deg(D).$$

The relationship between the degree and dimension may be summarized as follows. The first three statements hold for all curves, the last two for curves of genus 1:

- If $\deg(D) < 0$, then $\ell_k(D) = 0$.
- If $\deg(D) = 0$ and $D \not\sim 0$, then $\ell_k(D) = 0$.
- If $\deg(D) = 0$ and $D \sim 0$, then $\ell_k(D) = 1$.
- If $\deg(D) > 0$, then $\ell_k(D) = \deg(D)$.
- If D is effective, then $\ell_k(D) \geq 1$.

A.1c. No two points are linearly equivalent

Let $P, Q \in C(\bar{k})$ be two distinct points. If we had $P \sim Q$, then $P - Q$ would be the divisor of a function, implying the existence of a non-constant function in $\mathrm{L}(Q)$, contradicting $\ell_{\bar{k}}(Q) = 1$.

A.1d. Effective representatives

For D a k-rational divisor, the fact

$$\deg(D) > 0 \quad \Longrightarrow \quad \ell_k(D) = \deg(D)$$

tells us that the complete linear system $|D|_k$ (which comprises effective k-rational divisors linearly equivalent to D) is nonempty whenever $\deg(D) > 0$. In other words: *if D has positive degree, then the class $[D]$ has an effective k-rational representative.*

Thus, if D has degree 1, then the class $[D]$ is represented by a k-rational point. But, by A.1c, no two distinct points are linearly equivalent. Thus: *if D has degree 1, then the class $[D]$ has a* unique *k-rational point as representative.*

The last statement is true more generally. We no longer require D to be k-rational, but we do require the class $[D]$ to be k-rational, which means $D^\sigma \sim D$ for all Galois automorphisms σ. Temporarily taking our ground field to be $\bar{k}$, the previous paragraph tells us that $[D]$ has a unique $\bar{k}$-rational point P as representative. But then k-rationality of $[P]$ implies $P^\sigma \sim P$, and uniqueness forces $P^\sigma = P$. Thus P is k-rational. In short: *each k-rational divisor class of degree 1 has a unique k-rational point as representative.*

Warning. It is in general *not* the case that the divisor class group $\mathrm{Cl}_k(C)$ comprises k-rational divisors modulo linear equivalence. An element of $\mathrm{Cl}_k(C)$ is a k-rational class, i.e., a class $[D]$ so that each representative D satisfies $D^\sigma \sim D$; such a class need not admit a k-rational representative. However, as we saw above, on a curve of genus 1, each k-rational class of degree 1 does admit a k-rational representative.

A.2. The group law

The set $C(k)$ of k-rational points on C may be empty. When it is nonempty, then choosing any $O \in C(k)$ leads to the following composition rule: for $P, Q \in C(k)$, define $P \oplus Q$ to be the unique k-rational point (see A.1d) linearly equivalent to the degree 1 k-rational divisor $P + Q - O$.

The calculation

$$(P \oplus Q) \oplus R \sim (P \oplus Q) + R - O \sim (P + Q - O) + R - O = (P + Q + R) - 2O$$

renders moot the order in which P, Q, R appear and the order in which they are combined, showing the binary operation "$\oplus$" to be both commutative and associative. It is furthermore immediate that O is an identity element for this operation. Finally, given $P \in C(k)$, let $\ominus P$ be the unique k-rational point linearly equivalent to $2O - P$. Then $\ominus P$ is the additive inverse of P:

$$P \oplus (\ominus P) \sim P + (\ominus P) - O \sim P + (2O - P) - O = O.$$

Thus the operation "$\oplus$" defines an abelian group law on the set $C(k)$ with O as identity element.

In summary: *when $C(k)$ is nonempty, each choice of $O \in C(k)$ leads to an abelian group law on $C(k)$ with O as identity element.*

This abstract description of the group law is intrinsic to the curve. The reader may be familiar with the extrinsic "chord-and-tangent law" defined on nonsingular cubic curves in $\mathbf{P}^2_k$. (A description, along with pictures, appears in practically every book on elliptic curves.) That law has the following description: fix any $O \in C(k)$ to be the identity element, and then agree that three points in $C(k)$ sum to O if and only if they are collinear. Not every curve of genus 1 occurs as a cubic in $\mathbf{P}^2_k$. But for the ones that do, we have the following result:

Theorem A.2.1. *The intrinsic and extrinsic laws agree.*

Proof. Fix $O \in C(k)$. For $P, Q \in C(k)$, their intrinsic sum is the unique point linearly equivalent to $P + Q - O$. Now let "$\oplus$" denote the extrinsic law. If we show $P \oplus Q \sim P + Q - O$, then we have shown the two laws to agree.

Let $R \in C(k)$ be such that P, Q, R are collinear. (In other words, take the line through P and Q and find its third point of intersection with the curve. If $P = Q$, then use the tangent line.) The extrinsic law says $P \oplus Q \oplus R = O$. Thus R is the inverse of $P \oplus Q$. Let $S \in C(k)$ be such that O, R, S are collinear. Then S must be $P \oplus Q$. The two lines define a rational function that gives $P + Q + R \sim O + R + S$, whence $P + Q - O \sim S = P \oplus Q$. □

A.2a. Isogenies

When $C(k)$ is nonempty and $O \in C(k)$ has been fixed, the pair (C, O) is called an **elliptic curve**. A curve morphism

$$(C, O) \longrightarrow (C', O') \quad \text{with} \quad O \longmapsto O'$$

is called an **isogeny**. The **trivial isogeny** is the constant map with value O'. Non-trivial isogenies are finite morphisms and thus have a **degree**. Two elliptic curves are **isogenous** if there exists a non-trivial isogeny between them.

Theorem A.2.2. *Every k-isogeny $C \to C'$ is necessarily a group homomorphism $C(k) \to C'(k)$.*

Proof. Let $P, Q \in C(k)$. Then $P \oplus Q$ is the unique point linearly equivalent to $P + Q - O$. Since ϕ_* takes principal divisors to principal divisors, we have $\phi(P \oplus Q) \sim \phi(P) + \phi(Q) - \phi(O)$, whence $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$. □

Corollary A.2.3. *Any k-morphism $C \to C$ with a fixpoint $O \in C(k)$ is automatically a group endomorphism $C(k) \to C(k)$ of the elliptic curve (C, O).*

The above result is an ingredient into the structure theorem for morphisms of curves of genus 1. (See A.4.1.)

A.3. The jacobian action

Recall that a k-rational point on the jacobian J_C is the same thing as a k-rational divisor class on C of degree 0. In other words, $\mathrm{J}_C(k) = \mathrm{Cl}^0_k(C)$, and $\mathrm{J}_C(\bar{k}) = \mathrm{Cl}^0_{\bar{k}}(C)$. There is a canonical action of J_C on C, whose behavior on $\bar{k}$-valued points is:

$$\begin{aligned} \mathrm{J}_C(\bar{k}) \times C(\bar{k}) &\longrightarrow C(\bar{k}), \\ \big([Z], P\big) &\longmapsto \text{unique point linearly equivalent to } [Z + P]. \end{aligned}$$

Proposition A.3.1. *The action of J_C on C is simply transitive (and thus faithful and fixpoint-free).*

Proof. Let $P, Q \in C(\bar{k})$. The action is transitive since $[Q - P] \in \mathrm{J}_C(\bar{k})$ sends P to Q. Let $[Z] \in \mathrm{J}_C(\bar{k})$ also have that property. Then $Z + P \sim Q$, whence $[Z] = [Q - P]$. □

Thus J_C comprises a part of the group of curve automorphisms of C. The precise structure of that group is explained in A.4c.

A.3a. Torsion packets on curves of genus 1

Since J_C acts on C, for each $n \geq 1$ also $\mathrm{J}_C[n]$ acts on C, where $\mathrm{J}_C[n]$ is the kernel of multiplication-by-n:

$$\mathrm{J}_C[n](\bar{k}) = \mathrm{J}_C(\bar{k})[n].$$

Definition. An **n-torsion packet** on C is a collection of points in $C(\bar{k})$ that comprises one orbit under the action of $\mathrm{J}_C[n](\bar{k})$.

Thus we see: the set of n-torsion packets is in one-to-one correspondence with $(C/\mathrm{J}_C[n])(\bar{k})$.

If $P, Q \in C(\bar{k})$ lie in the same n-torsion packet, then $P - Q$ defines a class in $\mathrm{J}_C(\bar{k})[n]$, whence $nP \sim nQ$. Thus another description: *an n-torsion packet is a maximal collection of points in $C(\bar{k})$ so that if P, Q are any two of them, then $nP \sim nQ$.*

Another way to think about n-torsion packets is as follows. Let $T \subset C(\bar{k})$ be an n-torsion packet. Choosing any $O \in T$, we get the elliptic curve $(C_{\bar{k}}, O)$. Then T is simply the n-torsion on that curve, i.e., $T = (C_{\bar{k}}, O)[n](\bar{k})$, and the other n-torsion packets on C are the cosets of T in $(C_{\bar{k}}, O)(\bar{k})$. In summary, talking about an n-torsion packet on C is tantamount to saying, "here is a collection of points which *would* be the n-torsion *were* we to choose one of them as group law origin".

Proposition A.3.2. *The size of each n-torsion packet is the constant $\big|\mathrm{J}_C[n](\bar{k})\big|$. In particular, if $\mathrm{char}(k) \nmid n$, then each n-torsion packet comprises n^2 distinct elements of $C(\bar{k})$.*

Proof. The first statement follows from the action of J_C on C being simply transitive. The hypothesis $\mathrm{char}(k) \nmid n$ guarantees that $\mathrm{J}_C(\bar{k})[n]$ has order n^2. (As a group, it is isomorphic to $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, but as a $\mathrm{Gal}(\bar{k}/k)$-module, its structure can be more complicated.) □

Proposition A.3.3. *The Galois conjugate of an n-torsion packet is again an n-torsion packet. In other words, each n-torsion packet is either permuted among itself or swapped as a whole with some other n-torsion packet.*

Proof. Any point in an n-torsion packet determines the packet by taking that point's orbit under the action of $\mathrm{J}_C[n]$. Since $\mathrm{J}_C[n]$ and the action of J_C on C are both defined over k, what happens to an n-torsion packet is entirely determined by what happens to one of its representative points. Such a point either stays within the packet or moves to a different packet. The rest of the packet follows along. □

A.4. Morphisms

A.4a. Morphisms between curves of genus 1

In A.3, we saw that J_C acts simply transitively on C. Thus each $[Z] \in \mathrm{J}_C(\bar{k})$ gives rise to a distinct fixpoint-free curve automorphism of C. Applying this to two curves C and C' of genus 1, we obtain the following description of $\mathrm{Hom}(C_{\bar{k}}, C'_{\bar{k}})$.

Theorem A.4.1. *Fix choices of $O \in C(\bar{k})$ and $O' \in C'(\bar{k})$. Then each curve morphism $C_{\bar{k}} \to C'_{\bar{k}}$ can be decomposed uniquely in the form $\tau \circ \phi$, where $\tau \in \mathrm{J}_{C'}(\bar{k})$ and $\phi \in \mathrm{Hom}\big((C_{\bar{k}}, O), (C'_{\bar{k}}, O')\big)$. In other words, every morphism is a homomorphism followed by a translation.*

Proof. Call the morphism η. For existence of the decomposition, write $\eta = [\eta(O) - O'] \circ \big([O' - \eta(O)] \circ \eta\big)$. Since $[O' - \eta(O)] \circ \eta$ sends $O \mapsto O'$, it is a homomorphism from the elliptic curve (C, O) to the elliptic curve (C', O'). (That was A.2.2.) For uniqueness, say $\tau \circ \phi = \tau' \circ \phi'$. Then $\phi = \tau^{-1} \circ \tau' \circ \phi'$. Thus $\tau^{-1} \circ \tau'$ fixes O'. By the simple transitivity of the $\mathrm{J}_{C'}$-action, we must have $\tau = \tau'$, whence also $\phi = \phi'$. □

Remark. Instead of post-translating on C' after applying ϕ, one might hope to instead pre-translate on C. That works only if the morphism $C \to C'$ is assumed non-constant.

One might ask: what about morphisms $C \to C'$ that are k-rational? Is it necessarily the case that ϕ and τ in the theorem will also be k-rational? The answer is *no*: we have $\tau \circ \phi = (\tau \circ \phi)^\sigma = \tau^\sigma \circ \phi^\sigma$, but ϕ^σ need not take $O \mapsto O'$. But if O and O' are k-rational, then ϕ^σ does take $O \mapsto O'$, whence $\phi = \phi^\sigma$ and $\tau = \tau^\sigma$. We have proved:

Theorem. *Fix choices of $O \in C(k)$ and $O' \in C'(k)$, assuming they exist. Then each k-rational curve morphism $C \to C'$ can be decomposed uniquely in the form $\tau \circ \phi$, where $\tau \in \mathrm{J}_{C'}(k)$ and $\phi \in \mathrm{Hom}_k\big((C, O), (C', O')\big)$. In other words, every k-rational morphism is a k-rational homomorphism followed by a k-rational translation.*

A.4b. Endomorphisms of curves of genus 1

By the above results, we obtain the following description of morphisms $C_{\bar{k}} \to C_{\bar{k}}$, i.e., of $\mathrm{End}(C_{\bar{k}})$.

Theorem A.4.2. *Fix a choice of $O \in C(\bar{k})$. Then each curve morphism $C_{\bar{k}} \to C_{\bar{k}}$ can be decomposed uniquely in the form $\tau \circ \phi$, where $\phi \in \mathrm{End}(C_{\bar{k}}, O)$ and $\tau \in \mathrm{J}_C(\bar{k})$.*

Proof. Follows immediately from A.4.1. □

Remark. It would be nice to better elucidate the structure of the monoid $\mathrm{End}(C_{\bar{k}})$ as some kind of product between $\mathrm{End}(C_{\bar{k}}, O)$ and $\mathrm{J}_C(\bar{k})$. Unfortunately, the composition law appears to have no simple description. Given $\tau\phi$ and $\tau'\phi'$, how does one write $\tau\phi\tau'\phi$ in the desired form? As we'll see in the next section, when we restrict attention to automorphisms, we'll obtain a semidirect product.

Concerning k-rational morphisms $C \to C$, similar to before we can say:

Theorem. *Fix a choice of $O \in C(k)$, assuming one exists. Then each k-rational curve morphism $C \to C$ can be decomposed uniquely in the form $\tau \circ \phi$, where $\tau \in \mathrm{J}_C(k)$ and $\phi \in \mathrm{End}_k(C, O)$.*

To finish the story, we need to understand the structure of the endomorphism ring $\mathrm{End}(C_{\bar{k}}, O)$. Lying in there are the multiplication-by-n maps $[n]$, thus putting $\mathbf{Z} \subseteq \mathrm{End}(C_{\bar{k}}, O)$. When there is more than this, we say that the elliptic curve $(C_{\bar{k}}, O)$ has **complex multiplication**. The possibilities are as follows.

Theorem. *Fix $O \in C(\bar{k})$. Then $\mathrm{End}(C_{\bar{k}}, O)$ is one of the following:*

(1) $\mathbf{Z}$*;*

(2) *an order in the ring of integers of an imaginary quadratic extension of* $\mathbf{Q}$*;*

(3) *an order in a definite quaternion algebra over* $\mathbf{Q}$*.*

If k is a finite field, then the first possibility is ruled out. If k has characteristic 0, then the third possibility is ruled out.

Proof. See [Sil99, III.9]. □

A morphism $C_{\bar{k}} \to C_{\bar{k}}$ decomposed as above as $\tau \circ \phi$ is called a **pure translation** when $\phi = \mathsf{id}$. Thus $\mathrm{J}_C(\bar{k})$ is the group of pure translations of C.

Theorem A.4.3. *A non-identity morphism $C_{\bar{k}} \to C_{\bar{k}}$ is fixpoint-free if and only if it is a pure translation.*

Proof. That non-identity pure translations are fixpoint-free was explained in section A.3. For the other direction, we will establish the contrapositive. Assume that $\tau \circ \phi$ is a morphism with $\phi \neq \mathsf{id}$. We must show that the morphism has a fixpoint. The elliptic curve endomorphism $\mathsf{id} - \phi$ of $(C_{\bar{k}}, O)$ is non-constant whence surjective. Furthermore, the map τ corresponds to a translation map on $(C_{\bar{k}}, O)$, say by the point P. Since $\mathsf{id} - \phi$ is surjective, there exists $Q \in C(\bar{k})$ with $Q - \phi(Q) = P$. Then we have $(\tau \circ \phi)(Q) = P + \phi(Q) = Q$, showing $\tau \circ \phi$ to have a fixpoint. □

Corollary A.4.4. *A fixpoint-free morphism $C_{\bar{k}} \to C_{\bar{k}}$ is an automorphism.*

Remark. Fixpoints are discussed further in section A.4e.

A.4c. Automorphisms of curves of genus 1

Now we specialize to the case of isomorphisms $C_{\bar{k}} \to C_{\bar{k}}$, i.e., we describe $\mathrm{Aut}(C_{\bar{k}})$.

Theorem A.4.5. *Fix a choice of $O \in C(\bar{k})$. Then the curve automorphism group of $C_{\bar{k}}$ is*

$$\mathrm{Aut}(C_{\bar{k}}) = \mathrm{J}_C(\bar{k}) \rtimes \mathrm{Aut}(C_{\bar{k}}, O).$$

Proof. The unique decomposition aspect follows immediately from A.4.1. The semidirect product structure is evident by computing the group law: given $\tau \circ \phi$ and $\tau' \circ \phi'$, their composition $\tau\phi\tau'\phi'$ may be written $\tau(\phi\tau'\phi^{-1})\phi\phi'$, and now we merely have to convince ourselves that $\phi\tau'\phi^{-1}$ is a pure translation. In other words, we must convince ourselves that $\mathrm{J}_C(\bar{k})$ is a normal subgroup of $\mathrm{Aut}(C_{\bar{k}})$.

Let $[Z] \in \mathrm{J}_C(\bar{k})$ and $\phi \in \mathrm{Aut}(C_{\bar{k}})$. The action of $[Z]$ on $C(\bar{k})$ is to take any point $P \in C(\bar{k})$ to the unique point representing the divisor $Z + P$. What does $\phi[Z]\phi^{-1}$ do? First P goes to $\phi^{-1}(P)$, then $[Z]$ carries that to the unique point linearly equivalent to $Z + \phi^{-1}(P)$, and thus ϕ carries it to the unique point linearly equivalent to $\phi_*(Z) + P$. In short, $\phi \circ [Z] \circ \phi^{-1}$ is the same as $[\phi_* Z]$. □

Remark A.4.6. As described in the proof, the semidirect product structure tells us how to combine two automorphisms:

$$\big([Z], \phi\big) \circ \big([Z'], \phi'\big) = \big([Z] + [\phi_* Z'], \phi \circ \phi'\big).$$

Concerning k-rational isomorphisms $C \to C$, similar to before we can say:

Theorem. *Fix a choice of $O \in C(k)$, assuming one exists. Then the group of k-rational curve automorphisms of C is:*

$$\mathrm{Aut}_k(C) = \mathrm{J}_C(k) \rtimes \mathrm{Aut}_k(C, O).$$

To finish the story, we need to understand the structure of the automorphism group $\mathrm{Aut}(C_{\bar{k}}, O)$.

Theorem A.4.7. *The structure of $\mathrm{Aut}(C_{\bar{k}}, O)$ depends on the j-invariant of C and the characteristic of k:*

$$\mathrm{Aut}(C_{\bar{k}}, O) = \begin{cases} \boldsymbol{\mu}_2(\bar{k}), & \text{if } j(C) \neq 0, 12^3 \text{ and } \mathrm{char}(k) \neq 2; \\ \boldsymbol{\mu}_4(\bar{k}), & \text{if } j(C) = 12^3 \text{ and } \mathrm{char}(k) \neq 2, 3; \\ \boldsymbol{\mu}_6(\bar{k}), & \text{if } j(C) = 0 \text{ and } \mathrm{char}(k) \neq 2, 3; \\ C_2, & \text{if } j(C) \neq 0\,(= 12^3) \text{ and } \mathrm{char}(k) = 2; \\ C_4 \ltimes C_3, & \text{if } j(C) = 0\,(= 12^3) \text{ and } \mathrm{char}(k) = 3; \\ C_3 \ltimes Q_8, & \text{if } j(C) = 0\,(= 12^3) \text{ and } \mathrm{char}(k) = 2. \end{cases}$$

Remark. Here C_n denotes a cyclic group of order n, and Q_8 a quaternion group of order 8. We use $\boldsymbol{\mu}_n(\bar{k})$ in place of C_n in the first three cases, as this furthermore indicates the Galois module structure of the group. But when $\mathrm{char}(k) = 2, 3$, that structure depends on more than just the j-invariant, and is not given here.

Proof. See [Sil99, III.10.1, III.10.2] and the proof of [Sil99, A.1.2c]. □

Corollary A.4.8. *Each elliptic curve $(C_{\bar{k}}, O)$ admits a unique automorphism of order 2 (usually denoted $[-1]$). Its fixpoints are the points of 2-torsion $(C_{\bar{k}}, O)[2](\bar{k})$, and if Q is one of those points, then the same automorphism is also the $[-1]$-automorphism of the elliptic curve $(C_{\bar{k}}, Q)$.*

Proof. The first statement follows from the theorem. The second statement follows from uniqueness. □

Theorem A.4.9. *Fix a choice of $O \in C(\bar{k})$. In $\mathrm{Aut}(C_{\bar{k}}) = \mathrm{J}_C(\bar{k}) \rtimes \mathrm{Aut}\big((C_{\bar{k}}, O)\big)$, the order 2 automorphism of $C_{\bar{k}}$ with a fixpoint are precisely the elements of the form $\tau \circ [-1]$, where $\tau \in \mathrm{J}_C[n](\bar{k})$, and $[-1]$ is the unique order 2 automorphism of the elliptic curve $(C_{\bar{k}}, O)$.*

Proof. By A.4.5, our automorphism is of the form $\tau \circ \phi$ for some $\tau \in \mathrm{J}_C(\bar{k})$ and some $\phi \in \mathrm{Aut}\big((C_{\bar{k}}, O)\big)$. From the semidirect product structure (cf. A.4.6), it is easy to see that $\tau \circ \phi$ having order 2 implies ϕ itself has order 2. Therefore, by A.4.8, our automorphism is of the form $\tau \circ [-1]$.

It remains to show that every $\tau \in \mathrm{J}_C(\bar{k})$ can occur. In other words, for an arbitrary such τ, we must show that $\tau \circ [-1]$ has order 2 and a fixpoint. Now $\tau = \tau_P$ (translation-by-P) for some $P \in C(\bar{k})$. Let $Q \in C(\bar{k})$ be such that $Q \oplus Q = P$, where the group law is on $(C_{\bar{k}}, O)$. Then $\big(\tau \circ [-1]\big)(Q) = P \ominus Q = Q$, and $\tau_P \circ [-1] \circ \tau_P \circ [-1] = \tau_P \circ \big([-1] \circ \tau_P \circ [-1]\big) \circ \big([-1] \circ [-1]\big) = \tau_P \circ \tau_{\ominus P} = \mathsf{id}$. □

A.4d. Separable and inseparable degree of a morphism

Theorem A.4.10. *Let $\phi\colon C \to C'$ be a finite morphism of curves of genus 1. Then for all $Q \in C'(\bar{k})$ and all $P \in C(\bar{k})$,*

$$\#\phi^{-1}(Q) = \operatorname{sep\,deg}\phi,$$
$$\mathrm{e}_\phi(P) = \operatorname{insep\,deg}\phi.$$

Proof. Fix arbitrary $O \in C(\bar{k})$ and set $O' = \phi(O)$. Then ϕ is a non-constant isogeny $(C, O) \to (C', O')$. Now apply [Sil99, III.4.10a]. □

A.4e. The degree and fixpoints of a curve endomorphism

For any morphism $\eta\colon C \to C$, let $\#\operatorname{Fix}(\eta)$ denote the number of fixpoints of η lying in $C(\bar{k})$. In A.4b we saw that, after fixing a choice $O \in C(\bar{k})$, each morphism $\eta\colon C \to C$ has a unique decomposition as an endomorphism of (C, O) followed by a pure translation:

$$\eta = \tau \circ \phi, \quad \text{where } \phi \in \operatorname{End}(C, O) \text{ and } \tau \in \mathrm{J}_C(\bar{k}).$$

How this decomposition relates to the existence of fixpoints was given in A.4.3.

Theorem A.4.11. *In the above decomposition, we have:*

$$\deg(\tau \circ \phi) = \deg(\phi),$$
$$\#\operatorname{Fix}(\tau \circ \phi) = \begin{cases} \#\operatorname{Fix}(\phi), & \text{if } \phi \neq \mathsf{id}; \\ \infty, & \text{if } \phi = \mathsf{id} \text{ and } \tau = \mathsf{id}; \\ 0, & \text{if } \phi = \mathsf{id} \text{ and } \tau \neq \mathsf{id}. \end{cases}$$

Proof. Since pure translations have degree 1, we have $\deg(\tau \circ \phi) = \deg(\phi)$. The rest of the proof concerns fixpoints. Letting "$\ominus$" refer to subtraction on the elliptic curve (C, O), we can certainly say that $\#\operatorname{Fix}(\tau \circ \phi)$ is the same as the number of points in $C(\bar{k})$ sent to O by the map $(\tau \circ \phi) \ominus \mathsf{id}$.

Lemma. *The map $(\tau \circ \phi) \ominus \mathsf{id}$ is finite precisely when $\phi \neq \mathsf{id}$. Otherwise $(\tau \circ \phi) \ominus \mathsf{id}$ is the constant map with image $\tau(O)$.*

Proof. Observe that the action of τ is simply addition by the point $\tau(O) \in C(\bar{k})$; that is, $\tau(P) = P \oplus \tau(O)$.

If $\phi = \mathsf{id}$, then $(\tau \circ \phi) \ominus \mathsf{id}$ takes $P \mapsto P \oplus \tau(O) \ominus P$, so that $(\tau \circ \phi) \ominus \mathsf{id}$ is constant with image $\tau(O)$.

If $\phi \neq \mathsf{id}$, then there exists a $P \in C(\bar{k})$ with $P \neq \phi(P)$. Then $(\tau \circ \phi) \ominus \mathsf{id}$ takes $P \mapsto \phi(P) \oplus \tau(O) \ominus P$, while it takes $O \mapsto \tau(O)$. The two images are distinct precisely because $\phi(P) \ominus P \neq O$. Thus $(\tau \circ \phi) \ominus \mathsf{id}$ is non-constant, whence finite. □

We now continue with the proof of the theorem. Agreeing that constant maps have degree 0, the number of points in $C(\bar{k})$ sent to O by the map $(\tau \circ \phi) \ominus \mathsf{id}$ is the same as its separable degree so long as the map either is finite or is constant with image away from O. But it is constant with image O only when $(\tau \circ \phi) = \mathsf{id}$. Thus we have shown:

$$\#\operatorname{Fix}(\tau \circ \phi) = \operatorname{sep\,deg}((\tau \circ \phi) \ominus \mathsf{id}) \quad \text{if } \tau \circ \phi \neq \mathsf{id}.$$

By observing that $(\tau \circ \phi) \ominus \mathsf{id}$ carries $P \mapsto \phi(P) \oplus \tau(O) \ominus P$, we see that the "$\oplus\tau(O)$" part does not affect the degree, whence

$$\#\operatorname{Fix}(\tau \circ \phi) = \operatorname{sep\,deg}(\phi \ominus \mathsf{id}) \quad \text{if } \tau \circ \phi \neq \mathsf{id}.$$

Of course, we also have $\#\operatorname{Fix}(\phi) = \operatorname{sep\,deg}(\phi \ominus \mathsf{id})$ so long as $\phi \neq \mathsf{id}$, and thus our final conclusion is

$$\#\operatorname{Fix}(\tau \circ \phi) = \#\operatorname{Fix}(\phi) \quad \text{if } \phi \neq \mathsf{id}.$$

Of course, when $\phi = \mathsf{id}$, then $\tau \circ \phi$ is a pure translation, so $\#\operatorname{Fix}(\tau \circ \phi)$ is either ∞ or 0, according as whether $\tau = \mathsf{id}$. □

A.4f. Correspondence between morphisms and subgroups of J_C

Let (E,O) be an elliptic k-curve, where k is a perfect field. For each finite subgroup $K \subset E(\bar{k})$ that is $\mathrm{Gal}(\bar{k}/k)$-stable, there is the non-constant separable k-isogeny

$$\eta_K \colon E \longrightarrow \frac{E}{K}.$$

These are essentially the only non-constant separable isogenies with domain E, in the following sense. Let (E',O') be another elliptic k-curve. Every non-constant separable k-isogeny $\eta\colon E \longrightarrow E'$ factors as the following composition of non-constant separable k-isogenies:

$$\eta\colon E \longrightarrow \frac{E}{\mathrm{Ker}(\eta)(\bar{k})} \xrightarrow{\sim} E'.$$

(See [Sil99, III.4.9, III.4.12].)

Of course, two different isogenies can have the same kernel (for example, consider $\mathsf{id}\colon E \to E$ and $[-1]\colon E \to E$), so one must be cautious in formulating the above in terms of a one-to-one correspondence. We see that non-constant separable k-isogenies $E \to E'$ are in one-to-one correspondence with pairs $(K, E/K \xrightarrow{\sim} E')$, where K is a finite $\mathrm{Gal}(\bar{k}/k)$-stable subgroup of $E(\bar{k})$, and $E/K \xrightarrow{\sim} E'$ is a k-isomorphism.

We can eliminate "perfect" and "separable" from this correspondence by appealing to the language of schemes. Let (E,O) be an elliptic k-curve, where k is now an arbitrary field. For each finite subgroup k-scheme $K \subset E$, there is the non-constant k-isogeny

$$\eta_K \colon E \longrightarrow \frac{E}{K}.$$

If (E',O') is another elliptic k-curve, then every non-constant k-isogeny $\eta\colon E \longrightarrow E'$ factors as the following composition of non-constant k-isogenies:

$$\eta\colon E \longrightarrow \frac{E}{\mathrm{Ker}(\eta)} \xrightarrow{\sim} E'.$$

We can generalize this correspondence to curves of genus 1 as follows. Let C be a k-curve of genus 1. For each finite subgroup k-scheme $K \subset \mathrm{J}_C$, there is the finite k-morphism

$$\eta_K \colon C \longrightarrow \frac{C}{K}.$$

If C' is another k-curve of genus 1, then every finite k-morphism $\eta\colon C \to C'$ factors as the following composition of finite k-morphisms:

$$\eta\colon C \longrightarrow \frac{C}{\mathrm{Ker}(\hat{\eta}^*)} \xrightarrow{\sim} C'.$$

Here $\mathrm{Ker}(\hat{\eta}^*)$ is the finite subgroup k-scheme of J_C whose $\bar{k}$-valued points are

$$\mathrm{Ker}(\hat{\eta}^*)(\bar{k}) = \big\{\, [P-Q] \in \mathrm{J}_C(\bar{k}) \,:\, P,Q \in C(\bar{k}) \text{ and } \eta(P) = \eta(Q) \,\big\}.$$

Under the action of J_C on C, this subgroup acts simply transitively on each fiber of η; in particular, one can compute $\mathrm{Ker}(\hat{\eta}^*)(\bar{k})$ by focusing on one fiber:

$$\mathrm{Ker}(\hat{\eta}^*)(\bar{k}) = \big\{\, [P-Q] \in \mathrm{J}_C(\bar{k}) \,:\, P,Q \in \eta^{-1}(R) \,\big\}.$$

Since $|\eta^{-1}(R)| = \mathrm{sep\,deg}(\eta)$, the number of closed points in $\mathrm{J}_C[\eta]$ is $\mathrm{sep\,deg}(\eta)$. Multiplicities account for the inseparable degree contribution.

Just as, with a non-constant k-isogeny $\eta\colon E \to E'$ of elliptic k-curves there is a natural isomorphism $\mathrm{Ker}(\eta)(\bar{k}) \cong \mathrm{Aut}\big(\bar{k}(E_{\bar{k}})/\eta^*\bar{k}(E'_{\bar{k}})\big)$, with a finite k-morphism $\eta\colon C \to C'$ of k-curves of genus 1 there is a natural isomorphism

$$\mathrm{Ker}(\hat{\eta}^*)(\bar{k}) \xrightarrow{\sim} \mathrm{Aut}\big(\bar{k}(C_{\bar{k}})/\eta^*\bar{k}(C'_{\bar{k}})\big).$$

Finally, the following statements are equivalent for a finite k-morphism $\eta\colon C \to C'$ of k-curves of genus 1 (cf. [Sil99, III.4.10]):

- η is separable;
- η is unramified;
- $\#\operatorname{Ker}(\hat{\eta}^*)(\bar{k}) = \deg \eta$;
- The field extension $\bar{k}(C_{\bar{k}})/\eta^*\bar{k}(C'_{\bar{k}})$ is Galois.

This leads to the following Galois correspondences when k is perfect:

- Finite subgroup k-schemes of J_C are in inclusion-preserving correspondence with $\mathrm{Gal}(\bar{k}/k)$-stable finite subgroups of $\mathrm{Aut}\big(\bar{k}(C_{\bar{k}})/\bar{k}\big)$.
- Either of the above sets is in inclusion-reversing correspondence with finite-index $\mathrm{Gal}(\bar{k}/k)$-stable subfields of $\bar{k}(C_{\bar{k}})$.

A.5. Consequences of Riemann–Hurwitz on curves of genus 1

We recall the Riemann–Hurwitz theorem for curves of arbitrary genus.

Theorem A.5.1 (Riemann–Hurwitz)**.** *For a finite separable morphism $\phi\colon X_1 \to X_2$ between smooth projective curves,*

$$2\ \mathrm{genus}(X_1) - 2 = \deg(\phi)\big(2\ \mathrm{genus}(X_2) - 2\big) + \deg(R),$$

where R is the ramification divisor of ϕ on X_1, which, if the ramification is tame, looks like:

$$R = \sum_{P \in X_1(\bar{k})} \big(e_\phi(P) - 1\big)P.$$

Proof. See [Har77, IV.2.4]. □

Theorem A.5.2. *If there exists a finite and purely inseparable morphism $X_1 \to X_2$ between smooth projective curves, then* $\mathrm{genus}(X_1) = \mathrm{genus}(X_2)$.

Proof. See [Har77, IV.2.5]. □

Corollary A.5.3. *If $\phi\colon X_1 \to X_2$ is a finite morphism between smooth projective curves, then*

$$2\ \mathrm{genus}(X_1) - 2 \le \operatorname{sep}\deg(\phi)\big(2\ \mathrm{genus}(X_2) - 2\big). \tag{A.1}$$

Proof. The morphism can be factored into a purely inseparable morphism followed by a separable morphism. Now apply the previous two theorems. □

Theorem A.5.4. *The existence of a finite morphism $X_1 \to X_2$ between smooth projective curves implies* $\mathrm{genus}(X_1) \ge \mathrm{genus}(X_2)$.

Proof. If $\mathrm{genus}(X_2) = 0$, then there is nothing to prove. Otherwise, the right-hand side of (A.1) is non-negative, so we can eliminate $\operatorname{sep}\deg(\phi)$ to obtain $2\ \mathrm{genus}(X_1) - 2 \ge 2\ \mathrm{genus}(X_2) - 2$, which immediately gives the desired result. □

We can draw three consequences from Riemann–Hurwitz for curves of genus 1:

(1) The only finite morphisms with domain a smooth projective curve of genus 1 are:
   - finite maps between curves of genus 1, and
   - finite maps to $\mathbf{P}^1$, i.e., non-constant rational functions.

(2) Separable finite morphisms between smooth projective curves of genus 1 are unramified.

(3) More generally, the total ramification of a separable finite morphism from a curve of higher genus to a curve of genus 1 is independent of the degree of the morphism; however, at least with tame ramification, lower degrees force a higher number of branch points.

APPENDIX B

Maps to projective space: a coordinate-free approach

Let X be a scheme over a ring A, and let $\mathcal{L}$ be an invertible sheaf on X.

As described in [HAR77, §II.7], if $\mathcal{L}$ is generated by global sections, then to each finite ordered collection $\mathcal{B} = (s_0, \ldots, s_n)$ of global generators corresponds a unique morphism

$$\phi_{\mathcal{B}} \colon X \longrightarrow \mathbf{P}^n_A \tag{B.1}$$

with the properties $\phi^*_{\mathcal{B}}\big(\mathcal{O}(1)\big) \cong \mathcal{L}$ and $\phi^*_{\mathcal{B}}(x_i) = s_i$, where the x_i are the homogeneous coordinates on $\mathbf{P}^n_A$. If the collection $\mathcal{B}$ is linearly independent, then the image of (B.1) is **non-degenerate**, meaning: it does not lie in a hyperplane of $\mathbf{P}^n_A$.

By the universal property of the fibre product $\mathbf{P}^n_X := \mathbf{P}^n_A \times_A X$, each morphism (B.1) factors canonically as a morphism

$$\phi_{\mathcal{B}} \colon X \longrightarrow \mathbf{P}^n_X \tag{B.2}$$

followed by the canonical projection $\mathbf{P}^n_X \to \mathbf{P}^n_A$.

Our goal is to give a coordinate-free description of the map $X \to \mathbf{P}^n_X$ and of the composed map $X \to \mathbf{P}^n_A$. To do so, we will require X and A to be noetherian, and we will furthermore require $\mathrm{H}^0(X, \mathcal{L})$ to be a free A-module of finite rank, or at least require a submodule of $\mathrm{H}^0(X, \mathcal{L})$ that generates $\mathcal{L}$ to have those properties. (By [HAR77, II.5.19], these requirements are met if A is a field and X is projective over A.)

B.1. Background material

B.1a. Projective space bundles

Let X be a noetherian scheme. Associated to each locally free coherent sheaf $\mathcal{E}$ on X is the projective space bundle

$$\pi \colon \mathbf{P}(\mathcal{E}) \longrightarrow X. \tag{B.3}$$

Let us recall its definition and properties (cf. [HAR77, §II.7, p.162]). The sheaf

$$\mathcal{S} := \mathrm{Sym}(\mathcal{E}) := \bigoplus_{d \geq 0} \mathrm{Sym}^d(\mathcal{E})$$

is a quasi-coherent sheaf of graded $\mathcal{O}_X$-algebras, where each homogeneous part $\mathcal{S}_d$ is coherent, $\mathcal{S}_0 \cong \mathcal{O}_X$, and $\mathcal{S}$ is locally generated by $\mathcal{S}_1 = \mathcal{E}$. Thus we are in the situation denoted "(†)" in [HAR77, §II.7, p.160], and by definition

$$\mathbf{P}(\mathcal{E}) := \mathbf{Proj}(\mathcal{S}).$$

In other words, for each affine open $U \subseteq X$, we have

$$\pi^{-1}(U) \cong \mathrm{Proj}\big(\mathrm{H}^0(U, \mathcal{S})\big) = \mathrm{Proj}\big(\mathrm{Sym}\big(\mathrm{H}^0(U, \mathcal{E})\big)\big).$$

Furthermore, $\mathbf{P}(\mathcal{E})$ comes equipped with an invertible sheaf $\mathcal{O}(1)$ and there is a canonical surjective morphism $\pi^*(\mathcal{E}) \to \mathcal{O}(1)$, thus exhibiting $\mathcal{O}(1)$ as a "rank 1 quotient" of $\pi^*(\mathcal{E})$. Finally, if everywhere on X we have $\mathrm{Rank}(\mathcal{E}) \geq 2$, then $\pi_*\big(\mathcal{O}(d)\big) \cong \mathcal{S}_d$; in particular, $\pi_*\big(\mathcal{O}(1)\big) \cong \mathcal{E}$. (See [HAR77, II.7.11].)

Points correspond to rank 1 *quotients.* One way to think about $\mathbf{P}(\mathcal{E})$ is in terms of its T-valued points, which turn out to correspond to certain rank 1 sheaf quotients. Let $g\colon T \to X$ be a T-valued point of X, which will remain fixed throughout this paragraph. If $f\colon T \to \mathbf{P}(\mathcal{E})$ is a T-valued point over X (i.e., $\pi \circ f = g$), then f^* carries the exact sequence

$$\pi^*(\mathcal{E}) \longrightarrow \mathcal{O}(1) \longrightarrow 0$$

to the exact sequence

$$g^*(\mathcal{E}) \longrightarrow f^*\big(\mathcal{O}(1)\big) \longrightarrow 0.$$

Note that f^* is not only right-exact: it also preserves invertibility. Therefore, each T-valued point of $\mathbf{P}(\mathcal{E})$ over X gives rise to a rank 1 quotient of $\mathcal{E}$ on T, and this turns out to be a one-to-one correspondence (see [Har77, II.7.12]), which is easily verified to be functorial. In particular, when we exhibit a rank 1 quotient

$$g^*(\mathcal{E}) \longrightarrow \mathcal{L} \longrightarrow 0,$$

the corresponding T-valued point $f\colon T \to \mathbf{P}(\mathcal{E})$ has the property

$$f^*\big(\mathcal{O}(1)\big) \cong \mathcal{L}. \tag{B.4}$$

Change of base. Projective space bundles behave well under change of base. Let $h\colon X' \to X$ be a morphism of noetherian schemes, and let $\mathcal{E}$ be a locally free coherent sheaf on X. We will now establish a morphism $\mathbf{P}(h^*\mathcal{E}) \to \mathbf{P}(\mathcal{E})$ so that the diagram shown here commutes. One way to describe a morphism of schemes is to view the schemes as functors (assigning to each T the set of T-valued points) and then to describe a natural transformation of those functors. Thus, for each T-valued point $f\colon T \to \mathbf{P}(h^*\mathcal{E})$, which immediately gives us the T-valued point $\pi_2 \circ f$ of X' and the T-valued point $h \circ \pi_2 \circ f$ of X, we must produce (in a functorial fashion) a T-valued point of $\mathbf{P}(\mathcal{E})$ lying over $h \circ \pi_2 \circ f$. By our correspondence between T-valued points and rank 1 quotients, f corresponds to

$$(\pi_2 \circ f)^*(h^*\mathcal{E}) \longrightarrow f^*\big(\mathcal{O}(1)\big) \longrightarrow 0.$$

Since the left term is isomorphic to $(h \circ \pi_2 \circ f)^*(\mathcal{E})$, the exhibited rank 1 corresponds to a T-valued point of $\mathbf{P}(\mathcal{E})$. It is furthermore not difficult (but left as an exercise for the reader) to establish that the diagram is cartesian:

$$\mathbf{P}(h^*\mathcal{E}) = \mathbf{P}(\mathcal{E}) \times_X X'. \tag{B.5}$$

Coordinates. If $\mathcal{E}$ has finite rank everywhere on X, then the projective space bundle $\mathbf{P}(\mathcal{E})$ may be locally coordinatized as follows. Let $U \subseteq X$ be an open set on which $\mathcal{E}$ is free and has constant finite rank, and set n so that the rank is $n+1$. Let $\mathcal{O}_U$ denote the restriction of $\mathcal{O}_X$ to U. Let $\mathcal{B} = \{\, s_0, \ldots, s_n \,\}$ be a basis of global sections establishing the isomorphism $\mathcal{E}|_U \cong \bigoplus^n \mathcal{O}_U$. Observe that $\operatorname{Sym}(\mathcal{E}|_U)$ is isomorphic, via the association $s_i \leftrightarrow x_i$, to the polynomial ring $\mathcal{O}_U[x_0, \ldots, x_n]$; thus, $\mathbf{P}(\mathcal{E}|_U) \cong \mathbf{P}^n_U$, and the structure map $\pi\colon \mathbf{P}(\mathcal{E}|_U) \to U$ is then simply the canonical projection $\mathbf{P}^n_U \to U$. Of course, if $\mathcal{E}$ is globally free, then a single such coordinatization works for the entire projective space bundle.

B.1b. Starting with a free A-module

Let X be a noetherian scheme over a noetherian ring A. If V is a free module of finite rank $n+1$ over A, then $\mathcal{E} := V \otimes_A \mathcal{O}_X$ is a locally free coherent sheaf of rank $n+1$ on X. Here $V \otimes_A \mathcal{O}_X$ denotes the sheaf whose sections over an open set $U \subseteq X$ are $V \otimes_A \mathrm{H}^0(U, \mathcal{O}_X)$. (We view $\mathrm{H}^0(U, \mathcal{O}_X)$ as an A-module as follows: via restriction it is certainly a module over $\mathrm{H}^0(X, \mathcal{O}_X)$, and there is an obvious map $A \to \mathrm{H}^0(X, \mathcal{O}_X)$ associating to each $a \in A$ the corresponding constant function.) Similarly, $V \otimes_A \mathcal{O}_A$ is a locally free coherent sheaf of rank $n+1$ on $\operatorname{Spec}(A)$. Observe

$$V \otimes_A \mathcal{O}_X \cong s^*(V \otimes_A \mathcal{O}_A), \tag{B.6}$$

where $s\colon X \to \operatorname{Spec}(A)$ is the structure map.

In fact, both $V \otimes_A \mathcal{O}_A$ and $V \otimes_A \mathcal{O}_X$ are globally free, whence they may be globally coordinatized. They can both be coordinatized simultaneously by choosing a basis $\mathcal{B} = \{ s_0, \dots, s_n \}$ for V. Then the symbols $s_i \otimes 1$ compose a basis of global generators both for $V \otimes_A \mathcal{O}_A$ and for $V \otimes_A \mathcal{O}_X$.

In summary, we always have the commutative diagram

$$\begin{array}{ccccc} X & \xleftarrow{\pi} & \mathbf{P}(V \otimes_A \mathcal{O}_X) & \xleftarrow{\sim_{\mathcal{B}}} & \mathbf{P}^n_X \\ \downarrow{\scriptstyle s} & & \downarrow & & \downarrow \\ \operatorname{Spec}(A) & \longleftarrow & \mathbf{P}(V \otimes_A \mathcal{O}_A) & \xleftarrow{\sim_{\mathcal{B}}} & \mathbf{P}^n_A, \end{array}$$

where $\sim_{\mathcal{B}}$ indicates the isomorphism associated to a choice of basis $\mathcal{B}$ for V. By (B.6) and (B.5), describing an X-morphism $X \to \mathbf{P}(V \otimes_A \mathcal{O}_X)$, i.e., a section of π, is equivalent to describing an A-morphism $X \to \mathbf{P}(V \otimes_A \mathcal{O}_A)$.

B.1c. When the base is a field

When the base ring A is a field k, and K is a field extension of k, the following nice description of K-valued points of $\mathbf{P}(V)$ is useful. (Since $\operatorname{Spec}(k)$ has just a single point, the sheaf $V \otimes_k \mathcal{O}_{\operatorname{Spec}(k)}$ is just the constant sheaf associated to V, so we might as well use V to denote both the vector space and the sheaf.)

Let X be a noetherian scheme over k. Let V be as before: a free k-module of finite rank $n+1$. Fix a field extension $K \supseteq k$; in other words, choose a K-valued point $g\colon \operatorname{Spec}(K) \to \operatorname{Spec}(k)$. We already know that a K-valued point of $\mathbf{P}(V)$ lying over g is nothing other than a rank 1 sheaf quotient of the sheaf g^*V. But $\operatorname{Spec}(K)$ has a single point, so such a quotient amounts to a rank 1 vector space quotient of the vector space $V \otimes_k K$. This puts us squarely in the realm of linear algebra. By considering the kernel of a rank 1 quotient map, we see that rank 1 quotients are in one-to-one correspondence with hyperplanes. In summary, *the K-valued points of $\mathbf{P}(V)$ are the hyperplanes in $V \otimes_k K$.*

B.2. Coordinate-free version of $X \to \mathbf{P}^n_X$

Let X be a noetherian scheme over a noetherian ring A, and let $\mathcal{L}$ be an invertible sheaf on X that is generated by global sections. Viewing $\mathrm{H}^0(X, \mathcal{L})$ as an A-module, let $V \subseteq \mathrm{H}^0(X, \mathcal{L})$ be a submodule with the following properties:

- V generates $\mathcal{L}$;
- V is a free A-module of finite rank.

We claim that, under these assumptions, the projective space bundle

$$\pi\colon \mathbf{P}(V \otimes_A \mathcal{O}_X) \longrightarrow X.$$

has a canonical section

$$\phi_V\colon X \longrightarrow \mathbf{P}(V \otimes_A \mathcal{O}_X); \tag{B.7}$$

furthermore, there is a canonical isomorphism $\phi_V^*\big(\mathcal{O}(1)\big) \cong \mathcal{L}$, and if we choose a basis $\mathcal{B} = \{ s_0, \dots, s_n \}$ for V, whence $\mathbf{P}(V \otimes_A \mathcal{O}_X) \cong \mathbf{P}^n_X$, then we obtain the original map (B.2) described at the outset.

Before establishing the claim, let us remark on consequences. If we compose (B.7) with $\mathbf{P}(V \otimes_A \mathcal{O}_X) \to \mathbf{P}(V \otimes_A \mathcal{O}_A)$, we end up with

$$\phi_V\colon X \longrightarrow \mathbf{P}(V \otimes_A \mathcal{O}_A). \tag{B.8}$$

Under the basis $\mathcal{B}$, (B.8) recovers the original map (B.1). Since (B.1) pulls back an A-basis of $\mathrm{H}^0\big(\mathbf{P}^n_A, \mathcal{O}(1)\big)$ to an A-basis of $\mathrm{H}^0(X, \mathcal{L})$, pullback must give a canonical isomorphism of A-modules

$$\mathrm{H}^0\big(\mathbf{P}(V \otimes_A \mathcal{O}_A), \mathcal{O}(1)\big) \cong \mathrm{H}^0(X, \mathcal{L}). \tag{B.9}$$

In particular, the image of (B.8) is **non-degenerate**, meaning: it does not lie in a hyperplane. That is, no nonzero global section of $\mathcal{O}(1)$ vanishes identically on X.

Example. When A is a field k, X is a curve, and ϕ_V is the map associated to $V = \mathrm{H}^0\big(C, \mathcal{O}(D)\big)$, where D is a divisor on X, (B.9) says: equations for hyperplanes in $\mathbf{P}(V)$ are in one-to-one correspondence with $\big\{\, f \in k(X) \,:\, (f) + D \geq 0 \,\big\}$. This leads to a familiar fact: if we remove 0 from each vector space in (B.9) and then work modulo $k^\times$, classes on the left correspond to hyperplanes, while classes on the right correspond to **hyperplane sections**: effective divisors linearly equivalent to D. In short, (B.9) establishes a one-to-one correspondence between hyperplanes and hyperplane sections. When ϕ_V is an embedding, the correspondence is simply $H \mapsto H \cap X$; in general, one must instead choose an equation ℓ defining H, pull back ℓ to obtain a rational function $\phi_V^*\ell$ on X, and finally take the divisor of $\phi_V^*\ell$.

Proof of claim. We start by describing (B.7). Given a T-valued point $g\colon T \to X$, we must produce (in a functorial fashion) a T-valued point $T \to \mathbf{P}(V \otimes_A \mathcal{O}_X)$. We saw earlier that this is the same as producing a rank 1 quotient of $g^*(V \otimes_A \mathcal{O}_X)$. To do this, we simply apply g^* to the given rank 1 quotient $V \otimes_A \mathcal{O}_X \to \mathcal{L} \to 0$ on X. (The map $V \otimes_A \mathcal{O}_X \to \mathcal{L}$ is described as follows. To each global section $s \in V$ corresponds the morphism $\mathcal{O}_X \to \mathcal{L}$ defined by $f \mapsto f \cdot s$. Given a pair (s, f), where $s \in V$ and $f \in \mathrm{H}^0(U, \mathcal{O}_X)$, we "evaluate" s on f to obtain $f \cdot s \in \mathrm{H}^0(U, \mathcal{L})$. This pairing is bilinear and thus gives the map in question. It is surjective precisely because V generates $\mathcal{L}$.)

Having described (B.7), we now establish $\phi_V^*\big(\mathcal{O}(1)\big) \cong \mathcal{L}$. To do so, we again appeal to the description of ϕ_V as a natural transformation of scheme functors. For each T-valued point $g\colon T \to X$, we must establish an isomorphism of sheaves

$$g^*(\mathcal{L}) \cong \phi_V(g)^*\big(\mathcal{O}(1)\big).$$

The map $\phi_V(g)$ corresponds to the rank 1 quotient $g^*(V \otimes_A \mathcal{O}_X) \to g^*(\mathcal{L}) \to 0$, and thus, by (B.4), the pullback of $\mathcal{O}(1)$ is indeed isomorphic to $g^*(\mathcal{L})$.

Finally, to see that a choice of basis $\mathcal{B} = \{\, s_0, \ldots, s_n \,\}$ for V leads to our original map (B.2), it remains to verify, by the characterizing properties stated after (B.1), that the sections x_i in $\mathcal{O}(1)$ on $\mathbf{P}^n_A$ pull back to the sections s_i on X. We are looking at the composition

$$X \xrightarrow{\phi_V} \mathbf{Proj}\big(\mathrm{Sym}(V \otimes_A \mathcal{O}_X)\big) \xrightarrow{\mathcal{B}} \mathbf{Proj}\big(\mathcal{O}_X[x_0, \ldots, x_n]\big) = \mathbf{P}^n_X.$$

Under pullback, x_i on $\mathbf{P}^n_X$ corresponds to $s_i \otimes 1$ on $\mathbf{Proj}\big(\mathrm{Sym}(V \otimes_A \mathcal{O}_X)\big)$, which in turn corresponds to s_i on X. □

When A is a field k, (B.8) has an elegant description in terms of K-valued points, where K is a field extension of k. We already know that a fixed K-valued point $g\colon \mathrm{Spec}(K) \to X$ goes to the rank 1 quotient

$$g^*(V \otimes_k \mathcal{O}_X) \longrightarrow g^*\mathcal{L} \longrightarrow 0,$$

which gives a point on $\mathbf{P}(V \otimes_k \mathcal{O}_X)$. Under $\mathbf{P}(V \otimes_k \mathcal{O}_X) \to \mathbf{P}(V)$, that point goes to the rank 1 quotient

$$(s \circ g)^*(V) \longrightarrow g^*\mathcal{L} \longrightarrow 0,$$

which is a point on $\mathbf{P}(V)$, where s is the structure map $X \to \mathrm{Spec}(k)$. Since $\mathrm{Spec}(k)$ has a single point, the data of $(s \circ g)^*(V)$ is simply the K-vector space $V \otimes_k K$. (Cf. B.1c.) The kernel of

$$V \otimes_k K \longrightarrow g^*\mathcal{L}$$

is the hyperplane of all elements in $V \otimes_k K$ that map to 0 in the fiber of $\mathcal{L}$ above the point of X hit by g. *In short, ϕ_V carries the K-valued point g to the hyperplane of sections of $\mathcal{L}$ that vanish at g.* Therefore, it is not uncommon to see (B.8) described solely in the following terms:

$$\begin{aligned} \phi_V\colon X(K) &\longrightarrow \mathbf{P}(V)(K), \\ P &\longmapsto \{\, s \in V \otimes_k K \,:\, s_P = 0 \,\}. \end{aligned}$$

B.3. Mapping properties

Perhaps surprising at first, it is in general difficult, as we'll see below, to extend morphisms between schemes, or between sheaves, to morphisms between projective space bundles.

B.3a. Morphism of schemes

Let $f\colon X' \to X$ be a morphism of noetherian schemes over a noetherian ring A. If $\mathcal{L}$ is an invertible sheaf on X that is generated by global sections and such that $\mathrm{H}^0(X, \mathcal{L})$ is a free A-module of finite rank $n+1$, then $f^*\mathcal{L}$ is an invertible sheaf on X' that is generated by global sections, but $\mathrm{H}^0(X', f^*\mathcal{L})$ could have much larger rank. It would be nice if there existed maps f_* giving a commutative diagram:

$$\begin{array}{ccccc} X' & \xrightarrow{\phi_{f^*\mathcal{L}}} & \mathbf{P}\big(\mathrm{H}^0(X', f^*\mathcal{L}) \otimes_A \mathcal{O}_{X'}\big) & \longrightarrow & \mathbf{P}\big(\mathrm{H}^0(X', f^*\mathcal{L}) \otimes_A \mathcal{O}_A\big) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f_*} \\ X & \xrightarrow{\phi_{\mathcal{L}}} & \mathbf{P}\big(\mathrm{H}^0(X, \mathcal{L}) \otimes_A \mathcal{O}_X\big) & \longrightarrow & \mathbf{P}\big(\mathrm{H}^0(X, \mathcal{L}) \otimes_A \mathcal{O}_A\big) \end{array}$$

But there do not exist non-constant morphisms from a higher-dimensional projective space to a lower-dimensional one (see [Har77, Ex. II.7.3a]), whence a necessary condition for the existence of f_* is that $\mathrm{H}^0(X', f^*\mathcal{L})$ be a free A-module of rank $n+1$. By applying the correspondence between T-valued points and rank 1 quotients, one can check that existence of the f_* follows if the map

$$f^*\big(\mathrm{H}^0(X, \mathcal{L}) \otimes_A \mathcal{O}_X\big) \longrightarrow \mathrm{H}^0(X', f^*\mathcal{L}) \otimes_A \mathcal{O}_{X'}$$

of sheaves on X' is surjective. This gives a sufficient condition.

The one easy thing we can say is this: if f is an *isomorphism* of schemes, then we do obtain the maps f_*, and they will then also themselves be isomorphisms.

B.3b. Morphism of sheaves

Here it turns out, again, that we can't make a useful general statement. Let X be a noetherian scheme over a noetherian ring A. Let $f\colon \mathcal{L} \to \mathcal{L}'$ be a morphism of invertible sheaves on X, where both sheaves are generated by their global sections, and where both $\mathrm{H}^0(X, \mathcal{L})$ and $\mathrm{H}^0(X, \mathcal{L}')$ are free A-modules of finite rank (not necessarily the same rank). It would be nice if there existed a map f^* giving a commutative diagram:

$$\begin{array}{ccc} X & \longrightarrow & \mathbf{P}\big(\mathrm{H}^0(X, \mathcal{L}) \otimes_A \mathcal{O}_A\big) \\ \| & & \uparrow{\scriptstyle f^*} \\ X & \longrightarrow & \mathbf{P}\big(\mathrm{H}^0(X, \mathcal{L}') \otimes_A \mathcal{O}_A\big) \end{array}$$

To be able to define such a map f^*, we would need the induced map $\mathrm{H}^0(X, \mathcal{L}) \to \mathrm{H}^0(X, \mathcal{L}')$ to be surjective; otherwise we cannot guarantee that rank 1 quotients go to rank 1 quotients. But then f itself would be surjective, so by [Har77, Ex. II.7.1], f was an isomorphism to begin with. In summary, all we have been able to say here is the following: *if $f\colon \mathcal{L} \xrightarrow{\sim} \mathcal{L}'$ is an isomorphism of sheaves on X, then there is an induced commutative diagram as shown above, where f^* is an isomorphism.*

B.3c. Different subspaces of $\mathrm{H}^0(X, \mathcal{L})$

Let X be a noetherian scheme over a noetherian ring A, and let $\mathcal{L}$ be an invertible sheaf on X. If we have submodules $V \subseteq V' \subseteq \mathrm{H}^0(X, \mathcal{L})$, where V generates $\mathcal{L}$ (whence also V' generates $\mathcal{L}$), and both V and V' are free and of finite rank (generally not the same rank) as modules over A, then the inclusion map $V \to V'$ leads to a projection map

$$\mathbf{P}(V' \otimes_A \mathcal{O}_A) \dashrightarrow \mathbf{P}(V \otimes_A \mathcal{O}_A).$$

Note that the projection is not defined everywhere; however, it is defined at all points in the image of $\phi_{V'}$. If $\mathcal{B}$ is a basis for V and $\mathcal{B}'$ a basis for V' such that $\mathcal{B} \subseteq \mathcal{B}'$, and we use these bases to coordinatize the projective space bundles, then the projection displayed above becomes a usual

projection between projective spaces in which certain homogeneous coordinates are simply dropped.

$$\begin{array}{ccccc} X & \xrightarrow{\phi_{V'}} & \mathbf{P}(V') & \xrightarrow{\sim_{\mathcal{B}'}} & \mathbf{P}_A^{\mathrm{Rank}(V')} \\ \| & & \vdots & & \vdots \\ X & \xrightarrow{\phi_V} & \mathbf{P}(V) & \xrightarrow{\sim_{\mathcal{B}}} & \mathbf{P}_A^{\mathrm{Rank}(V)} \end{array}$$

B.4. Very ample invertible sheaves

Let X be a noetherian scheme over a noetherian ring A. To each invertible sheaf $\mathcal{L}$ that is generated by global sections and such that $\mathrm{H}^0(X, \mathcal{L})$ is a free A-module of finite rank $n+1$, we have associated the map

$$\phi\colon X \longrightarrow \mathbf{P}\big(\mathrm{H}^0(X, \mathcal{L}) \otimes_A \mathcal{O}_A\big).$$

We say that $\mathcal{L}$ is **very ample relative to** A when ϕ is an immersion. (Note that the map to $\mathbf{P}\big(\mathrm{H}^0(X, \mathcal{L}) \otimes_A \mathcal{O}_X\big)$ is *always* an immersion, so $\mathcal{L}$ is always very ample relative to X itself.)

If we forget about $\mathcal{L}$ and instead start with an immersion $\phi\colon X \to \mathbf{P}_A^n$, then $\phi^*\big(\mathcal{O}(1)\big)$ will be an invertible sheaf on X that is very ample relative to A. (After all, the map to projective space associated with $\phi^*\big(\mathcal{O}(1)\big)$ is easily seen to be ϕ itself.)

Bibliography

[ABD+64] M. Artin, J. E. Bertin, M. Demazure, P. Gabriel, A. Grothendieck, M. Raynaud, and J.-P. Serre. *Schémas en groupes. Fasc. 1: Exposés 1 à 4*. Institut des Hautes Études Scientifiques, Paris, 1963/1964.

[AKM+01] Sang Yook An, Seog Young Kim, David C. Marshall, Susan H. Marshall, William G. McCallum, and Alexander R. Perlis. Jacobians of genus one curves. *J. Number Theory*, 90(2):304–315, 2001.

[And] Greg W. Anderson. Lacunary wronskians on genus one curves. Preprint available from `http://www.math.umn.edu/~gwanders/`.

[And02] Greg W. Anderson. Abeliants and their application to an elementary construction of Jacobians. *Adv. Math.*, 172(2):169–205, 2002.

[BBB+00] C. Batut, K. Belabas, D. Benardi, H. Cohen, and M. Olivier. *PARI/GP, Version 2.1.5*. Bordeaux, 2000. available from `http://pari.math.u-bordeaux.fr/`.

[BS92] Dave Bayer and Mike Stillman. Computation of Hilbert functions. *J. Symbolic Comput.*, 14(1):31–50, 1992.

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner bases*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[Cal92] Chris Caldwell. A generalization of a result of Hurwitz and Mordell on the torsion subgroups of certain elliptic curves. *Rocky Mountain J. Math.*, 22(1):93–108, 1992.

[Cas60] J. W. S. Cassels. Arithmetic on curves of genus 1. II. A general result. *J. Reine Angew. Math.*, 203:174–208, 1960.

[Cas62] J. W. S. Cassels. Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups. *Proc. London Math. Soc. (3)*, 12:259–296, 1962.

[Cas91] J. W. S. Cassels. *Lectures on elliptic curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[CLO98] David Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.

[Con92] Ian Connell. Addendum to a paper of K. Harada and M.-L. Lang: "Some elliptic curves arising from the Leech lattice" [J. Algebra **125** (1989), no. 2, 298–310; MR 90g:11072]. *J. Algebra*, 145(2):463–467, 1992.

[Cre] John Cremona. mwrank 16Apr2004. available from `http://www.maths.nott.ac.uk/personal/jec/`.

[DHS98] Wolfram Decker, Agnes Eileen Heydtmann, and Frank-Olaf Schreyer. Generating a Noetherian normalization of the invariant ring of a finite group. *J. Symbolic Comput.*, 25(6):727–731, 1998.

[Dol82] Igor Dolgachev. Weighted projective varieties. In *Group actions and vector fields (Vancouver, B.C., 1981)*, volume 956 of *Lecture Notes in Math.*, pages 34–71. Springer, Berlin, 1982.

[Eis95] David Eisenbud. *Commutative algebra*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry.

[Fis] Tom Fisher. Invariants of the elliptic normal quintic. To appear.

[GPS01] G.-M. Greuel, G. Pfister, and H. Schönemann. Singular 2.0.4. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2001. `http://www.singular.uni-kl.de/`.

[GS] Daniel R. Grayson and Michael E. Stillman. Macaulay 2, a software system for research in algebraic geometry. Available at `http://www.math.uiuc.edu/Macaulay2/`.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[Har95] Joe Harris. *Algebraic geometry*. Springer-Verlag, New York, 1995. A first course, Corrected reprint of the 1992 original.

[Hul86] Klaus Hulek. Projective geometry of elliptic curves. *Astérisque*, (137):143, 1986.

[Kem96] Gregor Kemper. Calculating invariant rings of finite groups over arbitrary fields. *J. Symbolic Comput.*, 21(3):351–366, 1996.

[MSS96] J. R. Merriman, S. Siksek, and N. P. Smart. Explicit 4-descents on an elliptic curve. *Acta Arith.*, 77(4):385–404, 1996.

[Mum70] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[O'N01] Catherine O'Neil. Jacobians of genus one curves. *Math. Res. Lett.*, 8(1-2):125–140, 2001.

[Sel51] Ernst S. Selmer. The Diophantine equation $ax^3+by^3+cz^3=0$. *Acta Math.*, 85:203–362 (1 plate), 1951.

[Sil99] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York, 199? Corrected reprint of the 1986 original.

[Stu93] Bernd Sturmfels. *Algorithms in invariant theory*. Springer-Verlag, Vienna, 1993.

[VT] Fernando Rodriguez Villegas and John Tate. Jacobian of plane cubics. In preparation.

[Wei54] André Weil. Remarques sur un mémoire d'Hermite. *Arch. Math.*, 5:197–202, 1954.

[Wol03] Wolfram Research, Inc. Mathematica 5.0.1, 2003. `http://www.wolfram.com/`.